ThinManager 14.1 Thin Client Management Platform

Catalog Number 9541

Allen-Bradley
by ROCKWELL AUTOMATION

User Manual

Original Instructions

Important User Information

Read this document and the documents listed in the additional resources section about installation, configuration, and operation of this equipment before you install, configure, operate, or maintain this product. Users are required to familiarize themselves with installation and wiring instructions in addition to requirements of all applicable codes, laws, and standards.

Activities including installation, adjustments, putting into service, use, assembly, disassembly, and maintenance are required to be carried out by suitably trained personnel in accordance with applicable code of practice.

If this equipment is used in a manner not specified by the manufacturer, the protection provided by the equipment may be impaired.

In no event will Rockwell Automation, Inc. be responsible or liable for indirect or consequential damages resulting from the use or application of this equipment.

The examples and diagrams in this manual are included solely for illustrative purposes. Because of the many variables and requirements associated with any particular installation, Rockwell Automation, Inc. cannot assume responsibility or liability for actual use based on the examples and diagrams.

No patent liability is assumed by Rockwell Automation, Inc. with respect to use of information, circuits, equipment, or software described in this manual.

Reproduction of the contents of this manual, in whole or in part, without written permission of Rockwell Automation, Inc., is prohibited.

Throughout this manual, when necessary, we use notes to make you aware of safety considerations.

WARNING: Identifies information about practices or circumstances that can cause an explosion in a hazardous environment, which may lead to personal injury or death, property damage, or economic loss.

ATTENTION: Identifies information about practices or circumstances that can lead to personal injury or death, property damage, or economic loss. Attentions help you identify a hazard, avoid a hazard, and recognize the consequence.

IMPORTANT Identifies information that is critical for successful application and understanding of the product.

These labels may also be on or inside the equipment to provide specific precautions.

SHOCK HAZARD: Labels may be on or inside the equipment, for example, a drive or motor, to alert people that dangerous voltage may be present.

BURN HAZARD: Labels may be on or inside the equipment, for example, a drive or motor, to alert people that surfaces may reach dangerous temperatures.

ARC FLASH HAZARD: Labels may be on or inside the equipment, for example, a motor control center, to alert people to potential Arc Flash. Arc Flash will cause severe injury or death. Wear proper Personal Protective Equipment (PPE). Follow ALL Regulatory requirements for safe work practices and for Personal Protective Equipment (PPE).

The following icon may appear in the text of this document.

Identifies information that is useful and can help to make a process easier to do or easier to understand.

Preface

About This Publication 11
Download Firmware, AOP, EDS, and Other Files 11
Summary of Changes. 11
Additional Resources 11

Chapter 1

Quick Setup Overview

Microsoft 13
ThinManager 13
- Installation & Activation 13
- ThinManager Database Encryption 14
- Configuration 18

Network 19
- VLANs and Subnets 19
- Network Level Authentication (NLA) 19

Hardware Introduction. 20
Results 20

Chapter 2

Introduction

ThinManager User Access 22
Location Services 23
ThinManager Interface 23
- Menus 25
- Customizing the Toolbar 29
- Icons 30
- Terminals 31
- Display Servers 32

ThinManager Web Browser User Interface 37

Chapter 3

Licenses

ThinManager Master License 41
- ThinManager Redundancy 42
- Auto-synchronization for Redundancy 42
- Manual Synchronization for Redundancy 45
- Synchronization Certificate Authentication 47
- ThinManager License Process 48

FactoryTalk Activations 51
- FactoryTalk Activation Files 51

Chapter 4

ThinManager System

Windows Users 55
ThinManager Security Group Users. 55
ThinManager Users 55
- ThinManager User Manual Unlock 56

TLS Certificates 59
API 60

Chapter 5

Sources

Remote Desktop Servers 61
Microsoft Configuration 61
Defining Remote Desktop Servers in ThinManager 61
Remote Desktop Server Graph 72
Remote Desktop Server Status 73
Remote Desktop Server Group 77
Containers 83
Containers on Thin Clients 84
Terminal Profile Setup for Containers 88
Optix Container 90
Containers on Servers using Windows Server 2019 99
Container Host Server Installation 100
Install Container Images 102
Define the Container Host Display Server 104
Define the Container Host Display Client 105
Apply the Container Display Client to a Terminal 109
Install the TLS Certificates 110
IP Cameras 114
Configure the IP Camera 115
Define the IP Camera as a Display Server 115
IP Camera 117
Define the USB Camera as a Display Server 119
VNC Servers 122
Workstations 123
VCenter Servers 125
Snapshots 127
Adding a Virtual Server 129

Chapter 6

Content

Remote Desktop Services Display Clients 133
Desktop 134
Single Application Deployment with AppLink 141
Connection Options 151
Failover 161
Instant Failover 164
Camera Display Clients 165
Camera Overlay Template 167
Terminal Shadow 172
Shadow Any Terminal 172
Shadow a Specific Terminal 172
Shadow of the Terminal 172
Workstation Deployment 172
Step 1 – On the PC 172
Step 2 – Workstation Display Client 172
Add the Workstation Display Client to the Terminal 172

VNC Shadow 172
Shadow Any VNC Server 172
Shadow a Specific VNC Server 172
Virtual Screens 172
Virtual Screen Display Client Wizard 172
Predefined Templates 172
Add a Virtual Screen to a Terminal 172
Custom Overlays 172
Display Client Override on Virtual Screens 172
Terminal Shadow 181
Shadow Any Terminal 181
Shadow a Specific Terminal 184
Shadow of the Terminal 187
Workstation Deployment 190
Step 1 – On the PC 190
Step 2 – Workstation Display Client 192
Add the Workstation Display Client to the Terminal 195
VNC Shadow 200
Shadow Any VNC Server 200
Shadow a Specific VNC Server 202
Virtual Screens 205
Virtual Screen Display Client Wizard 205
Predefined Templates 208
Add a Virtual Screen to a Terminal 213
Custom Overlays 216
Display Client Override on Virtual Screens 226

Chapter 7

Devices

Terminal Configuration 231
Terminal Configuration Wizard in ThinManager 231
Active Directory User Login Account 257
Search for Active Directory User 257
Search for Active Directory Location 258
User Accounts in the Terminal Configuration Wizard 261
Copy Settings from another Terminal 273
Use Groups for Organization 275
Use Groups for Configuration 279
IP Configuration 289
ThinManager-ready Thin Client IP Configuration 290
Add and Configure Thin Clients 295
PXE Server and PXE Boot 296
Secure Boot 309
Local WinTMC Configuration 309
WinTMC Configuration in ThinManager 312
Mobile Devices 315
Configure an iOS Device in ThinManager 316
Guided Access on the iOS Device 327
Configure an Android Device 330
Configure a Windows Device 331

Chapter 8

ThinManager Users

Introduction. 333
ThinManager User Services Introduction 333
Permission-deployed Applications in ThinManager 335
Permission-deployed Applications Diagrams 335
ThinManager Access Group Creation 338
Add Access Group to a Display Client 341
Configure Terminals for Location Services 343
Create the ThinManager User without a Windows Account 347
Location Services Results 350
Log On to Location Services 351
Log Out of Location Services 354
Assign Roaming Display Clients to a ThinManager User 355
Roaming Display Clients in Location Services Diagrams 355
Create the ThinManager User via Active Directory 357
ThinManager Configuration Wizard 362
Add User-specific Display Clients 365
Log On with a ThinManager User Account 370
Log Out of Location Services 373
Roaming Applications for Non-domain Users 374
ThinManager User Groups 381
Add a ThinManager User to a ThinManager User Group 386
Batch Create ThinManager Users using Active Directory OU 389
Password and Account Management 393
Active Directory 393
Shortcut Method to Add Access Groups 401
ThinManager User Schedule 403
Card Readers and Fingerprint Scanners 406
Card and Badge Configuration for a ThinManager User 406
Fingerprint Reader 417
Location Services 426
Create a Location with the Location Configuration Wizard 427
Add a Location to a Terminal 435
Mobile Device Interactions with Location Services 440

Chapter 9

Locations

Unassigned Locations 443
Create an Unassigned Location 443
Fencing and Sub-Locations 449
Child Sub-locations 453
ThinManager User Access 457
Create a Location with Restricted Applications 458
Use Permissions to Restrict an Application 458
Add a Restricted Application to a Location 460
Put It Together 463
One QR Code, Multiple Actions 466
Calculate Permissions 469
Manual Interaction with Locations 471
Shadow 473

Transfer. 476
Transfer at the Location 478
Clone 480
Addition of Resolver Codes with Mobile Device 483
Assignment of Resolvers 483
Register QR Codes with an Android Device. 487
Bluetooth Beacons 490
Relevance Settings. 491
Bluetooth Beacons Defined on an iPad. 492
Bluetooth Beacons Defined on an Android 496
Wi-Fi Access Points 501
iPad-defined Wi-Fi Access Points 501
Android-defined Wi-Fi Access Points 504
GPS. 508
iPad-Registered GPS 508
Android-registered GPS 512
Add Actions to Resolver Codes 515
Interact with the Location 518
Shadow 520
Forced Transfer. 521
Transfer. 525
Clone 529

Chapter 10

Events

Create a ThinManager Event 533

Chapter 11

Packages

Firmware, Packages, and Modules 537
Update Packages and Files. 538
Customizing Packages 540
Configure Packages for a Model of Thin Client. 544
Configure Packages for an Individual Thin Client 546

Chapter 12

Modules

Module List. 549
Add a Module. 552
Individual Module Details 554
ICA Modules 554
Keyboard Modules 555
Key Block Module. 555
Key Block Single Key Module 555
Keyboard Configuration Module 556
On-Screen Keyboard Module 556
RF Ideas pcProx USB Module 557
Share Keyboard and Mouse Module 557
Language Modules 558
Language Selection Module. 558
Local Storage Modules. 558

USB Flash Drive Module. 559
USB Memory Card Reader Module 559
BootAssist 560
Miscellaneous Modules 566
Add Serial Port 566
Barcode Configuration Module 567
Bluetooth Module 567
Firmware Update Module 567
Instant Failover Module 568
Local Print Module. 569
MultiStation Configuration Module 569
Redundant Ethernet Module 569
Terminal Shadow Module 570
TermMon ActiveX Configuration Module 570
Time Zone Redirection Module 570
TMTerm DLL Configuration Module 571
USB to Serial Module 571
User Override Module. 571
Mouse Modules 572
Locate Pointer Module 572
Mouse Configuration Module. 572
PS/2 Mouse Module. 573
Serial Mouse Driver. 573
Share Keyboard and Mouse Modules 573
Network Modules 573
Domain Name System Module. 573
Network Time Protocol Module 574
Second Network Module 574
Third Network Module 575
RDP Modules 575
RDP Experience Module 575
RDP Port Module 575
RDP Serial Port Redirection Module. 575
RDP Session IP Module 576
Smart Card Module. 576
Relevance Modules 576
Bluetooth Module 576
iPhone Beacon 579
DigitalPersona UareU Fingerprint Reader 579
RF Ideas pcProx Modules. 580
TermMon ActiveX Configuration 583
USB Flash Drive Module. 584
Wavetrend Tag Reader (Package 5 Only) 584
Screen Saver Modules 584
MultiSession Screen Saver Module 584
Screen Saver Module. 585
Sound Modules 586
Universal Sound Driver 586
TermSecure Modules 587
Touch Screen 588

Serial Drivers 588
USB Touch Screen Driver 590
USB MultiTouch Screen Driver 591
Video Driver Modules 591
Custom Video Mode Module 592
Monitor Configuration Module 592

Chapter 13

ThinManager Server Configuration Wizard

Introduction Page 593
Unknown Terminals and Terminal Replacement Page 594
Terminal Authentication Page 595
Device Authentication 595
Terminal Replacement Page 596
Historical Logging Page 597
SysLog Configuration Page 598
Event Log Tab 600
System Schedule Page 601
Security Groups Page 602
Event Selection Page 605
Email or Windows Messaging Recipients Page 606
Database Management Page 609
HTTPS Server Settings Page 614
. 618
Shadow Configuration Page 619
ThinManager User Configuration Page 620
Docker Server Settings Page 621

Chapter 14

MultiMonitor

MultiMonitor Layout Page 624
MultiMonitor Display Client Selection Page 630
Override Function 631
Share Keyboard and Mouse Module 634
Master Thin Client Configuration 635
Replica Thin Client Configuration 636
Share Keyboard and Mouse with MultiMonitor 637

Chapter 15

Reports

Select Reports 639
Report Tab 640
Print Report 640
Report Template Installation 641

Chapter 16

Scheduling

System Scheduling of Reports 643
Schedule Configuration Backups 647

TermMon ActiveX

Chapter 17

Register the Control 652
Read-only Properties 652
Read-Write Properties 653
Events 653
Methods 654
Control Constants 656
TermMonEvent 657
TermMonCommand 657
TermMonConst 658
TermMonRelevance 658

Glossary 659

About This Publication

This publication provides comprehensive information for users of ThinManager® thin client management software.

Download Firmware, AOP, EDS, and Other Files

Download firmware, associated files (such as AOP, EDS, and DTM), and access product release notes from the Product Compatibility and Download Center at rok.auto/pcdc.

ThinManager resources are also available at thinmanager.com.

Summary of Changes

This publication contains the following new or updated information. This list includes substantive updates only and is not intended to reflect all changes.

Topic	Page
Web Browser User Interface Enhancements	27
Certificate Management	47
Updates to TLS Certificates	59
Container Versioning	83
FactoryTalk Optix Container	90
BootAssist	560
USB MultiTouch Screen Driver	591
TMC for Android Devices	235
TMC for iOS Devices	237
TMC for Windows Devices	238

Additional Resources

These documents contain additional information concerning related products from Rockwell Automation.

Resource	Description
EtherNet/IP Network Devices User Manual, ENET-UM006	Describes how to configure and use EtherNet/IP® devices to communicate on the EtherNet/IP network.
Ethernet Reference Manual, ENET-RM002	Describes basic Ethernet® concepts, infrastructure components, and infrastructure features.
System Security Design Guidelines Reference Manual, SECURE-RM001	Provides guidance on how to conduct security assessments, implement Rockwell Automation products in a secure system, harden the control system, manage user access, and dispose of equipment.
Industrial Components Preventive Maintenance, Enclosures, and Contact Ratings Specifications, publication IC-TD002	Provides a quick reference tool for Allen-Bradley industrial automation controls and assemblies.
Safety Guidelines for the Application, Installation, and Maintenance of Solid-state Control, publication SGI-1.1	Designed to harmonize with NEMA Standards Publication No. ICS 1.1-1987 and provides general guidelines for the application, installation, and maintenance of solid-state control in the form of individual devices or packaged assemblies incorporating solid-state components.
Industrial Automation Wiring and Grounding Guidelines, publication 1770-4.1	Provides general guidelines for installing a Rockwell Automation industrial system.
Product Certifications website, rok.auto/certifications.	Provides declarations of conformity, certificates, and other certification details.

You can view or download publications at rok.auto/literature.

Notes:

Quick Setup Overview

This chapter guides you through the actions needed to build and activate a ThinManager system.

Microsoft

Complete the following activities to install and configure Remote Desktop Services.

- Build a Remote Desktop Server with the supported Microsoft Windows Server operating system. Enable the Remote Desktop Services (Terminal Services) role. See Microsoft Configuration on page 61.
- Create a Microsoft Remote Desktop Licensing Server and add Remote Desktop Services Client Access Licenses (RDSCALs) for each thin client. These were called Terminal Server Client Access Licenses (TSCALs) in Server 2003. The servers also require a normal CAL.
- It is common to have each ThinManager-managed terminal automatically log in to the Remote Desktop Server when it boots up. Therefore, create a unique Windows user for each ThinManager-managed terminal. For domain deployments, this is done within Active Directory. For work group deployments, this is done on each Remote Desktop Server. Add the users to the Remote Desktop Users group to make sure each user has 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

This section describes how to install, activate, and configure ThinManager.

Installation & Activation

Perform the following actions to install and activate ThinManager.

Install ThinManager software onto a computer to create ThinManager Server. During ThinManager installation, you are prompted to enter an optional Windows user account to set the ThinServer service login account.

It is recommended to use a Windows User as the ThinServer Service Account and follow the principle of least privilege. For more information about changing the ThinServer Service Account, see Local Administrative Login for ThinServer on page 74.

- With ThinManager version 13, only 64-bit installations are supported, and 32-bit system installations are converted to 64-bit.
- During installation, there is a prompt to enable API. When enabled, User API Keys may be generated to execute endpoints. This can be enabled or

disabled later in the ThinManager Server Configuration wizard. See API on page 60 for more information.

- If using ThinManager Master Licensing, follow these steps.
  - Create a Master ThinManager License, see ThinManager Master License on page 41
  - Verify that the License Mode is set to ThinManager Master License, see Figure 44 on page 41
  - Add enough Product Licenses for each ThinManager-managed terminal
- If using FactoryTalk Activation, follow these steps. See FactoryTalk Activations on page 51.
  - Install the FactoryTalk Activation Manager on each computer where ThinManager is installed
  - Download the FactoryTalk Activations for ThinManager

It is not a requirement that you install Factory Talk Activation Manager on the ThinManager server as you can have a centralized license server that is not on the ThinManager server.

  - Change the License Mode in ThinManager to FactoryTalk Activation and assign the newly downloaded activations

ThinManager Database Encryption

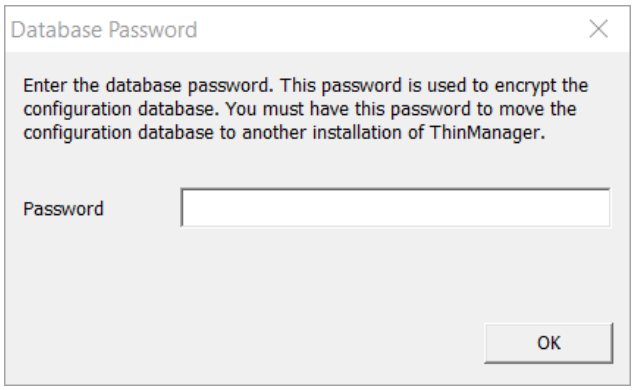
ThinManager 11.2 introduced a major encryption change, with the Advanced Encryption Standard, AES, used to encrypt the ThinManager database instead of the previous encryption key. This led to a few important changes.

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

Installation

When ThinManager 11.2 and later is first run, a dialog box appears, which prompts for a new database password.

Figure 1 - Database Password Dialog Box



1. Type a password into the Password field and click OK.

This password is used for the encryption key when the database is configured. There are no requirements for length or complexity. You can leave the Password field blank.

IMPORTANT In ThinManager 12 and earlier, the Database Password is unrecoverable if lost.

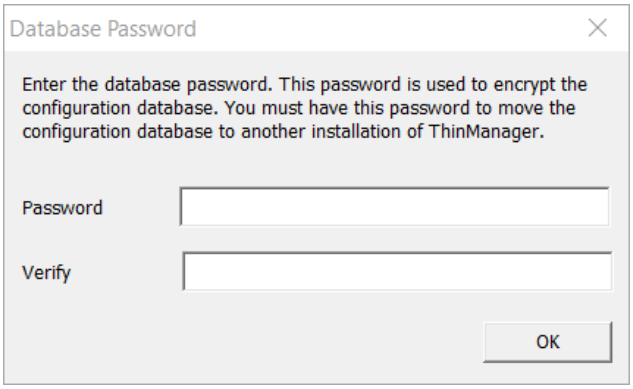
Manual Backup

To manually back up the database, follow these instructions.

1. Choose Manage>Backup.

   You are prompted to create a password for the backup.

Figure 2 - Database Password Dialog Box



2. Type the password into the Password field.
3. Type the password into the Verify field.
4. Click OK.

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

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

IMPORTANT In ThinManager 12 and earlier, the Database Password is unrecoverable if lost.

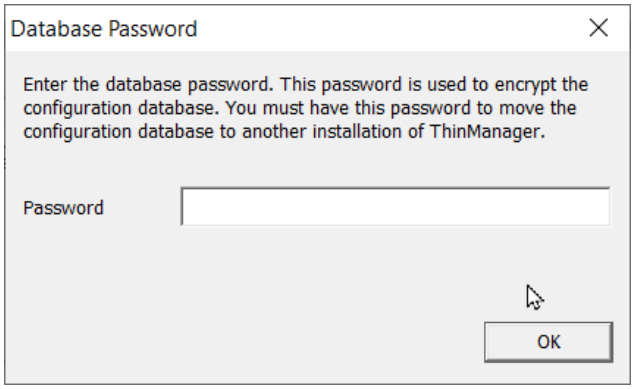
Manual Restore

To manually restore an encrypted backup, follow these steps.

1. Choose Manage>Restore.

   The Database Password dialog box appears and prompts for the backup database password, not the original database password.

Figure 3 - Database Password



2. Type the Password and click OK.

Automatic Backup

ThinManager can be configured to backup the configuration automatically. These automatic backups use the original password entered when ThinManager was configured.

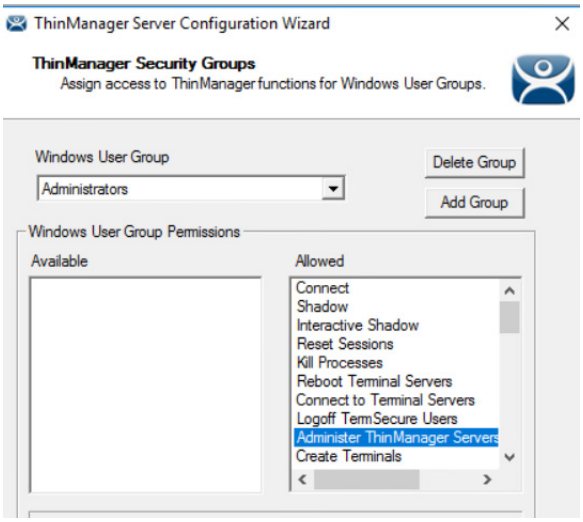
The backups are now be saved in C:\ProgramData\Rockwell Software\ThinManager instead of C:\Program Files (x86)\Rockwell Software\ThinManager.

Database Password Change

Prior to ThinManager 12.1, the running database password was unrecoverable if forgotten. With ThinManager 12.1, the running database password can be changed inside the ThinManager Server Configuration Wizard.

Users with the Administer ThinManager Servers role within ThinManager Security Groups can change the database password without knowing the previously set password. By default, Administrators Windows User Group has access to this role.

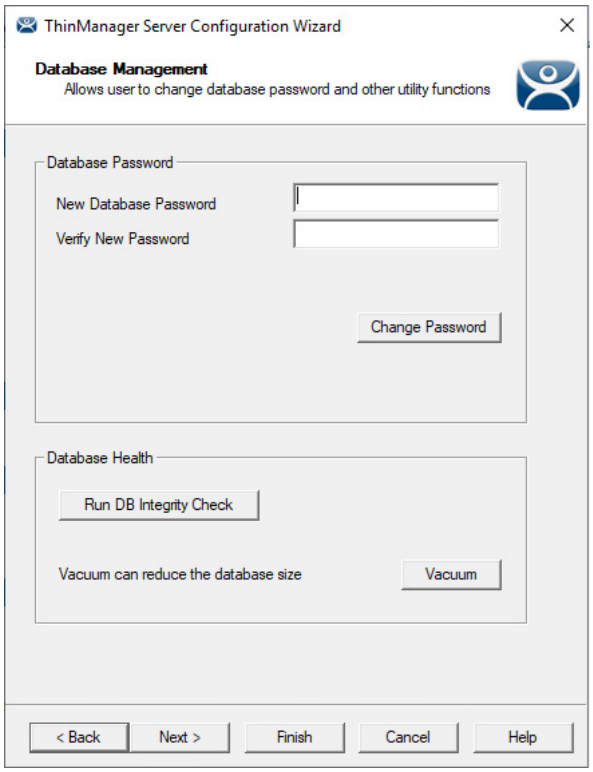
Figure 4 - ThinManager Security Groups Page



To change the database password, see Database Management Page on page 609.

1. Navigate to the Database Management page of the ThinManager Server Configuration Wizard. See ThinManager Server Configuration Wizard on page 593 for more information on how to open the wizard.

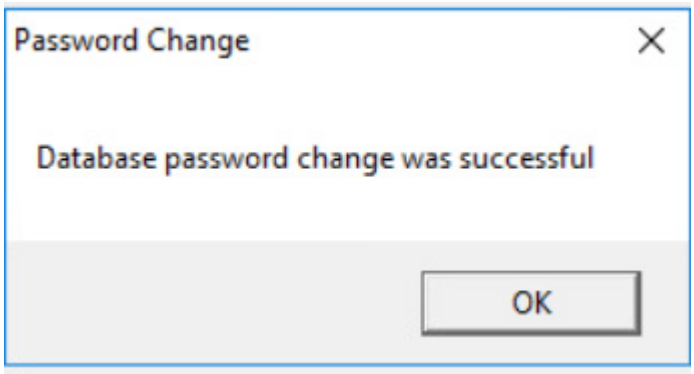
Figure 5 - Database Management Page



2. Type the new password in the New Database Password and Verify New Password fields.
3. Click Change Password to commit the changes.

   A dialog box confirms the database password change was successful.

Figure 6 - Successful Database Password Change dialog

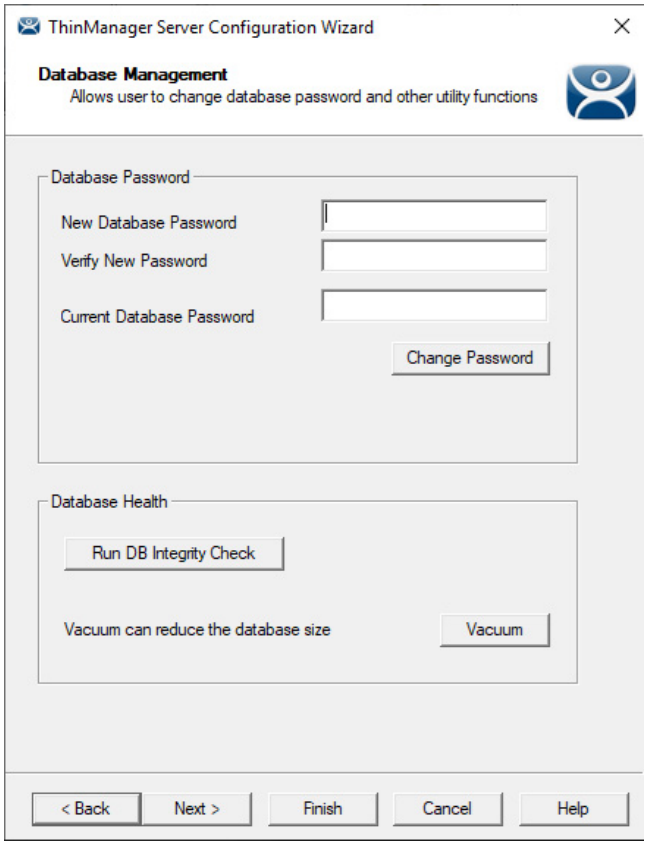


4. Click OK.

   The database password is changed.

User accounts without the Administer ThinManager Servers security role can change the running database password. However, they are prompted to enter the current database password. See Figure 7 on page 18.

Figure 7 - Current Database Password field



IMPORTANT Backups are still unrecoverable if the password is lost.

5. Click Vacuum to compress the running database, which is useful prior to database exportation or major database change.
6. Click Finish to exit the wizard.

Configuration

Perform the following actions to configure ThinManager.

- Define the Remote Desktop Servers at Display Servers> Remote Desktop Servers>Remote Desktop Server Wizard. See Defining Remote Desktop Servers in ThinManager on page 61 for information.
- Define the Display Clients at Display Clients> Remote Desktop Services>Display Client Wizard to deploy the applications. See Content on page 133 for information.
- Define the Terminals at Terminal> Terminal Configuration Wizard. See Terminal Configuration on page 231 for information.
- Associate the hardware to the Terminal configuration. See Terminal Hardware Page on page 234 for information.

Network

Thin clients and Remote Desktop Servers need a reliable network.

Verify that traffic is allowed on the network ports that follow in all software and hardware firewalls.

Port	Protocol	Description
UDP/67	DHCP – IP Address Assignment	Used by the PXE Server (if using PXE boot)
UDP/69	TFTP	
TCP/1494	Citrix ICA	Used by the ICA protocol (if using ICA instead of RDP)
UDP/1758	Mulitcast TFTP	Used if the default Multicast is enabled. If the network MTU size is not the default, then the packet size needs to be changed on the Multicast Configuration page of the ThinManager Server Configuration Wizard.
TCP/2031	Proprietary – Configuration	Used to pass the configuration from the ThinManager Server to the ThinManager thin clients
TCP/2376	Docker® Client Communication	Needed to allow an encrypted channel for the terminal to connect to a Container Host to display the Container content.
TCP/3268	LDAP	Used for LDAP queries targeted at the global catalog with Active Directory
TCP/3389	RDP	Used by the Microsoft RDP protocol (if using RDP in v2.4.1 or later)
UDP/4011	DHCP	Used when the DHCP server is on the ThinManager server or when using the UEFI BIOS to boot.
UDP/4900	TFTP	Used for the TFTP download of the firmware
TCP/5900	Proprietary – Shadow	Used to shadow Terminals. This can be changed on the Shadow Configuration page of the ThinManager Server Configuration Wizard.
TCP/8443	HTTPS	(Optional) Can be configured and used to deliver some modules to thin client after the firmware is delivered. If closed, the module falls back to UDP 69 or UDP 4900, depending on the hardware, for module delivery. Can be changed in ThinServer.
ICMP Echo Packets (Ping)	ICMP	Used by WinTMC and Enforce Primary
DHCP	DHCP	Configure as needed

VLANs and Subnets

You should have only one PXE server per network. It is beneficial to have a separate VLAN for each ThinManager Server pair that replies 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 passes that info through NLA to authenticate. The client logs in and starts a session without operator awareness.
- If a terminal does not have a valid Windows account entered in its configuration, then an NLA login screen is displayed, which requires a valid user account and password. This gets passed to the Remote Desktop Server for the login. A Windows Security/Login page is never displayed.

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

Hardware Introduction

A ThinManager-ready thin client can use Dynamic Host Configuration Protocol (DHCP) or a static IP address for the client and ThinManager Server IP address. Its BIOS instructs it to download the firmware.

A ThinManager-compatible thin client is a thin client that lacks the ThinManager BIOS. ThinManager-compatible thin clients do not store static IP addresses; so, each of them requires DHCP to assign the client IP address. The ThinManager Server IP address and bootfile name can be provided by a DHCP server or the ThinManager PXE Server.

For more information visit partners.thinmanager.com/terminals

Perform these actions with regard to 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.
  - To use Static addresses, open the IP Address menu on the thin client and enter the IP address of the thin client and the ThinManager Server.
  - To use DHCP, configure Option 066 for the IP address of the ThinManager Server, and Option 067 as acpboot.bin.
  - To use PXE Boot, enable PXE boot via Manage>PXE Server to launch the PXE Server wizard.
- Use either of the methods that follow to attach the terminals to ThinManager:
  - Turn on the terminal and select Create New Terminal when the offline terminals are listed.
  - Pre-create the terminals in ThinManager and select the proper terminal name when the terminal is turned on and offline terminals are listed.

Results

Step 1: The clients connect to the ThinManager Server and download the firmware and configuration.

Step 2: The configuration sends the clients to the Remote Desktop Server to log in and start a session, and delivers any additional content assigned to the terminal's configuration.

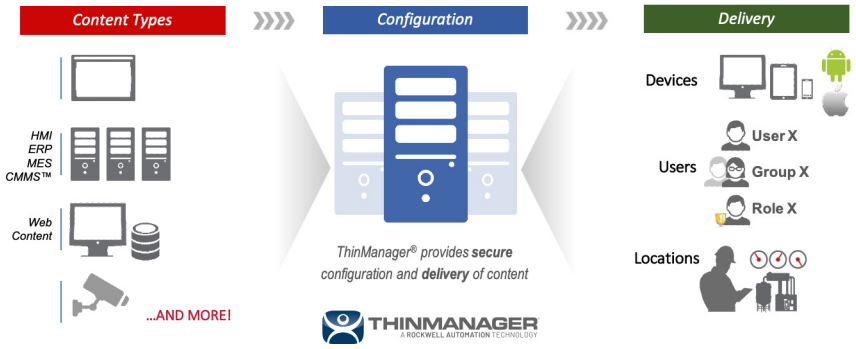
Introduction

ThinManager is a content delivery system that 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 covers the variations of content deployment using ThinManager® with Relevance®.

Figure 8 - Thin Manager 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. Each device connects to it to receive its configuration and instructions.

Figure 9 - Typical Simple Deployment

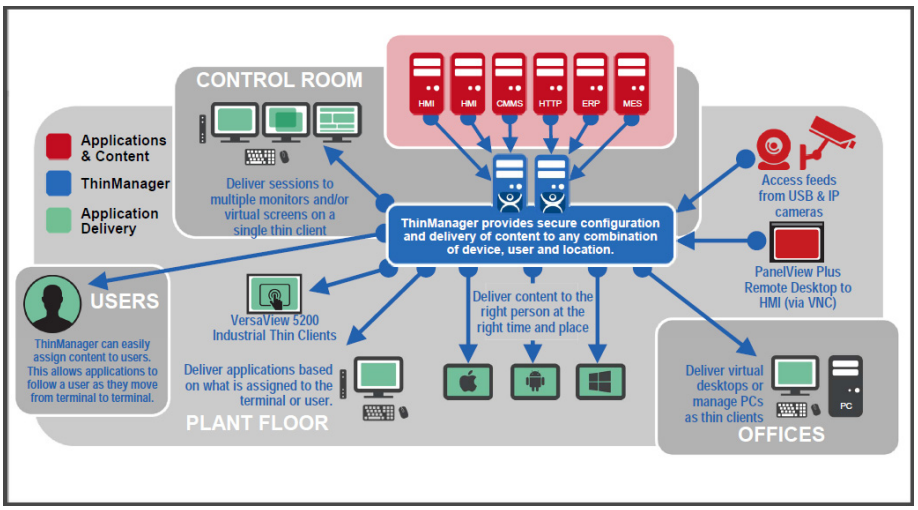
ThinManager is a software program that is installed on a computer or server in your system. The simplest use of ThinManager is to deploy a Windows application from a Windows Remote Desktop Server to a ThinManager-ready device. However, ThinManager provides many more options for deploying applications.

Figure 10 - Sources, Content, Devices, and User Options

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

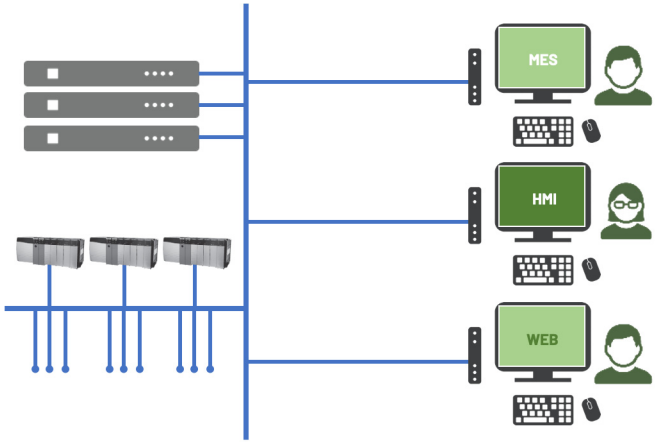
These options allow you to tailor a customized content delivery system.

Figure 11 - ThinManager Content Deployment



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

Figure 12 - Standard Industrial Architecture

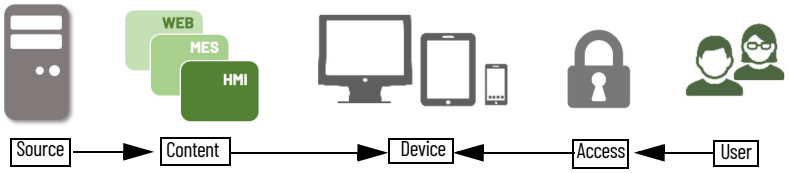


An industrial network pulls the I/O to the PLCs. The Remote Desktop Server hosts the sessions that run the HMI and talk to the PLCs to gather and display the data.

ThinManager User Access

ThinManager can provide additional security to the system that controls deployment of applications to users. This was formerly called TermSecure and is now integrated into ThinManager with Relevance as Access.

Figure 13 - Access



Location Services

The Location Services component builds on the ThinManager system in that it adds location to the application delivery. This allows content to be sent to the right person, at the right place, at the right time.

Figure 14 - Stylized Content Deployment

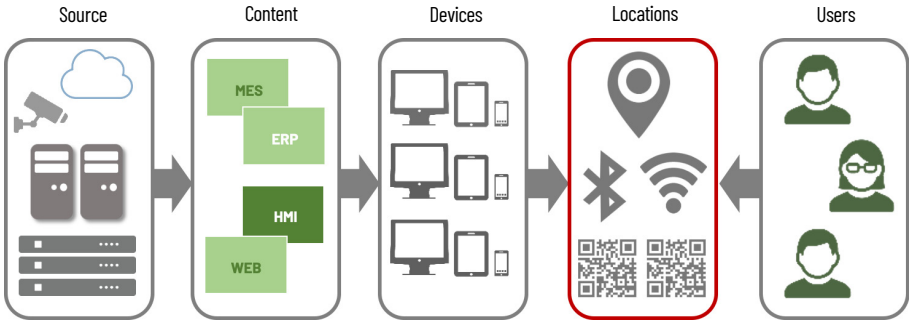
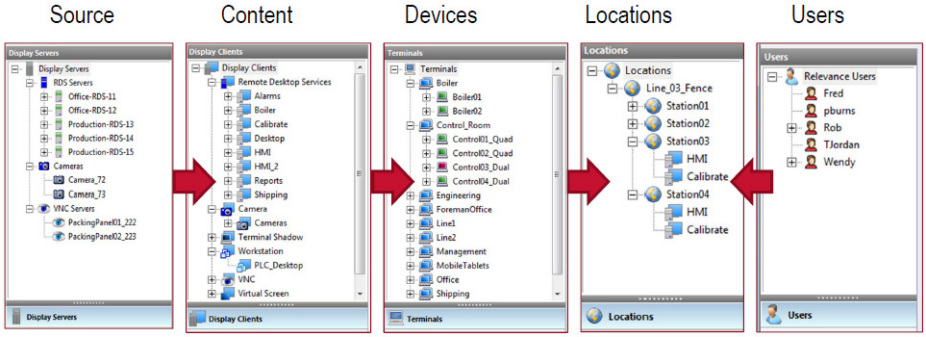


Figure 15 - Content Deployment in ThinManager Tree



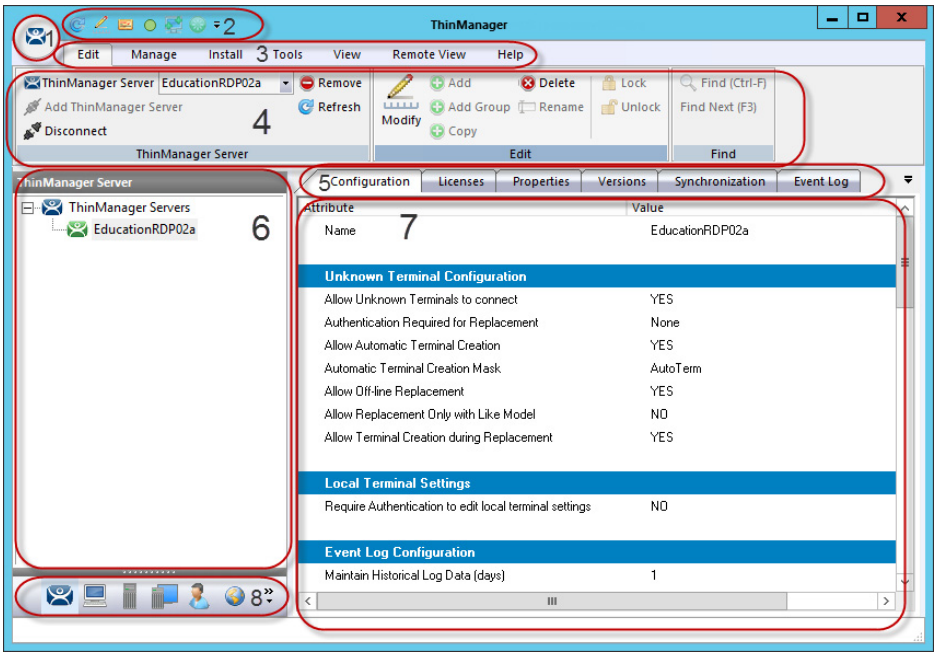
You create Locations in Location Services and send content to the locations. These can be assigned locations with a tethered terminal, or they can be unassigned locations that have no terminal at the location and are accessed solely by mobile devices.

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

ThinManager Interface

This section leads you through the important features on the ThinManager interface. Press F1 to find specific information while in the ThinManager program.

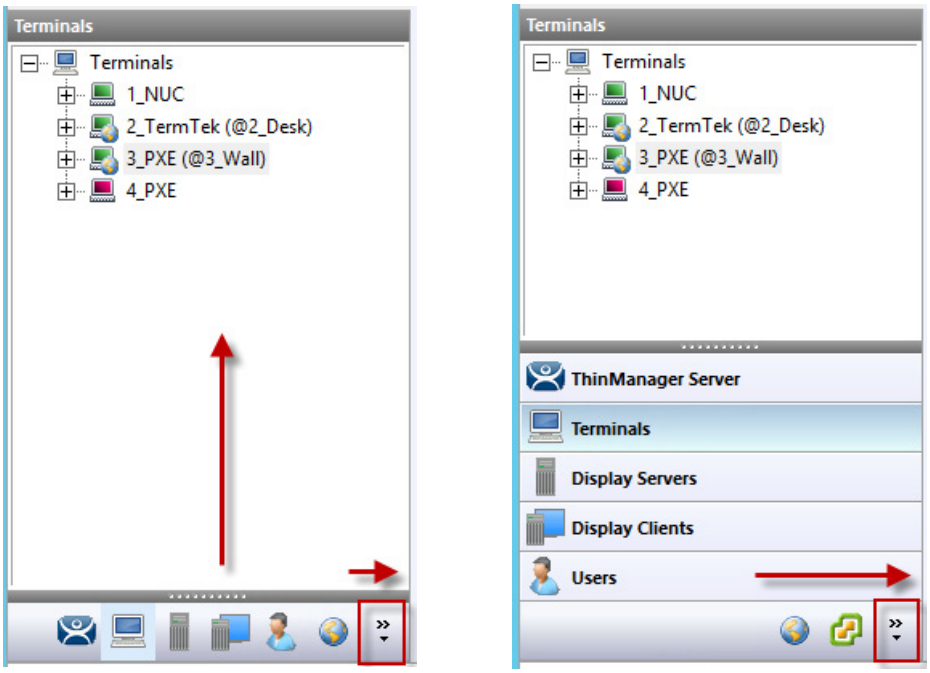
Figure 16 - ThinManager Interface



The ThinManager Interface has several components.

Note	Component	Description
1	Application Button	Launches the ThinManager Server Configuration wizard to configure global ThinManager settings.
2	Quick Access Toobar	Click the pull-down arrow to customize this toolbar. Add icons of commonly used tasks from the menu bar, like Restart, Send Message, Modify, Backup, and Shadow.
3	Menu Bar	Separates the functions into categories.
4	Ribbon Bar	Contains icons for the functions. Hide when unused via the Minimize the Ribbon command on the Quick Access pull-down arrow menu.
5	Detail Pane Tabs	Allows you to choose details to display. The tabs and detail selections change depending on what is selected in the tree. Drag the tabs to change the order.
6	Tree	Displays the components of ThinManager with the Outlook Bar Tab control so the branches of the ThinManager tree are shown one at a time.
7	Detail Pane	Displays the information for the selected tab for the highlighted tree component. The Detail Pane can be torn away by dragging the tab away from ThinManager. The Detail Pane can be re-docked 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.

Figure 17 - Tree Selector Buttons - Minimized Buttons at the Bottom/Buttons Stacked



Stacked the buttons allow you to make a quicker switch, but the minimized buttons allow more room to show components in a larger system.

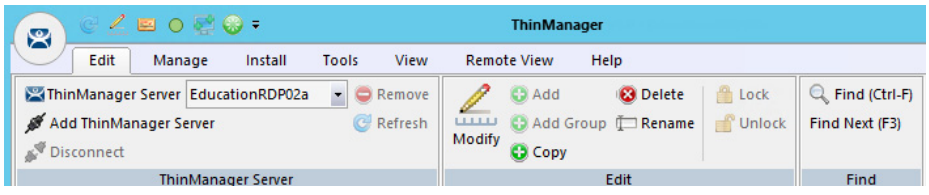
There is an arrow that allows customization tasks—you can hide or reorder the branches of the tree.

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 detail in the sections of the manual that cover setup and configuration.

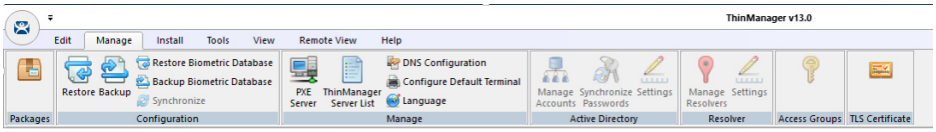
Figure 18 - Edit



Feature	Description
Add ThinManager Server	Allows connection to, and managment of, other ThinManager Servers from your local interface. Appropriate permissions on the remote computer are required for access. Intended for a remote connection, not the partner in a synchronized pair.
Disconnect	Breaks the connection to the remote ThinManager Server.
Remove	Deletes the remote ThinManager Server from the local list. Does not affect the remote ThinManager Server.
Refresh	Refreshes the data.
Modify	Opens the configuration wizard for a highlighted tree component.

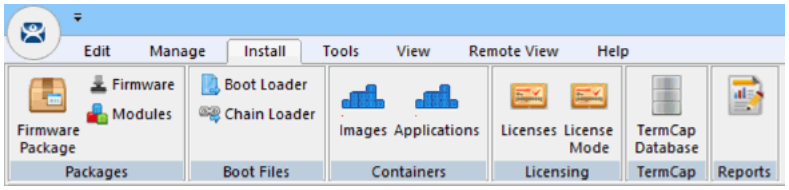
Feature	Description
Add	Launches a new configuration wizard for a highlighted tree component.
Add Group	Launches a group configuration wizard for a highlighted tree component.
Copy	Launches a dialog that allows you to create a copy of a highlighted item.
Delete	Deletes a highlighted item.
Rename	Renames a highlighted item.
Lock	Locks a highlighted item.
Unlock	Unlocks a locked item.
Find	Use to search for names, descriptions, IP addresses, and other data in the tree.
Find Next	Repeatedly search for a term.

Figure 19 - Manage



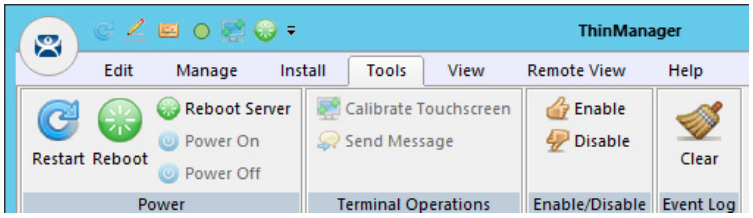
Feature	Description
Packages	Opens the Package Manager window.
Restore	Opens a file browser to let you restore a previously saved ThinManager configuration.
Backup	Opens a file browser that lets you back up and save a ThinManager configuration for emergency restoration. This backup can be automated using the Scheduler.
Restore Biometric Database	Opens a file browser to let you restore a previously saved Biometric database.
Backup Biometric Database	Opens a file browser to let you save your Biometric data.
Synchronize	Use to manually synchronize a pair of ThinManager Servers if you are not using the recommended automatic synchronization.
PXE Server	Launches the PXE Server configuration wizard.
ThinManager Server List	Opens the ThinManager Server configuration wizard for automatic synchronization.
DNS Configuration	Opens the DNS configuration wizard to allow ThinManager to resolve names using your DNS.
Configure Default Terminal	Allows configuration of the default Terminal if you are using auto-creation of Terminals.
Language	Opens the Language Module, where you can set the language on the terminal.
Web Management	Allows web access management when it is implemented in the future.
Manage Accounts	Allows password management of Active Directory accounts. See Manage Accounts Management on page 393 for details.
Synchronize Passwords	Allows synchronization of passwords between ThinManager and the Active Directory for the chosen accounts. See Synchronize Password on page 399 for details.
Settings (Active Directory)	Allows you to use Active Directory, set Password Settings, and select whether to use Windows Security Groups or Active Directory Organizational Units. See Settings on page 400 for details.
Manage Resolvers	Opens the Resolver Management window that lets you Add, Delete, and Edit resolvers added through a mobile device. See Mobile Device Interactions with Location Services on page 440 for details.
Settings (Resolver)	Opens the ThinManager Settings window that lets you define iBeacons and manage Bluetooth filtering.
Access Groups	Opens the Access Groups dialog box where you create access groups for ThinManager User Services. See ThinManager Access Group Creation on page 338 for details.
TLS Certificate	Opens the Manage TLS Certificates dialog, where you can generate certificates and/or add certificates from the Microsoft Certificate Store. These certificates include Browser Custom CA Certificate, Container Host Connection Cert, HTTPS Server Certificate, Syslog Client Certificate, ThinManager Server CA Certificate, and ThinManager Server Synchronization. See TLS Certificates on page 59 for details.

Figure 20 - Install



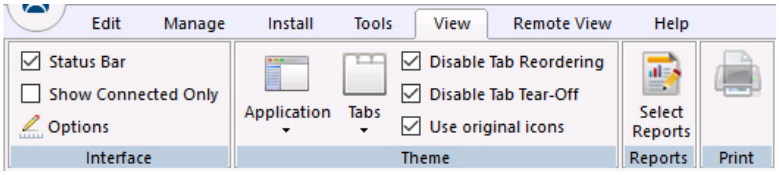
Feature	Description
Firmware Package	Updates a firmware package, which consists of a firmware version and the modules for that version.
Firmware	Updates the firmware without an update of modules.
Modules	Updates a module without an update of the firmware.
Boot Loader	Updates the boot loader used in PXE boot.
Chain Loader	Updates the chain loader used in PXE boot.
Images	Launches the Install Container Image dialog box. See Install Container Images on page 102 for more information.
Applications	Launches the Container Applications dialog box. See page 92 for more information.
Licenses	Launches the Licensing window to add licenses to ThinManager.
License Mode	Selects 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 is not listed.
Reports	Adds a report and SQL query if you need a newly released one before it is added in a service pack.

Figure 21 - Tools



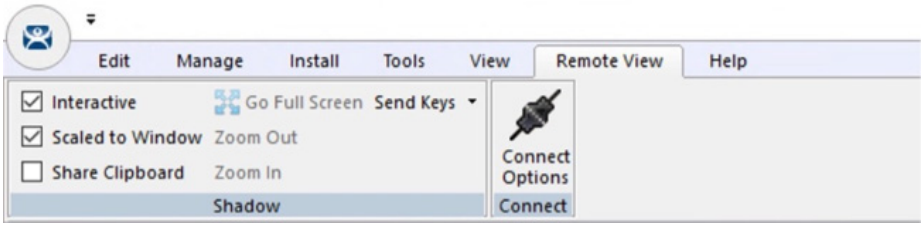
Feature	Description
Restart	Resends the configuration to a highlighted terminal.
Reboot	Cycles power to a highlighted terminal and reloads the firmware and configuration.
Reboot Server	Cycles power to a highlighted Remote Desktop Server. Although it will give you a warning prompt, do not use unless you are serious about restarting a Remote Desktop Server. All sessions end abruptly when the server is rebooted.
Power Off	Powers off a highlighted virtual machine or 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	Initiates the calibrate touchscreen program on a highlighted terminal.
Send Message	Sends a message to a highlighted terminal.
Enable	Re-enables a disabled terminal, Remote Desktop Server, or location.
Disable	Disables a highlighted terminal, Remote Desktop Server, or location. A terminal stops showing the session but shows a ThinManager splash screen. The session continues to run on the Remote Desktop Server. A disabled Remote Desktop Server kicks off all the ThinManager thin clients from the Remote Desktop Server, and forces them to a backup server. The Remote Desktop Server is still functional and allows RDP connections from other sources. This is useful to force 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	Clears the event log for the highlighted Terminal or Remote Desktop Server.

Figure 22 - View



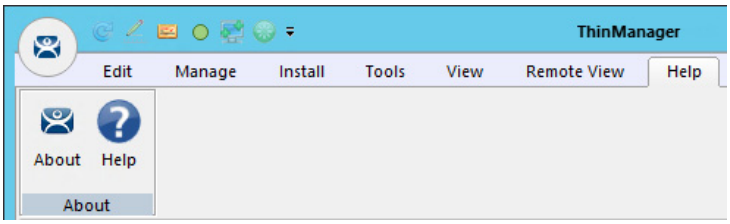
Feature	Description
Status Bar	Check to display the status bar at the bottom of the ThinManager interface.
Show Connected Only	Hides any unpowered or unconnected thin clients. Although it can be useful, it is best left checked as it can be confusing when the unpowered terminal is hidden.
Options	Launches the Options window with the settings for license notifications, and allows new terminals and users to initiate a Terminal Configuration Wizard or ThinManager User Configuration Wizard.
Application	Use to choose the color scheme for ThinManager.
Tabs	Use to choose the tab scheme for ThinManager.
Disable Tab Reordering	Check to lock the Detail Pane tabs in their current position. Normally, the tabs can be rearranged.
Disable Tab Tear-Off	Check to lock the Detail Pane tabs in their current position. Normally, the tabs can be dragged free from the ThinManager console.
Use Original Icons	Loads the icons into ThinManager defaulted in versions earlier than 13.01.00. When enabled, this setting requires ThinManager to be closed and relaunched to take effect.
Select Reports	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	Use to print a highlighted Report tab.

Figure 23 - Remote View



Feature	Description
Interactive	Check to click into and control a shadow session. Clear this option for view-only mode.
Scaled to Window	Shrinks the shadowed terminal to fit into the details pane. Clear this option to show it in the correct resolution with scroll bars to give you a closer view.
Share Clipboard	Check to share local clipboard with VNC and other Remote Connections. Clear this option to disable it.
Go Full Screen	Makes the shadowed terminal's image full screen. Use CTL+ALT+Break to undo full screen. To close ThinManager, use ALT+F4.
Send Keys	Sends the selected key sequence to a shadowed terminal.
Zoom In	Use to click inside a shadow session and zoom in for detail. This option is dimmed until the Interactive checkbox is cleared.
Zoom Out	Use to click inside a shadow session and zoom out for an overview. This option is dimmed until the Interactive checkbox is cleared.
Connect Options	Use to configure the RDP settings when you connect to a Remote Desktop Server console from ThinManager.

Figure 24 - Help



Feature	Description
About	Shows the version and build number of ThinManager.
Help	Launches the ThinManager Help.

Customizing the Toolbar

Select More Commands from the Customize Quick Access Toolbar pull-down menu to launch the Customize window and add icons of frequently used functions.

Figure 25 - Customize Quick Access Toolbar Menu

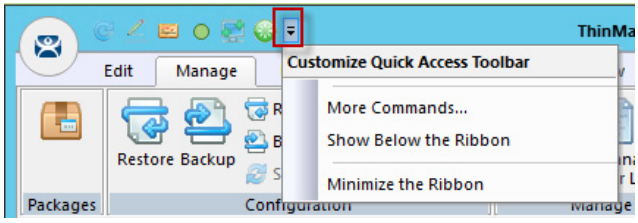
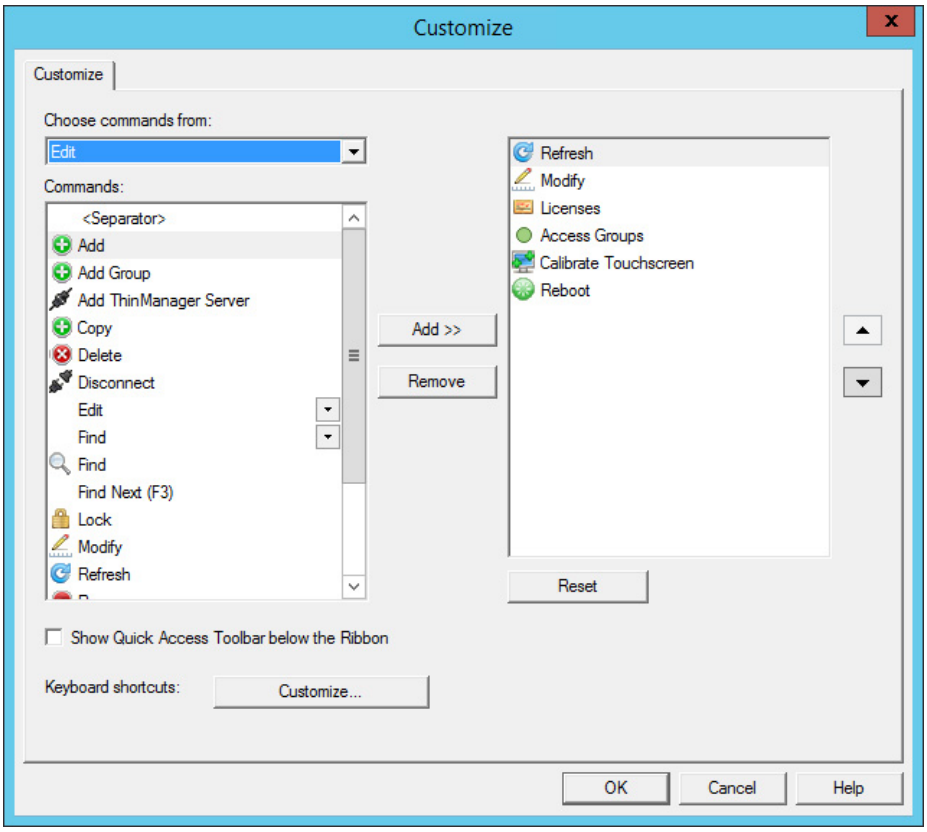
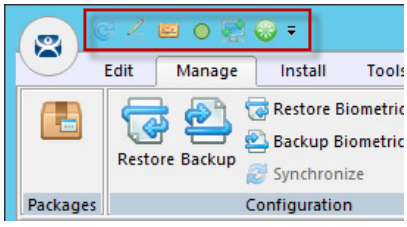


Figure 26 - Customize Window



Feature	Description
Choose commands from	Use to select commands from each group.
Commands	Lists the available command options. Select one and click Add to move it to the right-hand list to add it to the Quick Access bar. Adjust the order using the up and down arrows.
Show Quick Access Toolbar below the Ribbon	Check to move the Quick Access bar.

Figure 27 - Quick Access Toolbar



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

Icons

ThinManager tree icons show the status of components.

ThinManager Server

The ThinManager Server branch has two ThinManager icons.

Figure 28 - ThinManager Server Tree Icons

Icon	Description
Green ThinManager	ThinManager console is talking to the ThinServer.
Red ThinManager	ThinManager console is not talking to the ThinServer. Right-click on the icon and select Reconnect from the 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.

Terminals

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

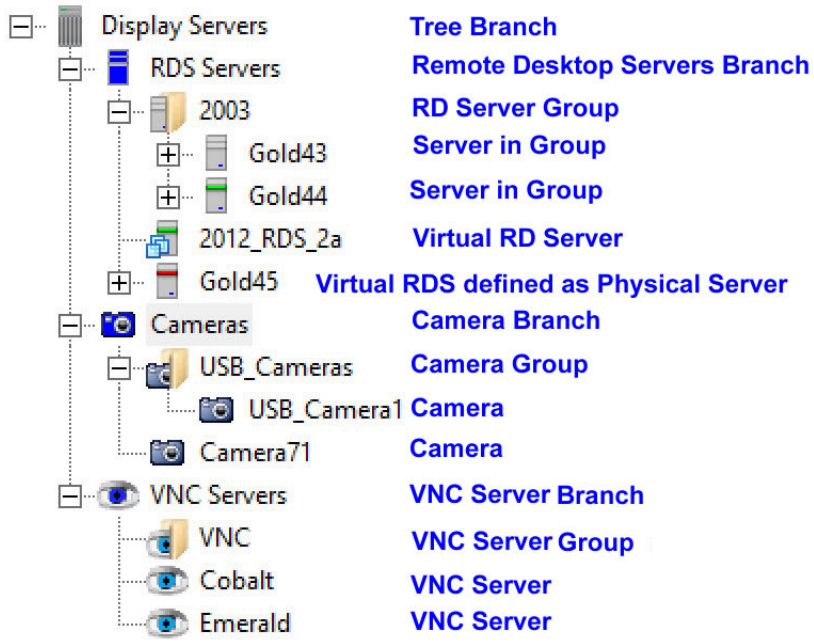
Terminal Tree Icons

Icon	Represents
Dual Monitor	A Terminal Group
Lock	A Terminal with an open configuration wizard
Exclamation Mark	A Terminal with a configuration change that needs a restart
Globe	A Terminal with an assigned Location, which is shown in parentheses
Green Monitor	A Terminal that is booted and connected to the ThinManager Server
Yellow Monitor	A Terminal that is going through the boot process
User	A Terminal that has a ThinManager User logged in to the Terminal. The user name is shown in parentheses.
Red Monitor	A Terminal that is either turned off or not able to communicate with the ThinManager Server
Red X	A Terminal that was Disabled using the Tools>Disable command

Display Servers

The Display Server tree has several different icons.

Figure 29 - Display Server Tree Icons



Icon	Represents
Blue Server	The Remote Desktop Server branch
Server with Folder	A Remote Desktop Server Group
Server with Virtual Boxes	A Virtual Server defined through the VCenter Server tool
Blue Camera	The Camera branch
Camera with Folder	A Camera Group
Gray Camera	A Camera
Blue Eye	The VNC Server branch
Cyan Eye with Folder	A VNC Server Group
Cyan Eye	A VNC Server

Figure 30 - Remote Desktop Server Icon Colors

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

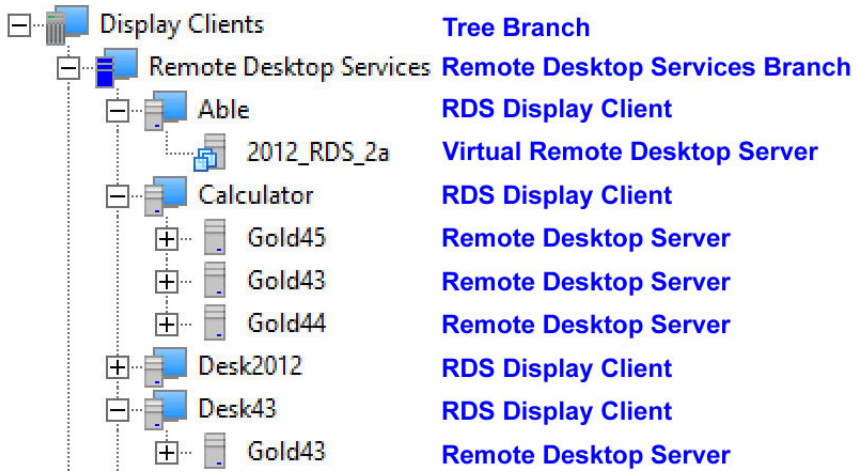
Icon	Represents
Server with Gray Stripe	A Remote Desktop Server without an administrative account
Server with Green Stripe	A Remote Desktop Server with a connection to the ThinServer using an administrative account
Server with Red Stripe	A Remote Desktop Server with an account but unable to make a connection to the ThinServer

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

Display Clients

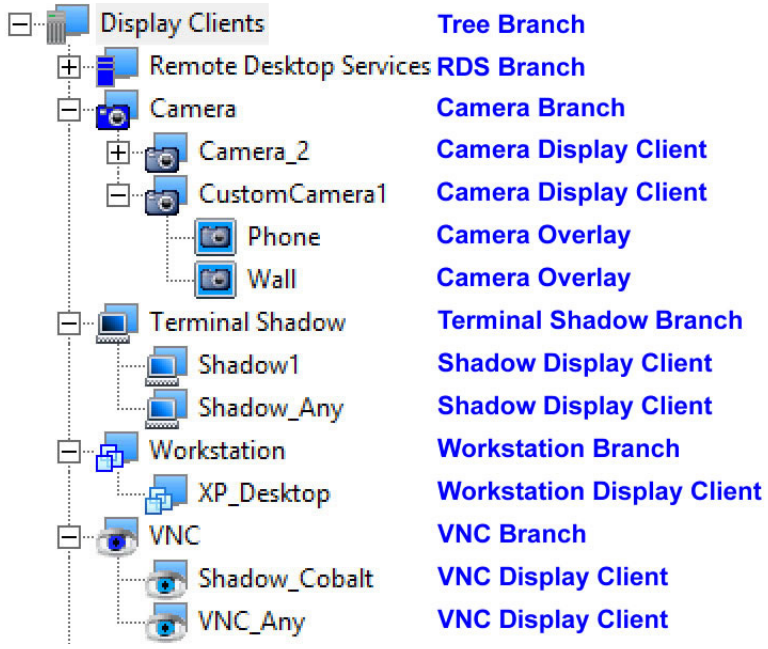
The Display Client branch has several icons.

Figure 31 - Remote Desktop Services Display Client Branch Icons



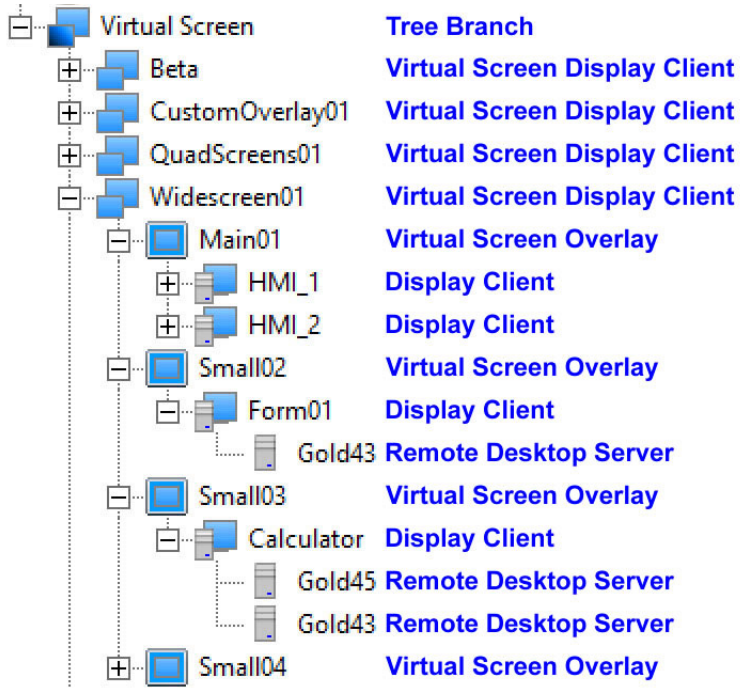
Icon	Represents
Dark Gray Server and Blue Monitor	The Display Client Tree Branch
Blue Server and Blue Monitor	The Remote Desktop Services Branch
Light Gray Server and Blue Monitor	A Remote Desktop Services Display Client
Gray Server	A Remote Desktop Server assigned to a Display Client

Figure 32 - Other Display Client Branch Icons



Icon	Represents
Dark Gray Server and Blue Monitor	The Display Client Tree Branch
Blue Server and Blue Monitor	The Remote Desktop Services Branch
Blue Camera and Blue Monitor	The Camera Branch
Gray Camera and Blue Monitor	A Camera Display Client
Gray Camera inside a Blue Box	A Camera Overlay assigned to a Display Client
Dark Blue Terminal and Blue Monitor	The Terminal Shadow Branch
Light Blue Terminal and Blue Monitor	The Terminal Shadow Display Client
Dark Blue Virtual Boxes and Blue Monitor	The Terminal Shadow Branch
Medium Blue Virtual Boxes and Blue Monitor	The Workstation Display Client
Dark Blue Eye and Blue Monitor	The VNC Server Branch
Light Blue Eye and Blue Monitor	The VNC Server Display Client

Figure 33 - Virtual Screen Display Client Branch Icons



Icon	Represents
Dark Blue Monitor and Blue Monitor	The Virtual Screen Branch
Blue Monitor and Blue Monitor	The Virtual Screen Display Client
Blue Square within a Blue Monitor	The Virtual Screen Overlay
A Light Gray Server and Blue Monitor	A Display Client. Assigned to the Overlay
A Light Gray Server	A Remote Desktop Services Server assigned to the Display Client on the Overlay

Lightning Bolts

Icons with lightning bolts indicate the connection status.

Figure 34 - Lightning Bolts

Icon	Represents
Green Lightning Bolt	Active connection that is visible in the foreground
Yellow Lightning Bolt	An active connection that is not displayed, 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	Defined connection that is not active.

ThinManager Users

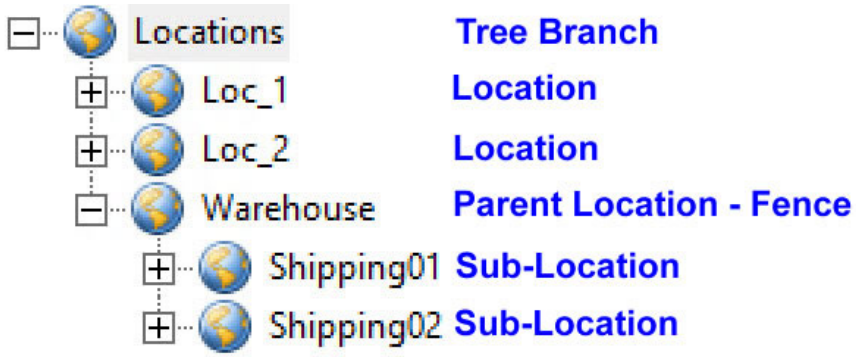
Figure 35 - ThinManager Users Tree

Icon	Represents
Light Blue Person	The ThinManager User Tree Branch
Two People	A ThinManager User Group
Red Person	A ThinManager User
Red Person with Blue Monitor	A ThinManager User that is logged in to a Terminal or Location. The Terminal is displayed in parentheses.

Locations

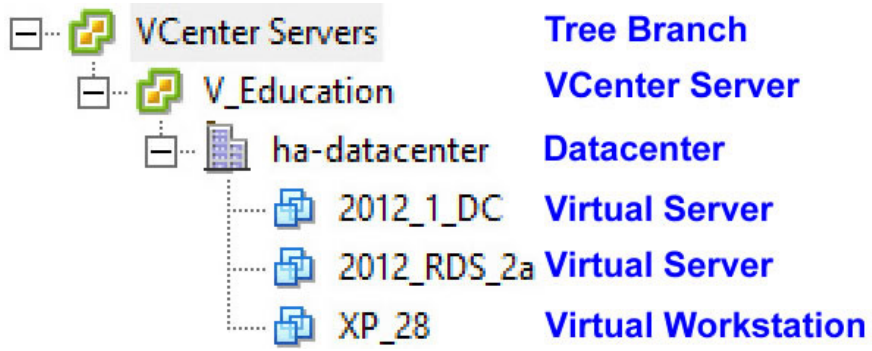
The Globe icon represents the Locations Tree Branch, Locations, Parent Locations, and Sub-Locations.

Figure 36 - Locations Tree



VCenter Servers

Figure 37 - VCenter Servers



Icon	Represents
Green and Yellow Squares	Either the VCenter Tree Branch or a VCenter Server
Gray Building	A VCenter Server Datacenter
Blue Virtual Squares	A Virtual Machine, both server and workstation

ThinManager Web Browser User Interface

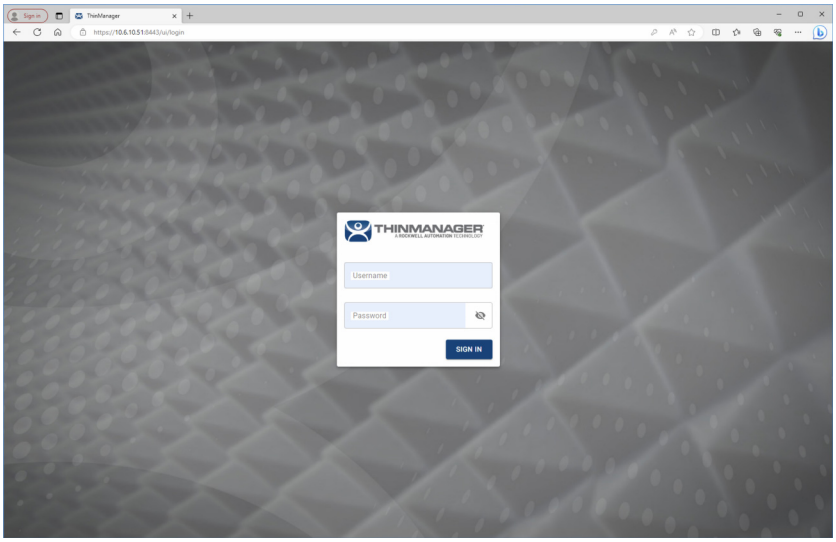
The ThinManager Web Browser User Interface is a read-only version of the ThinManager console, which can be used by designated users and groups, such as nonadministrative team members. Users are able to view asset configuration properties, shadow other terminals, and send terminal commands without the ability to alter the configurations themselves.

In order to access the Web Browser UI, the Web Client Endpoints must be enabled on the HTTPS Server Settings Page, under the Web Client Settings in the ThinManager Server Configuration Wizard. See Figure 866 on page 615 for more information.

Once the Web Client Endpoints are enabled, navigate to the following URL via the IP address of ThinServer: https://xx.xx.xx.xx:8443/ui/ to access the Web Browser UI.

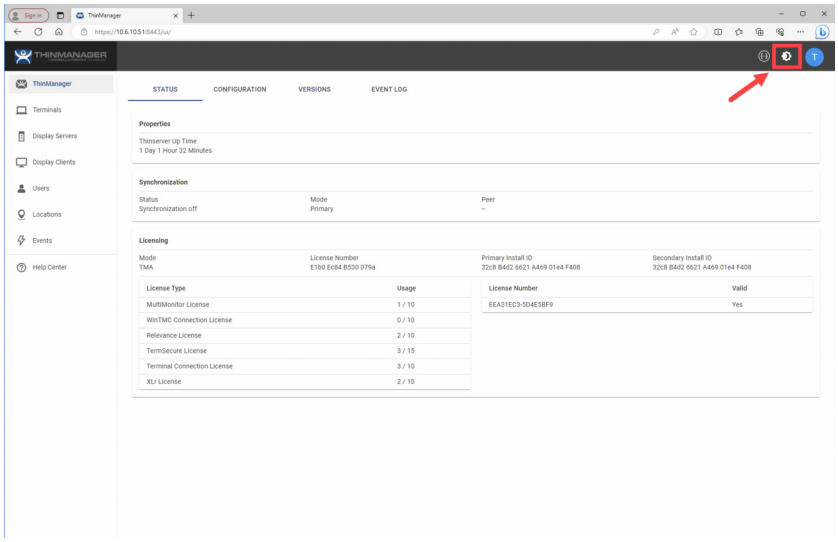
This browser-based user interface can be a display client and hosted by Remote Desktop Services or as a containerized and hosted display client.

Figure 38 - User Login Screen (Active Directory or ThinManager User Capable)



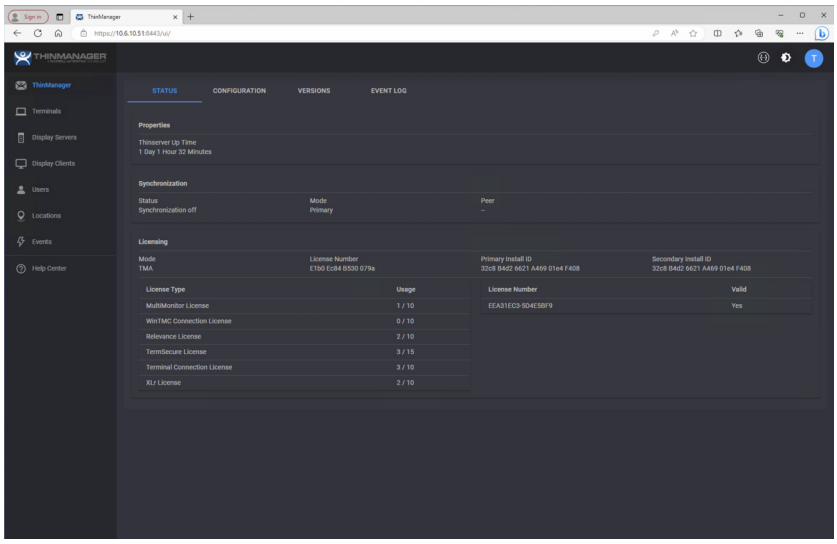
1. Enter the username and password of any user that is part of a valid ThinManager Security Group on the ThinManager Security Groups page of the ThinManager Server Configuration Wizard. See Figure 850 on page 602 for more information.

Figure 39 - ThinManager Status tab



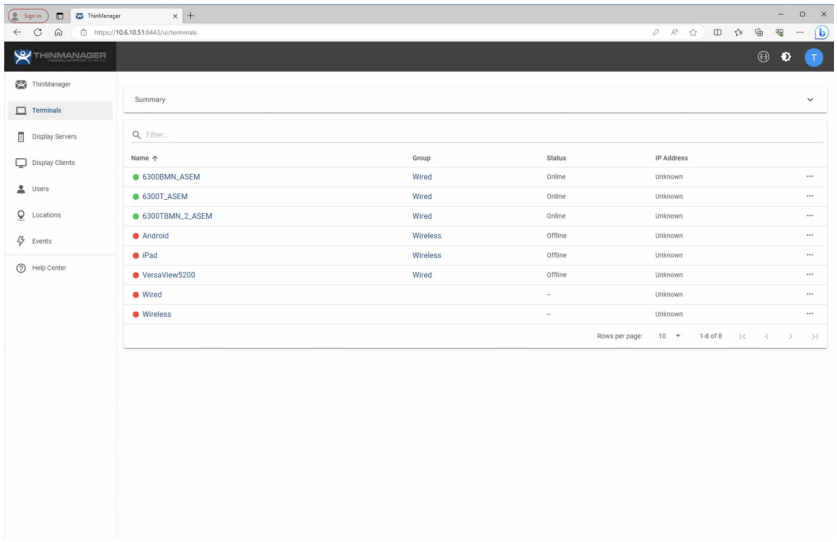
2. Click the sunburst icon to toggle between light and dark modes.

Figure 40 - Dark Mode



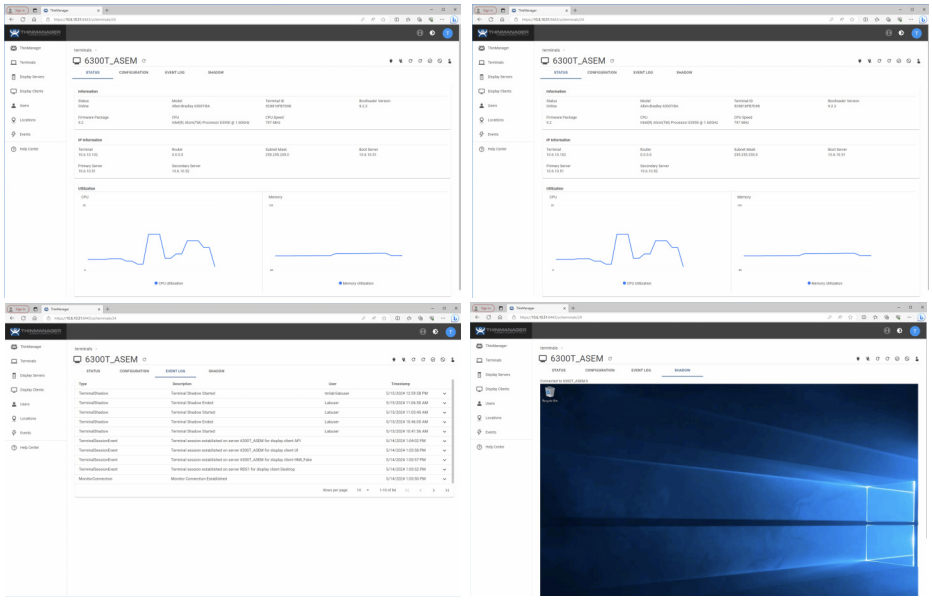
3. Click Terminals in the menu in the left panel.
   The Summary screen appears.

Figure 41 - Terminals Summary



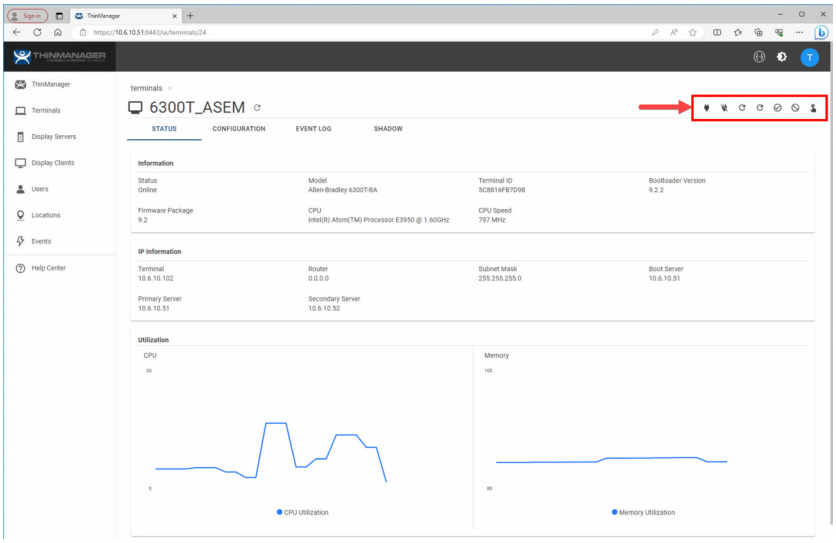
View your ThinManager Configuration, as well as environment elements, as you would in the ThinManager Graphical Interface. This includes ThinManagerServers, Terminals, Display Servers, Display Clients, Users, Locations, and Events.

Figure 42 - Terminals Status, Configuration, Event Log, and Shadow screens



Also, the browser-based user interface givesusers basic terminal functionality, including Power On, Power Off, Restart, Reboot, Enable, Disable, and Calibrate. See Figure 43 for an example of these functionality icons.

Figure 43 - Terminal Functionality Icons



Licenses

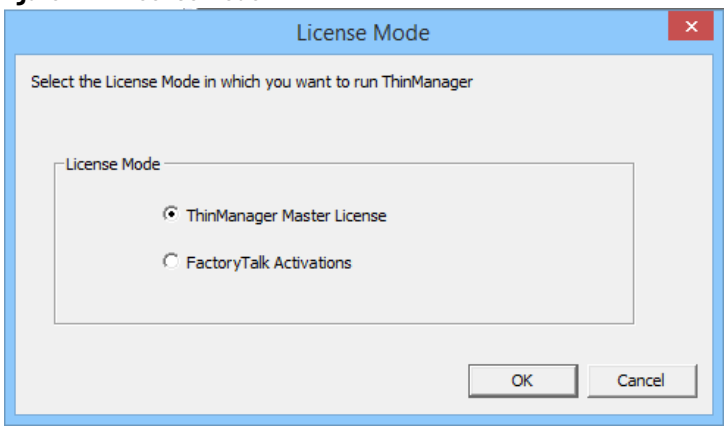
ThinManager has two license modes, ThinManager Master License and FactoryTalk Activations.

To choose the licensing mode, follow these steps.

1. Choose Install>License Mode from the ThinManager menu.

   The License Mode dialog box appears.

Figure 44 - License Mode



   a. To choose ThinManager Master License Mode, click ThinManager Master License.

   b. To choose FactoryTalk Activations License Mode, click FactoryTalk Activations.

2. Click OK.

ThinManager Master License

ThinManager Master License is the traditional ThinManager license, which is comprised of three components.

Component	Description
Product License	Provides permission for terminals to connect, and controls which features and functions the terminals have. Purchase from a ThinManager distributor.
Master License	A container for the Product Licenses, which is created by the user on the ThinManager License site and has the Product Licenses added to it. Activated with the Installation ID from the Licensing dialog box of the ThinManager application.
Activated License File	A file generated from the Master License and Installation ID on the ThinManager License site. Download and apply to ThinManager.

Product Licenses are connection licenses purchased from ThinManager distributors. V-FLEX licenses, which are flexible volume licenses, are available.

Greater detail on ThinManager licenses can be found in the ThinManager Knowledge Base at https://kb.thinmanager.com/index.php/License_Activation. Another good reference can be found here, https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1090218/loc/en_US#__highlight.

ThinManager Redundancy

Standard product licenses are available with redundancy. Enterprise server licenses include full redundancy.

Redundancy Type	Description
Full Redundancy	Licenses a synchronized pair of ThinManager servers so that one ThinManager server is available if the other is offline. Both synchronized ThinManager servers have the administrative console available.
Mirrored Redundancy	Licenses a synchronized pair of ThinManager servers so that one is available if the other is offline, but this option only activates the administrative console on one ThinManager server—the one designated as the primary ThinManager server. The other ThinManager server is designated as the secondary ThinManager server. From the secondary server, terminals can boot, but the ThinManager console is view-only.
Stand-Alone ThinManager	Licenses one stand-alone ThinManager. If the stand-alone ThinManager goes offline, the terminals continue to run. However, if a terminal reboots, it waits until the ThinManager server is online before it can rejoin the system.

Auto-synchronization for Redundancy

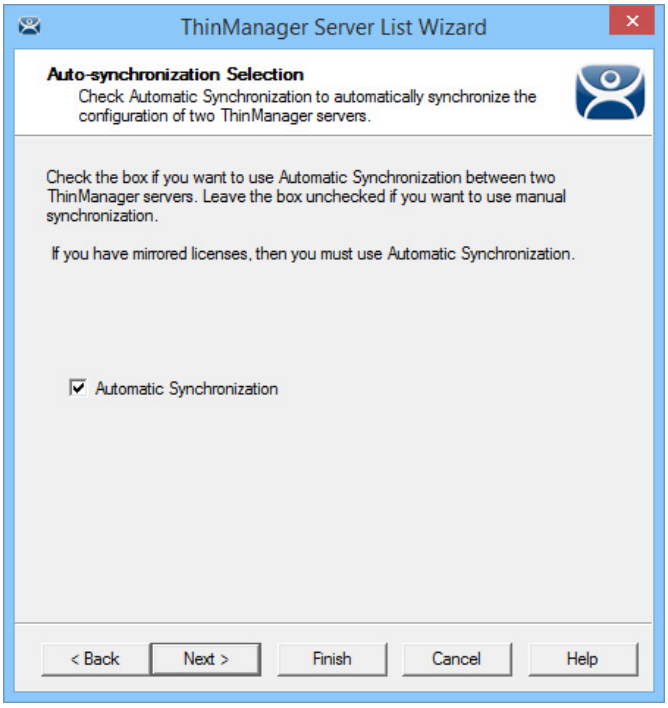
To have a Redundant ThinManager system, configure Auto-synchronization as described in the following steps.

1. From the menu bar on your Primary ThinManager Server, choose Manage>ThinManager Server List.

   The ThinManager Server List Wizard Introduction page appears.
2. Click Next.

   The Auto-synchronization Selection page appears.

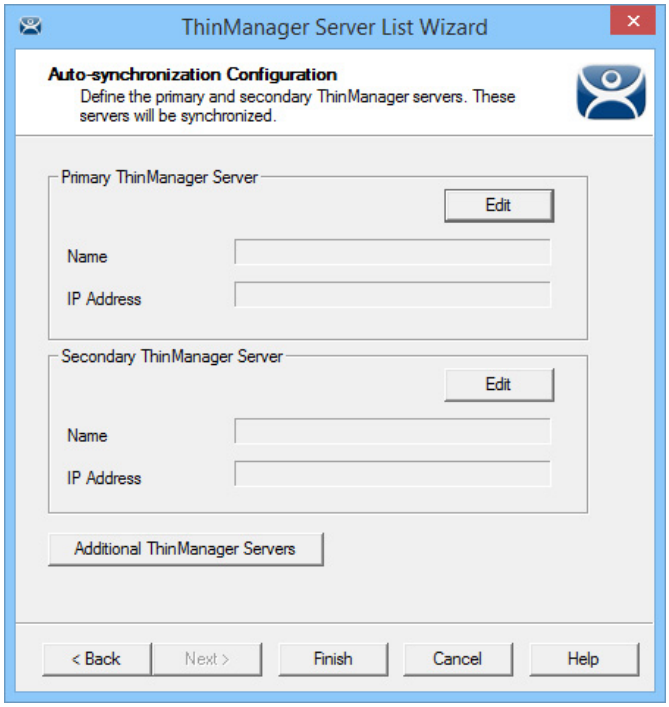
Figure 45 - Auto-synchronization Select Page



3. Check Automatic Synchronization and click Next.

   The Auto-synchronization Configuration page appears.

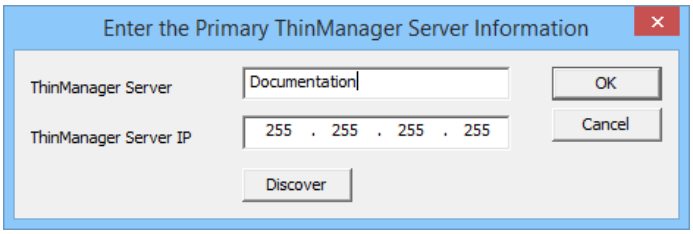
Figure 46 - Auto-synchronization Configuration Page



4. Click Edit in the Primary ThinManager Server section.

   The Enter the Primary ThinManager Server Information dialog box appears.

Figure 47 - Enter the ThinManager Server Information



a. Enter the name of your Primary ThinManager Server in the ThinManager Server field.

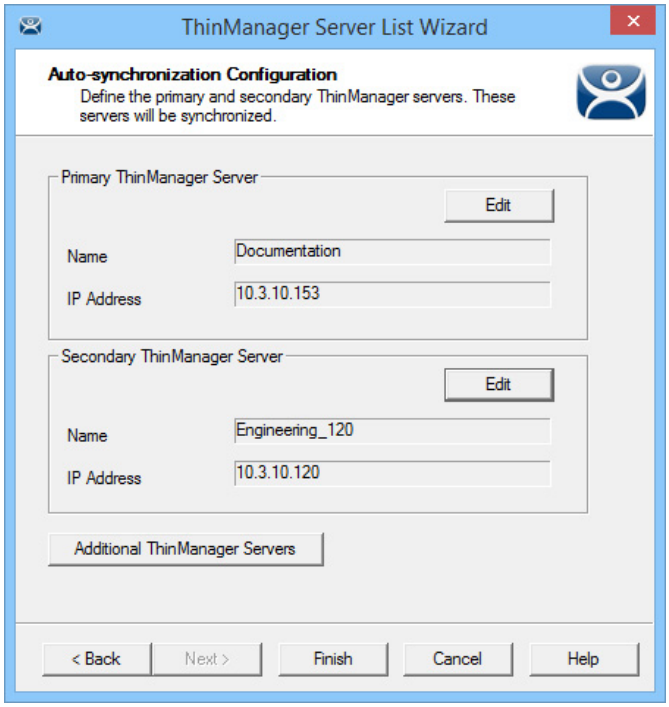
b. Click Discover to automatically populate the IP address in the ThinManager Server IP field. However, this field can be completed manually.

Do not click Discover to complete the ThinManager Server IP field manually.

c. Click OK.

5. Repeat step 4 for the Secondary ThinManager Server.

Figure 48 - Auto-synchronization Configuration Page

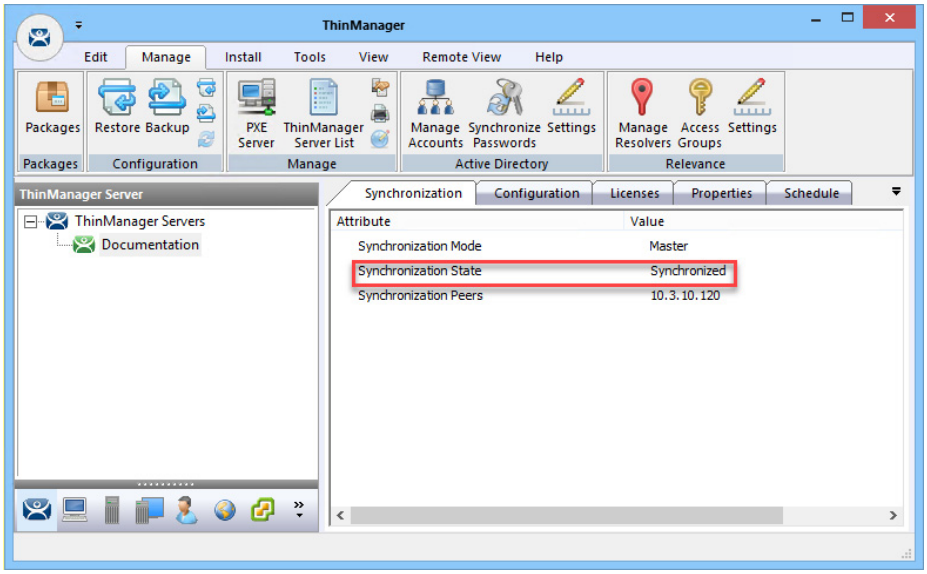


6. On the Auto-synchronization Configuration page, click Finish to begin auto-synchronization.

IMPORTANT With a Mirrored Redundancy License, it is important to select the Primary and Secondary ThinManager Servers carefully because only the Primary ThinManager Server has an administrative console. The Secondary ThinManager Server administrative console is view-only.

7. Highlight the ThinManager Server.

Figure 49 - Synchronization Tab



a. On the Synchronization tab, verify that the server's Synchronization State indicates 'Synchronized'.

Manual Synchronization for Redundancy

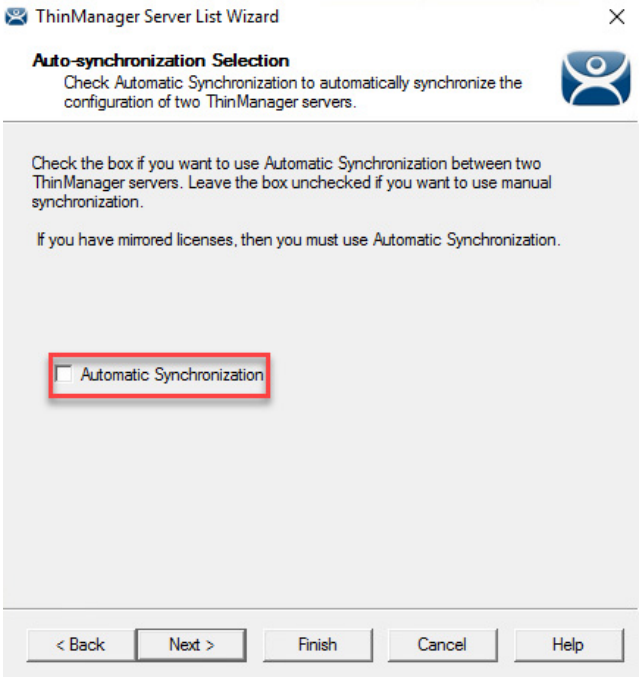
Follow these steps to use manual synchronization with a redundant ThinManager system.

1. On your Primary ThinManager Server, in the ThinManager Server tree, highlight the green ThinManager icon.
2. From the menu bar, choose Manage>ThinManager Server List.

   The ThinManager Server List Wizard Introduction page appears.
3. Click Next.

   The Auto-synchronization Selection page appears.

Figure 50 - Clear Automatic Synchronization Checkbox



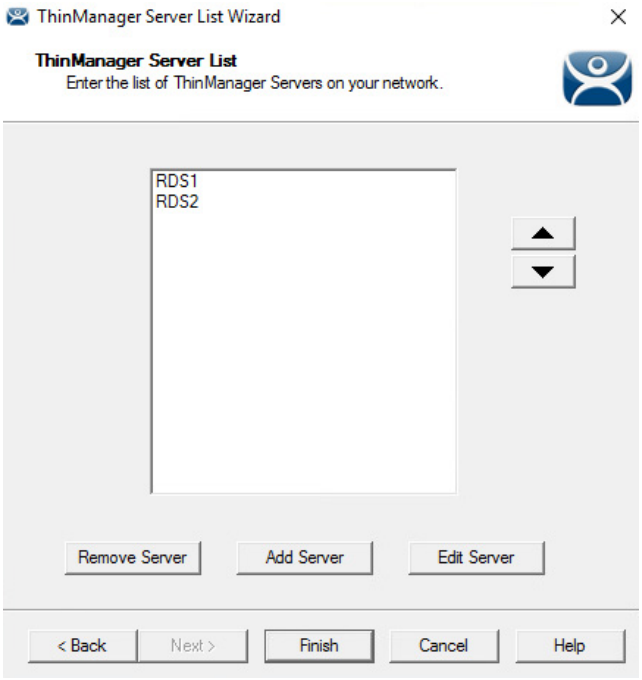
4. For manual synchronization, clear the Automatic Synchronization checkbox.

With mirrored licenses, you must use Automatic Synchronization.

5. Click Next.

   The ThinManager Server List page appears with your network ThinManager Servers displayed.

Figure 51 - ThinManager Server List Page

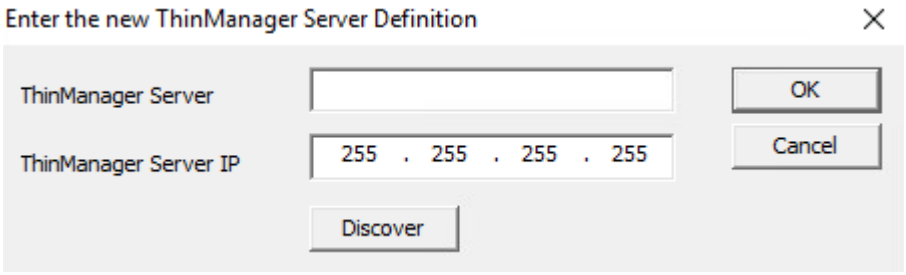


6. (Optional) Highlight a server and use the up and down arrows to change the order of the servers in the list.

7. (Optional) Highlight a server and click Remove Server to eliminate it from the ThinManager server list.
8. (Optional) Click Add Server to add a server to the list.

   A dialog box appears, in which you can define a new ThinManager server.

Figure 52 - ThinManager Server Definition Dialog

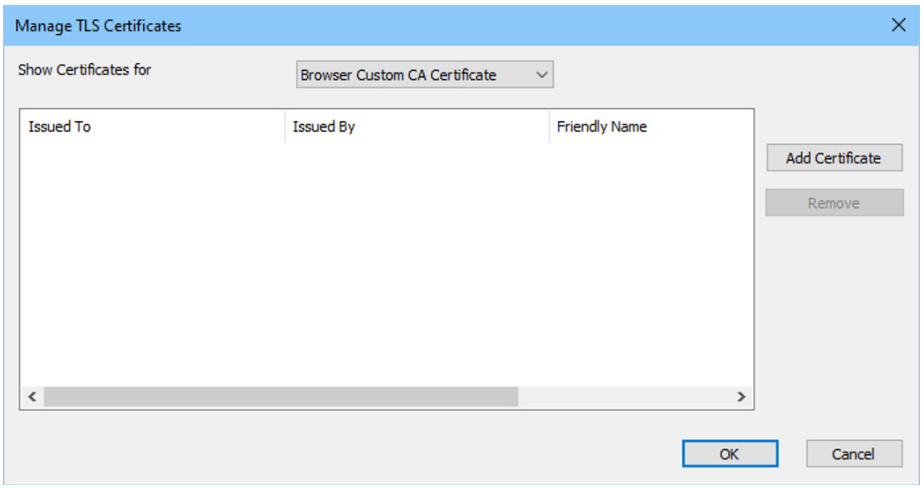


   a. Enter a ThinManager Server name.
   b. Click Discover to automatically populate the ThinManager Server IP field. Also, this field can be completed manually.
   c. Click OK.
9. Click Finish to complete your changes.

Synchronization Certificate Authentication

ThinManager provides the option to specify custom TLS certificates for ThinManager Server synchronization.

Figure 53 - Manage TLS Certificates



Follow these steps to load these new certificates onto your ThinManager server.

1. At the Manage TLS Certificates window, choose ThinManager Server Synchronization from the Show Certificates for pull-down menu. This action allows you to choose the type of certificate to use.
2. Select Add Certificate.

If the Add Certificate button is disabled, it is likely because there is already a certificate for ThinManager Server Synchronization. To ensure the list is empty, click the top row and then the Remove button.

3. From the Choose a Certificate window, either select an existing certificate from the Microsoft Certificate Store, or click Import. If you choose Import, then you can import an external certificate or generate a new certificate.

The remote server's certificate must be trusted by the local server. Do this by importing the synchronization partner's certificate into the local server's Microsoft Certificate Store. Either a self-signed certificate or a certificate generated by a trusted root may be used. If a partner ThinManager server fails and is replaced, you may have to update the certificates on one or both servers.

4. Click OK.

The default ThinManager installation does not use a certificate, which generates a ThinManager Synchronization failure due to no installed TLS certificates when upgrading from previous versions.

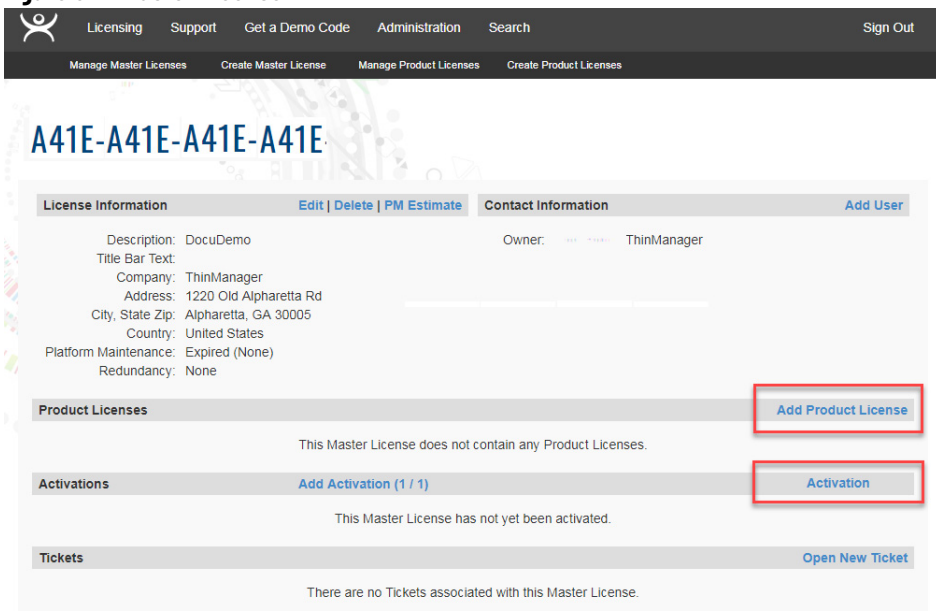
ThinManager License Process

Follow these steps to license ThinManager.

1. Purchase a Product License from a ThinManager distributor.
2. If you have a redundant product license, synchronize two ThinManager Servers. See Auto-synchronization for Redundancy on page 42.
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. Click the Create Master License link on the License Site menu bar.
6. Enter a description and complete the other fields.
7. Click Create.

   The License site displays the Master License.

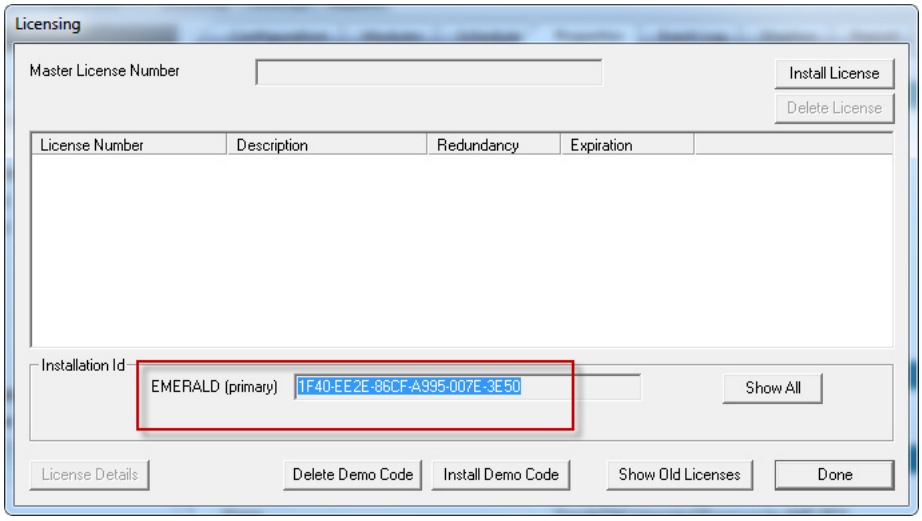
Figure 54 - Master License



8. Click Add Product License and enter the Product License.
9. Once the Product License is added, click Activation.

The Licensing dialog box appears.

Figure 55 - Stand-alone ThinManager Installation ID

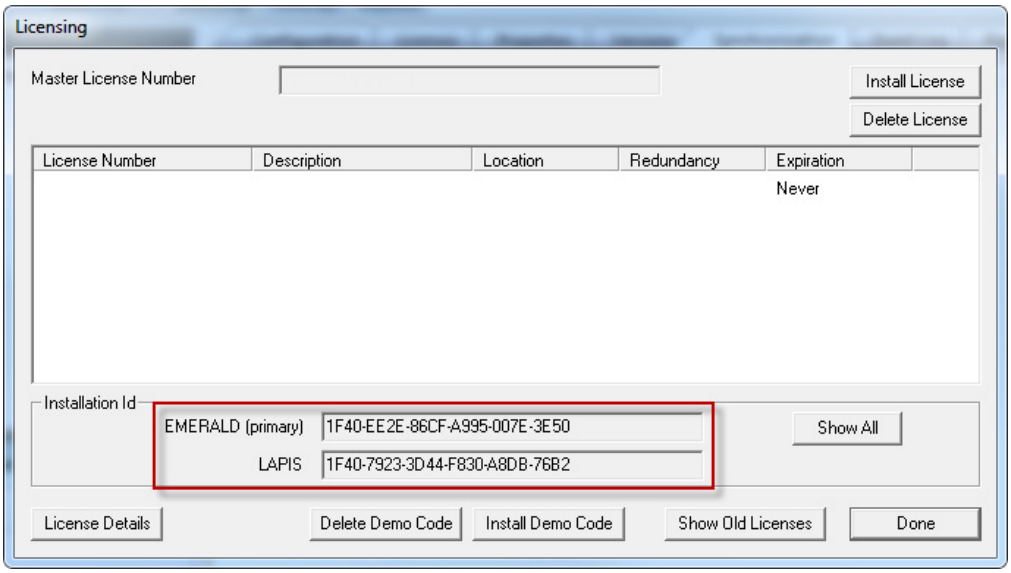


10. Enter the Installation IDs, which are found in the Licensing dialog box when you choose Install>Licenses.

    A stand-alone ThinManager has a single Installation ID at the bottom of the Licensing dialog box.

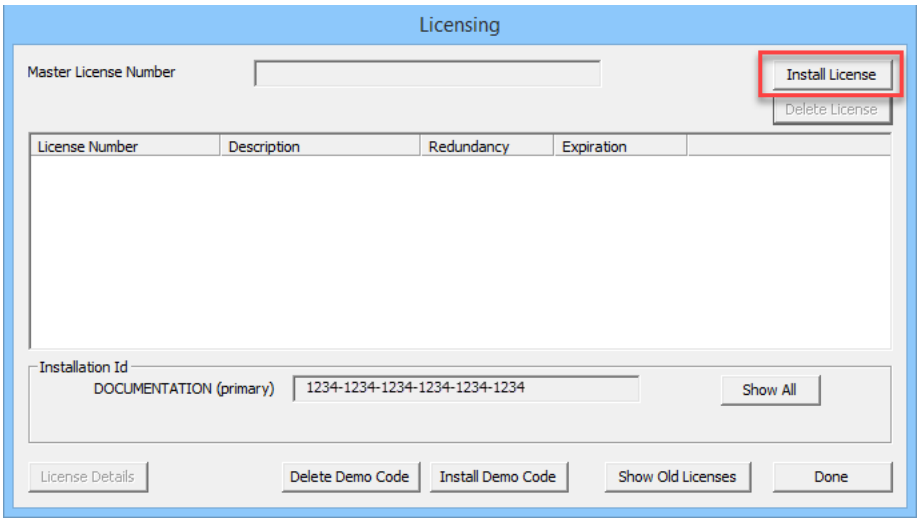
    A synchronized ThinManager system displays both the Primary and Secondary Installation IDs at the bottom of Licensing dialog box.

Figure 56 - Primary and Secondary Installation IDs



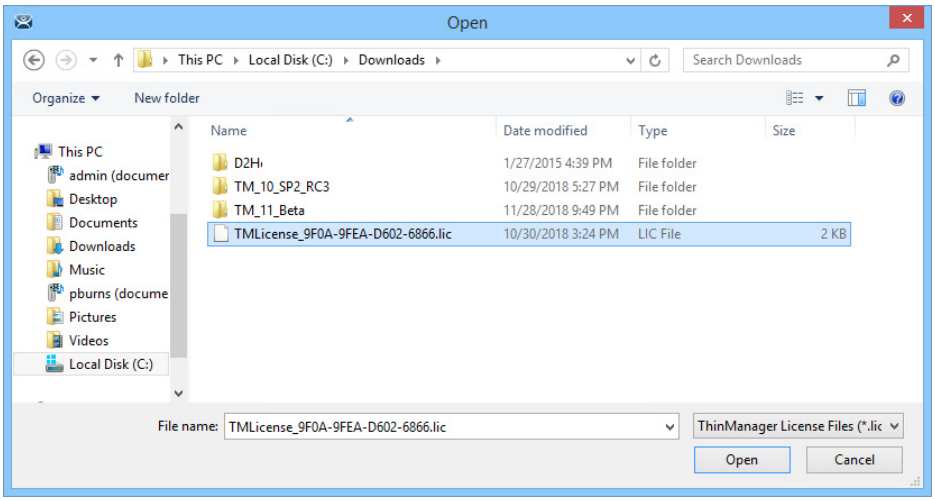
11. Once the Installation IDs are added, scroll down and click Create at the bottom of the Master License form.
12. Click the Download License link and save the license file.
13. Move the license file to the ThinManager Server but not into the ThinManager folder.
14. Choose Install>Licenses in the ThinManager menu to open the Licensing dialog box.

Figure 57 - Install License



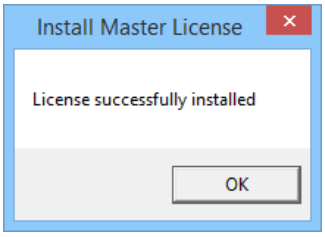
15. Click Install License.

Figure 58 - File Browser



16. Browse to the License file and click Open.

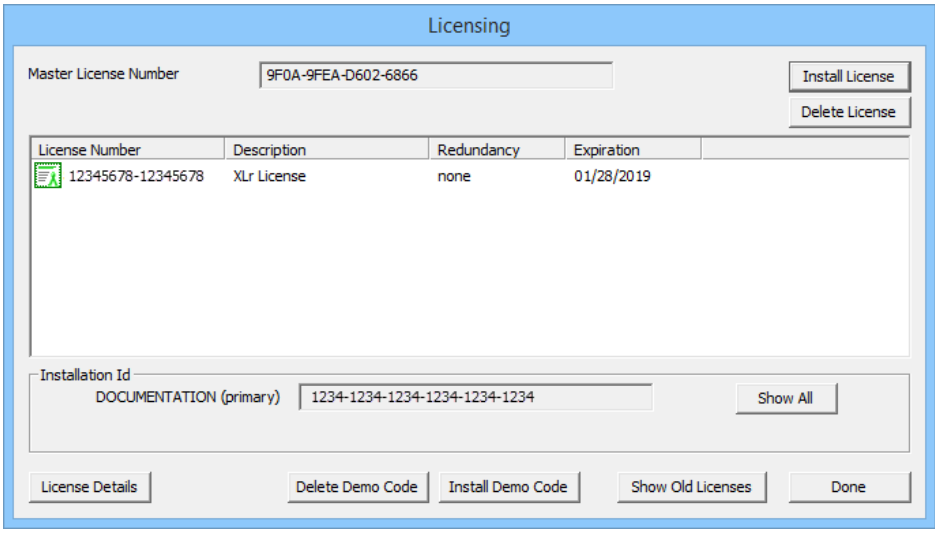
Figure 59 - Install Master License



A properly installed license is indicated.

17. Click OK.

Figure 60 - Installed License



A successfully installed license is shown in the Master License Number field, the Product Licenses are listed in the center section, and the Installation ID shows in the bottom field.

18. Click Done.

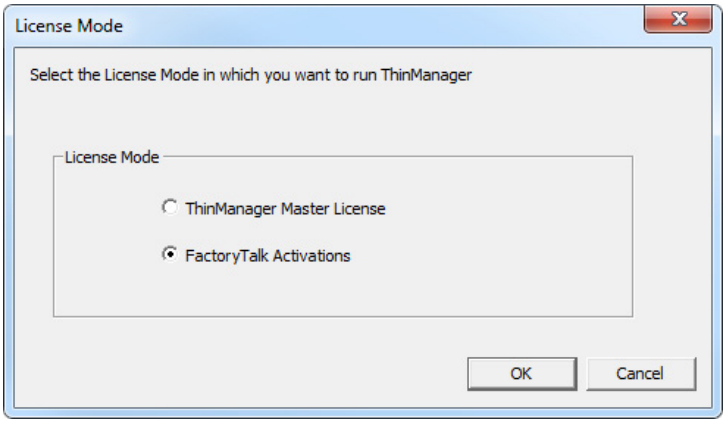
FactoryTalk Activations

The other license mode—besides ThinManager Master License—is FactoryTalk Activations.

Follow these steps to enter FactoryTalk Activations mode.

1. From the ThinManager menu, choose Install>License Mode to open the License Mode dialog box.

Figure 61 - License Mode



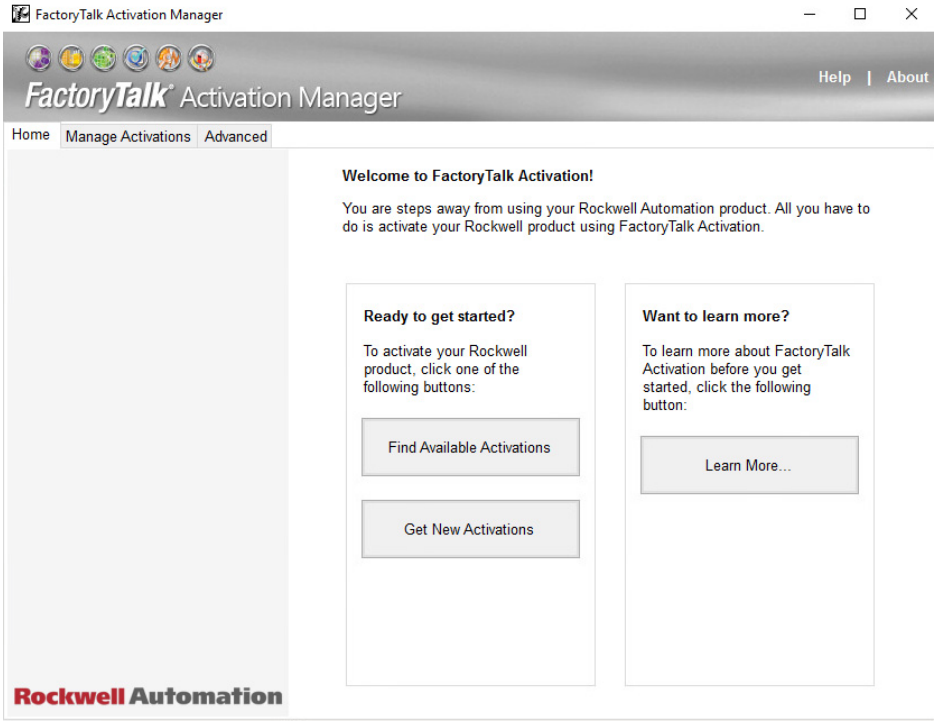
2. Click FactoryTalk Activations and OK.

FactoryTalk Activation Files

FactoryTalk Activation binds Rockwell Automation software product licenses to specific devices. Without activation, some Rockwell Automation products do not run, run with less than full functionality, or they run for a limited time and shut down. Therefore, before you can proceed with FactoryTalk

Activations in ThinManager, you must create activation files via the FactoryTalk Activation Manager.

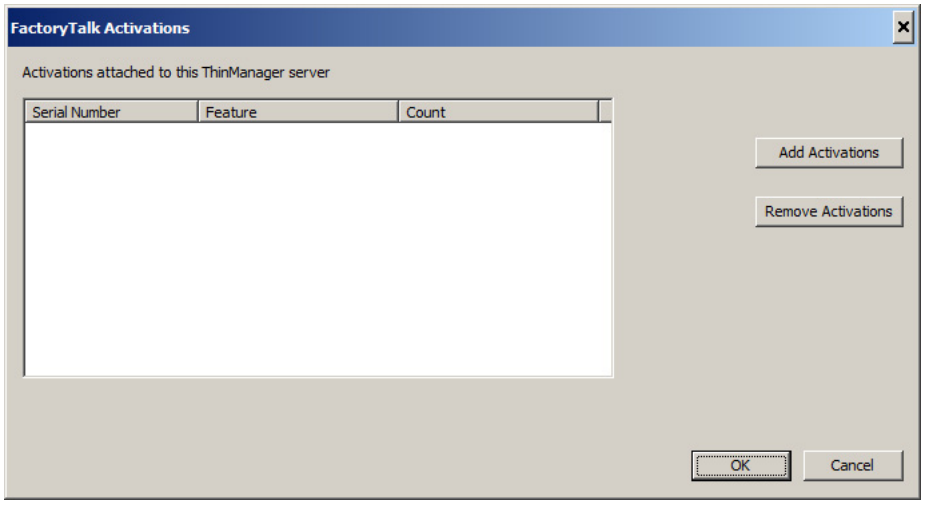
Figure 62 - FactoryTalk Activation Manager Home



When FactoryTalk Activation Manager is started, it detects whether an Internet connection exists. Available options for obtaining new activations differ depending on your Internet connectivity status. In FactoryTalk Activation Manager, click Help to find instructions on activation options.

3. Return to ThinManager and choose Install>Licenses to open the FactoryTalk Activations dialog box.

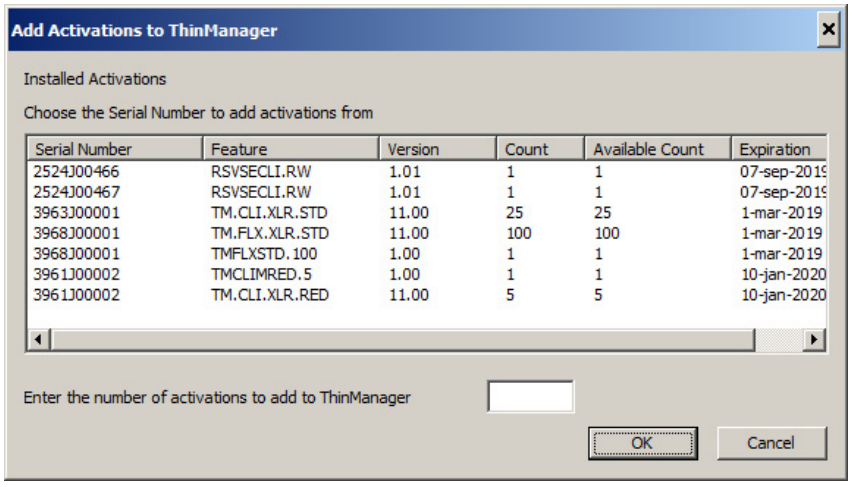
Figure 63 - FactoryTalk Activations



4. Click Add Activations.

The Add Activations to ThinManager dialog box appears, searches for and displays FactoryTalk activations.

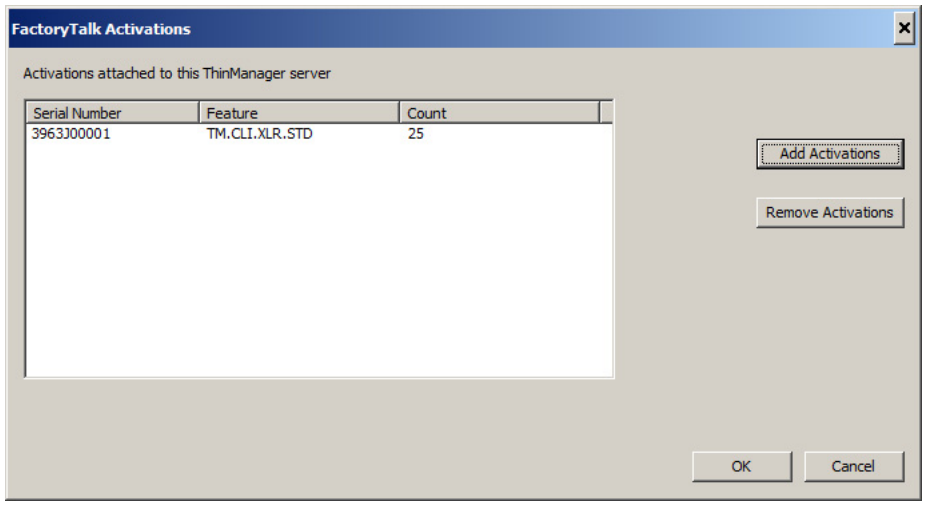
Figure 64 - Add Activations to ThinManager



5. Highlight the license to use with ThinManager, and, when enabled, in the Enter the number of activations to add to ThinManager field, specify how many licenses to add.
6. Click OK.

   The FactoryTalk Activations dialog box appears and shows the FactoryTalk licenses transferred.

Figure 65 - FactoryTalk Activations



7. Click OK.

Notes:

ThinManager System

There are three types of ThinManager system users: Windows™ Users, ThinManager Security Group Users, and ThinManager Users. The Windows Users may be local or domain accounts.

Windows Users

Windows Users are the Microsoft™ accounts created in Windows that allow access to the Windows Remote Desktop Servers. These are configured within, 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.

As a Microsoft best practice, each Terminal or Location needs a unique Windows account.

It is always a best practice to follow the principle of least privilege. Provide accounts used for auto-login of Windows sessions only with the privilege required to access the desired applications. For example, never use a Domain Administrator for auto-login.

ThinManager 8 introduced Active Directory integration to the ThinManager system, which is covered in Active Directory User Login Account on page 301.

ThinManager Security Group Users

ThinManager Security Group Users are Windows User Group members who were configured, in the ThinManager Server Configuration Wizard, to have varying levels of access and control within the ThinManager program. This pertains to access to the administrative console of ThinManager, 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 593.

ThinManager Users

ThinManager Users can go to a ThinManager-ready thin client and receive access to specific display clients based on their membership in an Access Group. ThinManager performs authentication a level above the Windows login. Formerly called TermSecure, this feature is currently integrated into the Relevance suite of functions.

ThinManager User Services give additional powers to grant or deny access to Windows applications but still rely on a Windows user account to log in to a Remote Desktop Server.

The following are various strategies for ThinManager Users.

- For a Terminal-specific Application, a user does not need a Windows account; but permission from an Access Group is required to open a hidden application.
- If a user is accessing their own User-specific Applications, they need a Windows account associated with them so they can log in and start these sessions. The ThinManager User can be created:
  - From an Active Directory account
  - To match the name of a Windows account, and use that Windows account without using Active Directory
  - With one name and be associated to a Windows account of a different, aliased name

See Active Directory User Login Account on page 301 for details.

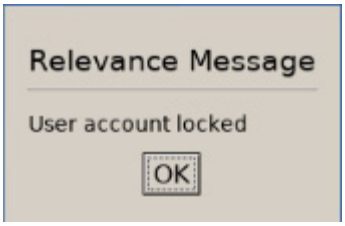
ThinManager User Manual Unlock

Locked ThinManager User accounts that are not Active Directory accounts can be manually unlocked in the ThinManager Admin Console. Typically, user accounts are locked after excessive unsuccessful login attempts. The number of attempts allowed is set by the Account Lockout Policy setting in ThinManager. Locked ThinManager ThinManager User accounts can be unlocked at any time, regardless of the Account Lockout Period duration.

When Active Directory user accounts are locked due to excessive incorrect login attempts, the account must be unlocked in Active Directory.

Locked ThinManager User accounts are indicated by a dialog box displayed on the terminal. See Figure 66.

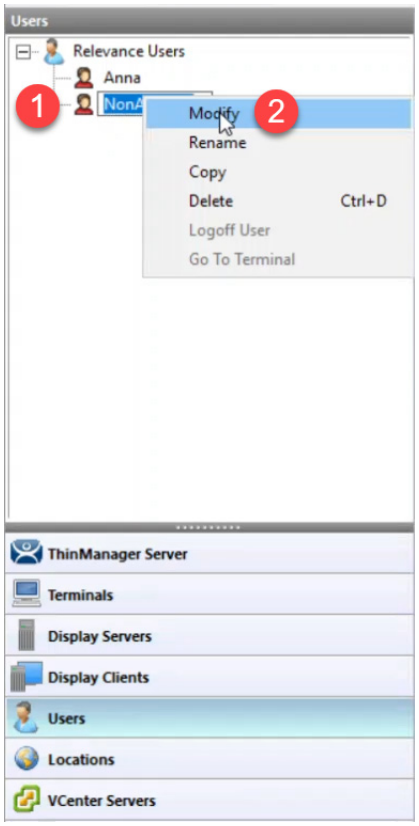
Figure 66 - ThinManager User Account Locked



To manually unlock a ThinManager User account, follow these steps.

1. Click OK in the dialog box on the terminal.

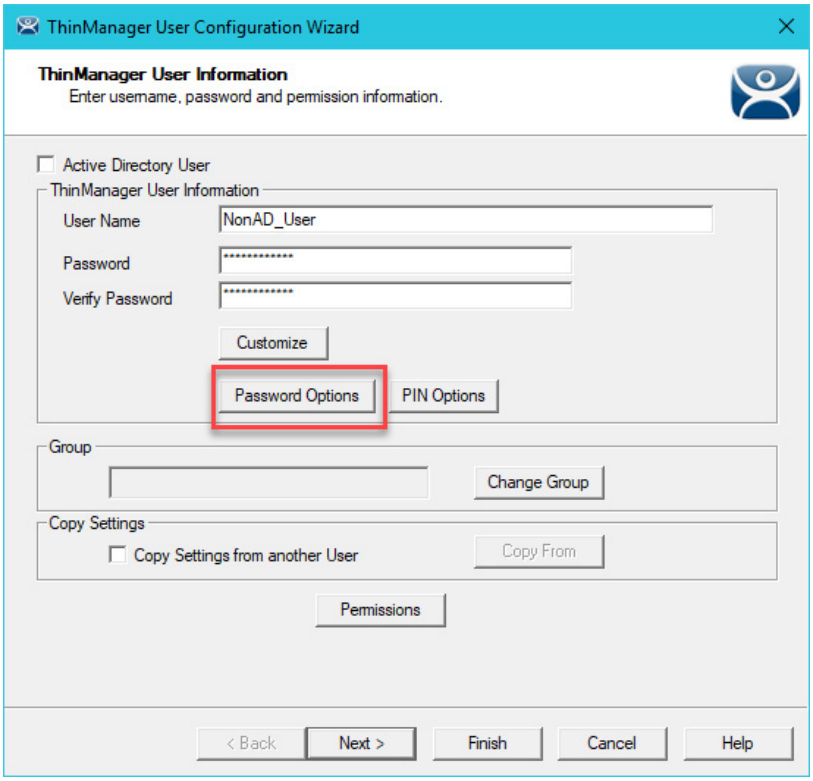
Figure 67 - ThinManager Users Pane



2. In ThinManager Admin Console, click Users to display the non-Active Directory user account.
3. Right-click on the locked user account, and then click Modify.

   The ThinManager User Information page of the ThinManager User Configuration Wizard appears.

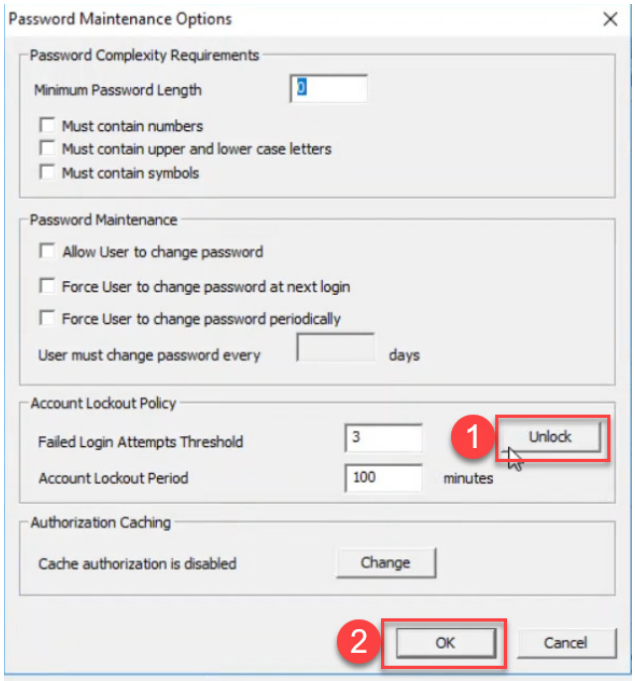
Figure 68 - ThinManager User Information page



4. Click Password Options.

   The Password Maintenance Options page appears.

Figure 69 - Password Maintenance Options page



5. Click Unlock, and then click OK to close the wizard.

   The user account is unlocked. Return to the terminal and attempt to log in to the user account again.

TLS Certificates

Complete management of a thin client solution sometimes requires connections to outside applications, logs, or servers. To secure those connections, certificates can be utilized or generated by ThinManager.

With ThinManager 14.1, certificates are no longer stored within the ThinManager configuration database. Instead, ThinManager utilizes the Microsoft Certificate Store and only stores the Certificate Store Name and the thumbprint of the selected certificate(s) in the ThinManager configuration database. Upon an upgrade to 14.1 from an earlier version, any stored certificate within the ThinManager configuration database is migrated automatically to the Microsoft Certificate Store.

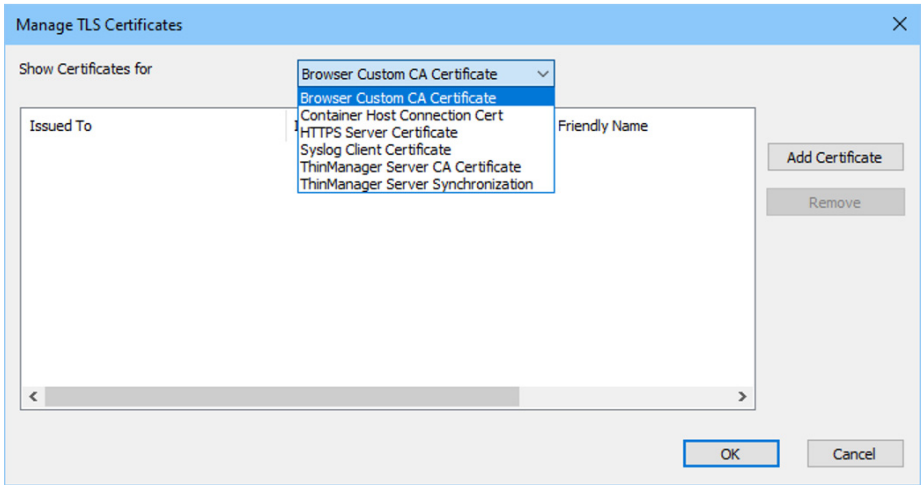
The Browser Custom CA Certificate allows for installation of a certificate to secure communications with web-based applications. When you leverage a web browser container display client on a terminal, ThinManager must be made aware of the web server's certificate to which the client connects.

ThinServer hosts an internal HTTPS server, which can be leveraged for the boot process instead of TFTP. Also, the HTTPS server must be enabled in order to use the API endpoints. For connection to the API, the HTTPS server certificate must be installed to have secure communication. The certificate can be generated in ThinManager and installed in the directory where your web browser is directed to look for certificates. The default for many web browsers is the Trusted Root Certification Authorities directory.

The Syslog Client Certificate allows for secure connections when syslog logging is enabled. For more information, see SysLog Configuration Page on page 598.

For Docker® Container Hosts, a TLS Certificate is needed to provide secure authentication between the Container Host and the ThinServer service. There are two certificates and one key that must be generated in ThinManager and copied to the Container Host. First, the ThinManager Server CA Certificate (formerly called the Docker Server CA Certificate) is required to establish a connection to a Docker server-hosted container. The second required certificate is the Container Host Connection Cert (formerly generated in Container Host Wizard). For more details, see Install the TLS Certificates on page 110.

Figure 70 - Manage TLS Certificates

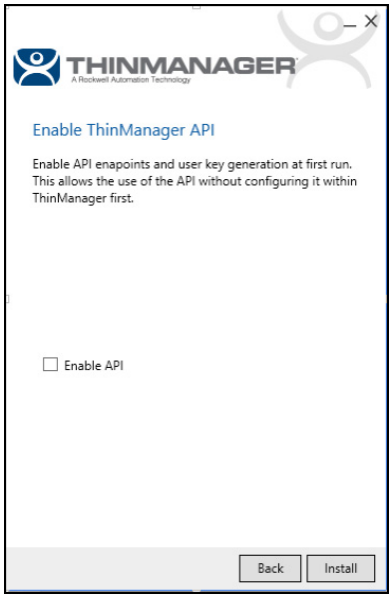


API

Representational State Transfer (REST)-conforming API can be used to assist in deployment and maintenance of the ThinManager system.

The API can be enabled during ThinManager installation, or post-installation, via the ThinManager Server Configuration Wizard for versions 13 and later. An optional checkbox appears in the installer.

Figure 71 - Enable API checkbox



API endpoint documentation is intended to be accessed via a web browser, which can be found at https://[thinserverhostIP]:[HTTPS port]/api/documentation. For example, to connect with the default port when ThinServer is installed on the local host, navigate to https://localhost:8443/api/documentation. The API supports GET, POST, PUT, and DELETE methods.

See HTTPS Server Settings Page on page 614 for more details.

Sources

There are three possible ThinManager sources: Remote Desktop Servers, IP Cameras, and VNC Server.

Remote Desktop Servers

Microsoft servers with Remote Desktop Services, formerly known as Terminal Services, provide the foundation of thin client computing, which consolidates management of the Windows environment to mainframe architecture. In this document, Remote Desktop Server refers to the computer and operating system, while Remote Desktop Services refers to the connection using the Remote Desktop Protocol.

To configure Remote Desktop Servers as sources:

- 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.

Microsoft Configuration

Refer to Microsoft for instructions on the use and configuration of a Microsoft server.

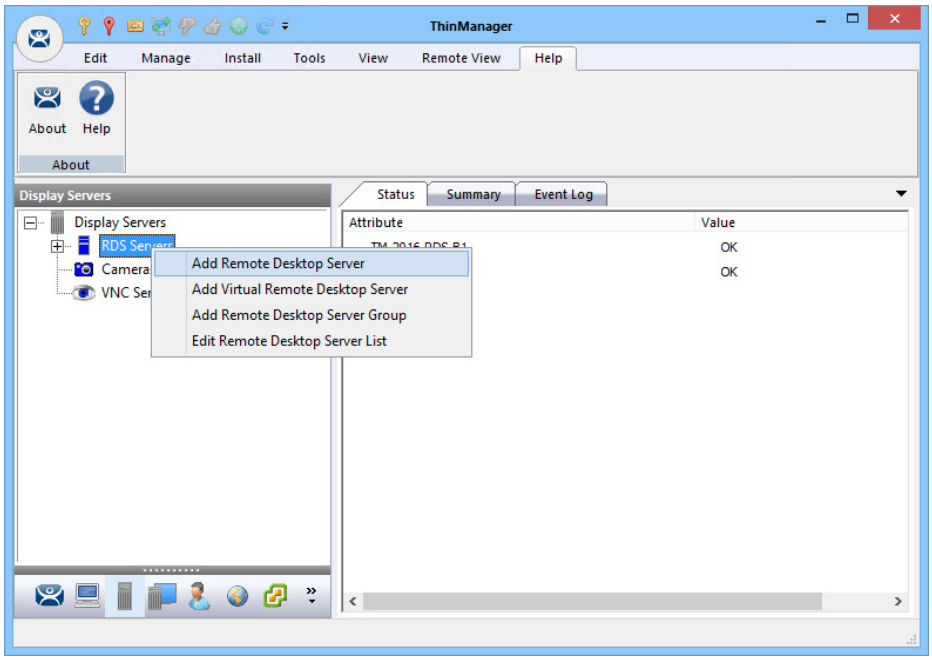
Here are a few common tips.

- Build a Remote Desktop Server with Microsoft 2008, 2008R2, 20012, 2016 or 2019 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 (RDS CAL) for each thin client. These are called Terminal Services Client Access Licenses (TS 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.

Defining Remote Desktop Servers in ThinManager

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

Display Servers Branch of the ThinManager Tree



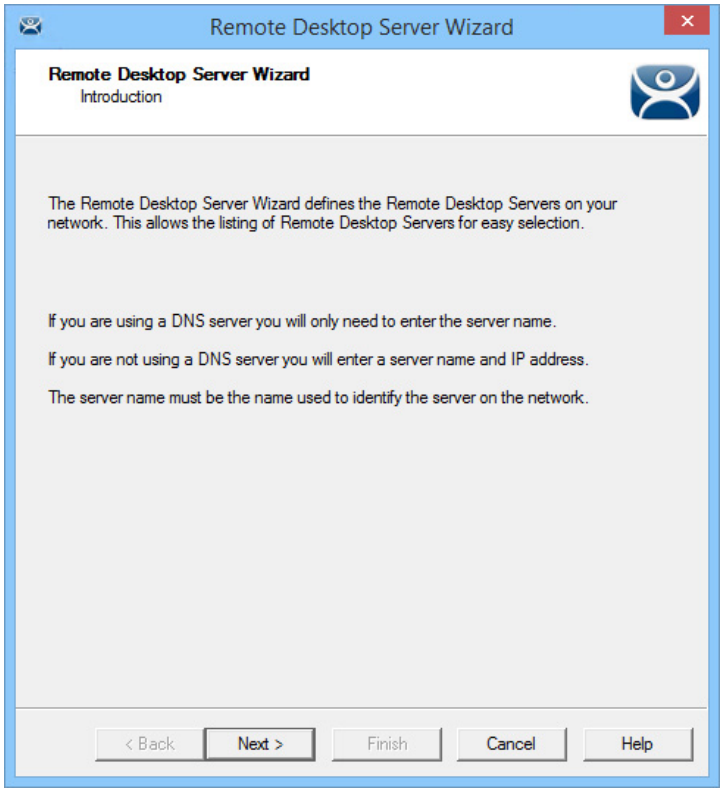
Perform the following to define Remote Desktop Servers as Display Servers.

1. Right-click RDS Servers in the Display Servers branch of the ThinManager tree.
2. Choose Add Remote Desktop Server to launch the Remote Desktop Server Wizard Introduction page, which provides instruction about DNS servers.

IMPORTANT If you are using a DNS server, click Cancel to close the Remote Desktop Server Wizard. Click Manage>DNS Configuration. The Domain Name Server Wizard appears where you define a DNS server.

3. Click Next.

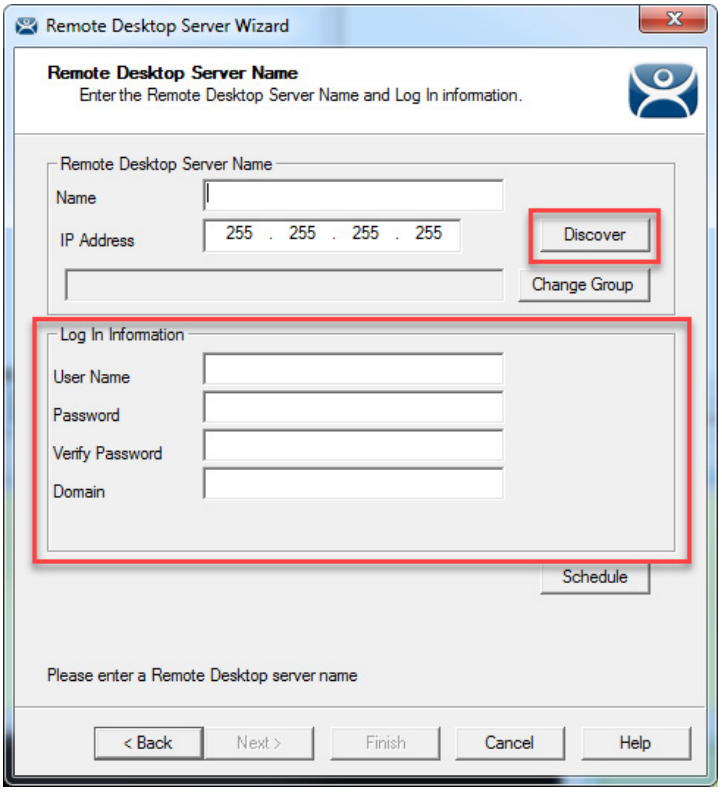
Figure 72 - Introduction - Remote Desktop Server Wizard



Non-Domain Remote Desktop Server

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

Figure 73 - Remote Desktop Server Name Page – Non-Domain



To define the Remote Desktop Server, perform the following steps.

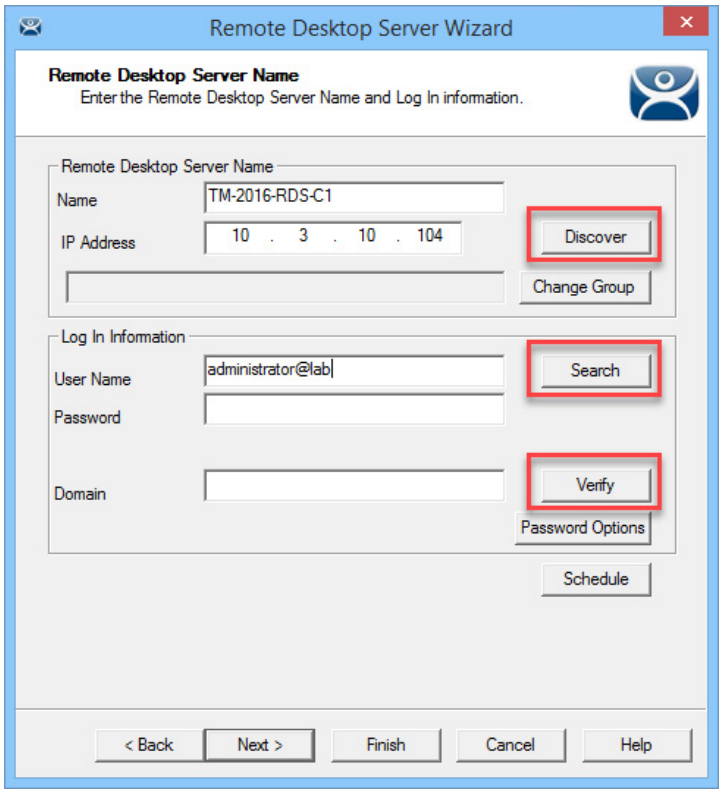
1. Enter the Remote Desktop Server Name.
2. Click Discover to validate the server name and auto-populate the IP address.
3. Complete the Log In Information fields to add an administrative account on the Remote Desktop Server.

   This step is required for SmartSession load balancing and server management from ThinManager as the Microsoft server only provides information to an administrator. The ThinServer connects to the Remote Desktop Server to retrieve CPU, Memory, and Session status for load balancing.
4. Click Change Group to add the Remote Desktop Server into a Remote Desktop Server Group.
5. Run the Remote Desktop Server Wizard for each Remote Desktop Server you want to add to the system.

Domain Member Remote Desktop Server

On the Remote Desktop Server Name page, the Search function allows you to search for a domain user account for the administrative login.

Figure 74 - Remote Desktop Server Name Page - Domain



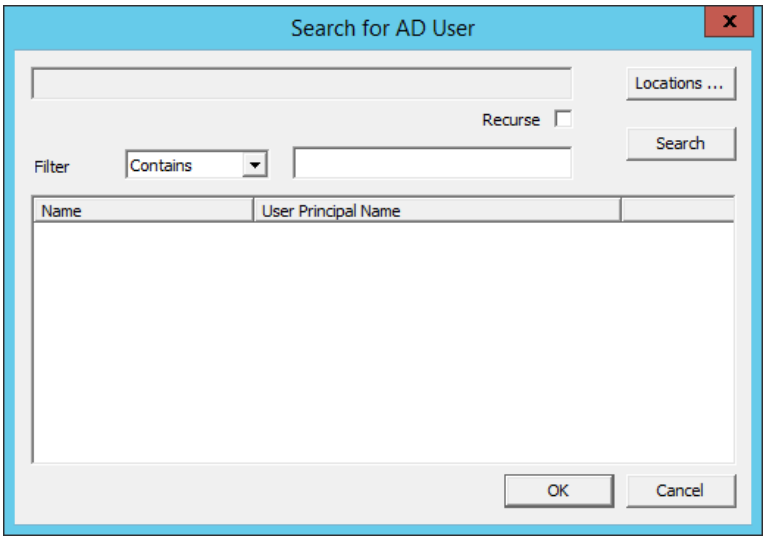
Perform the following to search for a administrative account.

1. Click Search.

   The Search for AD User dialog box appears, which allows you to select an Active Directory user.

This adds an administrative account to the Log In Information fields of the Remote Desktop Server Name page.

Figure 75 - Search for AD User

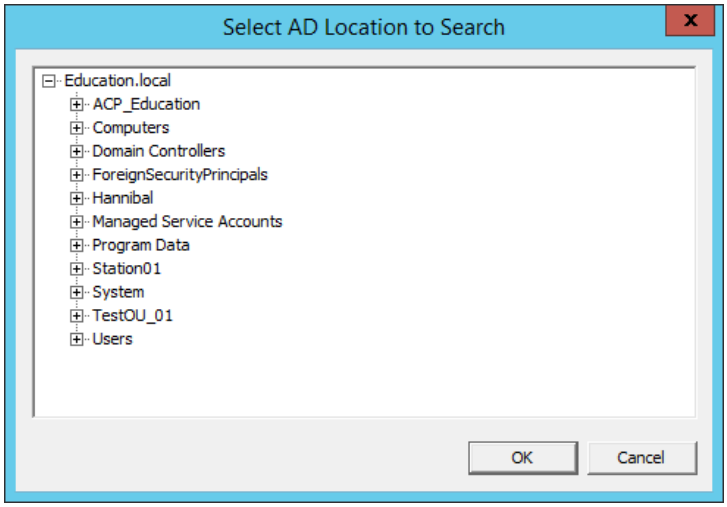


Feature	Description
Locations	Click and the Select AD Location to Search dialog box appears, where you choose which Organizational Unit (OU) to search
Recurse	Check this option to set the Search function to look in nested Windows Security Groups. To enable this function, set Choose AD Synchronization Mode to Security Group on the Active Directory System Settings dialog box to work. To open the Active Directory System Setting dialog box, click Manage>Active Directory>Settings.
Search	Searches the selected OU and populates the Name field with the OU members
Filter	Filters the results with either the Contains or Starts with function and the entry of the text box

2. Click Locations.

   The Select AD Location to Search dialog box appears.

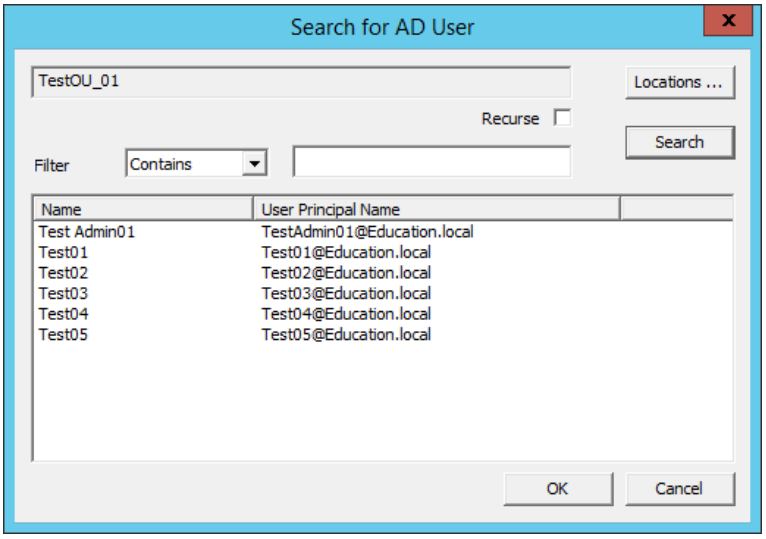
Figure 76 - Select AD Location to Search



3. Choose the branch of the Active Directory tree that contains the administrative user account.
4. Click OK.

The location appears in the Search for AD User dialog box with the list of domain users from that branch.

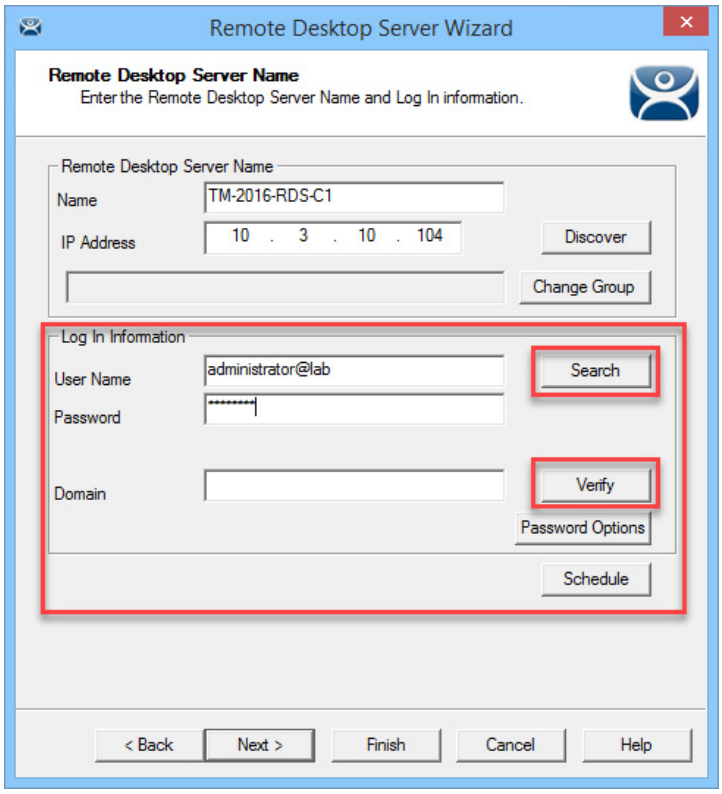
Figure 77 - Search for AD User



5. Choose the desired user and click OK.

   The domain user is populated to the User Name field of the Remote Desktop Server Name page.

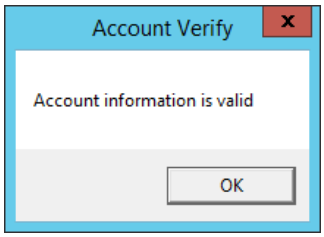
Figure 78 - Remote Desktop Server Wizard - Log In Information



6. Complete the Password field.
7. Click Verify to check whether the password is valid.

If correct, the Account Verify dialog box indicates that the password is valid.

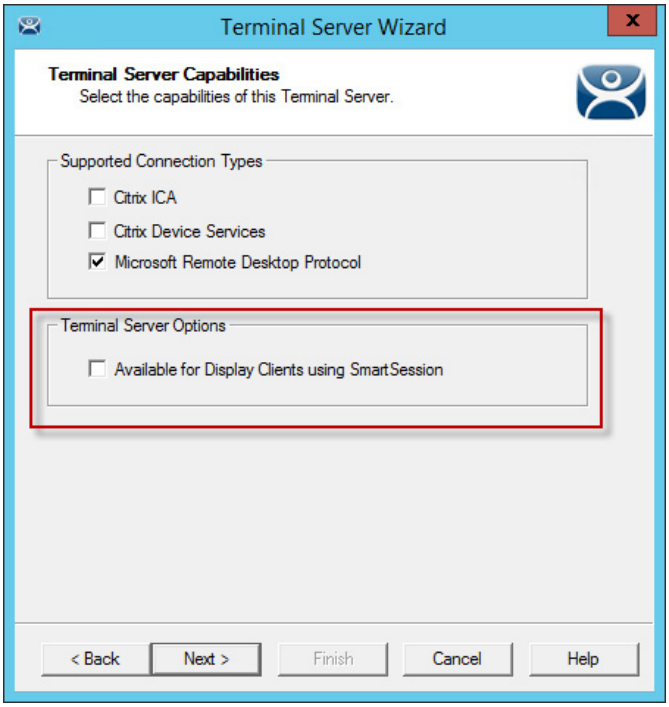
Figure 79 - Account Verify Dialog



8. Click OK to return to the Remote Desktop Server Name page.
9. Click Next to continue in the wizard.

   The Terminal Server Capabilities page appears.

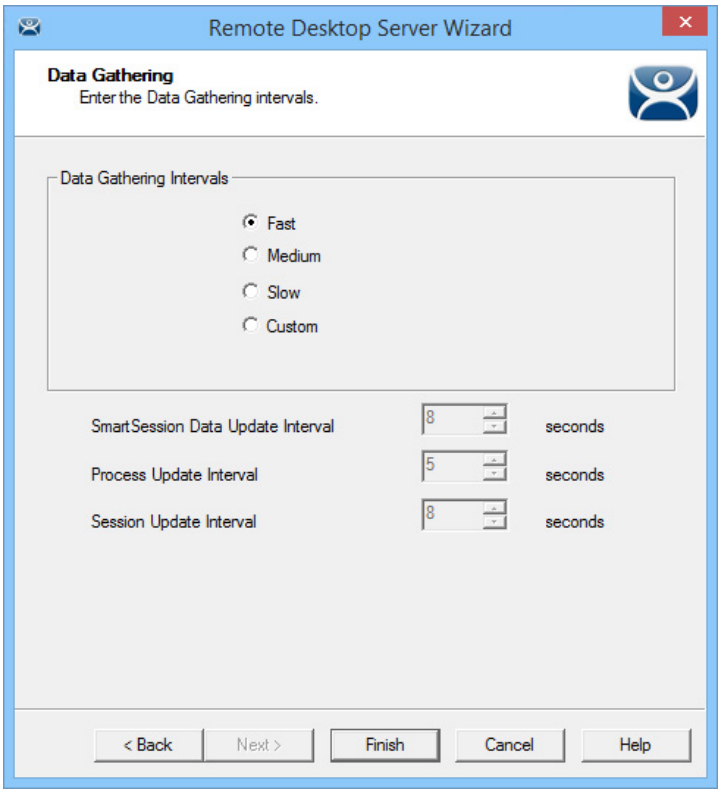
Figure 80 - Terminal Server Capabilities - Terminal Server Options



10. To use the Remote Desktop Server with SmartSession, check Available for Display Clients using SmartSession and click Next.

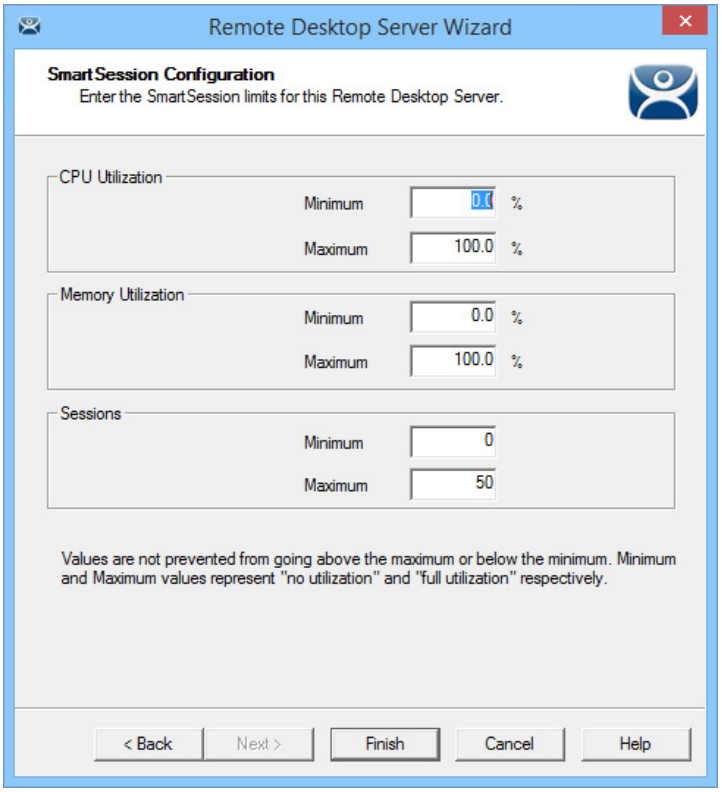
The Data Gathering page appears.

Figure 81 - Data Gathering



11. On the Data Gathering page, set the speed and frequency with which ThinManager polls Remote Desktop Servers. This covers both SmartSession and the data on the Users, Sessions, and Processes tabs of the server. Fast is the default Data Gathering Interval, but the interval can be changed for less frequent polling or to a custom value.

Figure 82 - SmartSession Configuration



If Available for Display Clients using SmartSession was checked to load balance on the Remote Desktop Server Capabilities page, then the wizard shows the SmartSession Configuration page.

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 156.

12. Click Finish to accept the changes and close the wizard.
13. Repeat this process for each Remote Desktop Server in use.

Citrix Servers

Citrix™ StoreFront is fully supported with ThinManager 12.1 and later when using container images with the embedded ICA client. See Containers on Thin Clients on page 84.

Support for Citrix ICA was deprecated starting with ThinManager Server 9.0. By default, the ability to configure a Remote Desktop Services Display Client to use Citrix ICA was removed. This was deprecated because ICA is a proprietary protocol that prevents it from being fully supported by all of the latest features of ThinManager such as mobile clients, Tiling, Virtual Screens, and so on. With that said, it is still possible to enable ICA in ThinManager.

To allow ICA configuration for ThinManager 9.0 and newer, follow these steps.

1. Open the registry editor and navigate to the option for 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
2. Add a new DWORD value named SupportICA with a value of 1
3. Restart the ThinServer service.
4. For redundant systems, make this change on both servers.

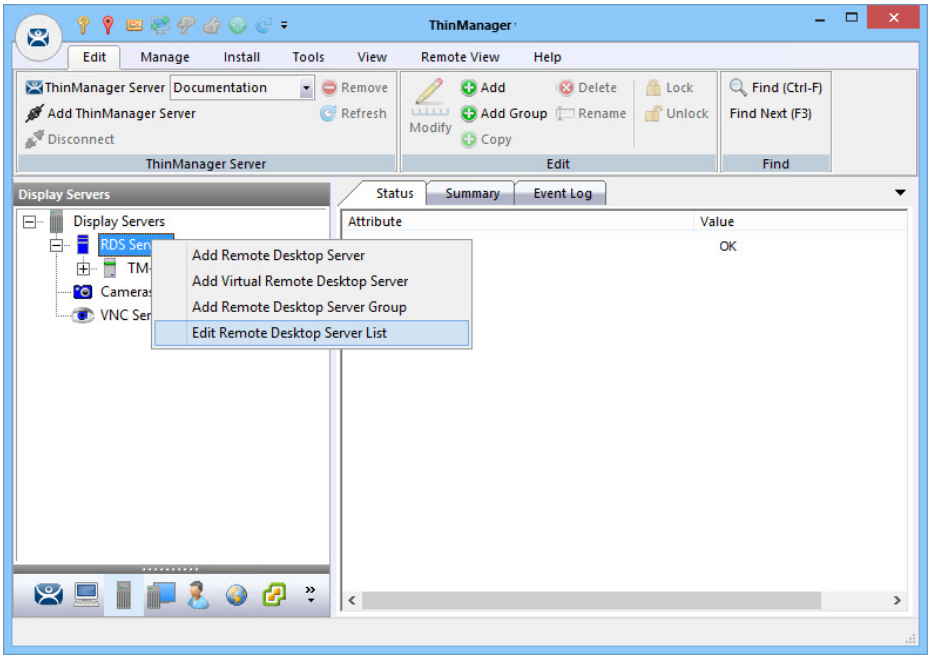
This is a one-time change that does not need to be made again; for example, after an upgrade.

ThinManager only supports the Citrix PNAgent on direct connections. Therefore, Citrix 7.x and later installations must enable PNAgent since it is no longer enabled by default. Citrix StoreFront is supported with containers in ThinManager version 12.1 and later.

Automatically Find Remote Desktop Servers

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

Figure 83 - Remote Desktop Server Branch - Display Servers Tree

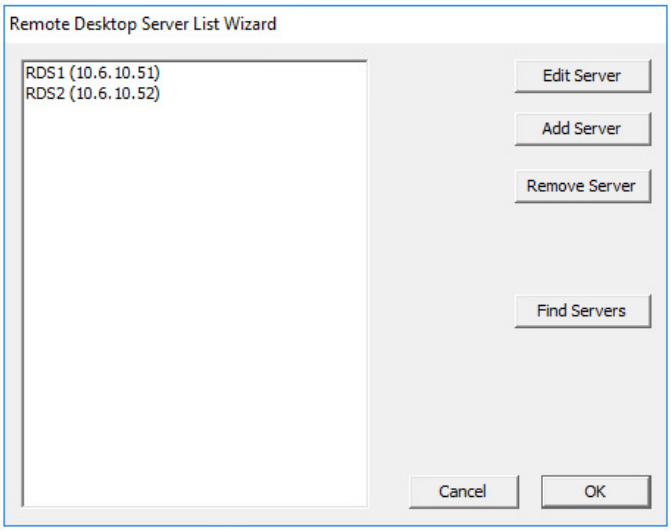


To find Remote Desktop Servers on the network, follow these steps.

1. Go to the Remote Desktop Server branch of the Display Server tree.
2. In the Display Server tree, right-click RDS Servers and choose Edit Remote Desktop Server List.

The Remote Desktop Server List Wizard appears.

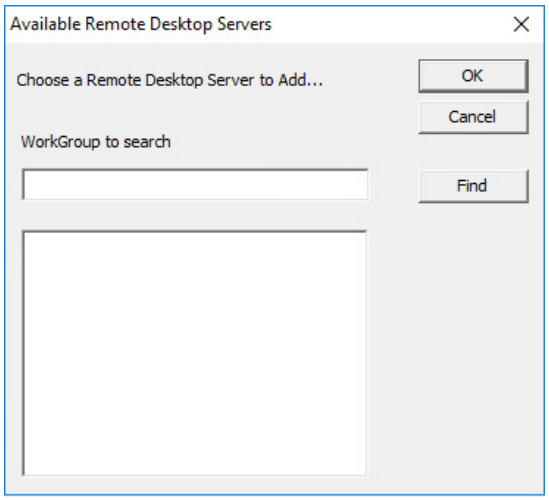
Figure 84 - Remote Desktop Server List Wizard



3. Click Find Servers.

   The Available Remote Desktop Servers dialog appears.

Figure 85 - Available Remote Desktop Servers



The Available Remote Desktop Servers list shows all Remote Desktop Servers that ThinManager can communicate with in a workgroup.

4. Choose the Remote Desktop Server to add and click OK.

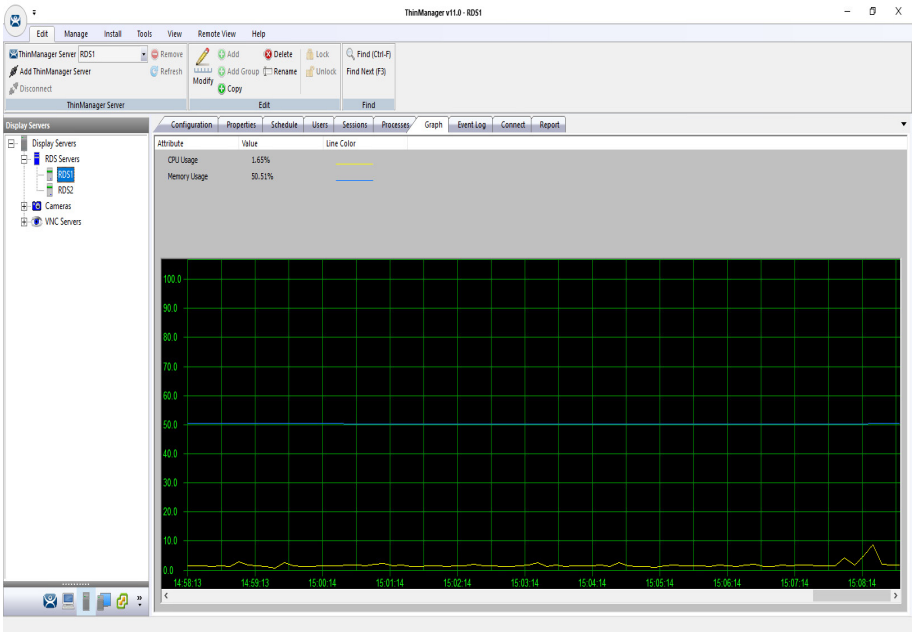
   The Remote Desktop Server Wizard appears, displaying the name and IP address.

5. Use the WorkGroup to search field to expand the search. Enter the workgroup and click Find to search again.

Remote Desktop Server Graph

The Remote Desktop Server Graph allows you to see the performance levels of the server.

Figure 86 - Remote Desktop Server Performance Graph



To view the performance levels of a Remote Desktop Server, highlight a Remote Desktop Server in the RDS Servers branch of the Display Servers tree and click the Graph tab.

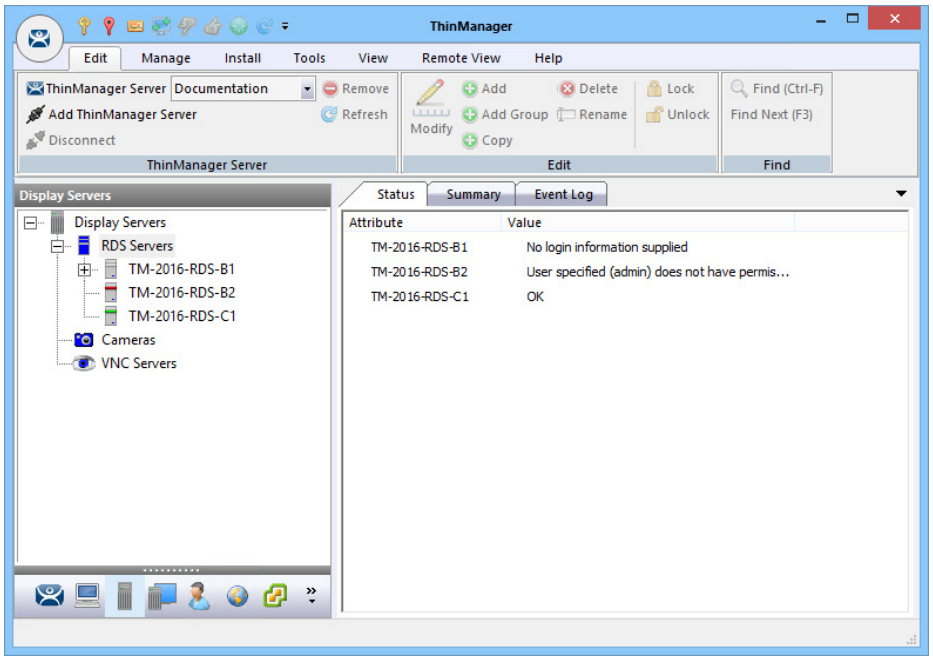
CPU Usage, Memory Usage, and Total Sessions are the values that ThinManager uses to calculate the SmartSession resource load.

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

Remote Desktop Server Status

Remote Desktop Server Status shows the connection status between ThinManager and the servers.

Figure 87 - Remote Desktop Server Status



To show the connection status between ThinManager and the servers, highlight the RDS Servers branch of the Display Servers tree and click the Status tab.

Ideally, the Remote Desktop Servers are configured properly so that ThinManager communicates with them and is able to pull load status into ThinManager for use in management and SmartSession load balancing.

Figure 88 - Remote Desktop Server Status Lights

Status Color	Meaning
Green	ThinServer can talk to the Remote Desktop Server and pull data using the administrative account you are using. “OK” is displayed as the Value on the Status tab.
Red	The server is offline or the administrative account failed to connect to the server.
Gray	The administrative account was left blank, and the ThinManager Server is not trying to communicate with the server. “No login information supplied” is the Value displayed on the Status tab.

A Red or Gray status does not mean that the Terminals cannot log in and run on the servers. These colors only indicate the ability of ThinManager to access the resources on the server.

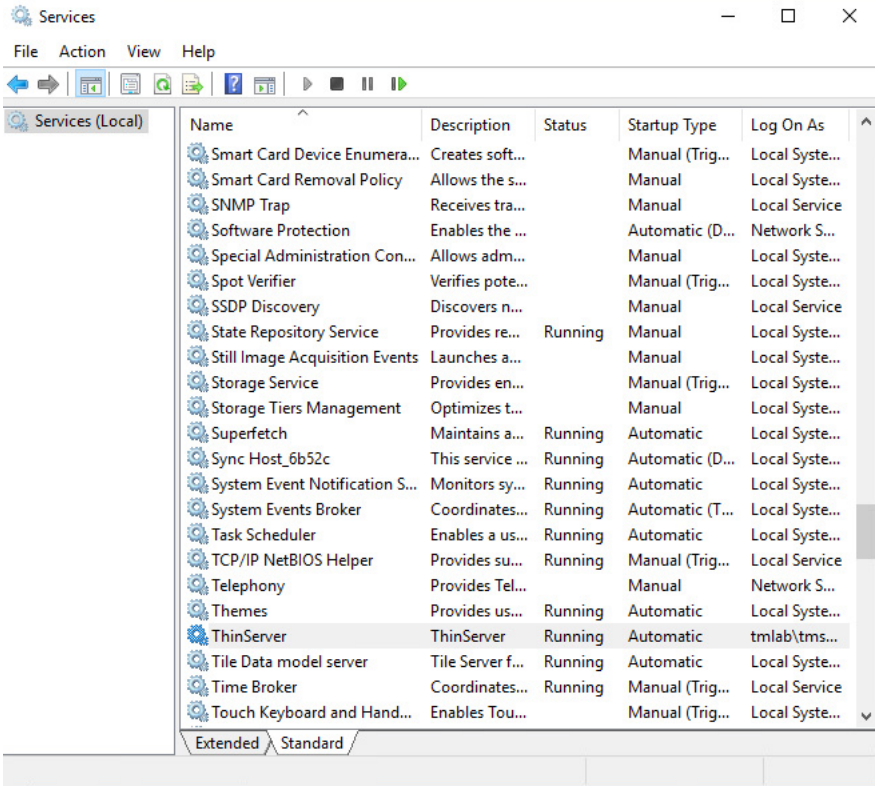
Solutions to Failed or No Connection

- For a gray status, reopen the Remote Desktop Server Wizard and enter an administrative account in the Log In Information fields on the Remote Desktop Server Name page.
- For a red status with a Value of "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.
- For a red status with a Value of "The RPC Server is unavailable" or "WTSAPI32.dll failed," then the Remote Desktop Server is offline or missing the Terminal Services/Remote Desktop Protocol role.

Local Administrative Login for ThinServer

Sometimes, large domains have issues where the connection times out before the domain controller validates the user name. To correct this issue, create a local administrative user account on each server, then have the ThinServer log in with this account. This speeds up data retrieval.

Figure 89 - Services in Windows 2016

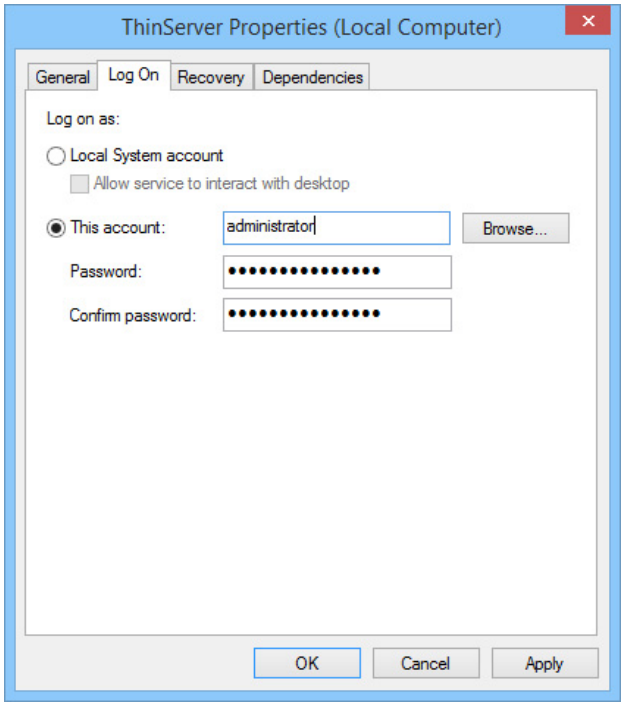


To change the ThinServer service login in Microsoft Services on your ThinManager Server, follow these steps.

1. To access the Windows Services dialog box, choose Control Panel>System and Security>Administrative Tools>Services, or choose Server Manager>Tools>Services.

2. Double-click on the ThinServer service. The ThinServer Properties dialog box appears.

Figure 90 - ThinServer Properties

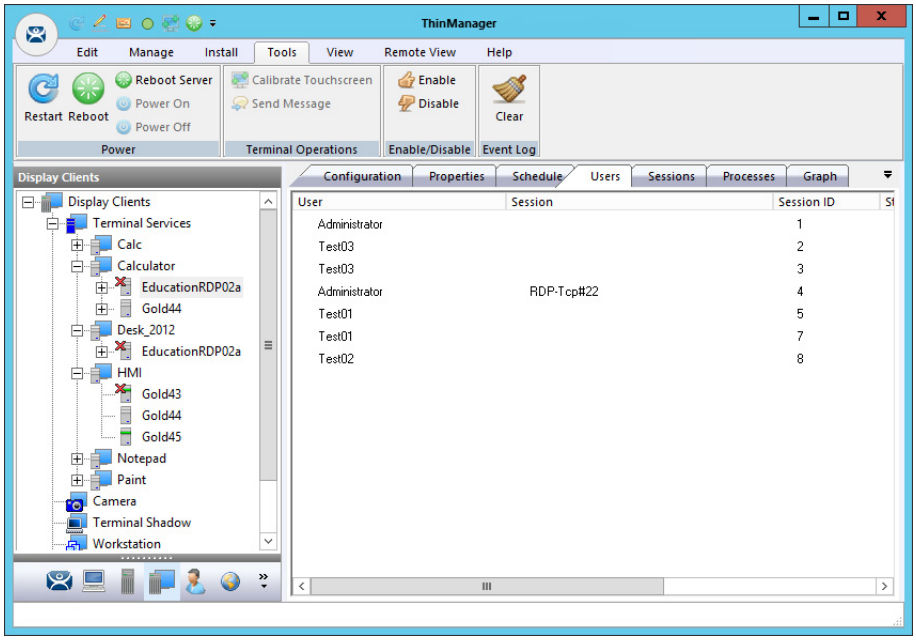


3. Click the Log On tab.
4. To change the log in account from the Local System account, click This account and specify the local administrative account. Make sure it is a member of the Administrative Group.
5. Click OK and restart the ThinServer service to apply the changes to the login.

Disable Remote Desktop Servers

ThinManager allows you to disable a Remote Desktop Server, which is useful for failover tests and updates. This feature allows you to move servers offline, one at a time, for updating. This action forces ThinManager-controlled thin clients to drop their connections and switch to an alternate server. This is useful for testing Failover and Instant Failover because the Terminals should switch to a back-up server. The network card on the server is not disabled—you can make RDP connections from a PC; but ThinManager thin clients stop using the server.

Figure 91 - Disabled Remote Desktop Servers in Display Clients



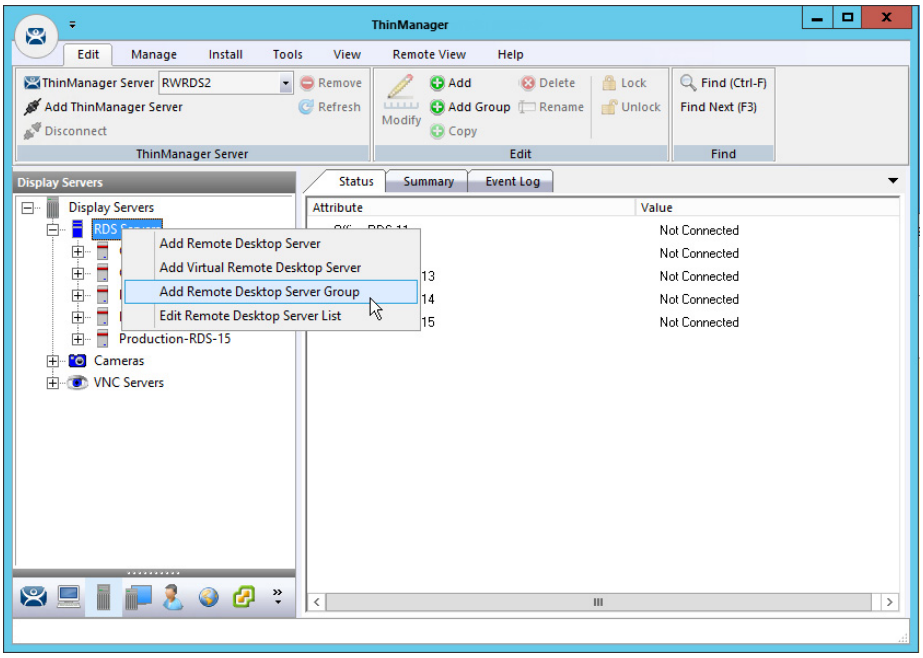
To disable a Remote Desktop Server, follow these steps.

1. Highlight the Remote Desktop Server icon in the Display Servers tree and choose Tools>Disable.
2. Once the Remote Desktop Server is disabled, reset the sessions on the Sessions tab. Right-click a session and choose Reset Session. Once the server is clear of sessions, patch and update the server and applications, and even reboot it if necessary. This does not impact production as all the Terminals are using a backup server.
3. Once the task is complete, choose Tools>Enable to allow the Terminals to use the server again.

Remote Desktop Server Group

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

Figure 92 - Add a Remote Desktop Server Group

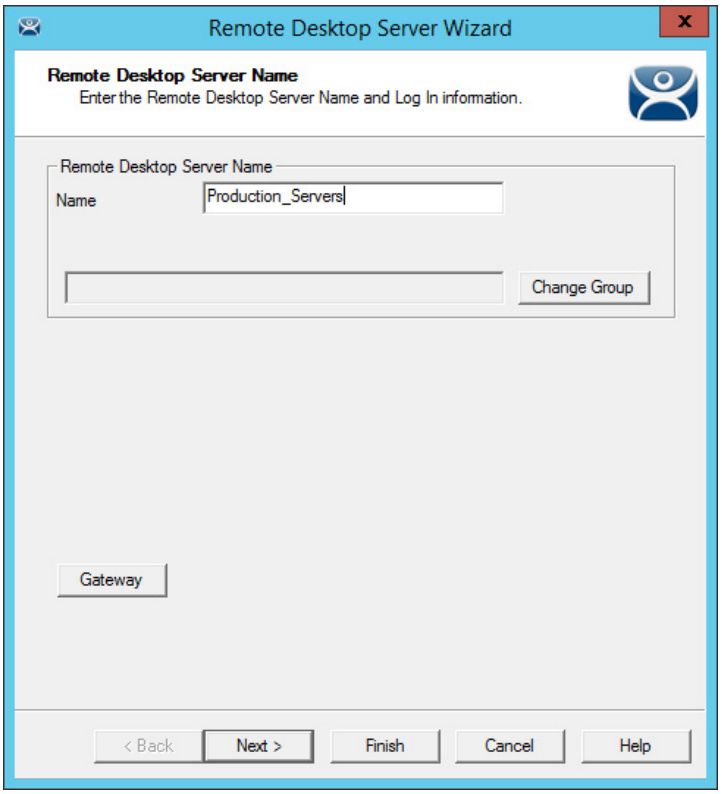


To add a Remote Desktop Server Group, follow these steps.

1. In the Display Servers branch, right-click RDS Servers and choose Add Remote Desktop Server Group.

   The Remote Desktop Server Wizard appears.

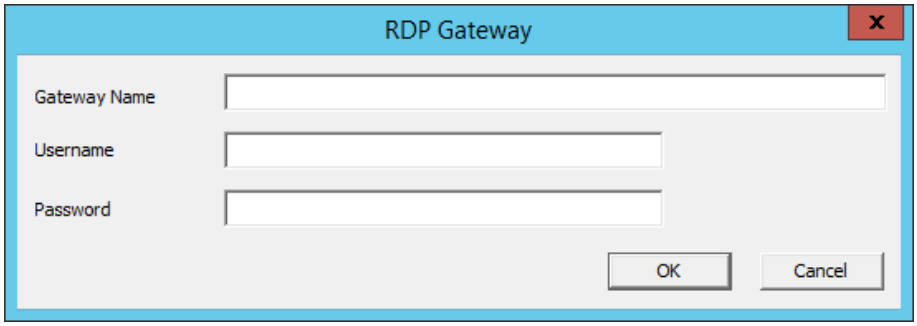
Figure 93 - Remote Desktop Server Name Page



2. Enter a name for the Remote Desktop Server Group.
3. Click Gateway.

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

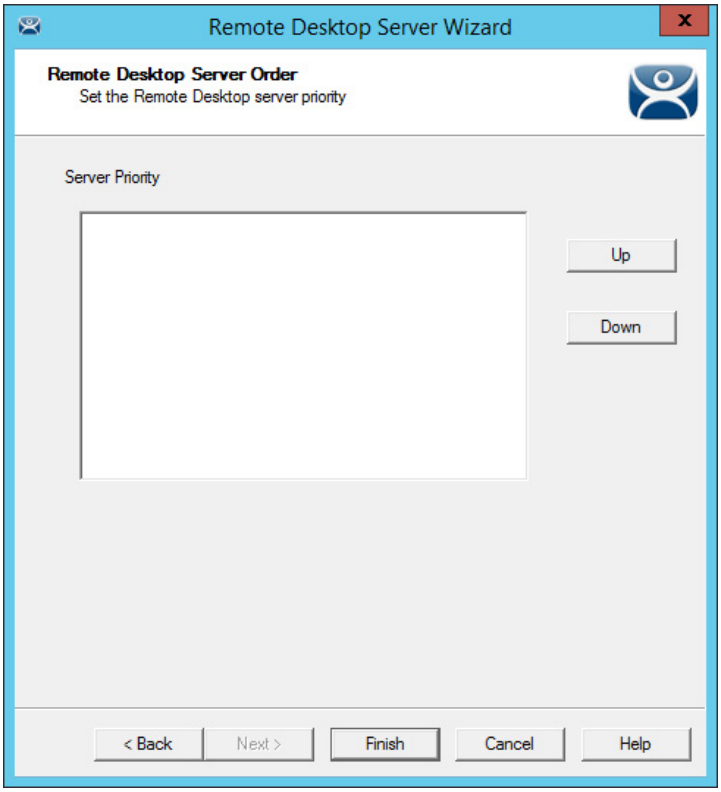
Figure 94 - RDP Gateway



4. Enter the Gateway Name, Username, and Password.
5. Click OK.

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

Remote Desktop Server Order Page

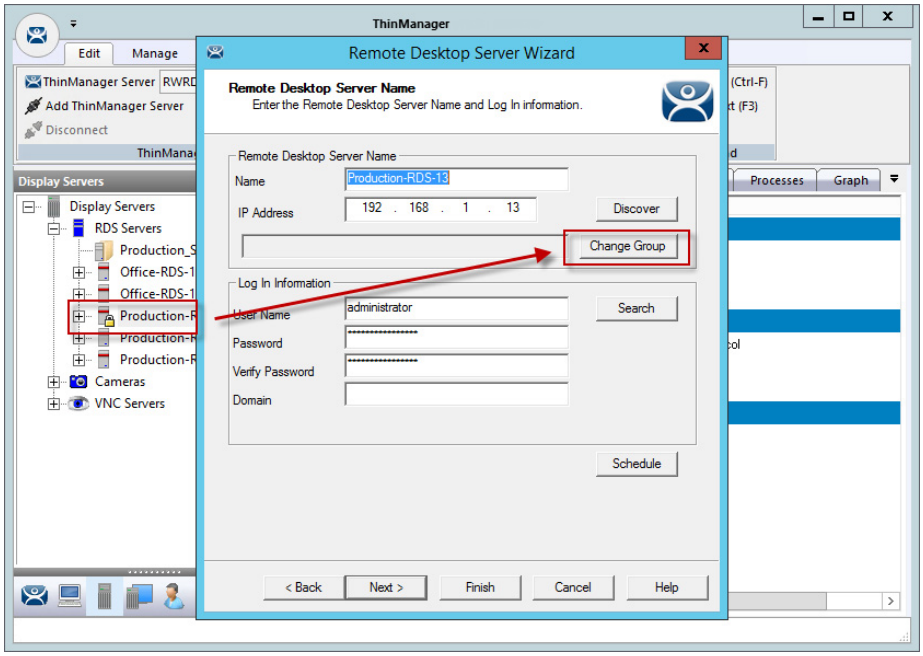


The Remote Desktop Servers are added individually in the Remote Desktop Server Wizard.

6. Double-click on the server under RDS Servers in the Display Server branch.

The Remote Desktop Server Name page of the Remote Desktop Server Wizard appears.

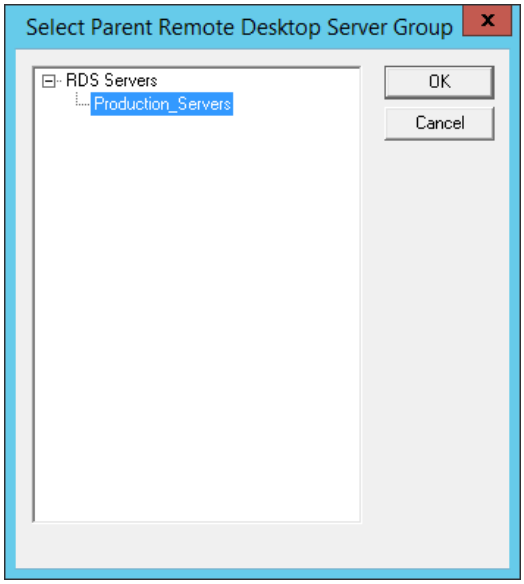
Figure 95 - Remote Desktop Server Name Page



7. Click Change Group.

   The Select Parent Remote Desktop Server Group dialog box appears.

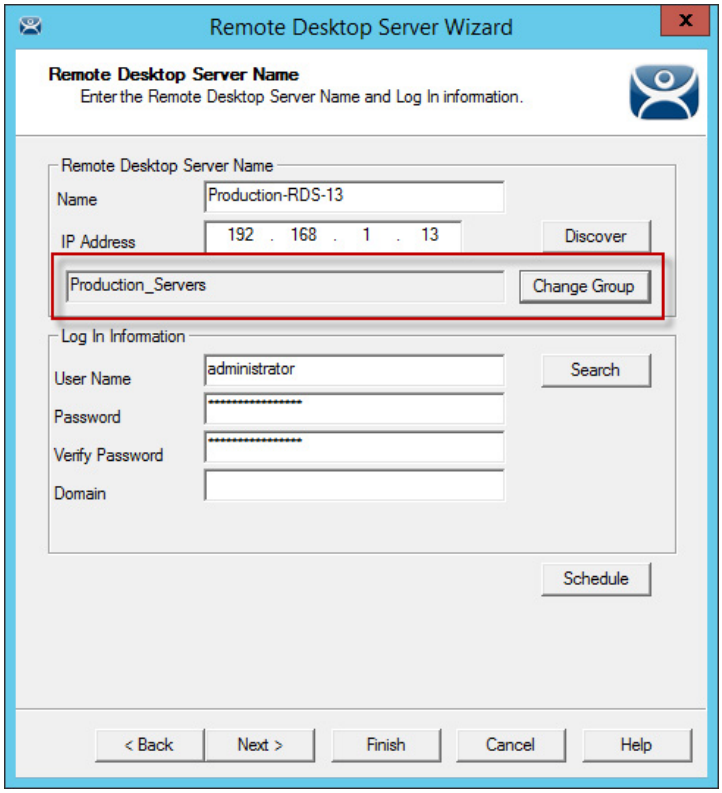
Figure 96 - Select Parent Remote Desktop Server Group



8. Choose the desired Remote Desktop Server and click OK to accept the changes.

The chosen Remote Desktop Server is populated to the Change Group field.

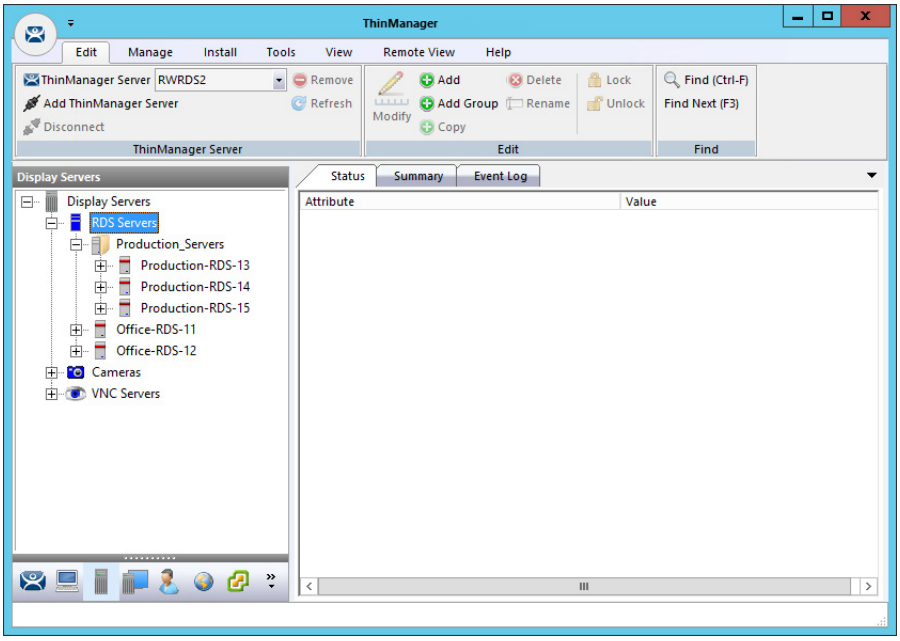
Figure 97 - Remote Desktop Server Name Page with RDS Group Membership



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

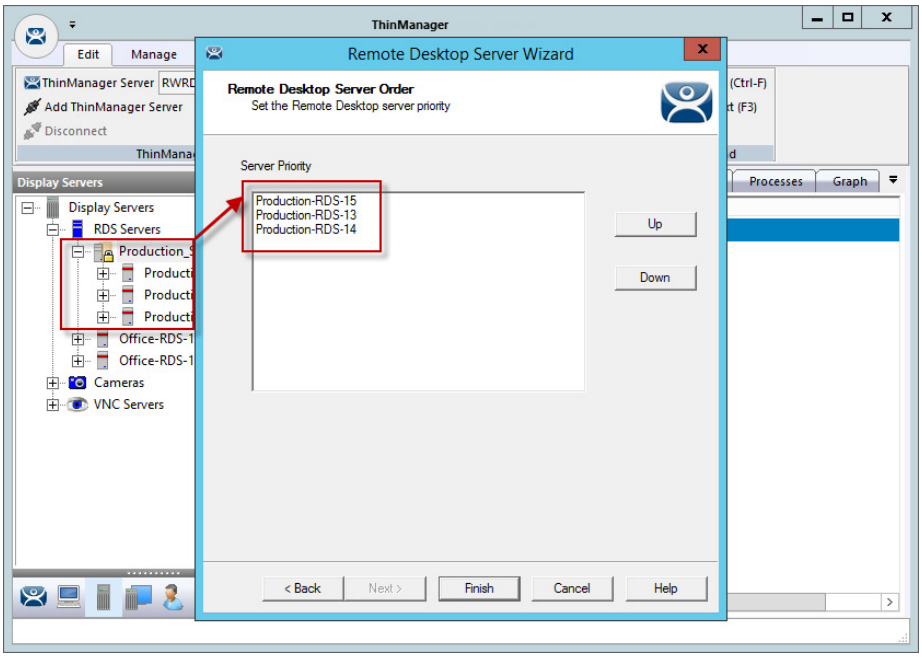
9. Repeat as needed.

Figure 98 - Remote Desktop Server Group with Member Remote Desktop Servers



The tree shows the member Remote Desktop Servers in the RDS Servers group.

Figure 99 - Remote Desktop Server Order Page



Button	Description
Up	Moves a highlighted Remote Desktop Server up in the priority list.
Down	Moves a highlighted Remote Desktop Server down in the priority list.

10. Open the Remote Desktop Server Group wizard and navigate to the Remote Desktop Server Order page to view the members of the Remote Desktop Server Group.

    The Remote Desktop Servers are used in the order listed.

11. Highlight a member server to move, then use the Up and Down buttons to change the order.
12. Click Finish.

Remote Desktop Server Groups and Display Clients

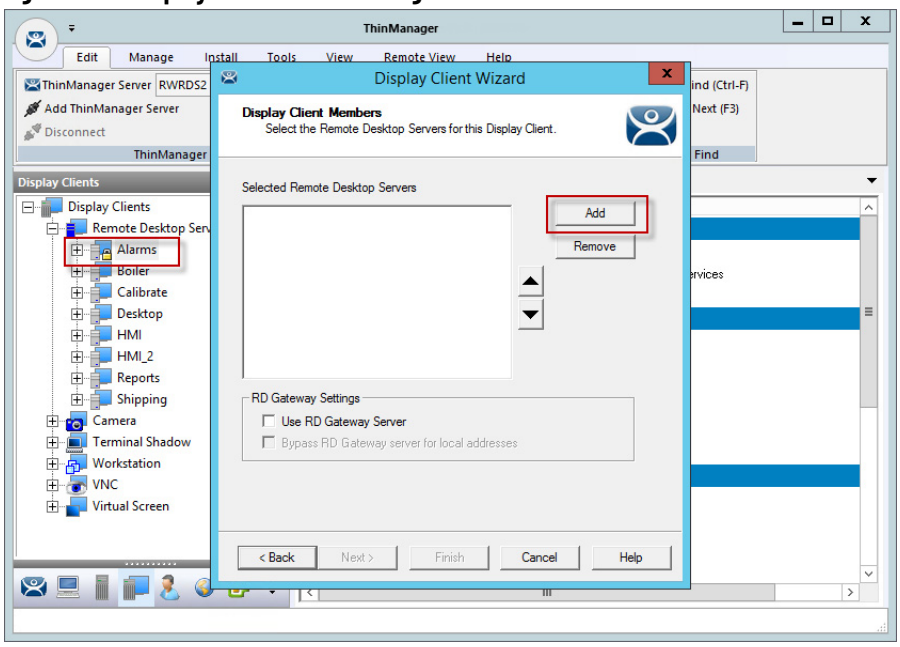
The Display Client Wizard appears differently when Remote Desktop Server Groups are configured versus not configured. The following steps depict when no Remote Desktop Server Groups are configured.

1. In the Display Clients branch, double-click a Display Client.

   The Display Client Wizard appears.

2. Click Next until the Display Client Members page appears.

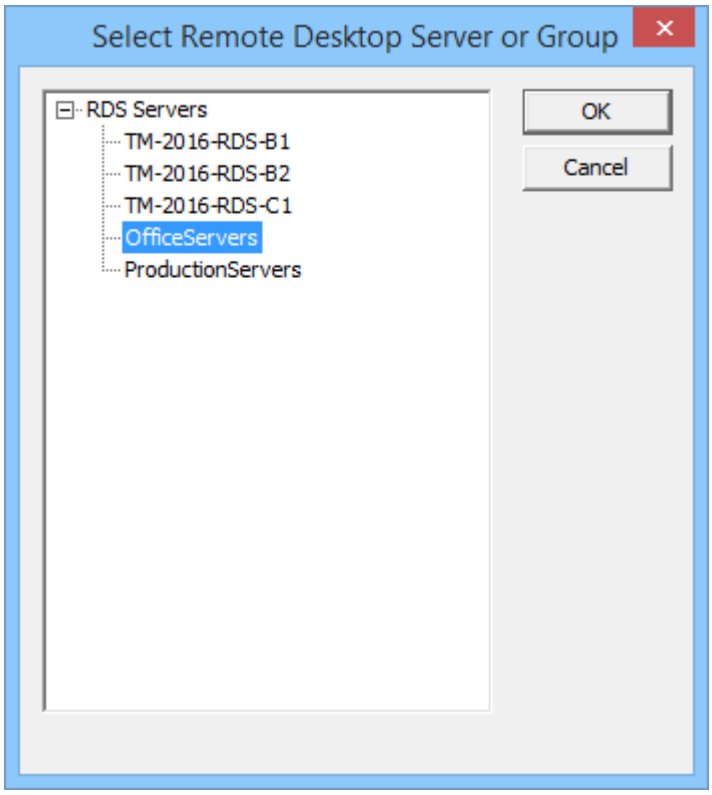
Figure 100 - Display Client Members Page



3. Click Add.

   The Select Remote Desktop Server or Group dialog appears, from which you may select a Remote Desktop Server Group, an individual Remote Desktop Server, or a Remote Desktop Server that is a member of a Remote Desktop Server Group.

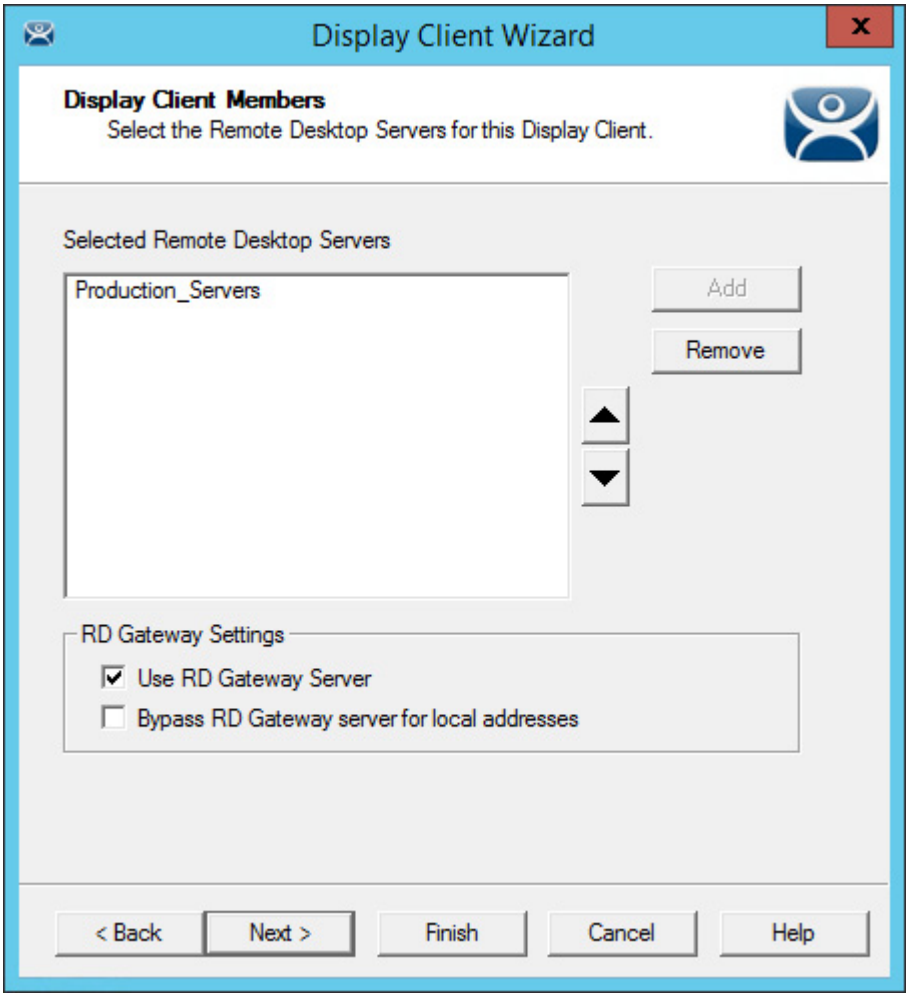
Figure 101 - Select Remote Desktop Server or Group



4. Highlight the desired Remote Desktop Server or group and click OK.
5. Repeat as needed.

Once a Remote Desktop Server or group is selected, it appears in the Selected Remote Desktop Servers list.

Figure 102 - Display Client Wizard – Display Client Member Page



Feature	Description
Use RD Gateway	Prompts the Display Client to use the Microsoft RD Gateway.
Bypass RD Gateway server for local address	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.

Navigation through the remaining Display Client Wizard pages follows those displayed when no Remote Desktop Server Groups are configured.

Containers

ThinManager version 12 introduced support for Containers as a method of managing and deploying hosted content, leveraging Docker® container technology.

There are two methods to deliver content with Containers:

1. Containers on thin clients (released with ThinManager version 12.1)
2. Containers on servers (released with ThinManager version 12.0)

Initially, ThinManager added support for Containers as a way to deliver a web browser to a thin client without requiring a Remote Desktop Server to do so. The original set of supported Container images included Chrome, Firefox,

Chrome with Citrix, and Firefox with Citrix, for which updates are provided on a quarterly basis at downloads.thinmanager.com.

ThinManager version 14.1 adds a new FactoryTalk Optix Container, as well as support for container versioning. To learn more, please refer to Optix Container on page 90. Additionally, version 14.1 adds the new BootAssist module specifically for ASEM hardware with on-board storage, which enables customers to optionally cache the thin client's firmware, terminal profile, Container image and/or Container application. For more details on BootAssist module, please refer to BootAssist on page 560.

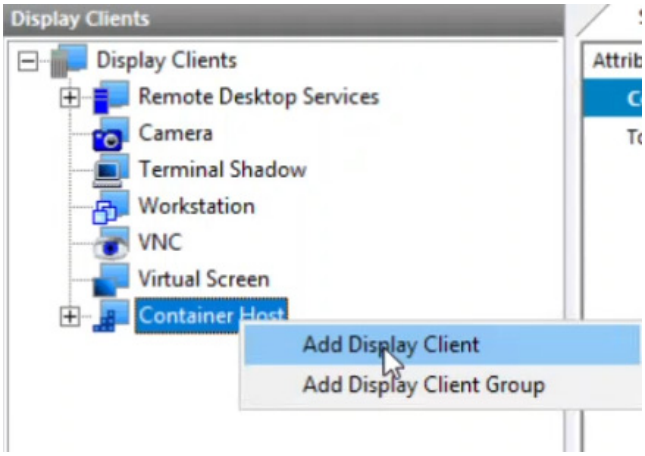
Since the ThinManager firmware is based on Linux, only Linux-based Containers can be deployed to a ThinManager-managed terminal.

Containers on Thin Clients

Hosting Containers on thin clients is new with ThinManager version 12.1. Previously, all web-based content required Windows servers using either Remote Desktop Services or (Docker) Container Hosts. These methods required resources such as RAM and CPU to be consumed locally on these designated servers. When electing to run containers on ThinManager-managed terminals, the required resources to run a web-browser Container, for example, are sourced from the designated terminal.

These steps illustrate how to create a Container Host Display Client to run on a thin client. For containers running on thin clients, a Display Server does not need to be created.

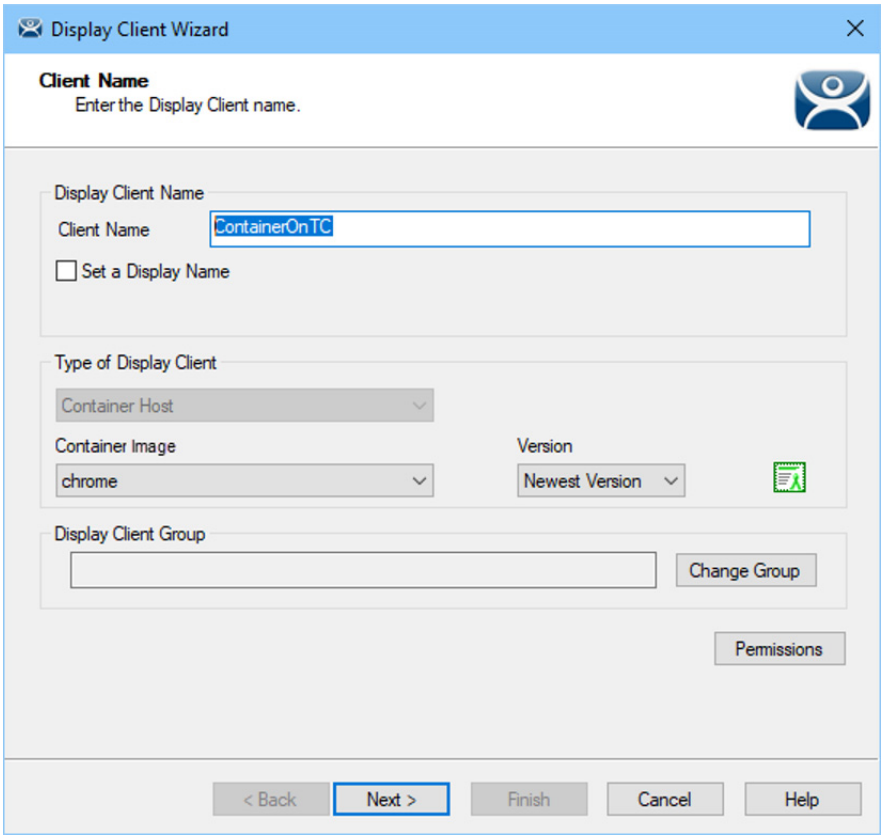
Figure 103 - Add a Display Client



1. Under the Display Client tree, right-click Container Host and choose Add Display Client.

The Client Name page of the Display Client Wizard appears.

Figure 104 - Client Name Page

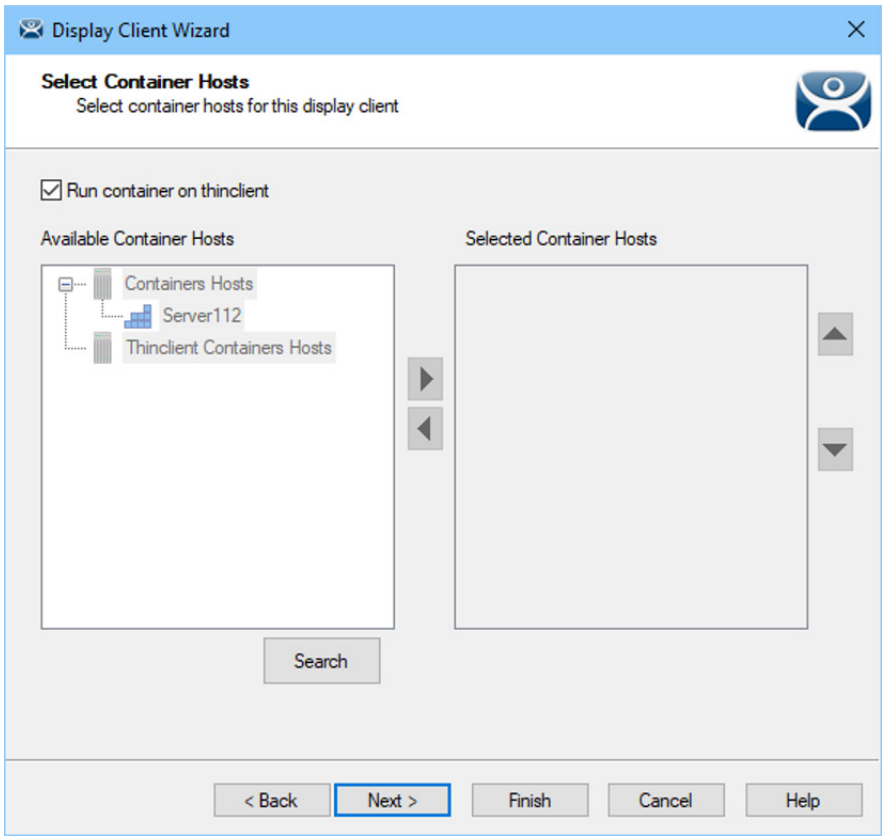


2. Type the Client Name.
3. From the Container Image pull-down menu, choose a Container image.
4. From the Version pull-down menu, choose the version of the Container Image to use for this Display Client.
   You may select a specific version, or Newest Version, which always uses the latest version of the Container Image available in ThinManager.

Container Image	Description
chrome	Launches the application with a Chrome browser.
FactoryTalk System Status / chrome	Launches the Display Client with the FactoryTalk System Status page in a Chrome browser.
optix_app	Launches the Display Client with an Optix container with which to associate a specific Optix application to be managed from ThinManager.
ViewPoint / chrome	Launches the Display Client with the FactoryTalk ViewPoint page in a Chrome browser.

5. Click Next through the wizard until the Select Container Hosts page appears.

Figure 105 - Select Container Hosts Page



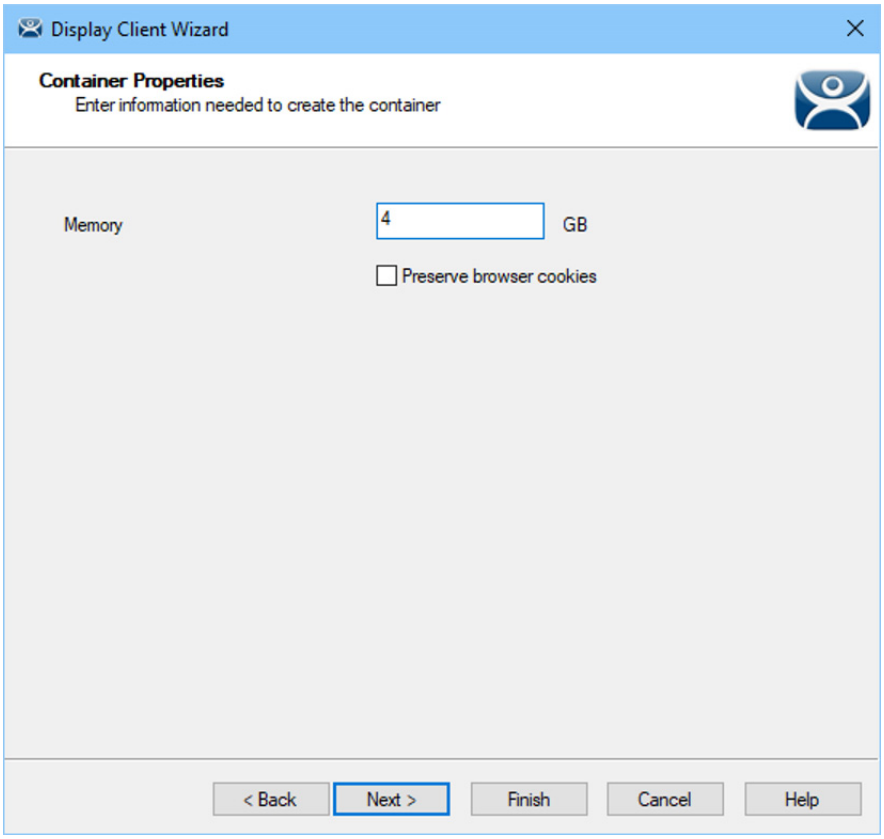
6. Choose the method to run a container on a thin client.

Container Application	Description
Run container on thinclient	Check to run the container on the thin client where the display client is assigned. The application uses resources from the local thin client. Clear this checkbox to make the Available Container Hosts/Selected Container Hosts option available.
Available Container Hosts/ Selected Container Hosts	Use the arrows to choose a thin client to host the Display Client. The container utilizes the Selected Container Hosts' resources to run the application rather than the resource of the terminal on which the Display Client is applied. This option is available when the Run container on thinclient checkbox is cleared.

7. Click Next.

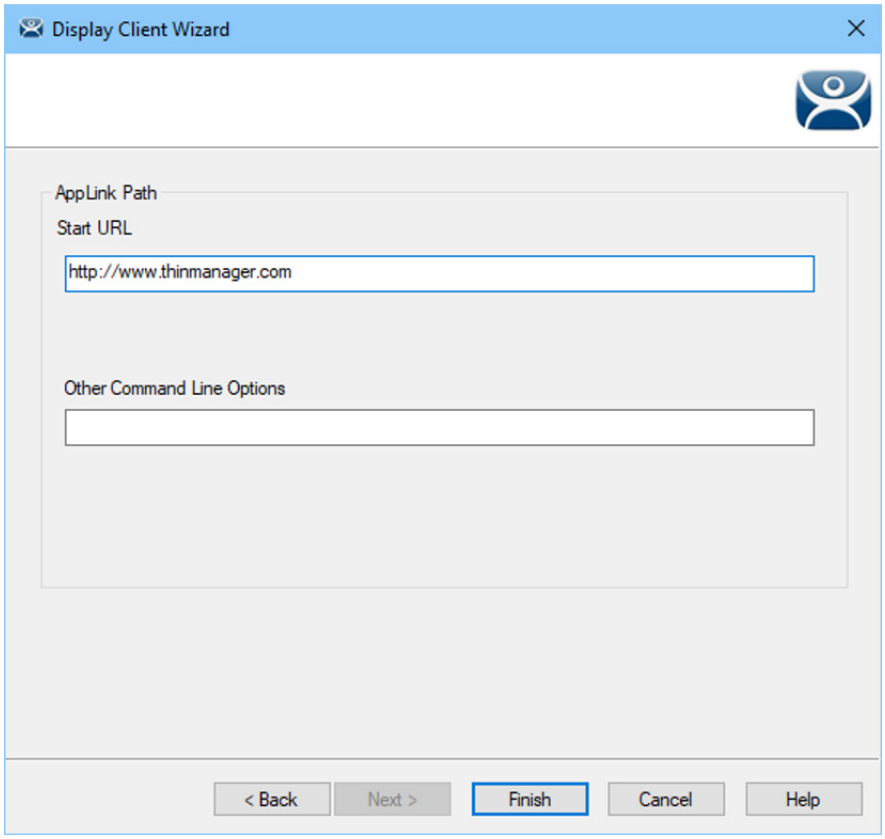
   The Container Properties page appears.

Figure 106 - Container Properties Page



8. Type the number of gigabytes of memory to allocate to the container in the Memory field. Adjust as needed. At least 1 GB is recommended, but it may need to be increased based on a specific application.
9. Check the Preserve browser cookies checkbox to store browser cookies in ThinServer and restore cookies when a new container is created for the terminal or user.
10. Click Next.

Figure 107 - AppLink Path Page



11. Type the application URL.
12. Click Finish to close the wizard.
13. Apply the Display Client to the terminal.

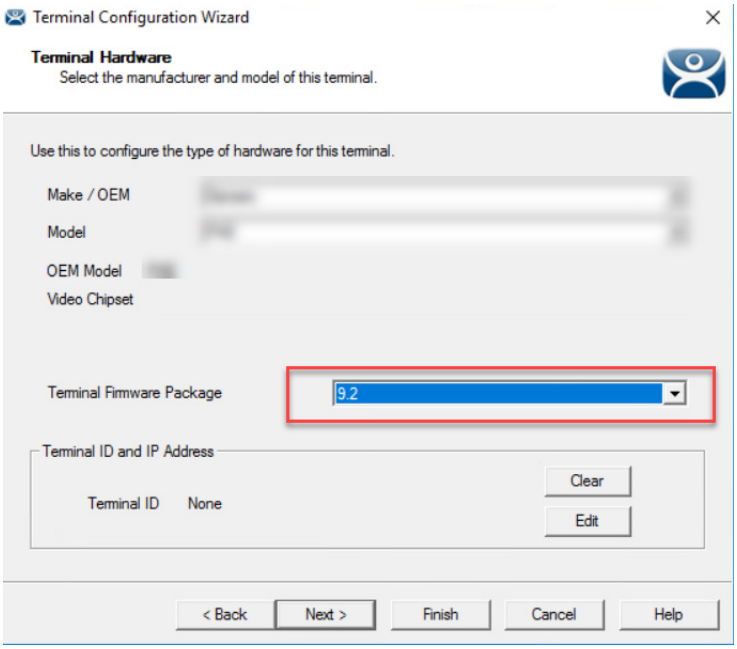
When creating a new Container Host Display Client, the Display Client Wizard provides different configuration options based on the Container Image selected. For example, when optix_app is selected as the Container Image, the Container Properties page of the wizard provides an option to Enable Container Local Storage, to Allow connection to Optix Web Presentation Engine (and specify a Web Presentation Engine Port), and to select a specific Optix Container Application. For more details, please refer to Optix Container on page 90.

14. Restart the terminal.

Terminal Profile Setup for Containers

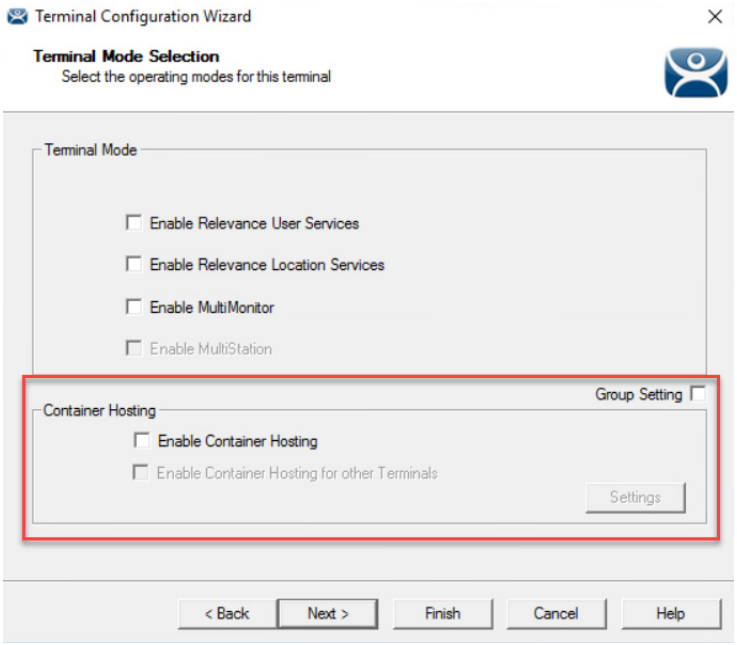
There are a few configuration requirements for terminals that are Container Hosts. Also, it is recommended that a terminal have at least 8 GB of RAM to host containers. This varies based on the application that runs inside the container.

Figure 108 - Terminal Hardware Page



1. For terminals that are Container Hosts, you must run at least Terminal Firmware Package 12.1.0-9.2 (shown as 9.2 in the Terminal Firmware Package drop-down menu). When this firmware is selected, an additional setting appears on the Terminal Mode Selection page of the wizard. Additional download and installation of terminal firmware package 12.1.0-9.2 or greater may be required.

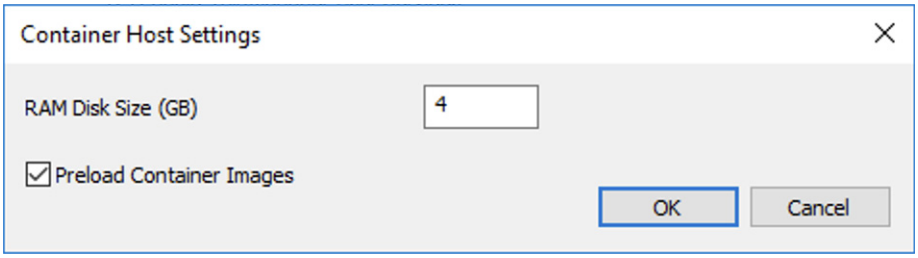
Figure 109 - Terminal Mode Selection Page



2. Complete the Container Hosting section of the Terminal Mode Selection page per these descriptions.

Setting	Description
Group Setting	Check to allow Enable Container Hosting and Enable Container Hosting for other Terminals settings to be applied to all terminals in the Terminal Group. This can be applied at the Terminal Group level only.
Enable Container Hosting	Check to enable Container Host Display Clients to run on this terminal.
Enable Container Hosting for other Terminals	Check to allow this terminal profile to appear in the Container Host Display Client Wizard to host containers for other thin clients.
Settings	Click to launch the Container Host Settings dialog, where Ram Disk Size can be changed, and there is an option to Preload Container Images.

Figure 110 - Container Host Settings



3. Complete the Container Host Settings dialog per these descriptions.

Setting	Description
Ram Disk Size (GB)	This value is the total write space of the container. The required minimum RAM Disk Space allocated is at least 4 GB. The default value is also 4 GB. This value varies per the application. It can be determined by the following formula: **[RAM Disk Size (GB)] = [Installed Container Image] + [Compressed Container Image] + [300 MB Docker Engine] + [Swap and Temporary Files Space]**, where RAM Disk Size (GB) cannot exceed the total RAM of the thin client.
Preload Container Images	Allows container images to load over HTTPS. Enabled by default. Clear to disable HTTPS port for the download of container images.

The RAM Disk Size and container Memory size are independent settings. The sum of RAM Disk Size and container Memory may not exceed the total physical memory (RAM) available on the thin client.

Optix Container

Starting with version 14.1, the ThinManager install includes a FactoryTalk Optix Container, which can be used to host an Optix application directly on a ThinManager-managed thin client. Optix applications deployed for use with the new ThinManager Optix Container support both the Native Presentation Engine and the Web Presentation Engine.

For Optix Runtime and Device Sizing, please refer to the FactoryTalk Hub. Based on the specifics of your Optix application, the hub offers sizing tools that provide guidance on the required Optix Runtime license, as well as a hardware recommendation. To deploy an Optix Container to a ThinManager-managed thin client, choose the ASEM 6300 as the alternative in the Device Sizing tool. If you only intend to use the device as a ThinManager-managed thin client, you can order the device without an Operating System. All ASEM 6300B, 6300P, and 6300PA devices ship with the ThinManager BIOS extension image, so they can be managed by ThinManager right out of the box.

The recommended workflow to utilize the Optix Container is to design and test your Optix application within Optix Studio as normal. When finished, export the application from Optix Studio, and then import it into the ThinManager Admin Console. Then, pair the Optix application with an Optix Container when you configure a Container Host Display Client in

ThinManager. The resulting Display Client can then be assigned to as many ThinManager terminals as required. Each terminal where you have assigned an Optix Container Display Client requires you to enter a unique Optix entitlement key in the Terminal Configuration Wizard.

As of the writing of this user manual, Optix 1.6 only supports online entitlements for Docker Container deployments, which means your thin client requires connectivity to the Internet in order for your Optix entitlement to be properly validated. If your thin client cannot connect to the Internet, Optix runs in a fully functional 2-hour demo mode.

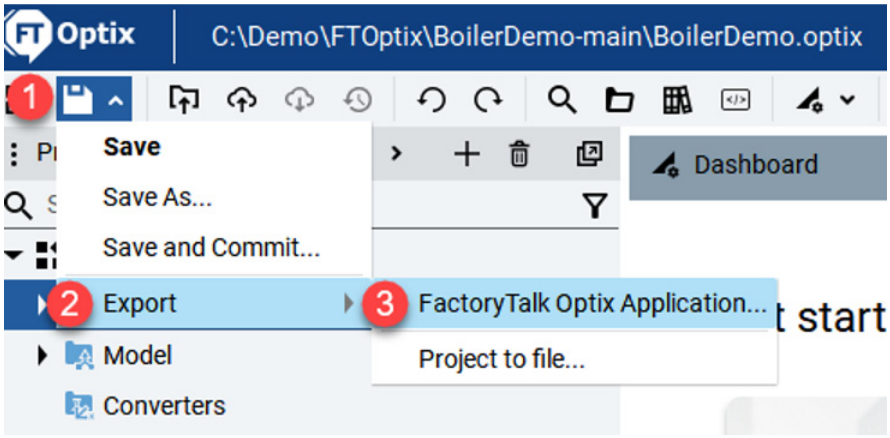
Deploying an Optix application to a thin client does require some special considerations. Since an overwhelming majority of ThinManager-managed thin clients do not have any permanent storage media, anything stored locally exists only in the thin client's memory and is lost upon rebooting the thin client. Therefore, if your Optix application requires DataStores that persist across thin client reboots, you need to utilize either an ODBC database and/or a Remote InfluxDB database for this data.

ThinManager 14.1 also includes a new module called BootAssist, which enables you to cache the ThinManager firmware, terminal profile, Container image, and/or Optix application image on a thin client's local storage; however, it does not support persisting data within the Optix Container. For more details, please refer to BootAssist on page 560.

Here are the steps to deploy the Optix Container:

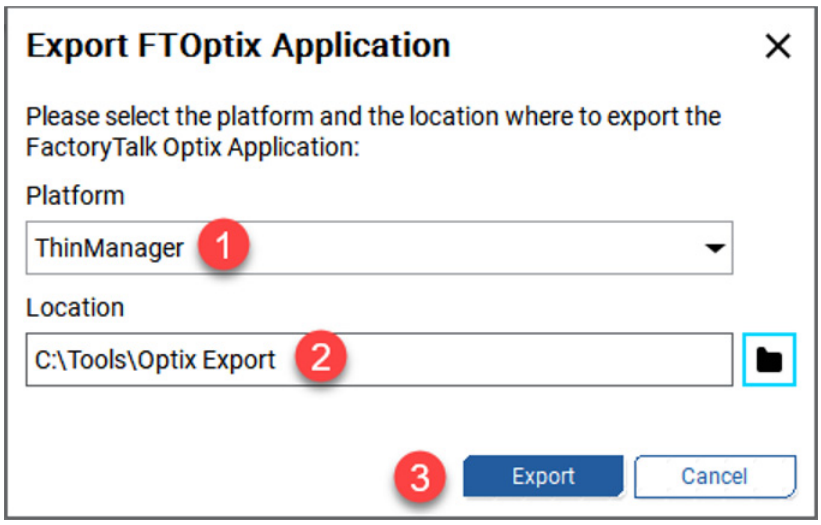
1. From Optix Studio, click the down arrow next to the Save icon, followed by Export | FactoryTalk Optix Application.

Figure 111 - How to open the FactoryTalk Optix Application



2. From the Export FTOptix Application window, select ThinManager from the Platform pull-down menu. Choose the Location where you would like to save the exported application and click the Export button.

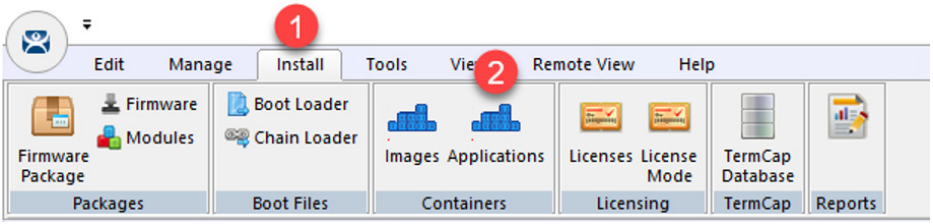
Figure 112 - Export FTOptix Application



The ThinManager option in the Platform pull-down menu was added in Optix 1.6. If you are running an earlier version of Optix, choose Ubuntu 22.04 x86 64-bit from the Platform pull-down menu. Then, you need to manually zip the exported application and make sure it does not include a top-level folder, to mimic how the ThinManager option functions in Optix 1.6 and newer.

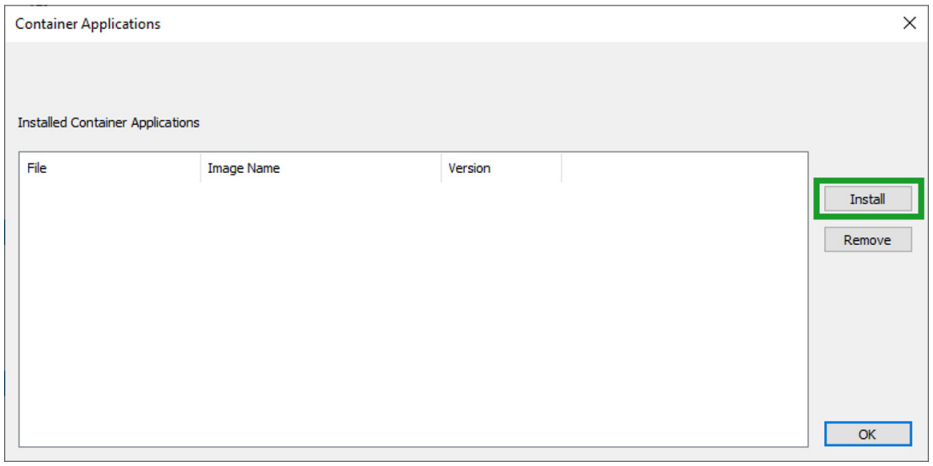
3. Copy the exported Optix application to the machine where you have ThinManager installed.
4. From the ThinManager Admin Console, select the Install ribbon, and then click the Applications icon from the Containers ribbon segment.

Figure 113 - Install > Applications



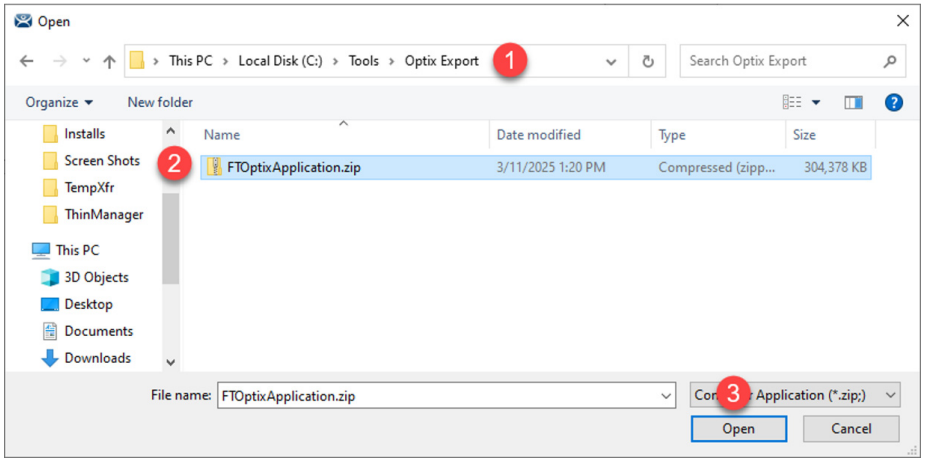
5. From the Container Applications window, click the Install button.

Figure 114 - Install Button on Container Applications window



6. Navigate to the file location of the exported Optix application and click the Open button.

Figure 115 - Optix Application file location

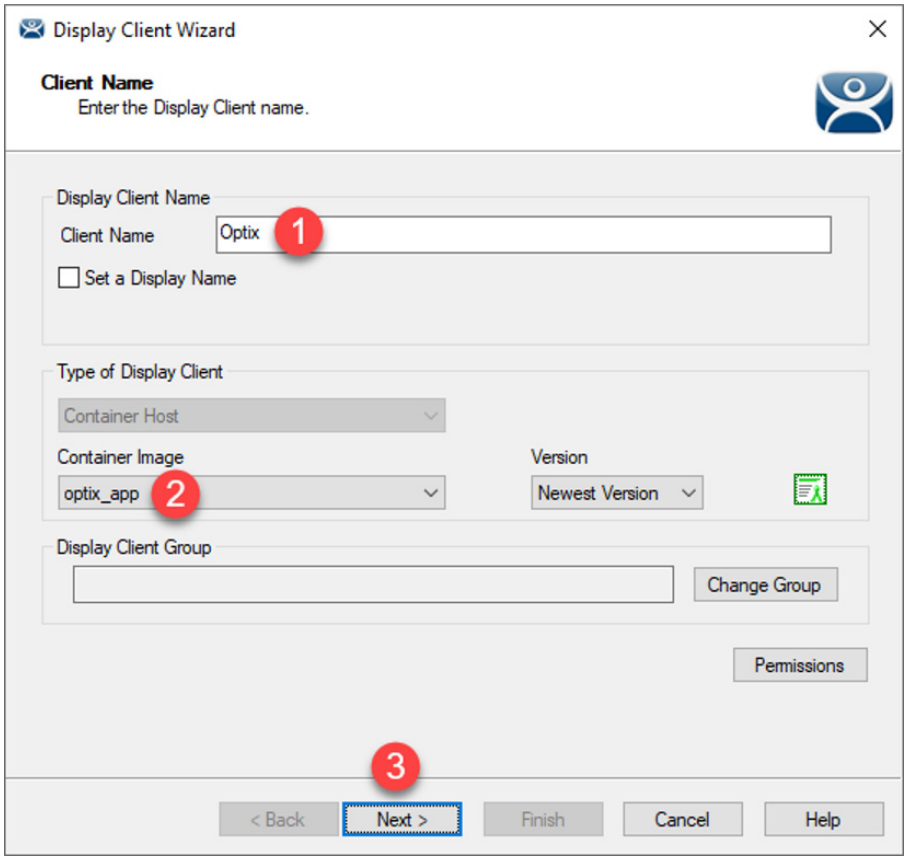


7. Click the OK button from the Container Applications window.

Figure 116 - OK button on Container Applications window

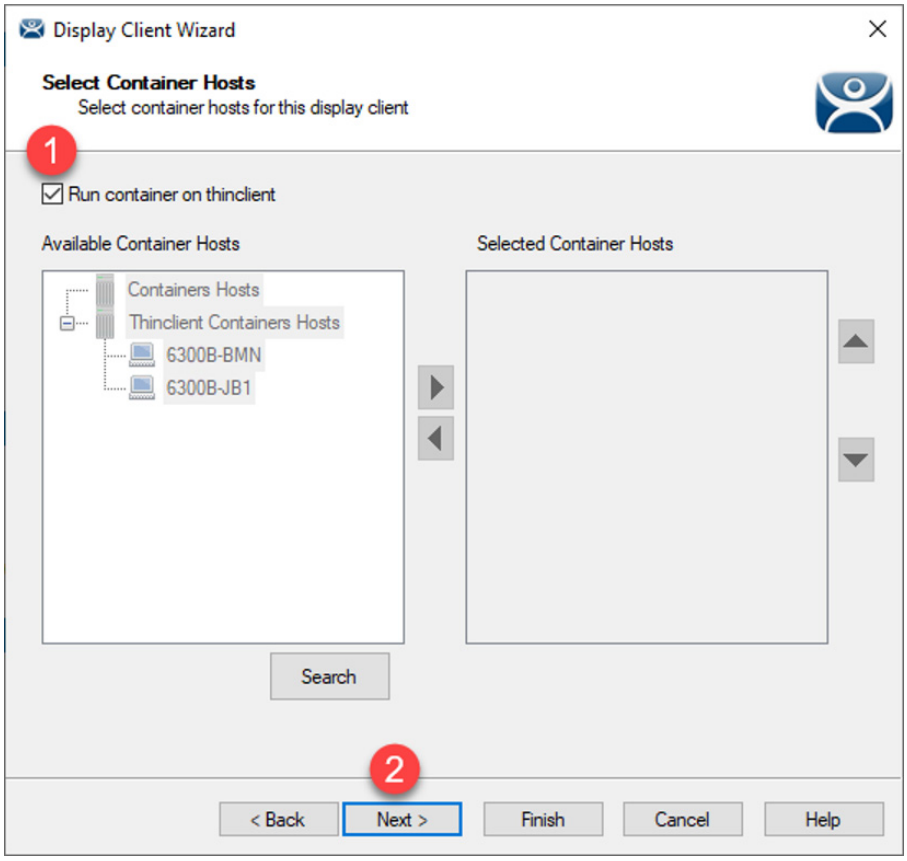
8. Create a new Container Host Display Client.
9. From the Client Name page of the Display Client Wizard, enter a Client Name, and select the optix_app Container Image.

Figure 117 - Client Name page



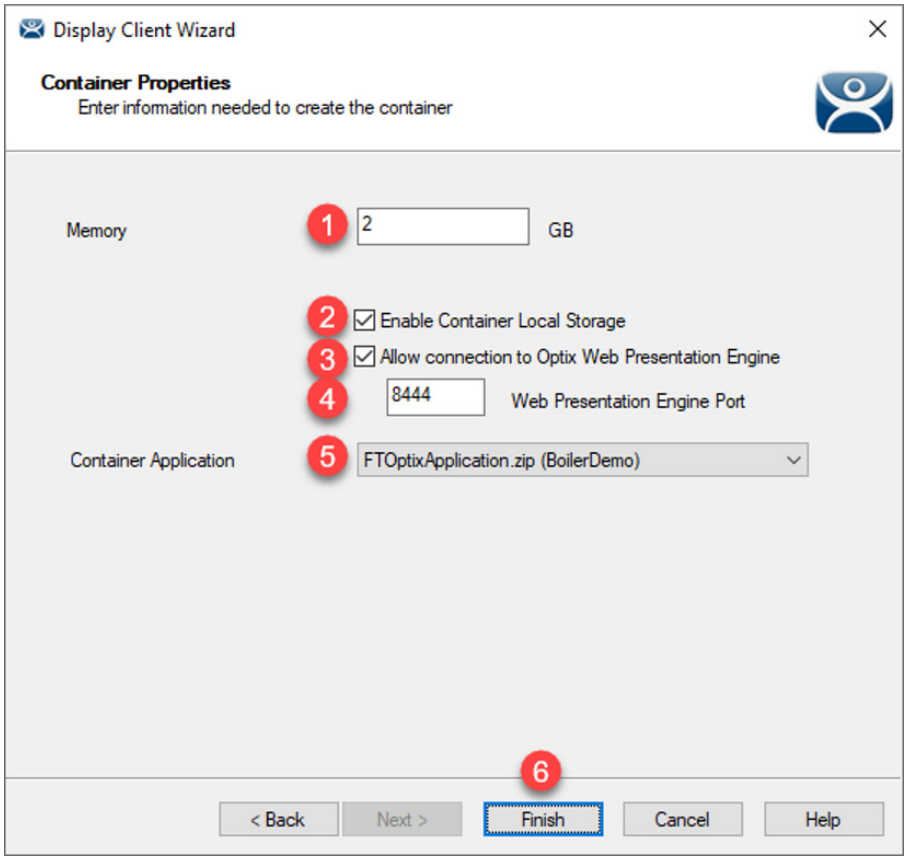
10. Navigate to the Select Container Hosts page of the wizard and check the Run container on thinclient checkbox.

Figure 118 - Select Container Hosts page



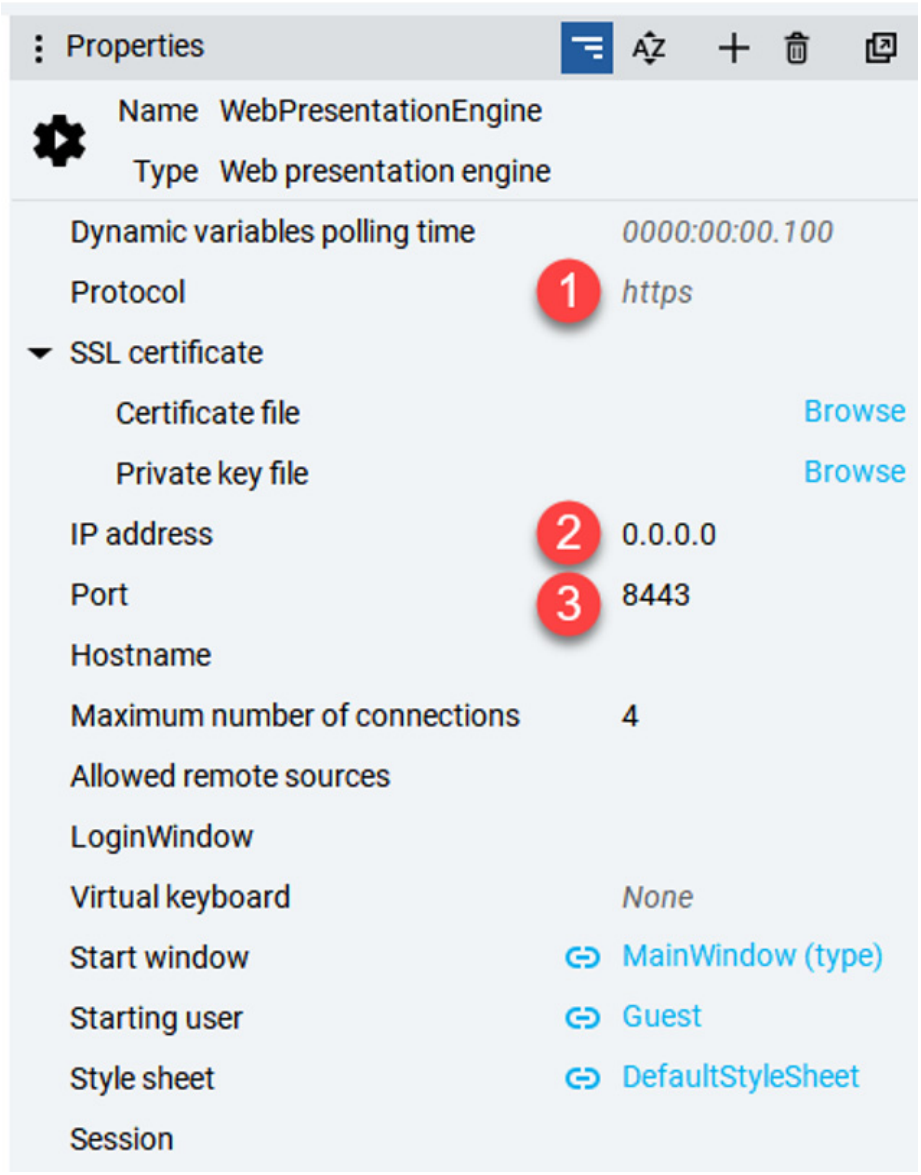
11. Skip to the Container Properties page of the wizard. Enter the maximum Memory in GB for the Container to use. Check the Enable Container Local Storage checkbox if you are using BootAssist, and you want the Optix application image to be cached within the Container. Select the Optix application from the Container Application pull-down menu.

Figure 119 - Container Properties page



If you have a Web Presentation Engine configured within your Optix application, you need to inform ThinManager of which external port incoming to the thin client is to be mapped into the Optix Container. In the example above, we have configured port 8444. So, in order to hit the Web Presentation Engine run within the Optix Container, we must open a web browser within the same network and enter https://w.x.y.z:8444 as our URL, where w.x.y.x is the IP address of the thin client where the Optix Container is running. ThinManager 14.1 only supports the mapping of external ports to port 8443 within the Optix Container; so, you must configure your Web Presentation Engine within Optix Studio to use port 8443. The relevant Web Presentation Engine settings in Optix Studio are shown below. If you are running multiple Optix Containers on the same thin client, and they are each configured for the Web Presentation Engine, then you need to make sure each Container Host Display Client is configured with a unique Web Presentation Engine Port. Again, each Optix application needs to have the Web Presentation Engine configured for port 8443.

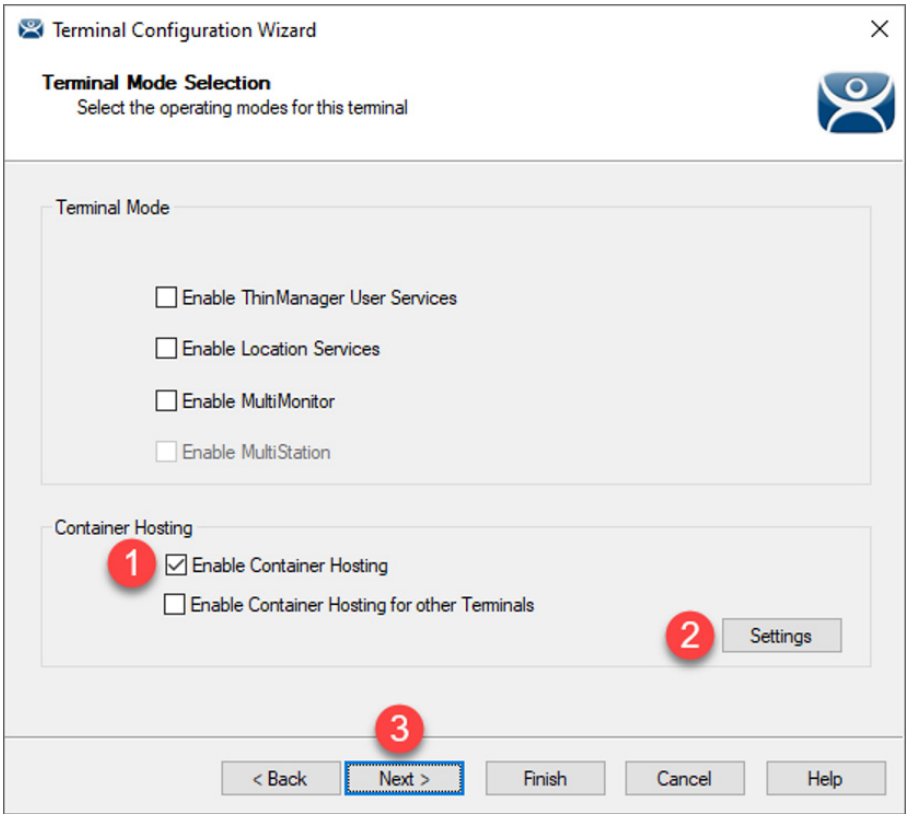
Figure 120 - Properties Settings



As noted earlier, the BootAssist module can cache the Container image as well as the Optix application image on local storage; however, it does not support persisting data within the Optix Container. For more details, please refer to BootAssist on page 560.

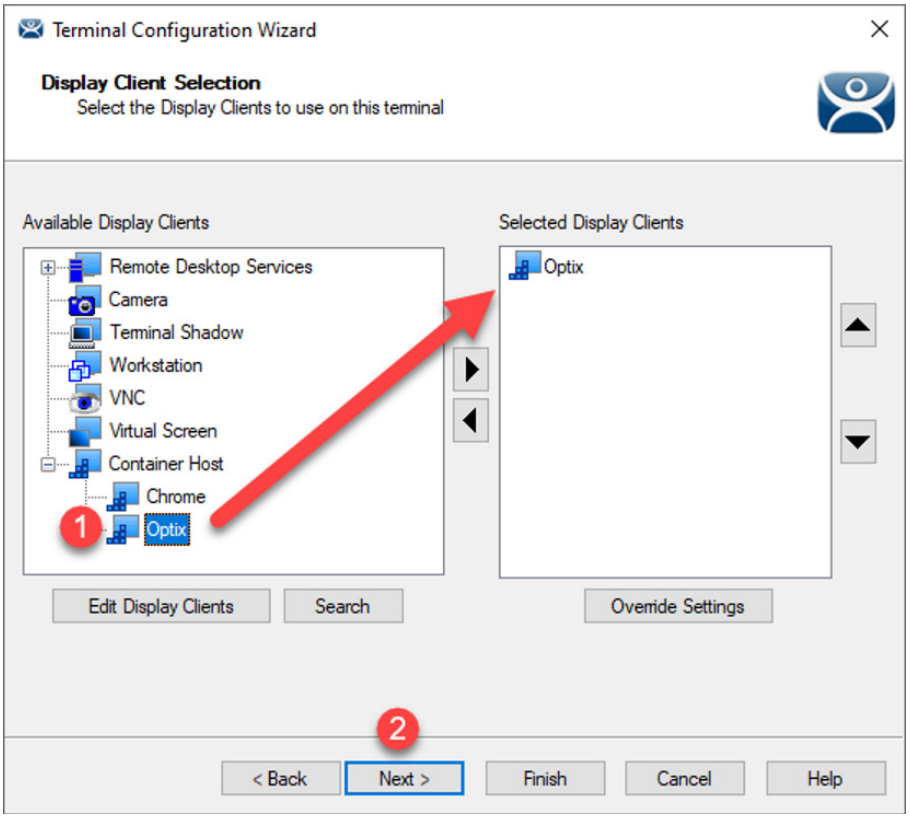
12. To apply the newly created Container Host Display Client to a terminal, double-click on the desired terminal from the Terminals tree or create a new terminal profile.
13. From the Terminal Configuration Wizard, navigate to the Terminal Mode Selection page of the wizard and check the Enable Container Hosting. Click Settings to confirm the RAM Disk Size (GB) is correct for your application and determine if you would like to Preload Container Images.
14. Click OK.

Figure 121 - Terminal Mode Selection page



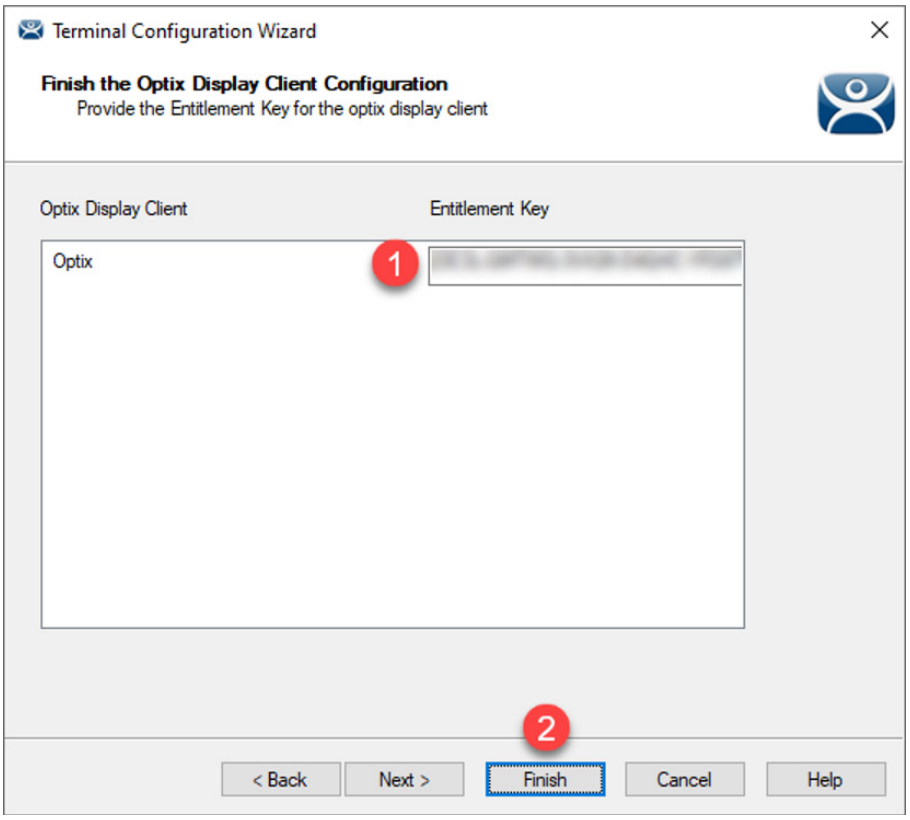
15. Navigate to the Display Client Selection page of the wizard and apply your newly created Container Host Display Client to the terminal.

Figure 122 - Display Client Selection



16. On the next page of the wizard, enter your Optix Entitlement Key, and then click Finish.

Figure 123 - Finish page



If you have more than one Container Host Display Client configured to use the optix_app Container image assigned to your terminal, you have an opportunity to provide a unique Entitlement Key for each.

17. Reboot the terminal to apply the changes.
18. Once the firmware and container images are delivered, the terminal switches to graphics mode, where the Optix application is extracted, downloaded, and launched.

Containers on Servers using Windows Server 2019

ThinManager leverages open-source Docker container technology for running Containers on servers. Container Deployment is similar to the deployment of Remote Desktop Services Servers.

1. Create a Windows 2019 Server and install Docker.
2. Install the Container image in ThinManager.
3. Define the Container Host as a Display Server.
4. Define the Container as a Display Client and add the Container Image to the Container Display Client.
5. Apply the Container Display Client to the Terminal.

   The Container Host needs two TLS Certificates and a TLS key installed, which provides secure authentication between the Container Host and the ThinServer service. The certificates can be generated with the TLS Certificate tool in ThinManager.
6. Generate the two certificates and the key, and move them to the Docker Container Host.

On boot, the thin client requests a connection to the container from ThinManager, which starts a container instance, if not already running, and returns the connection details to the thin client. Then, the thin client establishes a connection directly to the container.

This section shows the steps to configure the Container system in ThinManager, then covers the Certificate process once ThinManager is configured. It is possible to create the certificates during the ThinManager configuration process, but it is easier to understand if it is done as one procedure.

Container Host Server Installation

To make the selected server a Docker Container server, the script **Install-Docker.ps1** installs Hyper-V and Containers Roles.
Windows Server 2019 with Internet connection is required for the Docker Container Server solution in ThinManager. Offline installation is not available as the Internet is necessary to download files from Microsoft Servers and Rockwell Automation Servers.

If a virtual machine is not used, skip to Running the Script. To prepare your virtual machine, follow these steps to enable nested virtualization.

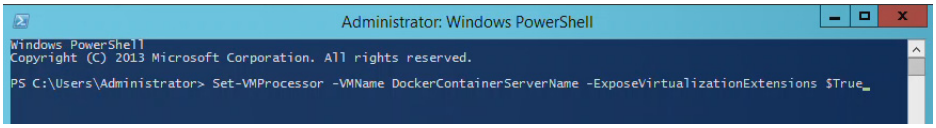
If a Hyper-V virtual machine is used, this setting can be set using PowerShell.

1. Power off the Docker Container Server virtual machine.
2. On the Hyper-V host, open PowerShell as an Administrator.

Figure 124 - Windows PowerShell

3. Type the following command:
   `Set-VMProcessor -VMName [VM Name] -ExposeVirtualizationExtensions $True`
   where [VM Name] is replaced by the Docker Container virtual machine name. See Figure 125.

Figure 125 - Type Command into PowerShell

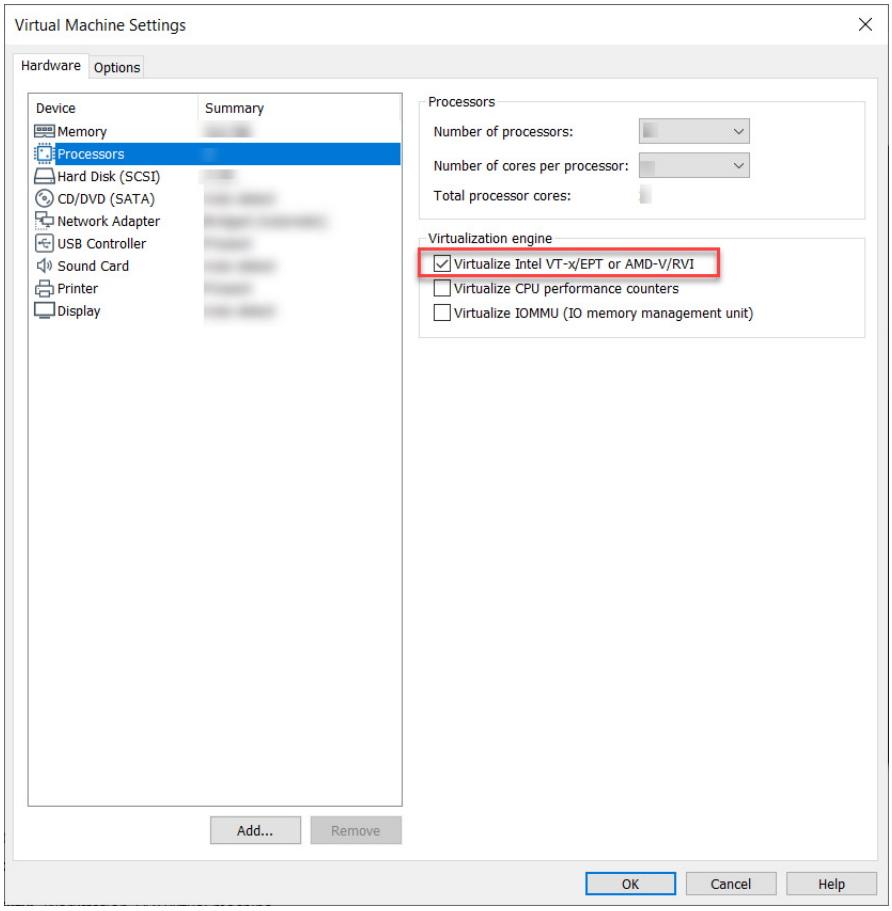


4. Press Enter to run the command.

If you use a VMware® virtual machine, this setting can be configured under Virtual Machine Settings.

1. Power off the Docker Container Server virtual machine.
2. Navigate to Virtual Machine Settings.

Figure 126 - Virtual Machine Settings



3. Click the Hardware Tab, and select Processors.
4. Under the Virtualization engine properties section, check Virtualize Intel VT-x/EPT or AMD-V/RVI.
5. Click OK.

Run the Script

Once the designated Server 2019 has Internet connectivity, run the script **Install-Docker.ps1** located in the installer files at:
\Common\12.0.0-ThinManager\Install-Docker.ps1
or at downloads.thinmanager.com.

The **Install-Docker.ps1** script has two components: the Installation of Hyper-V and the installation of Container roles. The virtual machine restarts during the installation processes of the Hyper-V and Containers roles, as required.

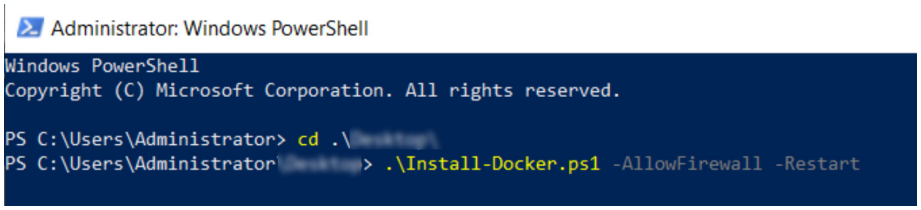
You must manually initiate the script a second time during this installation process as detailed below.

1. Open PowerShell as an Administrator.

Figure 127 - Windows PowerShell

2. Change the file directory as necessary to match the location of Install-Docker.ps1.

Figure 128 - Install Script



3. Type:
   `".\Install-Docker.ps1 -AllowFirewall -Restart".`
   and press Enter to run the script. See Figure 128.

Switch	Description
-AllowFirewall	Creates a Windows firewall rule, Docker SSL Inbound, to allow TCP2376, the default port for Docker. If this is not specified in this PowerShell command, it must be added manually to the Windows firewall rules.
-Restart	Automatically restarts the server after the installation of Hyper-V and Docker Containers. If it is omitted, the script prompts if a restart is required.
-Verbose	Enables more in-depth information about command processing.

4. Once the server restarts, repeat steps 1 through 3 to initiate the Install-Docker.ps1.
5. To complete the installation, restart the Docker service in Windows Services or restart the server.

For more information on the script, type the command:
`Get-Help .\Install-Docker.ps1`

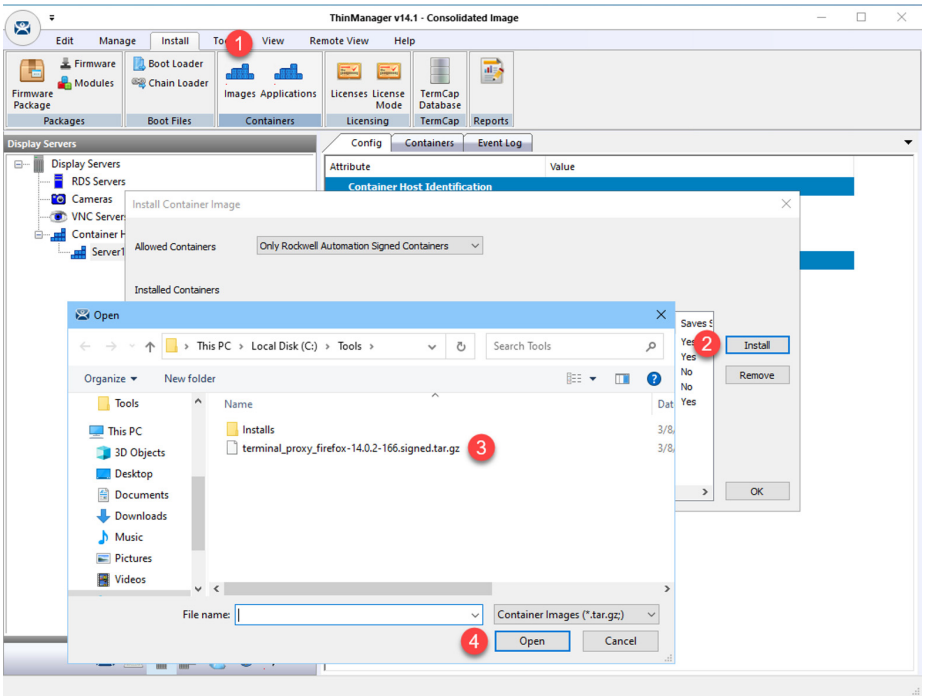
Install Container Images

The Container images are included as part on the ThinManager installation. Additional containers can be installed into ThinManager, similarly to firmware packages, as they become available. Installed containers can be downloaded from https://downloads.thinmanager.com/. The Installed Containers indicate the version of the container if Browser Cookies are stored for that container, and if the container is signed with a Rockwell Automation certificate.

A pull-down menu provides the ability to choose the container type that is allowed to be loaded onto terminals: All Containers (signed or unsigned), Only Rockwell Automation Signed Containers, or Only Signed Containers.

Technical support associated with a Software Maintenance contract is limited to containers provided and signed by Rockwell Automation, and does not extend to custom containers.

Figure 129 - Install Container Images



To install container images, follow these steps.

1. Choose Install>Images.

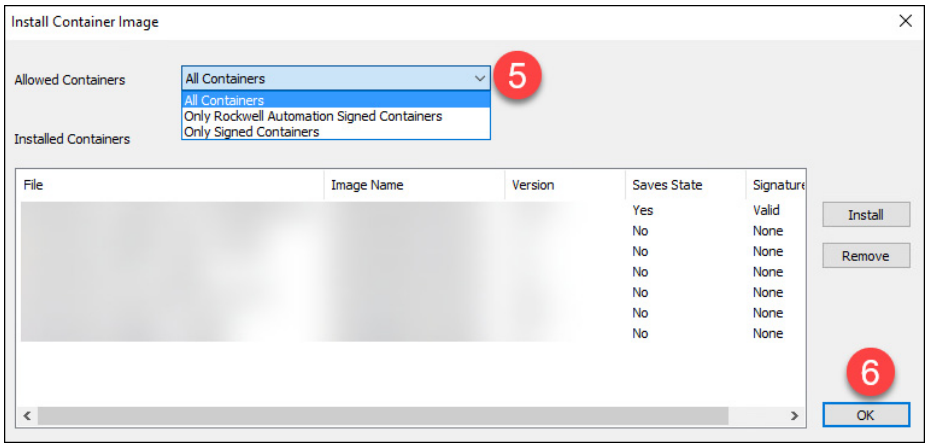
   The Install Container Image dialog box appears.

2. Click Install.

   The File Browser appears.

3. Selecting the Container Image ***tar.gz** file
4. Click Open.

Figure 130 - Allowed Container Selection



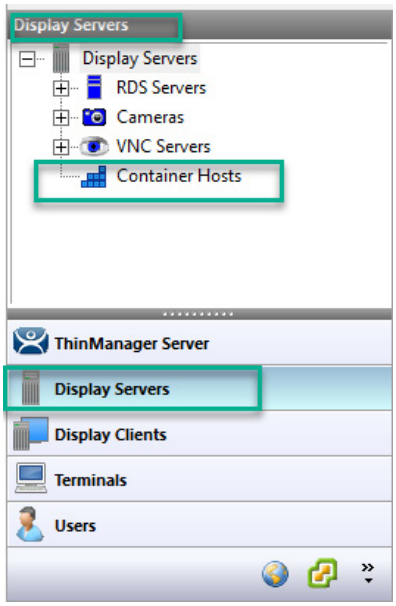
5. (Optional) Choose the type of containers that are allowed to be used on terminals by changing the setting in the Allowed Containers pull-down menu.
6. Click OK.

   The Container Image is installed.

Define the Container Host Display Server

The Container Host is a new branch of the Display Server branch of the ThinManager tree.

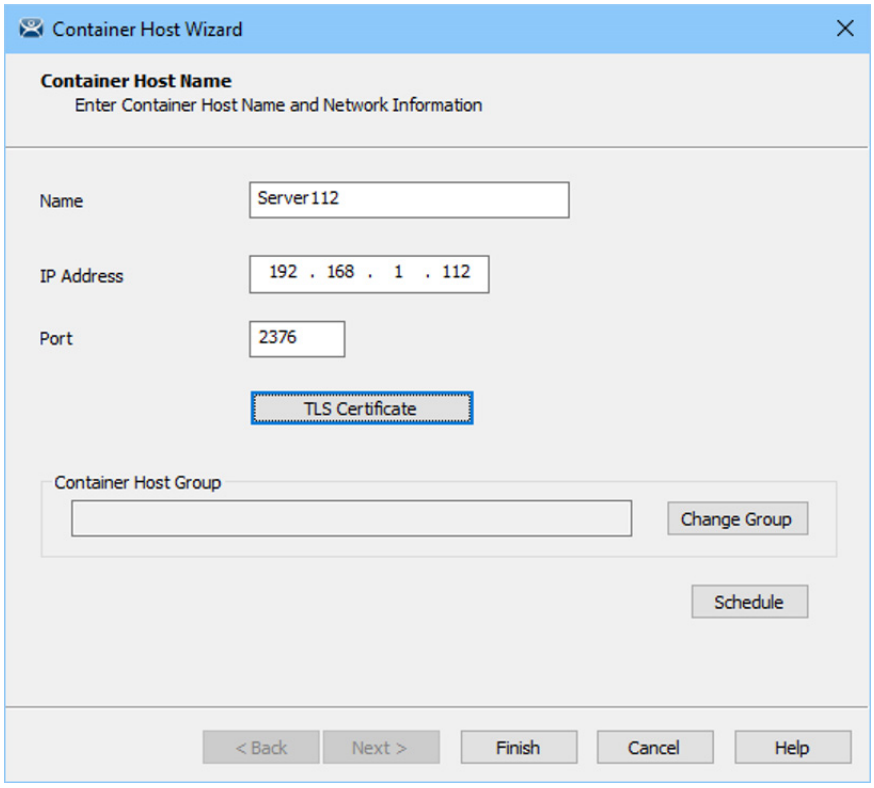
Figure 131 - Container Hosts in Display Server Branch



1. Right-click on the Container Hosts icon and choose Add Container Host.

   The Container Host Wizard appears.

Figure 132 - Container Host Wizard



2. Type the name of the Container Host in the Name field.
3. Type the IP address in the IP Address field.

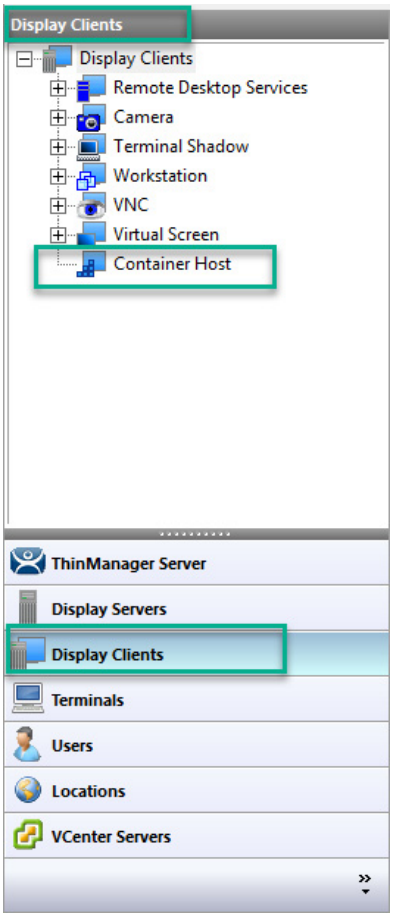
4. Type the port number that is used for the container connection. Port 2376 is the default port number, but it can be changed in the wizard if it was changed on the Container Host.
5. Click Finish to exit the Container Host Wizard.

You must click TLS Certificate to open the TLS Certificate dialog box, which allows you to save the Server Certificate and Server Key. See Install the TLS Certificates on page 110.

Define the Container Host Display Client

The Container Host is a new branch of the Display Clients branch of the ThinManager tree.

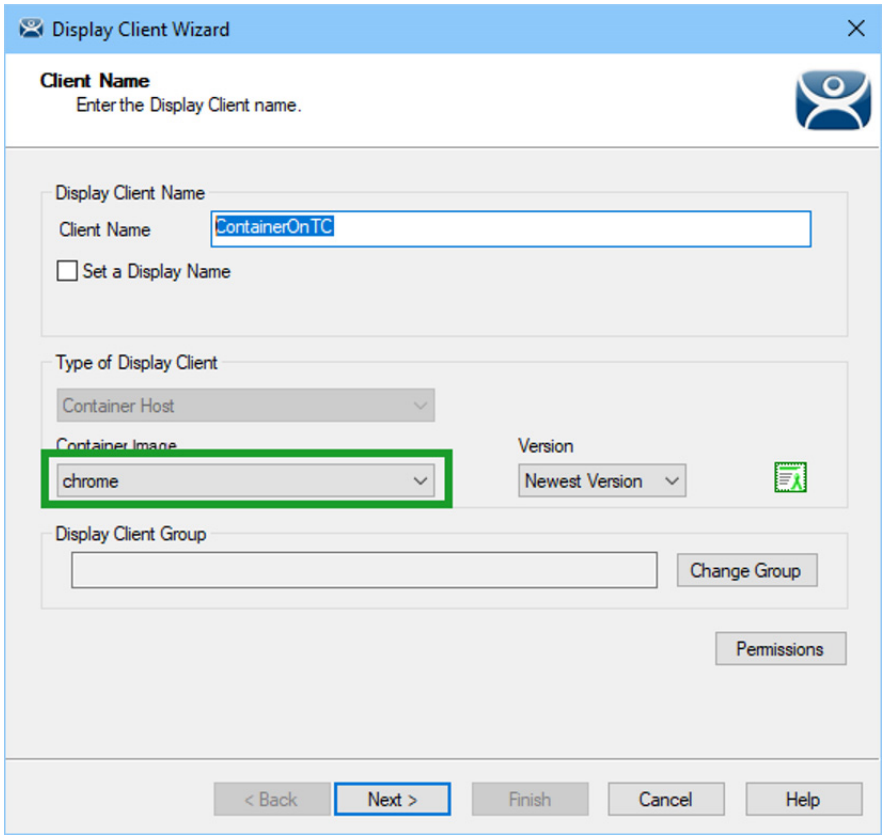
Figure 133 - Container Host in Display Clients Branch



1. Right-click on the Container Host icon and choose Add Display Client.

   The Display Client Wizard appears.

Figure 134 - Display Client Wizard

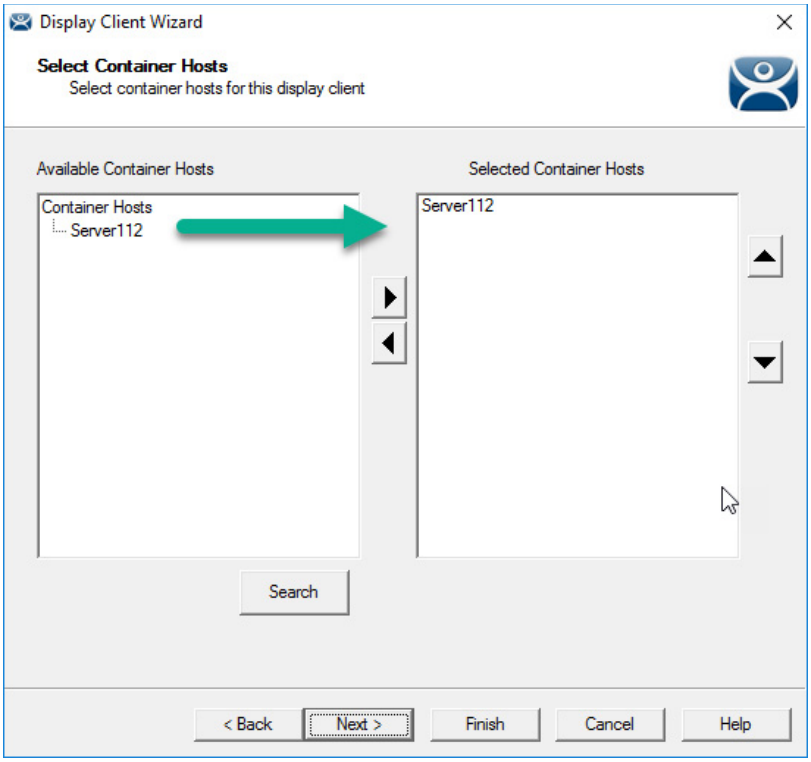


2. Type the name of the display client in the Client Name field.
3. Choose a Container Image from the Container Image pull-down menu. The chrome image is the default selection. See Install Container Images on page 102 for more information on installed Container Images.
4. Click Next.

   The Display Client Wizard continues with the typical pages and settings.

The Select Container Hosts page of the Display Client Wizard allows the selection of a Container Host much like Remote Desktop Servers are selected in Remote Desktop Server Display Clients.

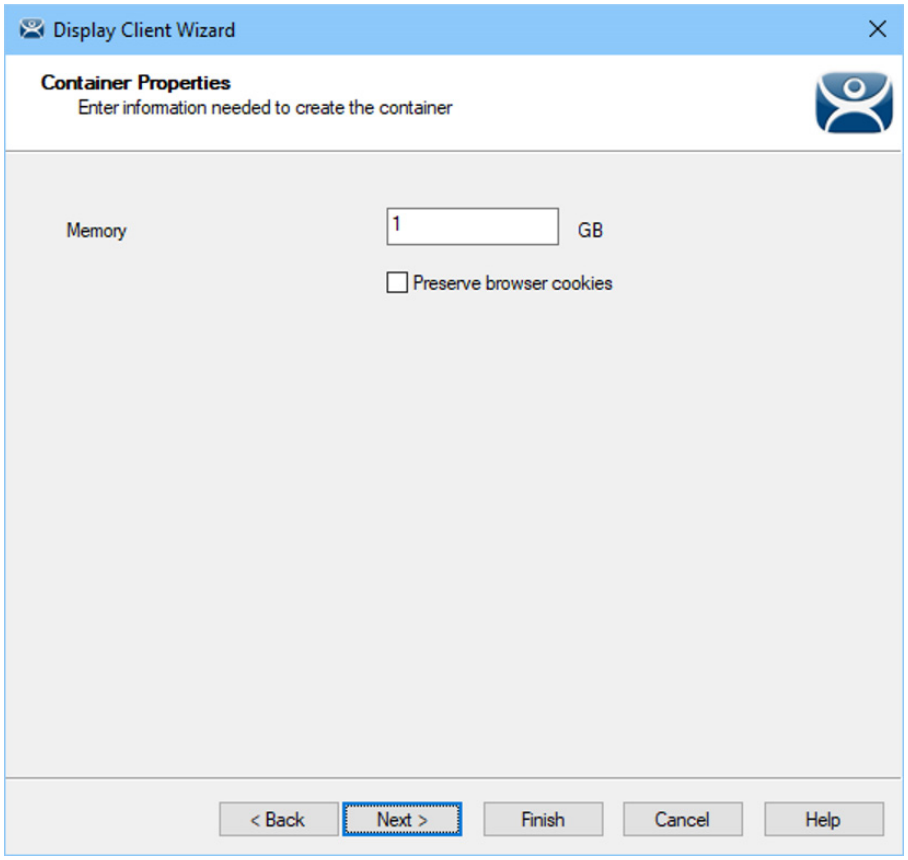
Figure 135 - Select Container Hosts Page



5. Select the Container Host of your choice for the Display Client.
6. Click Next to continue with the wizard.

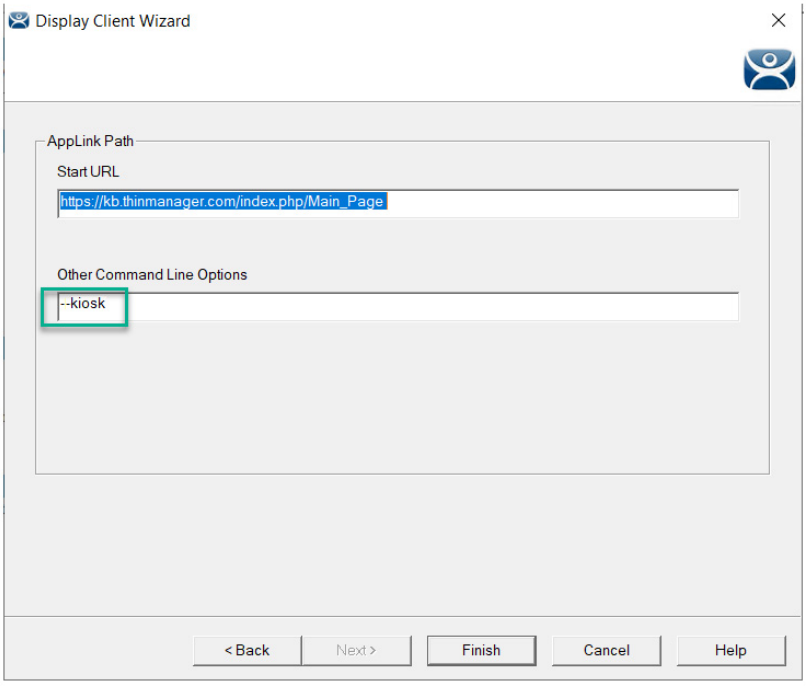
   The Container Properties page shows the maximum size the Docker Container uses. By default, the maximum size is 1 GB, but it can be changed.

Figure 136 - Container Properties



7. Click Next to continue.
8. The final page of the Container Display Client Wizard, which uses one of the web browser Container images, allows you to specify the Start URL and Other Command Line Options.

Figure 137 - AppLink Path Page



9. Type the URL of the desired web content to display.
10. In the Other Command Line Options field, type --kiosk.

The selected web browser Container starts in Kiosk Mode, which prevents user access to the browser address bar. The syntax of this switch may vary from browser to browser.

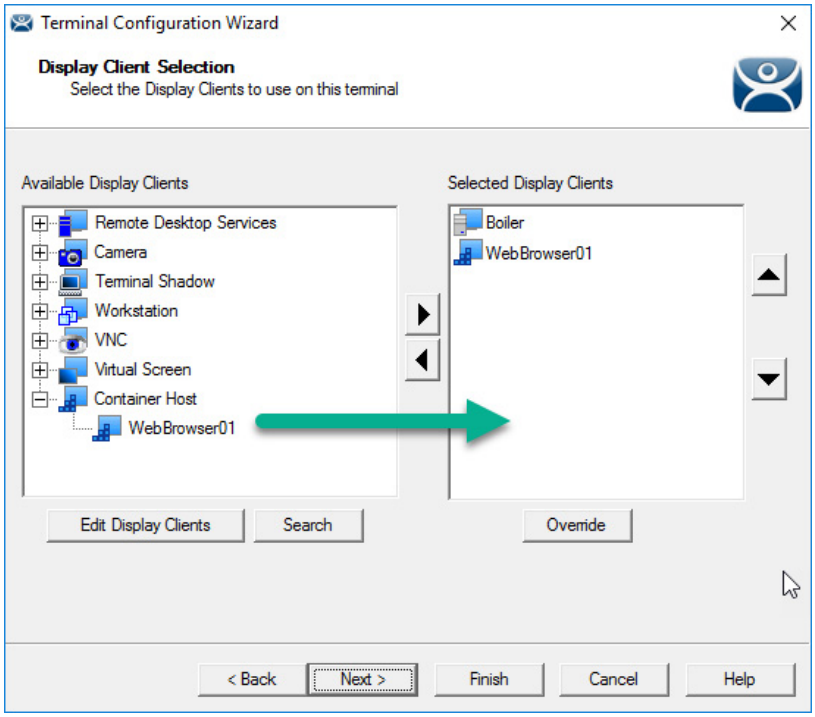
11. Click Finish to close the Wizard.

Apply the Container Display Client to a Terminal

Container Host Display Clients are added to thin clients, or terminals, like any other Display Client.

The Container Display Client is added on the Display Client Selection page with the other Display Clients.

Figure 138 - Display Client Selection Page

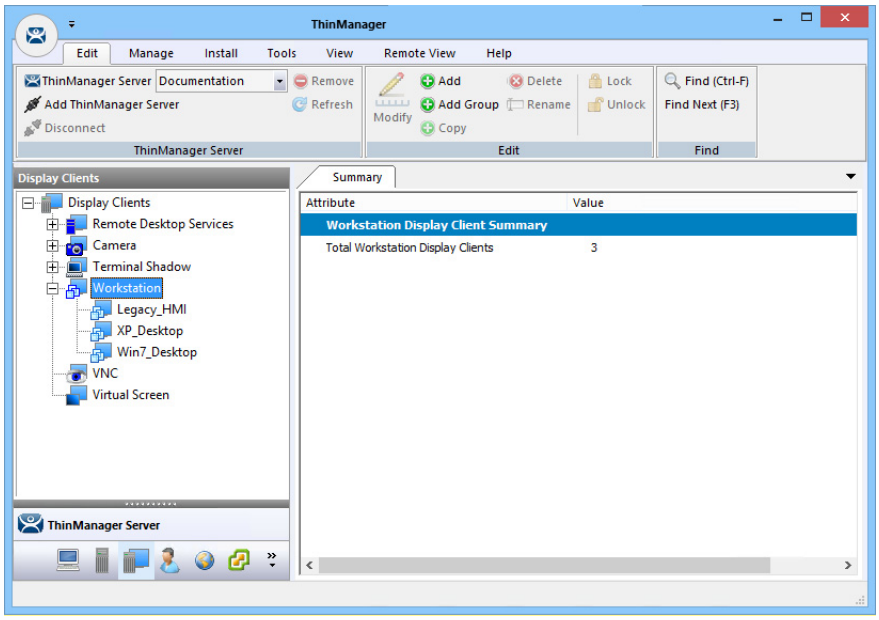


1. Expand the Container Host branch, highlight the Container Display Client, and click the right arrow.

   The selected Container Display Client launches when the terminal boots.

   Figure 139 shows the ThinManager Knowledge Base launches in the container on a thin client.

Figure 139 - ThinManager Knowledge Base in Container



Install the TLS Certificates

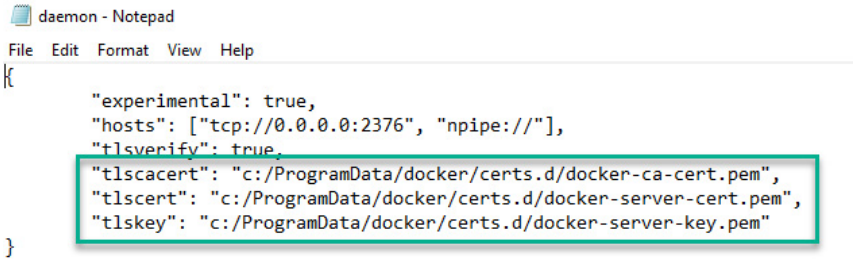
A TLS Certificate is needed to provide secure authentication between the Container Host and the ThinServer service. There are two certificates and one key that must be generated in ThinManager and copied to the Container Host.

When Docker is installed, a configuration folder that contains the file **daemon.json** is created, which contains the names and locations of the keys and certificates. This file is found at: C:\ProgramData\docker\config.

Three files are needed to add the two certificates and one key to the Container Host.

By default, the certificates and keys are saved at C:\ProgramData\docker\certs.d. You must manually create the certs.d folder.

Figure 140 - JSON File



Certificate Authority Certificate

The first certificate needed is the Certificate Authority (CA) Certificate, which is obtained from TLS Certificate window.

1. Choose Manage>TLS Certificate from the ribbon bar.

The Manage TLS Certificates window appears.

2. Select ThinManager Server CA Certificate from the Show Certificates for pull-down menu.
3. Double-click the certificate listed (yours likely has a different name).
4. On the Certificate Details window, click Save.

Figure 141 - Certificate Details

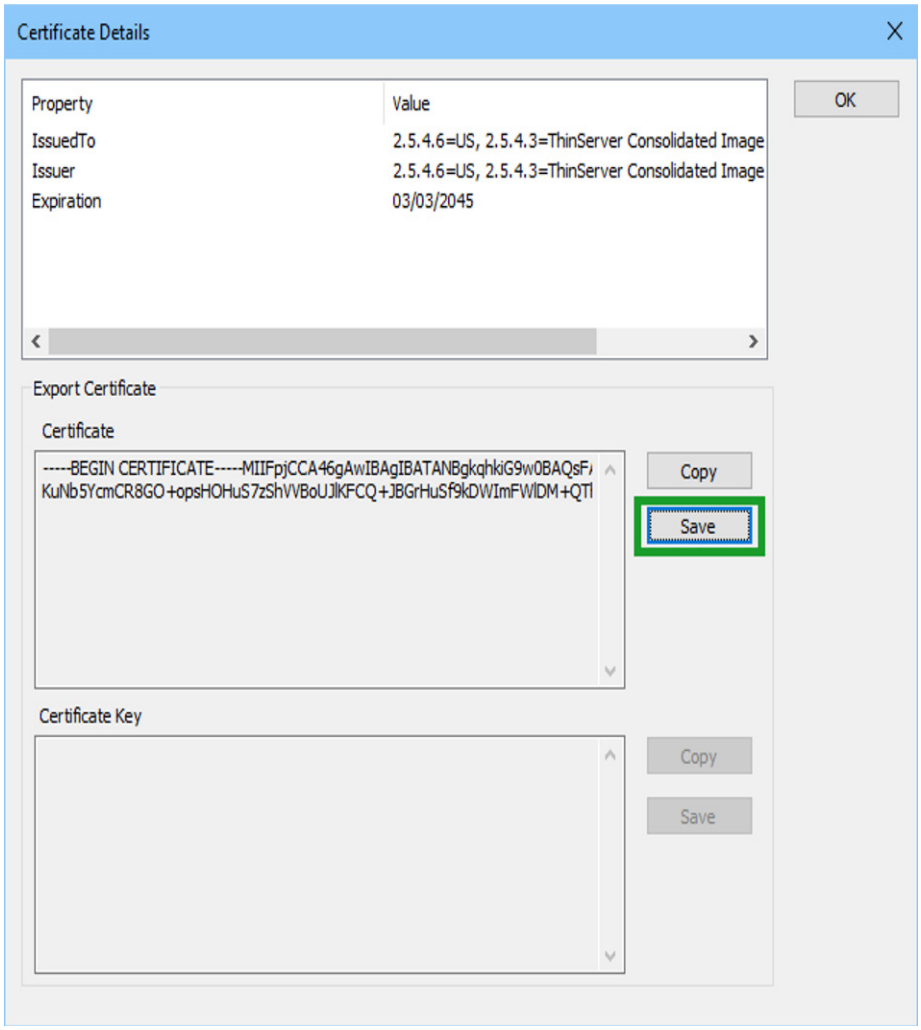
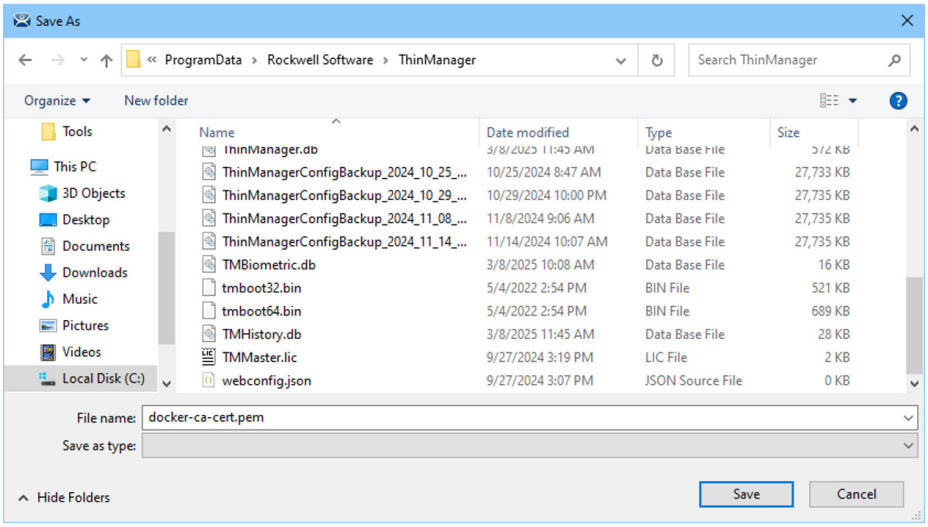


Figure 142 uses docker-ca-cert.pem as the CA certificate name. You must use the file name that was specified in the Docker configuration folder.

There is only one CA certificate needed per ThinManager system. However, this also means that a Docker Host cannot be shared by two independent ThinManager systems.

Figure 142 - CA Cerfiticate Name

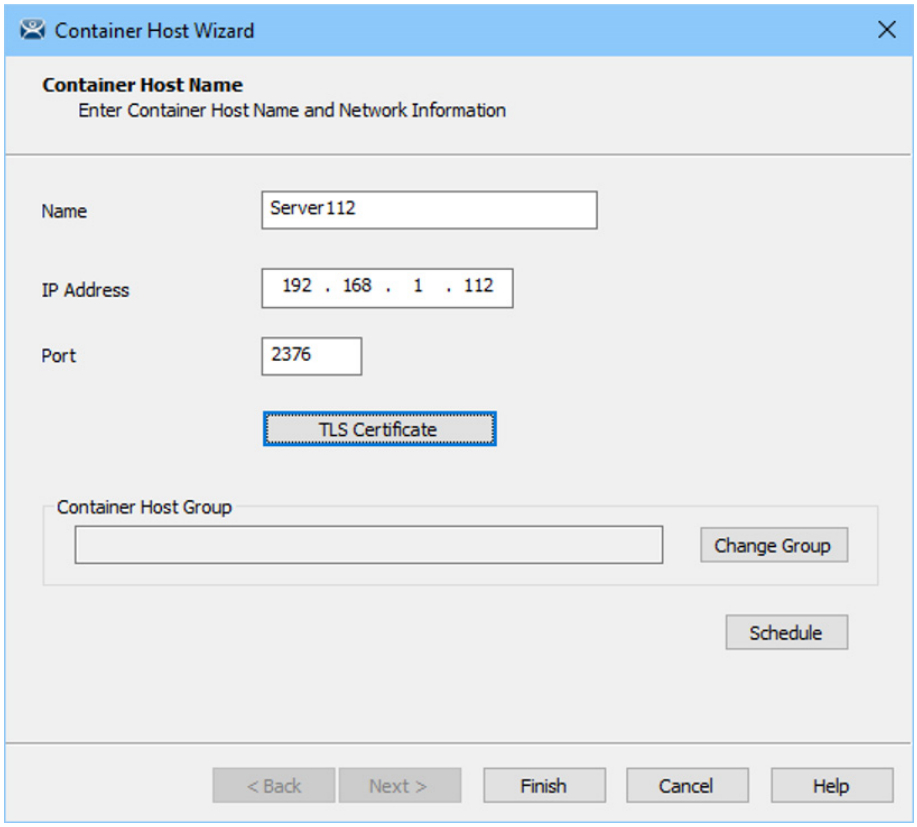


5. Click OK to exit the wizard.

Server Certificate

The second certificate is the Server Certificate, which is generated in the Container Host Display Server Wizard.

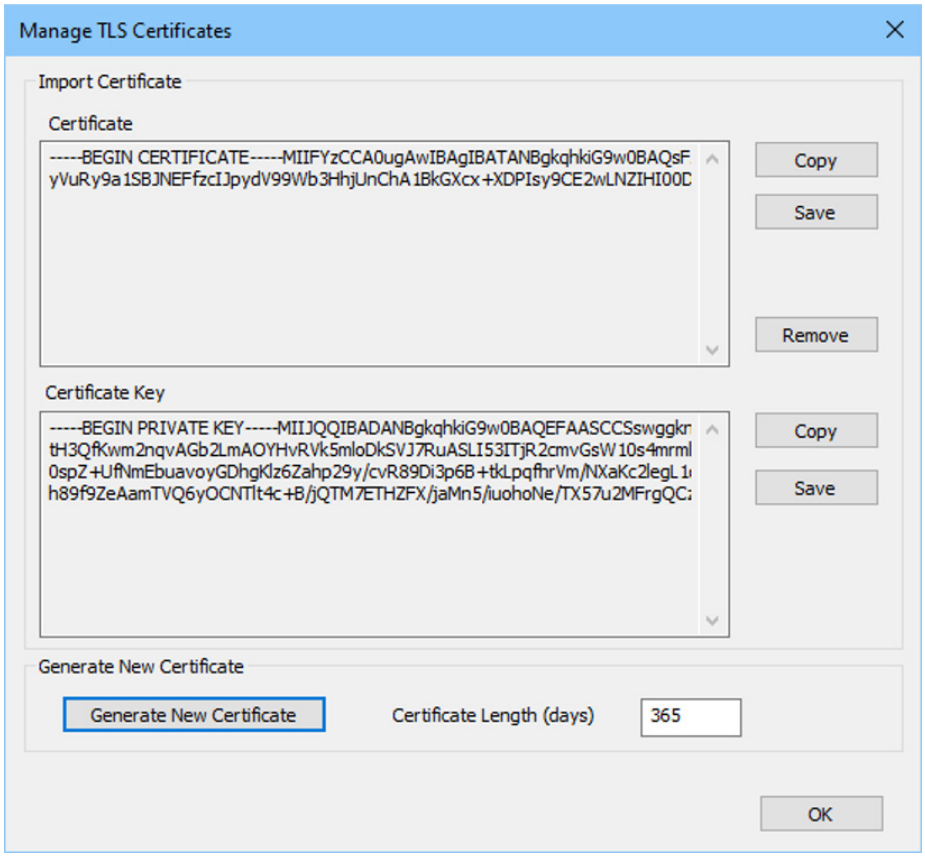
Figure 143 - TLS Certificate Button



1. Click TLS Certificate.

   The Manage TLS Certificates window appears.

Figure 144 - Manage TLS Certificate

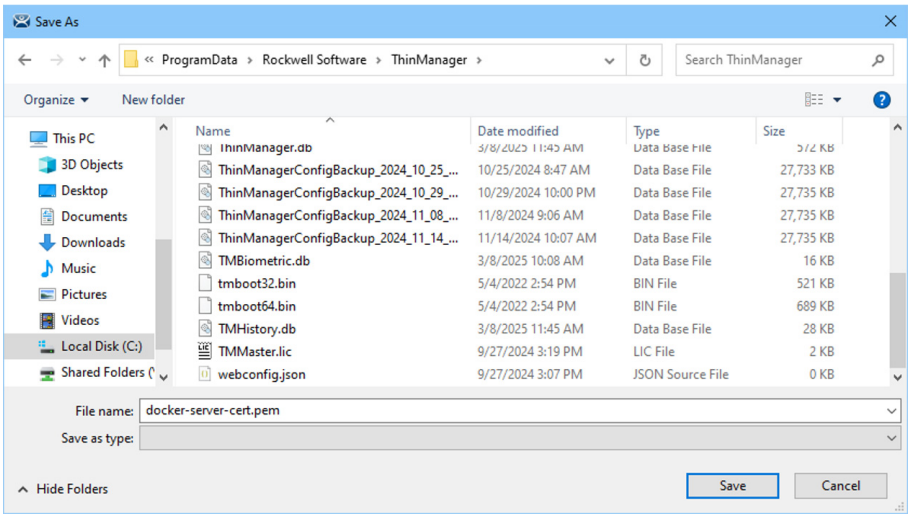


The Manage TLS Certificates window does not show the Certificate and the Certificate Key until Generate New Certificate is clicked. The generated Certificate and Certificate Key must be saved and copied to the Container Host.

2. Click Save for the Certificate.

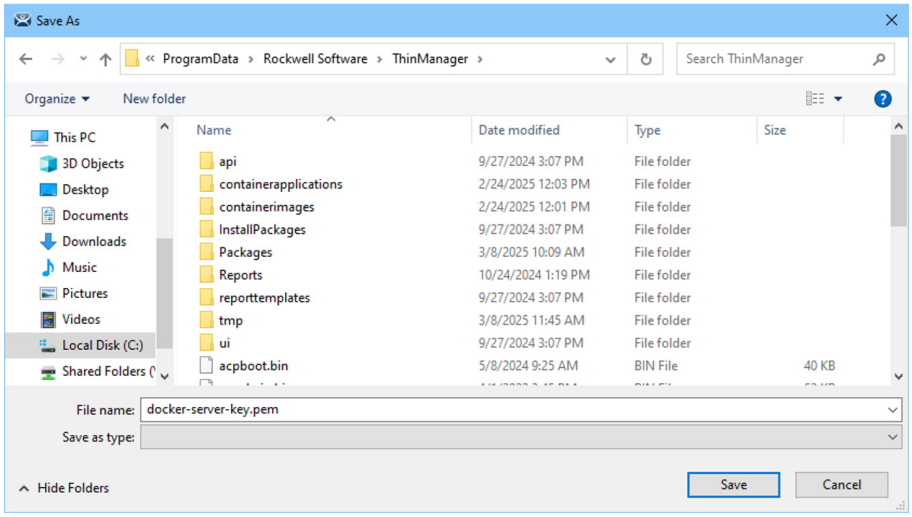
   By default, the Server Certificate is saved with a file name of docker-server-cert.pem, which must match the name specified in the Docker configuration folder.

Figure 145 - Save Server Certificate



3. Click Save for the Certificate Key.

Figure 146 - Save Certificate Key

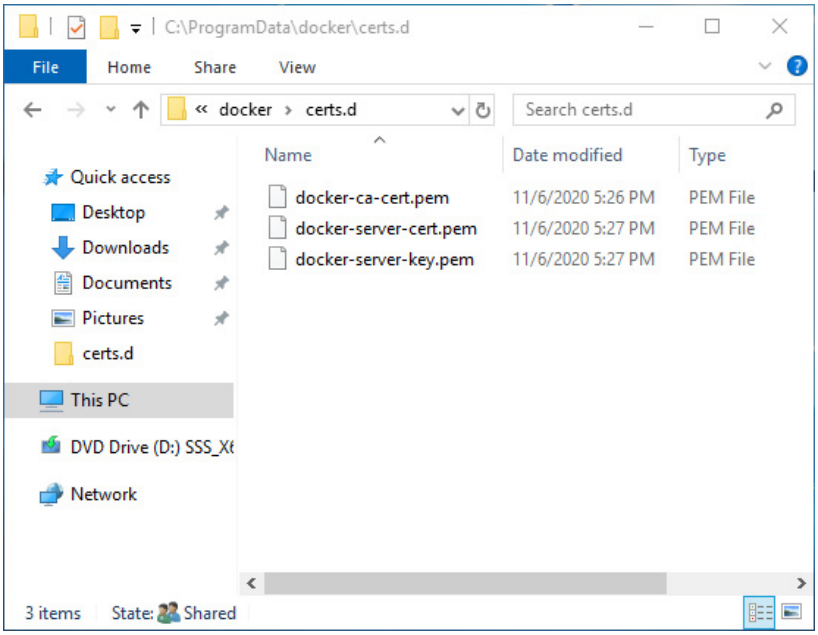


Install the Certificates

1. Open the Docker Container Host server.
2. Copy the three files to the default location, C:\ProgramData\docker\certs.d, or the location you specified in the Docker config file. You must create the **certs.d** folder manually.
3. Restart the Docker service to register the new certificates.

Figure 147 shows the three certificate files, generated through ThinManager, installed on the Container Host.

Figure 147 - Certificate Files on Container Host



IP Cameras

ThinManager supports cameras in the ThinManager system. Cameras, either IP or USB, can be configured to provide the camera feed to display clients on Terminals. This section covers how to define the camera as a Display Server. Delivery of the video to a Camera Display Client is covered in Camera Display Clients on page 165.

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

1. Configure the camera and add it to your network using the guidelines from the camera manufacturer.
2. Add the configured camera to ThinManager as a Display Server source.
3. Deploy the content of the cameras by creating a camera display client and applying it to the Terminals.

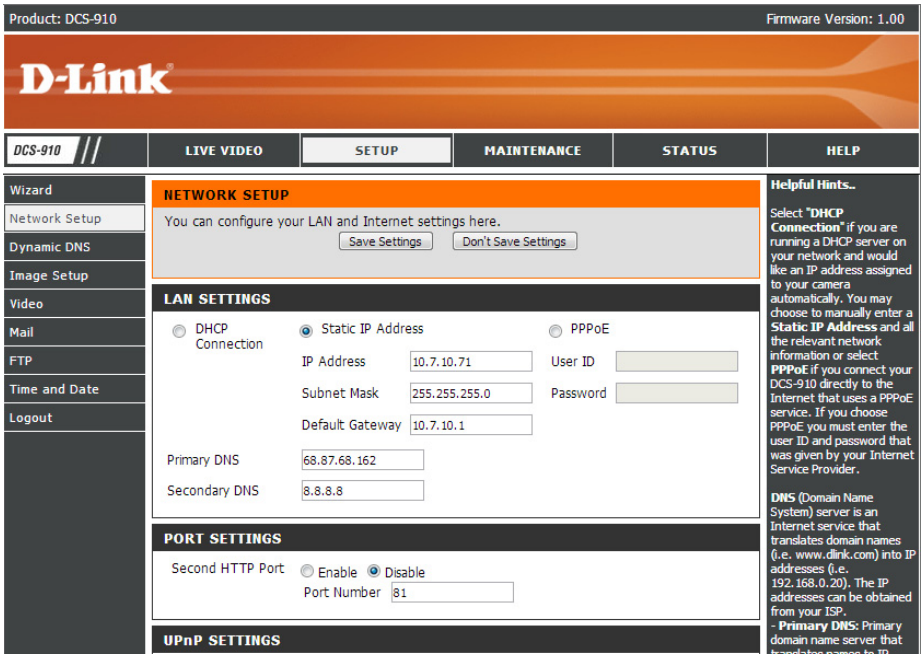
USB cameras are added to a Terminal and configured. See Define the IP Camera as a Display Server on page 115.

Configure the IP Camera

Each camera manufacturer distributes their cameras with a default IP address and a default administrative account. These need to be configured to add the camera to your network. Methods vary between vendors, but a web interface is common.

IMPORTANT Please follow the instructions from the camera manufacturer to configure your camera for use.

Figure 148 - Browser-based Camera Configuration

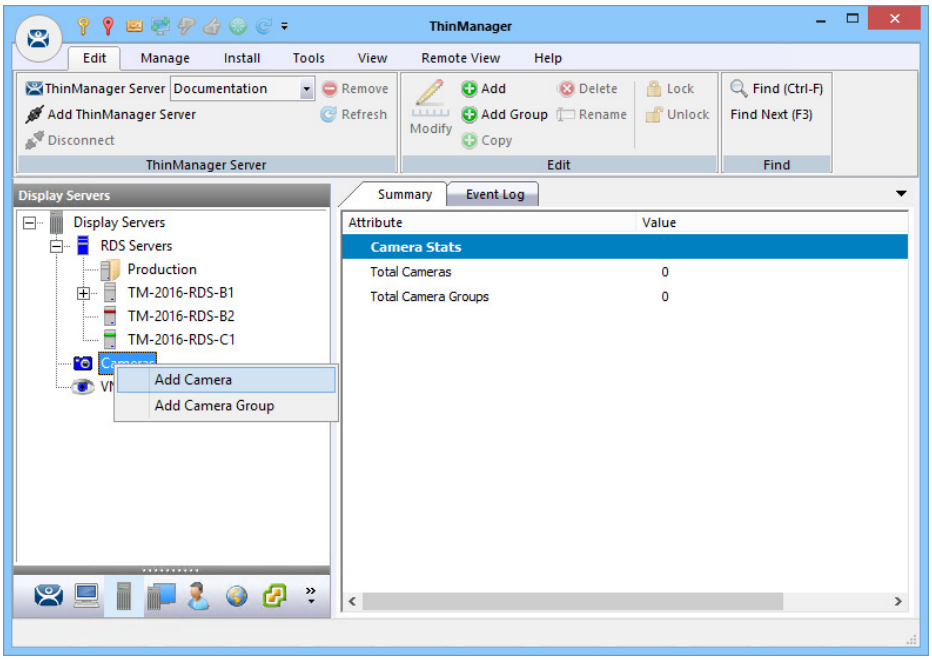


Define the IP Camera as a Display Server

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

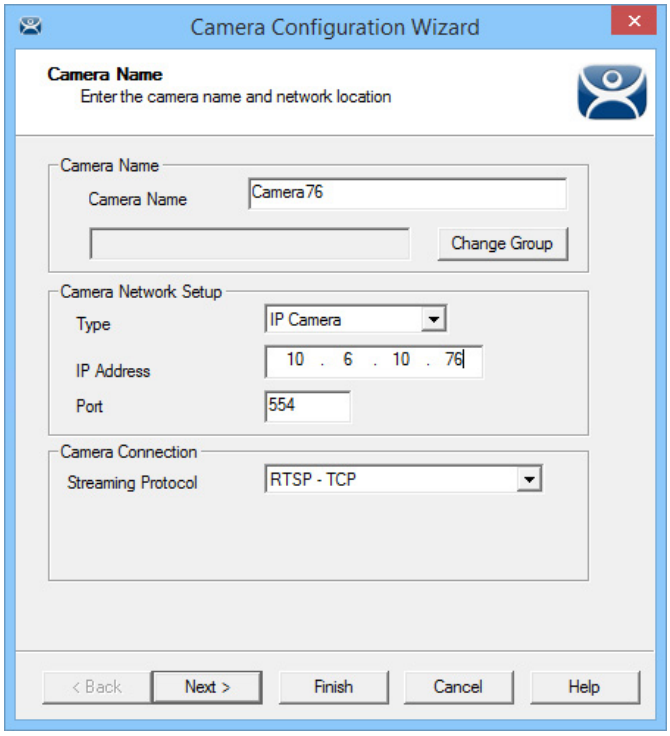
1. To open the Display Servers tree, click the Display Servers icon at the bottom of the ThinManager tree.

Figure 149 - Camera Branch of the Display Servers Tree



2. Right-click on the Cameras branch and choose Add Camera to launch the Camera Configuration Wizard.

Figure 150 - Camera Name Page



3. Complete the Camera Name field.
4. In the Camera Network Setup section, chose either USB Camera or IP Camera from the Type pull-down menu.

IP Camera

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

Choose a protocol that the camera uses from the following choices.

Legacy Motion JPEG

Legacy Motion JPEG is the original protocol configuration for IP cameras in ThinManager.

For this option, choose the make and model from a list contained in the TermCap database. ThinManager populates the necessary URL.

Motion JPEG

This protocol provides flexibility of camera choices because it does not require the use of a camera from the TermCap database.

Each camera uses a specific Motion JPEG URL, usually specified in the camera manufacturer's documentation.

Enter the Motion JPEG URL in the Custom URL field on the Camera Authentication page.

Real Time Streaming Protocol (RTSP)

RTSP is preferred as it is most widely supported by camera companies.

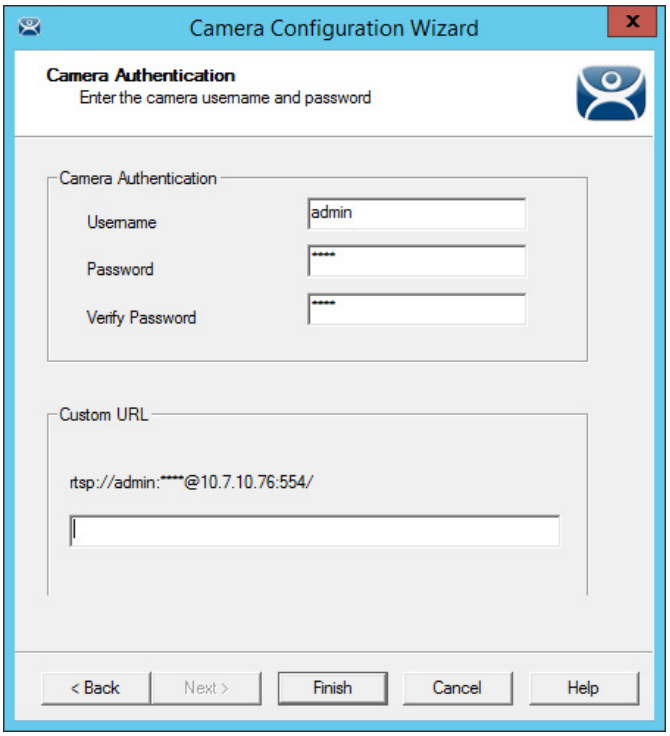
RTSP has several transport layers—HTTP, TCP, UDP, and UDP multicast. Specify the URL that specific camera uses for the video stream.

For this option, follow these steps.

1. Choose IP Camera from the Type pull-down menu.
2. Enter the IP address of the camera in the IP Address field.
3. Choose the desired transport method from the Streaming Protocol pull-down menu.
4. Click Next.

   The Camera Authentication page appears.

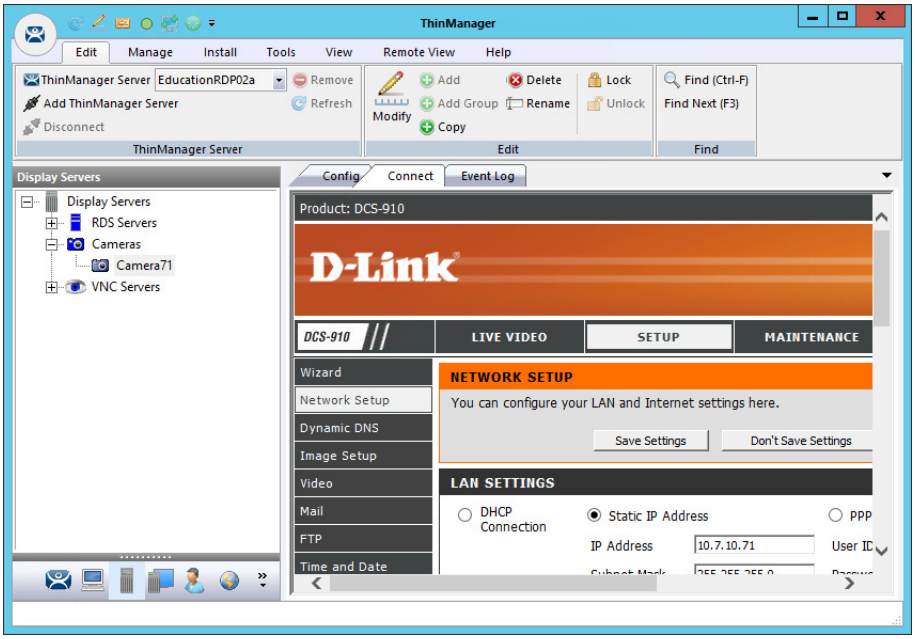
Figure 151 - Camera Authentication Page



5. Enter the Username and Password of the account for the camera that allows streaming. The thin client is unable to access the video feed without an account unless the camera allows anonymous access.
6. Enter the RTSP URL specified by the camera manufacturer in the Customer URL field.
7. Click Finish.

   The wizard closes and camera configuration is complete.

Figure 152 - Camera Management Dialog



To access the camera's browser control panel, highlight the camera in the ThinManager tree and click the Connect tab. Make changes as needed.

- 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 are available, but not the live video feed.

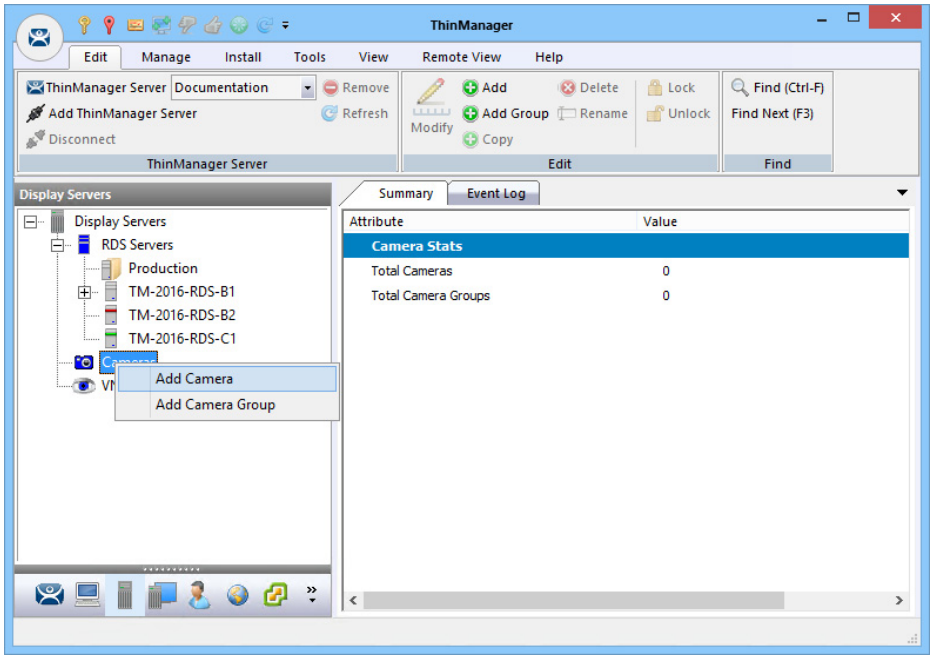
Define the USB Camera as a Display Server

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

To define the USB camera as a display server, follow these steps.

1. To open the Display Servers tree, click the Display Servers icon at the bottom of the ThinManager tree.

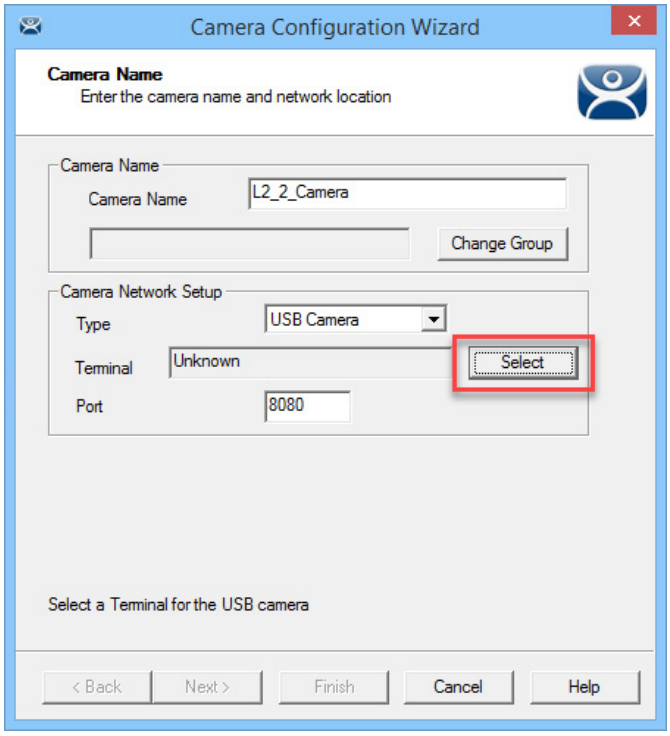
Figure 153 - Camera Branch of the Display Servers Tree



2. Right-click the Cameras branch and choose Add Camera.

   The Camera Configuration Wizard appears.

Figure 154 - USB Camera on Camera Name Page

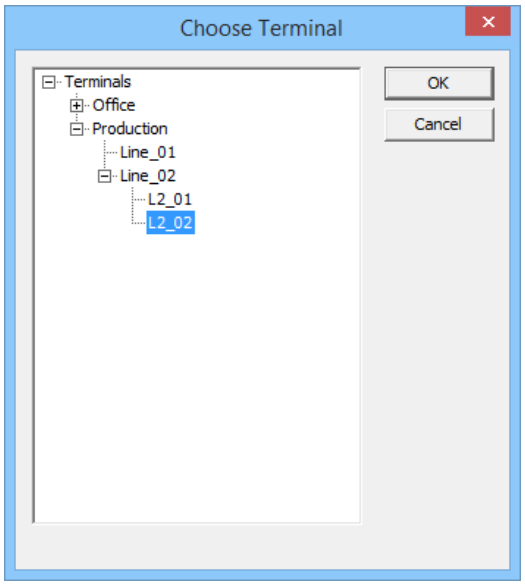


3. Complete the Camera Name field.
4. Select USB Camera from the Type pull-down menu.

   The Terminal field appears dynamically.
5. Click Select.

   The Choose Terminal dialog appears.

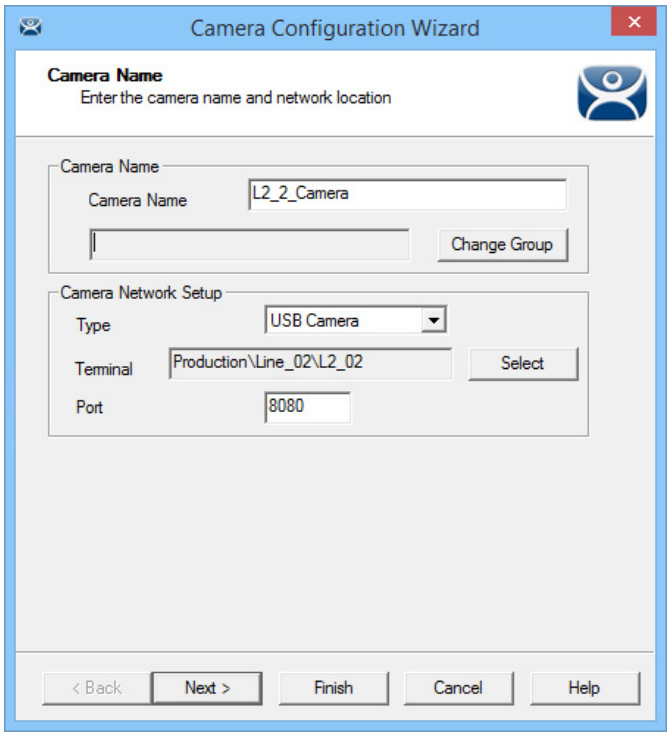
Figure 155 - Choose Terminal Dialog



6. Choose the correct Terminal and click OK.

   The Terminal appears in the Terminal field of the Choose Terminal dialog.

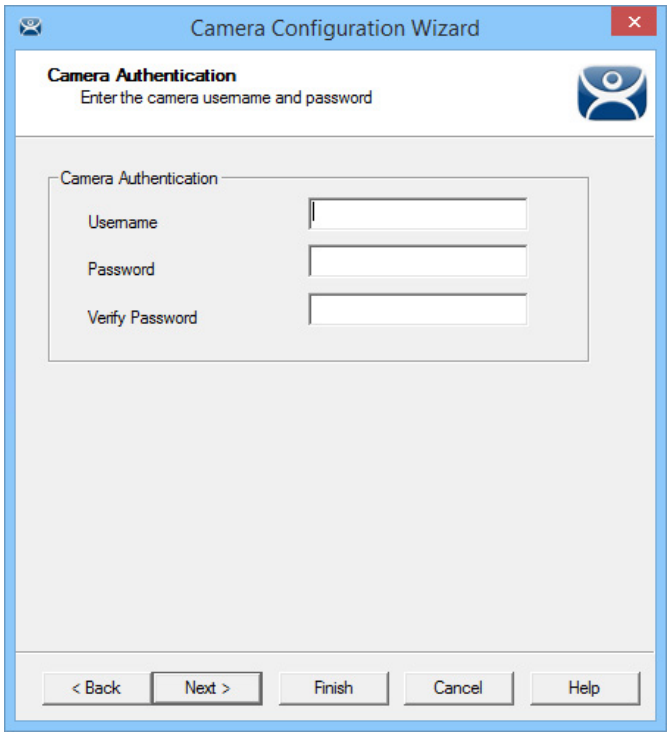
Figure 156 - Terminal Name in the Camera Name Page



7. Click Next.

   The Camera Authentication page appears.

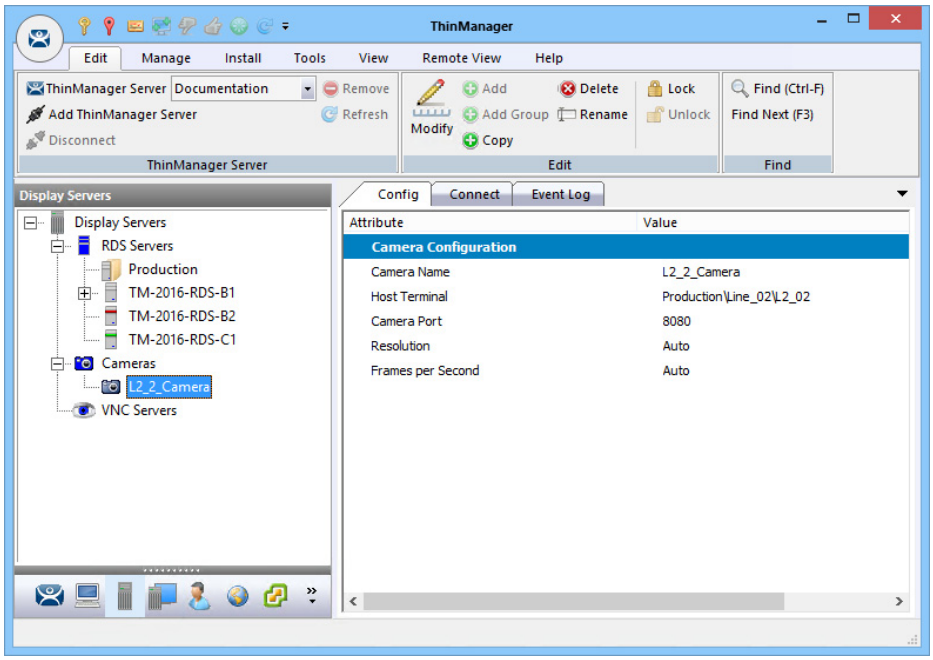
Figure 157 - Camera Authentication Page



8. Enter the administrative account Username and Password information if your USB cameras use authentication.
9. Click Finish.

   The camera appears in the Display Servers tree.

Figure 158 - Cameras in Display Servers Tree



A USB camera cannot be connected to and managed from the Connect detail pane in the ThinManager console.

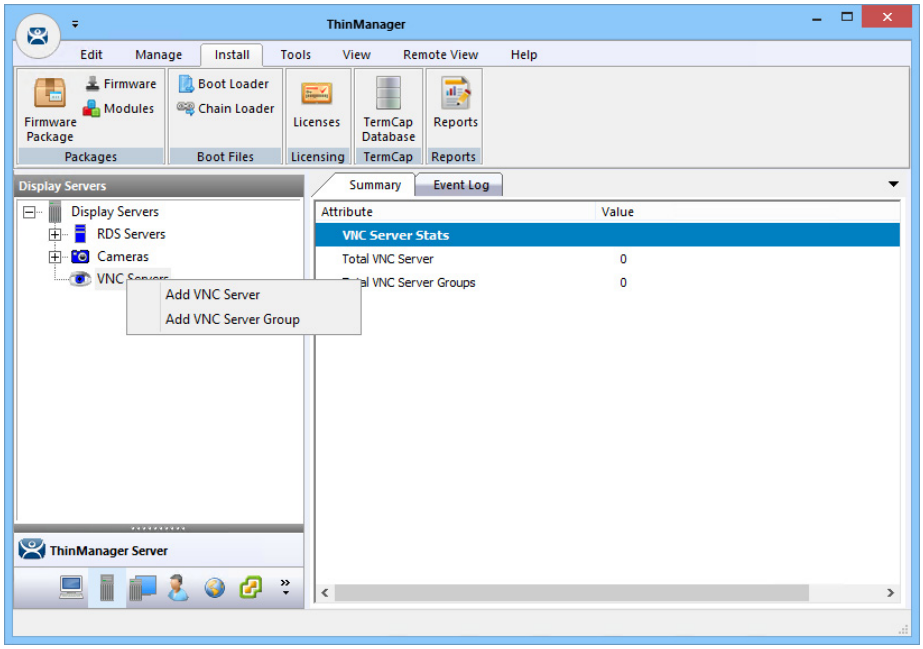
VNC Servers

ThinManager uses Virtual Network Computing (VNC) to shadow thin clients in various ways.

- From within the ThinManager Server console
- From another Terminal using a Terminal Shadow Display Client
- Through a connection to any VNC Server to shadow from the administrative console or through a display client

All of these options are useful in shadowing PanelView Plus panels.

Figure 159 - VNC Servers Branch of the Display Servers Tree



To define the VNC server, follow these steps.

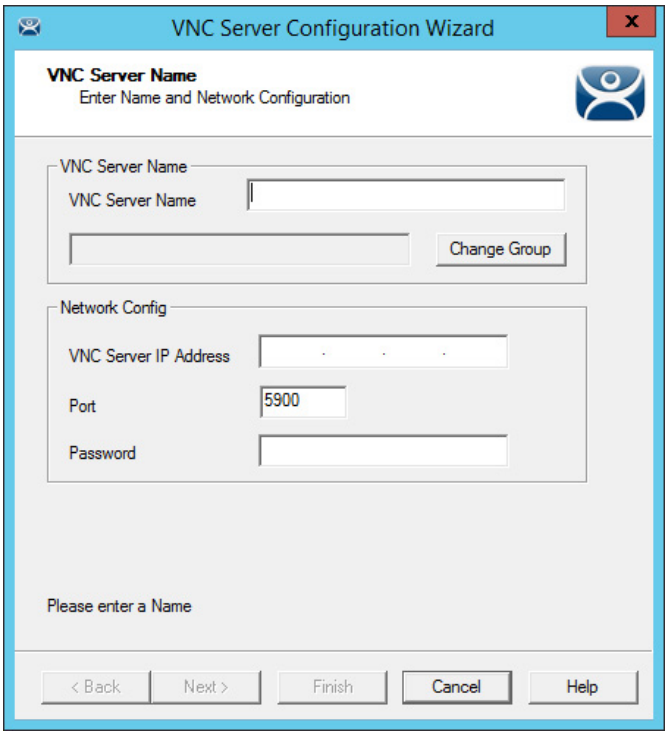
1. Click the Display Servers icon at the bottom of the ThinManager tree.

   The Display Servers tree is displayed.

2. Right-click the VNC Servers branch and choose Add VNC Server.

   The VNC Server Configuration Wizard dialog appears.

Figure 160 - VNC Server Name Page of the VNC Server Configuration Wizard



Required Settings	Description
VNC Server Name	Name of the device that is acting as the VNC server.
VNC Server IP Address	IP address of the device that is acting as the VNC server.
Port	The port that the VNC server is using. The default is 5900.
Password	Password for the VNC server, if needed.

3. Complete the fields on the VNC Server Name page.
4. Click Finish.

   You must create a VNC Display Client to deploy the VNC shadow. See VNC Shadow on page 200 for details.

Workstations

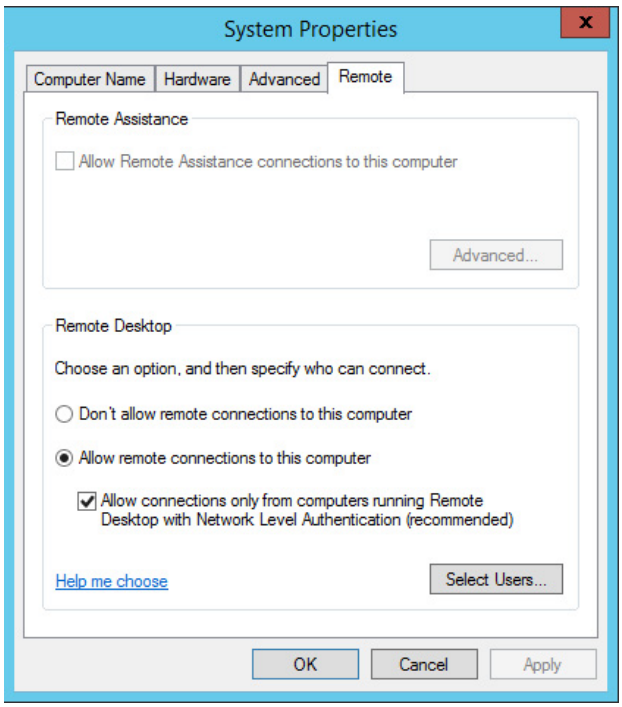
ThinManager takes advantage of Microsoft Remote Desktop Protocol (RDP) to allow you to port a workstation to a thin client. Use RDP connectivity to connect to physical or virtual workstations and transfer the desktop to another computer.

To activate the remote desktop function on the workstation, follow these steps.

1. Right-click the My Computer icon and choose Properties, or double-click the System icon in Control Panel.

The System Properties dialog appears.

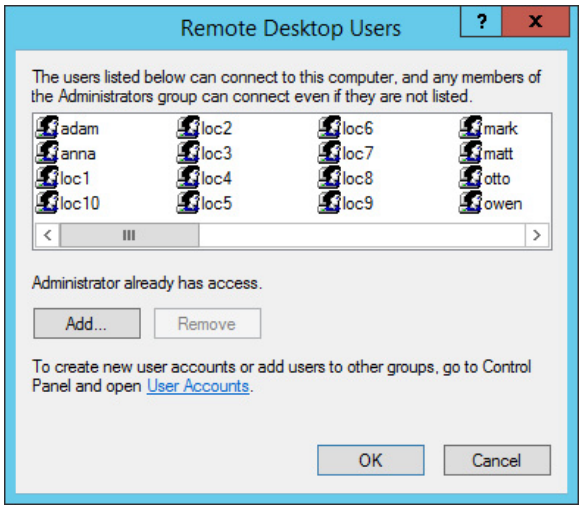
Figure 161 - Workstation System Properties



2. Under the Remote Desktop section, click Allow remote connections to this computer.
3. Click Select Users to specify which users can access the workstation.

   The Remote Desktop Users dialog appears.

Figure 162 - Remote Desktop Users



4. To grant permission to users, click Add.

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

   See Workstation Deployment on page 190 for details.

VCenter Servers

VCenter Server support is deprecated with ThinManager version 13. If a VCenter Server is configured prior to an update from an earlier version to version 13 or later, then the configuration is retained. VCenter Server configuration is not visible or available if the system is initially installed as version 13 or later, or if there is no existing configuration prior to an upgrade.

ThinManager is compatible with virtual machines, just as it is compatible with physical machines. The easiest way to handle virtual machines is to treat them as physical machines.

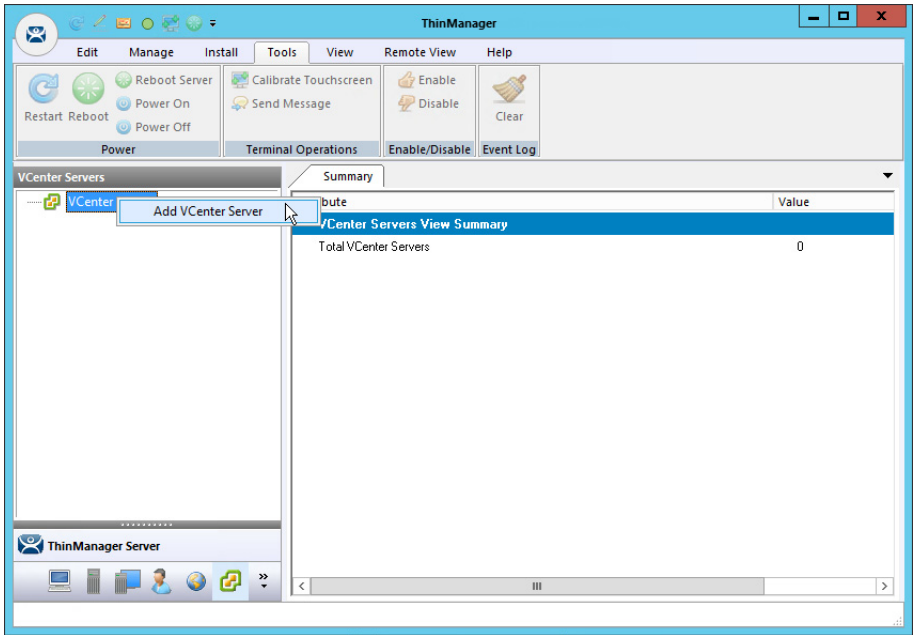
If you use VMware ESXi™, you can connect using the ThinManager interface to access several of the management features provided by VMware VCenter®.

To add a VCenter Server, follow these steps.

1. Click the VCenter Servers icon at the bottom of the ThinManager tree.

   The VCenter Servers tree appears.

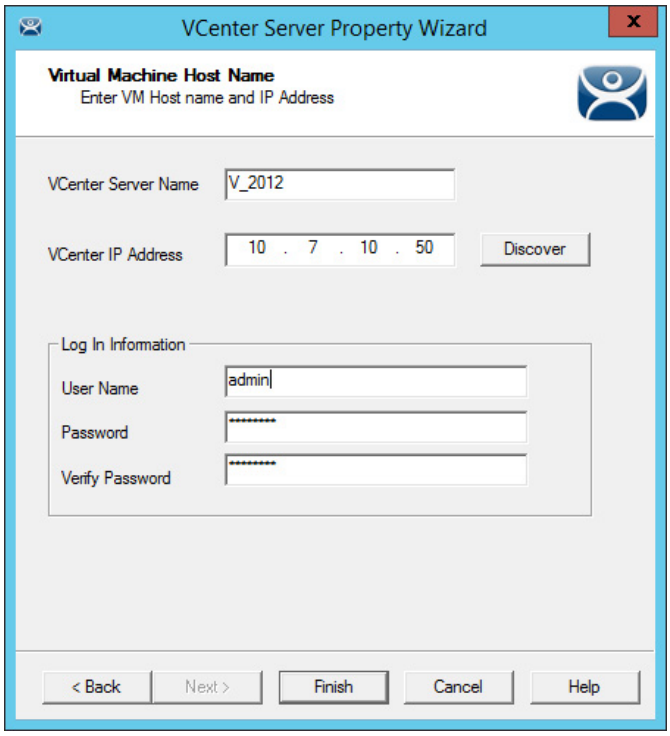
Figure 163 - VCenter Servers Tree



2. Right-click the VCenter Servers branch and choose Add VCenter Server.

   The VCenter Server Property Wizard appears.

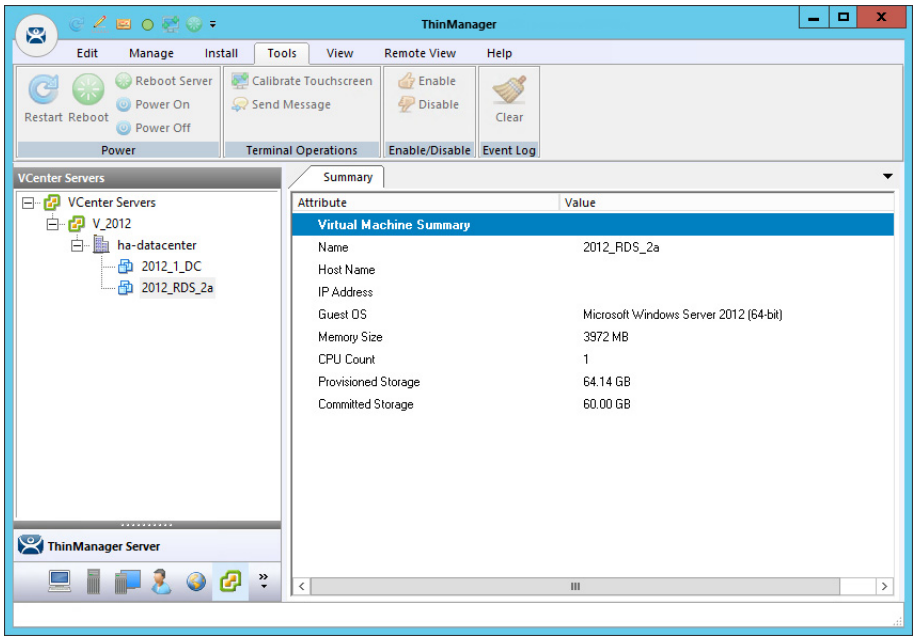
Figure 164 - VCenter Server Property Wizard



3. Complete the VCenter Server Name and VCenter IP Address fields.
4. Enter the administrative account information into the Log In Information fields.
5. Click Finish.

   After it connects and populates, highlight the newly added VCenter Server for it to appear in the Summary tab.

Figure 165 - Populated VCenter Servers Tree



6. In the VCenter Servers tree, right-click the VCenter Server for a list of the following options.

VCenter Server Function	Description
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 it
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

Snapshots

Snapshots save the state of the virtual machine in a file, which allows 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 state it was in prior to the changes.

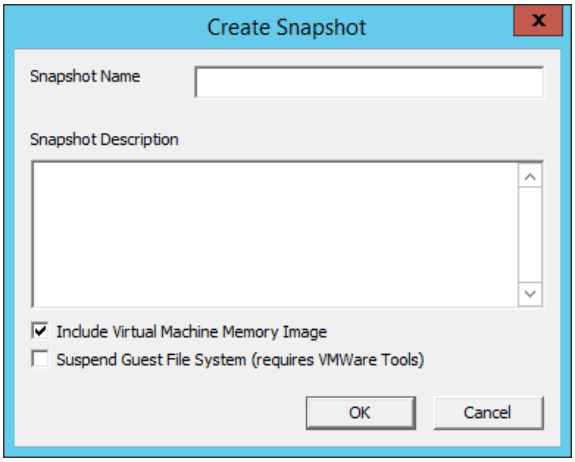
Create a Snapshot

To take a snapshot of the state of the virtual machine, follow these steps.

1. In the VCenter Servers tree, right-click the virtual machine and choose Snapshot>Take Snapshot.

   The Create Snapshot dialog appears.

Figure 166 - Create Snapshot



2. Enter the Snapshot Name and Snapshot Description.
3. Click OK to save the snapshot.

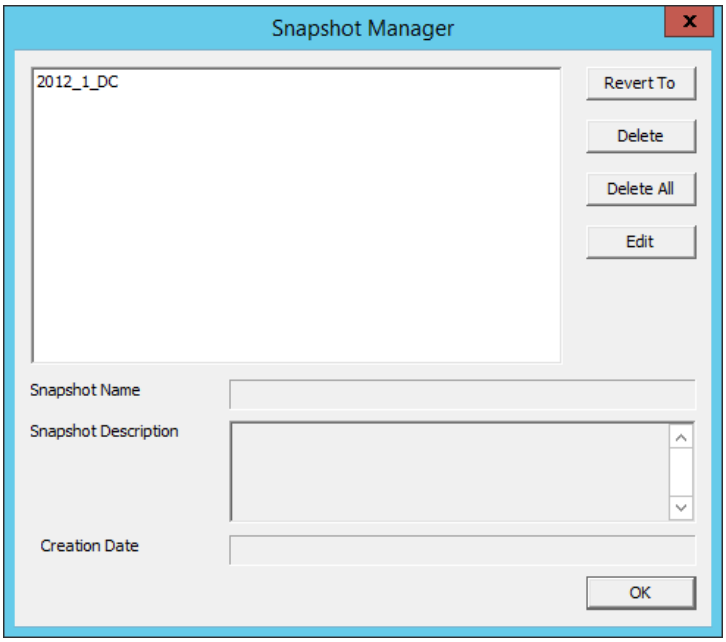
Multiple snapshots of a virtual machine can be taken.

Use a Snapshot

To make use of a snapshot, follow these steps.

1. In the VCenter Servers tree, right-click on the virtual machine and choose Snapshot>Snapshot Manager to launch the Snapshot Manager dialog box.

Figure 167 - Snapshot Manager



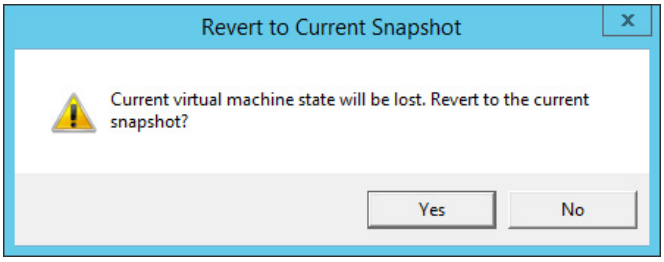
Snapshot Manager Buttons	Description
Revert To	Applies the selected saved snapshot
Delete	Deletes a highlighted snapshot
Delete All	Deletes all saved snapshots
Edit	Opens the Create Snapshot dialog to allow changes to the name and description
OK	Closes the Snapshot Manager

The Snapshot Manager dialog box displays all saved snapshots for the selected virtual machine, including the name, description, and creation date of a highlighted snapshot.

2. Click an action to take regarding a snapshot.

   A confirmation dialog box appears.

Figure 168 - Revert to Current Snapshot Warning



3. Click Yes to confirm the action.

The dialog box is dependent upon the snapshot action taken. The one shown above is only one example.

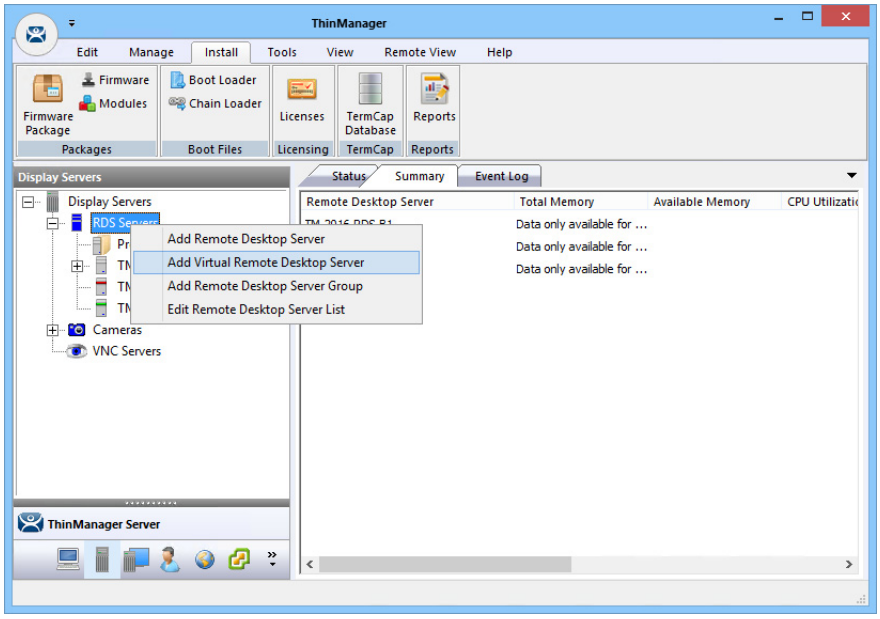
Adding a Virtual Server

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

Do define a Virtual Remote Desktop Server that resides on a VCenter Server, follow these steps.

1. Click the Display Servers icon at the bottom of the ThinManager tree to open the Display Servers tree.

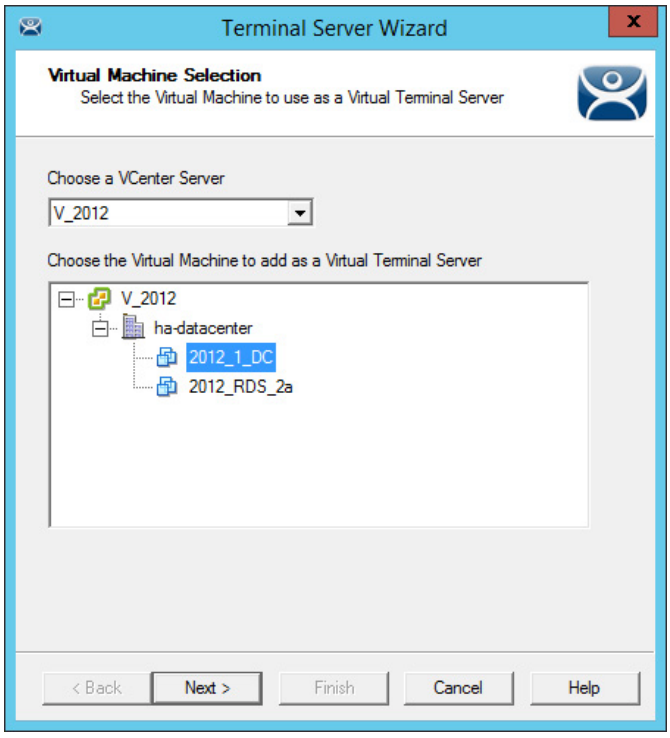
Figure 169 - Remote Desktop Servers Tree



2. Right-click the RDS Servers branch and choose Add Virtual Remote Desktop Server.

   The Virtual Machine Selection page appears.

Figure 170 - Virtual Machine Selection Page



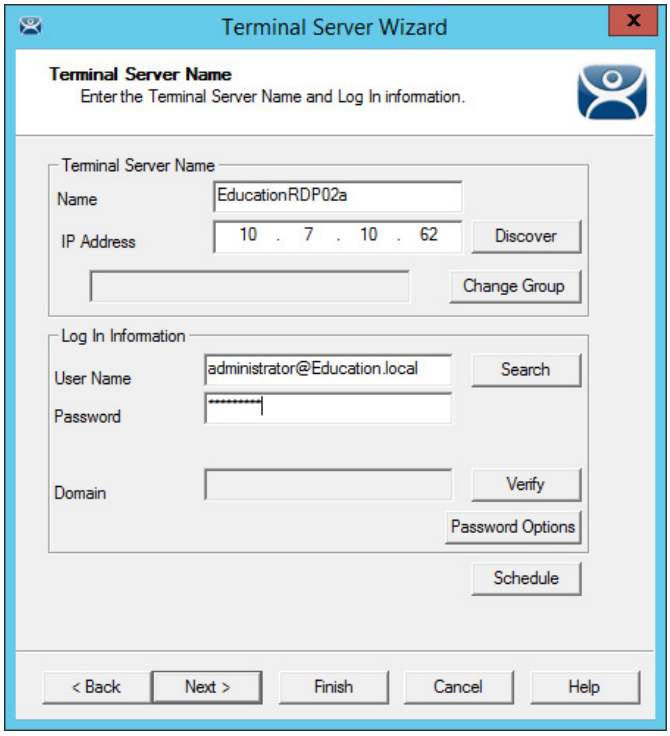
3. Choose your VCenter Server from the pull-down if you have multiple servers defined.

   The VCenter Server tree populates the selection box.

4. Choose the virtual Remote Desktop Server you want and click Next.

   The Terminal Server Name page appears.

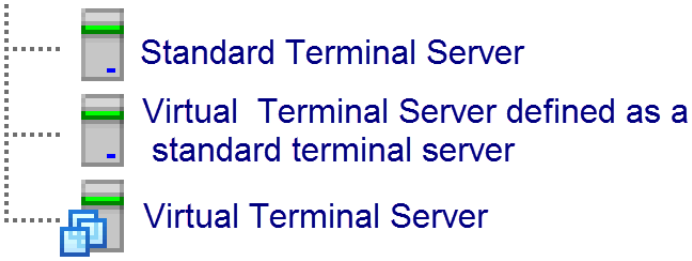
Figure 171 - Remote Desktop Server Name Page



5. Complete the Log In Information fields with the administrative account information as you do other Remote Desktop Servers. The IP address populates automatically.
6. (Optional) Click Next and check Available for Display Clients using SmartSession for load balancing.
7. Click Finish.

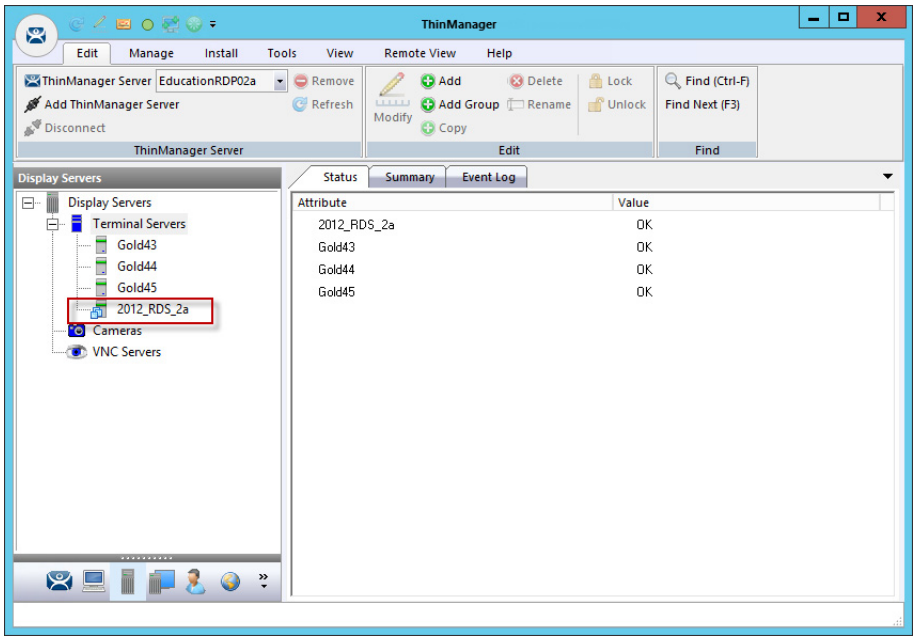
   The tree displays a different icon for a Remote Desktop Server when it is configured as a virtual Remote Desktop Server. A virtual Remote Desktop Server created as a physical Remote Desktop Server displays the same icon as a physical Remote Desktop Server.

Figure 172 - Remote Desktop Server Icons



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

Figure 173 - Display Servers Tree



Notes:

Content

Content is sent to devices through Display Clients. This chapter discusses the various display clients through which content is delivered.

Remote Desktop Services Display Clients

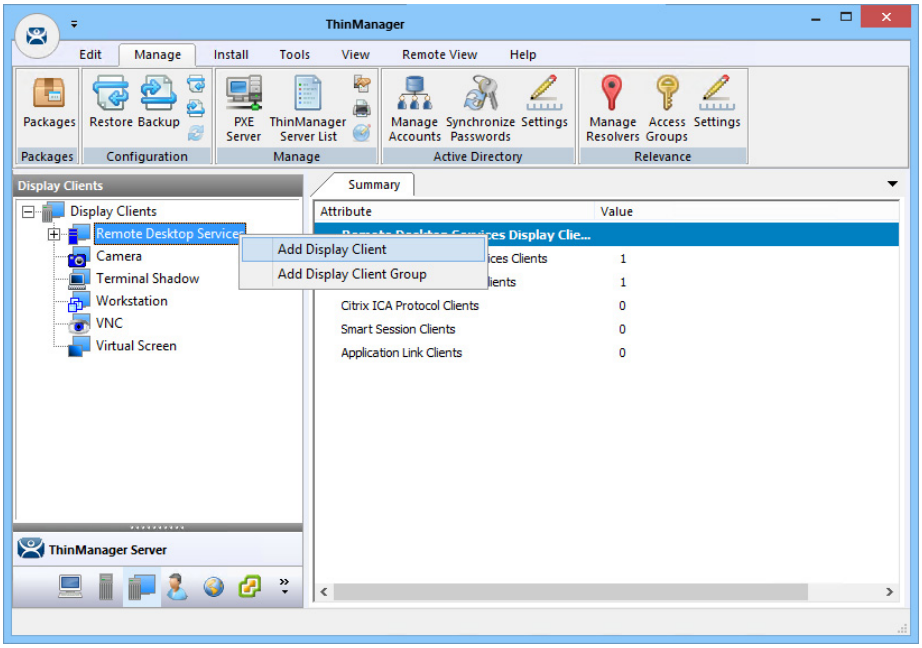
The most common content sent to a device is a Windows application. Applications are sent as Remote Desktop Services display clients. You can either give a user a full desktop, or limit them to a specific application with AppLink.

With MultiSession, ThinManager allows you to deploy several applications to a device at once. Use the Display Client Configuration Wizard to define applications.

To launch the Display Client Wizard, follow these steps.

1. Launch the Display Client Configuration wizard by selecting the Display Client icon at the bottom of the ThinManager tree.

Figure 174 - Launch the Display Client Configuration Wizard



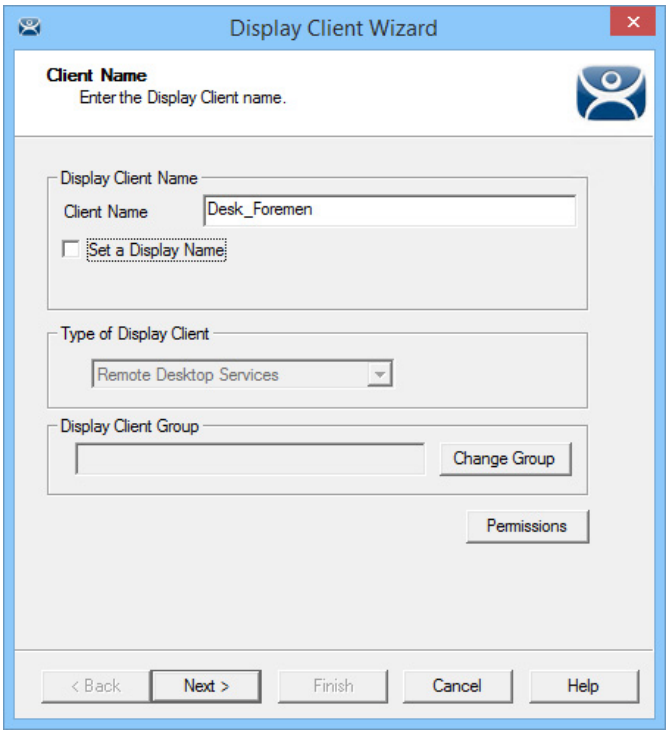
2. Right-click Remote Desktop Services, and choose Add Display Client.

   The Display Client Wizard appears.

Desktop

You can present a Desktop to a terminal for a user. The device can log in automatically with the terminal account. Alternatively, you can allow the user to log in manually so that they receive the desktop that is associated with their user account.

Figure 175 - Client Name Page of the Display Client Wizard



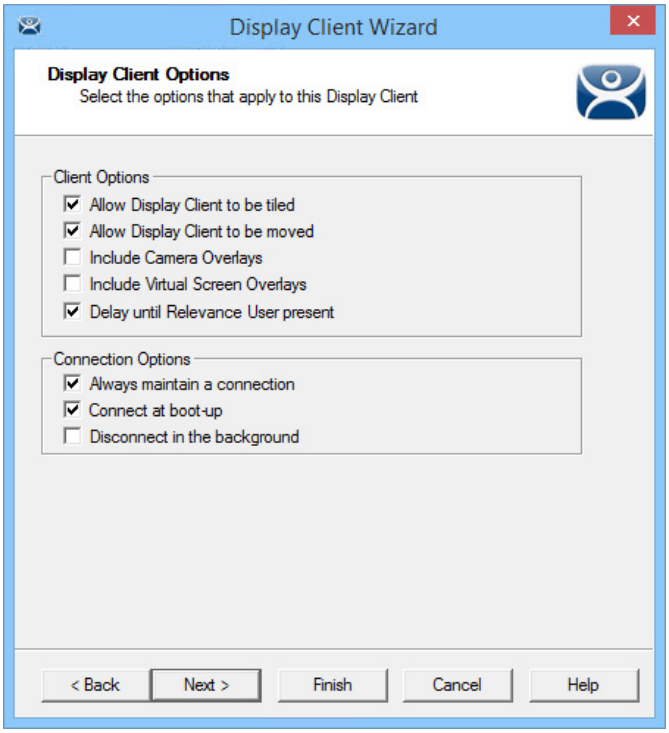
1. Enter a name for the display client in the Client Name field.

   The Type of Display Client field automatically populates when you open the Display Client Wizard as we did in the previous step. When you open the Display Client Wizard from the top-level Display Clients branch, you must choose the Type of Display Client you want from the pull-down menu.

2. Click Next.

   The Display Client Options page appears.

Figure 176 - Display Client Options Page

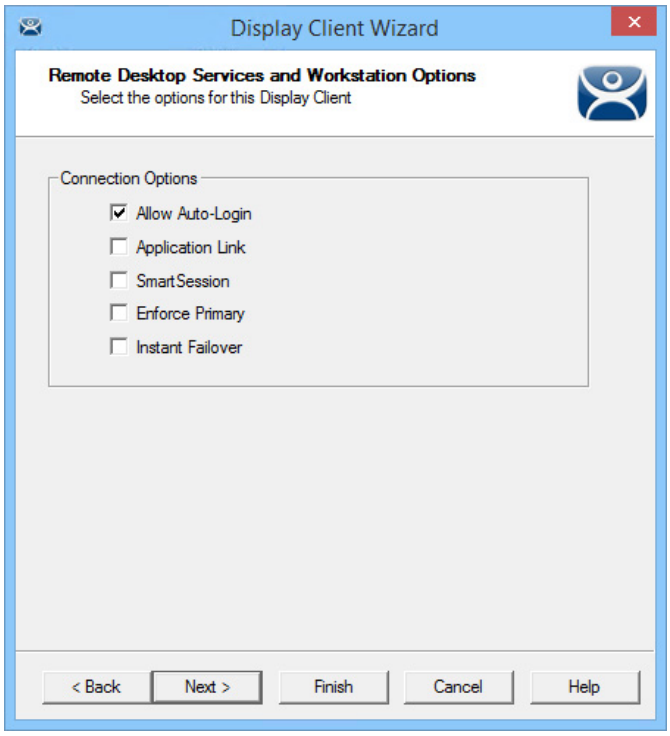


Setting	Description
Client Options	
Allow Display Client to be tiled	Allows the display client to be tiled.
Allow Display Client to be moved (MultiMonitor)	When using MultiMonitor, this setting allows the display client to be moved from screen to screen. A movable display client can be anchored with a setting on the Screen Options page of the Terminal Configuration Wizard.
Include Camera Overlays	Allows an IP camera overlay to be added to this display client.
Include Virtual Screen Overlays	Allows a display client overlay to be added to this display client. See Virtual Screens on page 205 for details.
Delay until ThinManager User present	Hides the display client until a ThinManager user logs in. When the display client launches, it uses the credentials of the ThinManager user to start the session.
Connection Options	
Always maintain a connection	Keeps a session active—it reconnects and restarts if it is closed. Clear the checkbox so the user can close a session and another session does not start automatically.
Connect at boot-up	Starts a session for the display client at boot-up. Clear the checkbox so a user action is required to start the session.
Disconnect in the background	In a MultiSession configuration, disconnects once it is moved into the background. Use to require fewer resources.

3. Check the options that apply to the Display Client and click Next.

   The Remote Desktop Services and Workstation Options page appears.

Figure 177 - Remote Desktop Services and Workstation Options Page



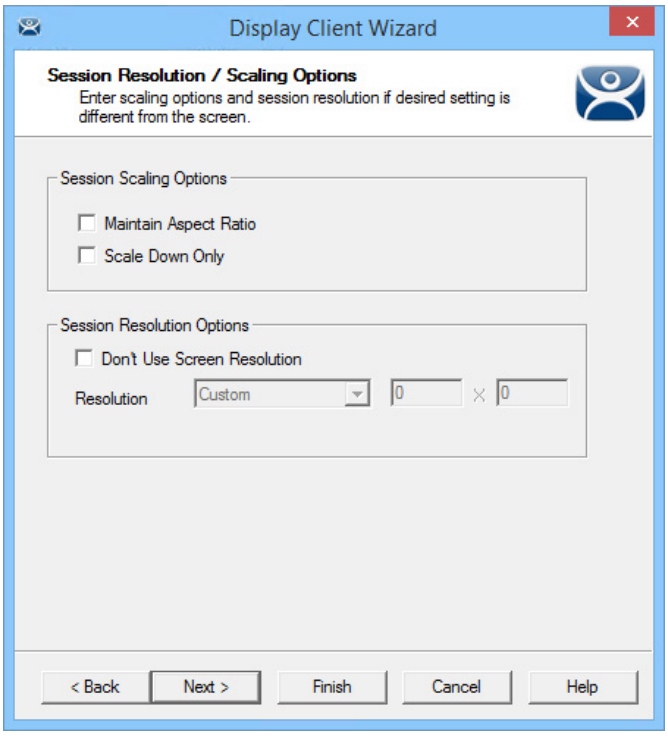
The Remote Desktop Services and Workstation Options page of the Display Client Wizard is key to Display Client configuration. These settings control how Remote Desktop Server content is deployed to the Terminal.

Setting	Description
Allow Auto-Login	Automatically logs in to the session when a user account is applied to the Terminal. Clearing this checkbox displays the login window and forces a manual login, which is useful to provide a user with a login based on their group policy.
Application Link	Launches a single application instead of a Desktop. The session lacks the Explorer shell and does not show Desktop icons or the Start menu. Close the AppLink program to end the current session and starts a new session with the application running. This setting allows the administrator to control content to the user in a simple manner without the need to use group policies. **Note**: This setting is not valid with workstations after Windows XP.
SmartSession	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	Makes a thin client reconnect to its original Remote Desktop Server if the RDS fails and recovers. Disabled when SmartSession is checked.
Instant Failover	Allows you to specify at least two Remote Desktop Servers. On startup, the Terminal connects and initiates sessions on two Remote Desktop Servers, but displays one session only. 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. With this setting, the display client looks for two active sessions; so, if one Remote Desktop Server fails, the display client starts a session on a third Remote Desktop Server if there is one in the server list.

4. (Optional) Clear the Allow Auto-Login checkbox if you want to provide the login prompt and force manual login.
5. Clear the Application Link checkbox to deploy to Desktop.
6. Click Next.

   The Session Resolution/Scaling Options page appears.

Figure 178 - Session Resolution/Scaling Options Page



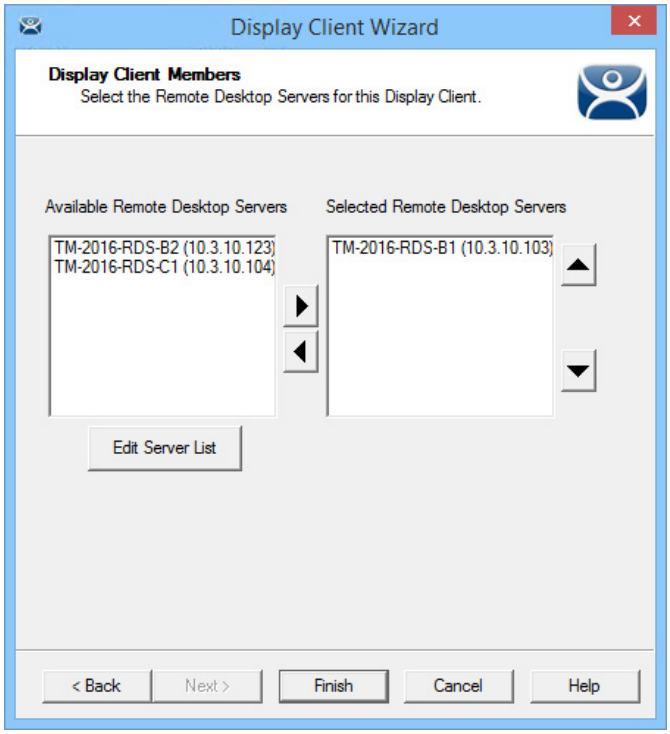
The Session Resolution/Scaling Options page sets the ability of the display client to scale the session. This page has parameters that can be configured:.

Setting	Description
Session Scaling Options	
Maintain Aspect Ratio	Keeps the aspect ratio of the session constant when scaling. With the checkbox cleared, the session fits the available display size.
Scale Down Only	Allows a session to be shrunk for a thumbnail, but does not expand it beyond the original size designation.
Screen Resolution Options	
Don't Use Screen Resolution	Overrides the session resolution and enables the Resolution settings for configuration of a new display resolution.
Resolution	Pull-down menus allow you to select a new resolution for the display when Don't Use Screen Resolution is checked.

7. Click Next.

   The Display Client Members page appears.

Figure 179 - Display Client Members Page



The Display Client Members page allows you to select the Remote Desktop Servers on which to run the application.

8. Click a server to highlight it, and use the left and right arrows to move the Remote Desktop Servers between the Available and Selected Remote Desktop Servers lists.

If your defined Remote Desktop Servers do not show in the list, it is likely you checked SmartSession on the Remote Desktop Services and Workstation Options page without checking Available for Display Clients using SmartSession on the Remote Desktop Server Capabilities page of the Remote Desktop Server Wizard.

To get your defined Remote Desktop Servers to appear in the list, follow these steps.

a. Click Edit Server List to open the Remote Desktop Server List Wizard.
b. Double-click or highlight the servers you want to appear in the list, and click Edit Server to open the Remote Desktop Server Wizard.
c. Click Next until you reach the Remote Desktop Server Capabilities page and check Available for Display Clients using SmartSession.
d. Click Finish.

Adding two Remote Desktop Servers to the Selected Remote Desktop Servers list provides failover. In normal failover, the terminal connects to the first Remote Desktop Server. If the connection fails, it connects to the second RDS.

SmartSession load balancing does not follow the list order. Instead, the terminal connects to the Remote Desktop Server with the most resources available.

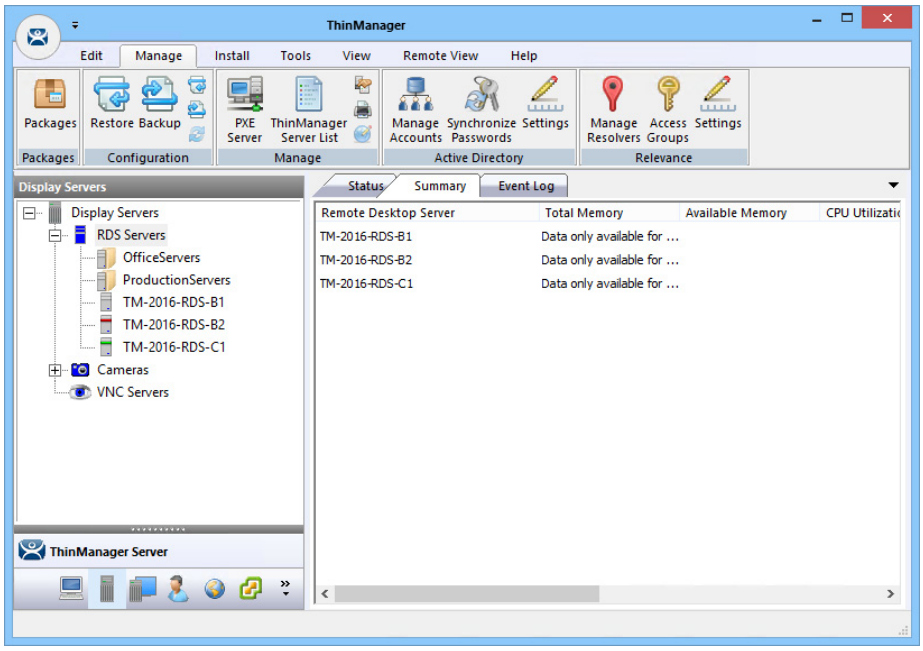
9. Click Finish.

The Display Client Wizard closes, and the new Display Client appears in the Remote Desktop Services branch Display Clients navigation pane.

Display Client Using Remote Desktop Server Groups

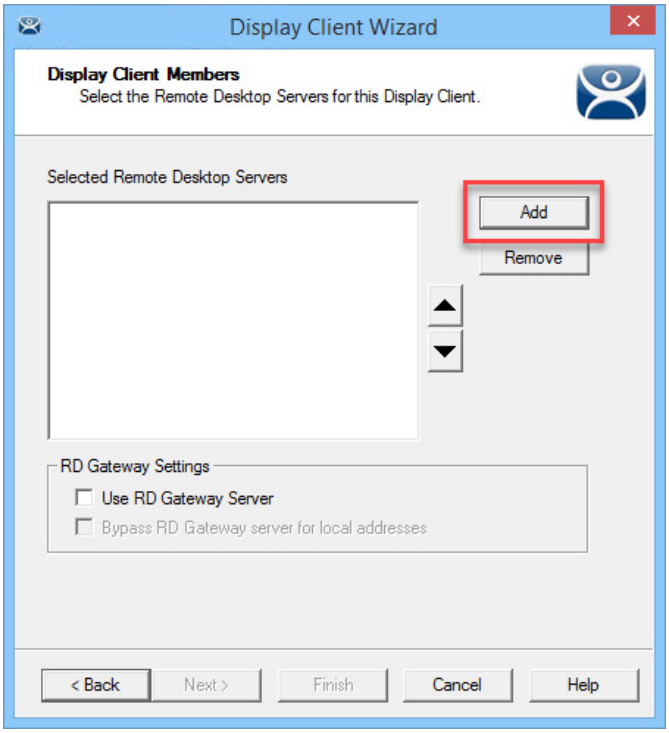
The Display Client Wizard appears differently when Remote Desktop Server Groups are used to speed selection of Remote Desktop Servers.

Figure 180 - Remote Desktop Server Groups Defined in the RDS Servers Tree



This example has two RDS Groups: OfficeServers and ProductionServers.

Figure 181 - Display Client Members Page with RDS Server Groups

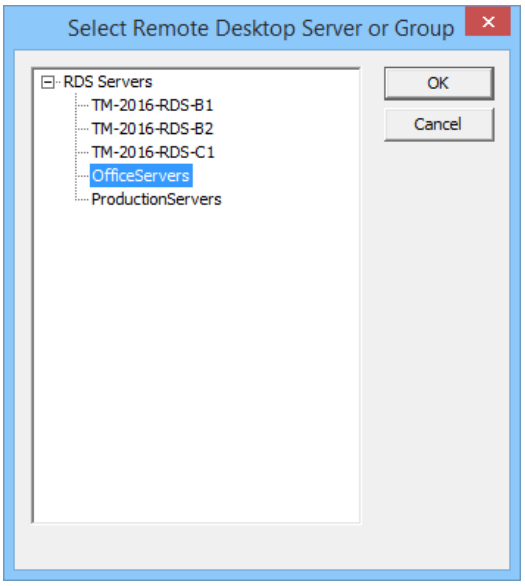


The Display Client Members page has a different format to select the Remote Desktop Servers.

1. Click Add.

The Select Remote Desktop Server or Group dialog box appears.

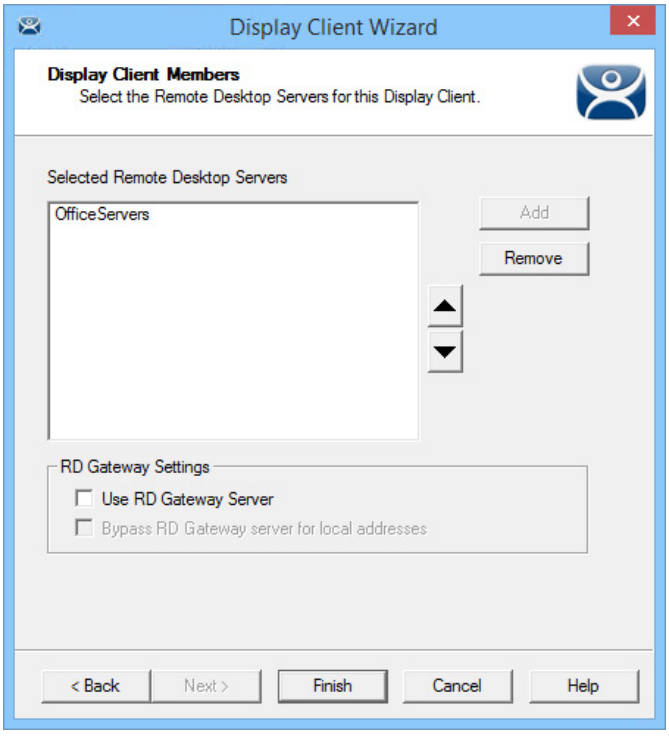
Figure 182 - Select Remote Desktop Server or Group



2. Highlight the desired RDS Group and click OK.

   The Display Client Members page appears with the desired RDS Group populated to the Selected Remote Desktop Servers field.

Figure 183 - Display Client Members Page with RDS Server Groups



Two RD Gateway Settings control the use of the Microsoft RDP Gateway.

Setting	Description
Use RD Gateway Server	Prompts the Display Client to use the Microsoft RD Gateway. See Remote Desktop Server Group on page 77.
Bypass RD Gateway server for local address	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.

3. Click Finish.

Single Application Deployment with AppLink

ThinManager uses its AppLink function to launch a single application, instead of a Desktop, which allows you to control what the user sees and interacts with.

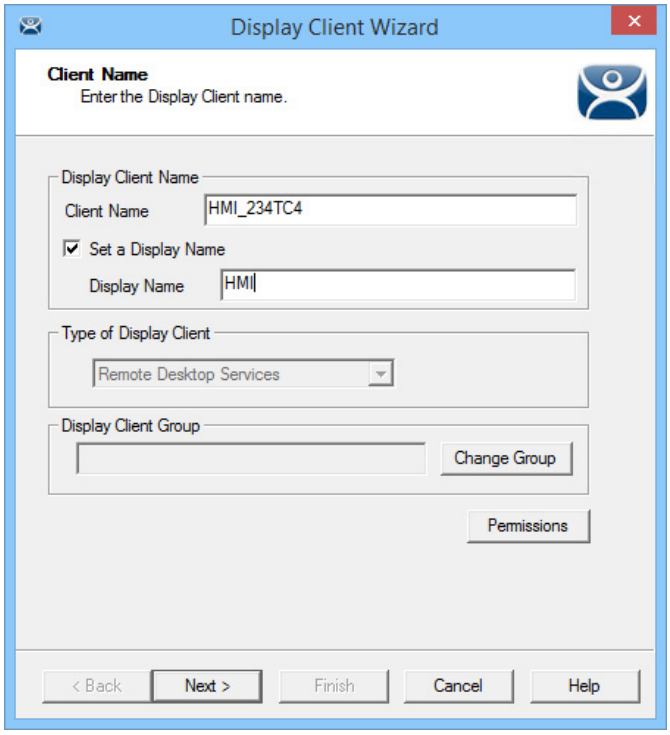
The application is launched instead of the Windows Explorer Desktop. Closing the application causes the terminal to disconnect and launch a new connection to the server with the application running.

To create a single application display client, launch the Display Client Configuration Wizard.

1. Click the Display Clients icon at the bottom of the ThinManager tree.
2. Right-click the Remote Desktop Services branch, and choose Add Display Client.

   The Client Name page of the Display Client Wizard appears.

Figure 184 - Client Name Page



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

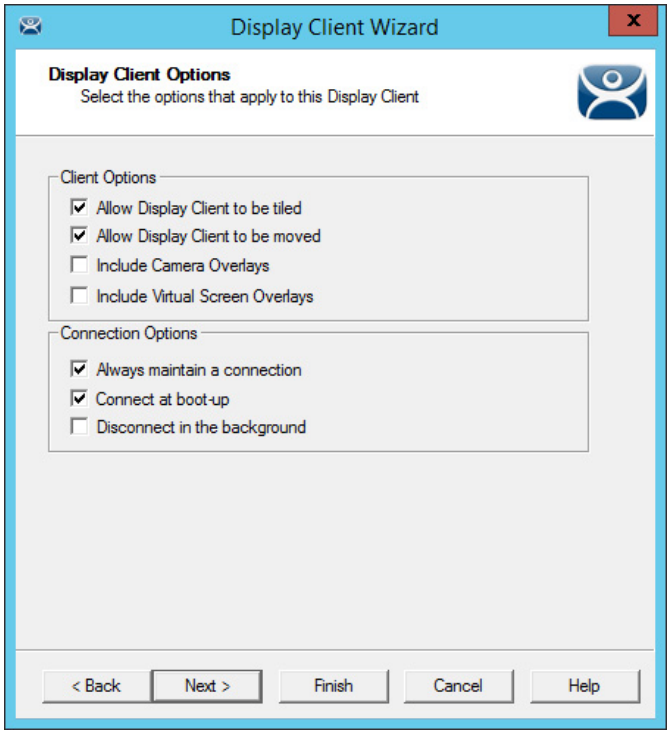
4. (Optional) Check Set a Display Name to enable the Display Name field and enter a simplified Display Client name in the tree.

The Type of Display Client is automatically chosen when you right-click the Remote Desktop Services branch. However, when you right-click the top-level Display Clients branch, you must choose the type from the Type of Display Client pull-down menu.

5. Click Next.

The Display Client Options page appears.

Figure 185 - Display Client Options Page



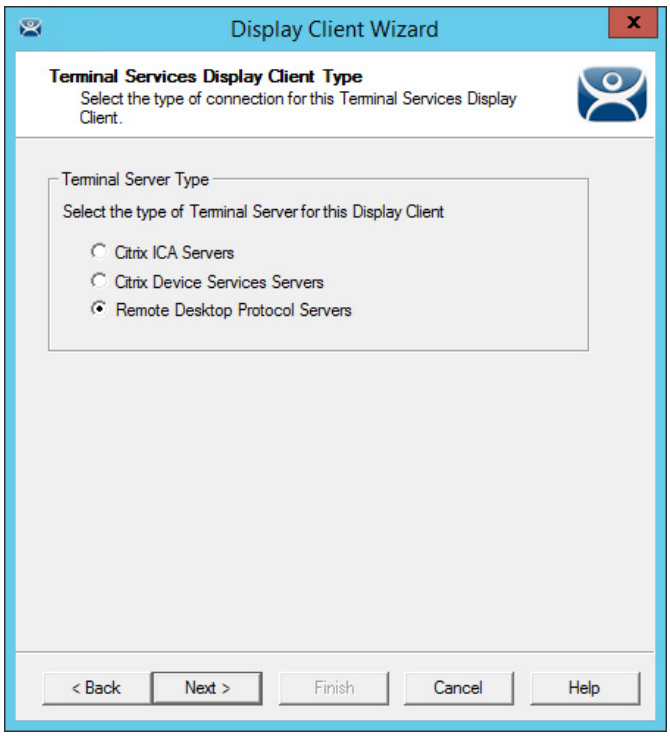
Setting	Description
Client Options	
Allow group to be tiled	Allows the Display Client Group to be tiled.
Allow Group to be moved (MultiMonitor)	Allows the Display Client to be moved from one MultiMonitor screen to another. A display client that allows it to be moved can be anchored with a setting on the Screen Options page of the Terminal Configuration Wizard.
Include IP Camera Overlays	Allows an IP Camera overlay to be added to this display client.
Include Virtual Screen Overlays	Allows a virtual screen overlay to be added to this display client. See Virtual Screens on page 205 for details.
Connection Options	
Always maintain a connection	Keeps a session active—restarts and reconnects—if it is closed. Clear this checkbox to allow the user to close a session and not have another session start automatically.
Connect at boot-up	Starts a session for this display client at boot-up. When the checkbox is clear, a user action is required to start the session.
Disconnect in background	A display client being used in a MultiSession configuration disconnects once it is moved into the background. Use this option to require fewer resources.

6. Choose the desired Client Options and click Next.

The Remote Desktop Services Display Client Type page appears.

This page is not shown unless you upgrade from a system with Citrix ICA, or you have added a registry entry as shown in Citrix Servers on page 69.

Figure 186 - Remote Desktop Services Display Client Type Page

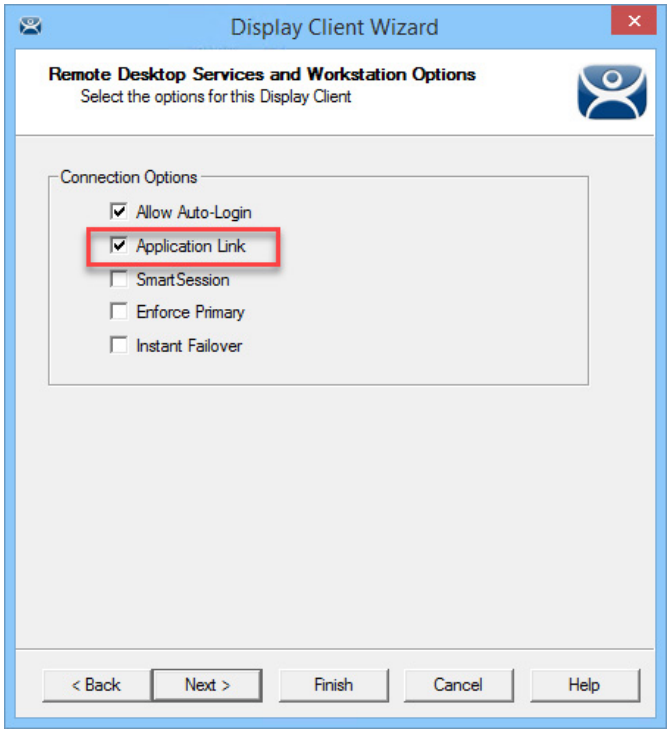


ThinManager thin clients can use the default Microsoft Remote Desktop Protocol (RDP) or Citrix ICA (Independent Computing Architecture).

7. Click the terminal server type to use with the display client and click Next.

   The Remote Desktop Services and Workstation Options page appears.

Figure 187 - Remote Desktop Services and Workstation Options



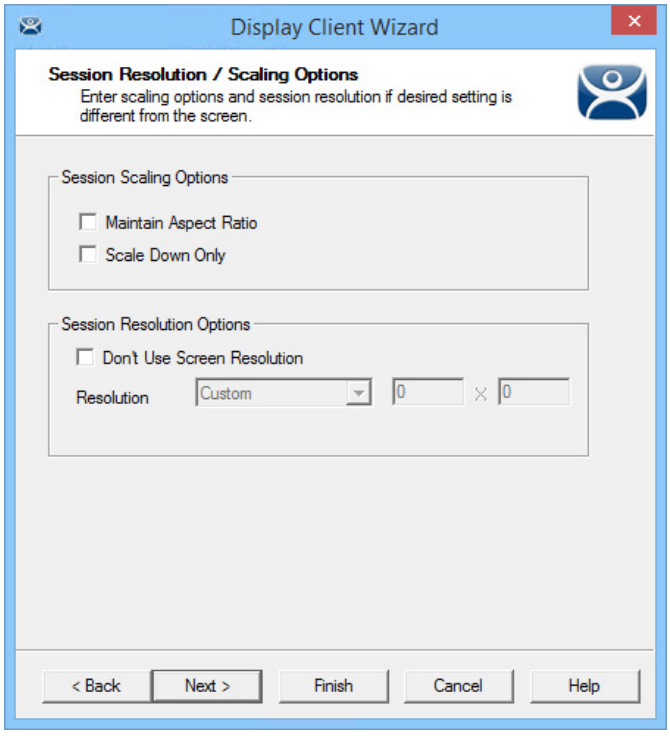
The Remote Desktop Services and Workstation Options page is the key page in Display Client configuration. These settings control how Remote Desktop Server content is deployed to the Terminal.

Connection Options	Description
Allow Auto-Login	Automatically logs in to the session if a user account is applied to the terminal, which is the typical setting. Clear this checkbox to display the log in window and force a manual login, which is useful in order 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 terminates the session and starts a new one as the application runs. This allows the administrator to control content sent to the user in a simple manner without needing to use group policies.
SmartSession	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	Tells a thin client to reconnect to its original Remote Desktop Server if that Remote Desktop Server failed and recovered. Not available when SmartSession is selected.
Instant Failover	Activates Instant Failover, in which you specify at least two Remote Desktop Servers. On boot the Terminal, it connects and starts sessions on two Remote Desktop Servers, but only displays one session. If the first Remote Desktop Server fails, the session of the second Remote Desktop Server session is immediately displayed, which eliminates any downtime due to Remote Desktop Server failure. An Instant Failover display client requires two active sessions in case one Remote Desktop Server fails, then the display client starts a session on a third Remote Desktop Server if one is in the server list. Instant Failover is free for ThinManager but requires a second application license as two active sessions are running the application.

8. Check Application Link to deploy a single AppLink application.
9. (Optional) Clear the Allow Auto-Login checkbox to provide the log in prompt and force manual login.
10. Click Next.

    The Session Resolution/Scaling Options page appears.

Figure 188 - Session Resolution/Scaling Options Page



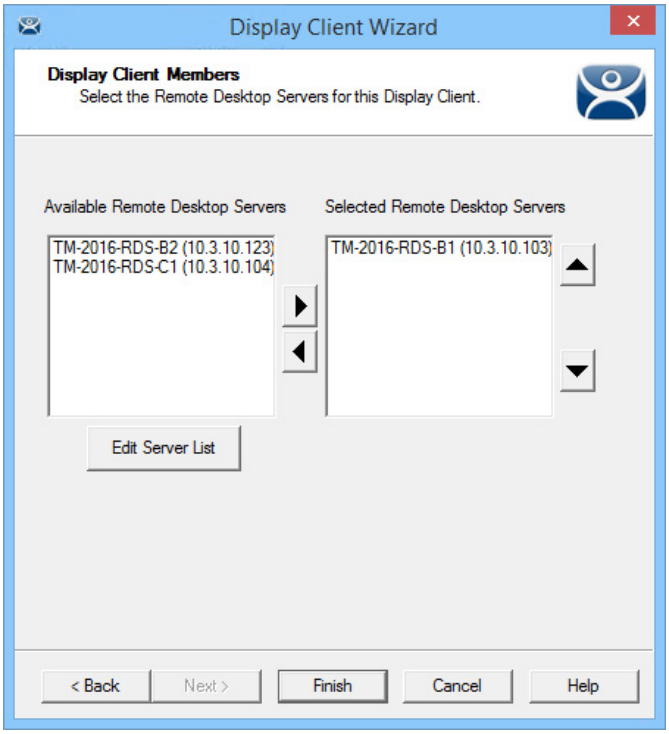
The Session Resolution/Scaling Options page sets the ability of the display client to scale the session. This page has parameters that can be configured.

Options	Description
Session Scaling Options	
Maintain Aspect Ratio	Keeps the aspect ratio of the session constant when scaling. Clear the checkbox for the session to fit the available display size.
Scale Down Only	Allows a session to be shrunk for a thumbnail, but does not expand it beyond the original size designation.
Screen Resolution Options	
Don't Use Screen Resolution	Allows for override of the session resolution and to set a new resolution for the display.
Resolution	Allows you to select a new resolution for the display when Don't Use Screen Resolution is checked.

11. Click Next.

    The Display Client Members page appears.

Figure 189 - Display Clients Members Page



The Display Client Members page of the Display Client Wizard allows the selection of Remote Desktop Servers on which you want the application.

12. Highlight the Remote Desktop Servers you want to use in the Available Remote Desktop Servers list and click the right arrow to move them to the Selected Remote Desktop Servers list.

If your defined Remote Desktop Servers do not appear in the Available Remote Desktop Servers list, it is likely you checked SmartSession on the Remote Desktop Services and Workstation Options page without checking Available for Display Clients using SmartSession on the Remote Desktop Server Capabilities page of the Remote Desktop Server Wizard.

To get your defined Remote Desktop Servers to appear in the list, follow these steps.

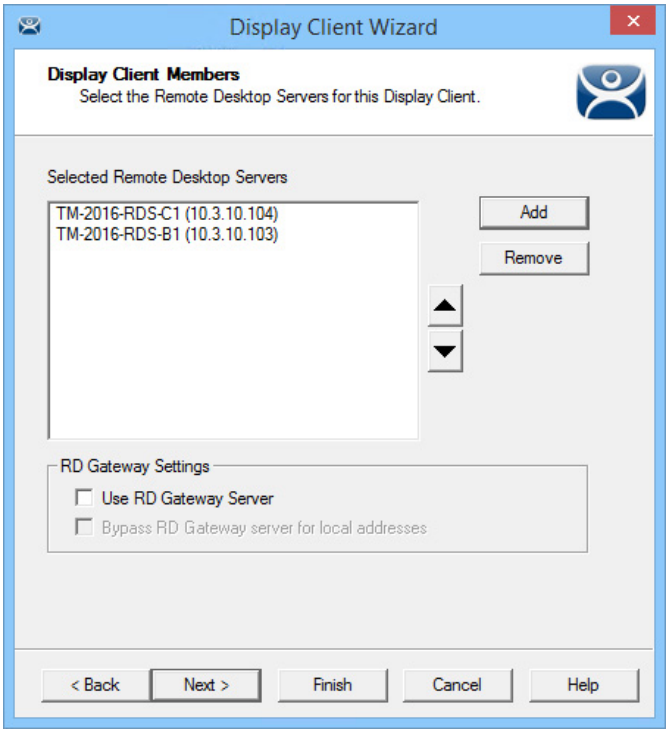
a. Click Edit Server List to open the Remote Desktop Server List Wizard.
b. Double-click or highlight the servers you want to appear in the list, and click Edit Server to open the Remote Desktop Server Wizard.
c. Click Next until you reach the Remote Desktop Server Capabilities page and check Available for Display Clients using SmartSession.
d. Click Finish.

Adding two Remote Desktop Servers to the Selected Remote Desktop Servers list provides failover. In normal failover, the terminal connects to the first Remote Desktop Server. If that fails, it connects to the second.

SmartSession load balancing does not follow the list order. Instead, the terminal connects to the Remote Desktop Server with the lightest load.

Alternatively, if Remote Desktop Server Groups are used to speed the selection of Remote Desktop Servers, then the Display Client Members page displays the Selected Remote Desktop Servers list only.

Figure 190 - Display Client Members Page



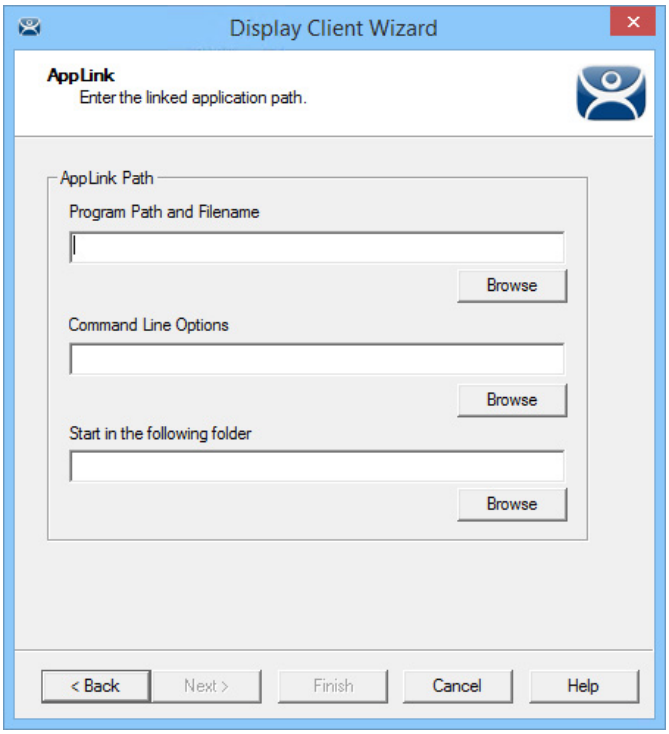
a. Click Add.

The Select Remote Desktop Server or Group dialog box appears.

b. Choose the Remote Desktop Servers or Groups and click OK.
c. Click Next.

The AppLink page appears.

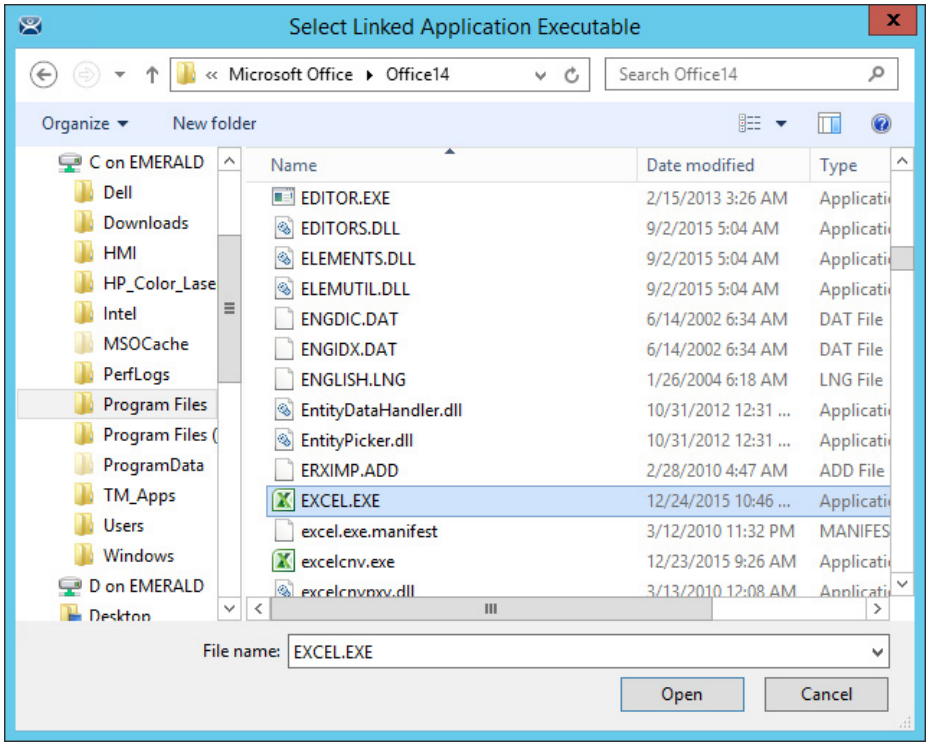
Figure 191 - AppLink Page



The AppLink Page contains a field for the path to the executable to launch the desired application.

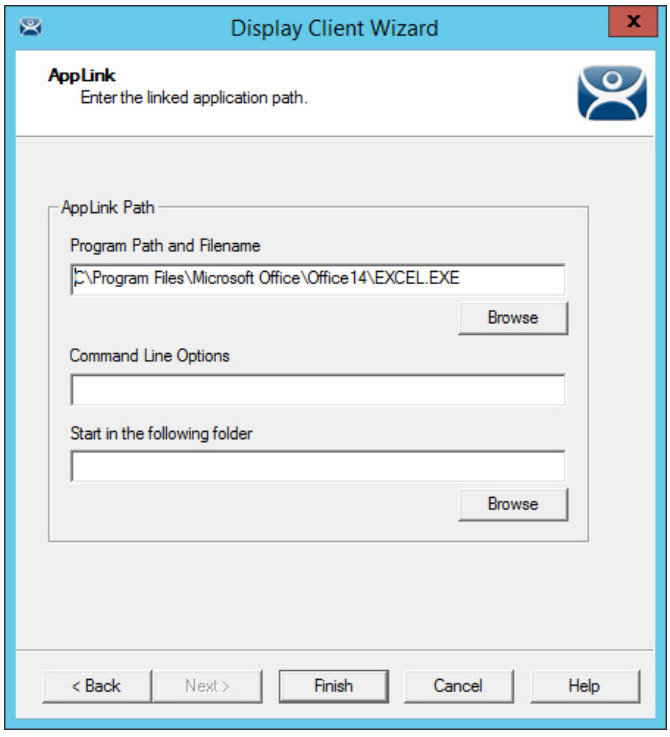
13. Enter the path to the application in the Program Path and Filename field, or click Browse, which launches a file browser.

Figure 192 - File Browser



a. If browsing to the file location, click Open to populate the Program Path and Filename field.

Figure 193 - Filled Program Path and Filename Field



14. Click Finish to complete the wizard and save the configuration.

Here are a few considerations for when you enter 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.

Create a batch file in the same location on each Remote Desktop Server. The batch file can be as simple as 3 lines, as follows.

```
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.

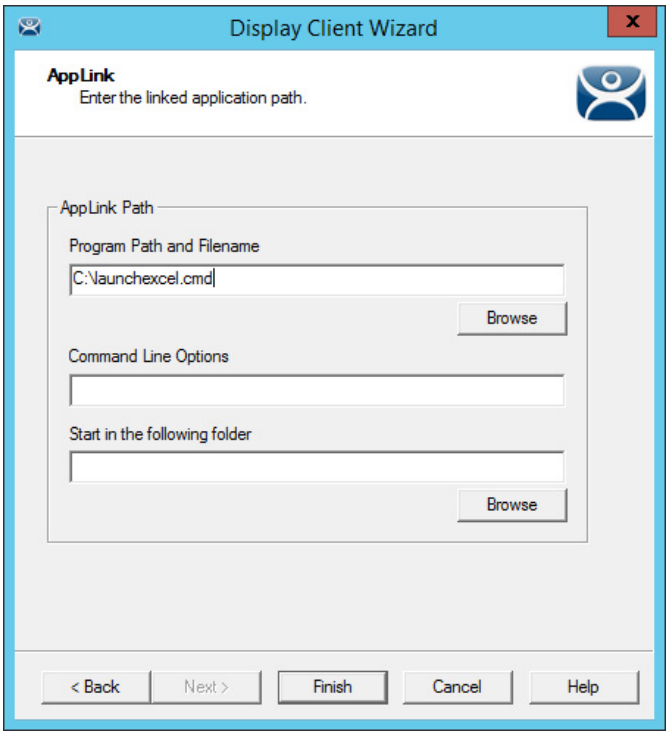
```
CD "C:\Program Files (x86)\Microsoft
Office\Office14"

Start EXCEL.EXE

CD\
```

This first line uses 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 is directed to the batch file.

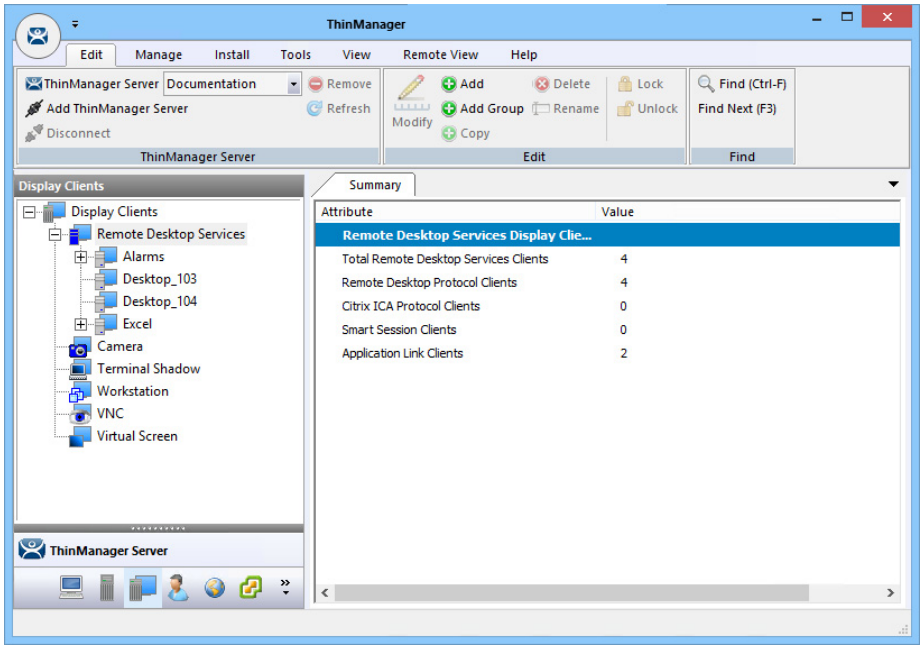
The batch file directs the terminal to the right location.

Figure 194 - Batch File as the Program Path



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

Figure 195 - Created Display Clients in ThinManager Tree



Once you have created a display client, it appears in the Display Clients branch of the ThinManager tree.

Connection Options

Remote Desktop Services Display Clients have a variety of Connection Options, which are controlled on the Remote Desktop Services and Workstation Options page of the Display Client Wizard.

Figure 196 - Remote Desktop Services and Workstation Options Page

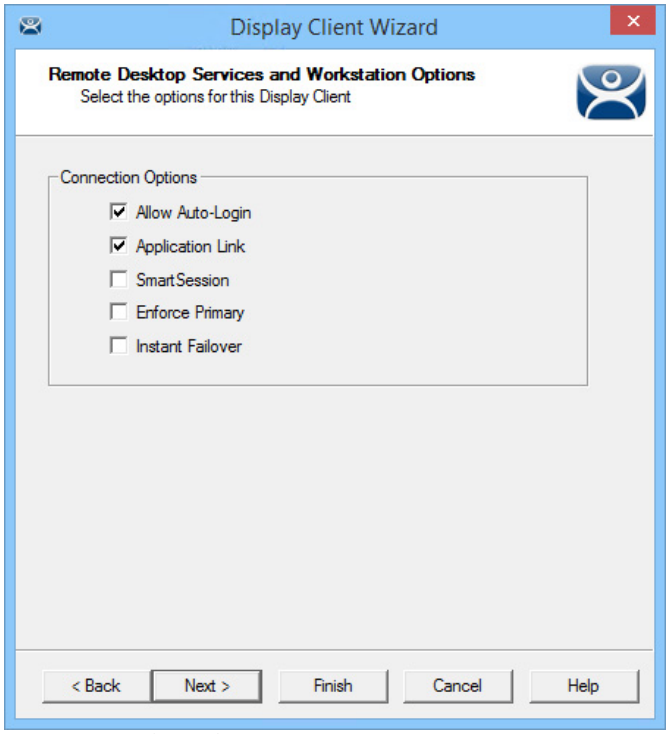


Table 1 - Connection Options

Connection Options	Description
Allow Auto-Login	Automatically logs in to the session if a user account is applied to the terminal, which is important for instant failover so that the backup session is immediately displayed without user intervention. This is the default setting. Clearing this checkbox displays the login window and forces a manual login, which 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 icons or a Start menu, which allows you to control a user's access. Closing the AppLink program ends the current session and starts a new session with the application running, which allows the administrator to control content to the user in a simple manner without needing to use group policies.
SmartSession	Adds SmartSession to the display client, which provides load balancing between member Remote Desktop Servers.
Enforce Primary	Causes a thin client to reconnect to its original Remote Desktop Server if that Remote Desktop Server fails and recovers. Thin Manager uses a list of assigned Remote Desktop Servers to which the terminal can connect. The top RDS is considered primary. Not available when SmartSession is selected.
Instant Failover	Allows you to specify at least two Remote Desktop Servers. On startup, the terminal connects and initiates sessions on two Remote Desktop Servers, but displays one session only. If the first Remote Desktop Server fails, the session of the second Remote Desktop Server session is displayed immediately, which eliminates any downtime due to Remote Desktop Server failure. With this setting, the display client looks for two active sessions; so, if one Remote Desktop Server fails, the display client starts a session on a third Remote Desktop Server if there is one in the server list.

1. Check the desired connection options and click Next.

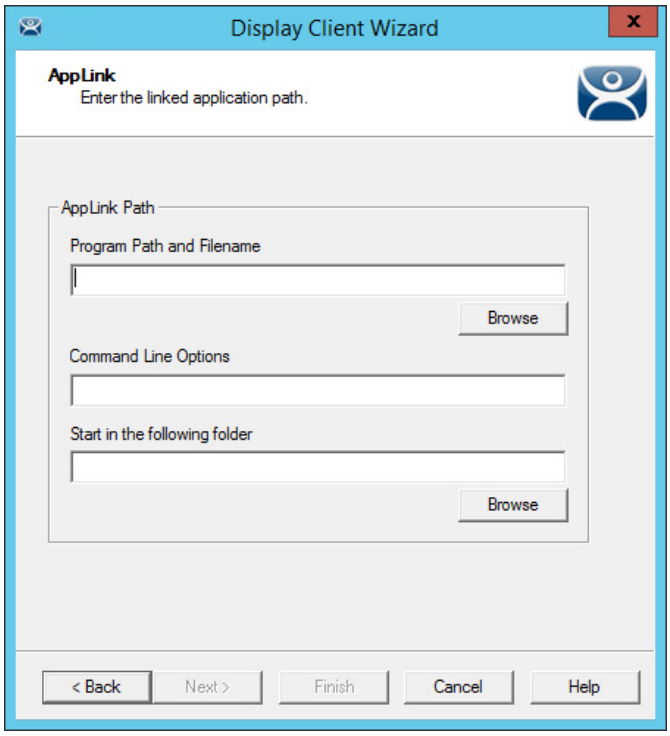
Allow Auto-Login

See the description of this connection option in Table 1.

Application Link (AppLink)

The following is information additional to the Deployment Option descriptions regarding Application Link in Table 1 on page 151.

Figure 197 - AppLink Page



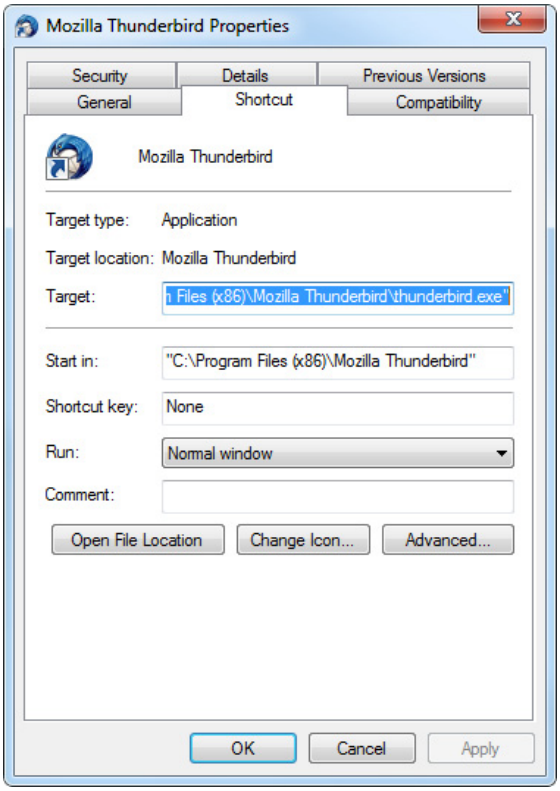
1. Complete the required fields on the AppLink page.

Field	Description
Program Path and Filename	Enter the path to the desired application in the field, or click Browse to navigate to the executable file using a browser.(1) (2)
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 order to specify the working directory for the program when using a relative path for the initial program. Click Browse to navigate to the executable file using a browser.(2) This field may not be required.

(1) Double-quotation marks may be needed when there is a space in the path.

(2) 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.

Figure 198 - 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 field contains the path to the executable. The Start in field contains the home directory for the application.

Figure 199 - AppLink Path

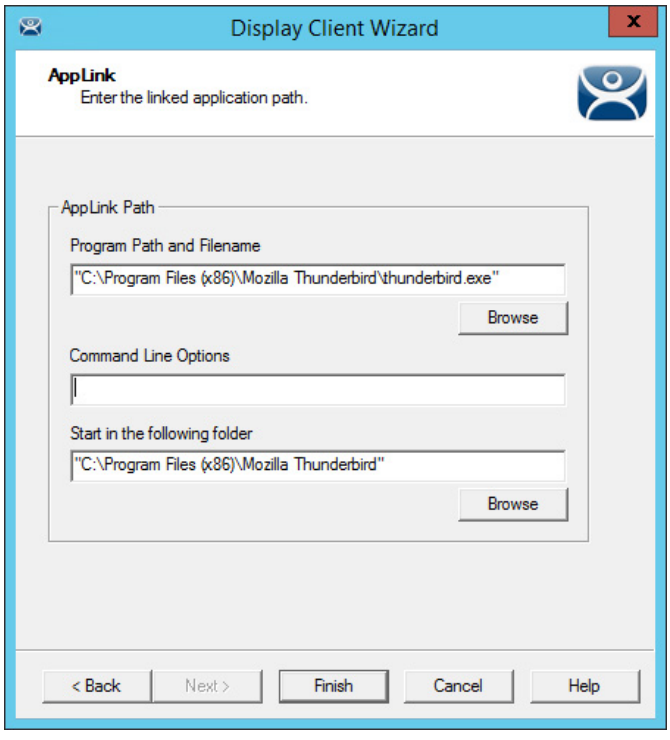


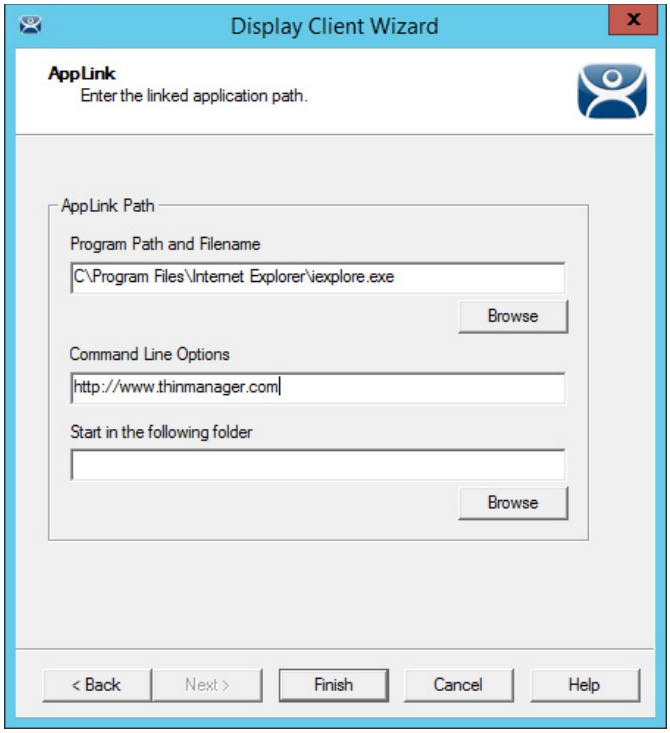
Figure 199 shows how the path data from the shortcut is used in AppLink.

The Target field from Figure 198 is equivalent to the Program Path and Filename field in Figure 199.

The Start in field in Figure 198 is equivalent to the Start in the following folder field in Figure 199.

Usually, the Start in the following folder is not needed.

Figure 200 - Website Deployment



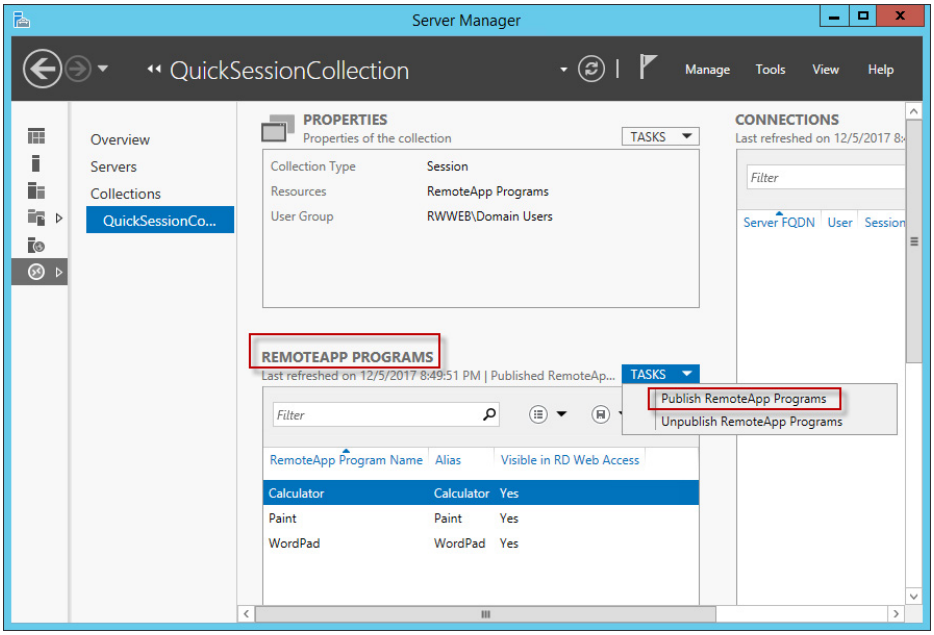
a. To launch a browser, include the URL of the desired site in the Command Line Options field.

Windows Server 2008, 2012, and 2016 need the AppLink path to be on the allow list in the Server Manager>Collections>RemoteApp Programs of the Remote Desktop Server.

Alternatively, follow these steps to configure the group policy to allow any initial program.

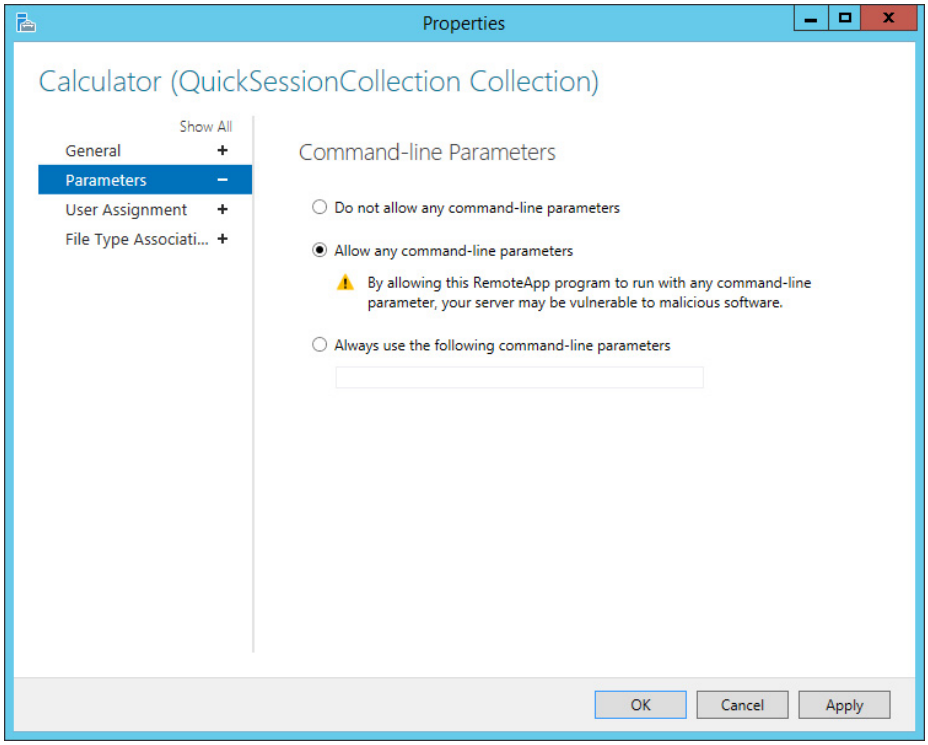
a. Open the Group Policy.
b. Navigate to Computer Configuration>Administrative Templates>Windows Components>Remote Desktop Services>Remote Desktop Session Host>Connections.
c. Set the Restrict Remote Desktop Services user to a single Remote Desktop Services session parameter to Enabled.

Figure 201 - RemoteApp Programs Allow List



2. Include the application in your allow list by using the Publish RemoteApp Programs task.
3. Once the application is published, right-click the application in your allow list to open the properties.

Figure 202 - Allow Any Command-line Parameters Setting

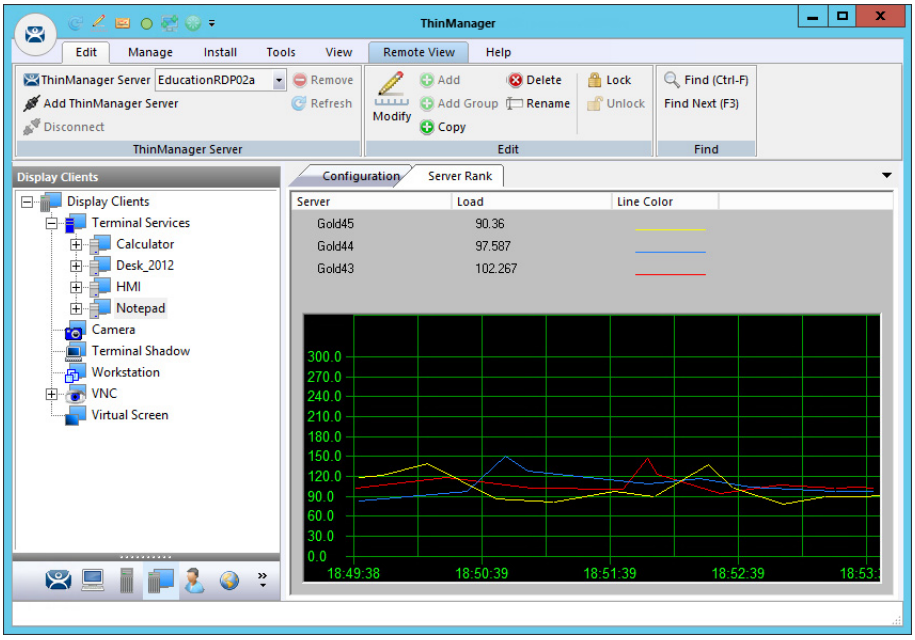


4. Under Command-line Parameters, click Allow any command-line parameters, which lets you pass specific files or URLs to the display client.
5. Click Apply and then OK.

SmartSession

The SmartSession Configuration page allows for the adjustment of SmartSession values by adjusting the weights of SmartSession settings. ThinManager multiplies the CPU utilization, memory (RAM) utilization, and number of sessions on the Remote Desktop Server by the weight shown to define the SmartSession Remote Desktop Server's available resources. The higher the weight value for a parameter, the greater importance that parameter has in the load determination for SmartSession.

Figure 203 - SmartSession Load Balancing Graph



ThinManager uses the following formula to calculate SmartSession load balancing.

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

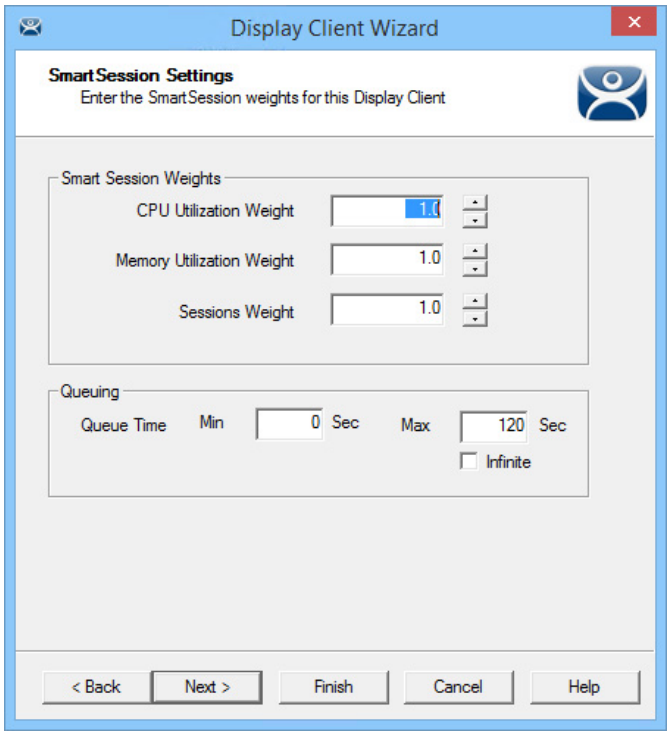
The load = (CPU weight x the CPU Use%) + (Memory weight x Memory Use%) + (Session weight x Session Number%)

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

SmartSession Weights

The Weight of the SmartSession parameter—processor, memory, or sessions—can be adjusted to make it a larger influence in the final calculation in total SmartSession load. The Weights can be changed on the SmartSession Settings page of the Display Client Wizard.

Figure 204 - SmartSession Settings Page of the Display Client Wizard



Field	Description
CPU Utilization Weight	The CPU mulitplier.
Memory Utilization Weight	The Memory multiplier.
Session Weight	The Session multiplier.
Queue Time Min (s)	Time a terminal waits in the queue before being sent to a Remote Desktop Server that has another terminal connecting. The terminal may wait longer than this value to connect if the CPU of the Remote Desktop Server exceeds the Maximum CPU Utilization defined on the SmartSession Configuration page of the Remote Desktop Server Configuration wizard.
Queue Time Max (s)	Maximum time a terminal waits in the queue before being sent to the Remote Desktop Server to log in regardless of the load.
Infinite	When checked, ThinManager waits until the CPU utilization of the Remote Desktop Server regains an acceptable range before sending other terminals to it to log in.

The SmartSessions Settings page only appears before the AppLink page if SmartSession is checked on the Remote Desktop Services and Workstation Options page, see Figure 196. The SmartSession Settings page allows you to change the weight of each SmartSession load balancing component.

Increasing the weight of one of the components increases its value and makes it more sensitive to overload of that resource. For example, if 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.

SmartSession Ranges

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

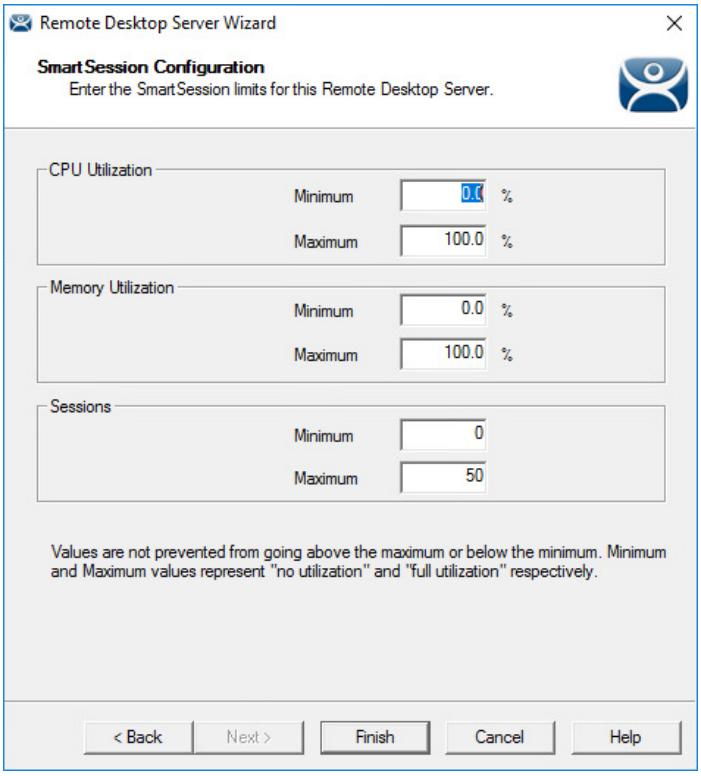
To open the Remote Desktop Server Wizard and adjust ranges, follow these steps.

1. Double-click the desired server on the Remote Desktop Servers branch of the Display Servers tree.

   The Remote Desktop Server Wizard appears.

2. In the Remote Desktop Server Wizard, click Next until the SmartSession Configuration page appears.

Figure 205 - SmartSession Configuration Page



Field	Description
CPU Utilization	The percentage of CPU usage on the Remote Desktop Server.
Memory Utilization	The percentage of Memory usage on the Remote Desktop Server.
Sessions	The number of sessions on a Remote Desktop Server.
Minimum	The value that ThinManager uses as the starting point of the load. A value below the Minimum is considered to be unused.
Maximum	The value that ThinManager considers the parameter as reaching 100% utilized and is unavailable.

Each resource that ThinManager measures for SmartSession load balancing has an adjustable range. The CPU Utilization and the Memory Utilization fields use a scale of 0...100%. The Sessions resource is based on 50 sessions, where 0 sessions is 0%, 25 sessions is 50%, and 50 sessions is 100% utilization.

If you are concerned about using all your resources on a server, you can lower the Maximum setting. For example, if you change the Sessions Maximum to 25, that means 25 sessions is 100% utilization, and ThinManager considers the server less available. Likewise, if you change the CPU Utilization Maximum to 75%, that tells ThinManager that the server is loaded at 75% CPU utilization, which leaves some spare CPU available.

These numbers can be left at the default settings unless you notice a performance problem. The Weights or Ranges can be adjusted through trial and error to determine the best performance.

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

3. Set the Minimum and Maximum values accordingly, and click Finish.

Queuing

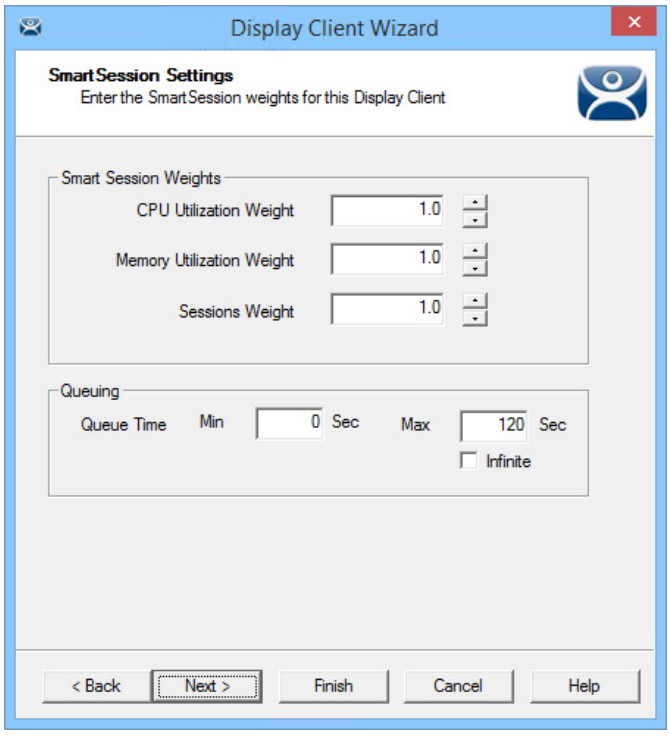
During failover, Queuing smooths the transition from one server to another.

At startup, a session usually requires more resources to initialize than it needs to run. If a server fails and all of its terminals switch to a back-up server, the many session startups may overload and strain the new server. This scenario is especially true with HMIs, SCADAs, and other applications that demand resources.

When a terminal first starts an application that uses SmartSession, ThinManager checks the resources of the member servers and sends the terminal to the server with the lightest load—the one with the most available resources.

Queuing acts like an intelligent bottleneck. When ThinManager detects all the servers have depleted their resources, it waits until the loads drop and resources become available before the server assignments are given to the terminals. Without Queuing, the terminals switch immediately, which places a demand on the system that greatly slows performance until all the sessions initialize and reach stable load levels.

Figure 206 - SmartSession Settings Page of the Display Client Wizard



Queuing is automatically applied to SmartSession Display Clients. The default settings provide a minimum wait time of 0 seconds and let terminals connect after 120 seconds even if the load does not decrease.

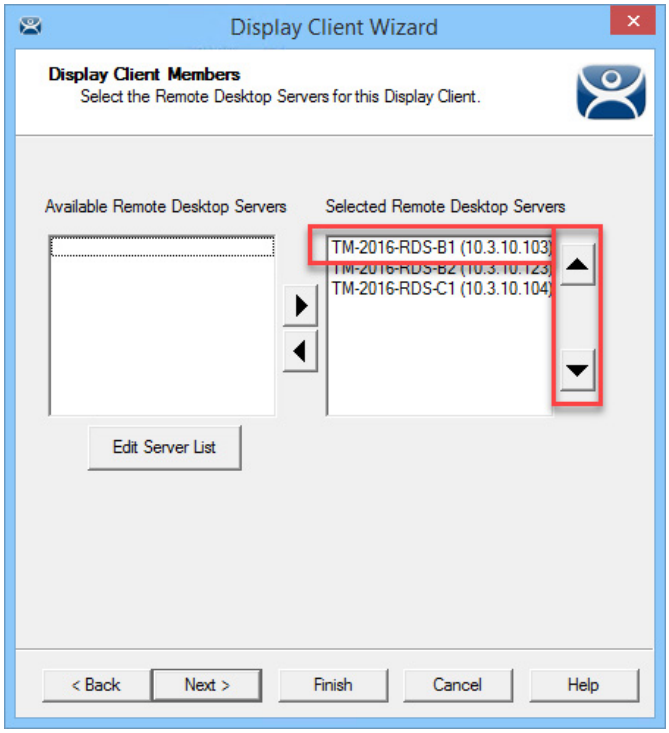
If the server is hindered by the default settings, try a longer interval. Check Infinite to keep the terminal waiting until the load decreases to an acceptable level. However, if the server has a problem, such as a memory leak, then the resources may never decrease enough to allow the terminals to connect. It is better to increase the Max field to a longer interval.

SmartSession load balancing and Queuing can be applied to a display client with a single member Remote Desktop Server. This configuration allows the single server to have the terminals connect in an orderly fashion, spreading the demand for start-up resources instead of all connecting at the same time and overloading the server.

Enforce Primary

ThinManager uses a list of Assigned Remote Desktop Servers to which the terminal can connect. The top Selected Remote Desktop Server is considered the primary Remote Desktop Server.

Figure 207 - Primary Remote Desktop Server



The thin client connects to the Remote Desktop Servers in the order of the Selected Remote Desktop Servers list. If the terminal fails to connect to the first one, it tries the second one, then the third one, 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 always tries to connect to this server. If the terminal is running on the primary server, and the server fails, then the terminal switches to a back-up server. However, the terminal

monitors the primary Remote Desktop Server. If the primary Remote Desktop Server becomes available, then the terminal switches back to its assigned Primary Remote Desktop Server.

Failover

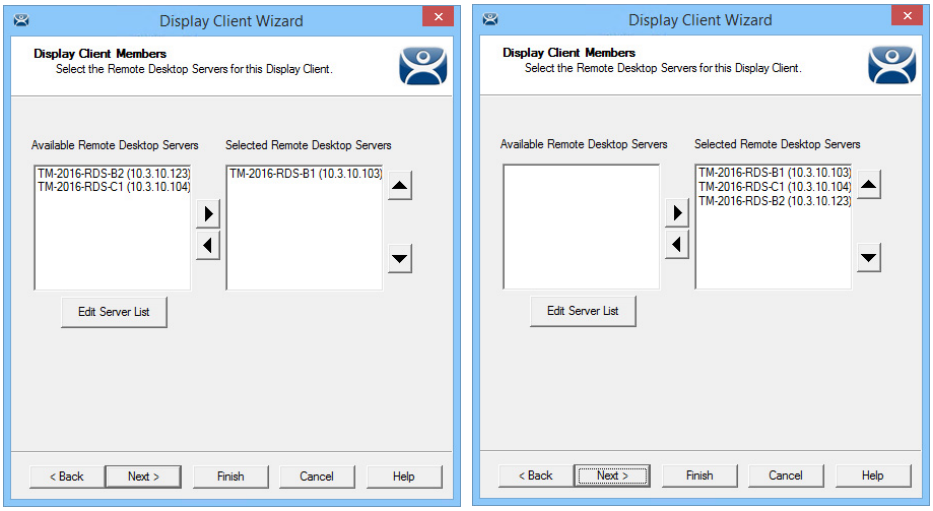
Failover in ThinManager is configured when two or more Remote Desktop Servers are assigned to a terminal. If the first server fails, the terminal detects it and switches to the back-up server, which prevents downtime and loss of productivity.

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

Here are the requirements for Failover.

- Two or more Remote Desktop Servers
- The same applications installed in identical locations on each Remote Desktop Server
- The same Windows accounts on each Remote Desktop Server

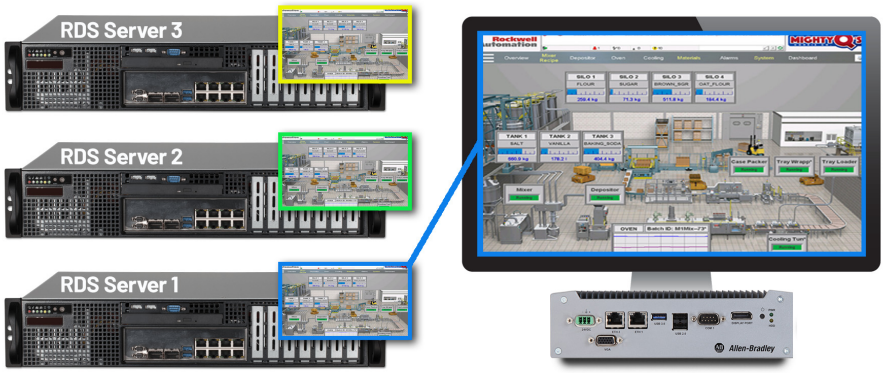
Figure 208 - Display Clients Without Failover and With Failover



To configure Failover, follow these steps.

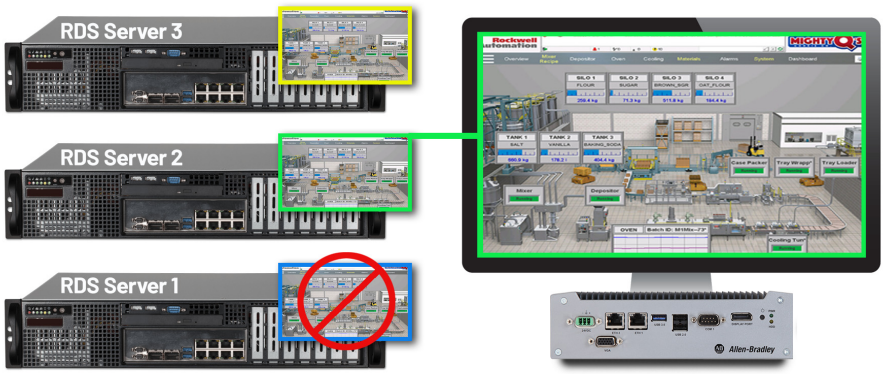
1. Define multiple Remote Desktop Servers using the Remote Desktop Server Wizard. For more information, see Defining Remote Desktop Servers in ThinManager on page 61.
2. Add two or more servers to the Selected Remote Desktop Servers list on the Display Client Members page of the Display Client Wizard.

Figure 209 - Terminal Connected to First Remote Desktop Server



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

Figure 210 - Terminal Connected to Second Remote Desktop Server



If the first Remote Desktop Server fails, the terminal detects it, disconnects, and tries the next server in the Selected Remote Desktop Servers list. It launches the same display client with the same credentials.

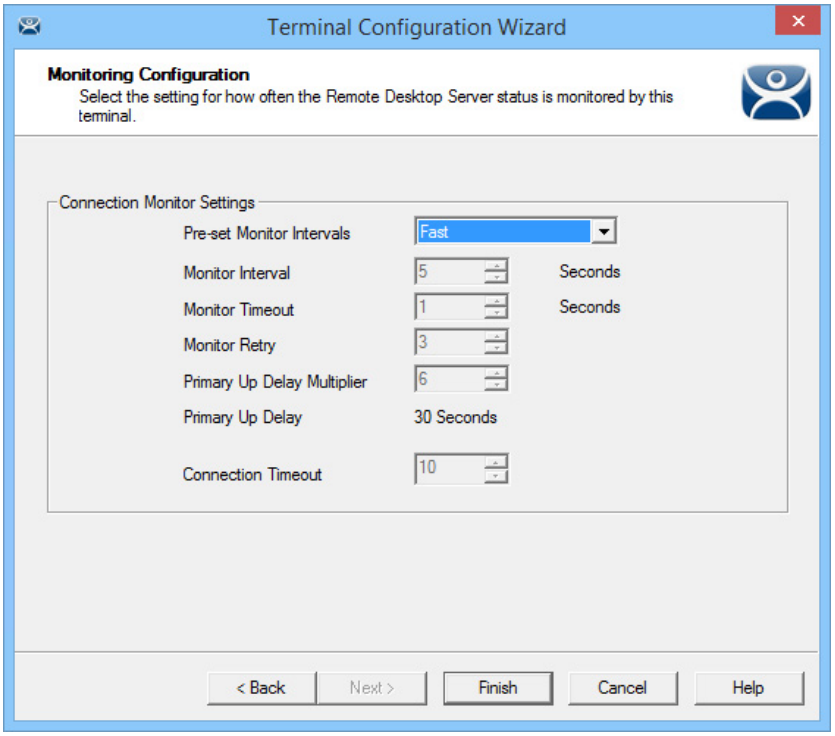
The speed in which server failure is detected can be modified on the Monitoring Configuration page of the Terminal Configuration Wizard.

To open the Terminal Configuration Wizard, follow these steps.

1. Click the Terminals icon at the bottom of the ThinManager navigation pane.
2. Right-click a terminal in the Terminals branch, and choose Modify.

   The Terminal Configuration Wizard appears, opened at the first page.
3. Click Next until the Monitoring Configuration page appears.

Figure 211 - Monitoring Connection Page of Terminal Configuration Wizard



Field	Description
Pre-set Monitor Intervals	
Custom	Allows administrator to change settings from defaults.
Fast/Medium/Slow	A set rate for the frequency with which the Remote Desktop Server status is checked.
Monitor Interval (s)	Time the terminal waits before it attempts to reconnect.
Monitor Timeout	Time interval between reconnection attempts.
Monitor Retry	Number of times the terminal tries to reconnect before failover.
Primary Up Delay Multiplier	A constant used to generate the Primary Up Delay time.
Primary Up Delay	A delay—usually, 30…60 seconds—added to allow a Remote Desktop Server to fully boot before the terminal tries to log in. Equal to the Monitoring Interval multiplied by the Primary Up Delay Multiplier. Prevents a terminal that uses Enforce Primary from a return to its primary Remote Desktop Server before it is ready.

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. If the connection is lost, the terminal tries to reconnect. If it fails, it connects to the next Remote Desktop Server in the Selected Remote Desktop Servers list.

Using the Fast setting, a terminal waits five seconds, tries to reconnect; waits one second, tries to reconnect a second time; waits a second, tries to reconnect a third time; then switches to the other server. This takes 10…20 seconds in a real-world scenario.

There are other settings, which include 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…20 seconds, but the applications need to load. If you do not want to wait for the application to load, you can use Instant Failover. See Instant Failover on page 164 for more information.

Instant Failover

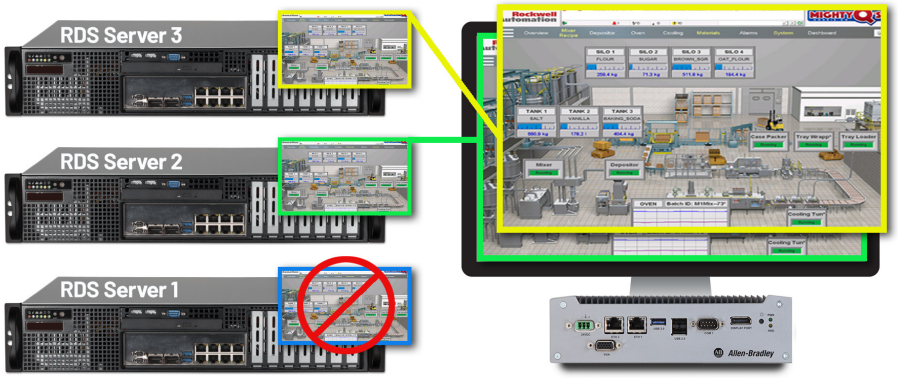
A Display Client configured with Instant Failover (see Figure 196 on page 151) sends the terminal to connect to two Remote Desktop Servers at startup, which gives it two active sessions.

You may need a second license from your application vendor in order to use Instant Failover.

Figure 212 - 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, which eliminates any downtime due to Remote Desktop Server failure.

Figure 213 - Terminal with Instant Failover and Backup Sessions



An Instant Failover display client has two active sessions; so, if one Remote Desktop Server fails, the display client starts a session on a third Remote Desktop Server if there is one in the Selected Remote Desktop Servers list.

These are the requirements for Instant Failover.

- Two or more Remote Desktop Servers
- The same applications installed in identical locations on each Remote Desktop Server
- The same Windows accounts on each Remote Desktop Server
- The Display Client needs Instant Failover checked on the Remote Desktop Services and Workstation Options page Display Client Wizard

Check Allow Auto-Login (see Figure 196 on page 151) so switching is automatic and does not require a user to log in to start the session. Also, see Enforce Primary on page 160.

Camera Display Clients

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

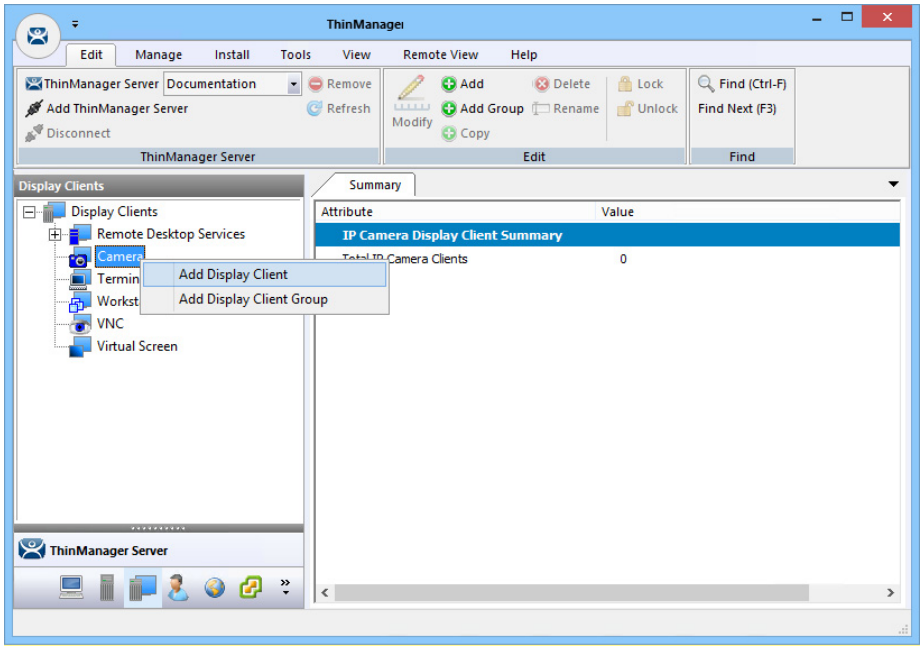
- Configure the camera device according to the camera vendor guidelines.
- Define the camera as a Camera Display Server.
- Create a Camera Display Client and add camera output as overlays. See Camera Display Clients on page 165.
- Add the Camera Display Client to a Terminal. See Terminal Configuration Wizard in ThinManager on page 231.

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

To define a Camera Display Client application for the terminal, follow these steps.

1. Click the Display Clients icon at the bottom of the ThinManager navigation pane.

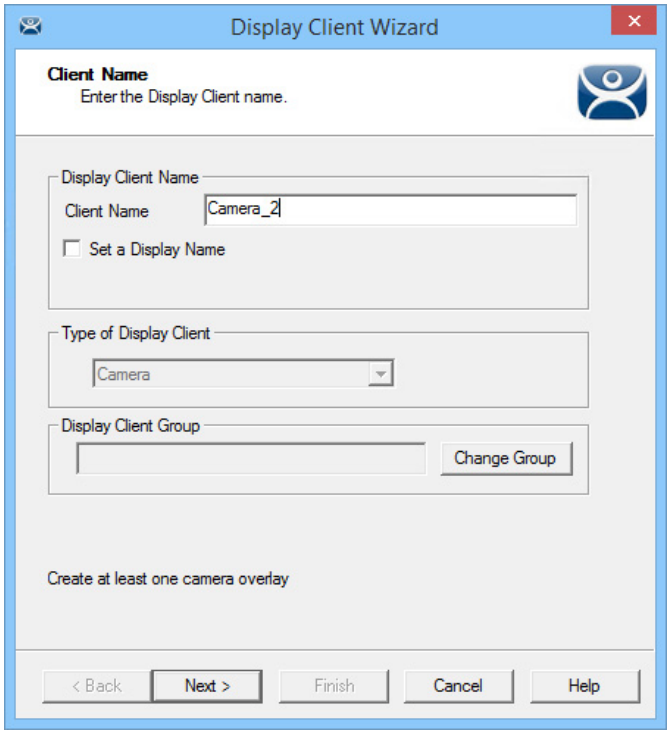
Figure 214 - Add Camera Display Client



2. Right-click on the Camera branch and choose Add Display Client.

   The Display Client Wizard appears, opened at the Client Name page, which sets the name and type of Display Client.

Figure 215 - Camera Display Client Name Page of the Display Client Wizard

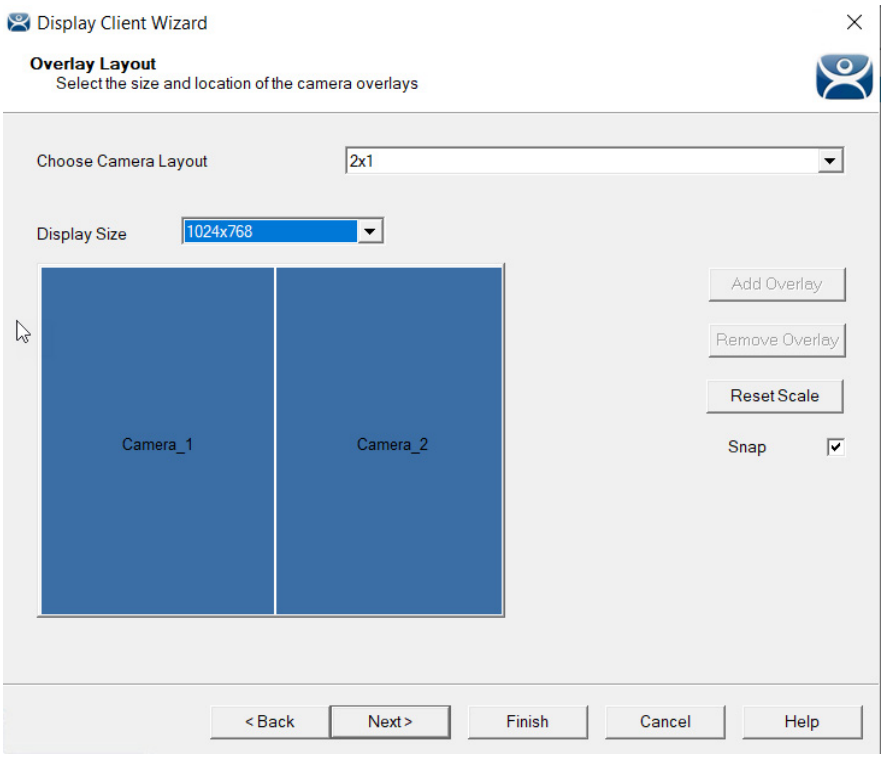


3. Complete the required fields.

Field/Setting	Description
Client Name	Use to name the Display Client.
Set a Display Name	Allows assignment of a different name to display in the ThinManager tree.
Type of Display Client	Choose Camera, which creates a Display Client that allows the use of IP cameras.
Change Group	Launches the Select Display Client dialog box, which allows you to add this Display Client to a Display Client Group.
Permissions	Launches the Permissions dialog box, which allows Relevance permissions to be set.

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

Figure 216 - Overlay Layout Page



4. Complete the required settings.

Camera feeds are laid out on the Overlay Layout page of the Display Client Wizard.

Setting	Description
Choose Camera Overlay	Choose a setting from the pull-down menu to set the layout of the displays from a single overlay to multiple overlays on the Display Client. Choices include formats from a single camera to 16 camera displays.
Display Size	Sets the display resolution size.
Add Overlay	Launches the Custom Overlay dialog box, which allows you to define the name, size, and location of the camera display.
Remove Overlay	Removes a highlighted overlay from the Display Client.
Permissions	Launches the Permissions dialog box, which allows Relevance permissions to be set.
Reset Scale	Adjusts all Overlays to fit within the screen.
Snap	Check to align the edges of the overlays, side by side.

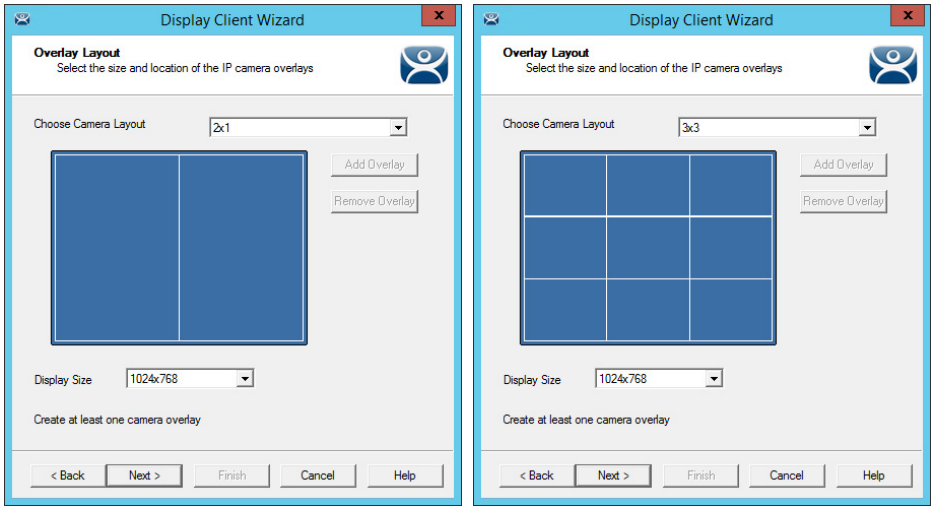
You can either use a camera overlay template or lay out a custom overlay.

Camera Overlay Template

The wizard provides a number of layouts.

1. Choose a camera grid from the Choose Camera Layout pull-down menu.

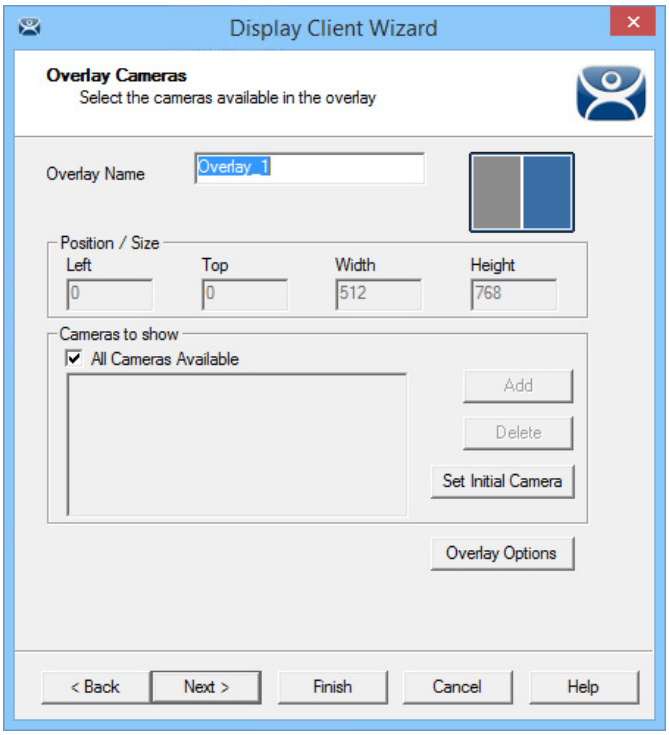
Figure 217 - 2x1 and 3x3 Grid Templates



2. Once a template is selected, click Next.

   The Overlay Cameras page appears, where the wizard lets you add a camera per grid.

Figure 218 - Overlay Cameras Page



3. Complete the required fields on the Overlay Camera page for each overlay.

Setting	Description
Overlay Name	Automatically generated, but can be changed as needed.
Position/Size	
Left	Sets the left edge location of the overlay (in pixels).
Top	Sets the top edge location of the overlay (in pixels).
Width	Sets the overlay width (in pixels).
Height	Sets the overlay height (in pixels).

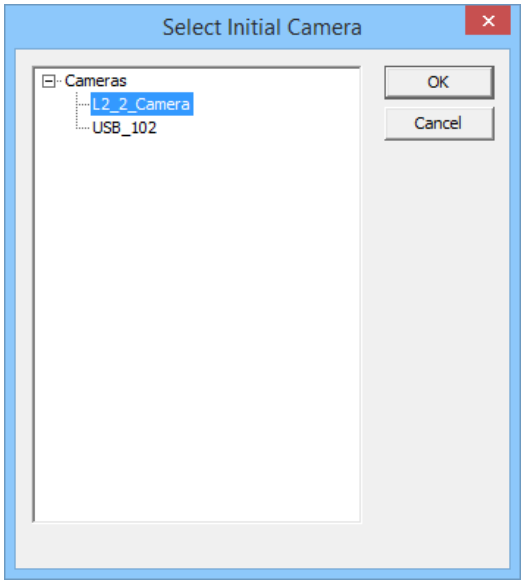
Setting	Description
Cameras to Show	
All Cameras Available	Makes all cameras available. Clear the checkbox to add specific cameras via Add.
Add	Use to add a camera to the overlay.
Delete	Deletes a camera from the overlay.
Set Initial Camera	Sets the initial camera from a series of cameras.
Overlay Options	Launches the Overlay Options dialog box.

The gray-shaded area represents the overlay to which you are assigning cameras. By default, All Cameras Available is checked, which makes all cameras available in that overlay.

4. Click Set Initial Camera.

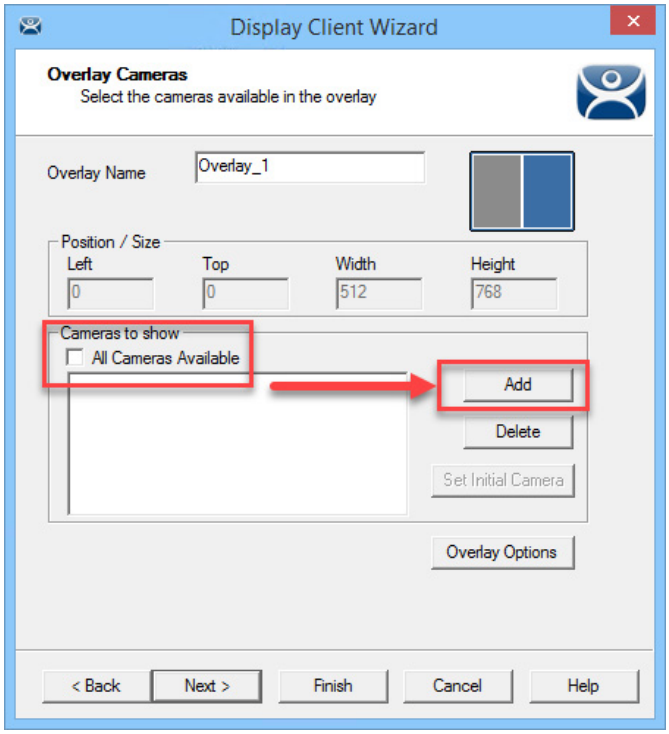
   The Select Initial Camera dialog box appears with a list of cameras from which to select.

Figure 219 - Select Initial Camera Window



5. Choose the camera to be displayed first, and click OK.

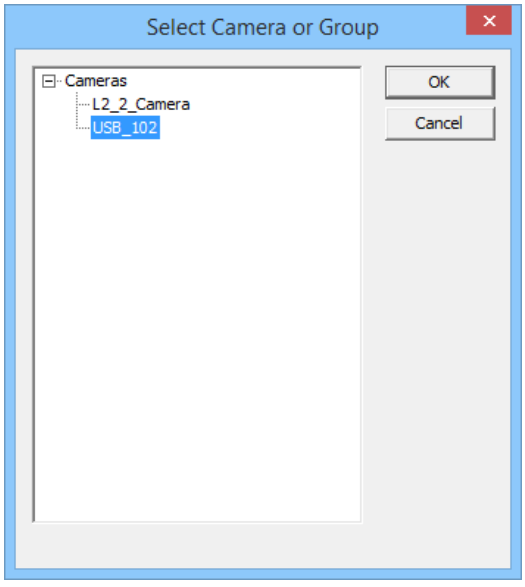
Figure 220 - Overlay Cameras Page



6. To limit the overlay to a smaller set of cameras, clear the All Cameras Available checkbox and click Add.

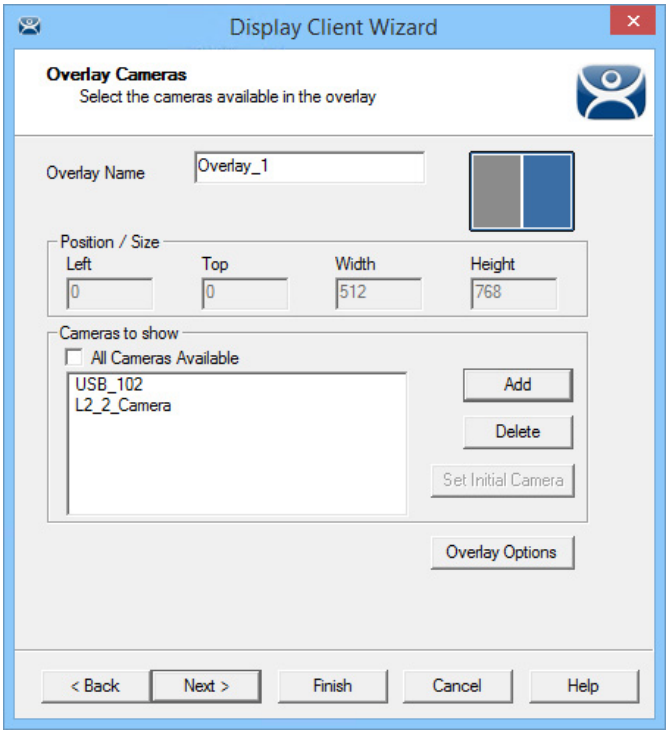
   The Select Camera or Group dialog box appears.

Figure 221 - Select Camera or Group



7. Choose a camera and click OK.
8. Repeat until all the desired cameras are chosen.

Figure 222 - Selected List of Cameras



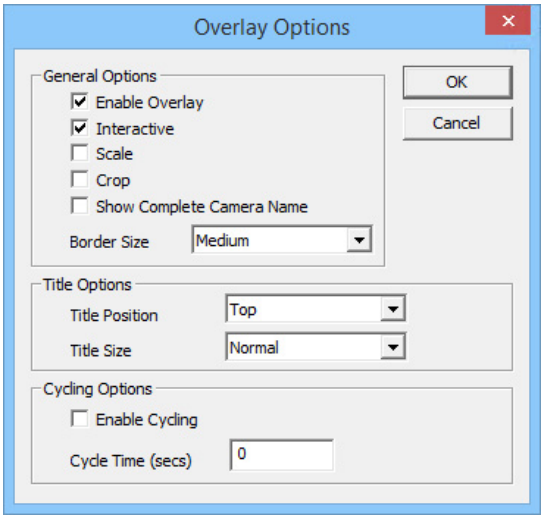
If multiple cameras are chosen, the top-listed camera appears first.

Overlay Options

1. Once the cameras for the overlay are added, click Overlay Options.

   The Overlay Options dialog box appears.

Figure 223 - Overlay Options



2. Choose the Overlay Options for the camera display, and click OK.

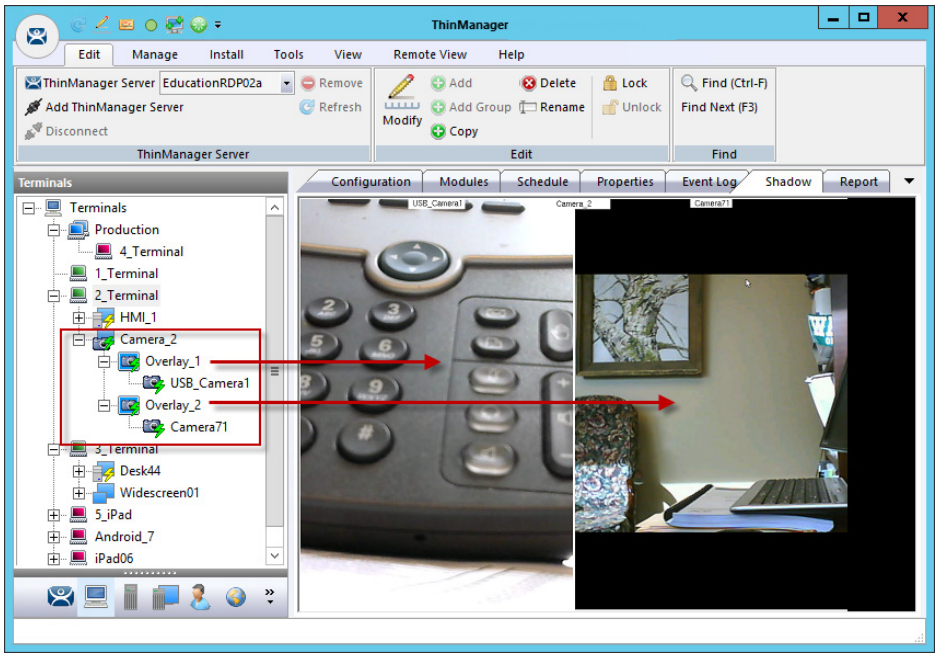
Option	Description
General Options	
Enable Overlay	Makes the overlay visible at startup. Clear this setting to start the display client with the camera in a disabled, nonvisible state. The TermMon ActiveX Control can be used by an application to enable the overlay.
Interactive	Allows user on the terminal to interact with the overlay. If the user clicks in the overlay area, they can perform functions such as switching cameras and making the overlay full screen.
Scale	Scales camera frames to the size of the overlay window. Aspect ratio is maintained.
Crop	Crops the camera frame if it is larger than the camera overlay. When combined with the Scale option, the overlay area is entirely filled.
Show Complete Camera Name	Allows the entire path of the camera to be displayed. The path includes any groups of which the camera is a member.
Border Size	Determines the size of the overlay outside border.
Title Options	
Title Position	Position of the camera name within the overlay.
Title Size	Size of the camera name when displayed within the overlay. Choose Don't Show Title to display no camera name.
Cycling Options(1)	
Enable Cycling	Cycles between the cameras assigned to the overlay.
Cycle Time	Time (in seconds) that the overlay displays each camera before switching to the next camera.

(1) Cycling Options are not available when All Cameras Available is checked on the Overlay Cameras page of the Display Client Wizard.

3. On the overlay Cameras page, click Finish.

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

Figure 224 - Shadow of a Terminal with a Camera Display Client



When the Camera Display Client is selected, the Terminal makes a connection to the camera and requests the feed using the administrative account entered when the camera was defined as a display server. This connection is active only if the camera display client is active. If you switch to another display client, then the Terminal drops the connection to the camera.

The overlays and cameras are shown with green lightning bolts when active and red lightning bolts when inactive.

Custom Overlays

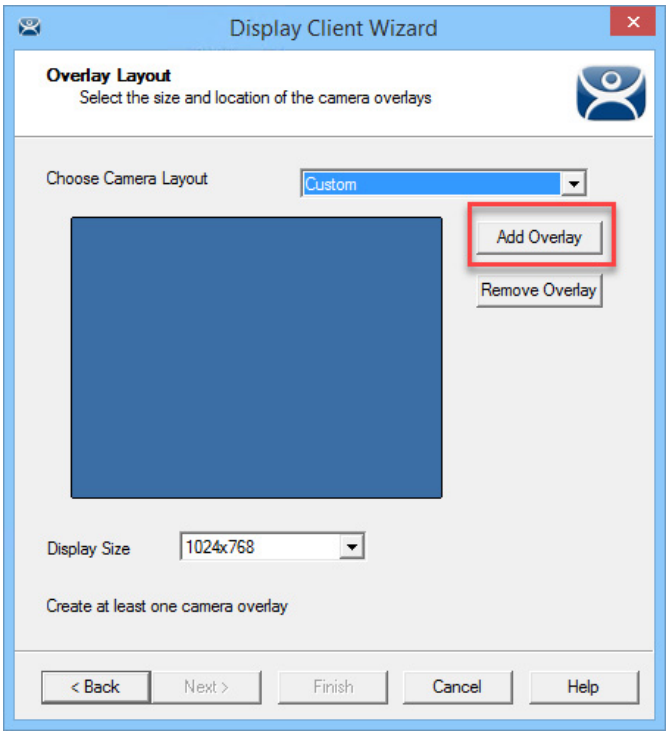
You can create custom overlays instead of using the templates.

To create a new Camera Display Client, follow these steps.

1. Right-click on the Camera branch of the Display Client tree and choose Add Display Client.

   The Add Overlay dialog box appears.

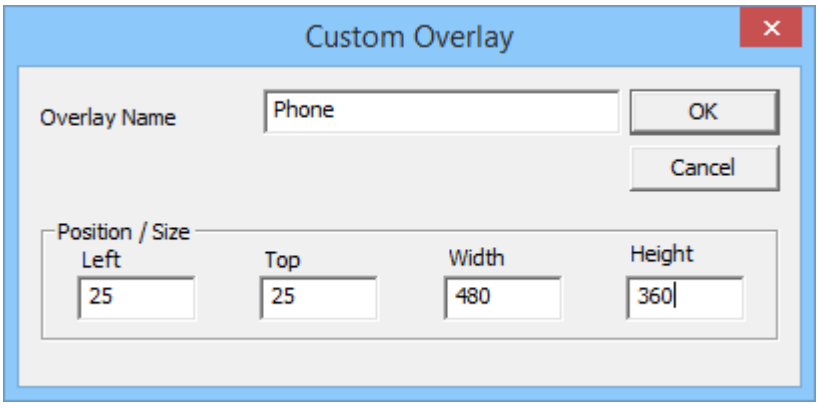
Figure 225 - Add Overlay



2. Click Add Overlay.

   The Custom Overlay dialog box appears.

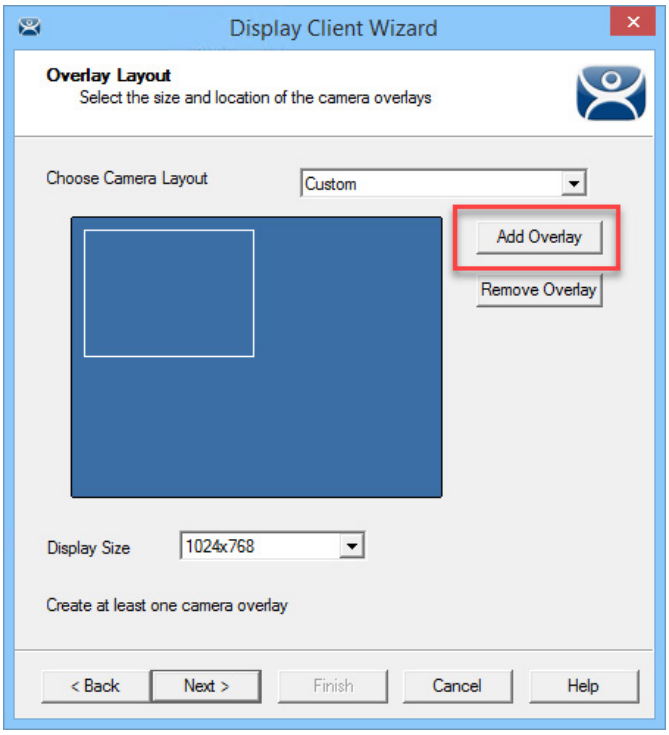
Figure 226 - Custom Overlay



The Custom Overlay dialog box defines the boundaries of the overlay.

3. Type the position of the overlay, in pixels, into the Left and Top fields.
4. Define the size of the overlay, in pixels, in the Width and Height fields.
5. Click OK.

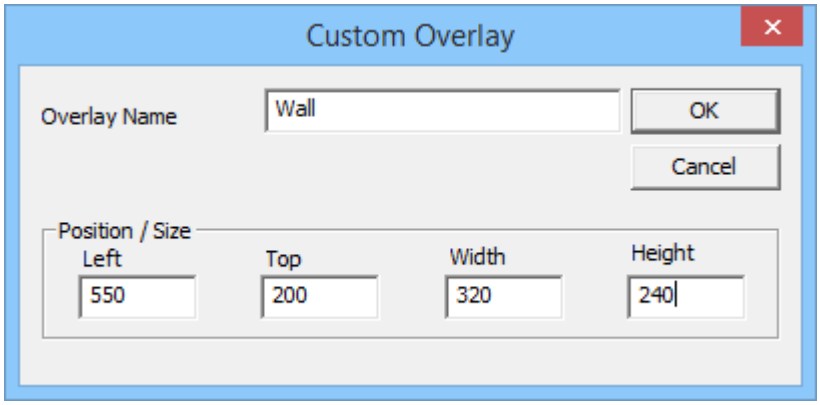
Figure 227 - Overlay Layout Page of the Camera Display Client Wizard



Once the Custom Overlay dialog box is closed, the Overlay Layout page shows the boundaries of the custom overlay.

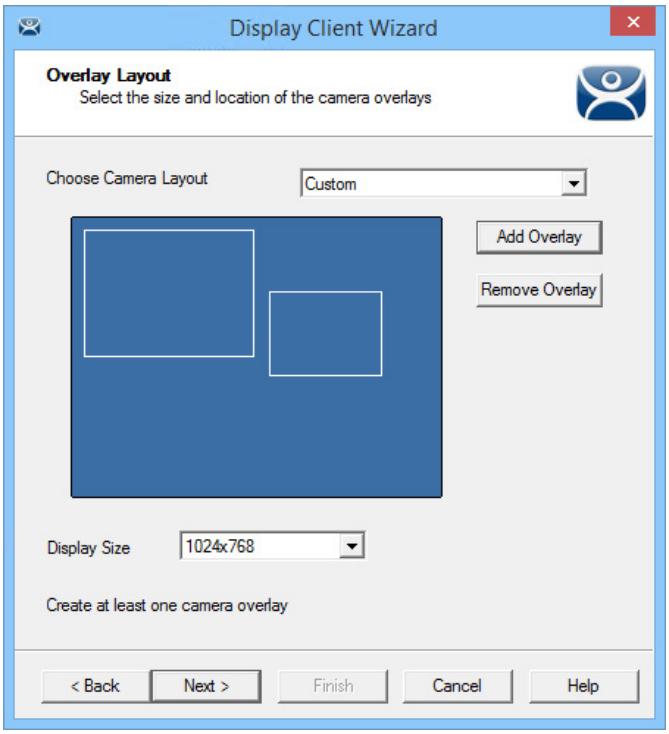
6. Click Add Overlay to add another overlay.

Figure 228 - Second Overlay



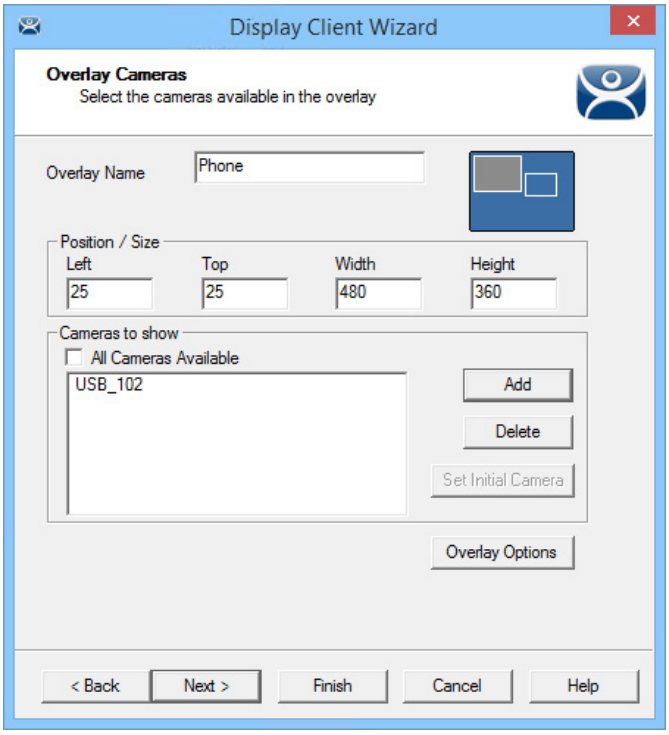
7. Repeat step 6 as needed.

Figure 229 - Overlay Cameras Page



The Display Client Wizard continues to add a camera or cameras to the overlays as it did for the configured templates.

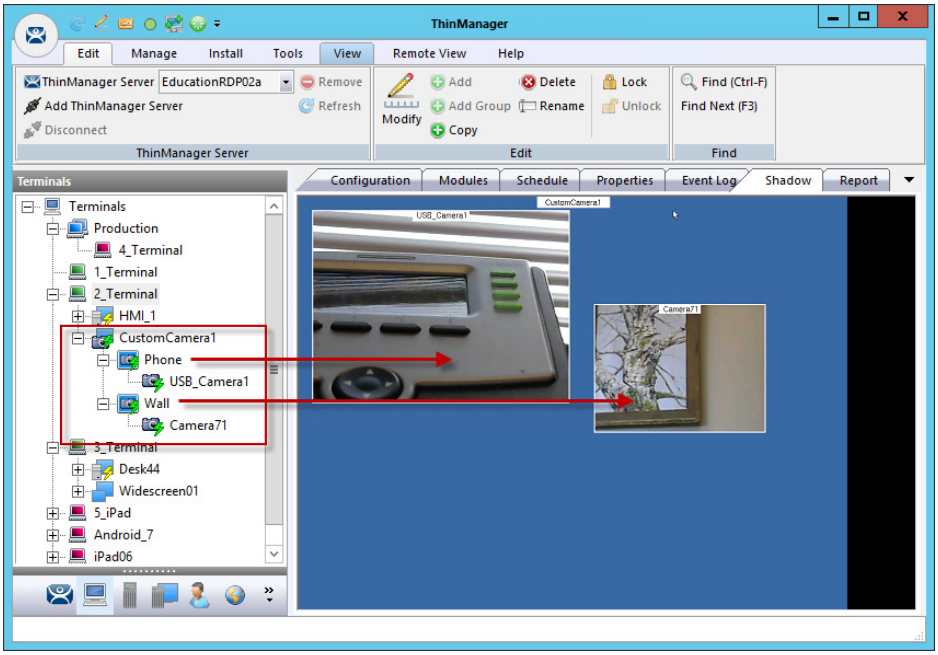
Figure 230 - Multiple Custom Camera Overlays



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

8. Click Finish when done.

Figure 231 - 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 is shown on the Terminal.

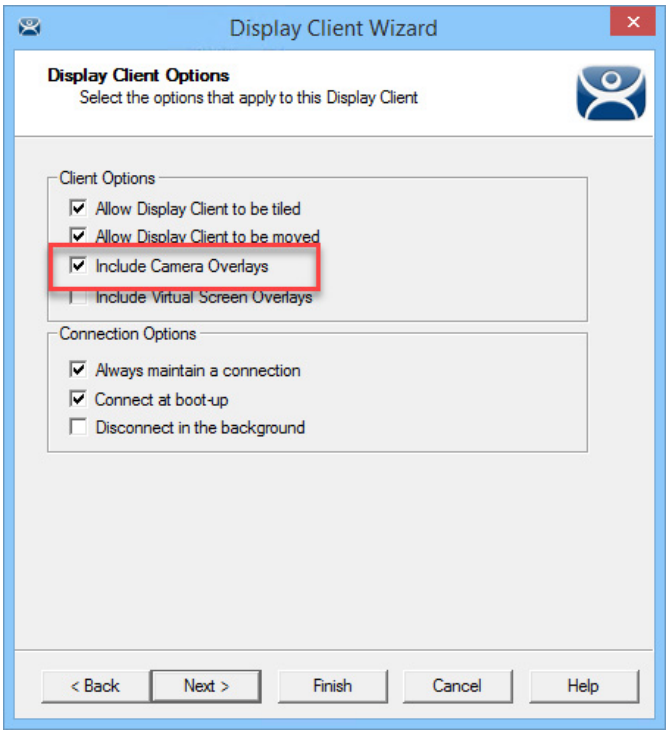
Adding a Camera to an Existing Application

Camera overlays are added to an application using the Remote Desktop Services Display Client Wizard. An overlay covers the screen of that display client in the area you define. You can hide and reveal the overlay with the TermMon ActiveX from ThinManager. See Cameras and the TermMon ActiveX on page 180.

To add a camera to an existing application, follow these steps.

1. Double-click on a Remote Desktop Services Display Client to open the Remote Desktop Services Display Client Wizard and click Next to navigate to the Display Client Options page.

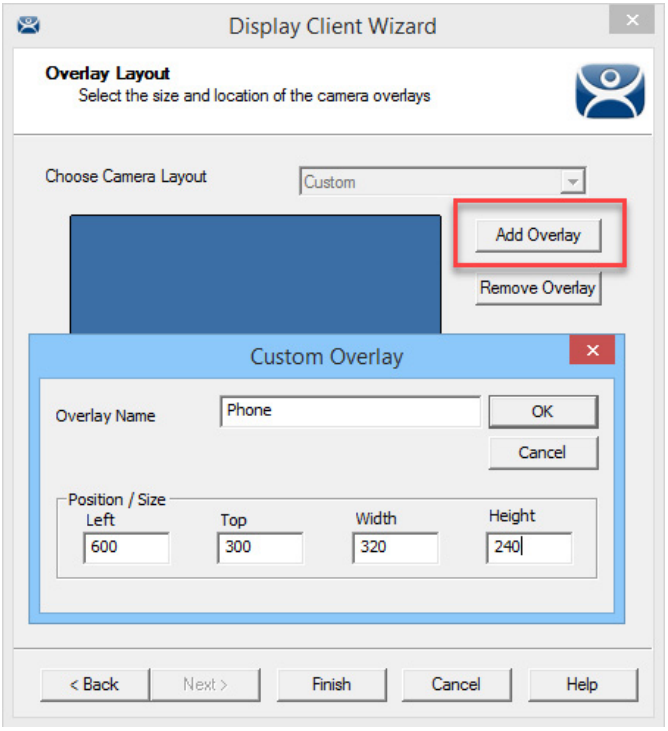
Figure 232 - Display Client Options Page



2. Check Include Camera Overlays, which adds an Overlay Layout page to the end of the wizard.
3. Click Next to navigate to the Overlay Layout page of the wizard.
4. Click Add Overlay.

   The Custom Overlay dialog box appears.

Figure 233 - Overlay Layout Page of the Display Client Wizard

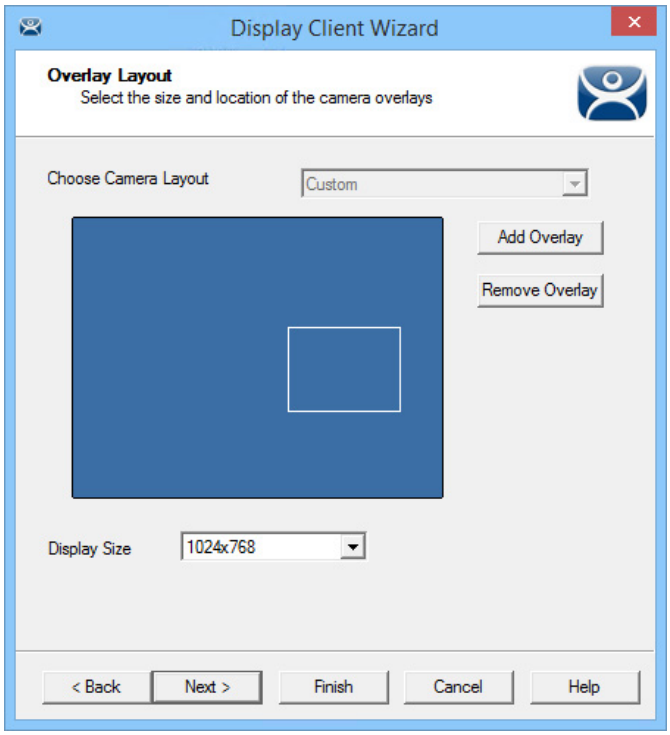


5. Enter the position of the overlay, in pixels, using the Left and Top fields.
6. Define the size of the overlay, in pixels, in the Width and Height fields

7. Click OK.

   The Overlay Layout page shows the boundaries of the custom overlay.

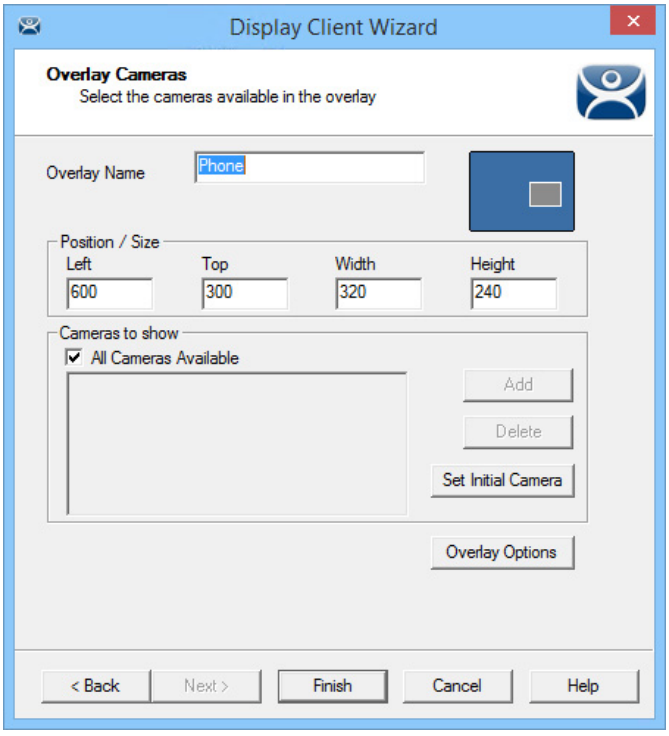
Figure 234 - Overlay Layout Page



8. Click Next to continue the wizard.

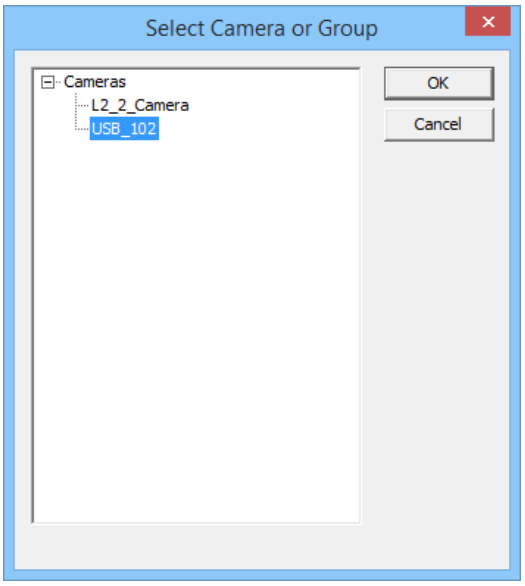
   The Overlay Cameras page appears.

Figure 235 - Overlay Cameras Page



9. Specify the cameras—check All Cameras Available or click Add to launch the Select Camera or Group dialog box to select a camera for the overlay.

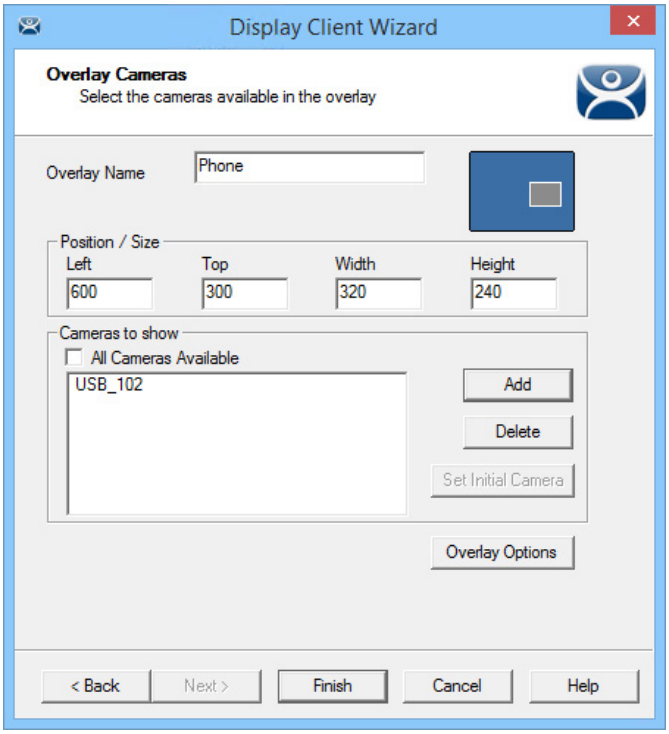
Figure 236 - Select Camera or Group



a. Highlight the desired camera and click OK.

b. Repeat as needed.

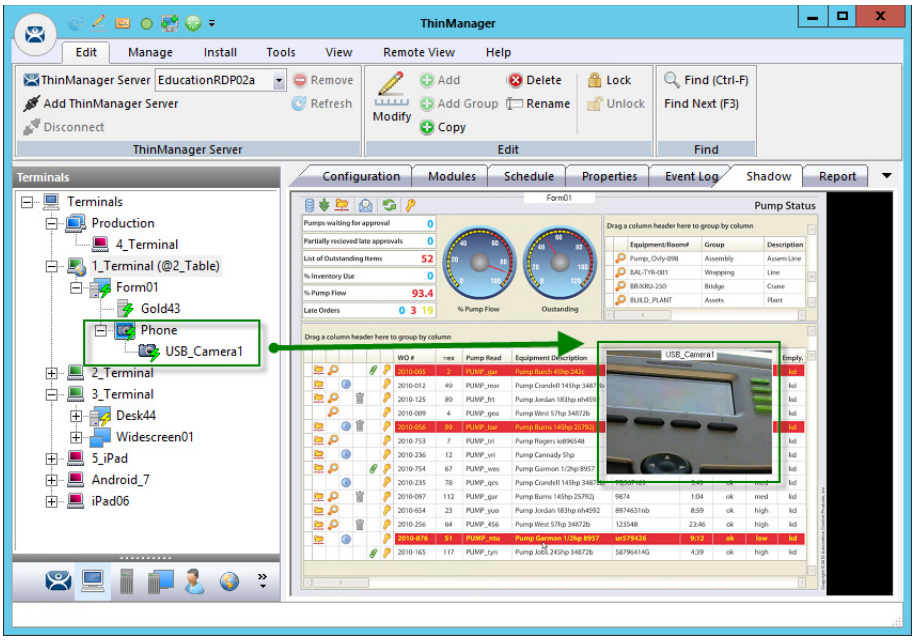
Figure 237 - Overlay Cameras Page



10. When the cameras are chosen and the options configured, click Finish to close the wizard.

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

Figure 238 - Embedded Camera in Application



Cameras and the TermMon ActiveX

Camera overlays added to an application cover the screen of that display client in the area you defined via the Overlay Cameras page. You can hide and reveal the overlay with the TermMon ActiveX from ThinManager.

The TermMon ActiveX Control file (termmon.ocx) is on the ThinManager CD. 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 termmon.ocx file to the computer where you want to use it. Register the file by executing

```
regsvr32 <path\termmon.ocx>
```

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

Available Commands for Use with Cameras

Commands	Description
CameraOverlayEnable	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, and the second parameter is the name of the overlay.
CameraOverlayDisable	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, and the second parameter is the name of the overlay.
CameraOverlayCycleStart	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, and the second parameter is the name of the overlay.
CameraOverlayCycleStop	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, and the second parameter is the name of the overlay.
CameraOverlaySwitchNext	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, and the second parameter is the name of the overlay.

Available Commands for Use with Cameras

Commands	Description
CameraOverlaySwitchPrev	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, and the second parameter is the name of the overlay.
CameraOverlayFullscreenEnter	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, and the second parameter is the name of the overlay.
CameraOverlayFullscreenExit	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, and the second parameter is the name of the overlay.
CameraOverlaySwitchByName	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; and 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	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; and the fourth parameter is the y position.
CameraOverlayResize	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; and the fourth parameter is the height.
CameraOverlayResizeMove	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 fourth parameter is the y position; the fifth parameter is the width; and the sixth parameter is the height.

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.

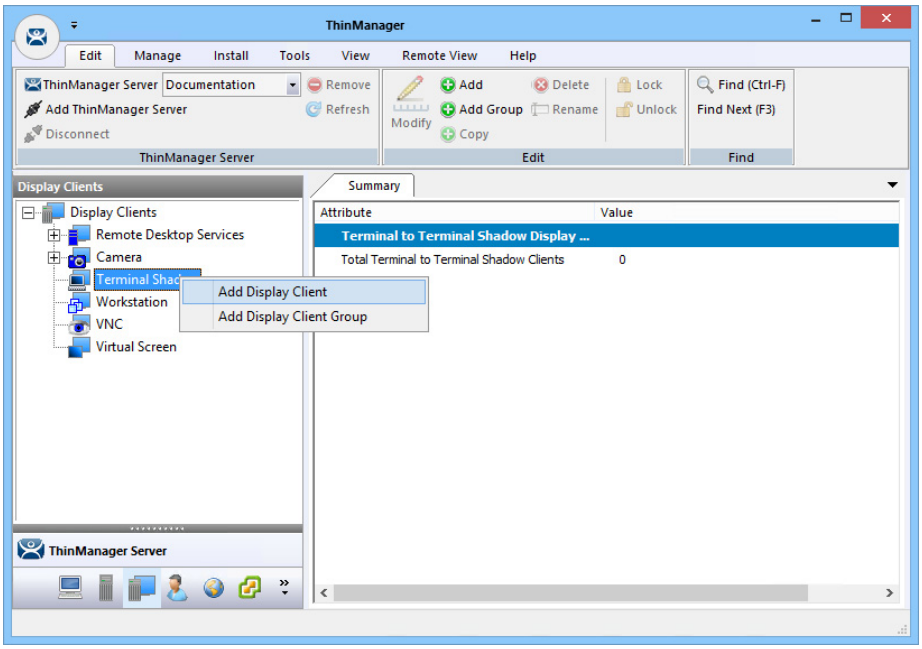
The ThinManager Terminal Shadow sends the screen display from the shadowed Terminal to the other Terminal. It does not redirect the display from the Remote Desktop Server, but sends the images from the actual shadowed Terminal.

The Terminal Shadow feature is set up and configured as a Terminal Shadow Display Client.

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 the need to travel to the specific problem area.

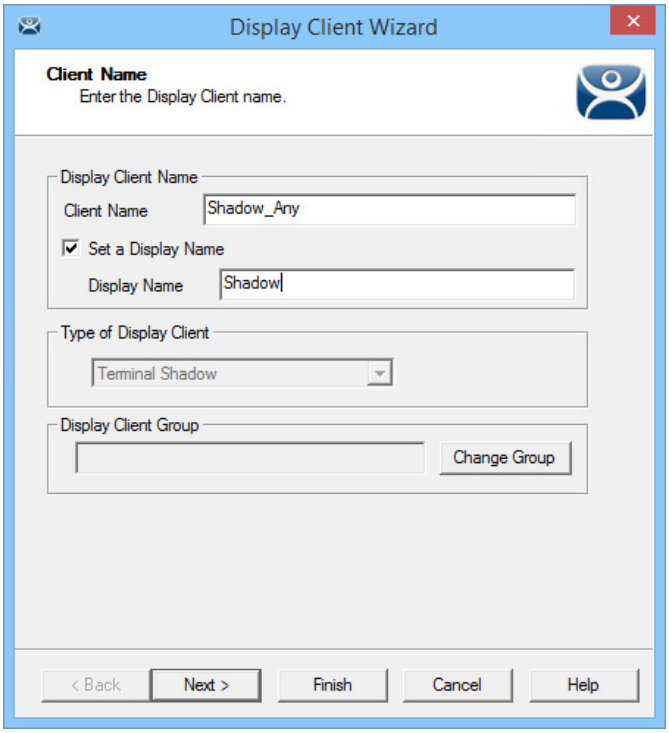
Figure 239 - Display Client Tree of ThinManager



1. To launch the Display Client Wizard, right-click on the Terminal Shadow branch of the Display Clients tree and select Add Display Client.

   The Client Name page appears.

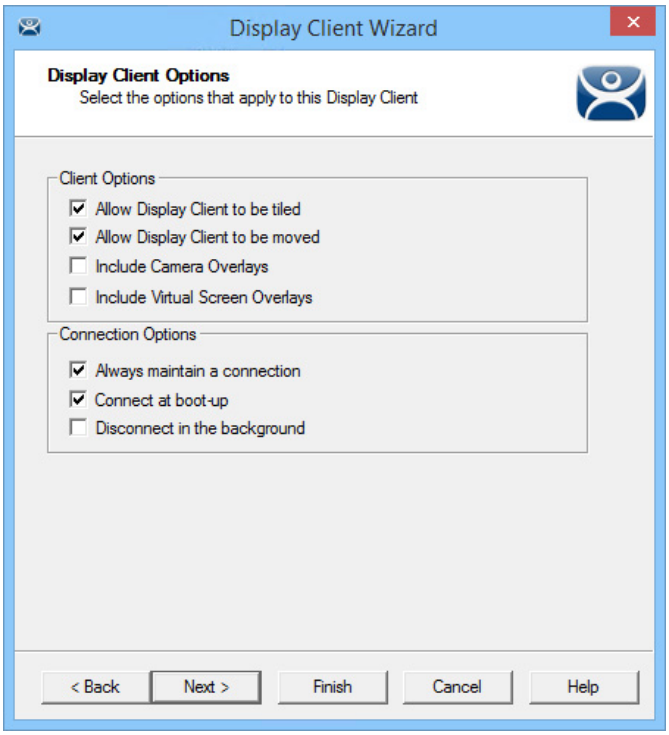
Figure 240 - Client Name Page of the Terminal Shadow Display Client Wizard



2. Enter a name for the Terminal Shadow display client.
3. (Optional) Click Set a Display Name to configure the display client to display an alternative name in the ThinManager Server tree.
4. Click Next.

   The Display Client Options page appears.

Figure 241 - Display Client Options Page



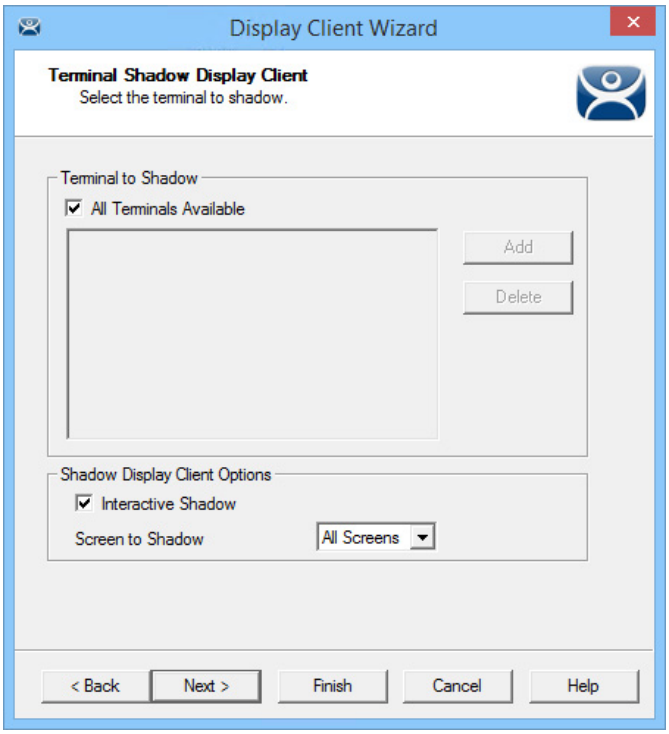
5. Check the following options as needed.

Setting	Description
Client Options	
Allow Display Client to be tiled	Allows the display client to be tiled.
Allow Display Client to be moved	Allows a Display Client to be moved from screen to screen. A movable display client can be anchored with a setting on the Screen Options page of the Terminal Configuration Wizard.
Include Camera Overlays	Allows an IP camera overlays to be added to this display client.
Include Virtual Screen Overlays	Allows a virtual screen overlay to be added like a camera overlay.
Connection Options	
Always maintain a connection	Keeps a session active, reconnecting and restarting if it is closed. Clear the checkbox to allow the user to close a session without an automatic start of another session.
Connect at boot-up	Starts a session for the Display Client at boot up. Clear the checkbox so a user action is required to start the session.
Disconnect in the background	In a MultiSession configuration, disconnects once it is moved into the background. Use to require fewer resources.

6. Click Next.

   The Terminal Shadow Display Client appears.

Figure 242 - Terminal Shadow Display Client Page



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

7. (Optional) Check All Terminals Available to add all of the Terminals to the Shadow menu.
8. (Optional) Clear the All Terminals Available checkbox and click Add to launch the Select Terminal or Group dialog box to select specific Terminals. See Shadow a Specific Terminal.

Shadow a Specific Terminal

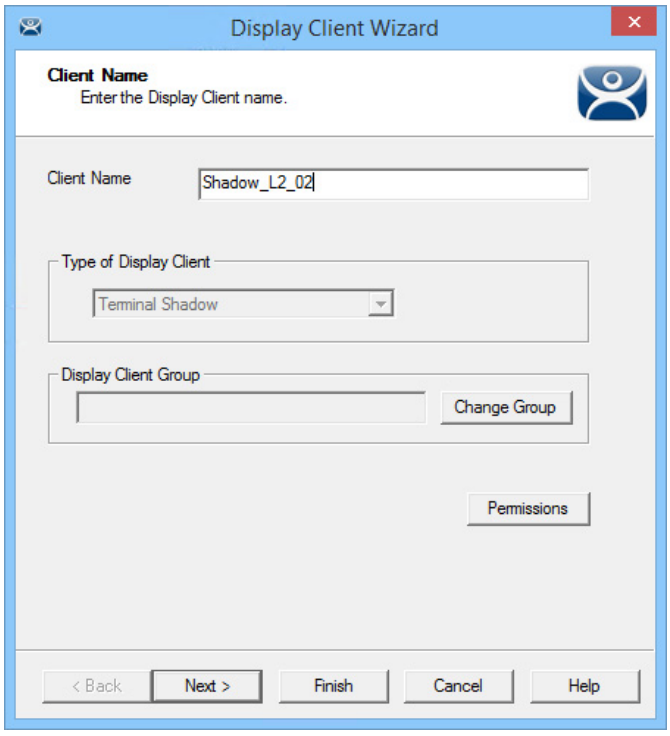
You can use the Terminal Shadow Display Client to shadow a specific Terminal, duplicating the display to another thin client. This can be helpful to provide a worker access to the HMI in various places in a large station, like a commercial oven at a baking line.

To shadow a specific terminal, follow these steps.

1. Right-click on the Terminal Shadow branch of the Display Clients tree and choose Add Display Client.

   The Client Name page appears.

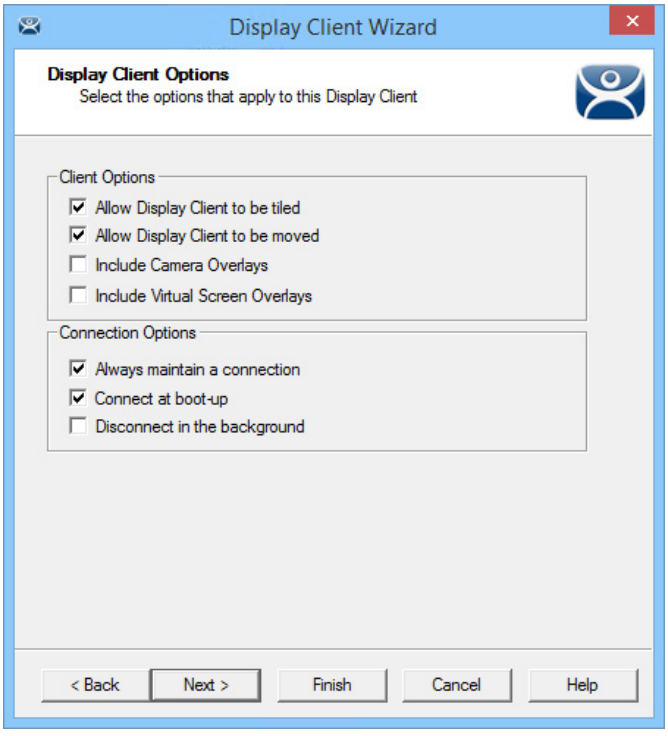
Figure 243 - Client Name Page



2. Enter a name for the display client in the Client Name field.
3. Click Next.

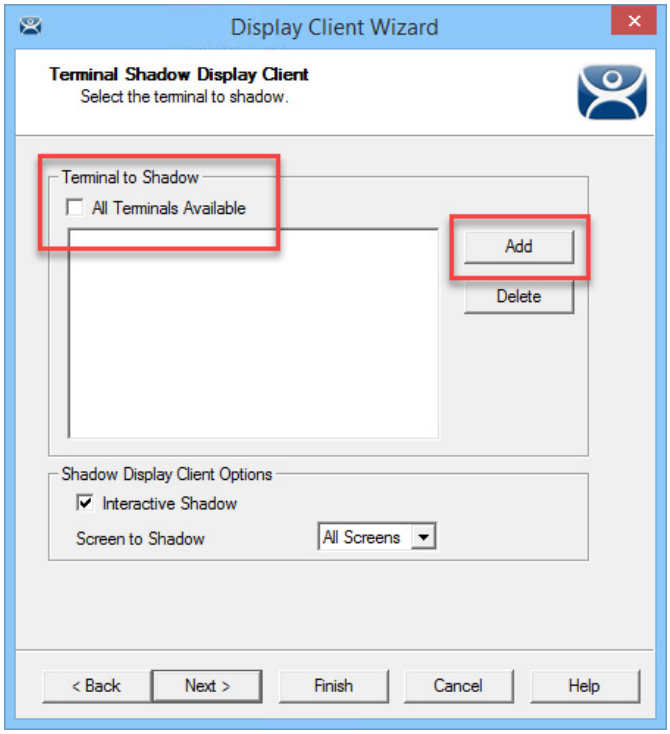
   The Display Client Options page appears.

Figure 244 - Display Client Options Page



The Terminal Shadow Display Client page appears.

Figure 245 - Terminal Shadow Display Client Page

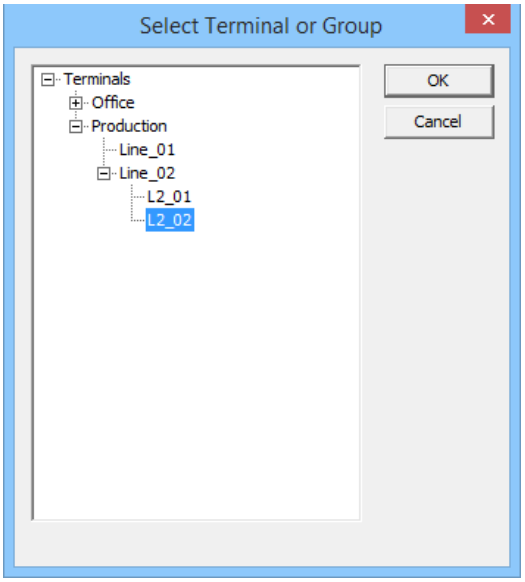


The Terminal Shadow Display Client page of the Terminal Shadow Display Client wizard is unique.

4. Clear the All Terminals Available checkbox and click Add.

   The Select Terminal or Group dialog box appears.

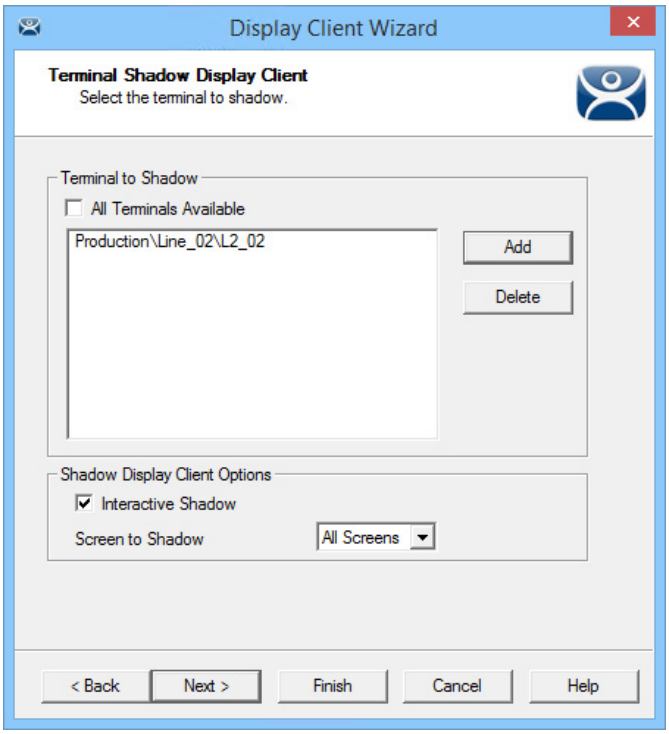
Figure 246 - Select Terminal or Group Window



5. Highlight a single group or a Terminal to add to the Shadow menu and click OK. For a Terminal, repeat as needed to select all the Terminals you want.

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

Figure 247 - Terminal Shadow Display Client Page

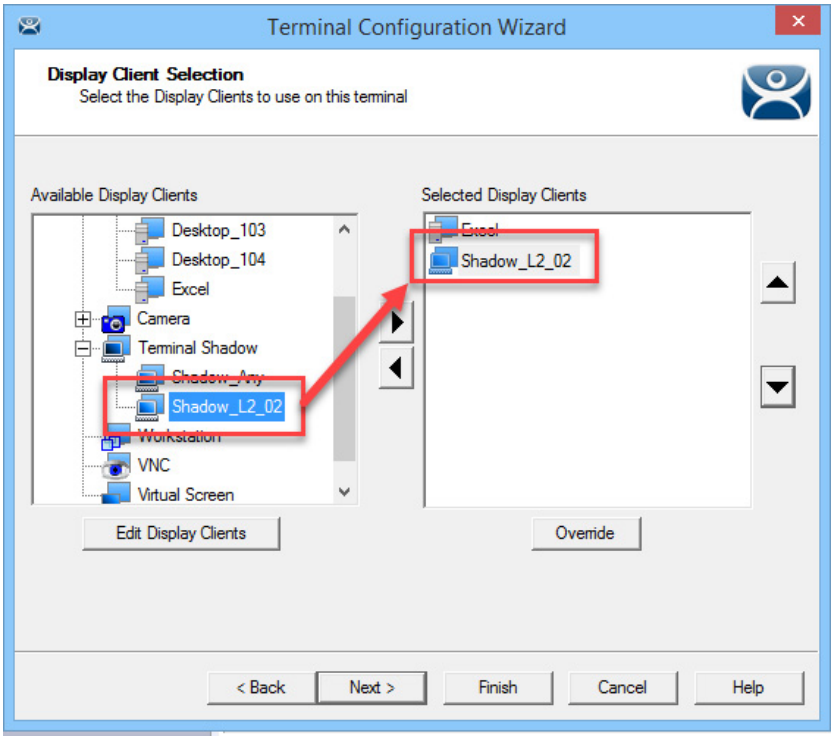


6. Check Interactive Shadow to allow the shadowing user to interact with the shadowed Terminal. Clear the Interactive Shadow checkbox to allow the shadow user read-only access.
7. Choose which screen of a MultiMonitor thin client to shadow from the Screen to Shadow pull-down menu.
8. Click Finish.

Shadow of the Terminal

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

Figure 248 - Display Client Selection Page of the Terminal Configuration Wizard

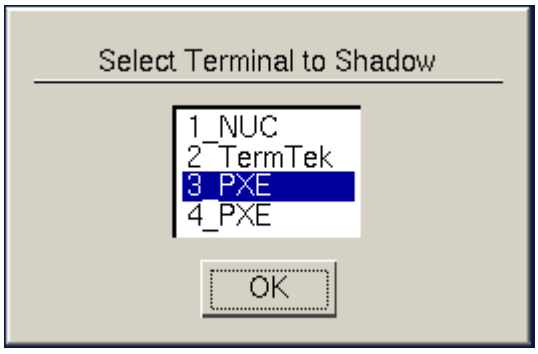


The Terminal Shadow display clients have an icon of a Terminal and a monitor session.

1. Move the desired Terminal Shadow display clients to the Selected Display Clients list. Double-click on them or use the arrows to move a highlighted display client.
2. Click Finish to save the configuration and restart the Terminal to send the configuration to the Terminal.

   The Select Terminal to Shadow dialog box appears when there are Terminal Shadow Display Clients with multiple Terminals.

Figure 249 - Shadow Menu



3. Highlight the Terminal you want to shadow and click OK.

   You are connected to the Terminal and display the screen from the shadowed thin client.

Display Client Group Selector During Shadow

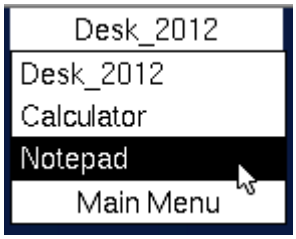
The Terminal Shadow display client is displayed in the Group Selector Menu of the Terminal to which it is assigned. The group selector shows the local display clients assigned to the Terminal.

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

Figure 250 - Local Terminal Menu Selector

To use the remote Terminal's Group Selector, choose Hide on the Local Group Selector, which hides the local selector and shows the Remote Group Selector.

Figure 251 - Remote Terminal Menu Selector



Once the Remote Group Selector menu is used, the local Terminal reverts to the Local Group Selector.

Figure 252 - ThinManager Interface Showing Group Selector Menus

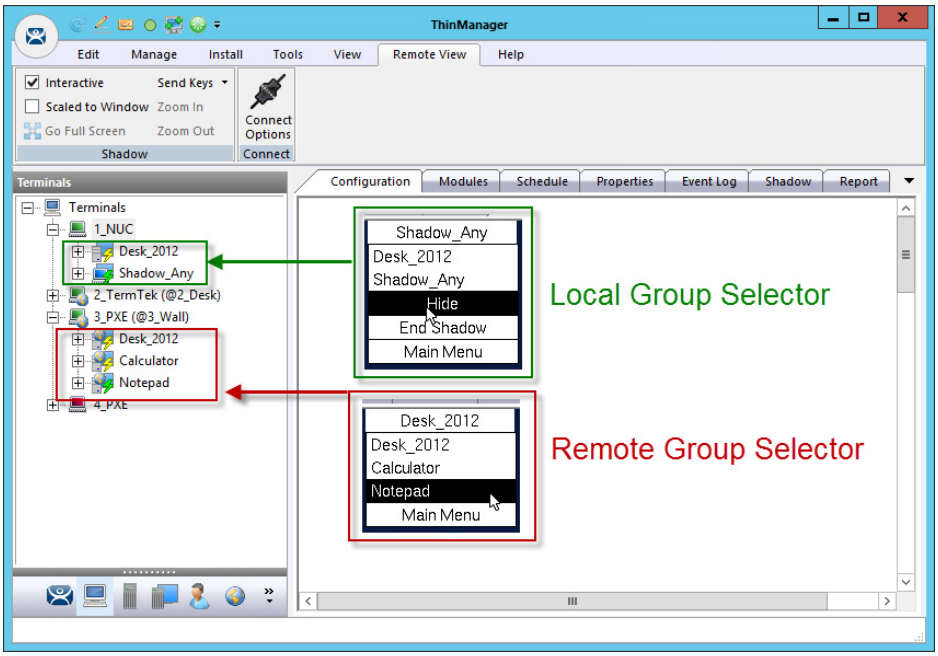


Figure 252 on page 189 shows the Group Selector menus for both the Local and the Remote Group Selectors.

Workstation Deployment

Microsoft built Remote Desktop Protocol, 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. RDP 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 ability is very helpful as it allows applications that are not RDS-compliant to be run on a workstation, but the user can receive the session on a hardened industrial thin client instead of a PC.

To transfer a workstation session to a thin client, the following are required.

- Turn on the Remote transfer on the PC
- Create a Workstation Display Client
- Apply the Workstation Display Client to a Terminal

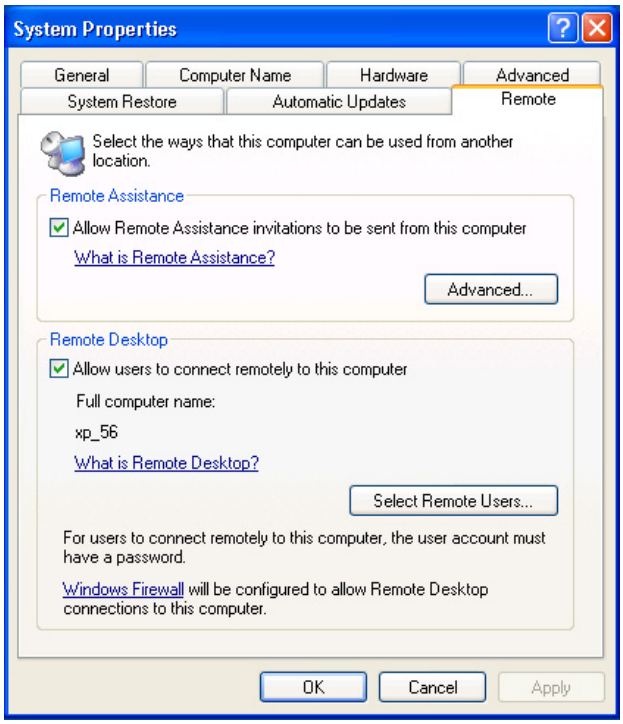
The workstation ca be a physical computer or a virtual desktop.

Step 1 – On the PC

To enable the Remote Desktop function on the workstation, follow these instructions. This example uses Windows XP. Consult Microsoft instructions for more detail.

1. Go to the workstation Control Panel and open the System Properties, or right-click My Computer and choose Properties.
2. Click the Remote tab.

Figure 253 - System Properties for XP Workstation



3. In the Remote Desktop section, check Allow users to connect remotely to this computer.
4. Click Select Remote Users.

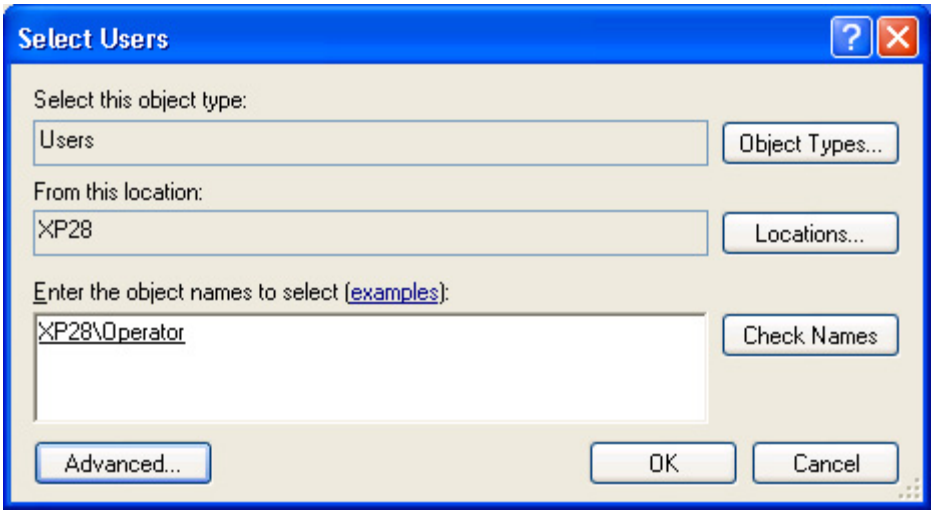
   The Remote Desktop Users dialog box appears, which shows the users authorized to connect to the computer to transfer the session.

Figure 254 - Remote Desktop Users Window

5. Click Add.

   The Select Users dialog box appears, from which you can authorize users.

Figure 255 - Select Users Window



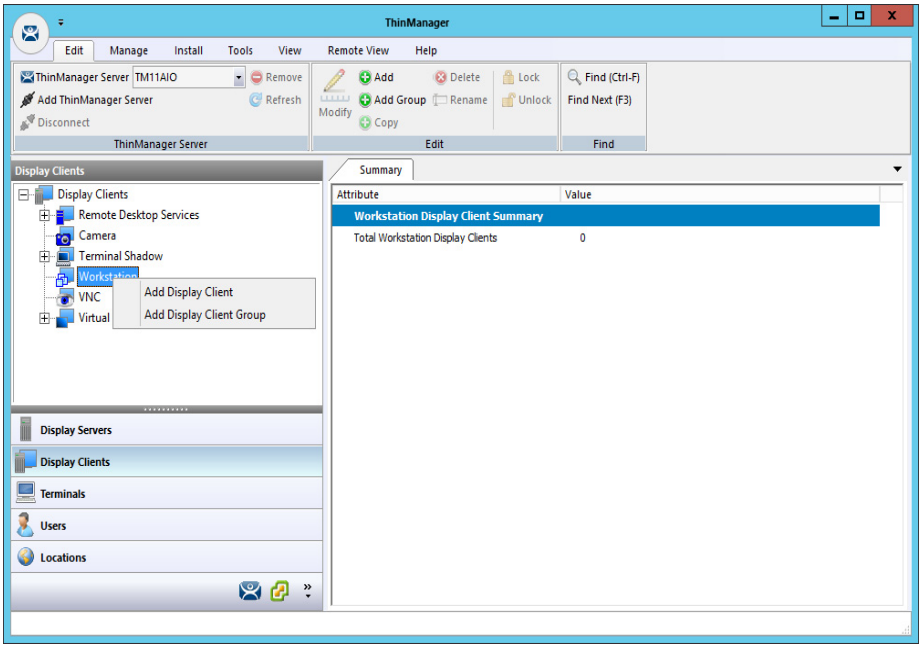
6. Enter the desired users to the text box.
7. Click Check Names to validate the users you entered.
8. Click OK to add the users.
9. Close all the windows to finish the tasks.

Step 2 – Workstation Display Client

Create a Workstation Display Client to act as a template for workstation deployment. The Workstation Display Client gets assigned to a specific workstation when it is applied to a terminal.

1. Open ThinManager to the Display Clients tree.

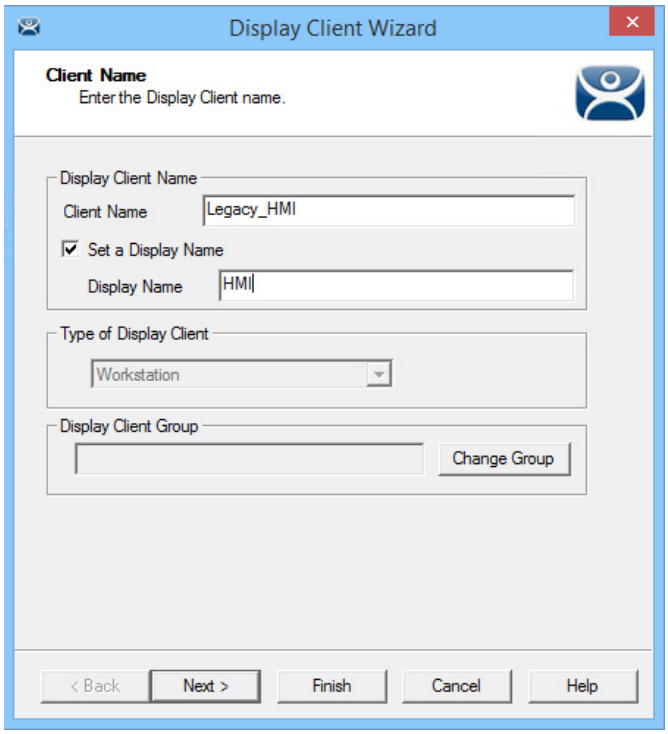
Figure 256 - Access the Workstation Display Client Wizard



2. Right-click on the Workstation branch of the Display Clients tree of ThinManager and choose Add Display Client.

   The Client Name page of the Workstation Display Client Wizard appears.

Figure 257 - Client Name Page

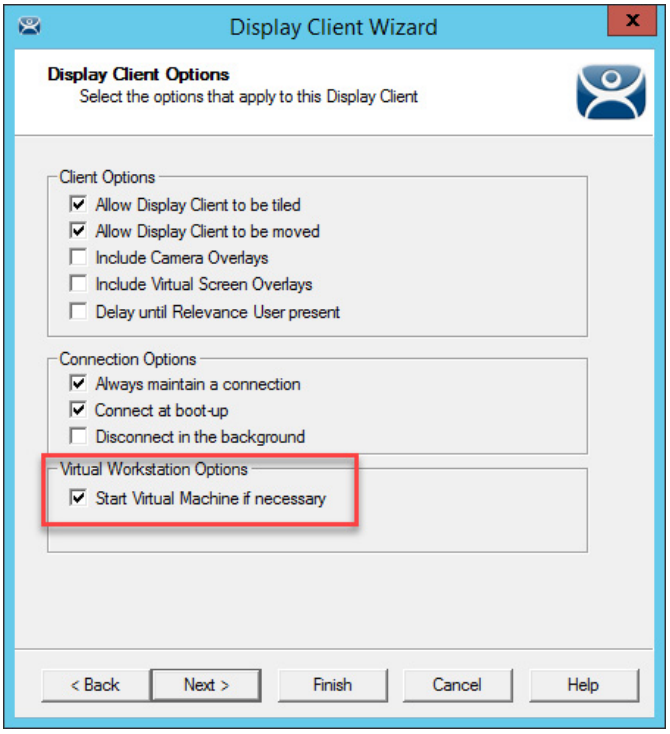


The Client Name Page of the Workstation Display Client wizard is similar to other Display Client Option pages.

3. Enter a unique name and select the Next button.
4. (Optional) Check Set a Display Name to show an alternative name in the ThinManager Server tree.
5. Click Next.

   The Display Client Options page of the Workstation Display Client Wizard appears, which is similar to other Display Client Options pages except for the Start Virtual Machine if necessary checkbox.

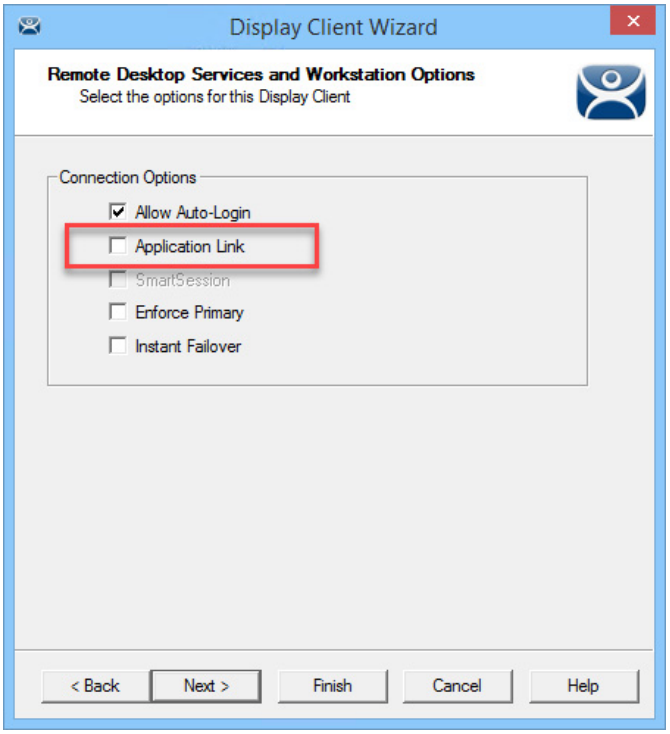
Figure 258 - Display Client Options Page



6. (Recommended) Check Start Virtual Machine if necessary.
7. Click Next.

   The Remote Desktop Services and Workstations Options page of the Workstation Display Client appears, which is similar to other display clients wizards.

Figure 259 - Remote Desktop Services and Workstation Options Page

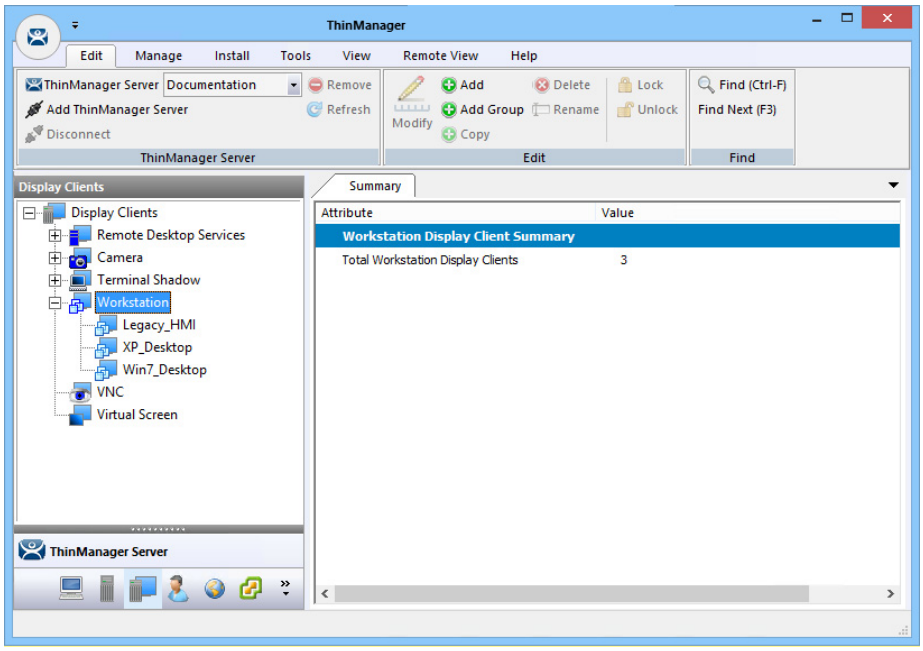


8. Leave the Application Link checkbox cleared in order to deploy the workstation as a desktop.

9. Click Finish to close the wizard.

   The completed display clients are displayed in the Workstation branch of the Display Clients tree.

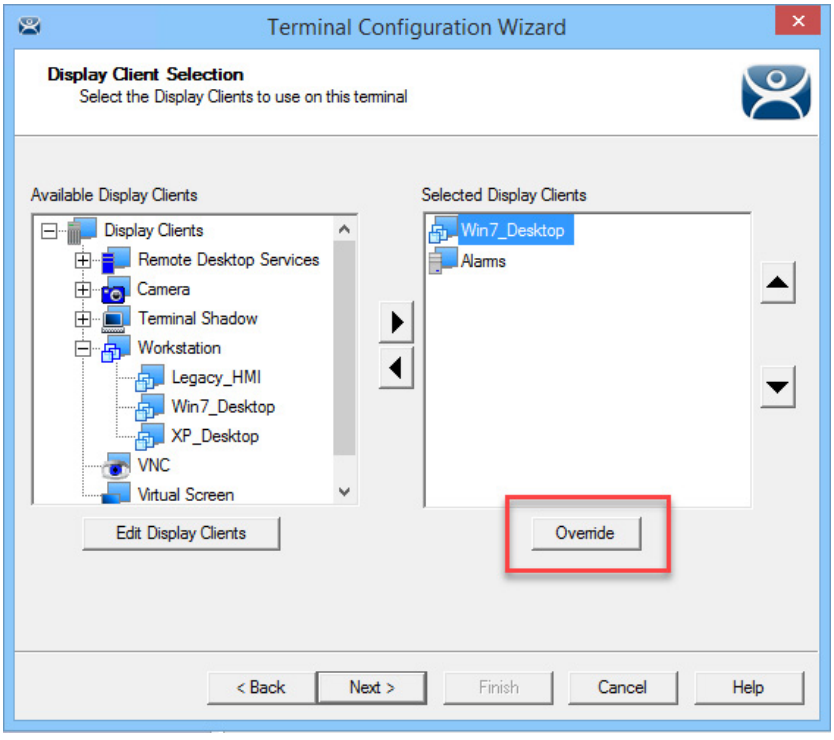
Figure 260 - Workstations in the Display Client Tree



Add the Workstation Display Client to the Terminal

1. Double-click on the Terminal in the Terminal branch of the ThinManager tree to open the Terminal Configuration Wizard.
2. Click Next until the Display Client Selection page appears.

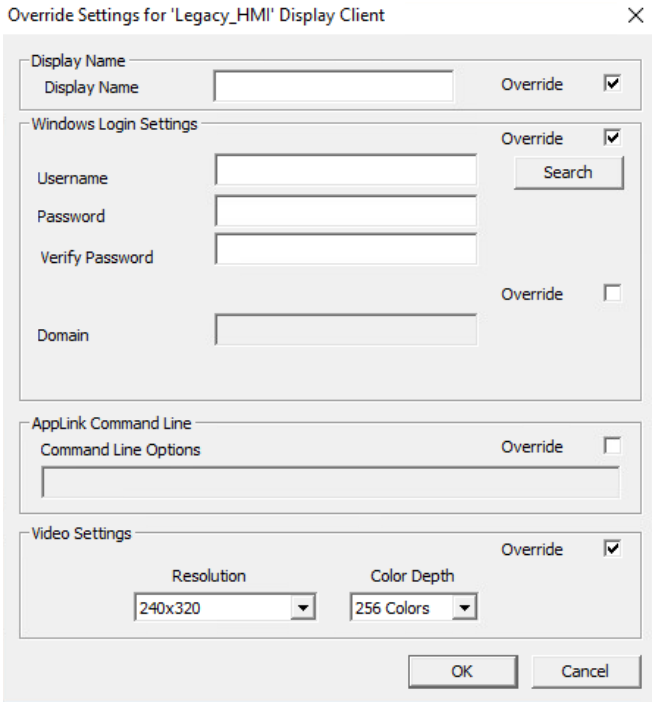
Figure 261 - Display Client Selection Page



3. Highlight the workstation to be added and click the right-facing arrow to add it to the Selected Display Clients list.
   a. If the workstation uses a different Windows account than the Terminal, highlight the workstation in the Selected Display Clients list, and then click Override to change the Windows account that is used for logging in.

      The Override Settings dialog box appears.

Figure 262 - Override Settings



   b. Check Override in the Windows Login Settings section and enter the workstation's correct user account credentials to the Username and Password fields. Enter the credentials manually or click Search.

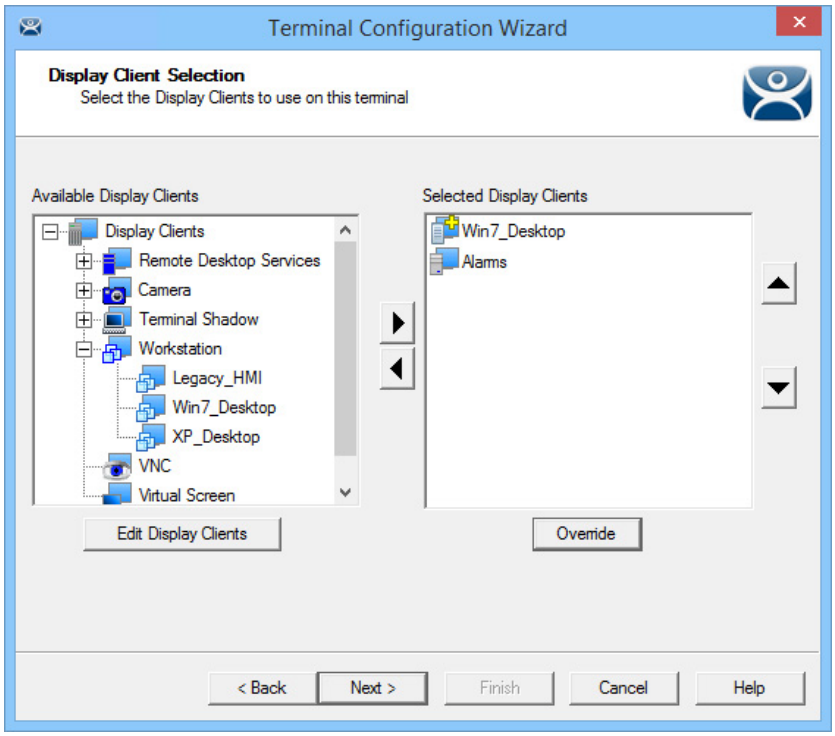
      The Search for AD User dialog box appears. Search pulls a user account from the Active Directory as shown on page 65.

   c. Check Override in the Video Settings section to choose Resolution and Color Depth from the pull-down menus.

   d. Click OK to return to the Display Client Selection page.

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

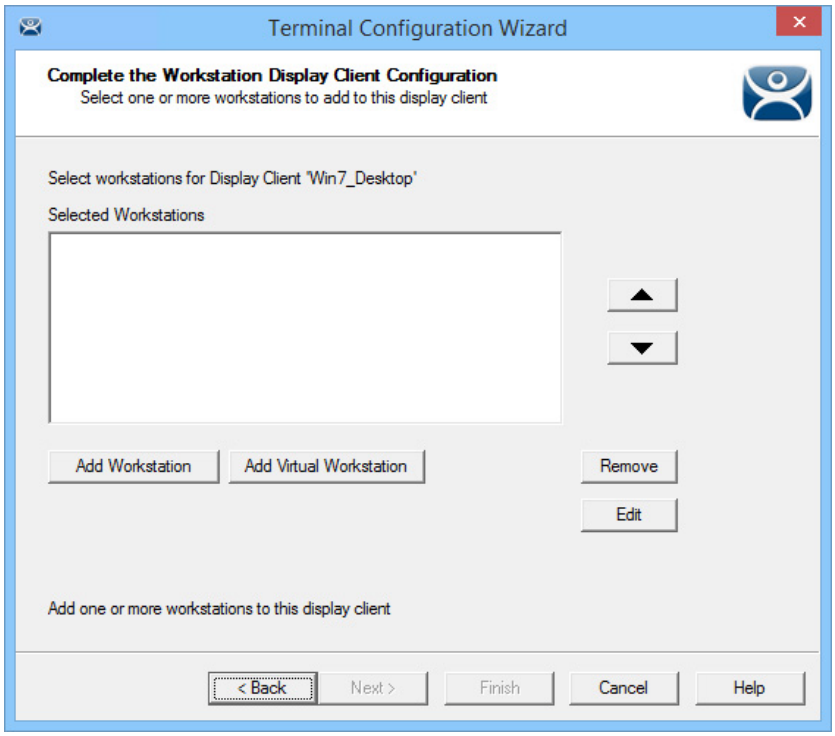
Figure 263 - Override Indicator



4. Click Next.

   The Workstation Display Client shows a new page—the Complete the Workstation Display Client Configuration Page appears, 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.

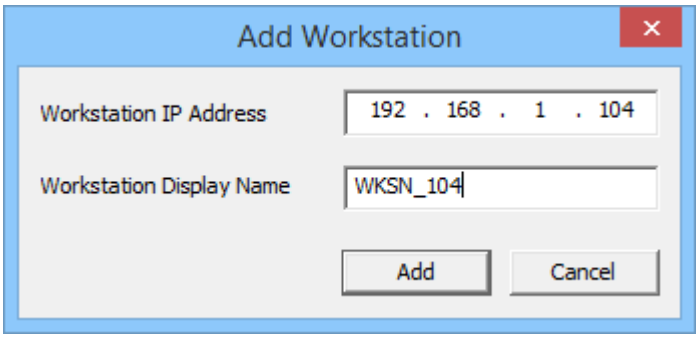
Figure 264 - Complete the Workstation Display Client Configuration Page



5. Click Add Workstation to add a physical workstation.

The Add Workstation dialog box appears, which allows you to specify a workstation by IP address and name.

Figure 265 - Add Workstation



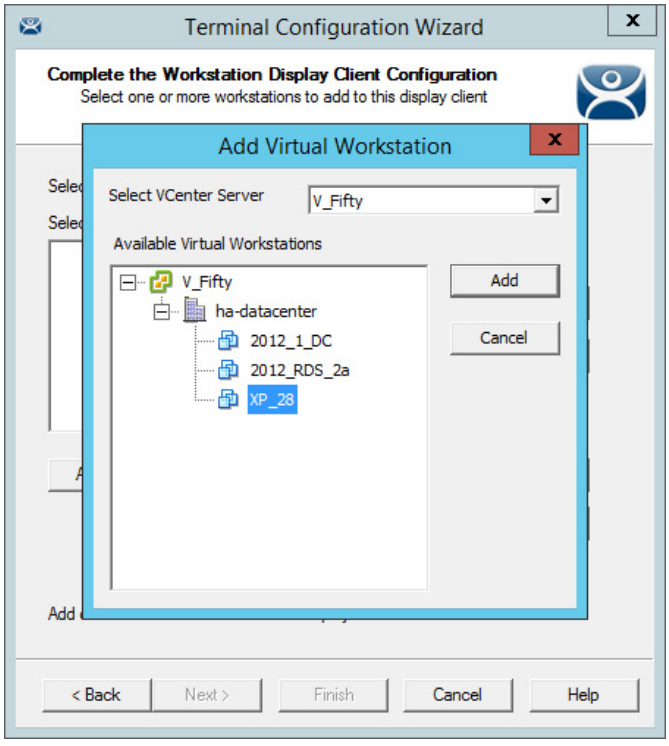
6. Complete the Workstation IP Address and Workstation Display Name fields.

   You may also use this dialog box to point to a virtual workstation. Complete the fields with the virtual machine's IP address and name.

7. Click Add.
8. (Optional) If your virtual machines are on a vCenter Server that is defined in ThinManager, click Add Virtual Workstation button on the Complete the Workstation Display Client Configuration page.

   The Add Virtual Workstation dialog box appears, which is populated by any VCenter Servers you have defined in ThinManager.

Figure 266 - Add Virtual Machine



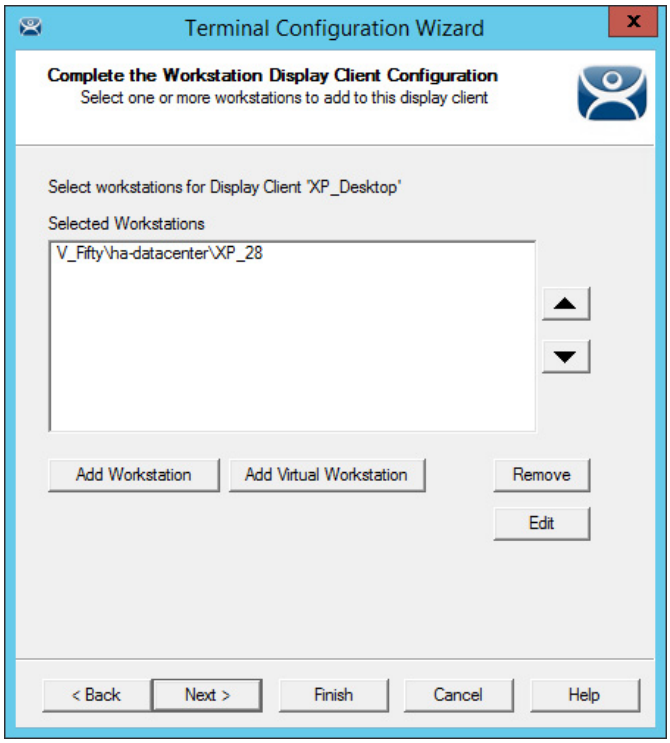
   a. Choose the vCenter Server from the Select vCenter Server pull-down menu.

   b. From the Available Virtual Workstations pane, expand the VCenter tree.

   c. Highlight the desired virtual workstation and click Add.

The workstation appears in the Selected Workstations pane on the Complete the Workstation Display Client Configuration page.

Figure 267 - Complete the Workstation Display Client Configuration Page

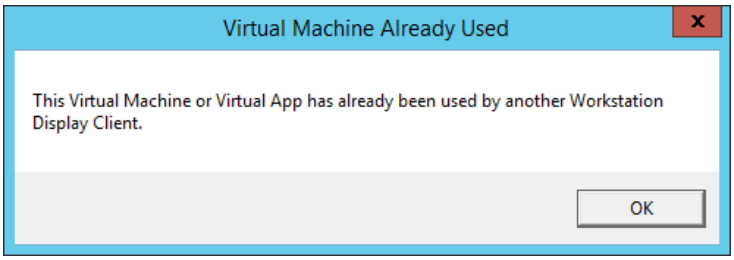


d. (Optional) Add a second workstation as a backup, if desired.

Workstations can have only one connection to a remote user as 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. A dialog box appears if a duplicate workstation is added.

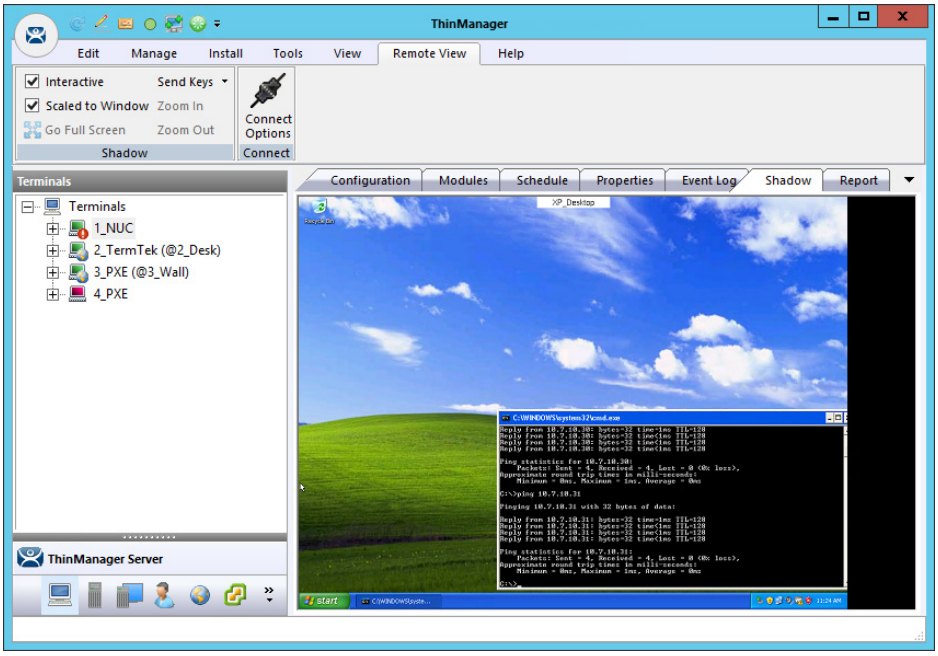
Figure 268 - Duplicate Workstation Warning



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

Once the Workstation Display Client is added to a Terminal and the Terminal is restarted, the Terminal connects to the workstation and transfers the workstation display to the Terminal.

Figure 269 - XP Workstation on a Thin Client



VNC Shadow

ThinManager can connect to a VNC Server and send the VNC shadow to a Terminal as a VNC Display Client.

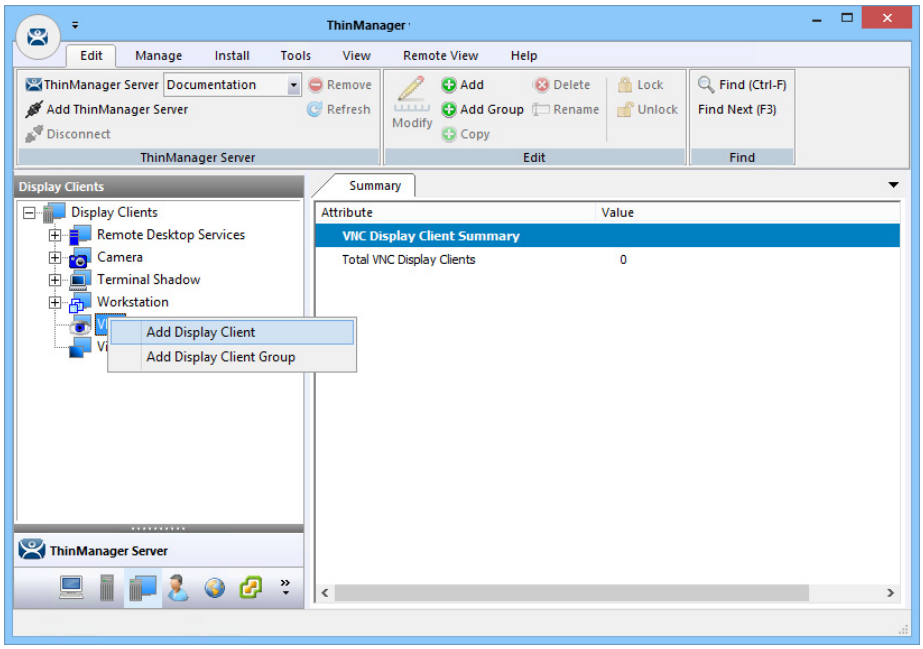
In order to do so, follow these steps.

1. Define the VNC Server as a Display Server source as shown in VNC Servers on page 122.
2. Create a Display Client to deploy the source on a client.

Shadow Any VNC Server

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

Figure 270 - Display Clients Tree

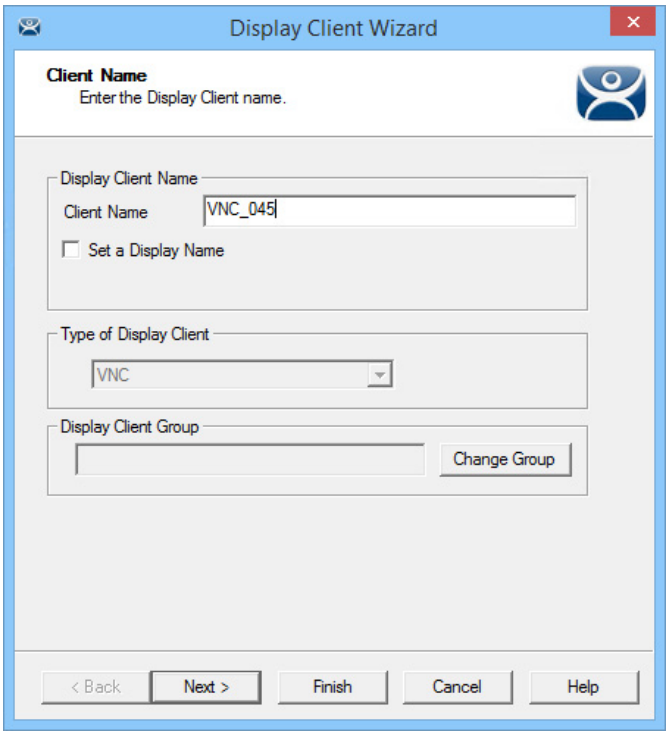


To shadow any VNC server, follow these steps.

1. Right-click on the VNC branch of the Display Clients tree and choose Add.

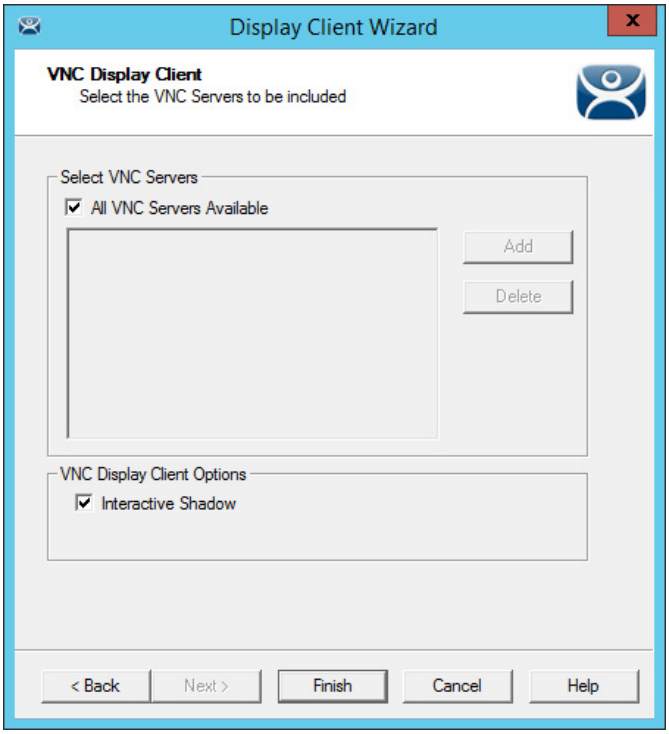
   The Display Client Wizard appears.

Figure 271 - VNC Display Client



2. Enter a Client Name and follow the wizard like other display clients.
3. (Optional) Click Set a Display Name to configure the display client to display an alternative name in the ThinManager Server tree.

4. Click Next until the VNC Display Client page appears.

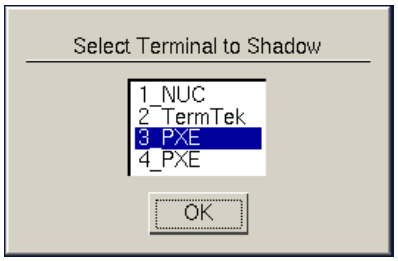


5. Click All VNC Servers Available to make all VNC servers available to shadow.
6. (Optional) Clear the Interactive Shadow checkbox to turn it off.
7. Click Finish to create the display client.

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

When you choose a VNC display client with multiple VNC servers, a menu that lists all available VNC servers appears.

Figure 272 - VNC Server Menu



8. Highlight the desired VNC server and click OK.

   The VNC server you chose is shadowed.

Shadow a Specific VNC Server

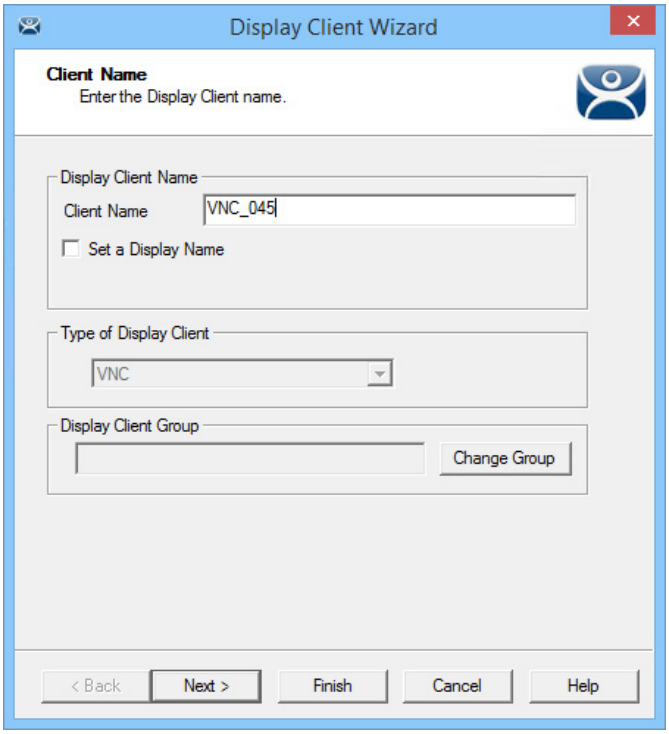
The VNC Display Client can be configured to show the output from a specific VNC server.

To configure a VNC Display Client to shadow a specific VNC server, complete these steps.

1. Right-click on the VNC branch of the Display Clients tree and choose Add Display Client.

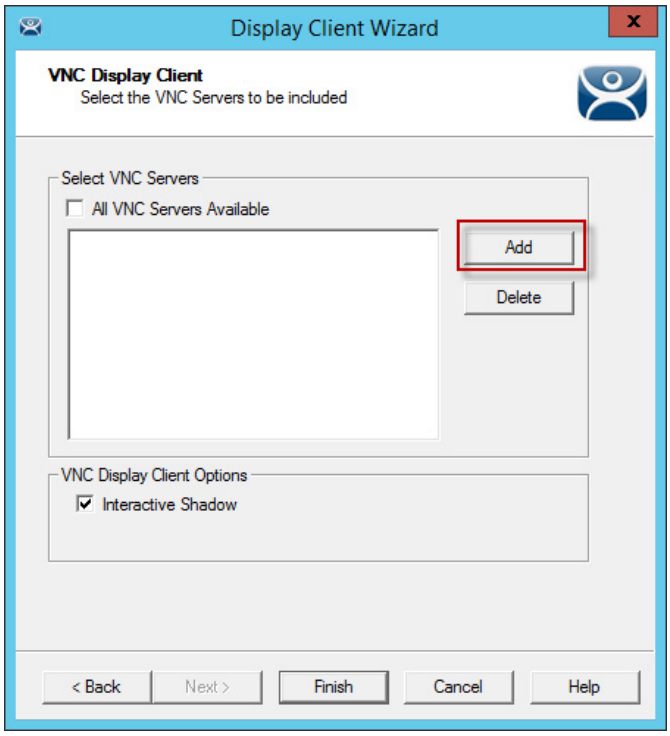
   The Display Client Wizard for Terminal Shadow appears.

Figure 273 - VNC Display Client Wizard



2. Complete the Client Name field.
3. (Optional) Click Set a Display Name to configure the display client to display an alternative name in the ThinManager Server tree.
4. (Optional) Click Change Group to put the display client into a group.
5. Click Next to follow the wizard like other display clients.

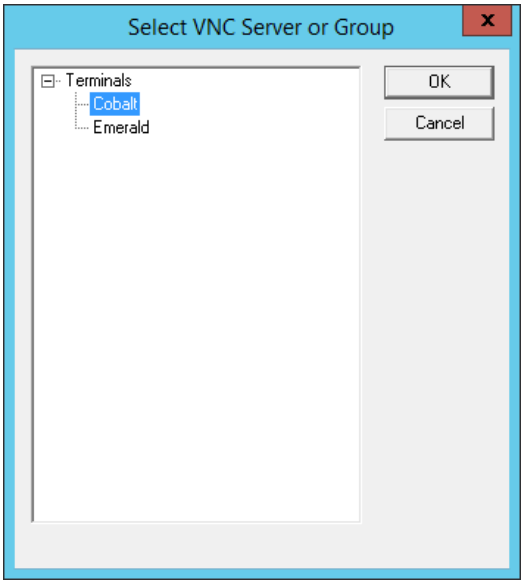
Figure 274 - VNC Display Client Page



6. Clear the All VNC Servers Available checkbox.
7. Click Add.

   The Select VNC Server or Group dialog box appears.

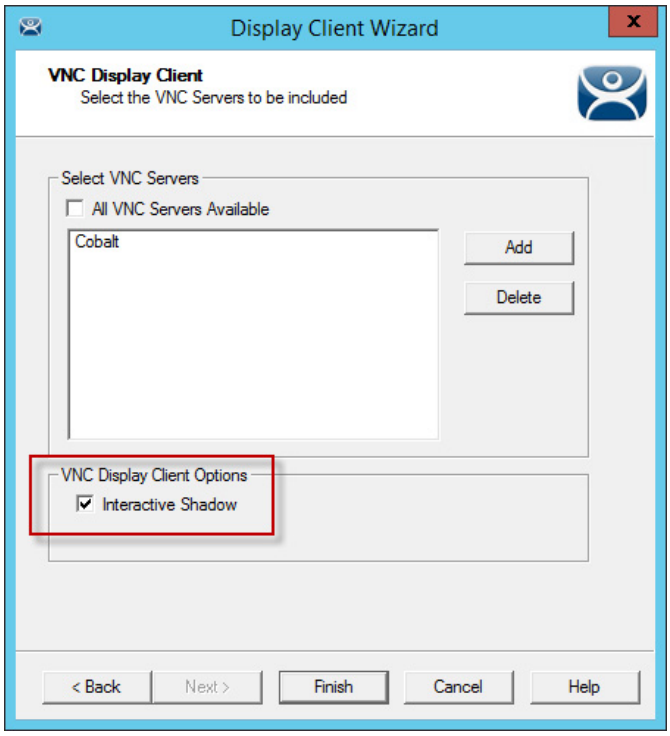
Figure 275 - Select VNC Server of Group



8. Highlight the VNC server you want to shadow and click OK.

   The chosen VNC server is added to the list to shadow on the VNC Display Client page.

Figure 276 - Chosen Server Added to VNC Display Client Page



9. (Optional) Click Add to repeat the process and add other VNC servers.
10. Click Finish to create the display client when done.
11. Clear the Interactive Shadow checkbox to turn it off. This puts the shadow in a read-only mode.

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

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

Virtual Screens

This 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.

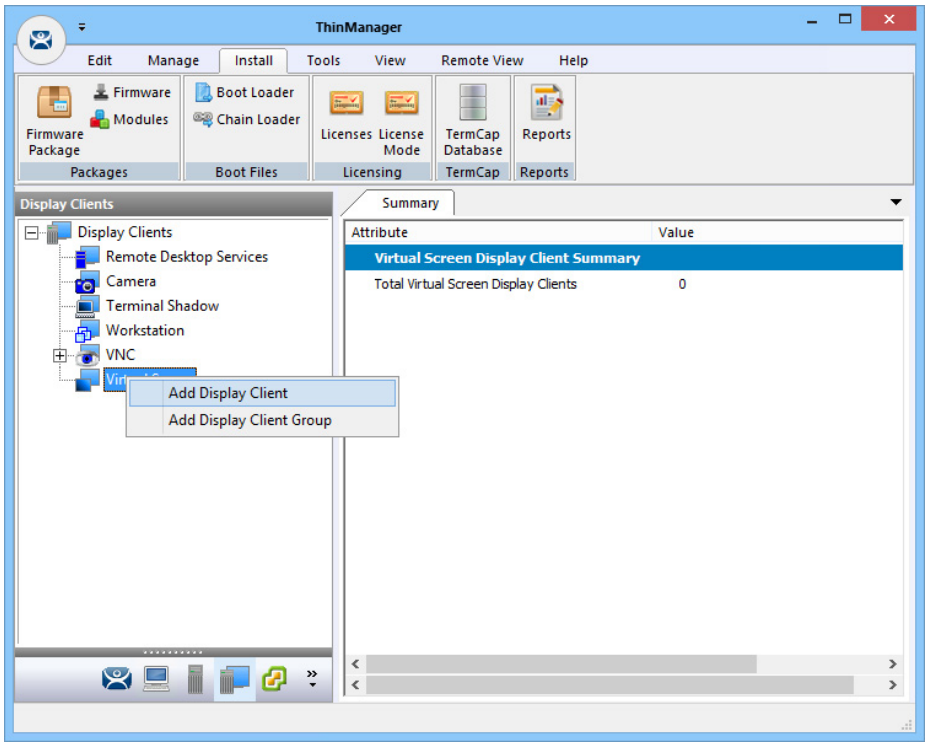
Virtual Screen Display Client Wizard

Virtual Screens are defined using the Display Client Configuration Wizard.

To define Virtual Screens, follow these steps.

1. Click the Display Clients icon at the bottom of the ThinManager tree.

Figure 277 - Launch the Virtual Screen Wizard

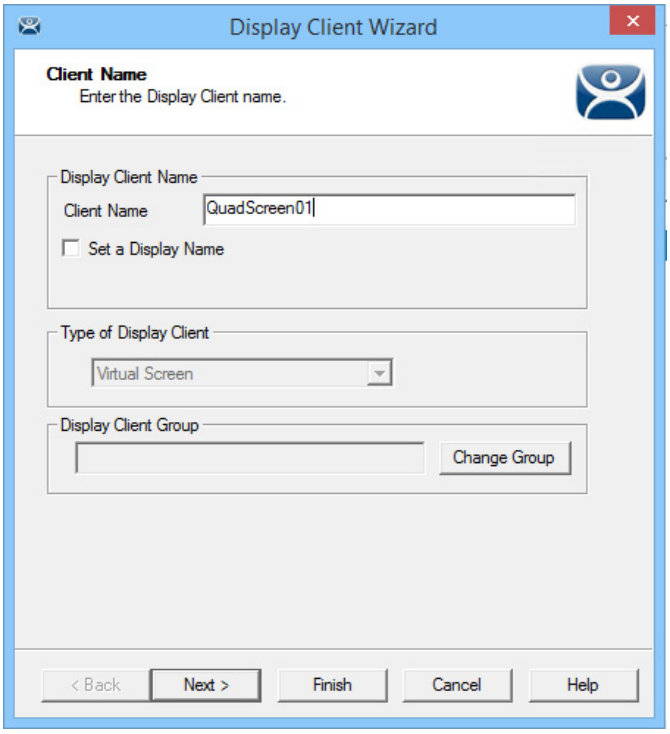


2. Right-click on the Virtual Screen branch, and choose Add Display Client.

   The Client Name page of the Display Client Wizard appears.

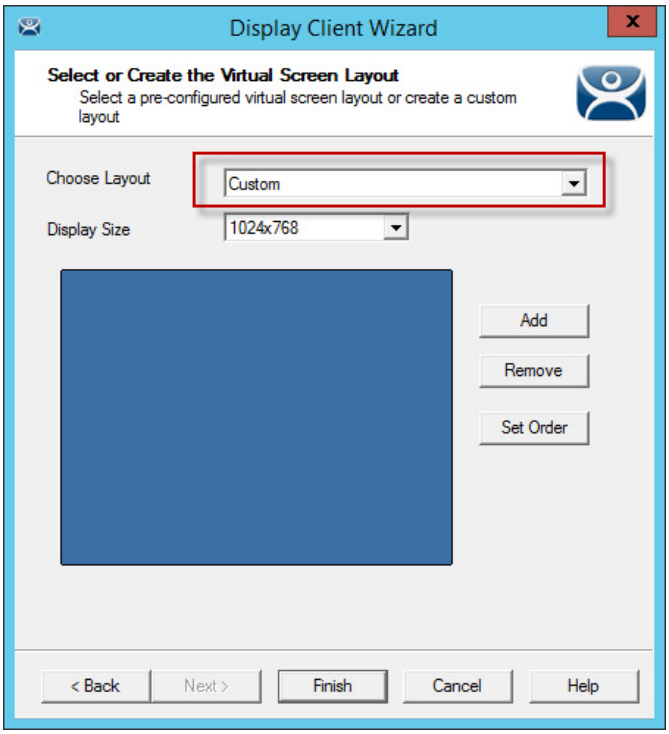
   The wizard starts like the Remote Desktop Services Display Client Wizard, but changes at the Select or Create the Virtual Screen Layout page.

Figure 278 - Client Name Page of the Display Client Configuration Wizard



3. Complete the Client Name field to name your display client.
4. Click Next to continue through the wizard until the Select or Create the Virtual Screen Layout page appears.

Figure 279 - Select or Create the Virtual Screen Layout Page



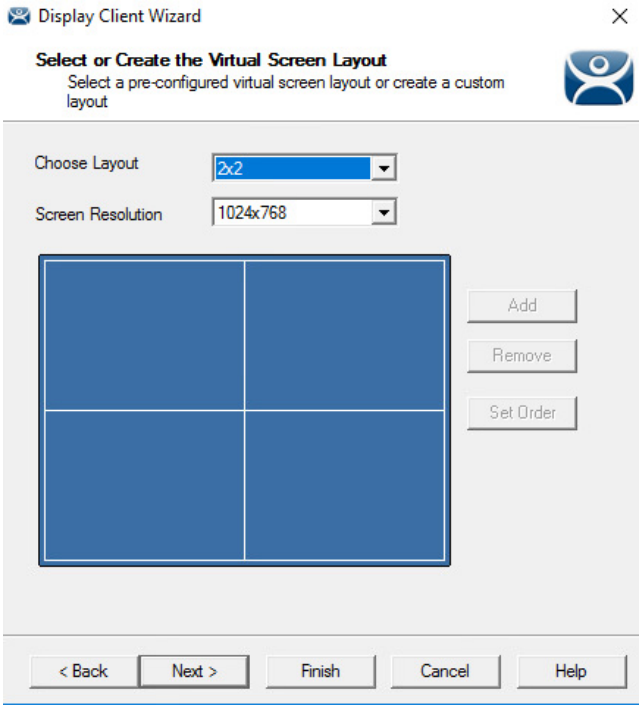
5. Complete the page per the following descriptions.

Setting	Description
Choose Layout	Use the pull-down menu to choose from templates or Custom, which requires the addition of at least one overlay via Add. See Predefined Templates on page 208 and Custom Overlays on page 216 for more information.
Screen Resolution	Use the pull-down menu to choose the of the Virtual Screen display client.
Add	Launches the Custom Overlay dialog box, which allows customer overlays to be defined.
Remove	Removes a highlighted overlay.
Set Order	Launches the Set Stacking Order of Virtual Screens dialog box, which allows the screens to be prioritized.

Predefined Templates

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

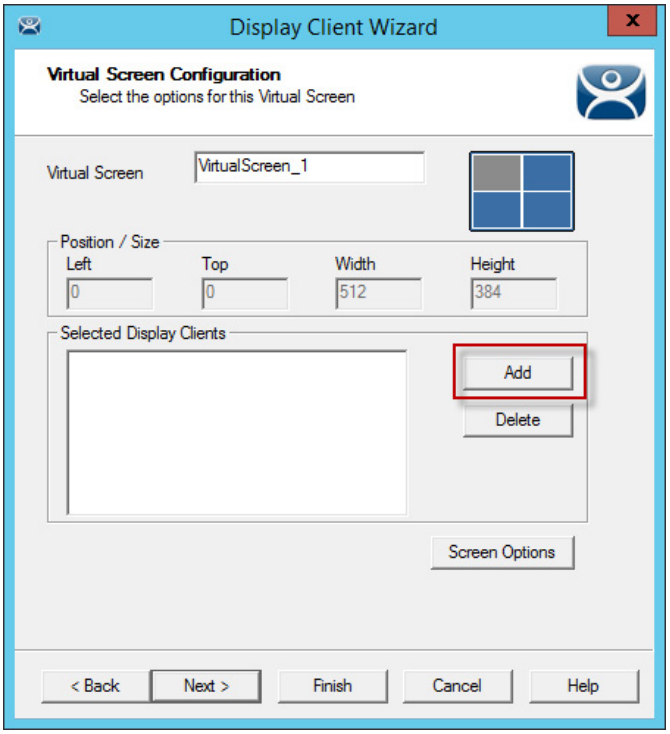
Figure 280 - Select or Create the Virtual Screen Layout Page



1. Choose a template from the Choose Layout pull-down menu.
2. Choose a display resolution from the Screen Resolution pull-down menu.
3. Click Next.

   The Virtual Screen Configuration page appears.

Figure 281 - Virtual Screen Configuration Page

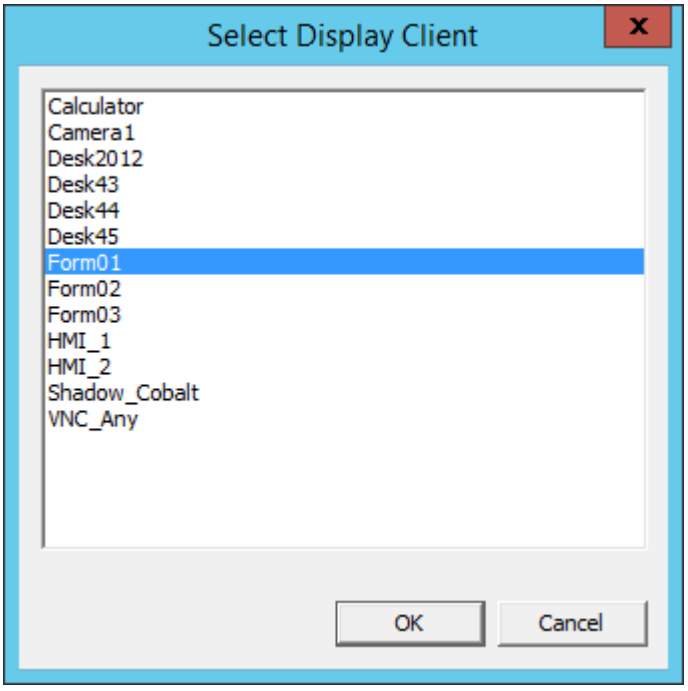


The wizard allows display clients to be added to each overlay.

4. Click Add to add a Display Client to the overlay.

   The Select Display Client dialog box appears, which lists all display clients.

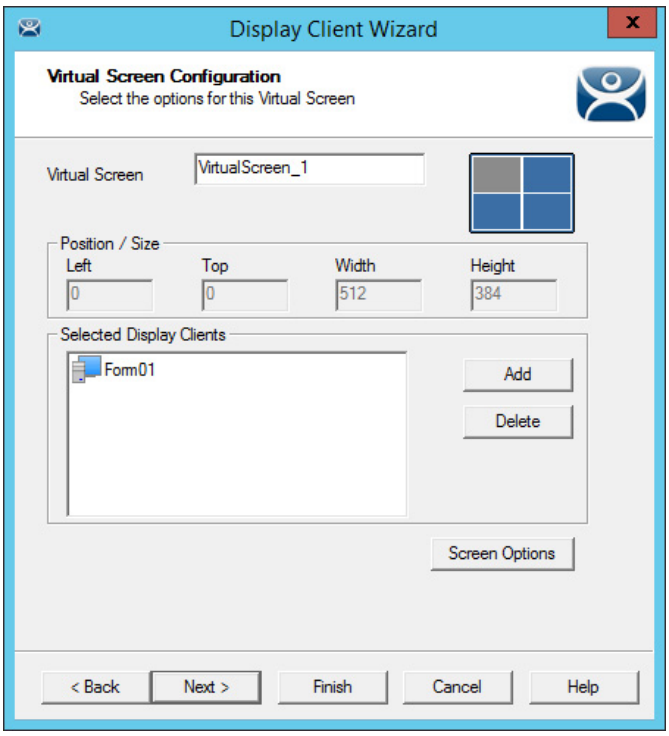
Figure 282 - Select Display Client Dialog



5. Highlight the desired Display Client and click OK.
6. Repeat as needed for the overlay.

The Display Client appears in the Selected Display Clients field. Each overlay may have one or more display clients in the overlay.

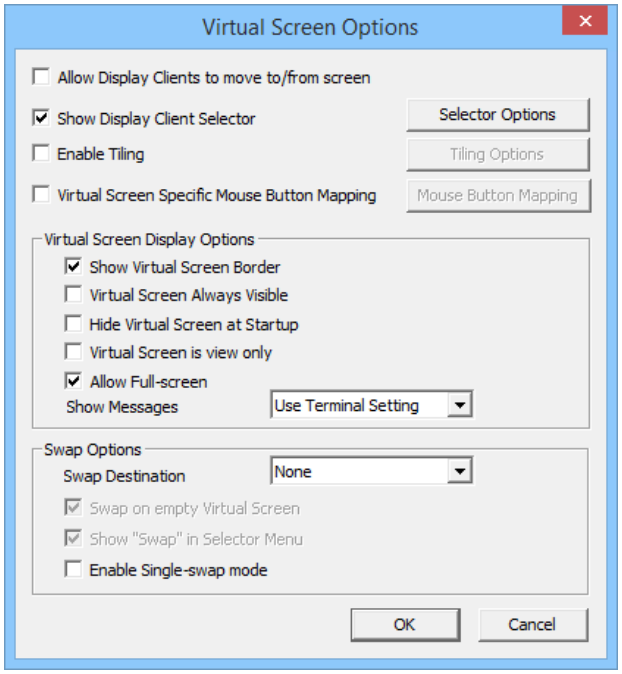
Figure 283 - Virtual Screen Configuration Showing Applied Display Client



7. Click Add to add more display clients.
8. (Optional) Highlight a display client and click Screen Options to apply virtual screen options.

   The Virtual Screen Options dialog box appears.

Figure 284 - Virtual Screen Options



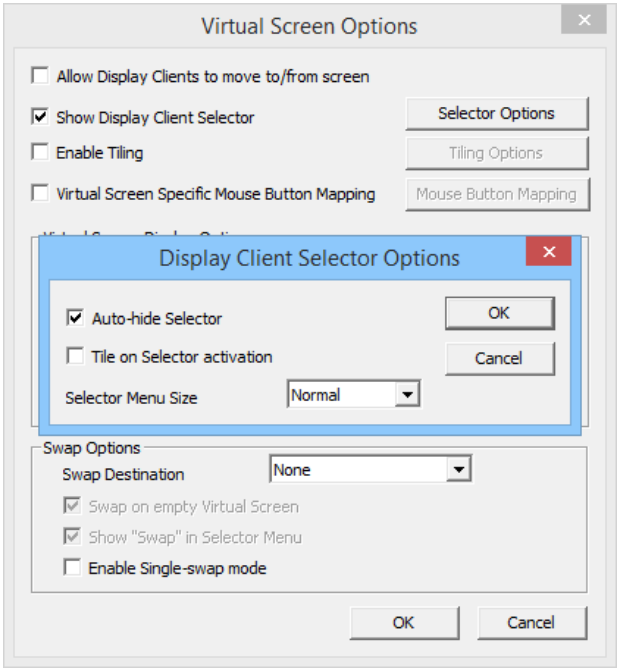
9. Choose the Virtual Screen Options per the following descriptions.

Option	Description
Allow Display Clients to move to/from screen	Allows movement of a display client from one overlay to the other, much like the movement of display clients between monitors on a MultiMonitor thin client.
Show Display Client Selector	Shows the pull-down selector at the top of the overlay. Click Selector Options to configure.
Selector Options	Use to configure selector options.
Enable Tiling	Allows tiling of Display Clients within the overlay if you have multiple display clients.
Tiling Options	Use to configure tiling options.
Virtual Screen Specific Mouse Button Mapping	Enables Mouse Button Mapping to configure the mouse with use with the Virtual Screens.
Mouse Button Mapping	Use to define mouse buttons as hotkeys.
Virtual Screen Display Options	
Show Virtual Screen Border	Shows a border between the overlays.
Virtual Screen Always Visible	If the user switches to a different display client, this overlay remains visible even though its display client is hidden.
Hide Virtual Screen at Startup	Hides the Virtual Screen at startup. It is intended to be used with the TermMon ActiveX, which toggles the overlay visibility.
Virtual Screen is view only	Displays the Display Client in the Virtual Screen, but makes it view-only and not interactive.
Allow Full-screen	Allows a Display Client to appear full screen and not show the sidebar.
Show Messages	Allows for control of the status message shown in the upper-left corner of the Terminal display.
Use Terminal Setting	Sets the Virtual Screen to follow the configuration of the Terminal.
Yes	Turns on the status messages.
No	Turns off the status messages.
Swap Options	
Swap Destination	Allows the location of the Virtual Screen, moved during a swap, to be specified.
Swap on empty Virtual Screen	Move the highlighted Virtual Screen to an empty Virtual Screen when selected from the pull-down Selector.
Show “Swap” in Selector Menu	Adds the Swap option to the pull-down Selector menu.
Enable Single-swap mode	Allows a single mouse click in a Virtual Screen window to initiate the swap.

10. Click Selector Options to configure the selector options.

The Display Client Selector Options dialog box appears.

Figure 285 - Display Client Selection Options



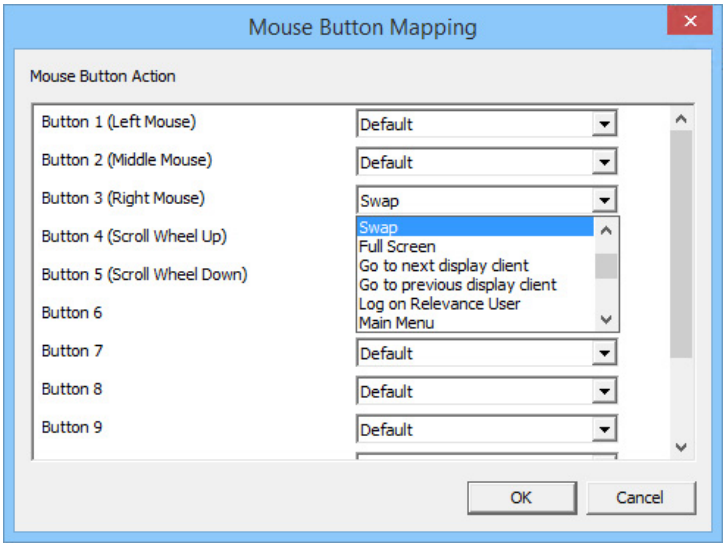
Choose from the following Display Client Selector options.

Option	Description
Auto-hide Selector	Hides the pull-down menu Display Client selector unless the mouse is positioned over it. Clear this checkbox to show the selector at the top-center of the screen.
Tile on Selector activation	Adds the tiling command to the pull-down menu when Auto-hide Selector is checked.
Selector Menu Size	Use this pull-down menu to set the font size of the text in the Display Client selector.

11. Click OK to close the Display Client Selector Options dialog box.
12. Click Virtual Screen Specific Mouse Button Mapping to activate the Mouse Button Mapping button.
    a. Click Mouse Button Mapping.

    The Mouse Button Mapping dialog box appears.

Figure 286 - Mouse Button Mapping Dialog Box



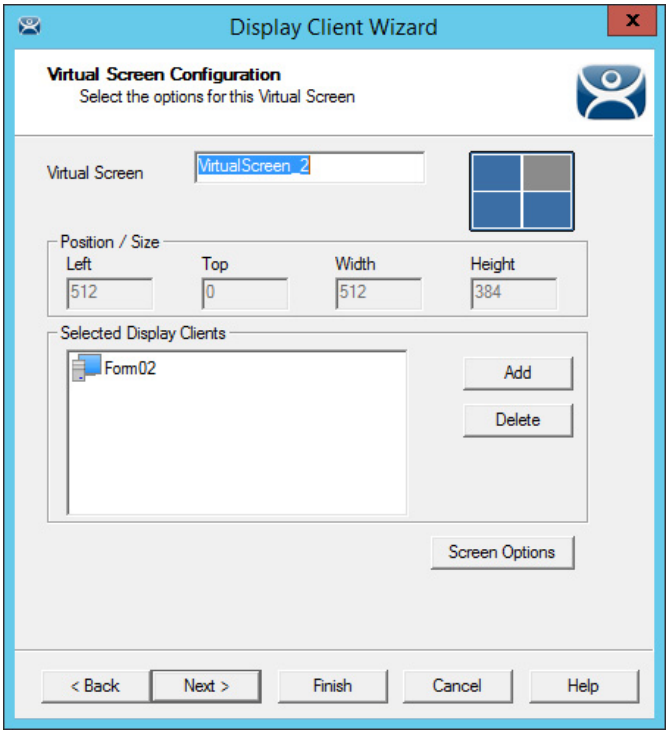
13. Complete the Mouse Button Mapping dialog box per the following settings. Each mouse button can be configured with a different function. Use Button 1 (Left Mouse) for touch screens without a mouse.

Setting	Description
Default	Leaves the button with its original action.
Calibrate Touch Screen	Initiates the touch screen calibration program.
Tile	Initiates the tiling of display clients.
Swap	Exchanges display clients in Virtual Screens.
Full Screen	Expands an overlay to Full Screen.
Go to next display client	Navigates to the next display client in the list.

14. Click Next to continue to the next overlay once all the dialog windows are closed.

The Display Client Wizard navigates from overlay to overlay, which allows you to add display clients to each one.

Figure 287 - Virtual Screen Configuration Page



15. Click Finish when the configuration is done.

Add a Virtual Screen to a Terminal

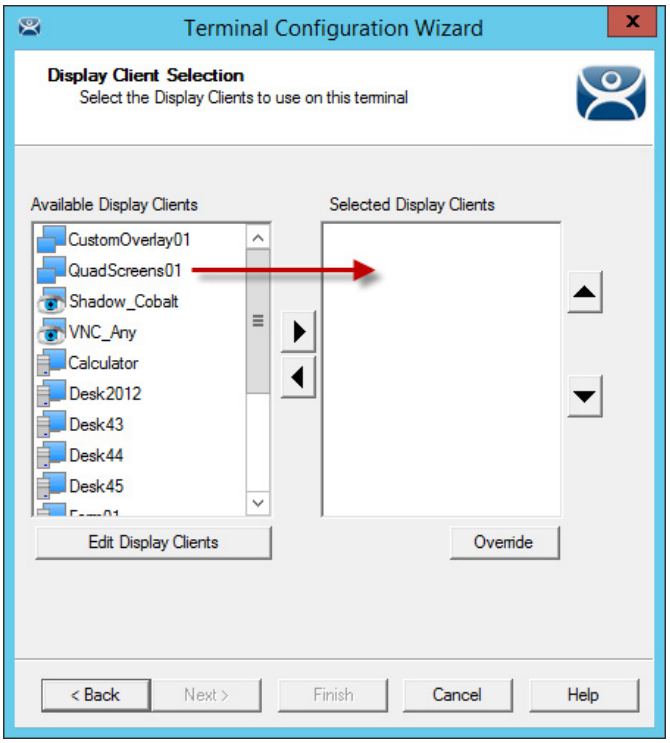
Virtual Screen Display Clients are added to a Terminal as any other Display Client.

1. Double-click on the Terminal in the Terminal tree.

   The Terminal Configuration Wizard appears.

2. Click Next until the Display Client Selection page appears.

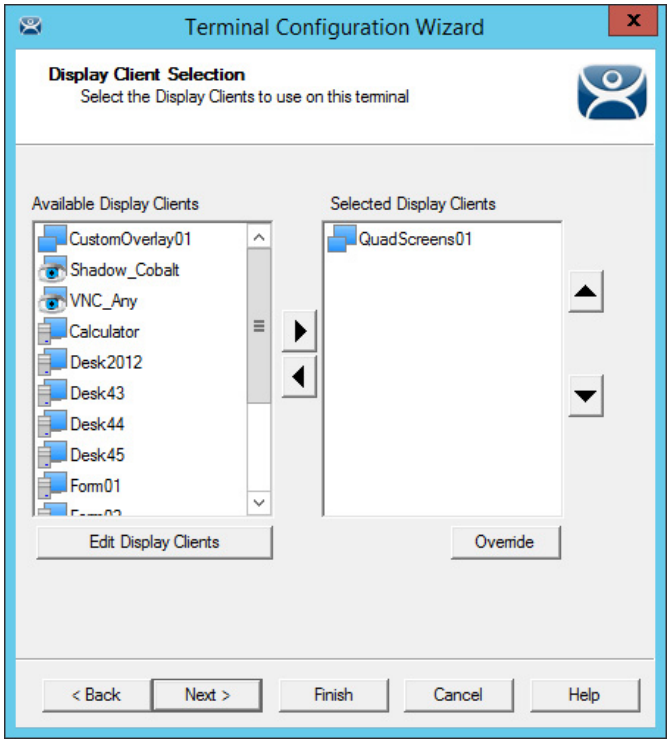
Figure 288 - Display Client Selection Page of the Terminal Configuration Wizard



3. Double-click or highlight the Virtual Screen Display Client in the list of Available Display Clients and click the right-facing arrow to move it to the Selected Display Clients pane.

   Once the Virtual Screen Display Client is in the Selected Display Clients list it is added to the Terminal.

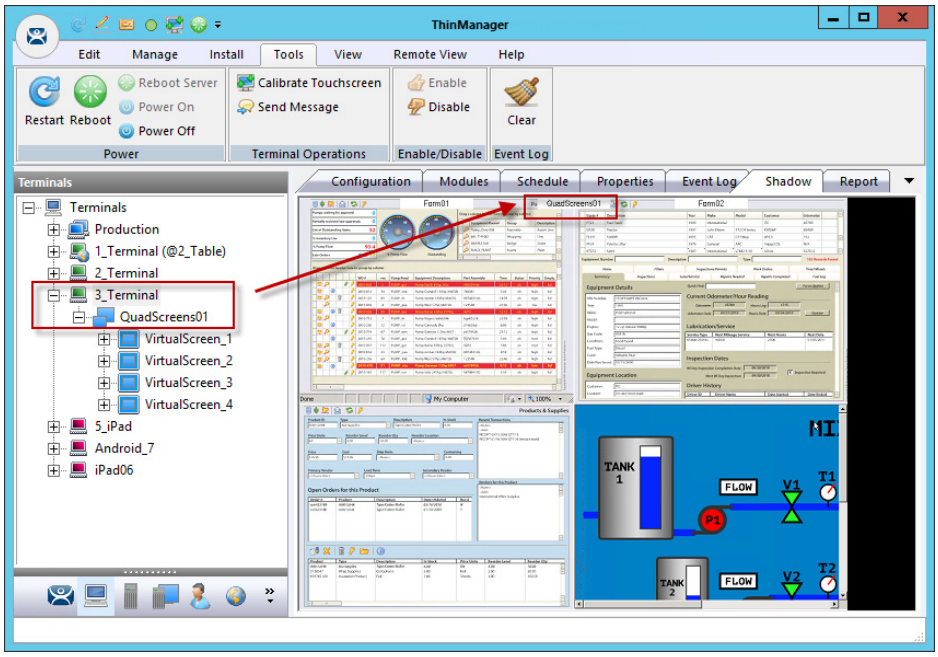
Figure 289 - Selected Display Clients



4. Click Finish and restart the Terminal to apply the change.

Figure 290 shows the QuadScreen01 Virtual Screen Display Client on a Terminal.

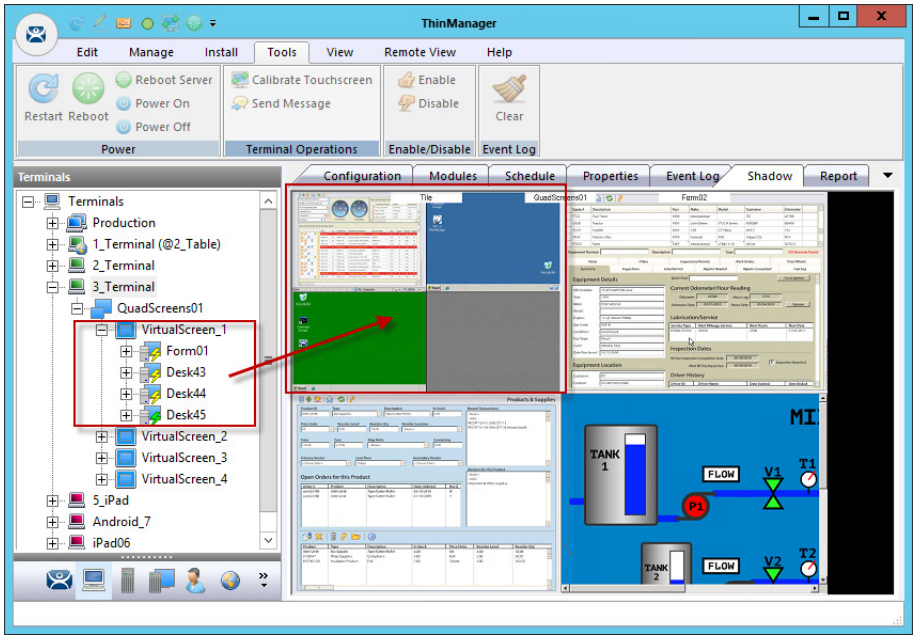
Figure 290 - Virtual Screen on the Terminal



The screen has four virtual screens added and showing.

If Enable Tiling is checked on the Virtual Screen Options dialog box, Figure 306 on page 224, then the display clients in an overlay are tiled as shown here.

Figure 291 - Tiling within an Overlay



Custom Overlays

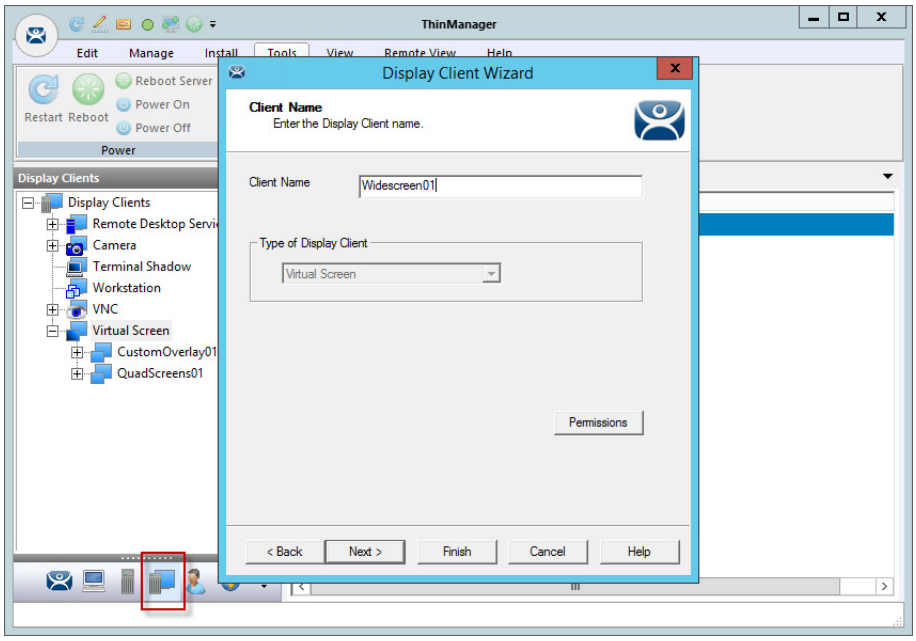
ThinManager provides the option of building and defining custom overlays instead of using the predefined templates. This section shows an example of a custom Virtual Screen display client with four custom overlays.

Define Virtual Screens with the Display Client Configuration Wizard.

1. Click the Display Clients icon at the bottom of the ThinManager tree.
2. Right-click on the Virtual Screen branch and choose Add Display Client.

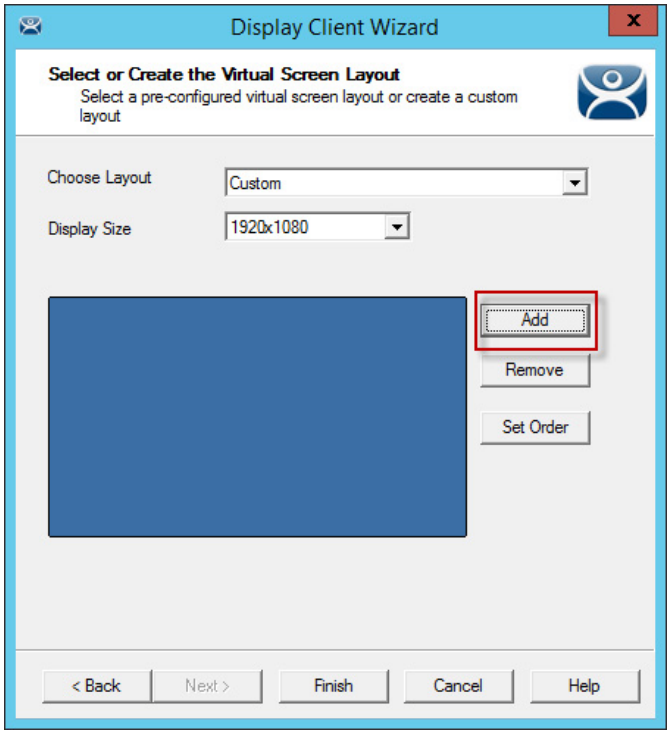
   The Client Name page of the Display Client Wizard appears.

Figure 292 - Display Client Wizard for Virtual Screens



3. Complete the Client Name field to name your display client.
4. Click Next until the Select or Create the Virtual Screen Layout page appears.

Figure 293 - Custom Overlay Layout

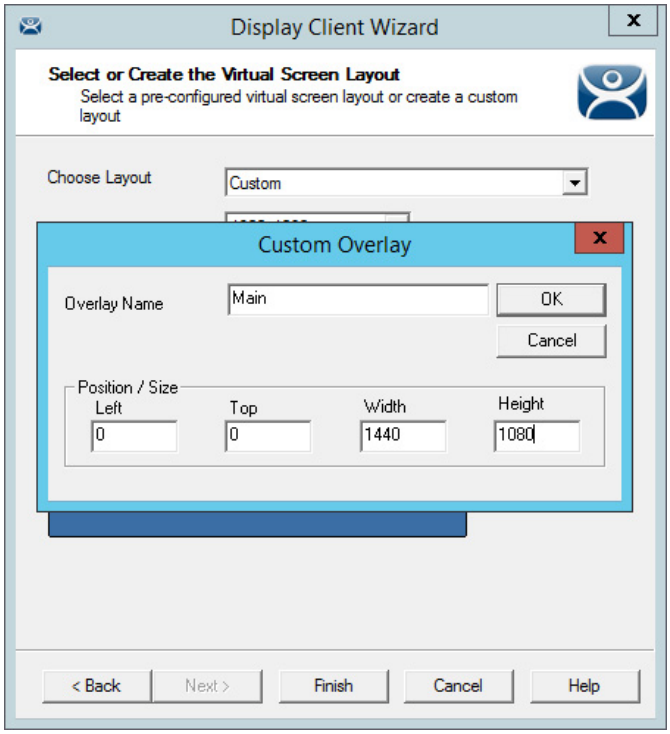


The initial Virtual Screen is a blank canvas and needs at least one overlay added.

5. Click Add.

   The Custom Overlay dialog box appears.

Figure 294 - Custom Overlay Layout



Complete the Custom Overlay field settings per the following descriptions to set the size and location of the custom overlay.

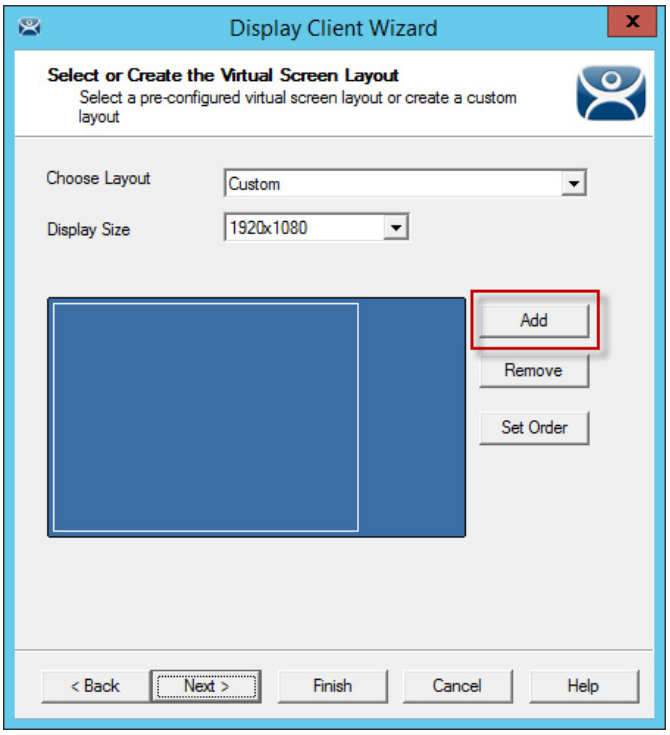
Setting	Description
Overlay Name	Provides a name to the overlay.
Position/Size	
Left	Sets the position of the left edge of the overlay.
Top	Sets the position of the top edge of the overlay.
Width	Sets the width of the overlay.
Height	Sets the height of the overlay.

This example creates a 1440 x 1080 overlay that is touching the upper-left corner.

6. Click OK to accept the settings.

   The created Overlay is shown in Overlay window when done.

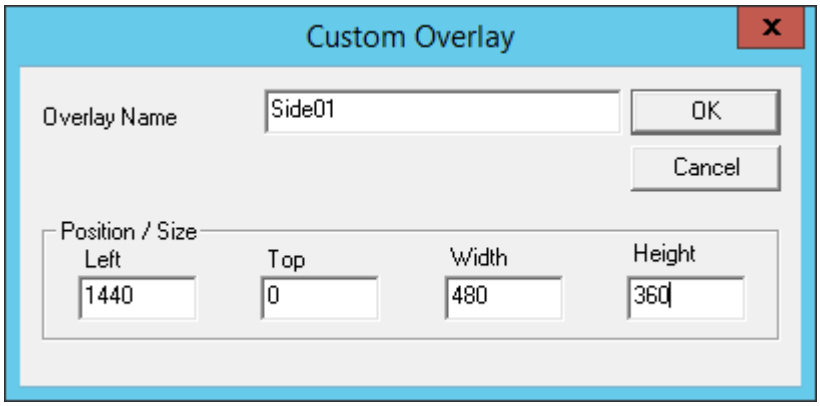
Figure 295 - Created Overlay



7. Click Add.

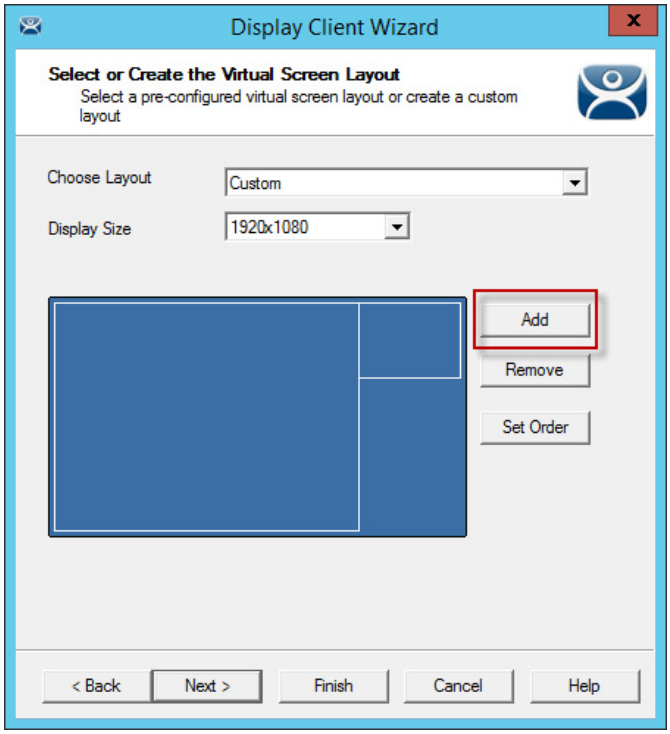
The Custom Overlay dialog box appears again. The example in Figure 296 uses an overlay that is 1440 pixels from the left edge and has a screen resolution of 480 x 360 pixels.

Figure 296 - Custom Overlay #2



8. Click OK to accept the settings.

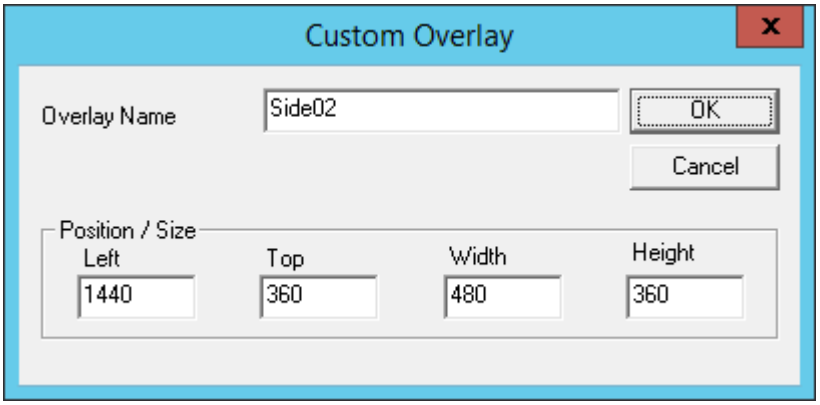
Figure 297 - Display of Created Overlay



9. Click Add.

The Custom Overlay dialog box appears for the next overlay.

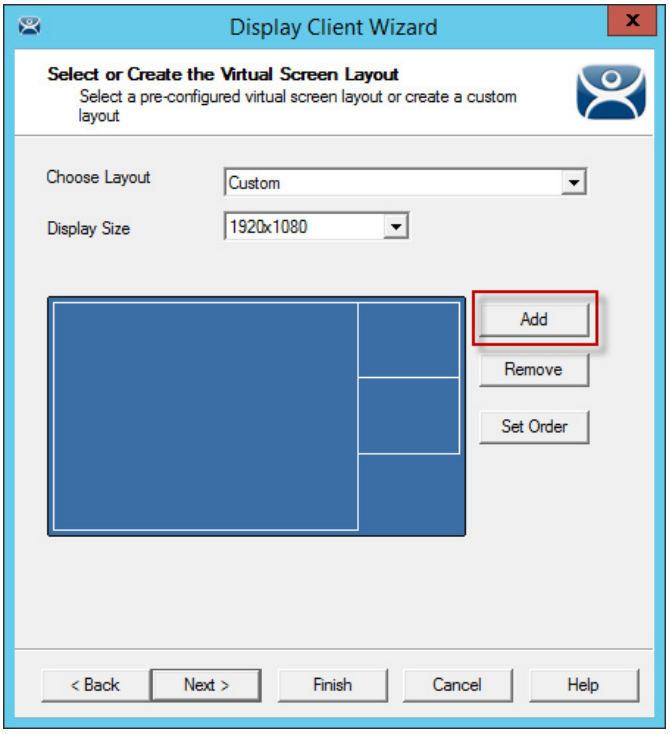
Figure 298 - Custom Overlay #3



This example uses an overlay that is 1440 pixels from the left edge, 360 pixels from the top, and has a screen resolution of 480 x 360 pixels.

10. Click OK to accept the settings and return to the Select or Create the Virtual Screen Layout page.

Figure 299 - Display of Created Overlay



11. Click Add to launch the Custom Overlay dialog box for the next overlay.

Figure 300 - Custom Overlay #4

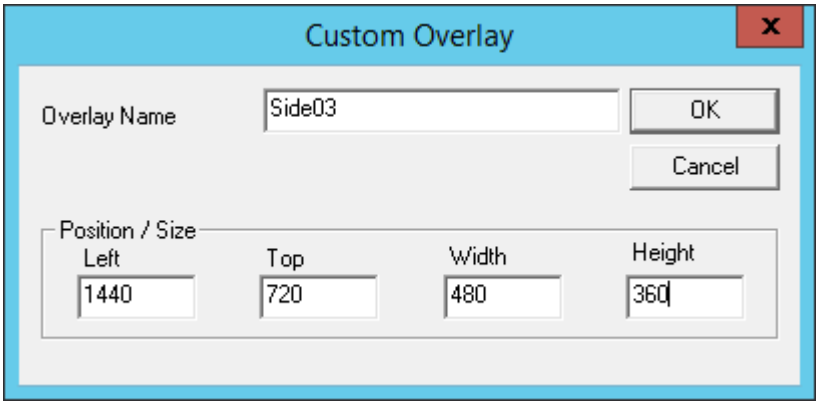


Figure 300 uses an overlay that is 1440 pixels from the left edge, 720 pixels from the top, and has a screen resolution of 480 x 360 pixels.

12. Click OK to accept the settings and return to the Select or Create the Virtual Screen Layout page.

Figure 301 - Display of Created Overlay

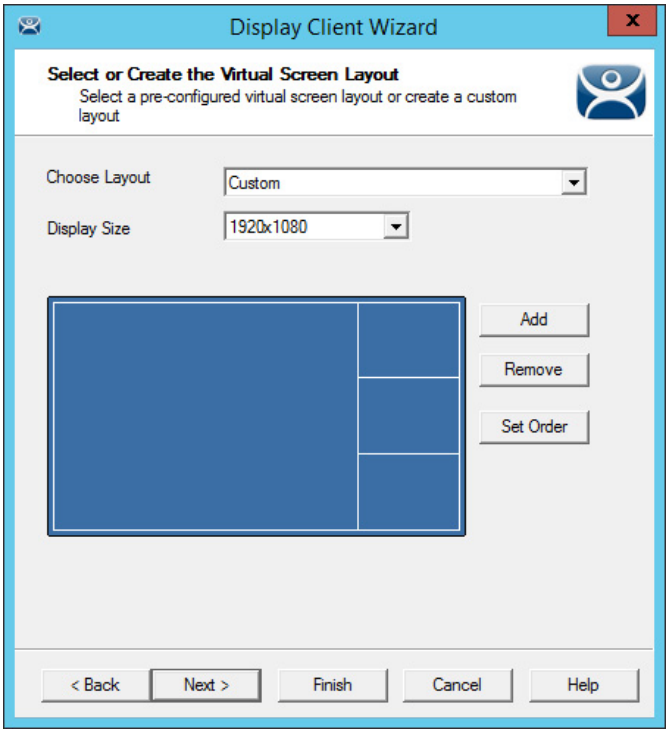
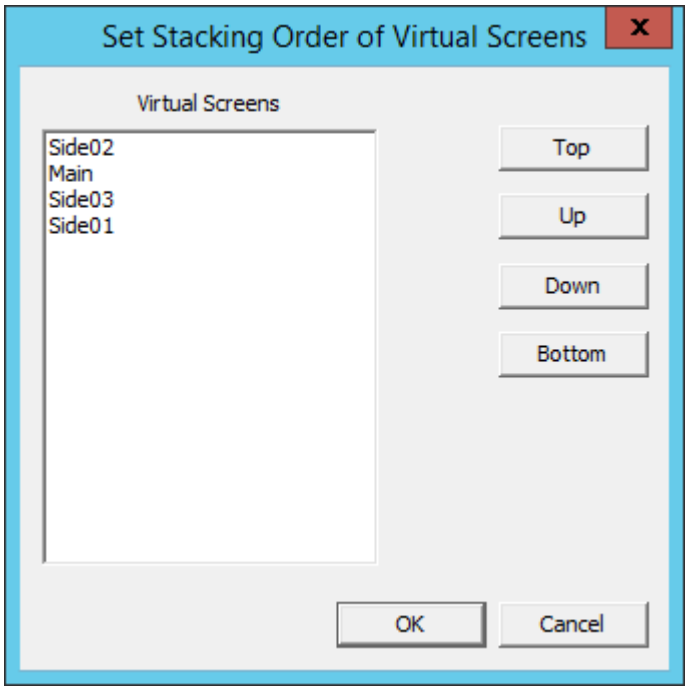


Figure 301 shows the completed layout of the overlays.

13. Click Set Order.

    The Set Stacking Order of Virtual Screens dialog box appears. This is important when the overlays overlap.

Figure 302 - Set Stacking Order of Virtual Screens



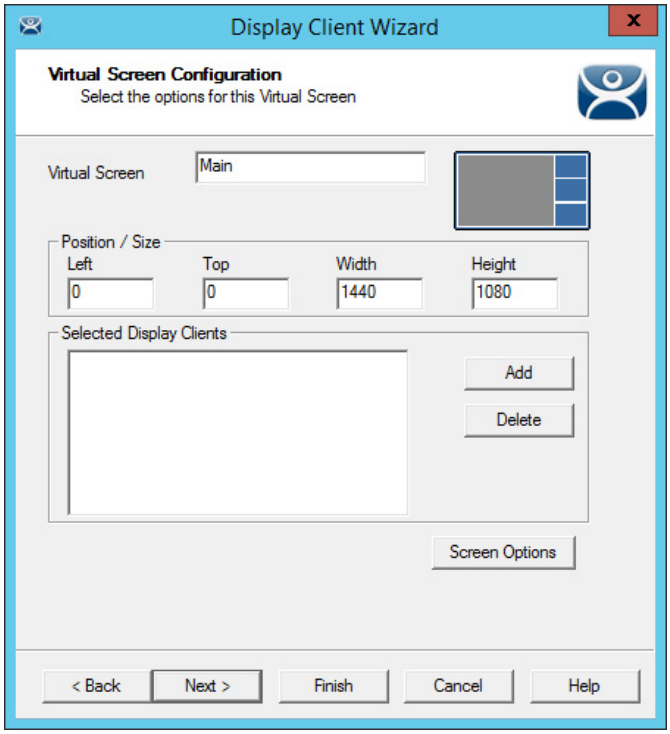
14. Highlight the virtual screen and click Top, Up, Down, or Bottom per their respective descriptions to set the priority of stacked overlays.

Field/Buttons	Description
Virtual Screens	Lists the overlays added to the virtual screen.
Top	Moves a highlighted overlay to the top of the list.
Up	Moves a highlighted overlay higher on the list.
Down	Moves a highlighted overlay lower on the list.
Bottom	Moves a highlighted overlay to the bottom of the list.

15. Click OK to return to the Select or Create the Virtual Screen Layout page.
16. Click Next.

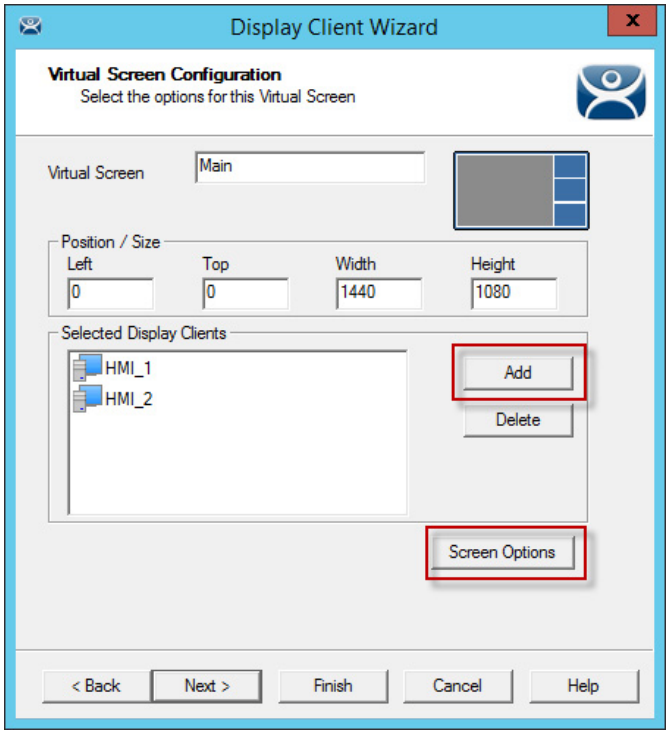
The Virtual Screen Configuration page appears, where you add display clients to the overlays. Each custom overlay needs a display client.

Figure 303 - Adding Display Clients to the Virtual Screens



The wizard shows one overlay at a time. Display clients can be added as shown in Predefined Templates on page 208.

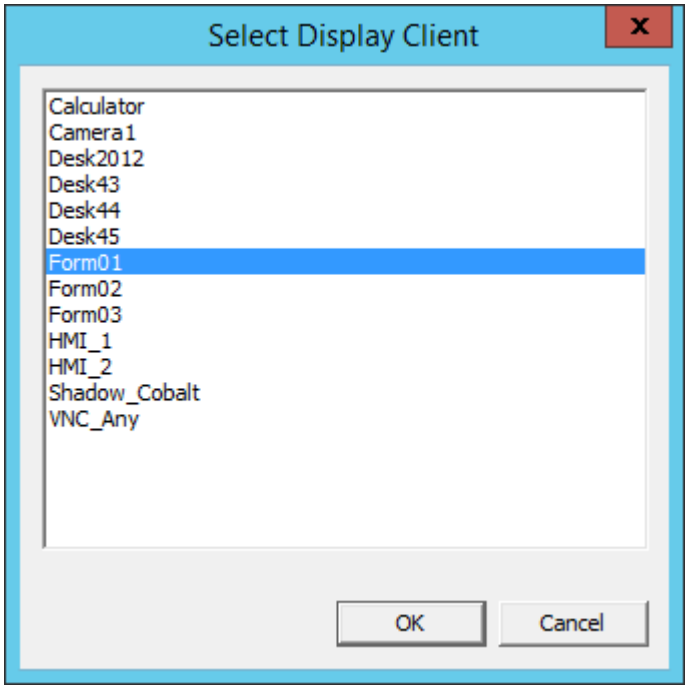
Figure 304 - Adding Display Clients to the Virtual Screens



17. Click Add.

    The Select Display Client dialog box appears, where you can select a display client from a list of all display clients.

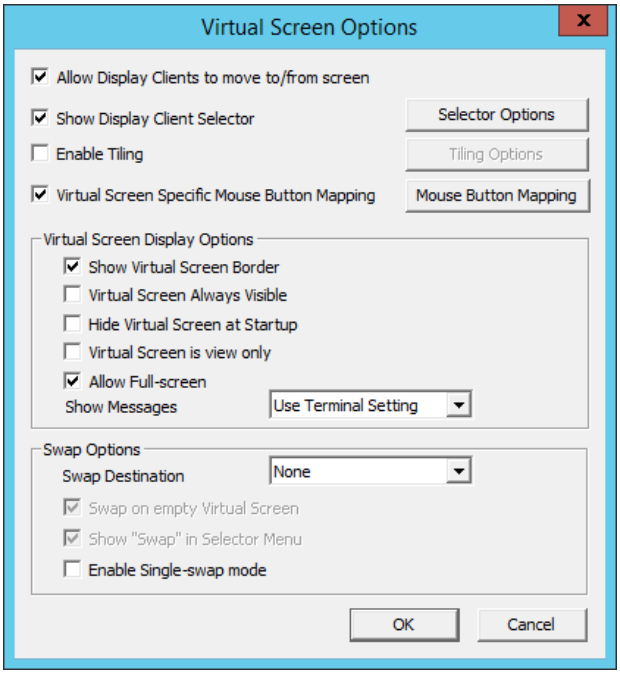
Figure 305 - Select Display Client



18. Highlight the desired Display Client and click OK to return to the Virtual Screen Configuration page.
19. Click Screen Options.

    The Virtual Screen Options dialog box appears.

Figure 306 - Virtual Screen Options



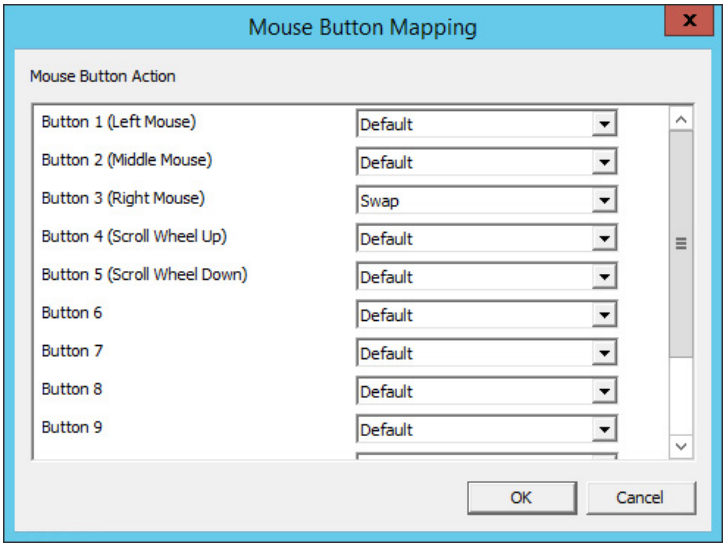
20. Choose the Virtual Screen Overlay options per the following descriptions.

Option	Description
Allow Display Clients to move to/from screen	Allows movement of a display client from one overlay to the other, much like the movement of display clients between monitors on a MultiMonitor thin client.
Show Display Client Selector	Shows the pull-down selector at the top of the overlay. Click Selector Options to configure.
Selector Options	Use to configure selector options.
Enable Tiling	Allows tiling of Display Clients within the overlay if you have multiple display clients.
Tiling Options	Use to configure tiling options.
Virtual Screen Specific Mouse Button Mapping	Enables Mouse Button Mapping to configure the mouse with use with the Virtual Screens.
Mouse Button Mapping	Use to define mouse buttons as hotkeys.
Virtual Screen Display Options	
Show Virtual Screen Border	Show a border between the overlays.
Virtual Screen Always Visible	If the user switches to a different display client, this overlay remains visible even though its display client is hidden.
Hide Virtual Screen at Startup	Hides the Virtual Screen at startup. It is intended to be used with the TermMon ActiveX, which toggles the overlay visibility.
Virtual Screen is view only	Displays the Display Client in the Virtual Screen, but makes it view-only and not interactive.
Allow Full-screen	Allows a Display Client to appear full screen and not show the sidebar.
Show Messages	Allows for control of the status message shown in the upper-left corner of the Terminal display.
Use Terminal Setting	Sets the Virtual Screen to follow the configuration of the Terminal.
Yes	Turns on the status messages.
No	Turns off the status messages.
Swap Options	
Swap Destination	Allows the location of the Virtual Screen, moved during a swap, to be specified.
Swap on empty Virtual Screen	Move the highlighted Virtual Screen to an empty Virtual Screen when selected from the pull-down Selector.
Show “Swap” in Selector Menu	Adds the Swap option to the pull-down Selector menu.
Enable Single-swap mode	Allows a single mouse click in a Virtual Screen window to initiate the swap.

21. Click Mouse Button Mapping.

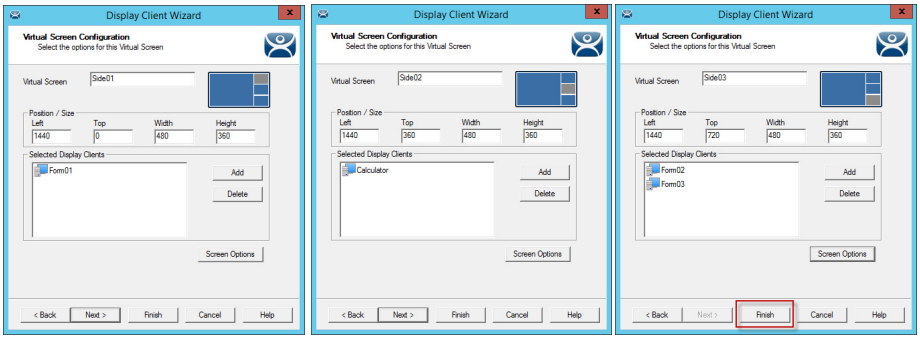
The Mouse Button Mapping dialog box appears, where you configure actions for the mouse buttons through pull-down menus.

Figure 307 - Mouse Button Mapping



22. Click OK to return to the Virtual Screen Options dialog box.
23. Click OK on the Virtual Screen Options dialog box to return to the Virtual Screen Configuration page, which repeats for each overlay.

Figure 308 - Each Overlay is Configurable

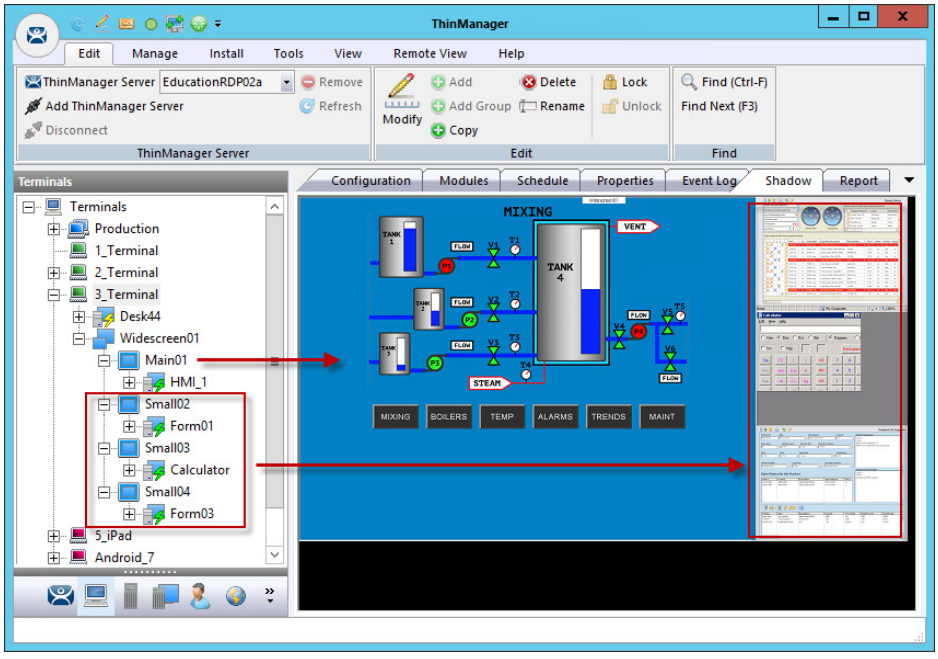


24. Click Next to go to the next overlay. The wizard navigates to each overlay, which allows the selection of display clients and settings.
25. Click Finish button when done.

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

Figure 309 on page 226 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 be tiled, if desired.

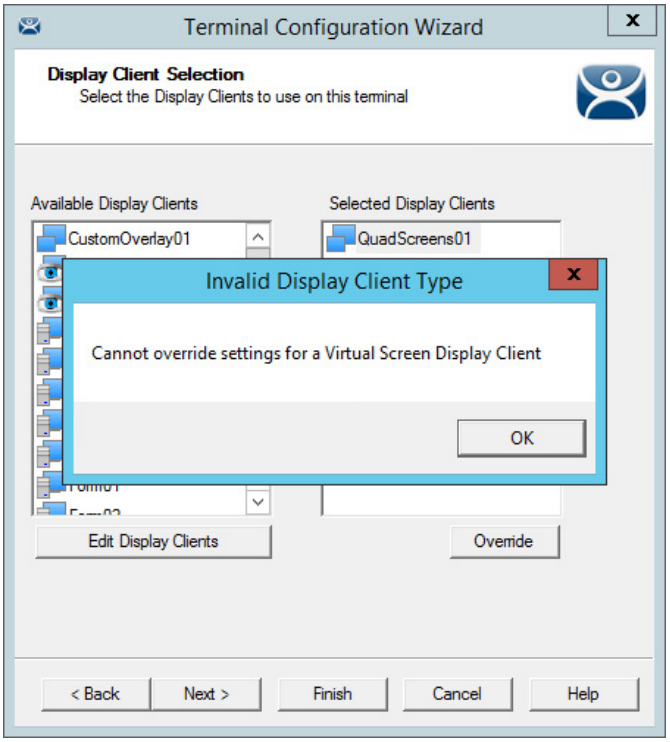
Figure 309 - Custom Overlay in Action



Display Client Override on Virtual Screens

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

Figure 310 - Display Client Selection Page Error

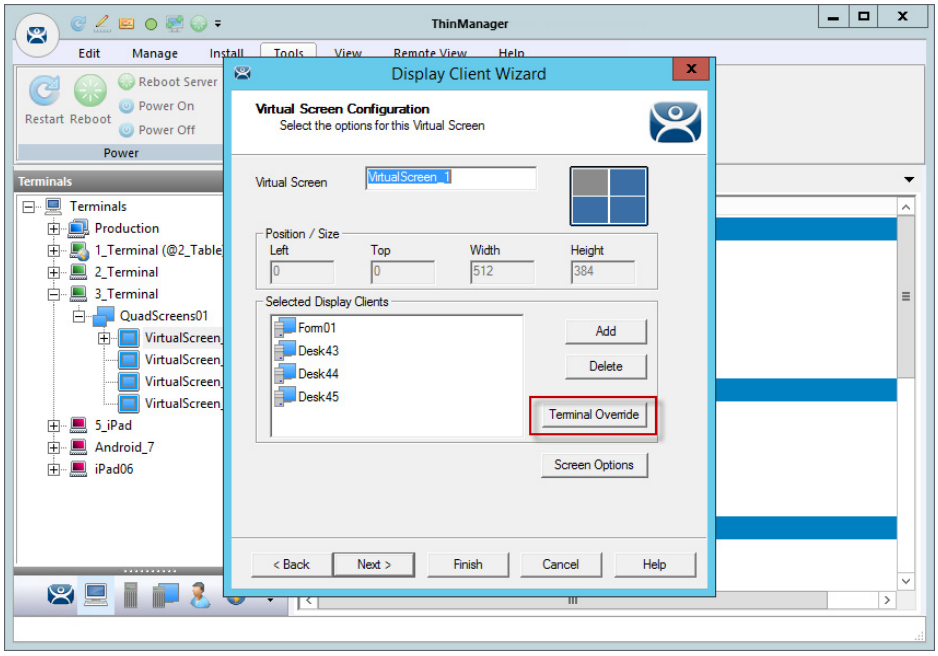


Virtual Screens do not allow an override on the Display Client Selection page of the Terminal Configuration Wizard. It is done from the ThinManager tree instead.

1. Double-click on the Virtual Screen under the Terminal in the Terminal tree of ThinManager.

   The Display Client Wizard appears.

Figure 311 - Virtual Screen Configuration Page

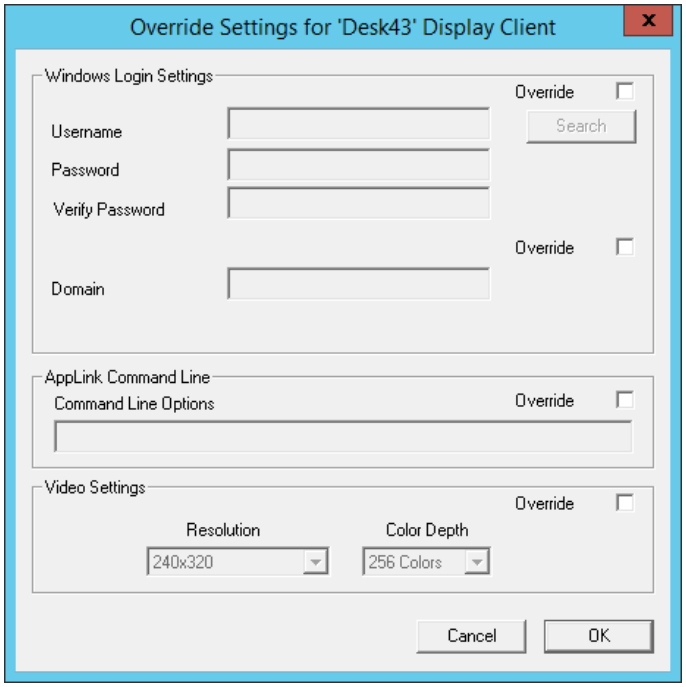


2. Click Next until the Virtual Screen Configuration page appears. The Terminal Override button is enabled.

3. In the Selected Display Clients pane, highlight the display client you want to alter and click Terminal Override.

   The Override Settings dialog box for that display client appears, which allows normal display client overrides. See Login Requirements Page on page 242 for details.

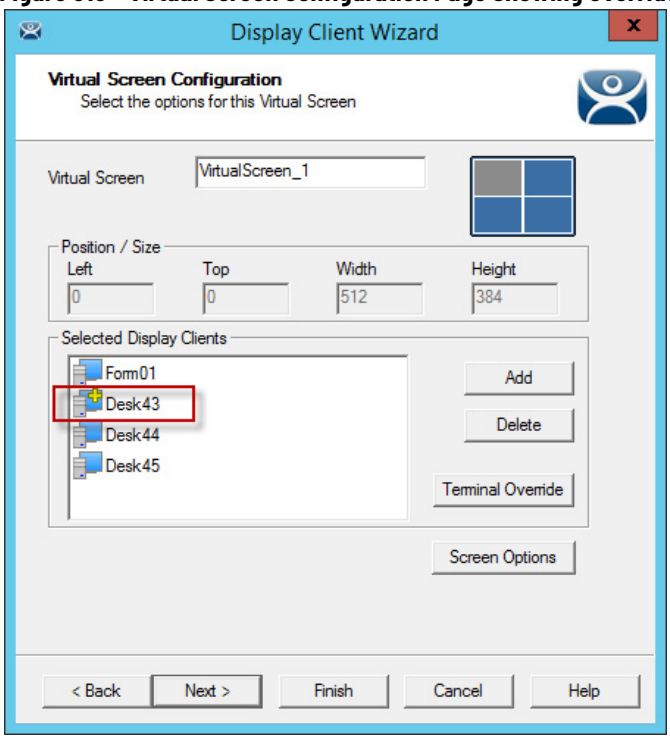
Figure 312 - Override Settings Page



4. Click Override in the sections to which the changes apply and click OK.

   On Virtual Screen Configuration page, a yellow plus sign on the Display Client indicates that it has a changed setting.

Figure 313 - Virtual Screen Configuration Page Showing Override



5. Click Finish.

Notes:

Devices

Terminal Configuration

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

- ThinManager-ready thin clients
- ThinManager-compatible thin clients
- Android Devices
- iOS® Apple® Devices
- Windows® PCs and Surface tablets

Two steps are required to add a device. First, the device must be pointed to the ThinManager Server to receive a configuration. Second, a configuration must be created in ThinManager for the device to download.

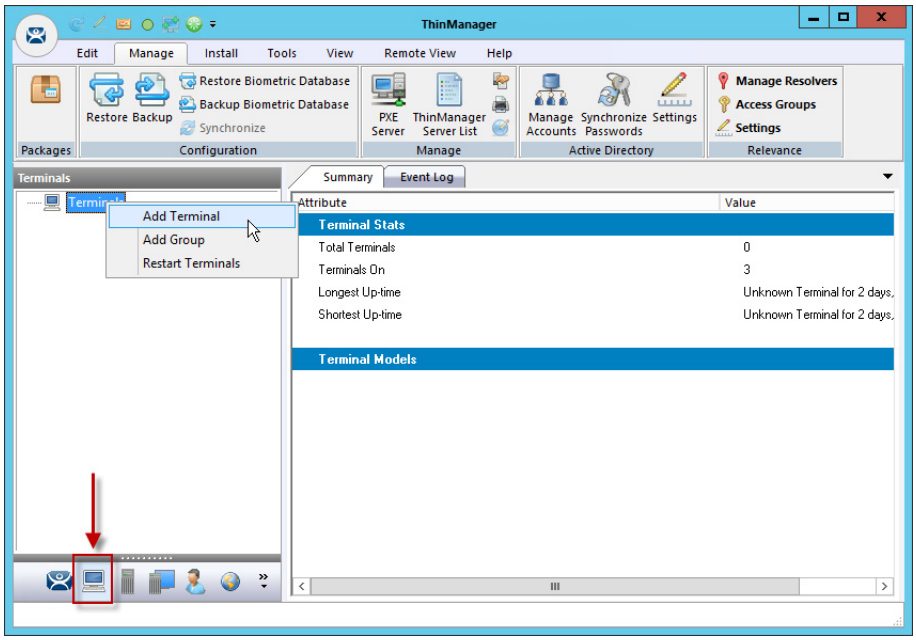
In this section, we explain the configuration of the device in ThinManager, then show how to connect each hardware device to ThinManager.

Terminal Configuration Wizard in ThinManager

To configure the device in ThinManager, follow these steps.

1. Click the Terminals icon at the bottom-left of ThinManager to display the Terminals tree.

Figure 314 - Terminal Branch of the ThinManager Tree



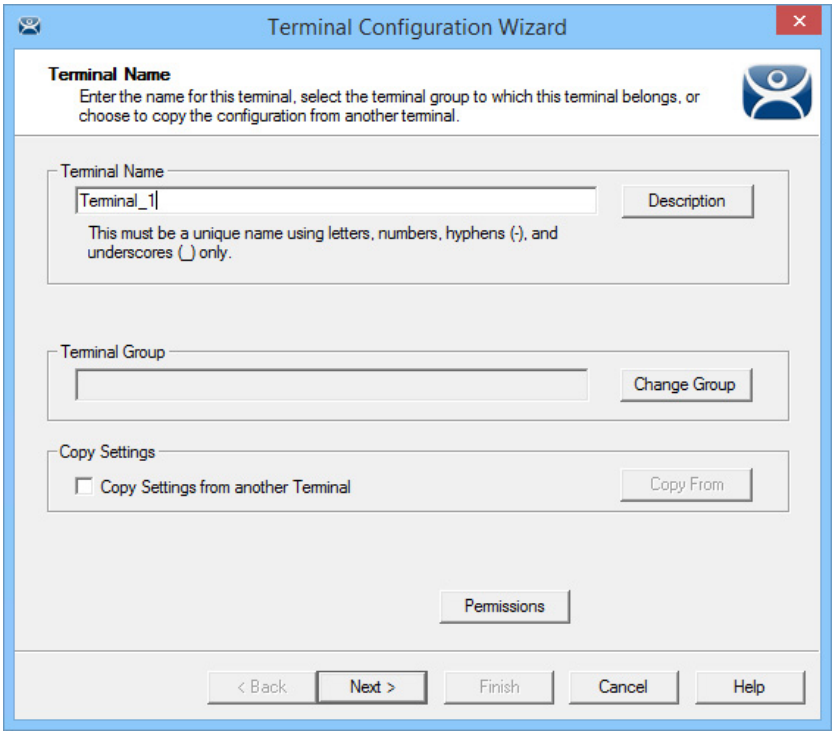
2. Right-click on the Terminals branch and choose Add Terminal.

The Terminal Configuration Wizard appears, opened at the Terminal Name page.

Terminal Name Page

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

Figure 315 - Terminal Name Page



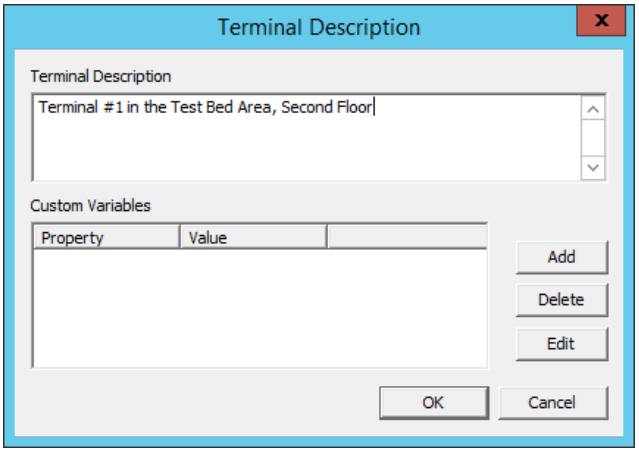
1. Complete the Terminal Name page per the following options and descriptions.

Field/Button	Description
Terminal Name	Specifies the terminal name in ThinManager. This must be a unique name using letters, numbers, hyphens, and underscores only.
Description	Launches the Terminal Description dialog box, where you can add extra information about the Terminal.
Terminal Group	Adds the terminal to a group of terminals via Change Group.
Change Group	Launches the Select Terminal Group window, which displays a tree of available groups to select.
Copy Settings from another Terminal	Click to activate Copy From button.
Copy From	Allows quick creation of terminal in that it launches the Select Terminal dialog box with a tree that allows you to apply a terminal configuration that already exists to the new terminal. See Copy Settings from another Terminal on page 273 for details.
Permissions	Applies ThinManager permissions to the Terminal. See Permission-deployed Applications in ThinManager on page 335 for details.

a. (Optional) Click Description.

The Terminal Description dialog box appears.

Figure 316 - Terminal Description Dialog Box



b. Complete the Terminal Description dialog box per the descriptions that follow.

Field/Button	Description
Terminal Description	Allows an extensive description to be added to the Terminal when the Terminal names are industrialized, like "USP_MX10_L1_qty" or "Prod_TrayPkgShrkWrp_OIT".
Custom Variables	Allow a variable to be applied for advanced functionality.
Add	Opens the Custom Variable dialog box for adding a custom variable.
Delete	Deletes a highlighted custom variable.
Edit	Click to change the settings for the highlighted variable in the Custom Variable dialog box.

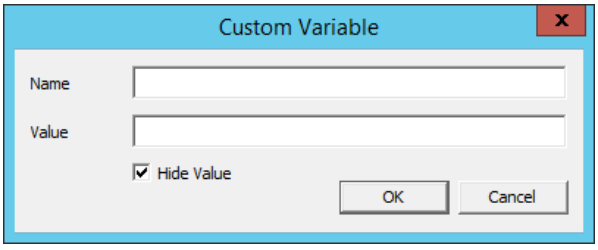
Custom variables allow a single display client to be created with a custom variable as part of the path. Each user, Terminal, or location has specific data in the custom variable to modify the content that the display client delivers, which allows one display client to do the work of many.

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

2. (Optional) Add a Custom Variable.
   a. Click Add.

   The Custom Variable dialog box appears.

Figure 317 - Custom Variable Dialog Box



b. Complete the Custom Variable dialog box per these steps.

Field/Button	Description
Name	Assigns the name to the custom variable.
Value	Assigns the value or content to the custom variable.
Hide Value	Obscures the text in the Value field. Clear the checkbox to display the value.
OK	Accepts the changes and closes the dialog box.
Cancel	Closes the dialog box without changes saved.

c. Click OK to close the Custom Variable dialog box.

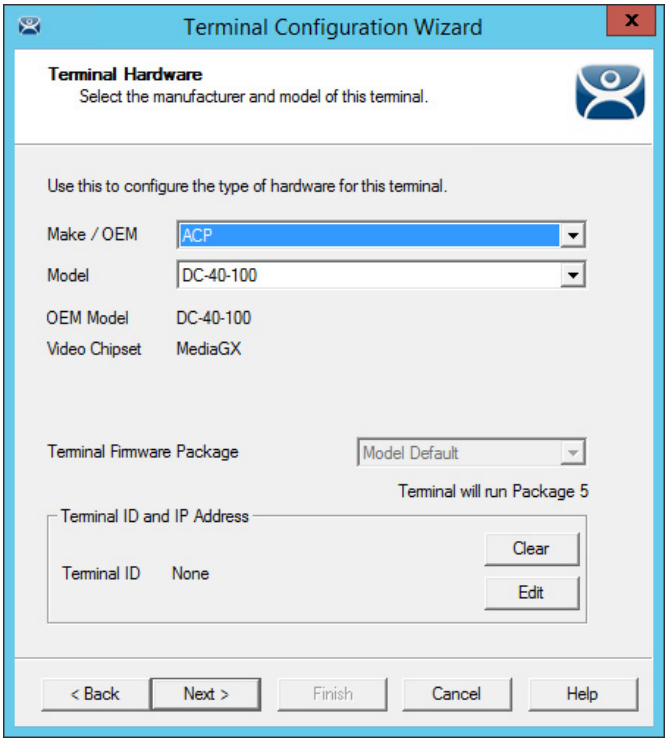
d. At the Terminal Description dialog box, click OK.
e. At the Terminal Name page, click Next.

The Terminal Hardware page appears.

Terminal Hardware Page

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

Figure 318 - Terminal Hardware Page of the Terminal Configuration Wizard



1. Complete the Terminal Hardware page per the descriptions that follow.

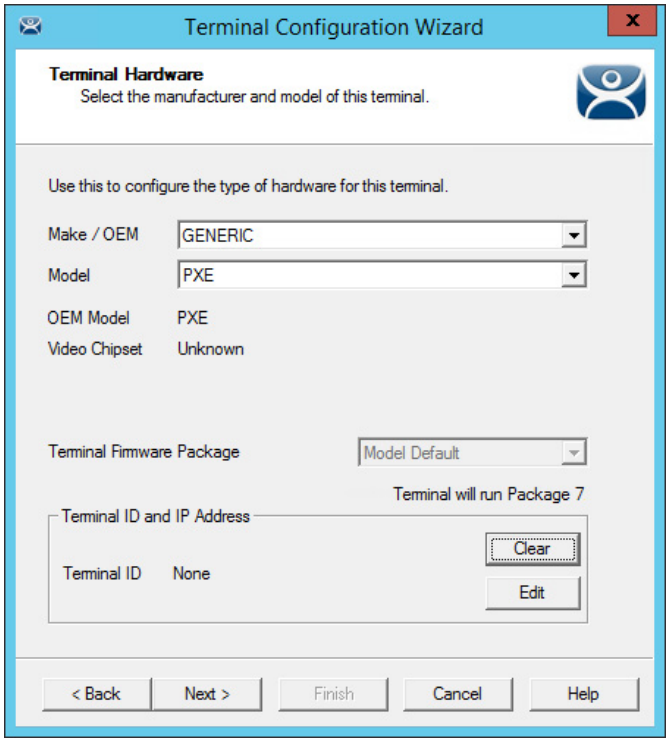
Field/Button	Description
Make/OEM	Choose the make of the hardware from the pull-down menu.
Model	Choose the model of the hardware from the pull-down menu.
OEM Model	Displays the actual model as listed in the TermCap.
Video Chipset	Displays the video chipset used once the terminal connects to ThinManager as listed in the TermCap.
Terminal Firmware Package	Use the pull-down menu to change the firmware package that the terminal uses. Must be enabled in Package Manager (Manage>Packages).
Clear	Removes the Terminal ID identifier from the configuration of an active terminal. The MAC address of the terminal is used for the Terminal ID. Clearing the Terminal ID frees hardware that is already tied to a configuration and allows the terminal to be tied to a different configuration without deleting its original configuration. It also allows the make and model of the hardware to be changed.
Edit	Launches the Edit Terminal ID dialog box that allows for the manual change of the MAC address of the configuration. Allows for the replacement of an old terminal by entering the MAC address of the replacement. Entering the new MAC address allows the new terminal to boot and retrieve its configuration without selecting the terminal from the list. Once a MAC address is registered within ThinManager, you can assign a static IP address to it if the Terminal is PXE Booting and if the ThinManager PXE Server is set to Not Using Standard DHCP Server. See Figure 424 on page 308.

Use the correct Make and Model if you can, which allows you to configure the Terminal to match the capabilities of the hardware used.

When a Terminal connects to its configuration for the first time, ThinManager adjusts the configuration to match the actual hardware used and not the preconfigured hardware selected to prevent errors. 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 to identify the Terminals. The Terminal ID field is automatically populated when hardware is associated with the configuration.

Figure 319 - PXE Boot Configuration for ThinManager-compatible Thin Clients



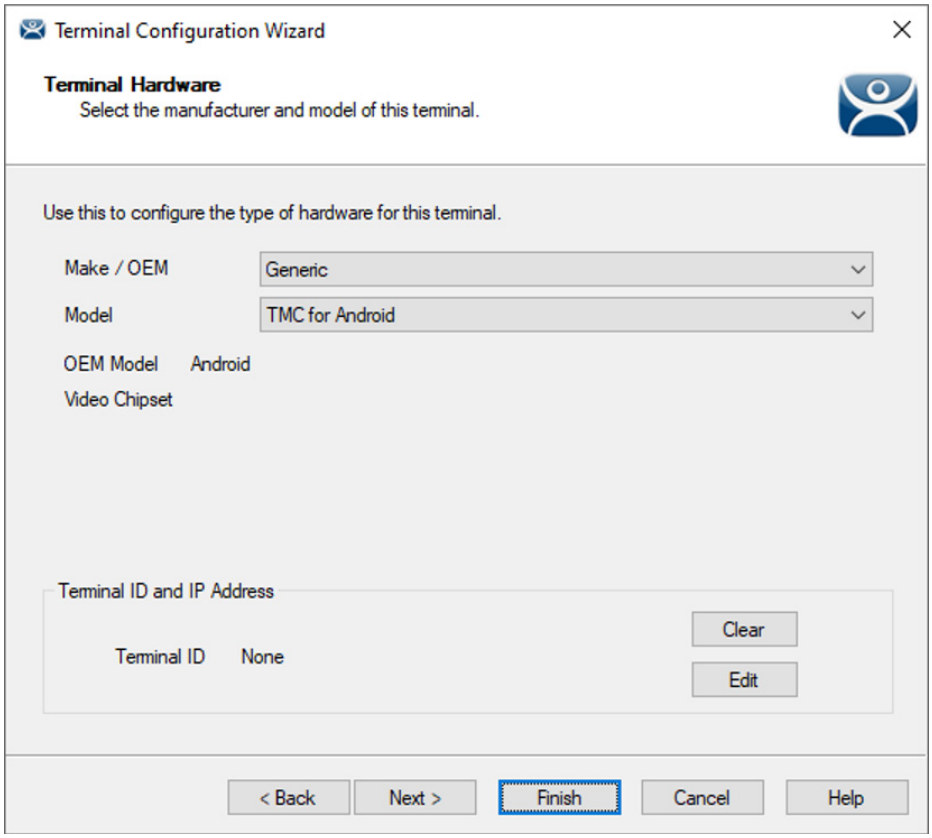
2. Configure the ThinManager-compatible thin clients as GENERIC/PXE as they use PXE boot to download their firmware.
3. Configure the PXE Server in ThinManager at Manage>PXE Server. See PXE Server and PXE Boot on page 296 for information.
4. Click Next.

   The Terminal Options page appears.

Android Devices

ThinManager has an Android application called TMC for Android—formerly aTMC—that enables the delivery of managed content to an Android device, much like a thin client, with the exception that there is an underlying Android OS that is not managed by ThinManager. TMC for Android can be found in the Google Play Store under the name TMC for Android, or on the ThinManager downloads page.

Figure 320 - Hardware Configuration for Android Devices



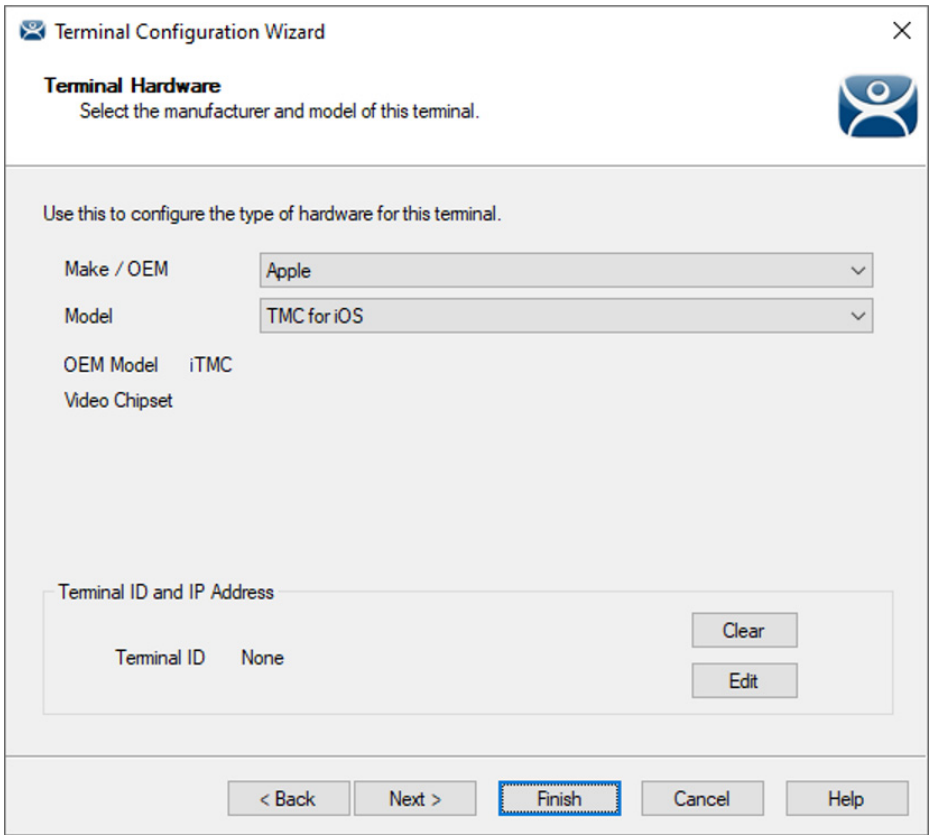
- Choose GENERIC/ TMC for Android as the Make and Model of the hardware.

Apple Devices

Similar to Android Devices, ThinManager has an iOS application called TMC for iOS—formerly called iTMC—that enables you to deliver managed content to an Apple mobile device much like a thin client, with the exception that there is the underlying iOS, which is not managed by ThinManager. TMC for iOS can be found in the Apple App Store under the name ThinManager Client (TMC).

As indicated above, the original iOS application for ThinManager was called iTMC. It can be selected on the Terminal Hardware page of the ThinManager Configuration Wizard by selecting Apple / iTMC (Legacy) for the Make and Model pull-down menus. The new TMC for iOS application is based on the same codebase as TMC for Android, and TMC for Windows, which provides a consistent user experience across these different hardware platforms. We no longer add new features to legacy iTMC, but continue to provide security updates for 2 years beyond the initial release date of TMC for iOS.

Figure 321 - Hardware Configuration for Apple iPad



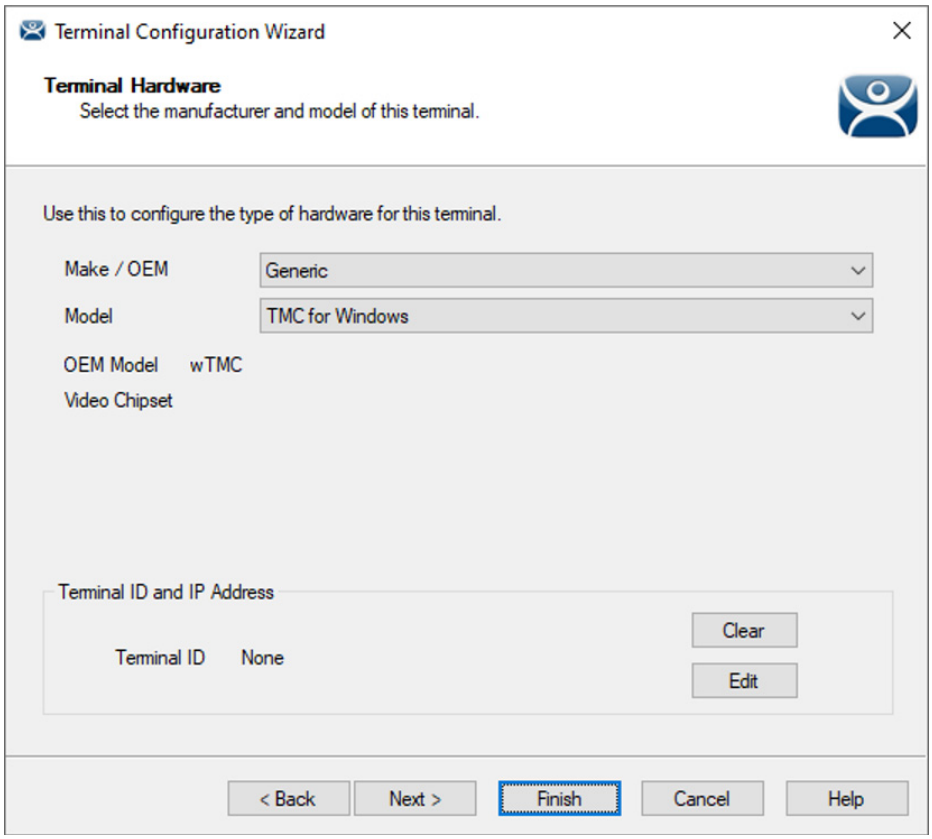
- For iOS devices, choose Apple/TMC for iOS as the Make and Model of the terminal.

Windows Devices

Similar to Android and iOS Devices, ThinManager has a Windows application called TMC for Windows—formerly called WinTMC—that enables you to deliver managed content to a Windows mobile device, much like a thin client, with the exception that there is the underlying Windows OS, which is not managed by ThinManager. TMC for Windows can be found on the ThinManager downloads page.

As indicated above, the original Windows application for ThinManager was called WinTMC. It can be selected on the Terminal Hardware page of the ThinManager Configuration Wizard by selecting Generic/ WinTMC (Legacy) for the Make and Model pull-down menus. The new TMC for Windows application is based on the same codebase as TMC for Android, and TMC for iOS, which provides a consistent user experience across these different hardware platforms. We no longer add new features to legacy WinTMC, but continue to provide security updates for 2 years beyond the initial release date of TMC for Windows.

Figure 322 - Hardware Configuration for WinTMC Clients

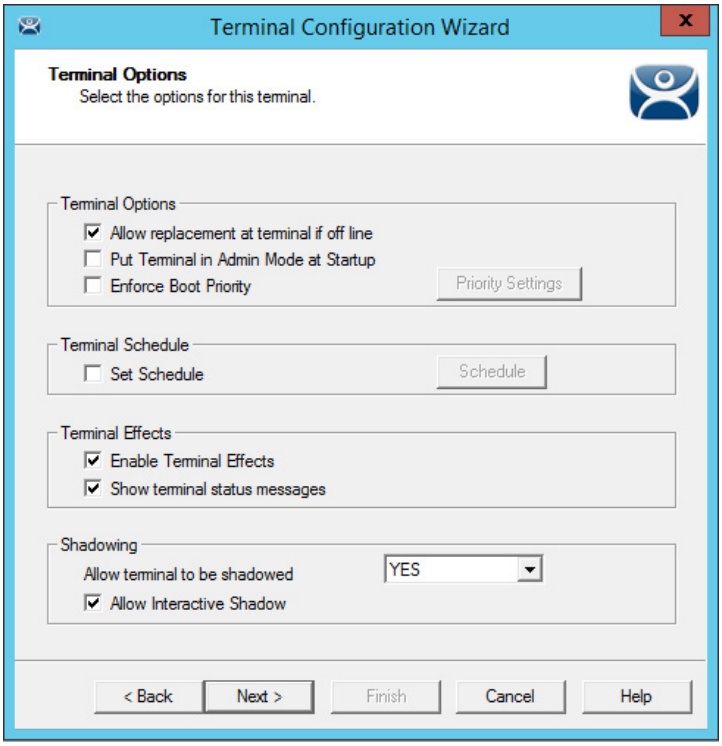


- Choose GENERIC/WinTMC as the Make and Model of the terminal.

Terminal Options Page

The Terminal Options page starts the configuration process.

Figure 323 - Terminal Options Page of the Terminal Configuration Wizard



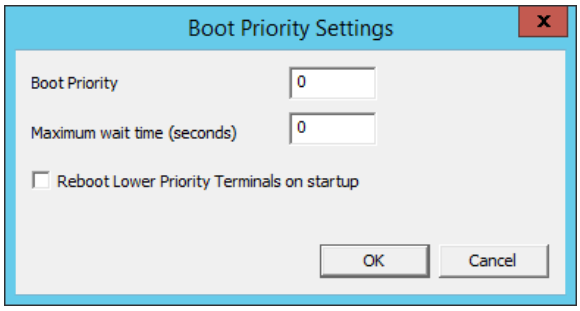
1. Complete the Terminal Options page per these descriptions.

Setting/Button	Description
Terminal Options	
Allow replacement at the terminal if off line	Allows the terminal to appear in the replacement list during a new terminal connection.
Put Terminal in Admin Mode at Startup	Turns the Terminal on without showing the display clients, which is useful to use as the Terminal to register HID cards or fingerprint scans.
Enforce Boot Priority	Allows you to set an order for the Terminals to boot when many reboot at once.
Priority Settings	Launches the Boot Priority Settings dialog box.
Terminal Schedule	
Set Schedule	Makes Schedule active.
Schedule	Launches the Event Schedule dialog box for the terminal. For more information, see Figure 575 on page 405.
Terminal Effects	
Enable Terminal Effects	Allows the desktops in MultiSession to slide smoothly into the desktop instead of appearing instantaneously.
Show terminal status messages	Allows the Terminal to display status messages in the upper-left corner of the screen. Clear the checkbox to hide the messages from the operator.
Shadowing	
Allow terminal to be shadowed	Sets the Shadowing setting, which allows configuration of Shadowing Options.
No	Prevents the Terminal from being shadowed by anyone.
Ask	Asks the user to allow shadowing. The user must click Yes in a message dialog box before shadowing is allowed.
Warn	Displays a dialog box that alerts that the Terminal that it is to be shadowed, but does not require user input before shadowing is allowed.
Yes	Allows shadowing to occur without warning or user input.
Allow Interactive Shadow	Allows users with Shadowing permission to interactively shadow the Terminal. Clearing this checkbox puts it into a read-only mode.

a. Click Priority Settings.

The Boot Priority Settings dialog box appears.

Figure 324 - Boot Priority Settings



b. Complete the Boot Priority Settings dialog box per the descriptions that follow.

Setting	Description
Boot Priority	Sets the priority level of the terminal, with 1 as the highest priority and 99 as the lowest. The higher the number, the lower the priority.
Maximum wait time (seconds)	Sets the maximum interval the Terminal waits before starting to reboot.
Reboot Lower Priority Terminals on startup	Reboots lower priority (higher number) Terminals when this Terminal reboots, which is useful if the lower priority Terminals are running an application that has a dependency on the higher priority (lower number) Terminal.

c. Click OK.

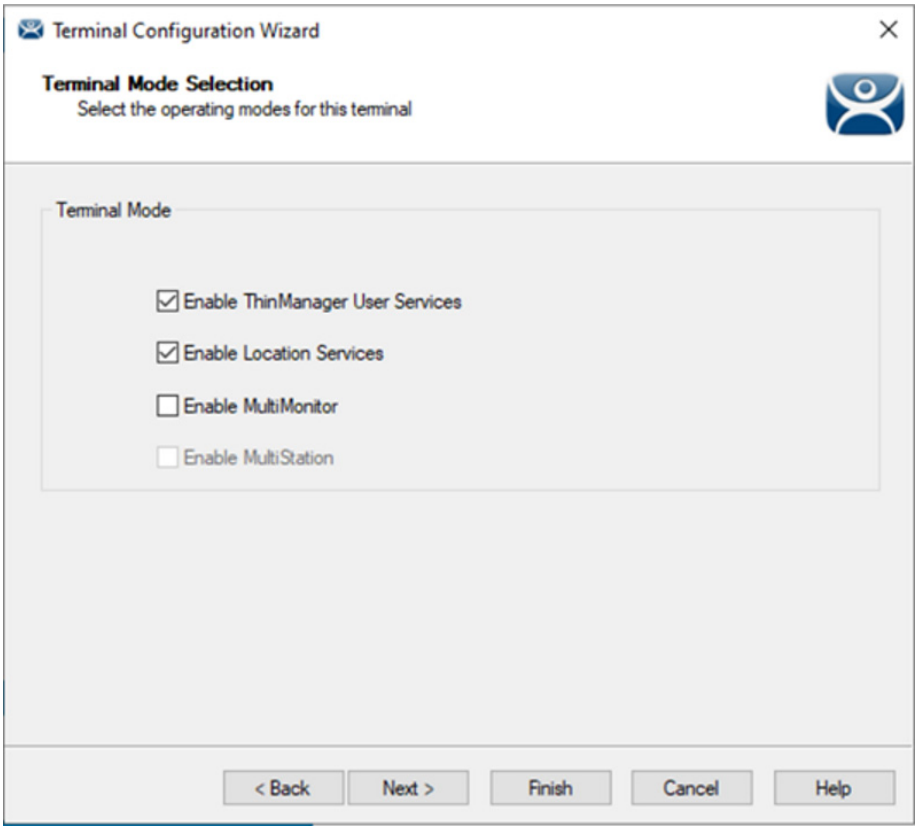
2. Click Next to continue the configuration.

The Terminal Mode Selection page appears.

Terminal Mode Selection Page

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

Figure 325 - Terminal Mode Selection



1. Complete the Terminal Mode Selection page per these descriptions.

Setting	Description
Enable ThinManager User Services	Uses Permissions and the membership of an Access Group to grant or deny access to applications, Terminals, or locations. See Permission-deployed Applications in ThinManager on page 335 for details.
Enable Location Services	Allows the Terminal to be assigned a Location and use the location features. Location Services on page 426.
Enable MultiMonitor	Allows you to configure the Terminal to use two to five monitors depending on the hardware capability. MultiMonitor on page 623.
Enable MultiStation	An advanced MultiMonitor 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. See Select Hotkey Dialog Box on page 254.

MultiStation is supported on firmware platform versions 6.0 through 9.0. Firmware platform 9.1 and greater leverage a different Linux kernel in which MultiStation is not technically viable; therefore, MultiStation is not supported on firmware platform versions 9.1 or newer. The MultiStation checkbox is not be available in ThinManager when newer firmware packages are selected. The recommendation to accomplish the same outcome of MultiStation is to either:

- use thin client hardware that support firmware versions 9.0 or earlier, or
- use more thin client hardware for the additional independent stations needed

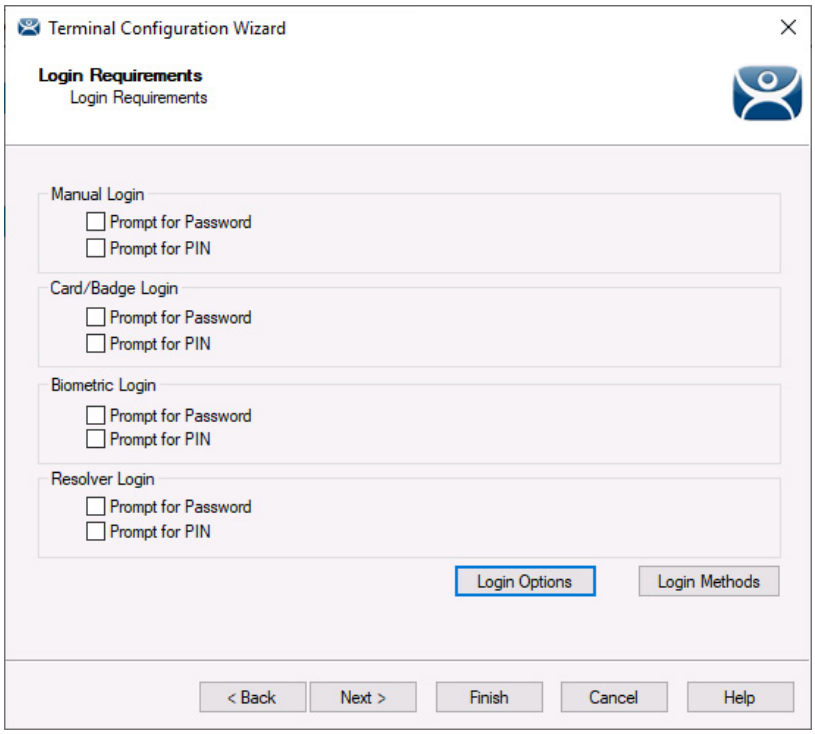
2. Click Next.

   The Login Requirements page appears.

Login Requirements Page

The Login Requirements page assigns login options for several login types. Here, you can control login methods at the terminal and whether to allow automatic logins, a password, or a Personal Identification Number (PIN).

Figure 326 - Login Requirements Page

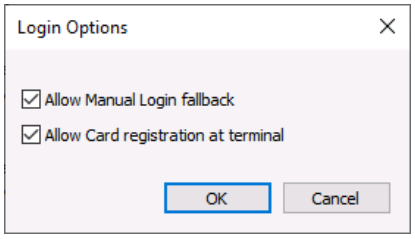


Setting	Description
Manual Login	Sets the authentication method for manual logins
Prompt for Password	When checked, the user is required to enter a password
Prompt for PIN	When checked, the user is required to enter a Personal Identification Number (PIN)
Card/Badge Reader	Sets the authentication method for logins with a card or badge
Biometric Login	Sets the authentication method for logins with a fingerprint reader
Resolver Login	Sets the authentication method for logins using a resolver like a Bluetooth® device
Button	
Login Options	Press to launch the Login Options window to control badge enrollment access at the terminal and behavior on a failed-badge attempt
Login Methods	Launches the Login Methods Allowed window to define login methods allowed on the terminal.

1. Complete the Terminal Options page per these descriptions.
2. To control badge enrollment access and behavior on a failed-badge attempt, click Login Options.

   The Login Options window appears.

Figure 327 - Login Options Window



Setting	Description
Allow Manual Login fallback	When enabled, the user is prompted to log in manually after a failed card/badge login attempt, if allowed. Card/Badge Login must be enabled in Login Methods Allowed.
Allow Card registration at terminal	When enabled, the user can enroll a card/badge at the thin client terminal. Assignment of unknown badge at terminal during user login can be disabled via this function.

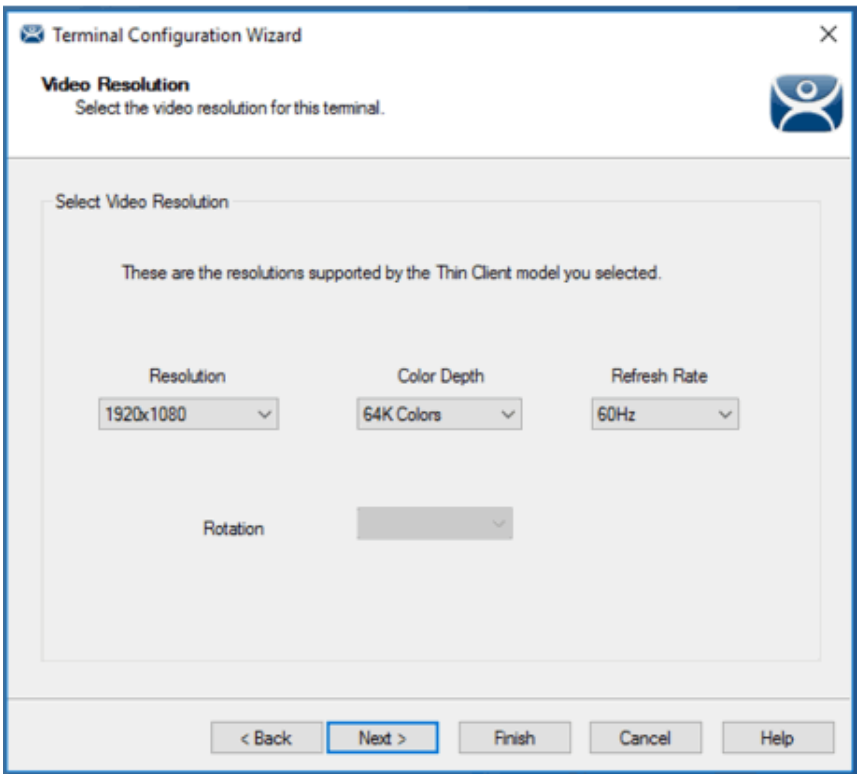
3. Choose the behavior of the login attempt.
4. Click OK.

   You are returned to the Login Requirements page.
5. Click Next.

   The Video Resolution page appears.

Video Resolution Page

Figure 328 - Video Resolution Page



The Video Resolution page allows you to choose the desired resolution, color depth, refresh rate, and rotation of the monitor connected to the terminal. Click Next.

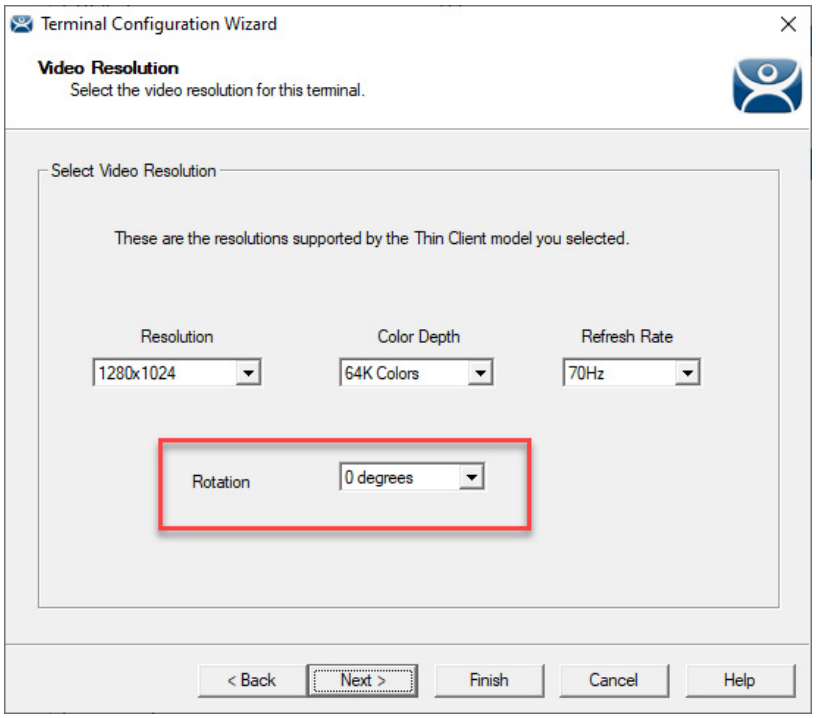
The Video Resolution page appears.

Video Resolution Page

The Video Resolution page of the Terminal Configuration Wizard lets you choose the Resolution, Color Depth, Refresh Rate, and Rotation for your monitor.

The resolutions in the pull-down menus are dependent on the make and model of hardware used.

Figure 329 - Video Resolution



Setting	Description
Resolution	Choose the desired screen size from the pull-down menu, which lists the sizes available for the hardware chosen on the Terminal Hardware page. **Note**: WinTMC configurations offer a Full Screen option.
Color Depth	Choose the desired color depth from the pull-down menu, which contains the values available for the hardware chosen on the Terminal Hardware page.
Refresh Rate	Choose the desired refresh rate for the monitor from the pull-down menu, which contains the values available for the hardware chosen on the Terminal Hardware page. Adjustment to this setting can fix issues where the screen pans.
Rotation (for portrait mode)	Choose the desired rotation (0°, 90°, 180°, or 270°) from the pull-down menu to set the clockwise rotation of the attached monitor. **Note**: Available for terminals that use Firmware 9.1 and later.

Match the Resolution and Color Depth settings to your monitor's specifications for a clear picture.

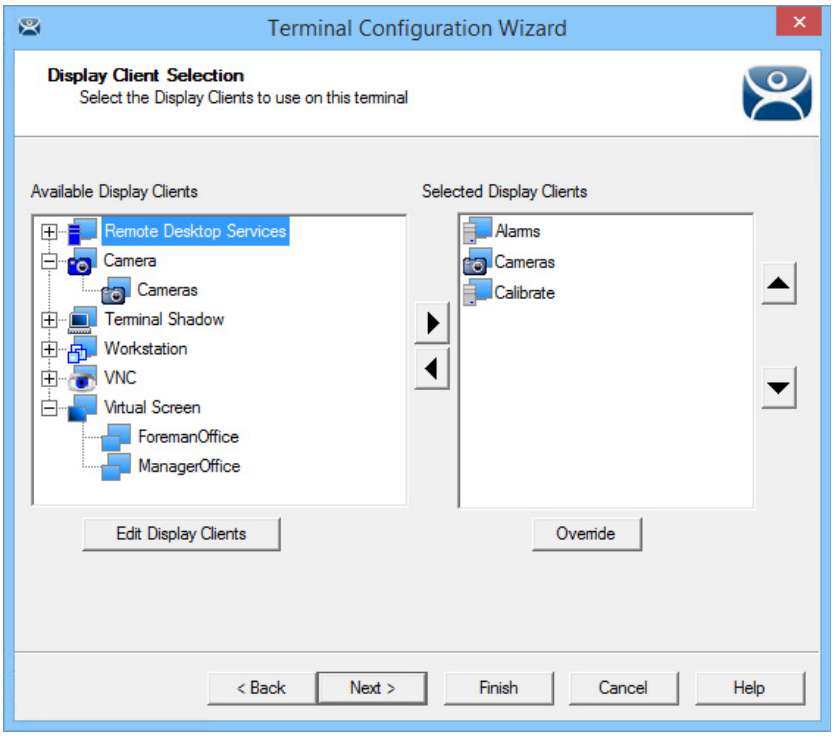
1. After making your choices, click Next.

   The Display Client Selection page appears.

Display Client Selection Page

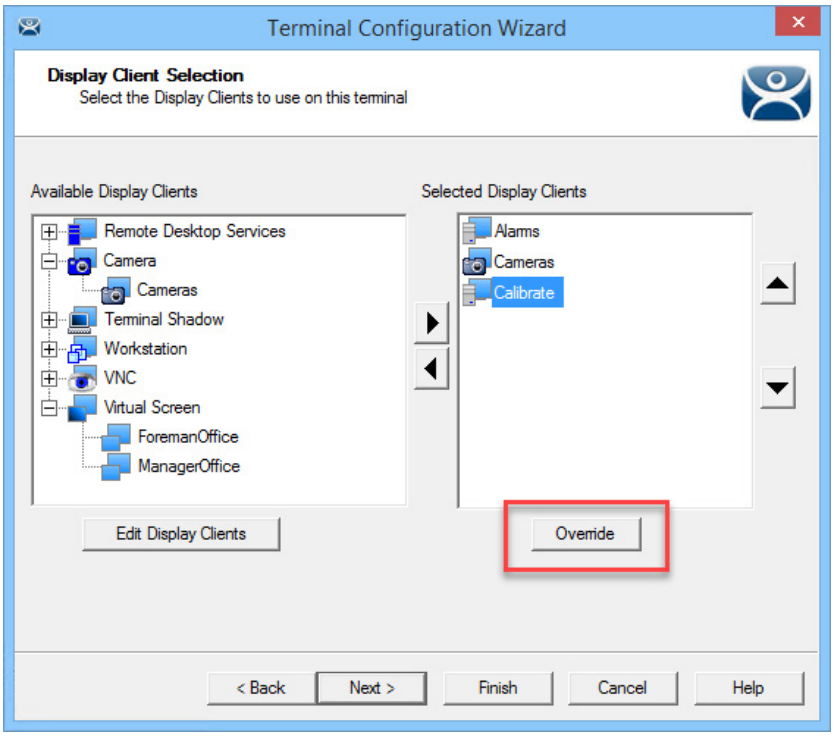
The Display Client Selection page allows the applications to be assigned to the Terminal.

Figure 330 - Display Client Selection Page



1. Move created display clients from the Available Display Clients list to the Selected Display Clients list to add them to the Terminal configuration. Double-click or highlight the display client and use the right arrow.

Figure 331 - Display Client Selection Page of the Terminal Configuration Wizard

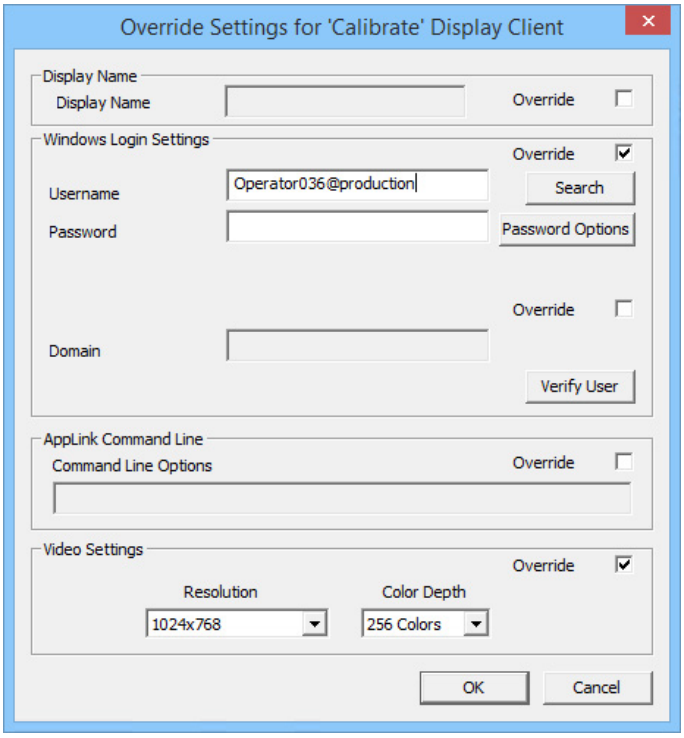


The addition of two or more display clients is MultiSession, which provides the ability to deploy applications from different servers with ease.

2. Click Override.

   The Override Settings dialog box appears.

Figure 332 - Override Settings Dialog Box



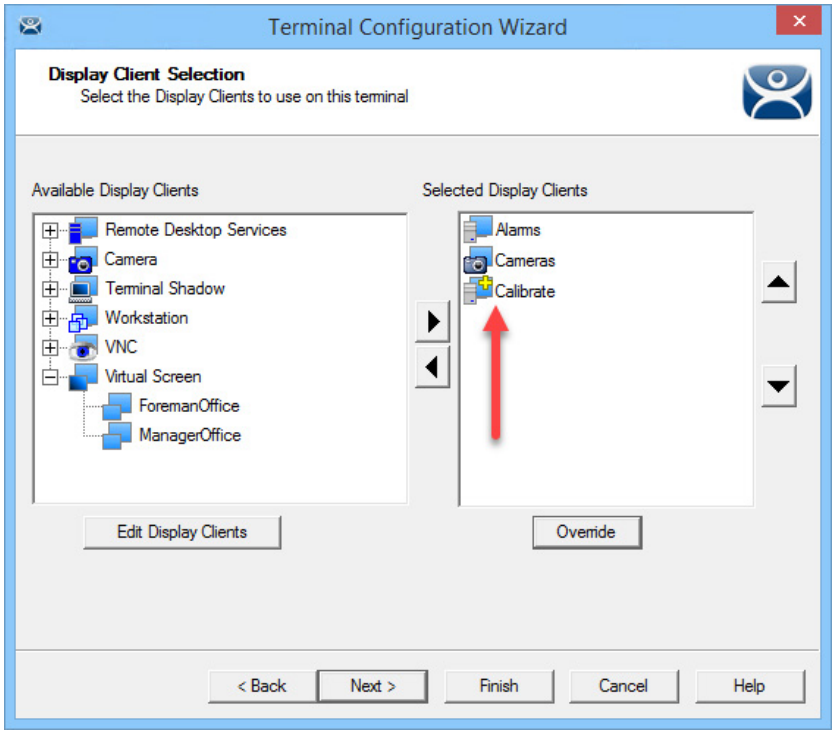
The Override Settings page allows you to change the Display Name of the terminal, the user account used for login, add a command line option, or change the resolution.

In a domain environment, you can use the Search button to pull a user account from the Active Directory. See Active Directory User Login Account on page 257.

3. Click OK.

   The Override Settings dialog box closes.

Figure 333 - Override Indicator Icon



If a Display Client has a setting overridden, then the Display Client shows a Changed icon in the Selected Display Clients list.

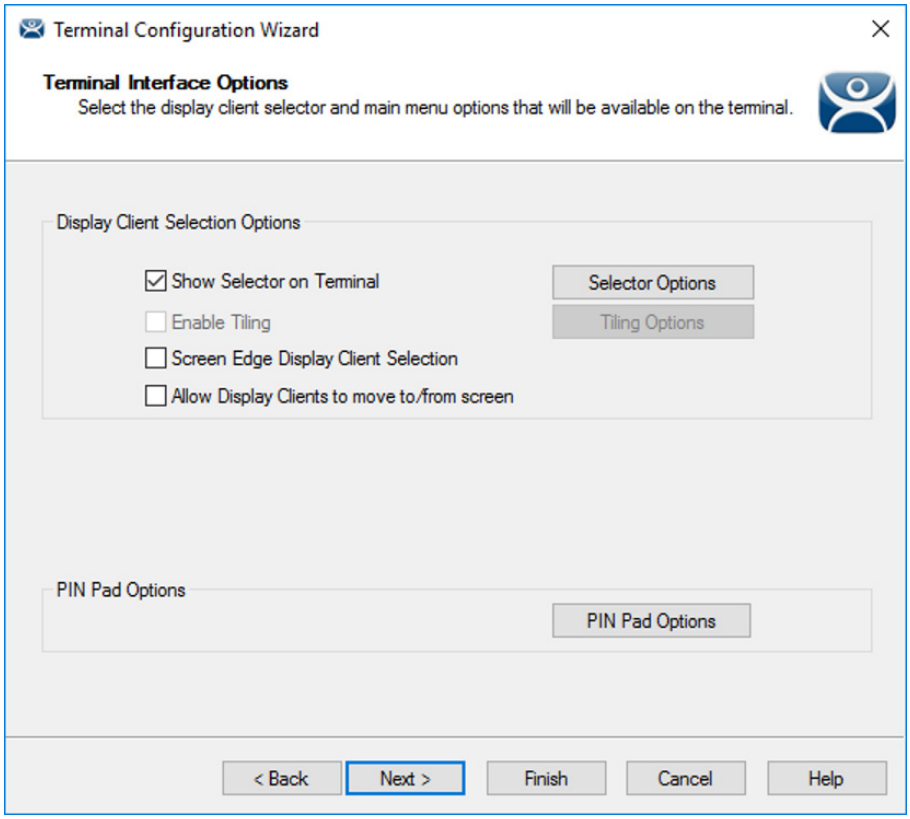
4. Click Next on the Display Client Selection page.

   The Terminal Interface Options page appears.

Terminal Interface Options Page

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

Figure 334 - Terminal Interface Options Page



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

1. Complete the mouse options for switching as described here.

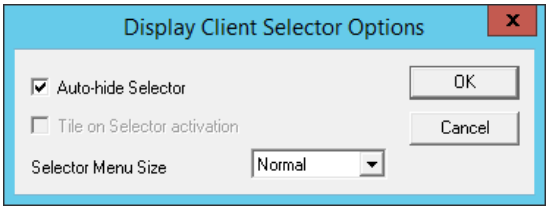
Setting/Button	Description
Display Client Selection Options	
Show Selector on Terminal	Displays an on-screen pull-down menu that can be activated by mouse.
Selector Options	Launches the Display Client Selector Options dialog box, which contains settings for tiling sessions when using MultiSession.
Enable Tiling	Allows Display Clients to be tiled on the monitor to provide an overview of all sessions at once.
Tiling Options	Launches the Tile Options dialog box, which has the settings for tiling sessions when using MultiSession.
Screen Edge Group Selection	Activates a feature that switches windows if the mouse is moved off screen.
Allow Display Clients to move to/ from screen	Allows a display client to be moved to any active screen on a MultiMonitor thin client.
Pin Pad Options	Opens the Pin Pad Options dialog box, which allows you to configure the PIN pad when using a Personal Identification Number instead of a password.

   a. Click Selector Options.

      The Display Client Selector Options dialog box appears.

The Display Client Selector is hidden in the top center of the Terminal screen and is revealed when the mouse is moved to the center of the top edge.

Figure 335 - Display Client Selector Options



b. Complete the Display Client Selector Options dialog box as described.

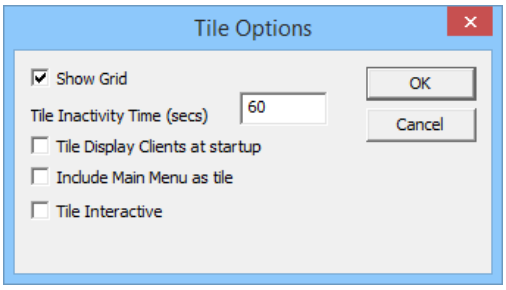
Setting	Description
Auto-hide Selector	Hides the pull-down Display Client Selector menu until the mouse hovers over the top-center of the screen. Clear the checkbox to show the pull-down Display Client Selector at the top-center of the screen.
Tile on Selector activation	Tiles the sessions when an auto-hid selector is activated.
Selector Menu Size	Sets the size of the text in the Display Client Selector.

c. Click OK to accept changes.

d. Click Tiling Options.

The Tile Options dialog box appears.

Figure 336 - Tiling Options



The Tile Options window has several settings for tiling sessions when using MultiSession.

e. Complete the Tile Options dialog box as described.

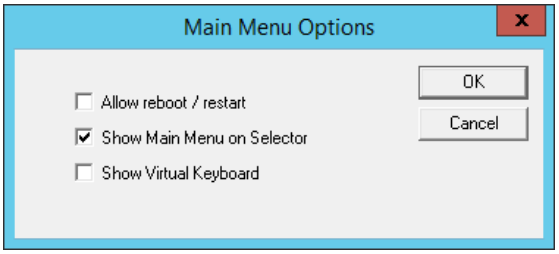
Setting	Description
Show Grid	Shows tiled sessions in a grid with each grid labeled with the session name while the session is loading.
Tile Inactivity Time (secs)	Sets the length of time that the Terminal screen stays focused on a selected session before reverting to a tiled state due to inactivity.
Tile Display Clients at startup	Shows the sessions tiled when the Terminal first connects to its sessions.
Include Main Menu as tile	Includes a session displaying the TermSecure Main Menu.
Tile Interactive	Allows 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 Display Client Selector pull-down menu or the tiling hotkey (CTRL + T), if enabled.

f. Click OK to accept changes.

g. Click Main Menu Options.

The Main Menu Options dialog box appears.

Figure 337 - Main Menu Options



The Main Options dialog box that has the settings for Main Menu when using ThinManager User Services. It is not visible unless ThinManager User Services is chosen on the Terminal Mode Selection page.

2. Complete the Main Menu Options dialog box as described here.

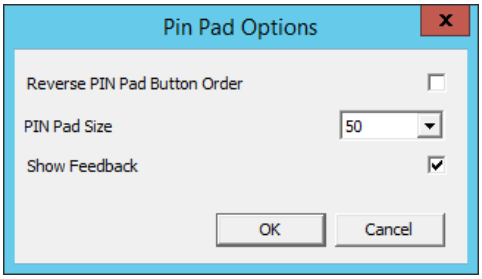
Setting	Description
Allow Reboot/Restart	Adds a terminal Restart and Reboot button on the Main Menu.
Show Main Menu on Selector	Lists the Main Menu as an option on the Display Client Selector pull-down menu.
Show Virtual Keyboard	Launches a virtual keyboard with the Main Menu open so the operator can log in manually.

a. Click OK.

b. Click Pin Pad Options.

The Pin Pad Options dialog box appears.

Figure 338 - Pin Pad Options Window



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

3. Complete the Pin Pad Options dialog box as described here.

Setting	Description
Reverse Pin Pad Button Order	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	Sets the size of the pin pad as a percentage of the screen.

4. Click Next on the Terminal Interface Options page.

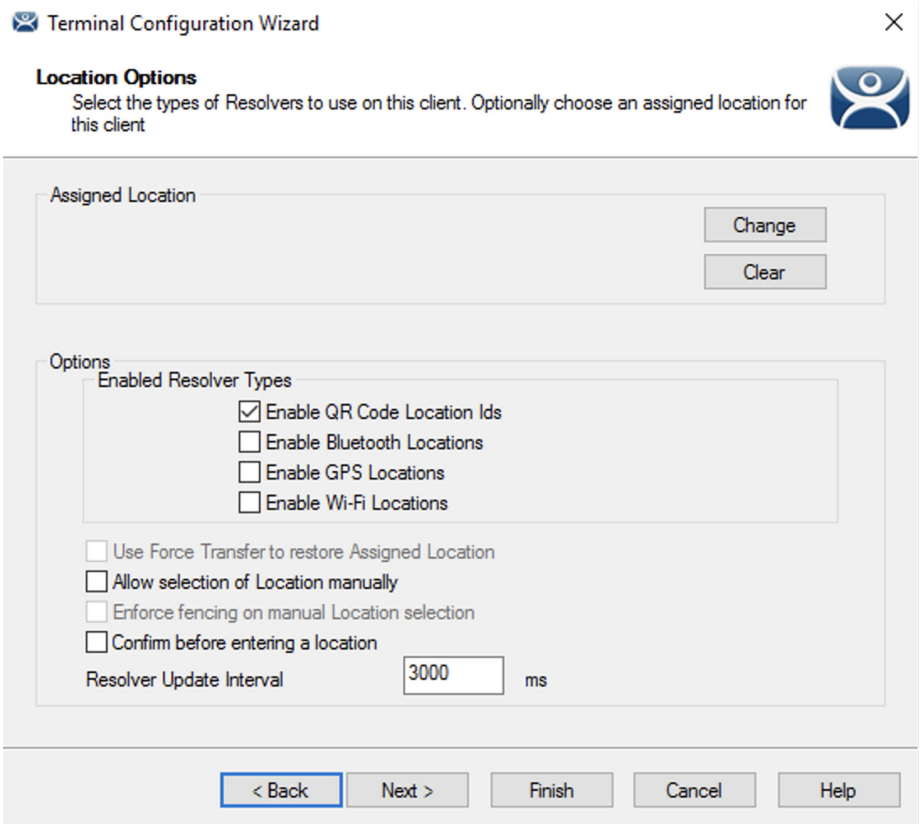
If no Location Services are checked, the Hotkey & Mouse Button Configuration page appears here. See Figure 479 on page 347 for more information.

The Location Options page appears.

Location Options Page

The Location Options page allows the setting of the location options.

Figure 339 - Location Options Page



Choose the Options before assigning a location, which locks the Options. If you need to change an option, click Clear to clear the location, change the option, and then reassign the Location.

1. Choose the Options as described here.

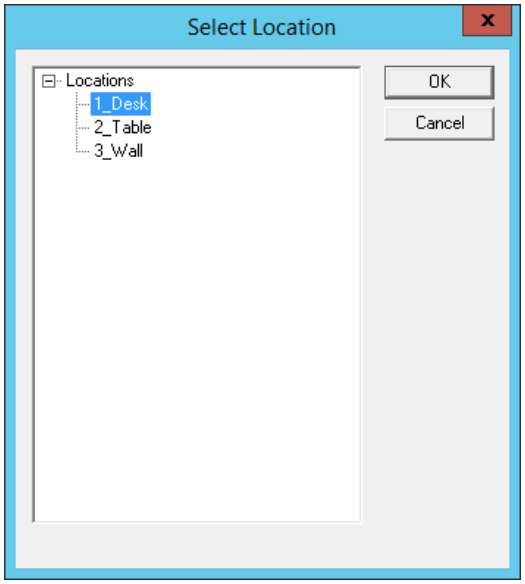
Setting	Description
Assigned Location	
Change	Launches the Select Location dialog box.
Clear	Clears the Assigned Location.
Enabled Resolver Types	
Enable QR Code Location Ids	Allows the scanning of a QR code to determine the location.
Enable Bluetooth Locations	Allows the use of Bluetooth beacons to determine the location.
Enable GPS Locations	Allows the Global Positioning System of the mobile device to determine the location.
Enable Wi-Fi Locations	Allows the signal strength of Wi-Fi access points to determine the location.
Use Force Transfer to restore Assigned Location	Lets an operator restore a transferred session without asking permission.
Allow Selection of the Location manually	Lets the user select the location manually from a menu on the mobile device. If this checkbox is cleared, then the user must use a Resolver.
Enforce fencing on a manual Location selection	Allows a manual login anywhere from that Terminal, which could be helpful on a control room Terminal. When chosen, this enforces fencing on that Terminal when a location is selected manually.
Confirm before entering a location	Enables a dialog box that is shown each time a user enters an area.
Resolver Update Interval	The frequency that the resolver updates.

Regarding Enable Resolver Types, ThinManager has several methods of resolving the location to allow specific applications to get sent to specific locations. Each method selected requires configuration to associate a location with the Resolver data.

2. Click Change.

   The Select Location dialog box appears.

Figure 340 - Select Location Window

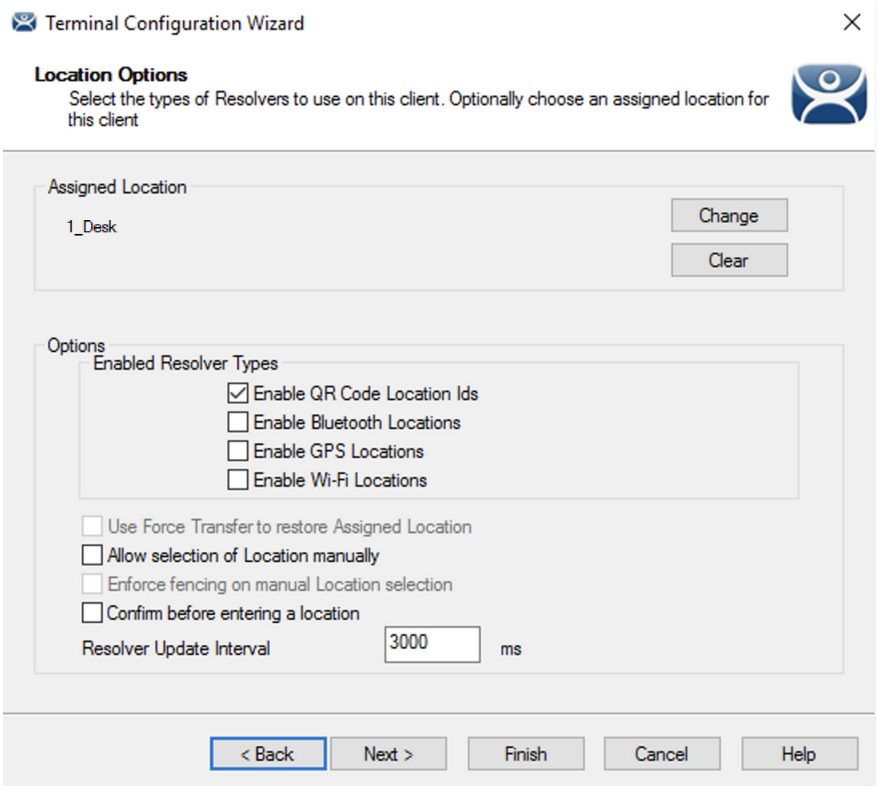


The created Locations are displayed in the Select Location tree.

3. Highlight the desired Location and click OK.

   Once the Location is assigned, the Options are locked.

Figure 341 - Location Assigned

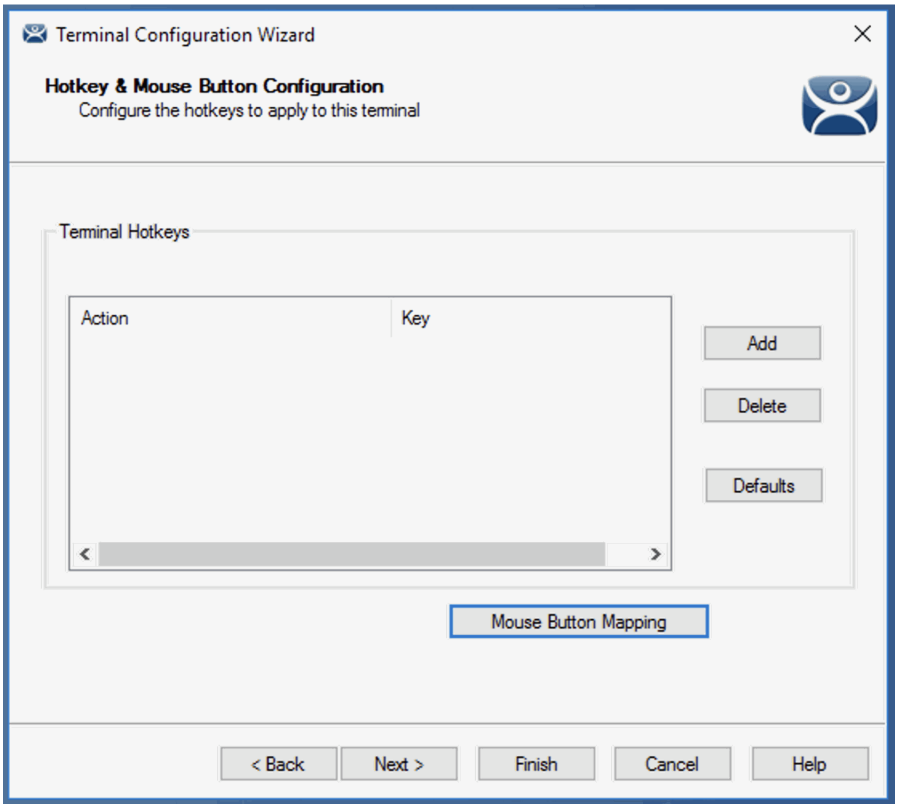


4. Click Clear to clear the location and make the options available if you need to change an option, then re-assign the Location.
5. Click Next.

   The Hotkey & Mouse Button Configuration page appears.

Hotkey & Mouse Button Configuration Page

Figure 342 - Hotkey & Mouse Button Configuration Page

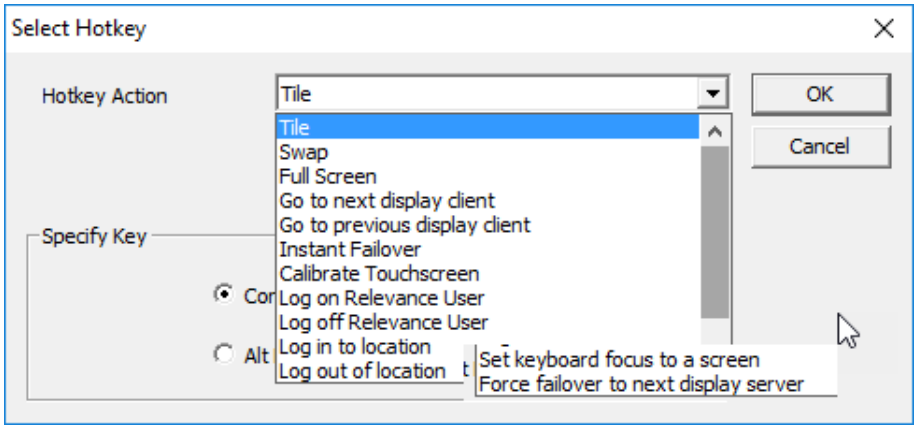


1. Click Add.
   The Select Hotkey Dialog Box appears.

Select Hotkey Dialog Box

The Select Hotkey dialog box allows you to configure hotkeys for display client switching.

Figure 343 - Select Hotkey



2. Complete the Select Hotkey dialog box per these descriptions.

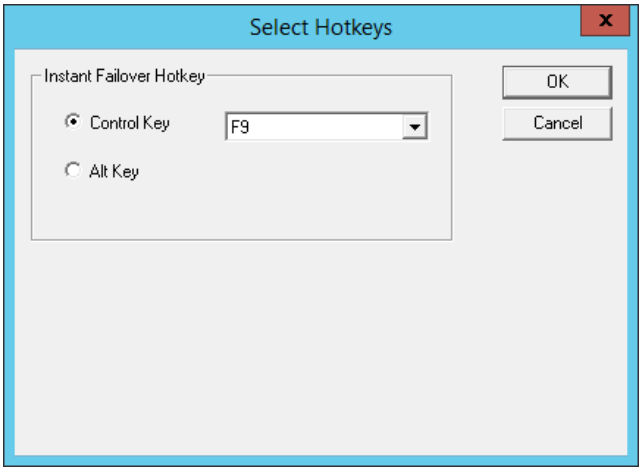
Setting	Description
Tile	Initiates the Tiling of display clients.
Swap	Exchanges display clients in Virtual Screens.
Full Screen	Expands an overlay to Full Screen.
Go to next display client	Navigates to the next display client in the list.

Setting	Description
Go to previous display client	Navigates to the last-used display client.
Instant Failover	Allows hotkey switch between different sessions of a terminal using MultiSession.
Calibrate Touchscreen	Initiates the touch screen calibration program.
Log on ThinManager User	Opens the ThinManager Login dialog box.
Log off ThinManager User	Logs off the ThinManager User.
Log in to location	Opens a login dialog box.
Log out of location	Logs off the user from the location.
Set keyboard focus to a screen	Directs the output of the keyboard to the specified screen. **Note**: to use this setting, the terminal must have MultiMonitor enabled. Set the Hotkey parameter to designate which screen receives the output.
Force failover to next display server	Allows you to fail over the active Remote Desktop Display Server set on a specified Display Client to another listed Remote Desktop Display Server. The failover affects the designated Display Clients only, and it does not disable or fail over the Display Server elsewhere. This setting is effective for Display Clients configured for Failover, instant Failover, and SmartSession. **Note**: this setting does not work on Display Clients set to Enforce Primary.

a. (Optional) Choose Enable Instant Failover Hotkey, and then click Change Hotkey, which allows the hotkeys to be changed from the default.

The Select Hotkeys dialog box appears.

Figure 344 - Select Hotkeys for Instant Failover



The default hotkey for Instant Failover switching is set to Control+F9.

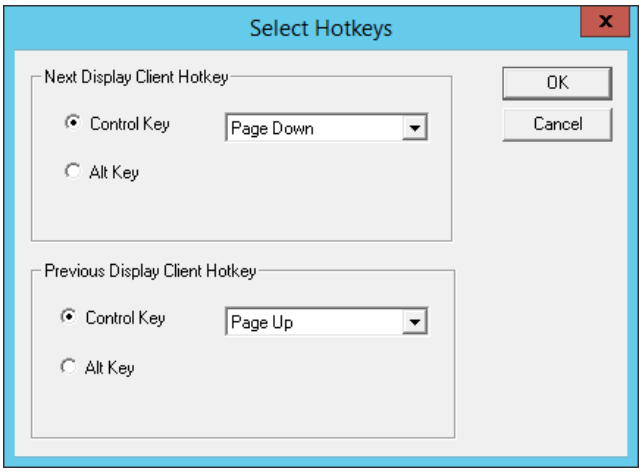
b. Click Alt Key or choose another function key from the pull-down menu.

c. Click OK to accept changes.

d. (Optional) Click Enable Display Client Hotkeys, and then click Change Hotkeys, which allows the MultiSession switching hotkeys to be changed from the defaults.

The Select Hotkeys dialog box appears.

Figure 345 - Select MultiSession Switching Hotkeys



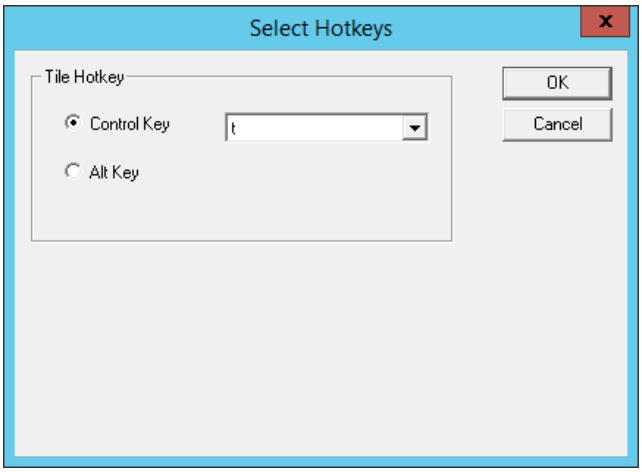
The default hotkey for MultiSession switching is set to Control+Page Up and Control+Page Down.

e. Click Alt Key or use the pull-down menu to select another hotkey.

f. Click OK to accept changes or Cancel to close.

g. (Optional) Choose Enable Tiling Hotkey, and then click Change Hotkey, which allows the hotkey to be changed from the default.

Figure 346 - Select SessionTiling Hotkeys



The default hotkey for SessionTiling activation is set to Control+t.

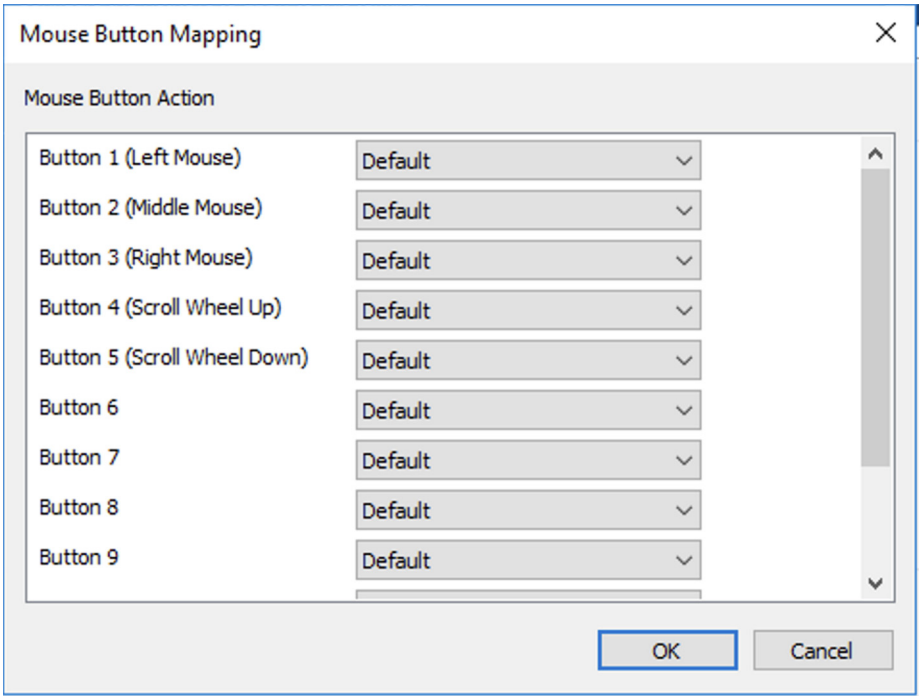
h. Click Alt Key or use the pull-down menu to select another hotkey.

i. Click OK to continue or the Cancel button to close without accepting changes.

3. Click Next on the Hotkey & Mouse Configuration page to continue the configuration.
4. Click Mouse Button Mapping.

   The Mouse Button Mapping dialog box appears, which allows you to configure actions for the mouse buttons through pull-down menus.

Figure 347 - Mouse Button Mapping



5. Click OK to accept any setting changes and close the window.
6. Click Next on the Hotkey Configuration page.

   The Log In Information page appears, which is used to specify a Windows Account that is used to log on to all Display Clients assigned to the Terminal automatically. See Figure 355 on page 262.

Active Directory User Login Account

A ThinManager Server deployed in a domain can pull an Active Directory account into the Username field of the Log In Information page of the Terminal Configuration Wizard. See Figure 441 on page 324.

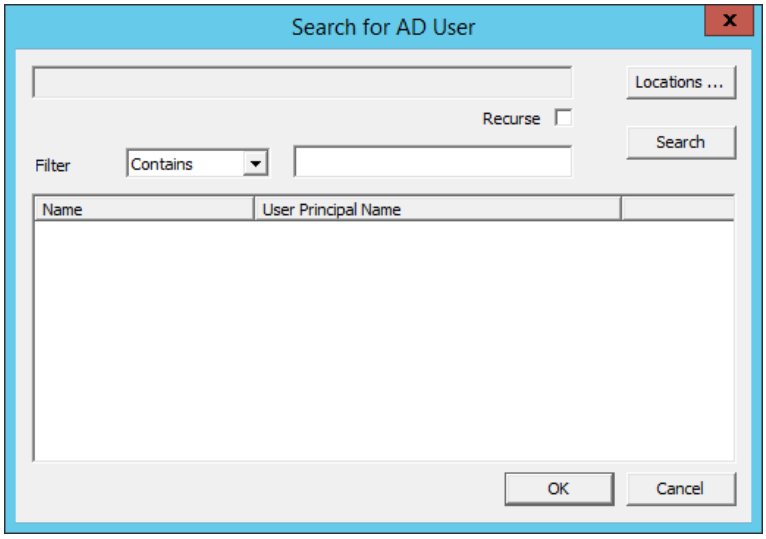
Search for Active Directory User

1. Click Search, which launches a series of dialog boxes that allows you to select a domain user account for the Terminal login account.

   The method is the same on Display Servers, Terminals, and ThinManager Users.

   A Search for AD User dialog box appears that allows you to select an Active Directory user.

Figure 348 - Search for AD User Dialog Box



Buttons	Description
Locations	Opens the Select AD Location to Search dialog box to select the Organizational Unit (OU) to search.
Search	Searches the selected OU and populates the Name field with the OU members.
Options	
Filter	Filters results with either the Contains or Starts With function and what is entered into the text box.
Recurse	Sets the Search function to search nested Windows Security Groups when searching a Windows Security Group. The Choose AD Synchronization Mode must be set to Security Group on the Active Directory System Settings dialog box to work. Choose Manage>Active Directory>Settings to open the Active Directory System Settings dialog box.

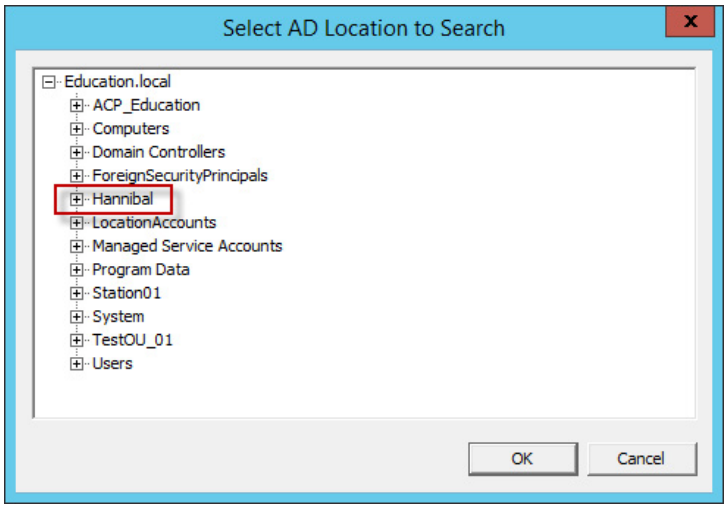
Search for Active Directory Location

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

2. Click Locations.

   The Select AD Location to Search dialog box appears.

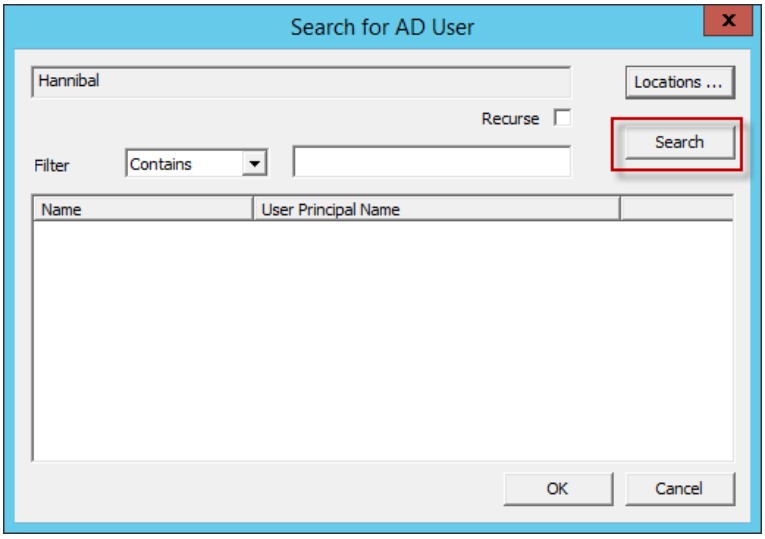
Figure 349 - Select AD Location to Search Dialog Box



3. Highlight the branch of the Active Directory tree that contains your administrative user account and click OK.

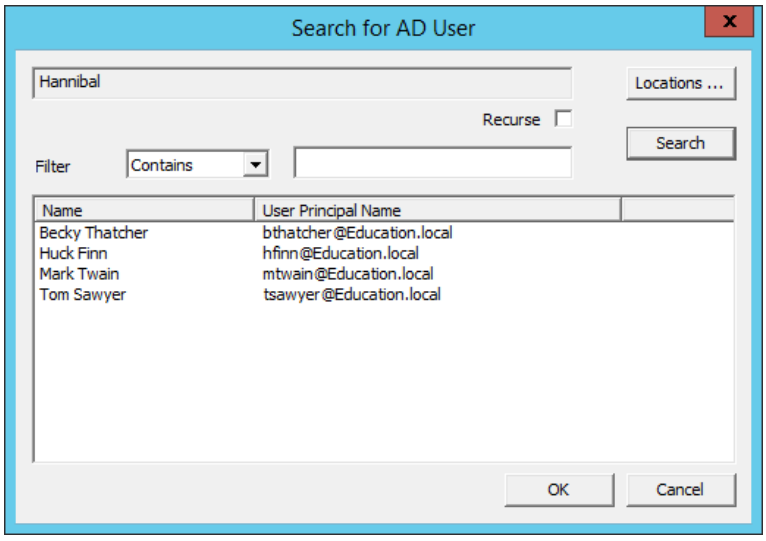
The organizational unit is listed as the location.

Figure 350 - Search Organizational Unit



4. Click Search to populate the dialog box with the users.

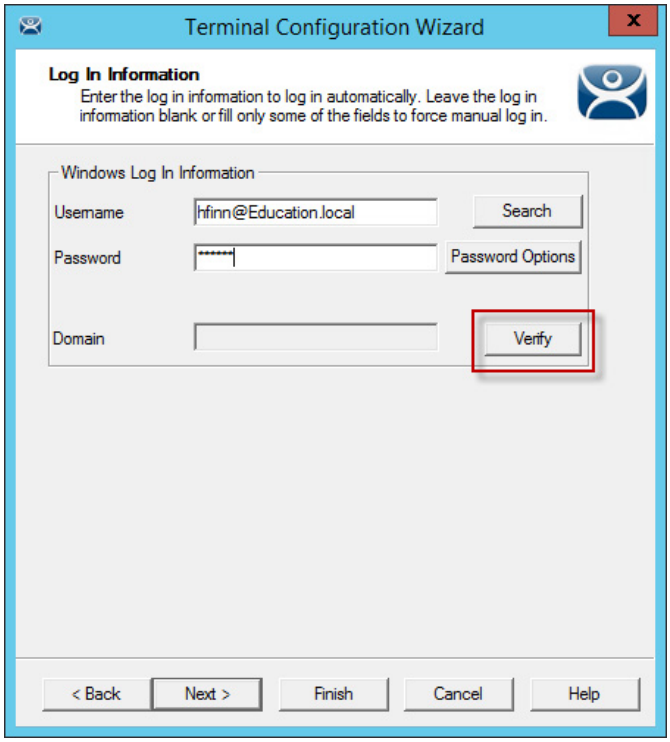
Figure 351 - Search for AD User Dialog Box



5. Highlight the desired user and click OK.

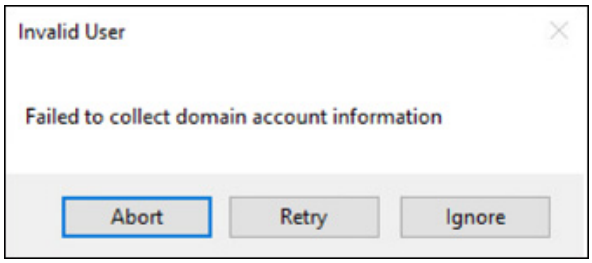
   The domain user is added to the Username field of the Log In Information page.

Figure 352 - Remote Desktop Server Name—Domain



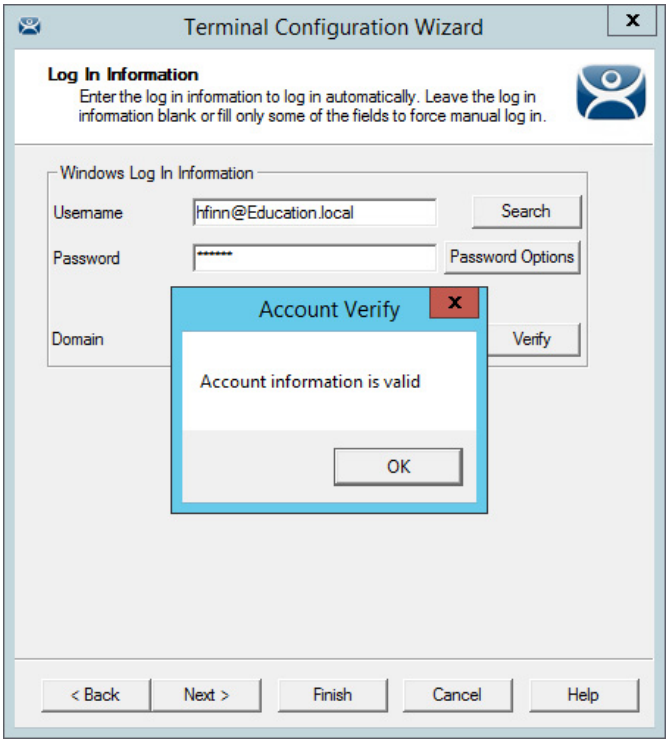
6. Type the password in the Password field.
7. Click Verify to check whether the password you entered is valid.
8. Once it is verified, click Next to continue with the wizard.

Figure 353 - Invalid User



a. If the dialog box indicates an invalid user, click Retry or Ignore. If Ignore is clicked, the user bypasses the credential check.

Figure 354 - Valid Password Message



b. If the dialog box indicates a valid user account, click OK to close the Account Verify dialog box.

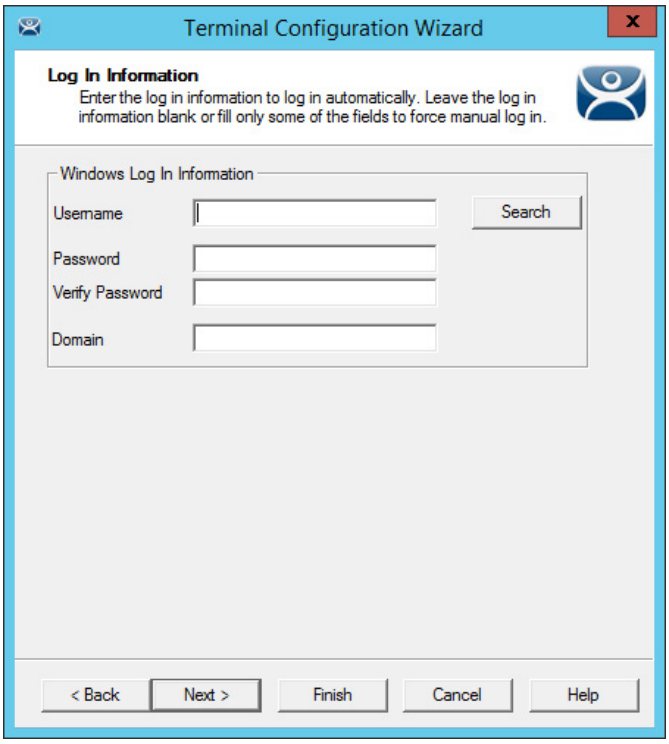
9. Click Next to continue the configuration wizard.

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 can apply Microsoft security as desired.

Figure 355 - Log In Information Page

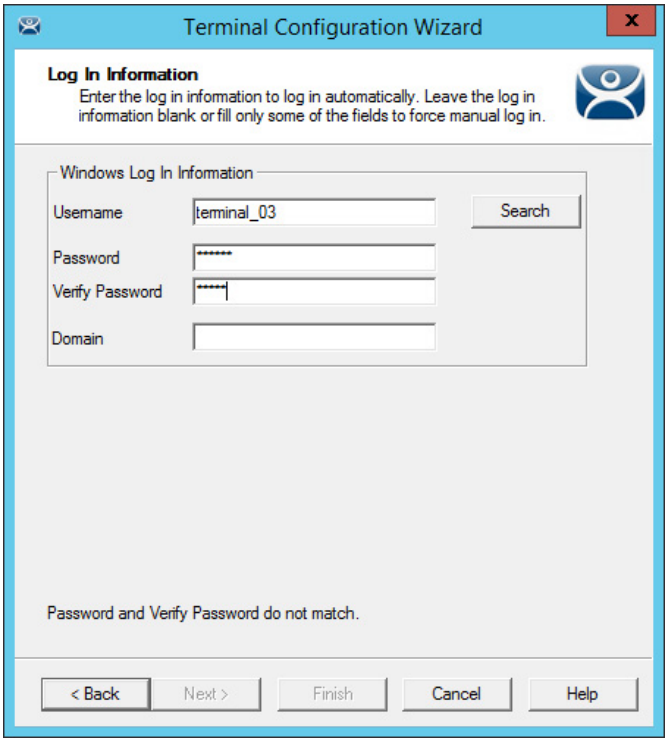


Leaving the Windows Log In Information fields blank forces the user to manually log in to their sessions, which is useful for office settings or shared Terminals. In this case, each user logs in with their personal account and gets the privileges that the administrator granted them.

Local Windows User Accounts

Complete the Windows Log In Information fields with an established Windows account to allow the Terminal to log in automatically and start sessions without user action. Completing this page is useful in industrial settings, where the Terminals are public and always run.

Figure 356 - Completed Log In Information Page



1. Complete the Log In Information page as described here.

Setting	Description
Username	A local Windows account.
Password	The password for the local Windows account. Complete this field if you want the Terminal to log in automatically.
Verify Password	Confirm the password. Complete this field if you want the Terminal to log in automatically.
Domain	Complete this field to use a domain Windows account.

Leave the fields blank to require the user to log in manually each time the Terminal connects.

Individual display clients can be set to require a manual login by clearing the Allow Auto-Login checkbox on the Remote Desktop Services and Workstation Options page of the Display Client Wizard. See Figure 177 on page 136.

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. See Figure 261 on page 195.

2. Click Next to continue the configuration.

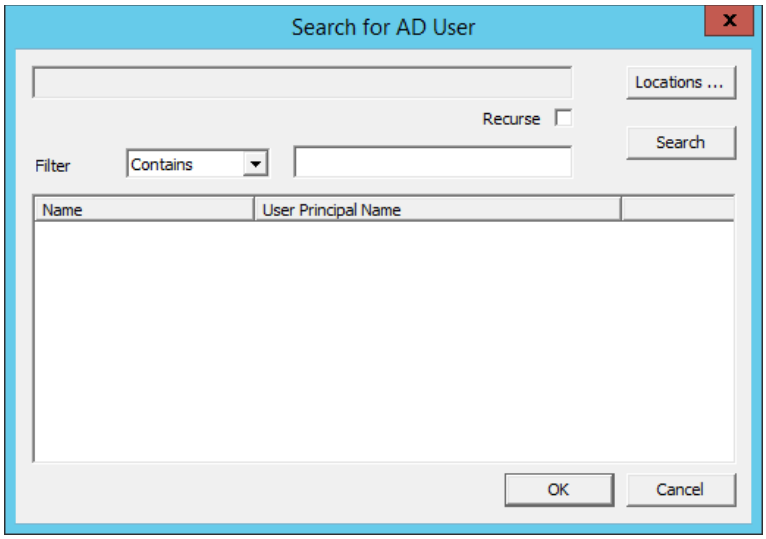
Active Directory User Login Account

A ThinManager Server in a domain can pull an Active Directory account into the Username field using the Search button. This launches a series of dialog boxes, which allow you to select a domain user account for the Terminal login account.

1. Click Search.

   The Search for AD User dialog box appears, which allows you to select an Active Directory user.

Figure 357 - Search for AD User Window



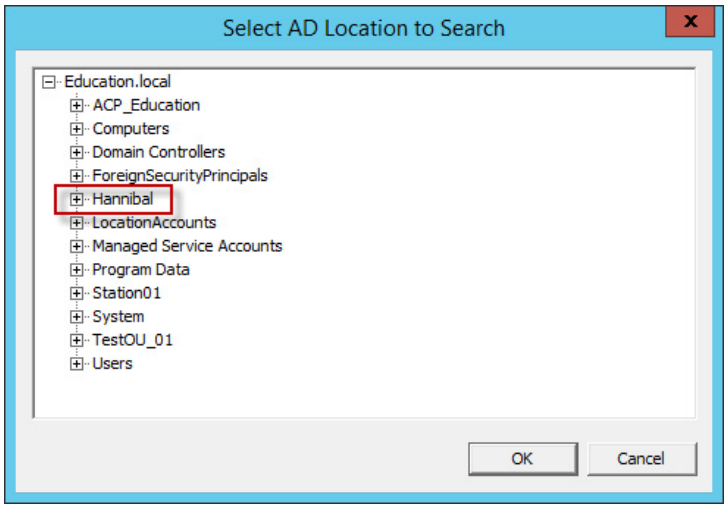
2. Complete the Search for AD User dialog box per these descriptions.

Button/Setting	Description
Locations	Opens the Select AD Location to Search dialog box to select the Organizational Unit (OU) to search.
Search	Searches the selected OU and populates the Name field with the OU members.
Filter	Filters the results with either the Contains or Starts With function and what you type into text field.
Recurse	Sets the Search function to search nested Windows Security Groups when you search a Windows Security Group. The Choose AD Synchronization Mode must be set to Security Group on the Active Directory System Settings dialog box to work, which is launched from Manage>Active Directory>Settings.

3. Click Locations.

   The Select AD Location to Search dialog box appears.

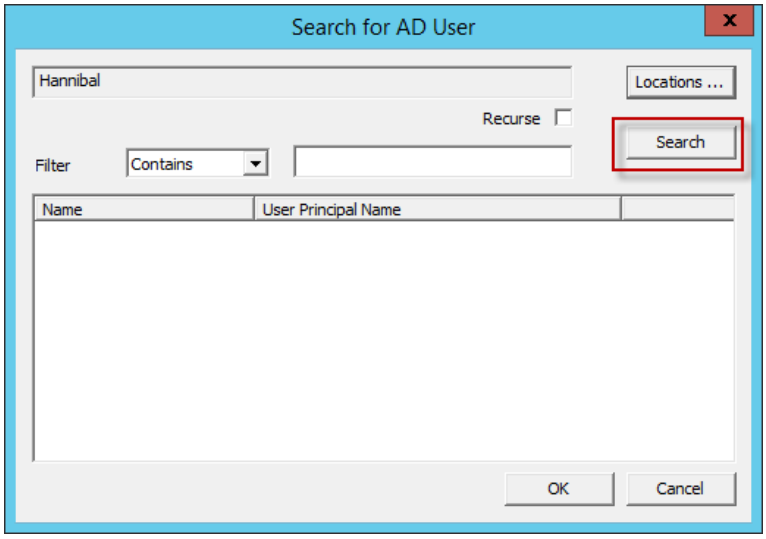
Figure 358 - Select AD Location to Search



4. Highlight the branch of the Active Directory tree that contains your administrative user account and click OK. Highlighting an Active Directory branch reopens the Search for AD User window with the list of domain users from that branch.

   The OU is propagated to the location field of the Search for AD User dialog box.

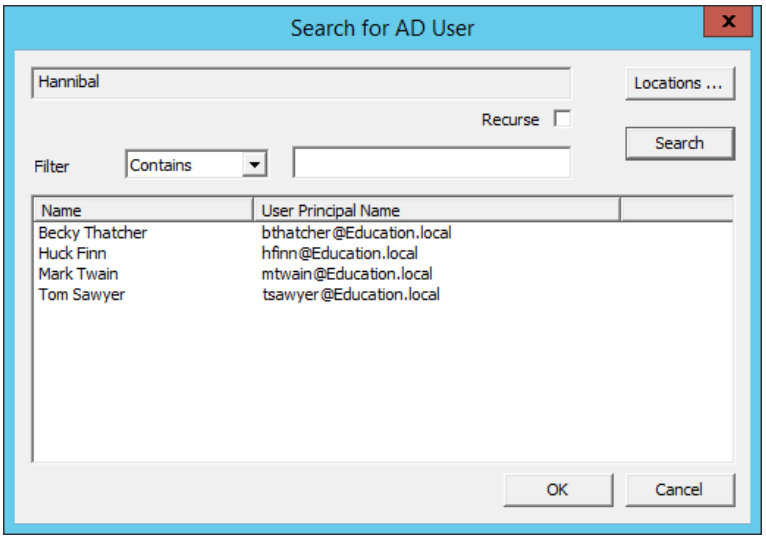
Figure 359 - Search Organizational Unit



5. Click Search.

   The list of domain users from that branch are populated to the dialog box.

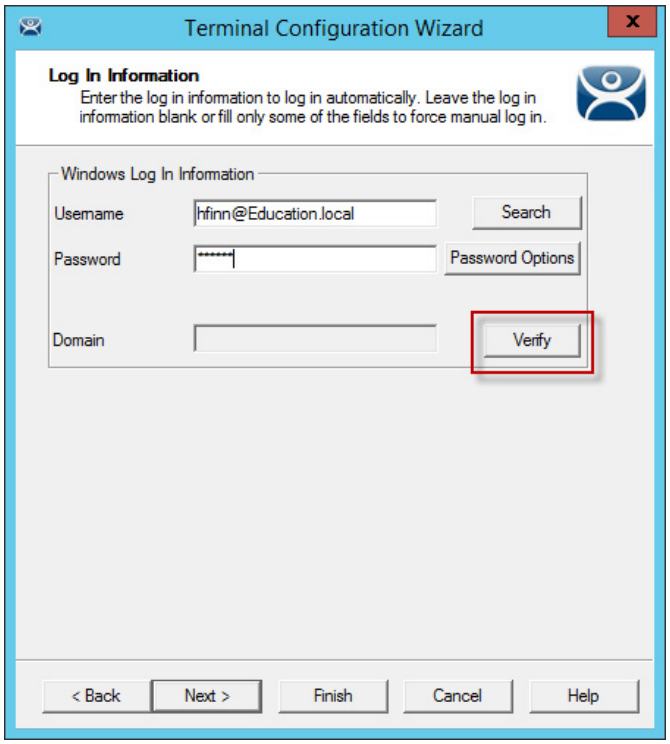
Figure 360 - Search for AD User Window



6. Highlight the desired user and click OK.

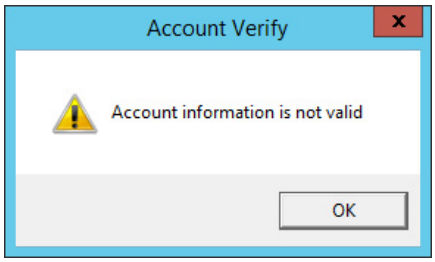
   The domain user is added to the Username field of the Log In Information page.

Figure 361 - Domain User Added to Username Field



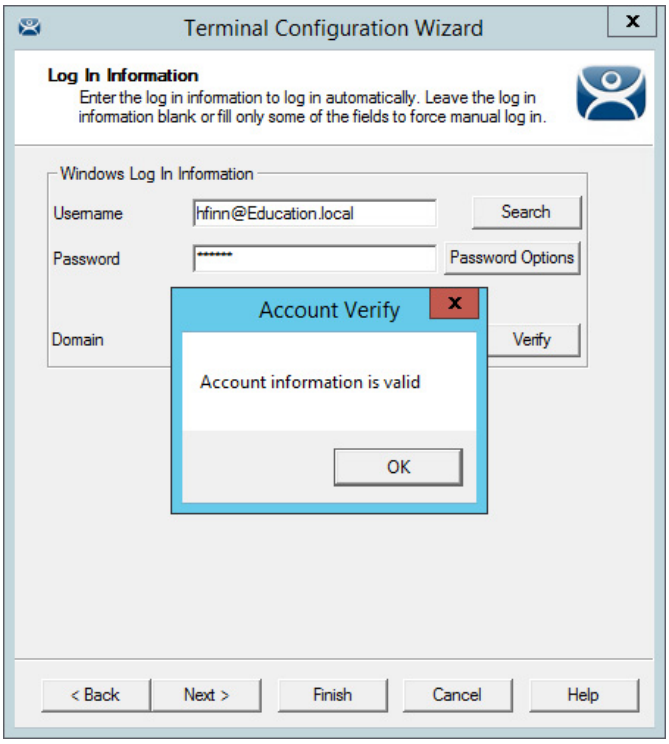
7. Type the correct password into the Password field.
8. Click Verify to check whether the password entered is correct.
   a. If you receive a message of an invalid account, click OK and try again.

Figure 362 - Invalid Account Message



   b. If you receive verification, click OK..

Figure 363 - Valid Password Message



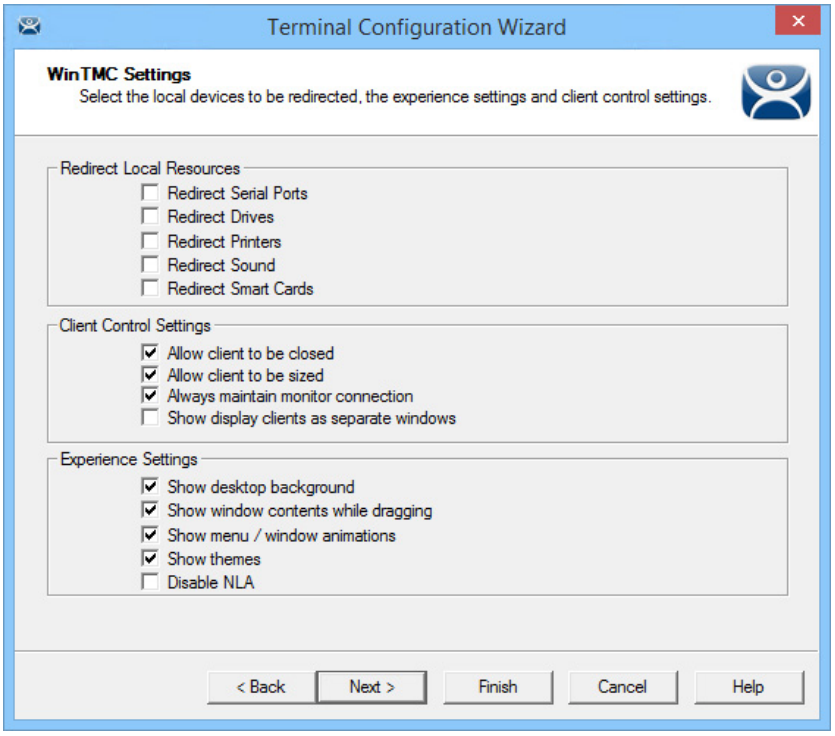
9. Click Next to continue in the configuration wizard.

   The WinTMC Settings page appears.

WinTMC Settings

A Terminal configured as a WinTMC Terminal displays a WinTMC Settings page in the configuration wizard for WinTMC clients. These only apply to connections made by the WinTMC application.

Figure 364 - WinTMC Settings Page



1. Complete the WinTMC Settings page per these descriptions.

Setting	Description
Redirect Local Resources	
Redirect Serial Ports	Makes local serial ports available in a session.(1)
Redirect Drives	Makes local drives available in a session.(1)
Redirect Printers	Makes your local printer available in a session.
Redirect Sound	Allows audio played in your session to play locally.(1)
Redirect Smart Cards	Makes your smart card available in a session.(1)
Client Control Settings	
Allow client to be closed	Enables your user to close the client (WinTMC program).
Allow client to be sized	Enables your user to resize the client.
Always maintain monitor connection	Keeps the monitoring connection active when WinTMC is closed to allow shadowing. Clear this checkbox to release the WinTMC license when the WinTMC program is closed but denies shadow access.
Show display clients as separate windows	Displays multiple Display Clients as separate windows rather than in one window shell.
Experience Settings	
Show desktop background	Enables your user to select a Windows Desktop Background. If not selected, the background is a solid color.
Show window contents while dragging	Allows the window contents to be shown while the window is being dragged.
Show menu/window animations	Enables menu/window animations on the client.
Show themes	Enables your user to select a Windows Theme.
Disable NLA	Disables the user of Network Level Authentication for the client.

(1) Does not work when you connect to a Remote Desktop Server running Windows 2000 or earlier.

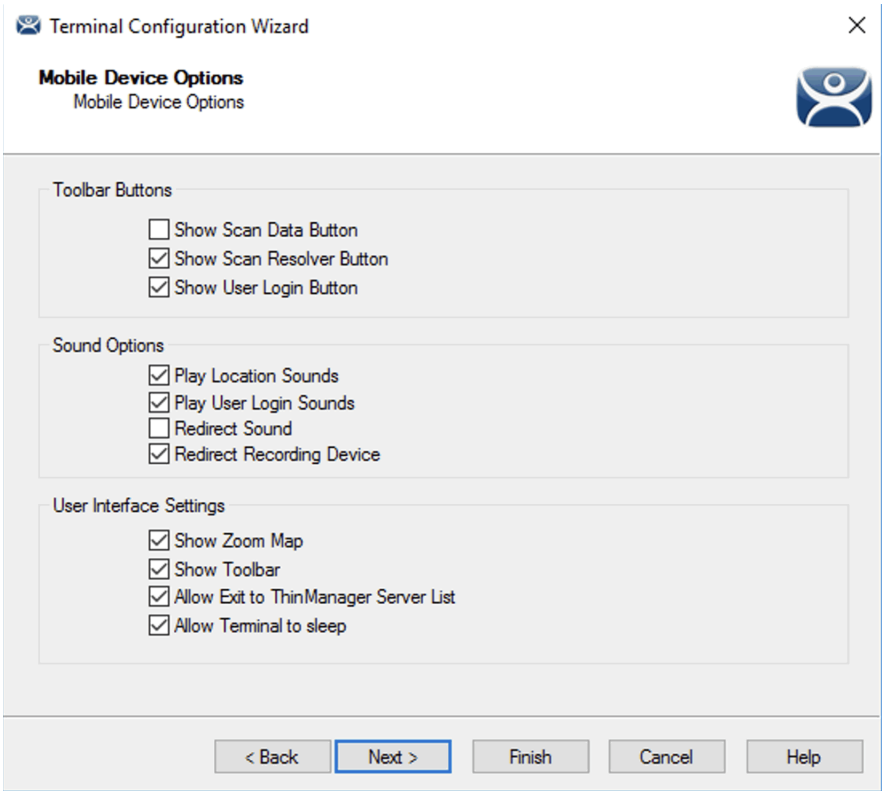
These functions may be denied by user policies or Remote Desktop Server configuration. Check the Microsoft Local Policy, Group Policy, and Remote Desktop Services Configuration.

2. Click Next.

Mobile Device Settings

A Terminal configured as a TMC for Android, TMC for iOS, iTMC (Legacy), or TMC for Windows displays a Mobile Device Options page.

Figure 365 - Mobile Device Options



The Mobile Device Options page has several settings that control the user experience on mobile devices. This page allows you to disable features normally displayed in the mobile apps.

1. Complete this page per the these descriptions.

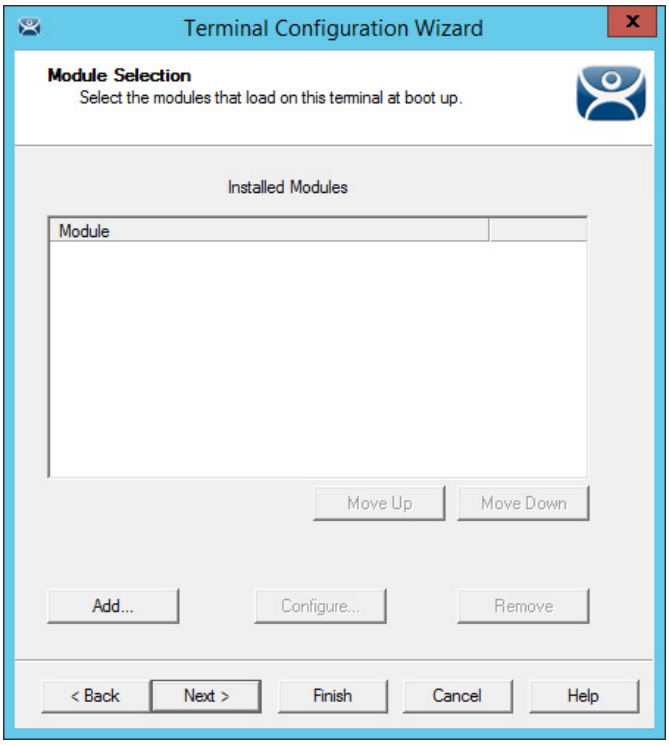
Setting	Description
Toolbar Buttons	
Show Scan Data Button	Clear this checkbox to hide the Scan Data button.
Show Scan Resolver Button	Clear this checkbox to hide the Scan Resolver button.
Show User Login Button	Clear this checkbox to hide the User Login button.
Sound Options	
Play Location Sounds	Plays a sound when a location is entered.
Play User Login Sounds	Plays a sound when the user logs in as a TermSecure or ThinManager user.
Redirect Sound	Allows audio played in your session to play locally.(1)
Redirect Recording Device	
User Interface Settings	
Show Zoom Map	Clear this checkbox to hide the screen map while zooming.
Show Toolbar	Clear this checkbox to hide the app toolbar.
Allow Exit to ThinManager Server List	Clear this checkbox to prevent the user from leaving the app to switch ThinManager Servers.
Allow Terminal to sleep	Clear this checkbox to keep a tablet from going into sleep mode.

(1) Does not work when you connect to a Remote Desktop Server running Windows 2000 or earlier.

2. Click Next.

Module Selection

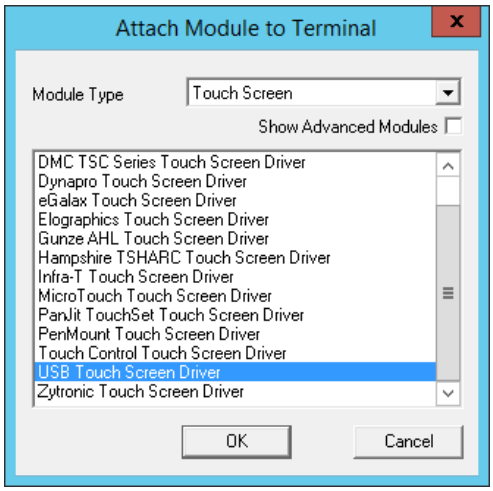
Figure 366 - Module Selection Page of the Terminal Configuration Wizard



Modules are components that provide additional functions to a Terminal but are not required for running the basic configuration. Modules include touchscreen and sound drivers, dual Ethernet® port modules, USB drives, screen savers, and so on.

1. Click Add to launch the Attach Module to Terminal dialog box, which allows you to choose a module to add to the Terminal.

Figure 367 - Attach Module to Terminal



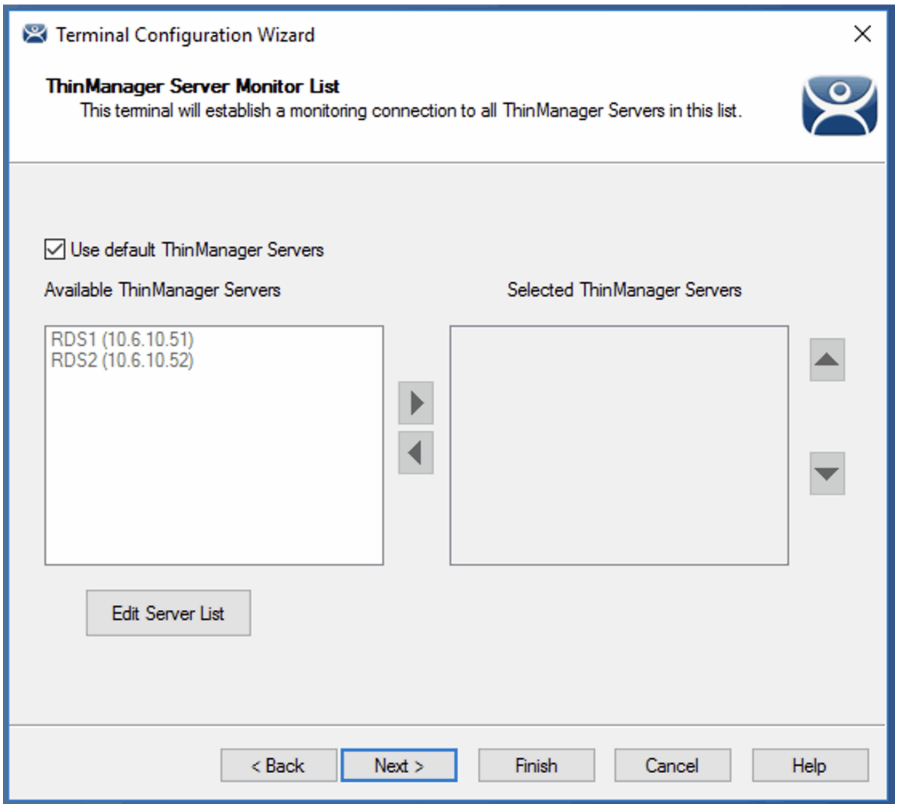
2. Click OK to add the module and return to the Module Selection page.

Modules are covered in detail in Modules on page 549.

3. Click Next on the Module Selection page to continue the configuration.

   The ThinManager Server Monitor List page appears.

Figure 368 - ThinManager Server Monitor



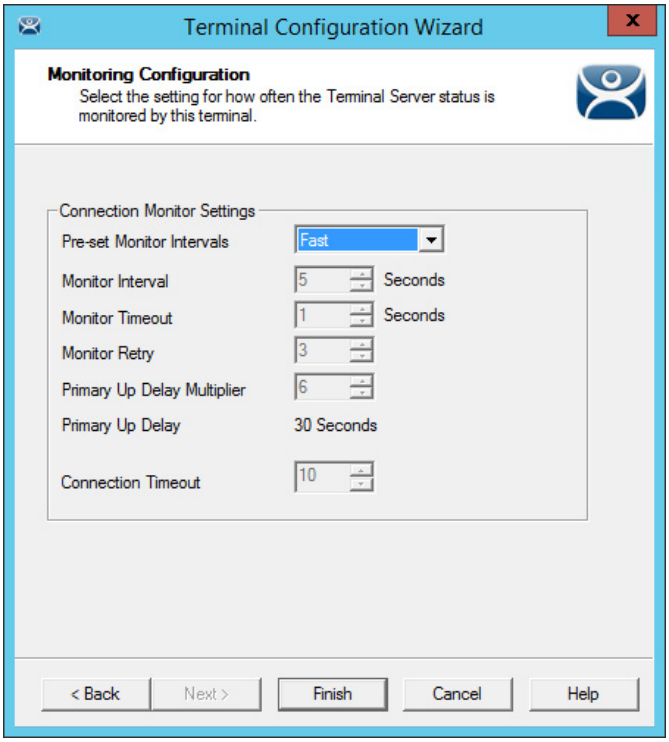
The ThinManager Server Monitor List page is a legacy page from earlier versions of ThinManager and is not used for this version. This page was used before Auto-Synchronization was added to ThinManager. This page was needed to list the ThinManager Servers for the Terminals. Auto-Synchronization does this automatically; so, the page does not appear when using Auto-Synchronization.

However, the ThinManager Monitor List page remains as part of the configuration wizard to prevent problems when upgrading from an old ThinManager system to a modern one.

4. Click Next to continue the configuration.

   The Monitoring Configuration page appears, which sets the speed with which failover is detected and initiated.

Figure 369 - Monitoring Configuration Page



A thin client creates a socket connection to the Remote Desktop Server. If the socket is disconnected, the Terminal tries to reconnect and fails over based on these settings.

5. Complete the Monitoring Configuration based on these descriptions.

Setting	Description
Pre-set Monitor Interval	
Fast/Medium/Slow	These setting have a set rate for the frequency whith which the Remote Desktop Server status is checked.
Custom	Allows the administrator to change the settings from the defaults.
Monitor Interval	The period of time the Terminal waits after losing the socket connection before it tries to reconnect.
Monitor Timeout	The period of time the Terminal waits between tries.
Monitor Retry	The number of times the Terminal tries to reestablish a connection before failing over.
Primary Up Delay Multiplier	A constant used to generate the Primary Up Delay time.
Primary Up Delay	A delay added (usually set to 30 or 60 seconds) to allow a Remote Desktop Server to get fully booted before the Terminal tries to login. This time period is equal to the Monitoring Interval multiplied by the Primary Up Delay Multiplier. This setting prevents a Terminal using Enforce Primary from switching back to its primary Remote Desktop Server before it is ready.
Connection Timeout	The amount of time in which a Terminal tries to connect to a Remote Desktop Server before giving up to try the next server.

The Fast setting is recommended.

Faster rates cause a quicker failover, but more frequent checks on Remote Desktop Server status cause more network traffic. Slower rates cause less traffic, but they slow the failover speed a little.

6. Click Finish to save the settings.

Copy Settings from another Terminal

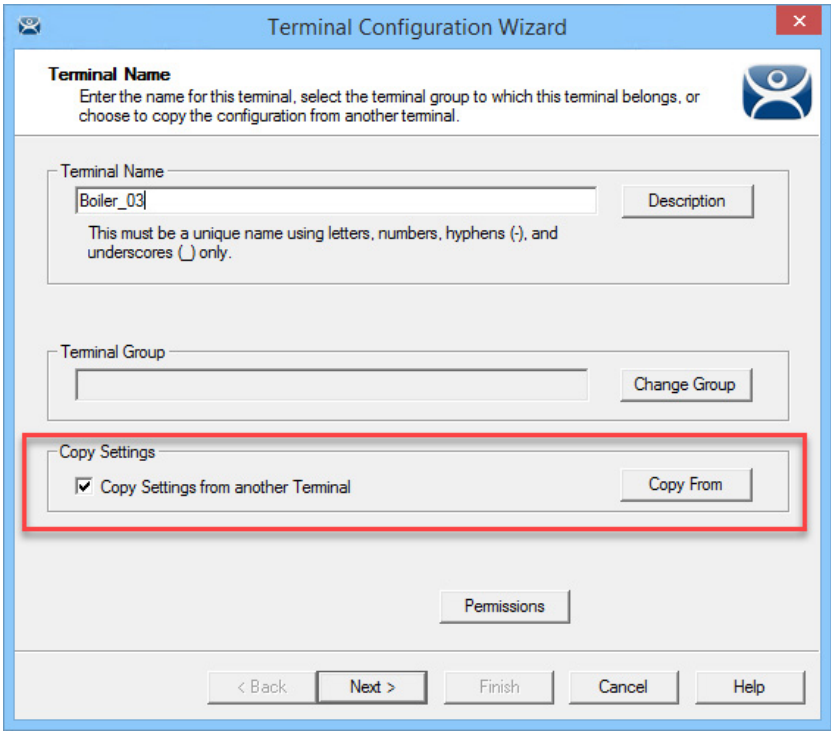
You can copy the settings from one Terminal during the creation process to speed the configuration.

To create a new Terminal, follow these steps.

1. Right-click on the Terminals branch and choose Add Terminal.

   The Terminal Name page of the Terminal Configuration Wizard appears.

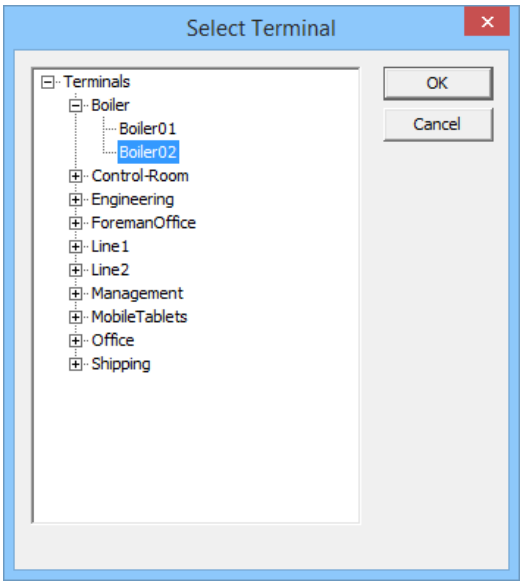
Figure 370 - Terminal Name Page



2. Check Copy Settings from another Terminal.
3. Click Copy From.

   The Select Terminal dialog box appears, which shows a tree with all of the created Terminals.

Figure 371 - Select Terminal



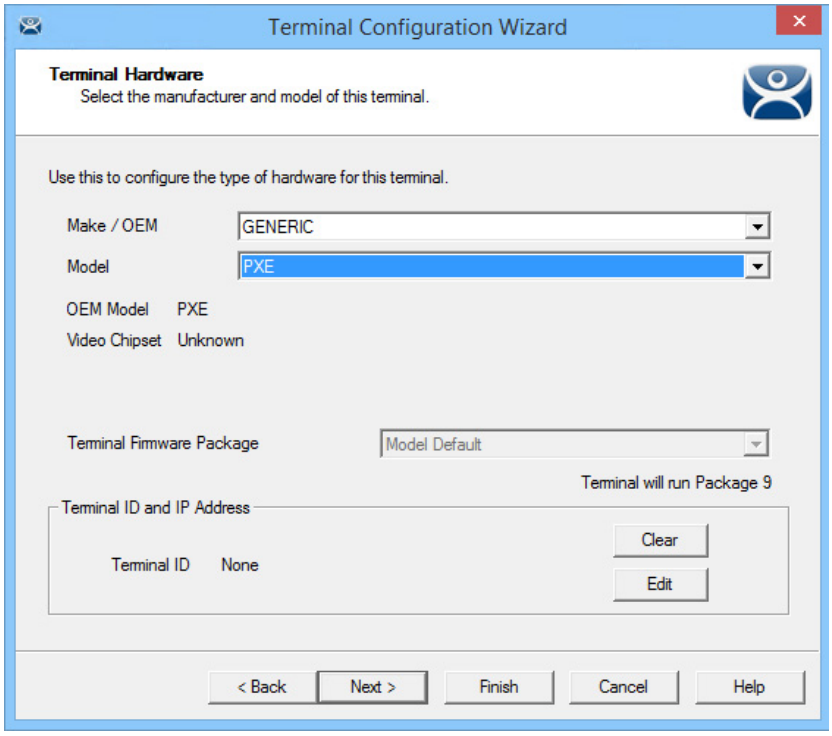
4. Highlight a Terminal and click OK.

   The dialog box closes and the configuration is applied from the highlighted Terminal to the new Terminal.

5. Click Next.

   The Terminal Hardware page appears, where the new Terminal gets Terminal hardware applied to it.

Figure 372 - Terminal Hardware Page



6. Choose the hardware Make and Model to make Finish available.

You should also verify the Username and Password on the Windows Log In Information page since every Terminal needs a unique Windows account login. See Figure 618 on page 433 for more details.

Use Groups for Organization

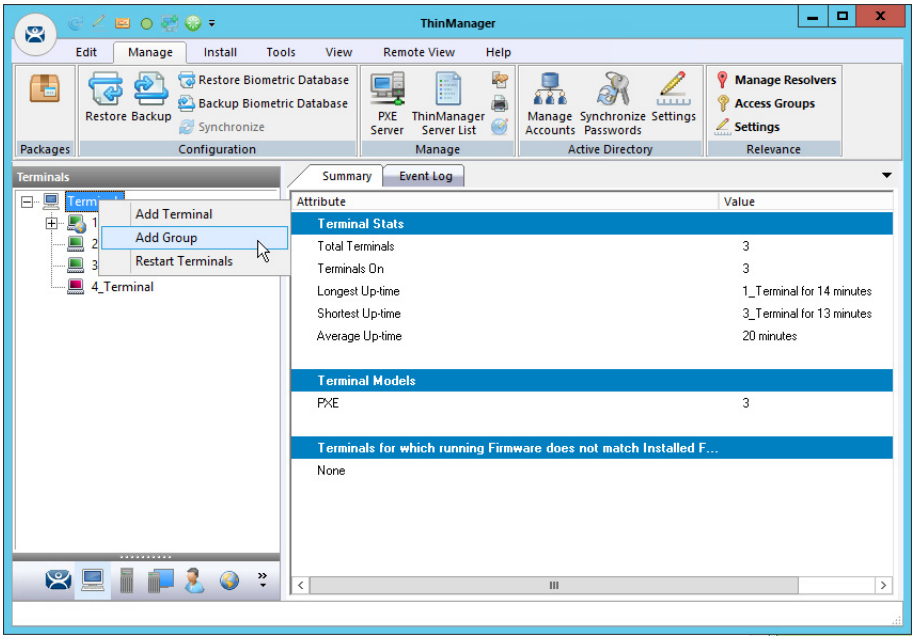
ThinManager allows the consolidation of Terminals into Terminal Groups. which are used like folders to organize the Terminals into functional or geographic groups. The Group Setting checkbox allows settings to be applied to all members of the group to speed configuration and change deployment.

Any group setting is passed down to its members.

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

1. Click the Terminal icon at the bottom of the ThinManager tree to open the Terminals tree.

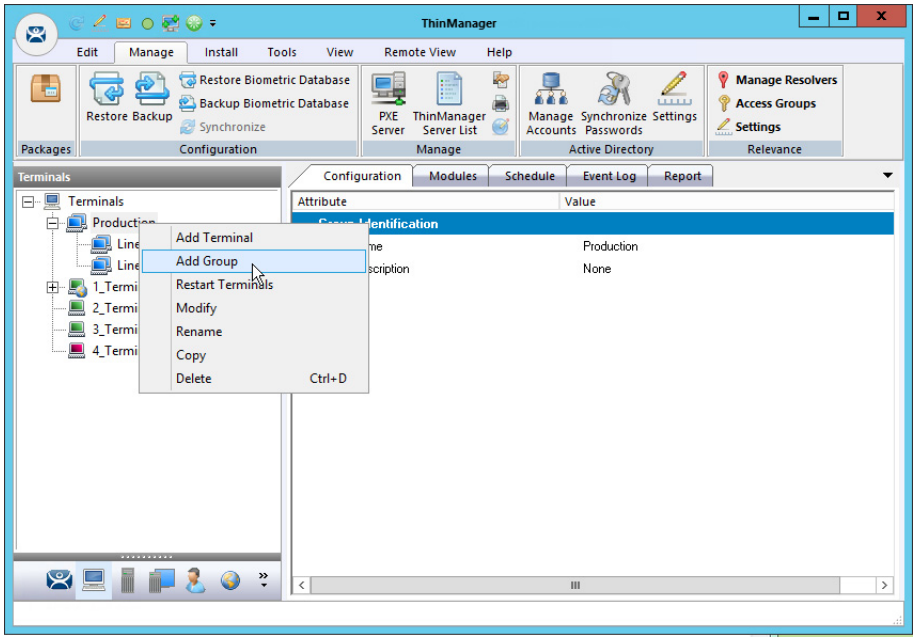
Figure 373 - Add Group Command



2. Right-click on the Terminals branch and choose Add Group.

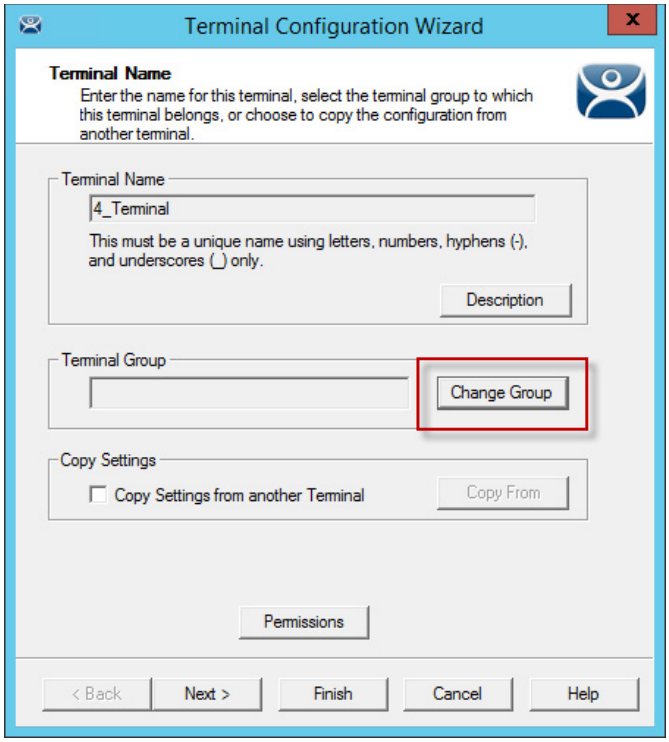
   The Terminal Configuration Wizard appears. The wizard for the Group parallels the Terminal Configuration Wizard since the group is a collection of Terminals.

Figure 374 - Add Group Menu



3. (Optional) Right-click on a group and choose Add Group to add a subgroup, which adds a group under the highlighted group.

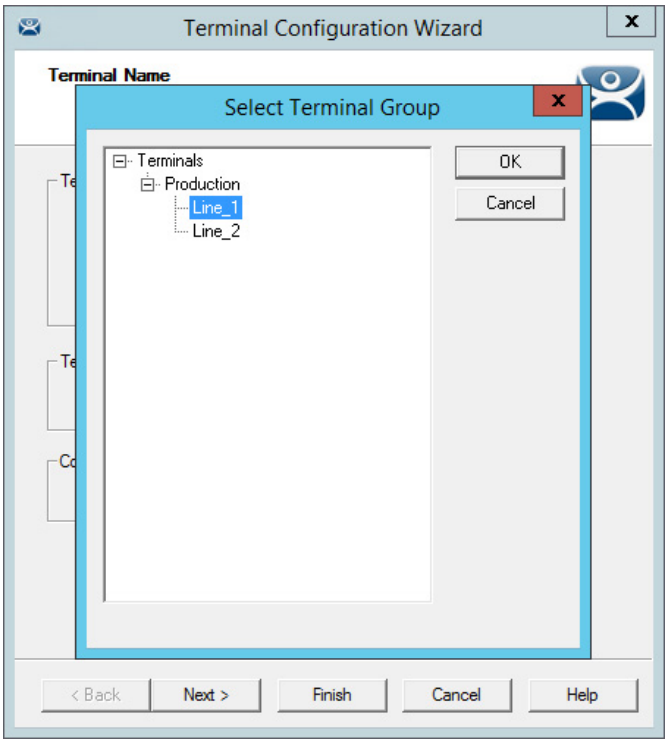
Figure 375 - Change Group Button



4. Click Change Group to add a Terminal.

   The Select Terminal Group dialog box appears, which lists the groups and subgroups.

Figure 376 - Select Terminal Group

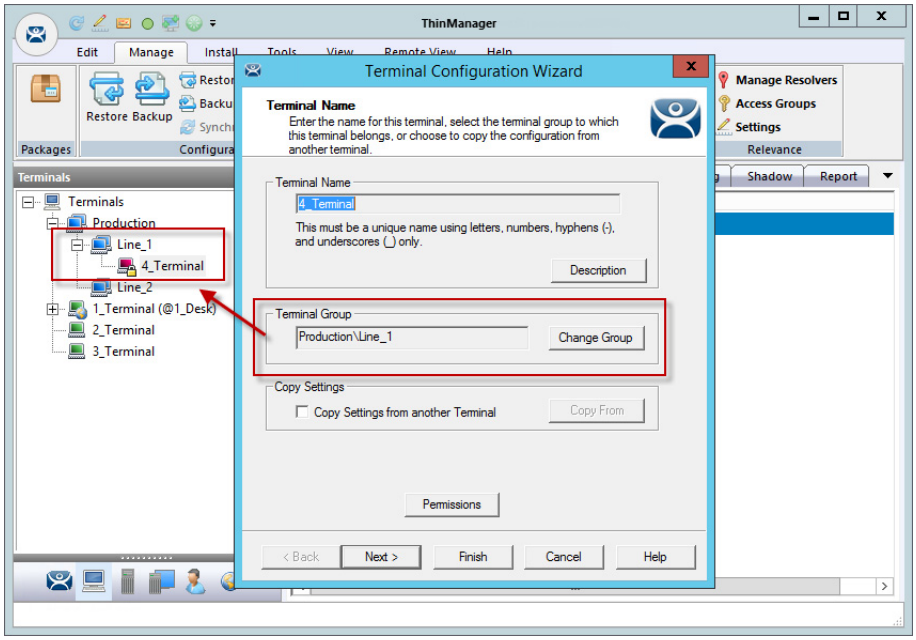


5. Expand the tree as needed, highlight the desired group, and click OK.

   The Terminal is assigned to the selected group.

6. Click Finish to close the wizard and apply the changes before you continue. If you need to adjust the configuration, close the wizard and then reopen it.

Figure 377 - Group Membership



The group appears in the Terminal Group field, and the Terminal appears nested in the group in the Terminals tree.

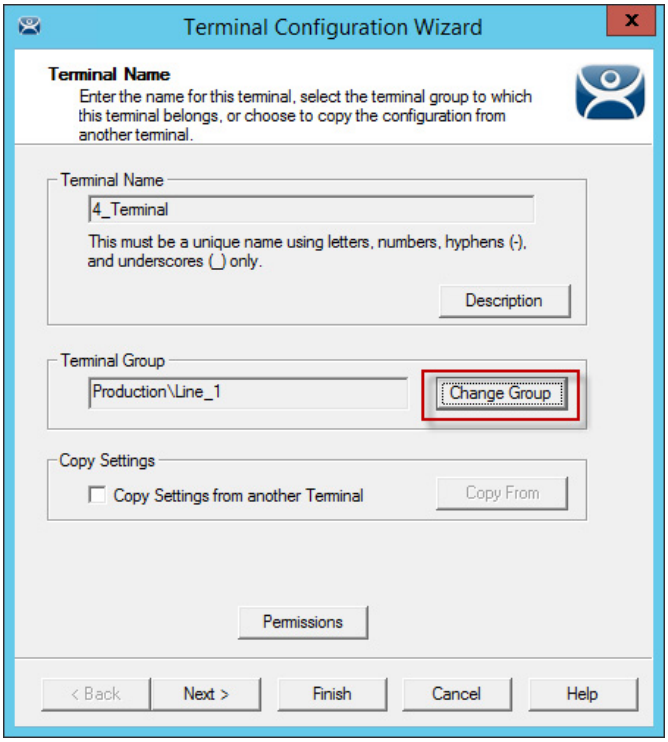
Moving Out of a Group

A Terminal can be removed from a group by moving it to the Terminals branch of the Select Terminal Group dialog box.

1. Double-click on the Terminal you want to change in the Terminals tree.

   The Terminal Name page of the Terminal Configuration Wizard appears.

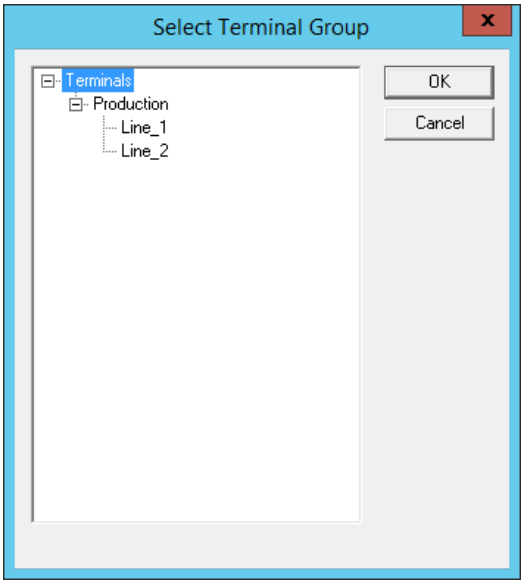
Figure 378 - Change Group Button on the Terminal Name Page



2. Click Change Group.

   The Select Terminal Group dialog box appears.

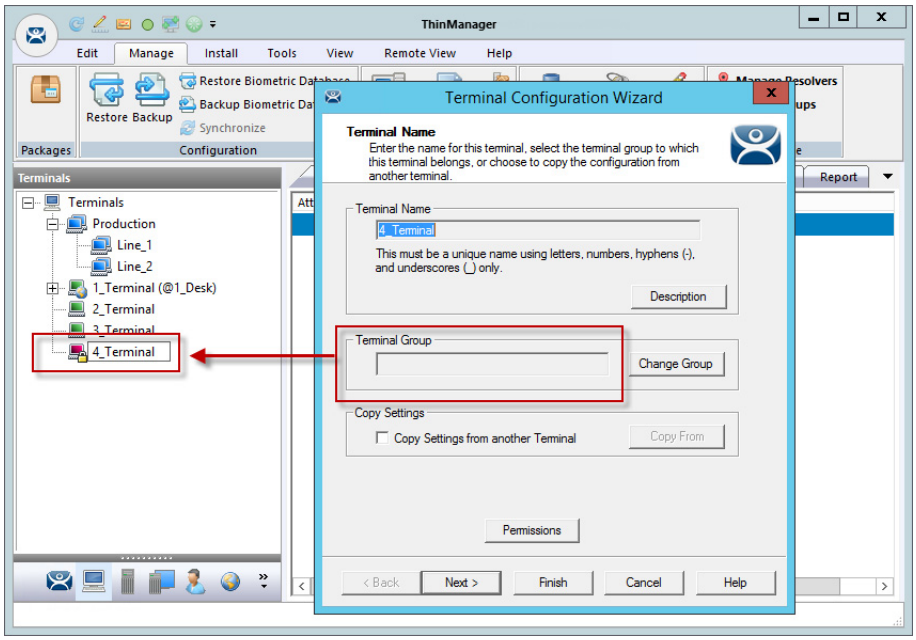
Figure 379 - Select Terminal Group Window



3. Choose the top-level Terminals in the Terminal Group tree and click OK.
4. In the Terminal Configuration Wizard, click Finish.

   The changes are applied. If you need to adjust the configuration, close the wizard, then reopen it.

Figure 380 - Terminals Tree Showing Ungrouped Terminal



Once the wizard is closed, the ThinManager Terminals tree shows the Terminal under the Terminals branch and the Terminal Group field of the Terminal Name page is empty.

Use Groups for Configuration

ThinManager Terminal Groups can be used for faster configuration as settings configured at the group level are applied to all the Terminals in the group. You can use Group Setting with every setting in the Group Configuration Wizard.

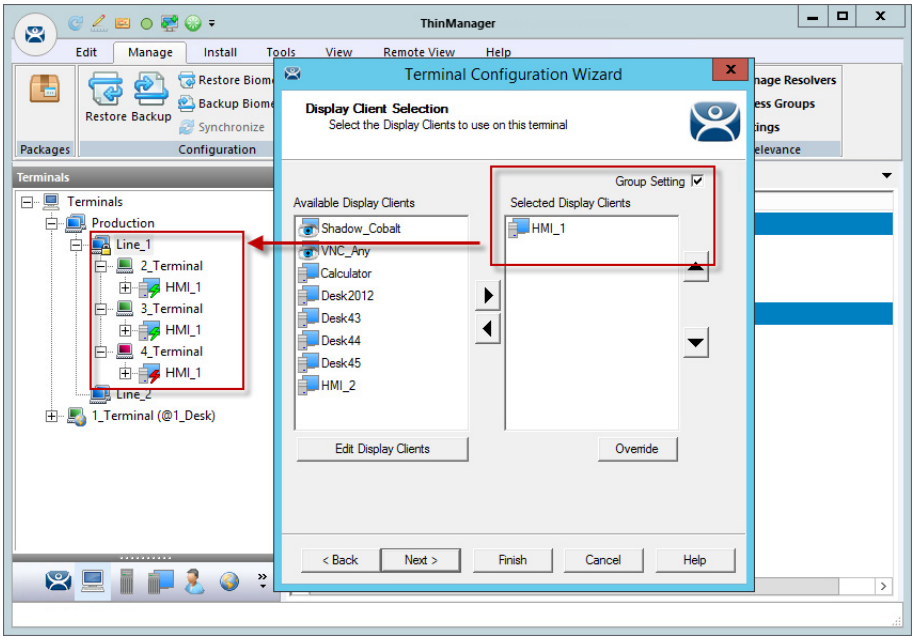
Adding display clients is easy when you use Group Settings.

1. In the Terminals tree, double-click on a Terminal.

   The Terminal Group Name page of the Terminal Configuration Wizard appears.
2. Click Next until the Display Client Selection page appears.

   Figure 381 shows that Line_1 group has three Terminals with a single display client assigned.

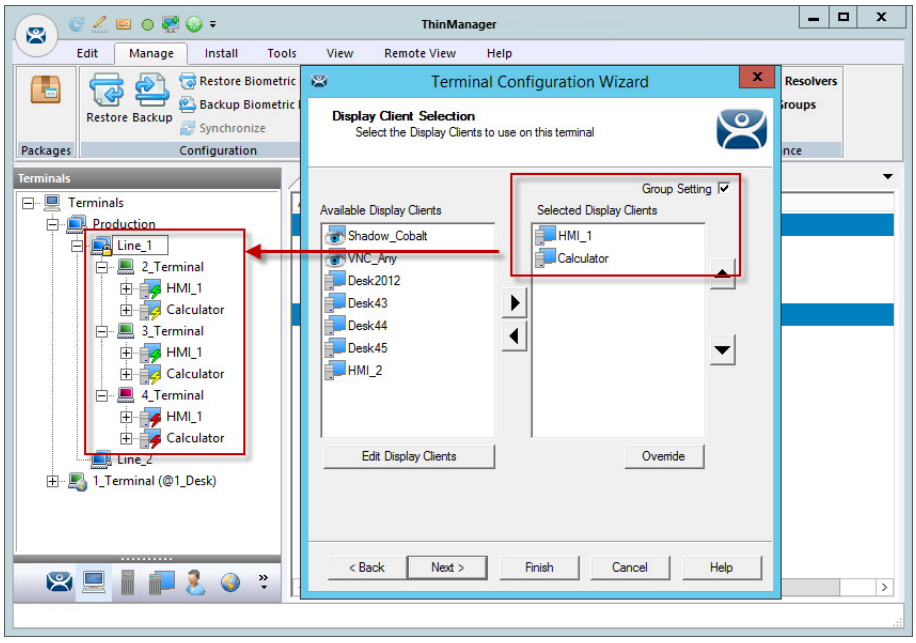
Figure 381 - Display Client Deployed With Group Settings



3. Check Group Setting.
4. Change the Selected Display Clients.
5. Click Finish.
6. Restart the Terminals.

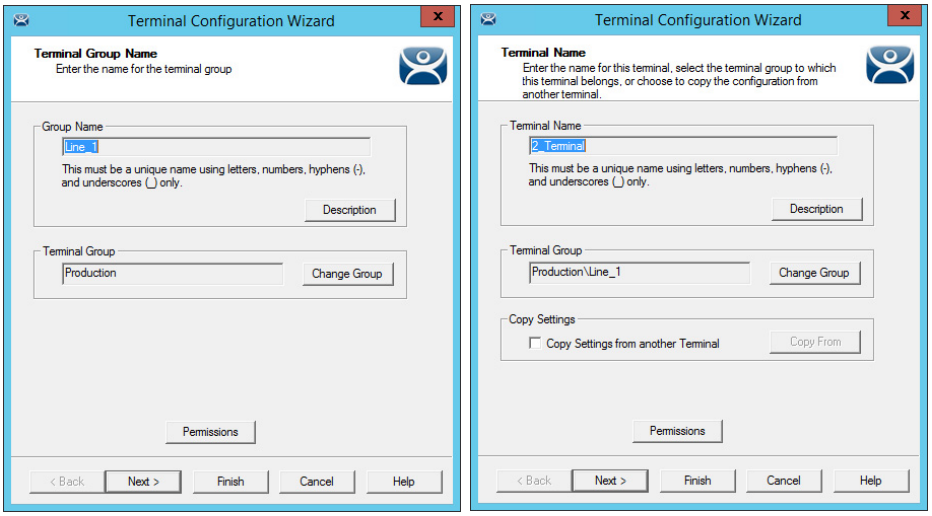
Figure 382 shows that the Line_1 group had its group display clients changed one time, and the change was propagated to all the member Terminals.

Figure 382 - Display Clients Deployed With Group Settings



To demonstrate the effects of using Group Setting, the following figures show the Group Configuration Wizard on the left and the Terminal Configuration Wizard of a member Terminal on the right.

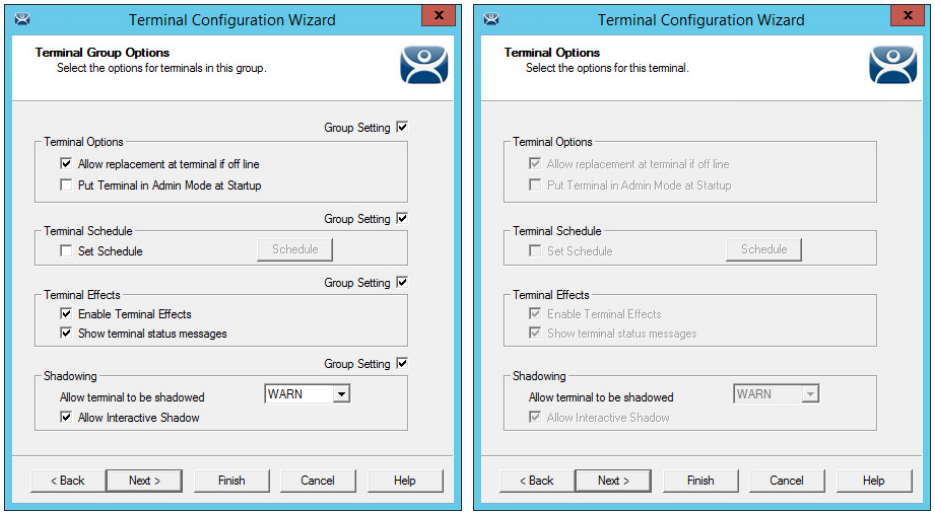
Figure 383 - Terminal Group Name and Terminal Name Pages



The left figure shows the opening screen of the Group Configuration Wizard while the right figure shows the Terminal Configuration Wizard of a group member.

The Group Configuration Wizard does not show the Terminal Hardware page since that is an individual selection, not a group selection. The Terminal Configuration Wizard shows the Terminal Hardware page, where you select the hardware for the individual device.

Figure 384 - Terminal Group Options and Terminal Options Pages



On the left, Group Settings is checked in the Group Configuration. On the right, the Terminal Configuration inherits Group Settings; therefore, Group Settings is dimmed.

Figure 385 - Group Terminal Mode Selection and Terminal Mode Selection Pages

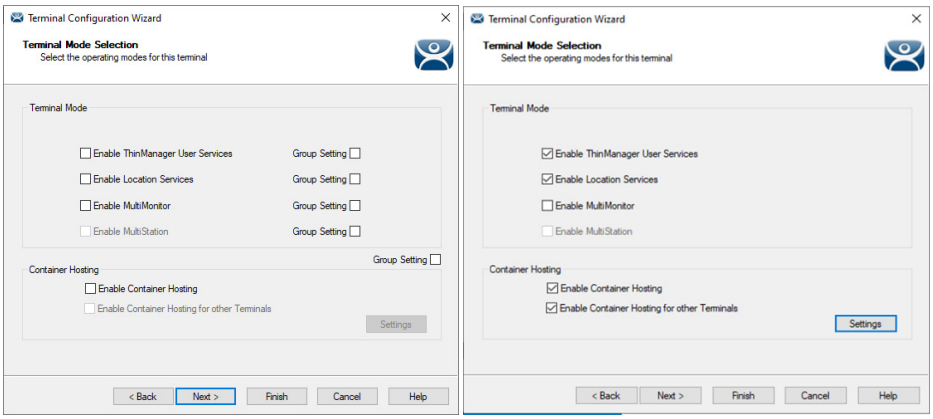
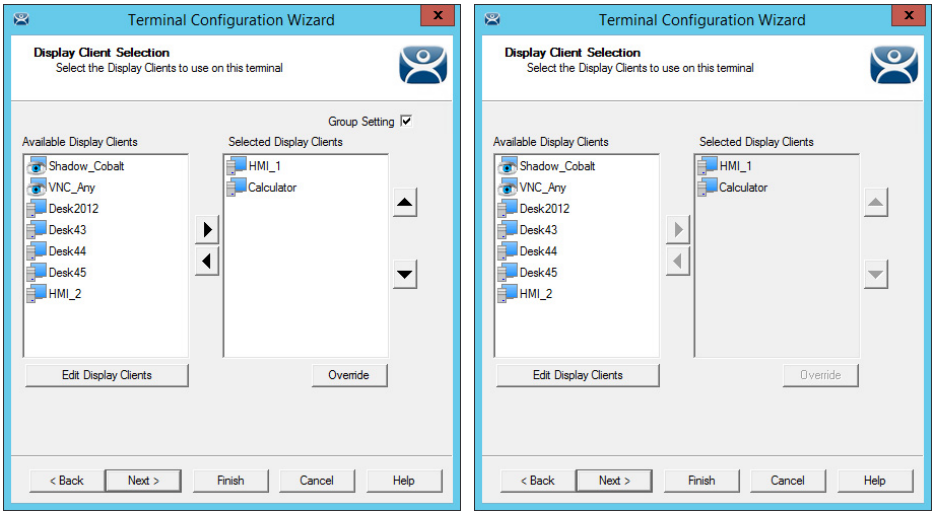


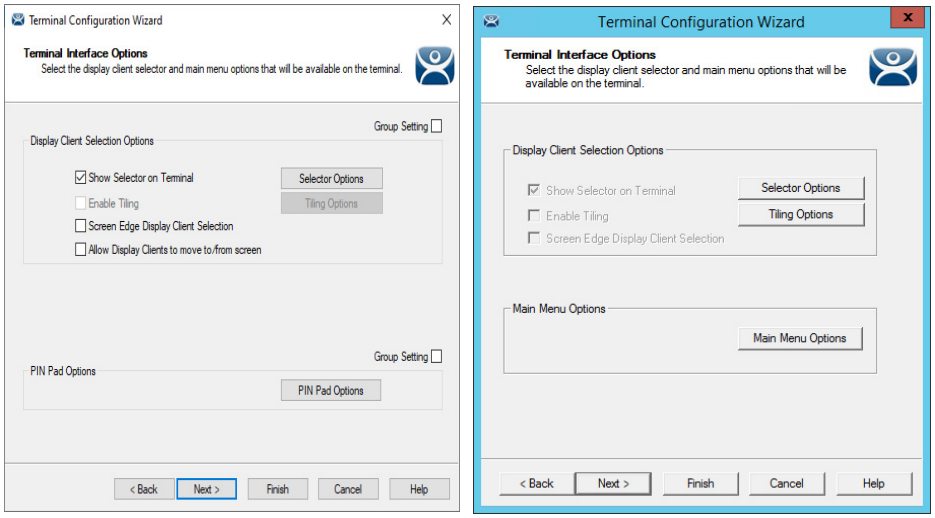
Figure 386 - Group Display Client Selection and Terminal Display Client Selection Pages



Choose display clients on the Group Configuration Wizard and check Group Setting to assign those display clients to all member Terminals. You cannot add or subtract from the list in the Terminal Configuration Wizard.

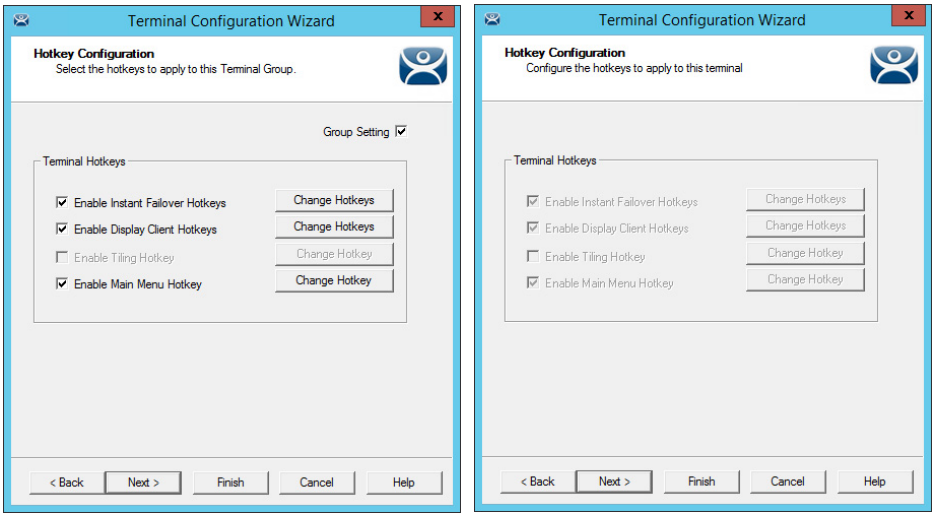
The Group Setting is efficient when all members of a group run the same applications. If members need a different application, clear the Group Setting checkbox and assign the display clients.

Figure 387 - Group Terminal Interface Options and Terminal Interface Options Pages



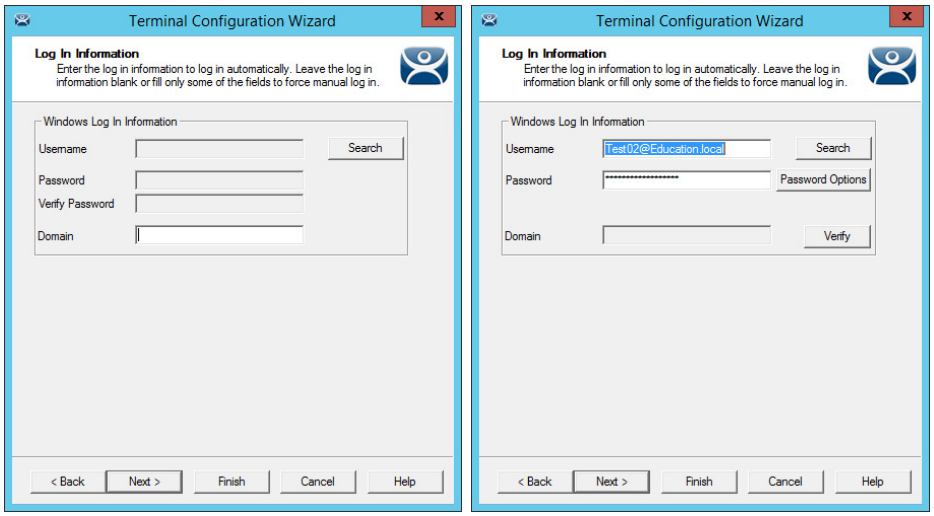
On the left, the Group Configuration has Group Settings checked. On the right, the Terminal Configuration has the settings dimmed because it is inheriting the Group Settings.

Figure 388 - Group Hotkey Configuration and Terminal Hotkey Configuration Pages



On the left, the Group Configuration has the Group Settings checked. On the right, the Terminal Configuration has the settings dimmed because it is inheriting the Group Settings.

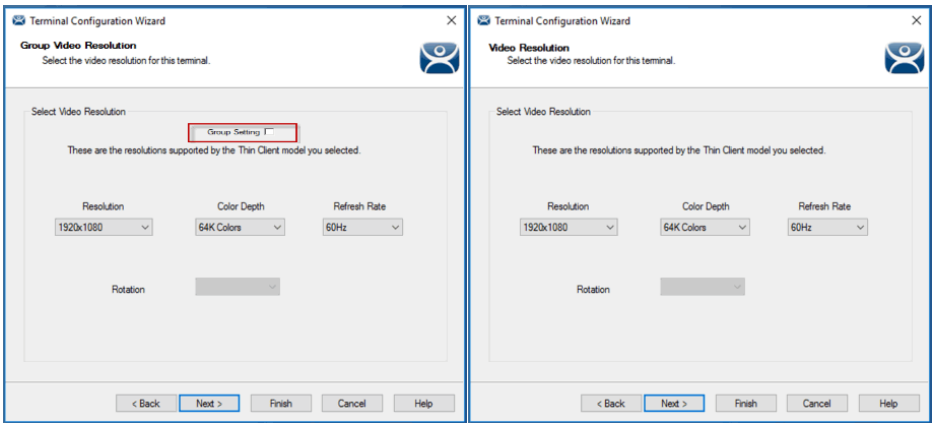
Figure 389 - Group Log In Information and Terminal Log In Information Pages



The Group Log In Information page is dimmed and does not 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.

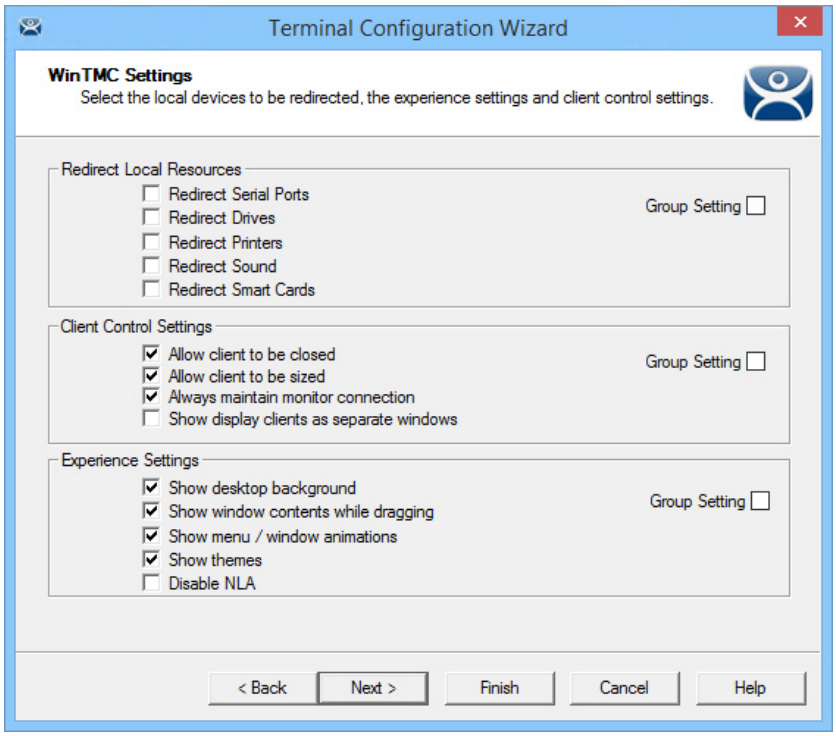
Figure 390 - Group Video Resolution and Terminal Video Resolution Pages



The video resolution can be applied to all members of a group. However, if the monitor size is changed unexpectedly, you must clear the Group Settings checkbox and apply the resolutions individually.

Since resolution may vary from terminal or station, it is not better to set video resolution at the group level.

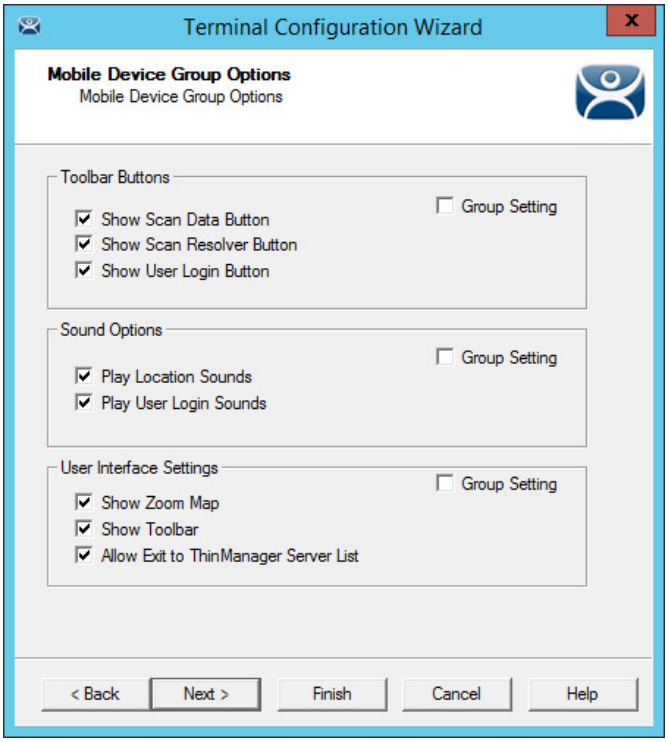
Figure 391 - WinTMC Settings



The Group Configuration Wizard has a WinTMC Settings page, which allows configuration of WinTMC clients with Group Settings.

The WinTMC Settings page does not appear in the Terminal Configuration Wizard unless GENERIC/WinTMC is chosen as the Make and Model on the Terminal Hardware page.

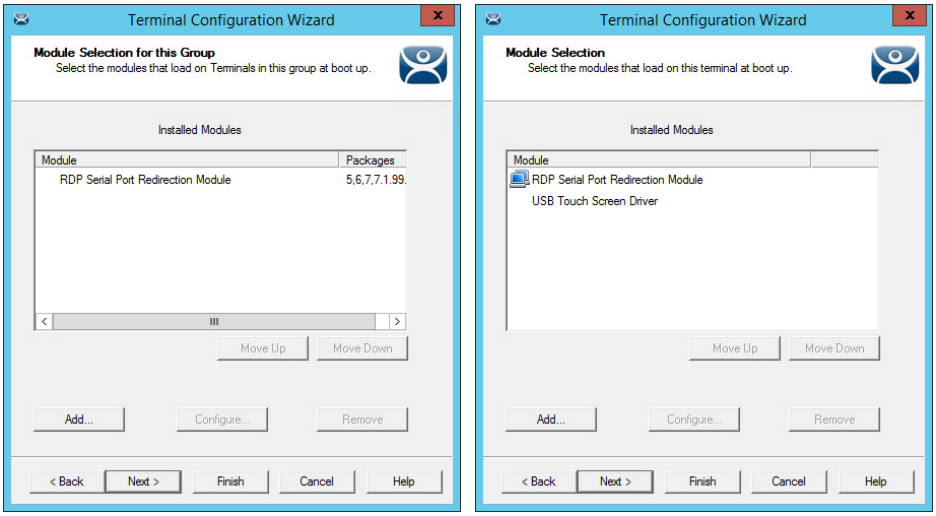
Figure 392 - Mobile Device Group Options



The Group Configuration Wizard has a Mobile Device Group Options page, which allows mobile clients to be configured with Group Settings.

This page does not appear on the Terminal Configuration Wizard unless GENERIC/Android Device or Apple/iOS is chosen as the Make and Model on the Terminal Hardware page.

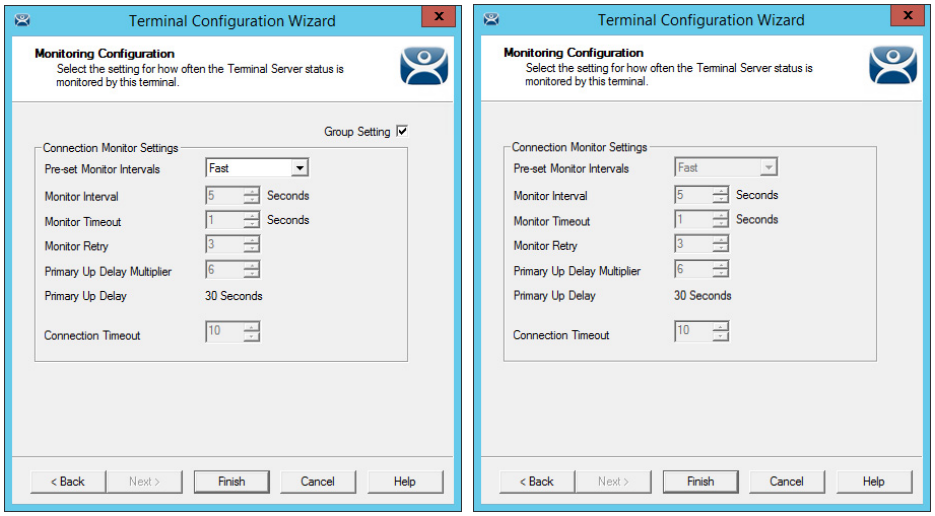
Figure 393 - Group Module Selection and Terminal Module Selection



Modules can be added at the Group and Terminal levels. Modules selected for a group display a Group icon on the Module Selection page of its members.

The left-side image in Figure 393 shows a module added to the group configuration. The image on the right shows that module on the Terminal with the Group icon to show from where it originated. Also in the image at right, the USB touch screen module was added to the Terminal, but does not show a group icon.

Figure 394 - Terminal Group Name and Terminal Name



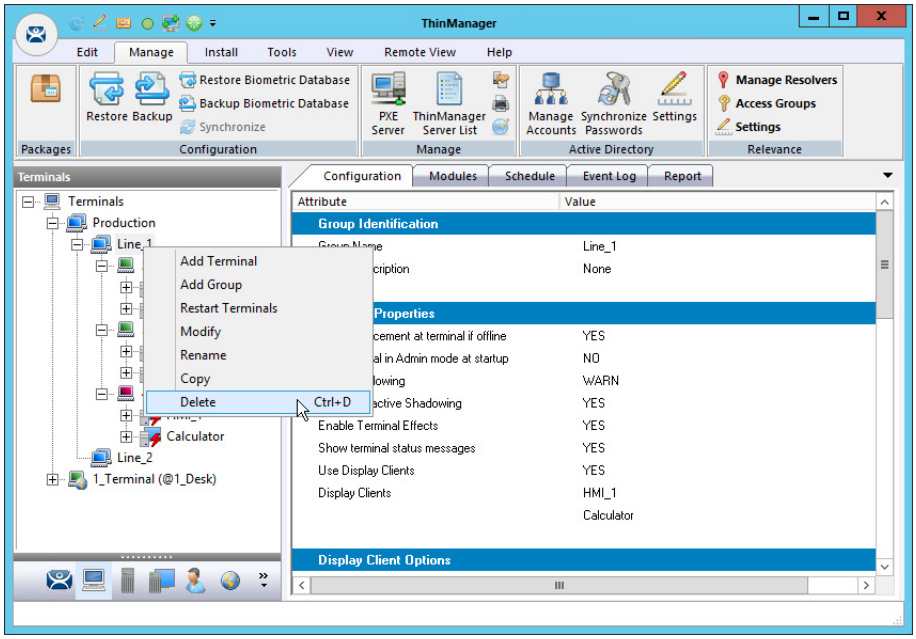
In Figure 394, the Group Configuration on the left has the Group Settings selected. The Terminal Configuration on the right has the settings dimmed because it is inheriting the Group Settings.

Deleting Old Groups

Follow these steps to delete an unnecessary group.

1. Click the Terminals icon at the bottom-left of ThinManager to open the Terminals tree.

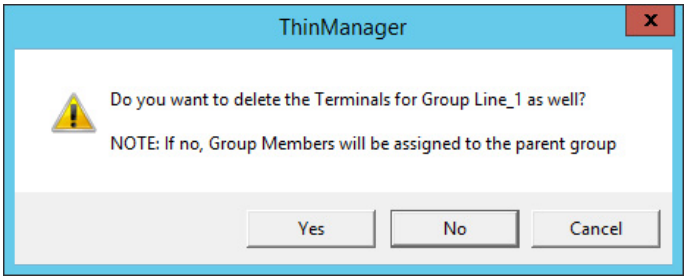
Figure 395 - Delete Option on Group Right-click Menu



2. Right-click on the group and choose Delete.

   The Delete dialog box appears.

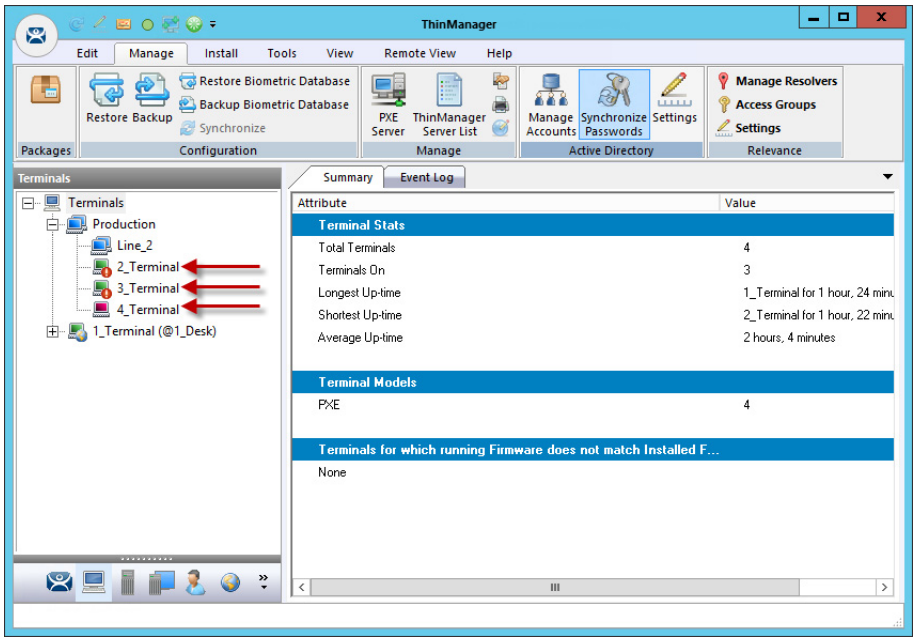
Figure 396 - Delete Dialog Box



IMPORTANT Read the dialog box before taking an action to prevent the loss of needed Terminals.

3. Click Yes, No, or Cancel.
   a. Click Yes to delete the group **and** member Terminals.
   b. Click No to delete the group but leave the Terminals under the Terminals tree.
   c. Click Cancel closes the dialog without deletion.

Figure 397 - Terminal Tree Showing Terminals without the Group



The Terminals from Line_1 are now nested under the Production group in the Terminals tree.

EXAMPLE The two active Terminals from the Line_1 group are showing the Alert icon, indicating that they must be restarted to load the changed configurations.

IP Configuration

These are the six types of Terminals that can be used in a ThinManager system.

- ThinManager-ready thin clients
- ThinManager-ready wireless thin client (certain hardware only, see thinmanager.com/hardware for compatibility)
- ThinManager-compatible thin clients
- WinTMC client for Windows PCs
- iTMC client for iOS, iPads, and iPhones
- aTMC client for Android mobile devices

Each type has a different method for connecting to ThinManager to receive its configuration.

A ThinManager-ready thin client is shipped from the factory with the ThinManager BIOS on board. A ThinManager-ready thin client requires these four things to connect to the ThinManager system:

- An IP address for the thin client
- The ThinManager Server Address

A ThinManager-ready wireless thin client contains a different Boot Loader that has unique WiFi connection settings. It requires the same configuration details as a wired thin client as mentioned above, but also requires:

- SSID
- Network password

A ThinManager-ready thin client can use Dynamic Host Configuration Protocol (DHCP) or a static IP address for the client and ThinManager Server IP address. Its BIOS instructs it to download the firmware.

A ThinManager-compatible thin client is a thin client that lacks the ThinManager BIOS. ThinManager-compatible thin clients do not store static IP addresses; so, each of them requires DHCP to assign the client IP address. The ThinManager Server IP address and bootfile name can be provided by a DHCP server or the ThinManager PXE Server.

A ThinManager-compatible thin client requires these 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 these two things to connect to the ThinManager system.

- The installation of the WinTMC program
- The IP address of the ThinManager Server

The iTMC 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 these 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 these 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

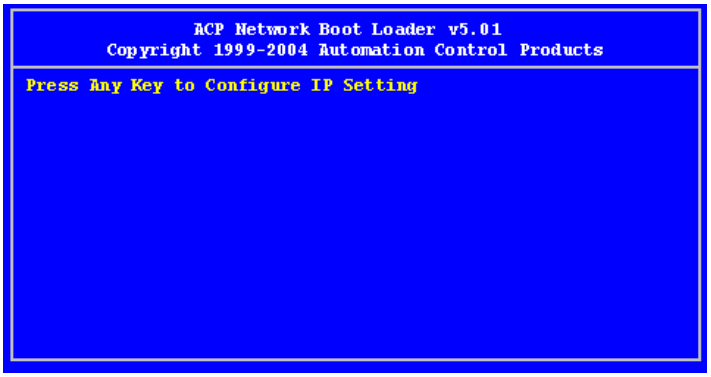
ThinManager-ready Thin Client IP Configuration

DHCP

A ThinManager-ready thin client is shipped from the factory set to use DHCP (Dynamic Host Configuration Protocol).

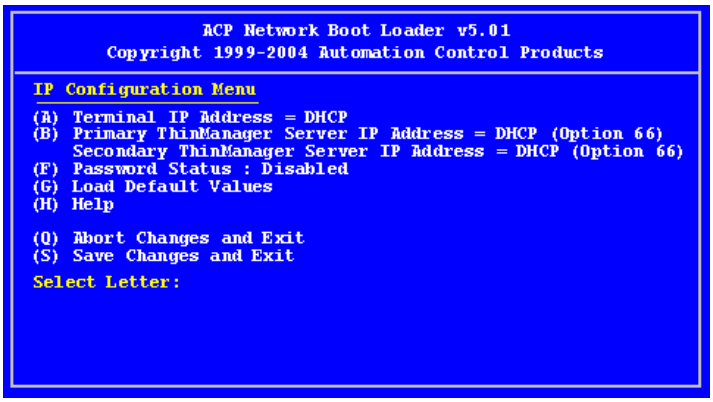
1. After the Terminal is turned on, a prompt to press any key to configure the IP setting appears. Press the space bar.

Figure 398 - IP Configuration Prompt Page



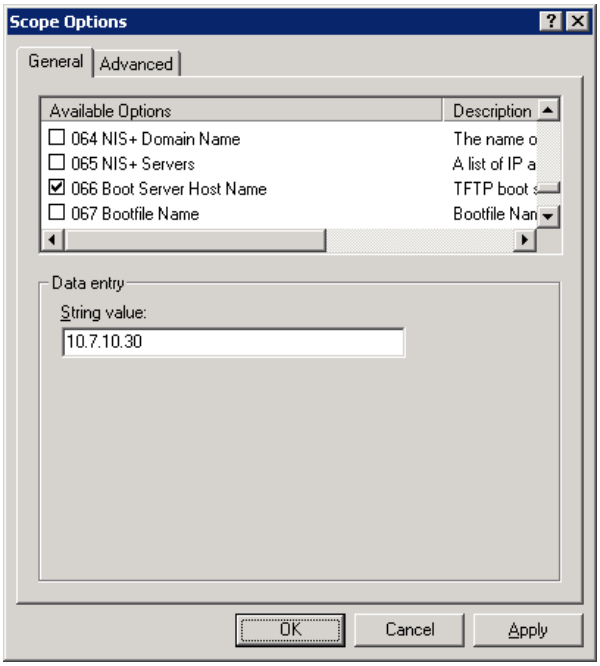
The IP Configuration Menu appears.

Figure 399 - IP Configuration Menu Page



Out of the box, ThinManager-ready thin clients use DHCP, which assigns an IP address to the thin client. However, the thin client also needs the IP address of the ThinManager Server. ThinManager Server's IP address can be provided by the DHCP server using Option 066, Boot Server Host Name.

Figure 400 - Microsoft DHCP Server



2. Check option 066 Boot Server Host Name, and enter the IP address of the ThinManager Server in the String value field to have the DHCP server send the IP address to the ThinManager-ready thin clients.

   PCs and laptops that use DHCP ignore this setting.

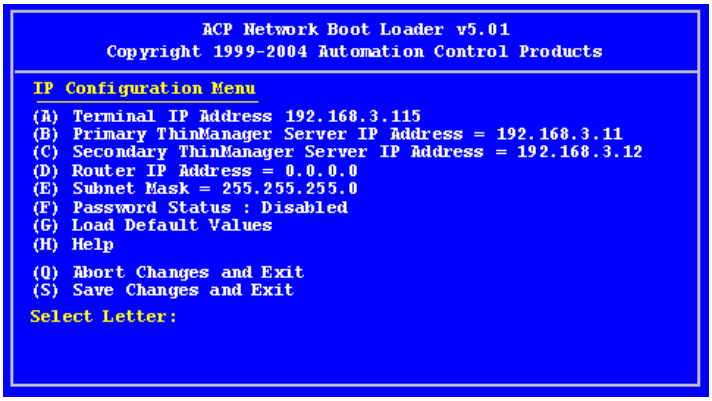
Static IP Addressing

Most models of ThinManager-ready thin clients allow the usage of static IPs, which are set on the IP Configuration Menu.

1. Press any key at the IP Configuration Prompt page.

   The IP Configuration Menu appears.

Figure 401 - IP Configuration Menu – Static IP



2. Press A to allow the client IP address to change from DHCP to static.
3. Type the static IP address for the client, including the separating periods, and press Enter.

Once the Terminal has a static IP assigned, the IP Configuration Menu is shown to allow the setting of other values.

Setting	Configuration	Description
(A)	Terminal IP Address	A unique address for the Terminal.
(B)	Primary ThinManager Server IP Address	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 connects 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 not used, set to 0.0.0.0.
(E)	Subnet Mask	Set to 0.0.0.0.
(F)	Password Status	Set this to your subnet mask. 255.255.255.0 is a standard setting. **IMPORTANT:** Do not forget this password.
(G)	Load Default Values	Resets the ThinManager-ready thin client to the original IP values.
(H)	Help	Launches Help to explain the IP Configuration Menu.
(Q)	Abort Changes and Exit	Cancel any setting changes and let the Terminal continue to boot with the old settings.
(S)	Save Changes and Exit	Apply any changes and allow the Terminal to continue to boot with the new settings.

4. 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.

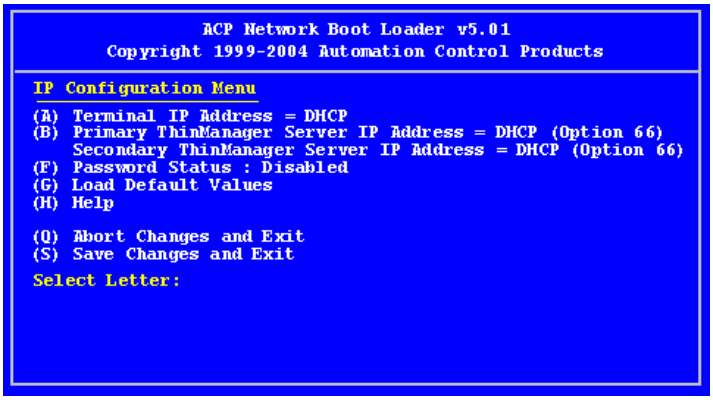
Hybrid IP Addressing

ThinManager-ready thin clients with Boot Loader 5.01 and later can use DHCP to assign the Terminal IP address. However, they can assign the ThinManager Server IP address as a static IP in the IP Configuration Menu, as well.

1. Boot your thin client and press the spacebar when prompted on the IP Configuration Prompt page.

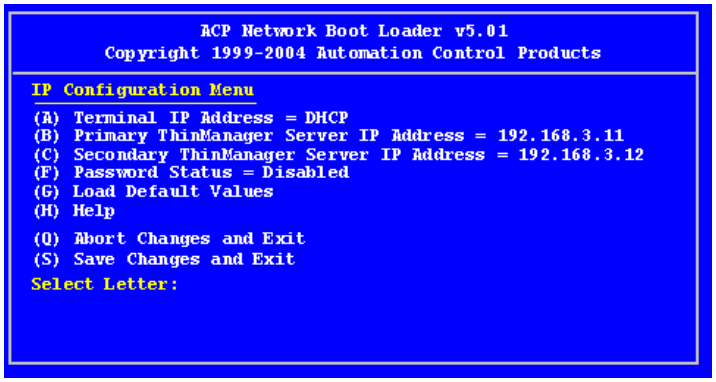
   The IP Configuration Menu appears.

Figure 402 - Boot Loader Default Values



2. Press B to add a static IP for the ThinManager Server.
3. Type the address.

Figure 403 - DHCP with Static ThinManager Server



4. Once a ThinManager Server is assigned, type C to allow a redundant secondary ThinManager Server to be assigned.
5. Type S to save the changes and allow the connection to the ThinManager Server.

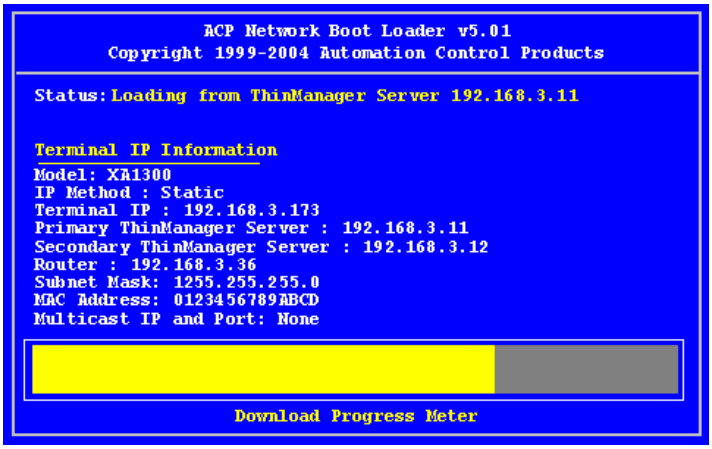
   The Terminal nows boot using DHCP.

The Escape key lets you exit the entry field and return to the IP Configuration Menu.

Firmware Download

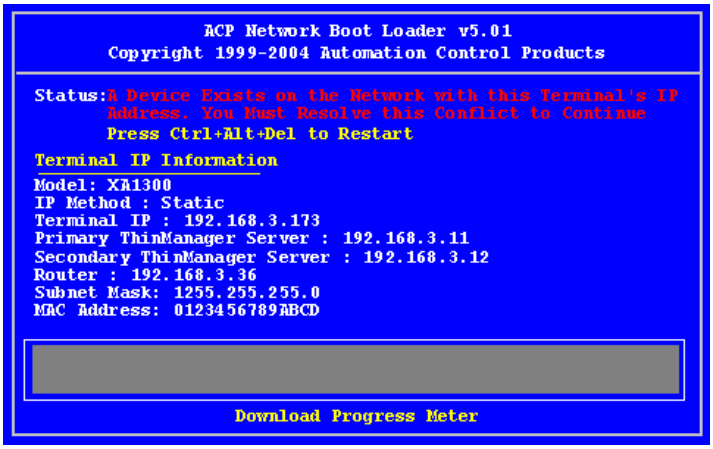
Once the ThinManager-ready thin client is configured, the Terminal connects to the ThinManager Server and downloads the firmware and configuration.

Figure 404 - Firmware Download



If the static IP address for the Terminal is a duplicate of another IP address on the network, an error message is displayed, and the firmware download stops.

Figure 405 - Duplicate IP Address Error

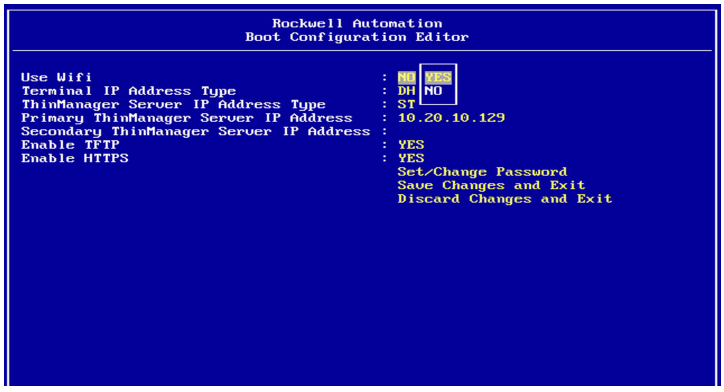


A Terminal with an error message needs to be rebooted and the IP address corrected, see Figure 405. This is the error message: “A Device Exists on the Network with this Terminal’s IP Address. You Must Resolve this Conflict to Continue.”

Wireless Boot

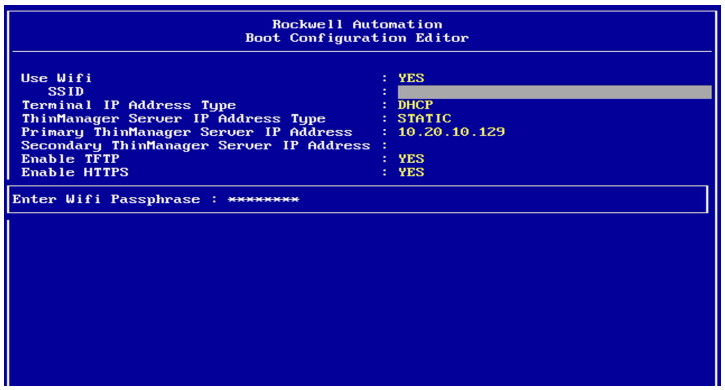
Only applies to ThinManager-ready and specific hardware devices.

Figure 406 - Use Wifi



1. Select Yes at the Use Wifi prompt.

Figure 407 - Enter SSID



2. Enter the SSID of the wireless network.
3. Follow the instructions for wired thin clients to complete the configuration. See ThinManager-ready Thin Client IP Configuration on page 290.

Add and Configure Thin Clients

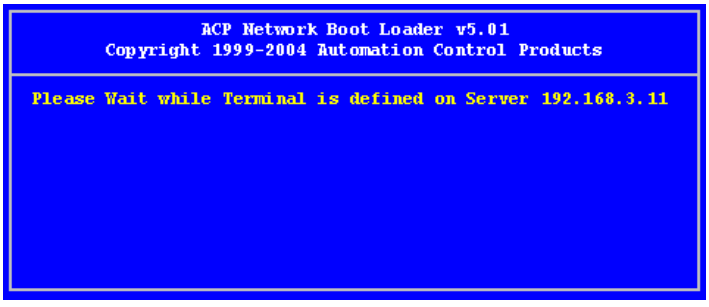
Connect and Start Wizard

When a Terminal is turned on for the first time, it initiates the Create New Terminal mode given one of the conditions that follow are true.

- No Terminals are defined in ThinManager.
- All the defined Terminals are currently connected.
- All the defined Terminals that are turned off have the Allow replacement at terminal if off line checkbox cleared on the Terminal Group Options page. See Figure 384 on page 281.

When a Terminal enters the Create New Terminal Mode, the Terminal launches the Terminal Configuration Wizard on the ThinManager Server. The Terminal displays a dialog box that indicates to wait until the configuration is finished before you proceed.

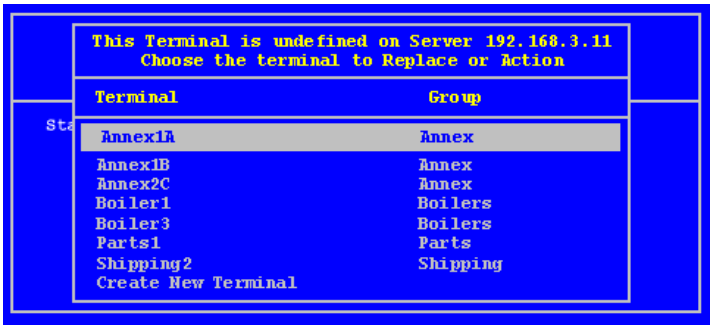
Figure 408 - Create New Terminal Mode Screen



Preconfigure and Select Configuration

The Replace or Create New Terminal Mode is initiated when a Terminal is turned on for the first time and Allow replacement at terminal if off line is checked on the Terminal Group Options page. See Figure 384 on page 281.

Figure 409 - Replace or Create New Terminal Mode



The dialog box displays all the offline Terminals that the Terminal can replace. Groups are displayed, which requires a pull-down menu to the desired Terminal.

Highlight the desired Terminal name using the keyboard and press Enter.

The Terminal retrieves the selected configuration and assumes its identity.

If a Terminal has previously connected to ThinManager and received its configuration, rebooting it does not present the option to select a different terminal configuration.

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 and ThinManager Server IP addresses. Its BIOS instructs 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. Therefore, each of these thin clients is assigned an IP address by a DHCP 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.

PXE Server Modes

There are four modes or methods that a ThinManager-compatible thin client can use to receive information.

- Using standard DHCP server
- Using standard DHCP server on this machine
- Using standard DHCP server with Boot Options (PXE Disabled)

- Not using standard DHCP server

Table 2 - ThinManager-compatible Thin Client IP Sources

Mode/Method	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

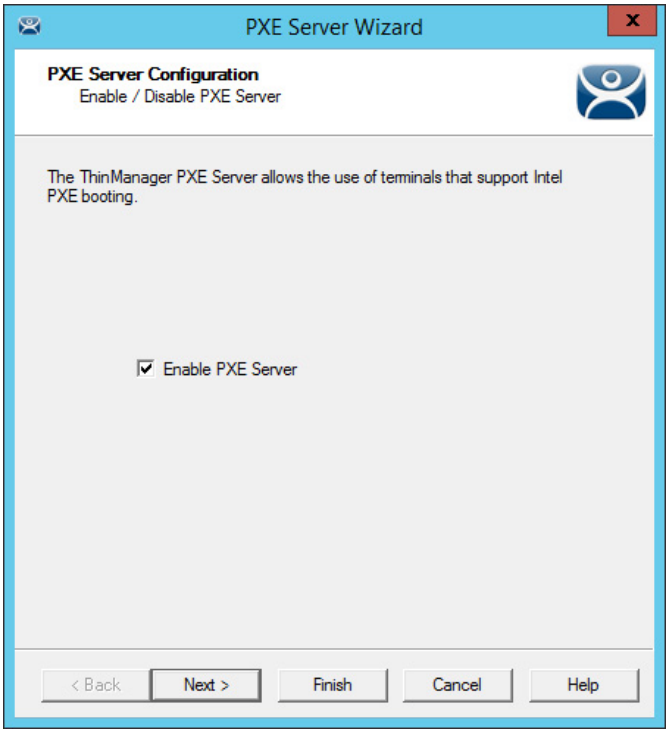
Using Standard DHCP Server

Use the Using standard DHCP server mode when you have an existing DHCP server in your system to pass out the IP addresses.

1. Choose Manage>PXE Server to open the PXE Server Wizard.

   The PXE Server Configuration page appears.

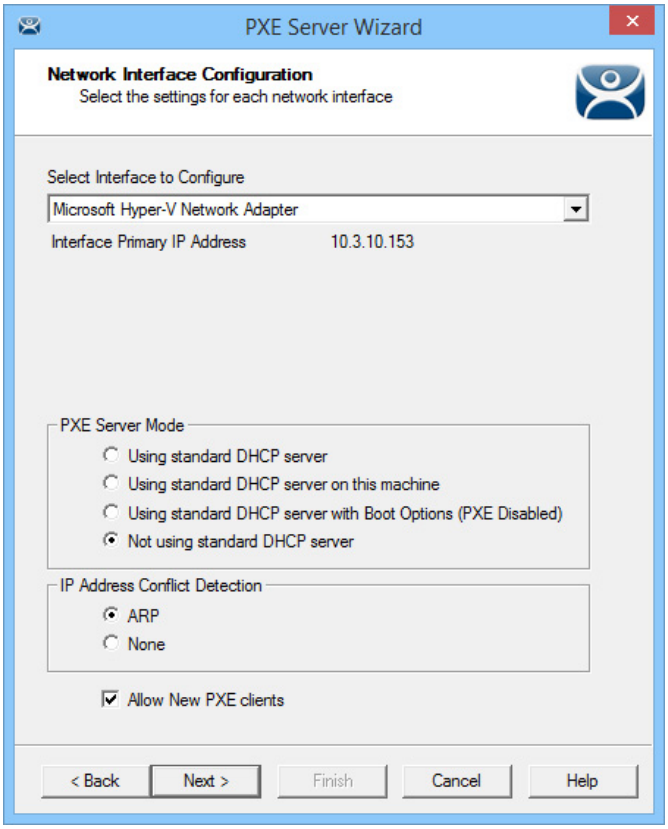
Figure 410 - PXE Server Configuration Wizard



2. Check Enable PXE Server and click Next.

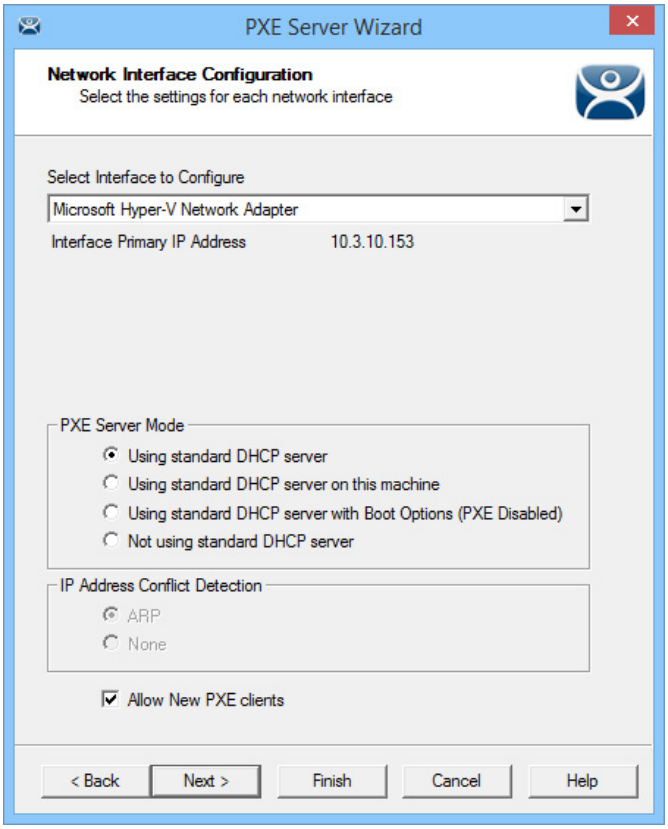
   The Network Interface Configuration page appears.

Figure 411 - Network Interface Configuration Page of PXE Server Configuration



Setting	Description
Select Interface to Configure	Pull-down menu allows the network interfaces to be configured individually if ThinManager Server has multiple network cards.
PXE Server Mode	
Using standard DHCP server	Uses existing DHCP server to provide client IP addresses while the ThinManager PXE server provides the ThinManager IP and boot file name.
Using standard DHCP server on this machine	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 must be open on the computer.
Using standard DHCP server with Boot Options (PXE Disabled)	Allows DHCP server to provide all needed information. Use if your DHCP server is configured to use Option 066 (Boot Server Host Name) with the ThinManager Server IP address. You must use Option 067 (Boot file name) set to *acpboot.bin*.
Not Using standard DHCP server	Allows PXE thin clients to connect to ThinManager, which provides all necessary information, through the selected network interface. Clear this checkbox if you only want known clients to connect.
IP Address Conflict Detection	
ARP	Checks for conflicts in the Address Resolution Protocol.
None	Does not check for conflicts in the Address Resolution Protocol.
Allow New PXE Clients	Allows unknown PXE thin clients to connect to ThinManager through the selected network interface. Clear the checkbox to allow only known clients to connect, which is a security feature that can prevent the provision of PXE information to new PXE boot ThinManager-compatible thin clients.

Figure 412 - Synchronized Network Interface Configuration Page



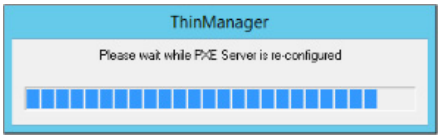
A synchronized ThinManager Server has a pull-down menu for the network interface on both ThinManager Servers.

The easiest method of PXE boot is if you have an existing DHCP server.

3. Choose Using standard DHCP server and click Finish.

   The PXE Server Initialization dialog box appears.

Figure 413 - PXE Server Initialization Dialog



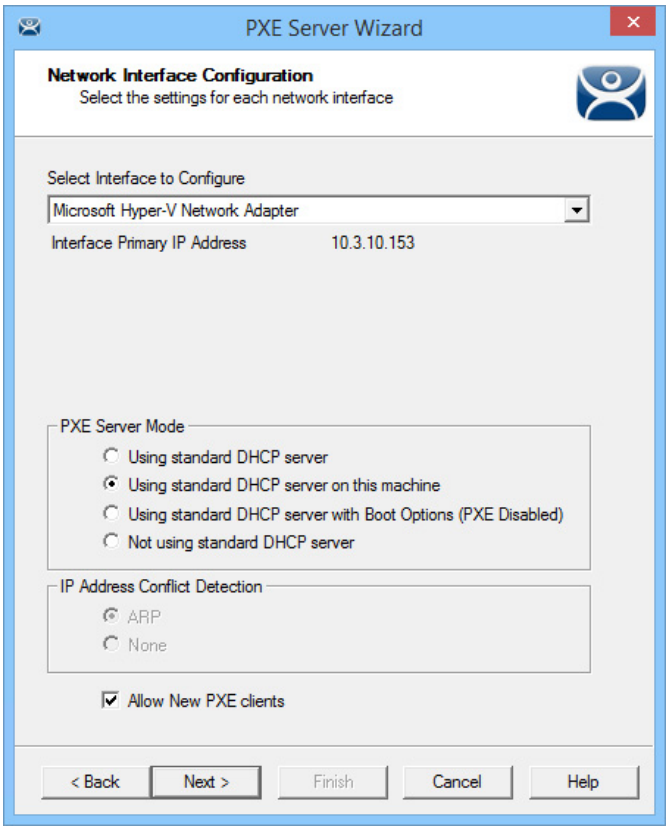
The PXE server initializes and becomes active.

When the ThinManager-compatible thin client is turned on, it requests the DHCP and PXE information. The DHCP server responds with the client IP address. ThinManager responds with the PXE boot information, and the thin client connects to ThinManager.

Using Standard DHCP Server on this Machine

Use the Using standard DHCP server on this machine mode when you have an existing DHCP server in your system to assign the IP addresses, and it is installed on the ThinManager Server.

Figure 414 - 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 must be open for this setting, and it is also required for Unified Extensible Firmware Interface (UEFI) boot PXE clients.

Using standard DHCP server with Boot Options

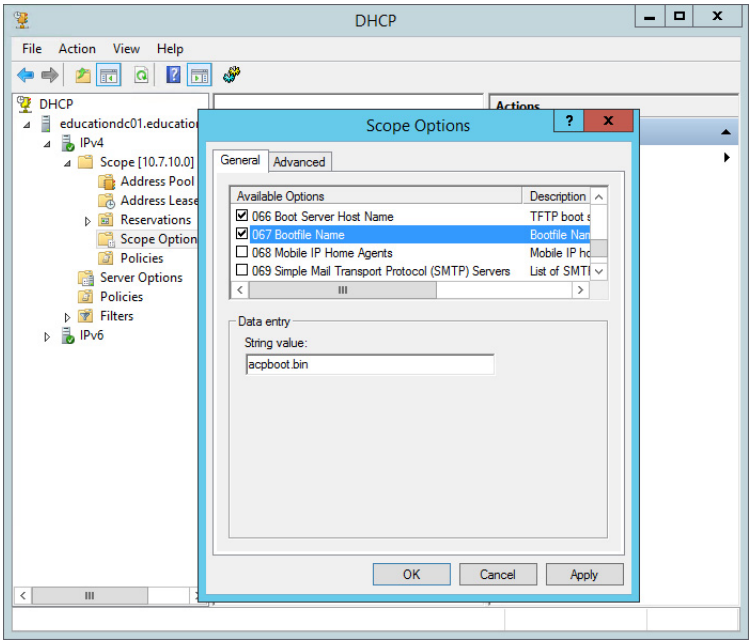
Use the Using standard DHCP server with Boot Options (PXE Disabled) mode when you have an existing DHCP server that is not on the ThinManager Server and want it to provide all the information.

The DHCP server needs to be configured to provide Option 66, Boot Server Host Name, and Option 67, Bootfile Name.

On the DHCP Server

1. Choose Start>Administrative Tools>Computer Management on your Microsoft DHCP server to open the Microsoft DHCP Service.

Figure 415 - Microsoft 2012 Server DHCP Scope Options



2. Right-click on Scope Options in the Scope tree and choose Configure Options.

   The Scope Options dialog box appears.

3. Scroll to and check Option 066 Boot Server Host Name. Type 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.
4. Scroll to and check Option 067 Bootfile Name. Type `acpboot.bin` in the String value field.

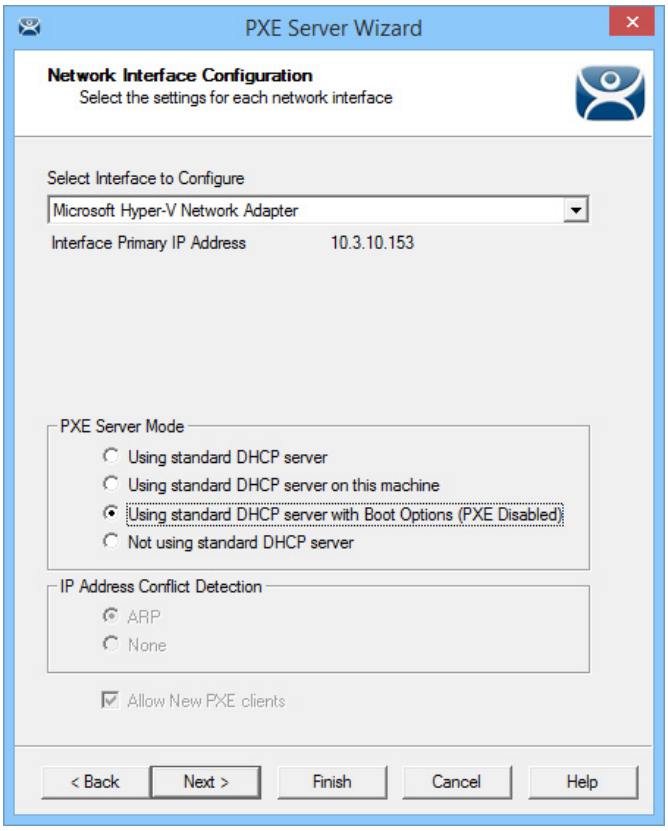
The DHCP server is allowed to provide the boot information to both ThinManager-ready thin clients using the default DHCP and ThinManager-compatible thin clients via PXE boot. DHCP server is able to do this because we configured a DHCP to provide IP addresses, the ThinManager Server IP address as Option 066 and the acpboot.bin bootfile as Option 067.

In ThinManager

1. Choose Manage>PXE Server to open the PXE Server Wizard.
2. On the PXE Server Configuration page, check Enable PXE Server.
3. Click Next.

   The Network Interface Configuration page appears.

Figure 416 - Network Interface Configuration Page



4. In the PXE Server Mode section, choose Using standard DHCP server with Boot Options (PXE Disabled).
5. Click Finish.

   The PXE server is configured.

When the ThinManager-compatible thin client is turned on, it makes a DHCP request. The DHCP server responds with the client IP address, ThinManager IP address, and name of the bootfile to download. The ThinManager-compatible thin client connects to ThinManager.

Not using standard DHCP server

Use the Not using standard DHCP server mode 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.

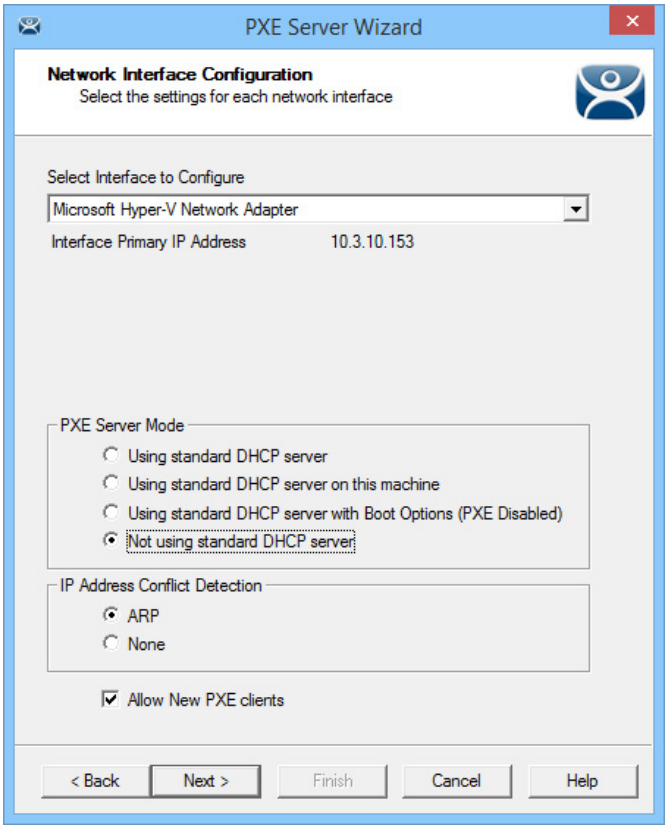
ThinManager only passes IP addresses to terminals making a PXE request. It ignores traditional DHCP requests.

1. To open the PXE Server Wizard, choose Manage>PXE Server.

   The PXE Server Configuration page appears.
2. Check Enable PXE Server.
3. Click Next.

   The Network Interface Configuration page appears.

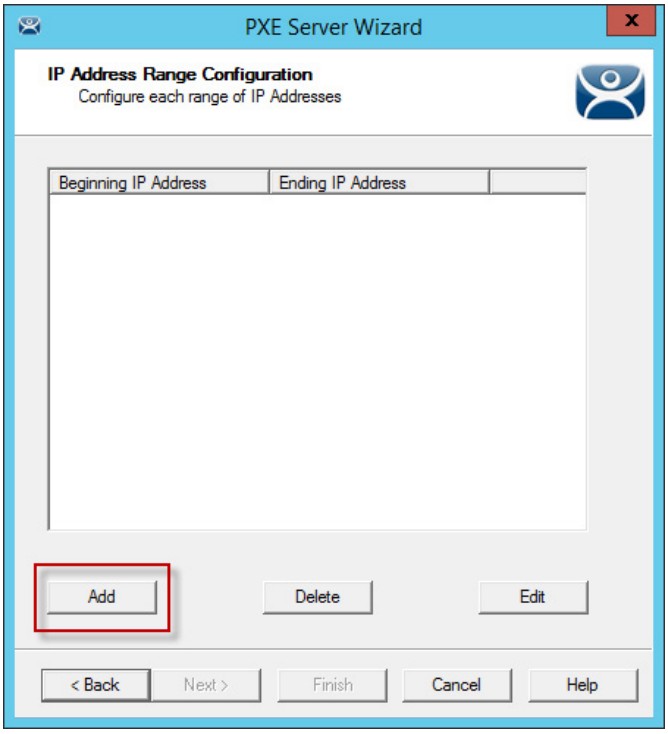
Figure 417 - Network Interface Configuration Page



4. Click Not using standard DHCP server.
5. (Optional) Click ARP to have the IP Address Conflict Detection check for conflicts in the Address Resolution Protocol.
6. (Optional) Check Allow New PXE clients to control whether ThinManager gives PXE information to new PXE boot ThinManager-compatible thin clients.
7. Click Next.

   The IP Address Range Configuration page appears.

Figure 418 - IP Address Range Configuration

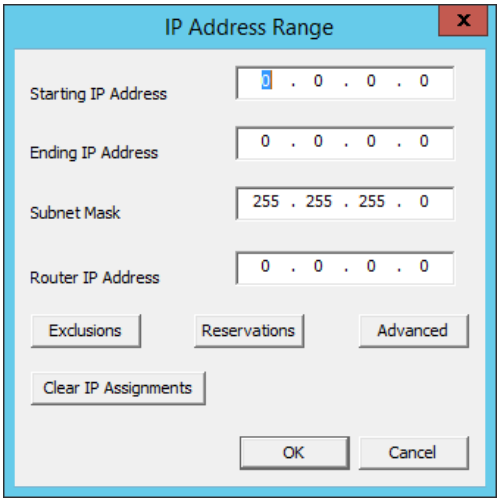


The ThinManager Server needs to have a range of available IP addresses so that it can give the ThinManager-compatible thin clients their IP addresses.

8. Click Add.

   The IP Address Range dialog box appears.

Figure 419 - IP Address Range



9. Complete the IP Range dialog box per these descriptions.

Setting	Description
Starting IP Address	Type the first IP address for the PXE Server to assign.
Ending IP Address	Type the last IP address for the PXE Server to assign.
Subnet Mask	The subnet mask of the network.
Router IP Address	If needed, type the IP address of your router. Leave as 0.0.0.0 if not needed.
Buttons	
Exclusions	Launches the Exclusions dialog box to exclude a specific IP address from the available page.

Setting	Description
Reservations	Launches the Reservations dialog box that allows you to reserve a specific IP address to be assigned to a thin client based on the thin client MAC add address.
Advanced	Launches the Advanced IP Range Settings dialog box, which allows the addition of DHCP options.
Clear IP Addignments	Clears the settings from the IP Address Range dialog box.

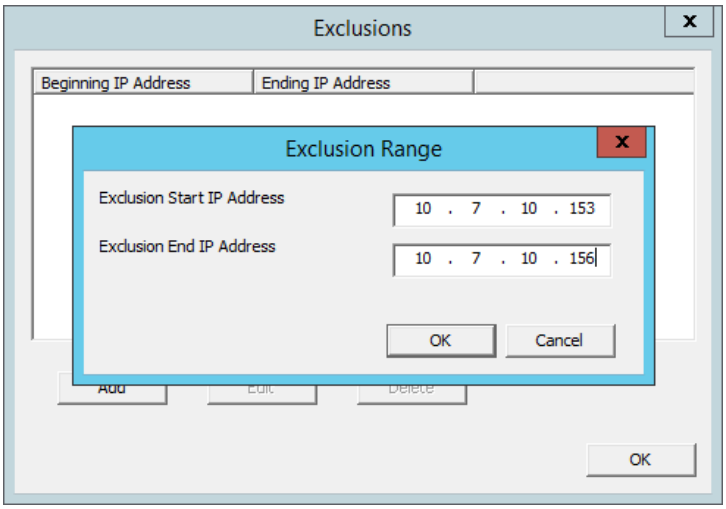
Exclusions

To add an exclusion to the IP address range, complete these steps.

1. On the Exclusions dialog box, click Add.

   The Exclusion Range dialog box appears.

Figure 420 - Exclusions and Exclusion Range Dialog Boxes



2. Type the Exclusion Start IP Address.
3. Type the Exclusion End IP Address.

To exclude a single IP address, enter it in the Exclusion Start IP Address field.

4. Click OK to close the Exclusion Range dialog box.
5. Click OK to close the Exclusions dialog box.

   The range of IP addresses to exclude from assignment is complete.

Reservations

Reservations allow 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.

Reservations in the PXE Server

To add a Reservation, complete these steps.

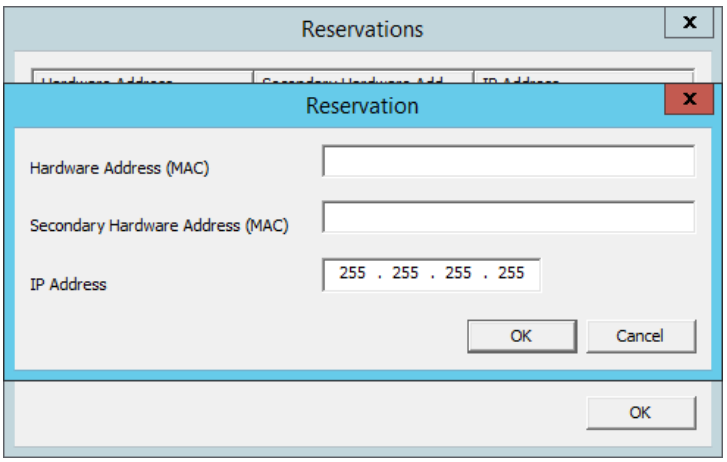
1. On the IP Address Range dialog box, click Reservations.

   The Reservations dialog box appears.

2. Click Add.

The Reservation dialog box appears.

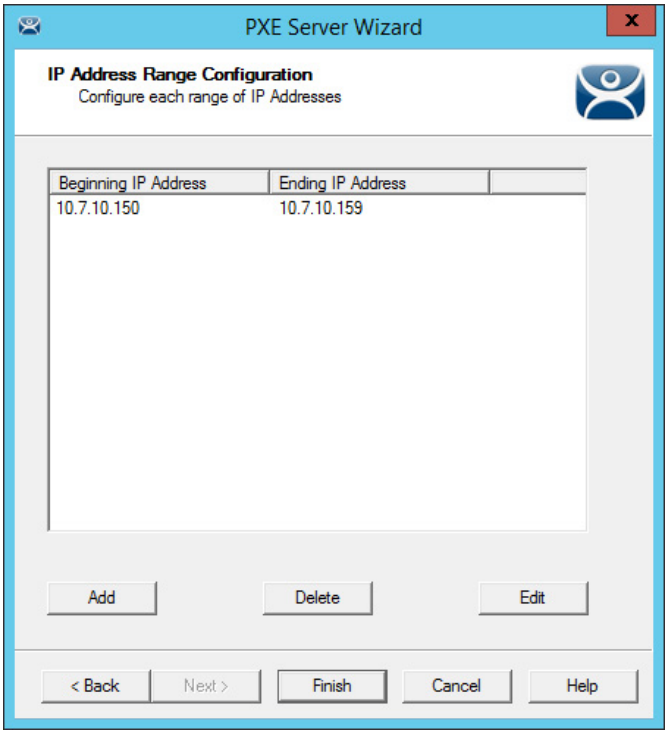
Figure 421 - Reservation Window in the PXE Server



3. Type the MAC address from the ThinManager-compatible thin client in the Hardware Address (MAC) field.
4. Type a secondary MAC address if the ThinManager-compatible thin client has two NICs. These MAC addresses are often on the serial number label.
5. Type the IP Address you want to assign to it.
6. Click OK on the Reservation dialog box.
7. Click OK on the Reservations dialog box.

   The IP address range is displayed on the IP Address Range Configuration page when the IP Address Range dialog box is closed.

Figure 422 - IP Address Range in PXE Server



The ThinManager PXE server is not a true DHCP server. It only issues IP addresses to PXE boot devices. It does not assign IP addresses to other computers, laptops, or devices.

Reservations in the Terminal Configuration Wizard

ThinManager has an easy way to reserve IP addresses for PXE boot thin clients.

Follow these steps.

1. Turn on the device and associate it with a configuration.

Figure 423 - Original Assigned IP Address

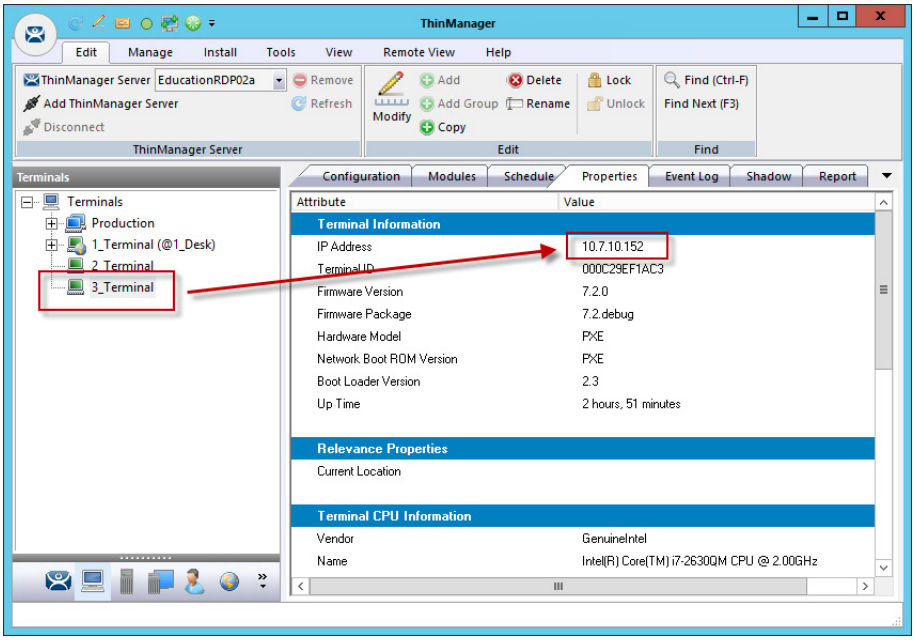


Figure 423 shows the original IP address.

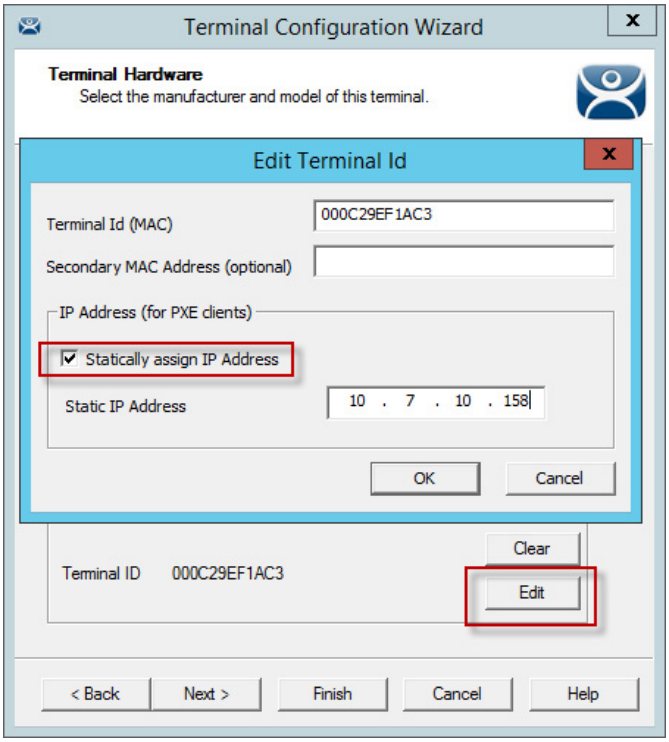
2. Turn off the device. You cannot change the IP address of a Terminal that is on.

   When off, the Terminal icon in the tree turns red.

3. Double-click on a turned off Terminal in the ThinManager tree to open the Terminal Configuration Wizard.
4. Navigate to the Terminal Hardware page and click Edit.

   The Edit Terminal Id page appears, which is only be active on Terminals that are off.

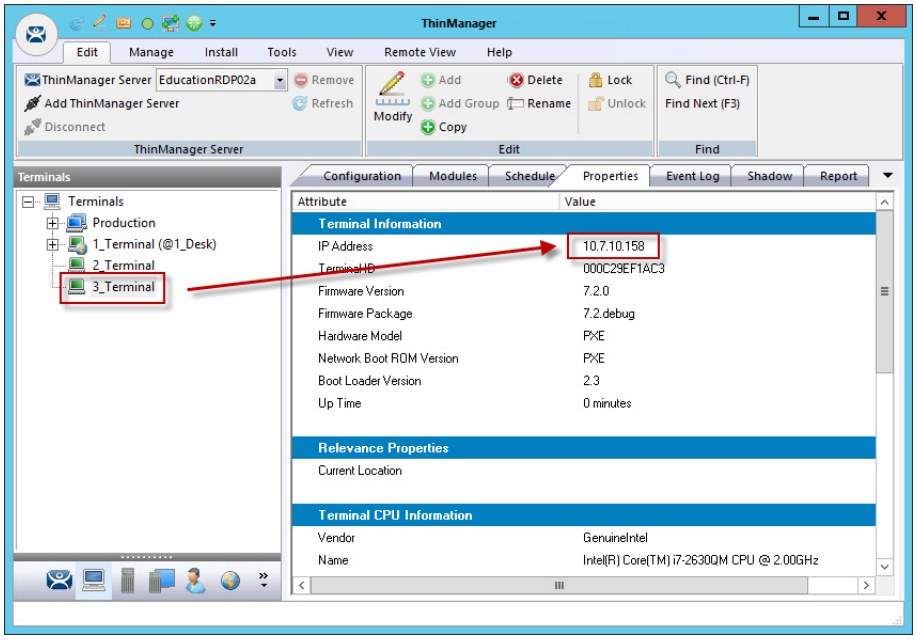
Figure 424 - Edit Terminal ID Window



5. Check Statically assign IP Address, which allows you to set a static IP reservation when addresses are assigned with the ThinManager PXE server.
6. Click OK to close the Edit Terminal Id page.
7. Click Finish to close the Terminal Configuration Wizard.
8. Right-click the Terminal, and choose Restart.

   It is now assigned the new IP address.

Figure 425 - Newly Assigned IP Address



An advantage of using ThinManager to assign IP addresses is, if you do a replacement, the replacement Terminal is assigned the reserved IP address.

Secure Boot

Firmware versions 13.2.0 and later are signed, which includes the modules packaged with the firmware. This allows the user to take advantage of Secure Boot on supported ThinManager-ready hardware devices. Terminals that are not ThinManager-ready also support secure boot when configured properly. For non-ThinManager-ready terminals, additional certificates must be installed on the device.

When secure boot is enabled in the BIOS of a terminal, it checks the signature of the Boot Loader and firmware files. If there is a mismatch, the firmware does not boot. If Secure Boot is disabled, the signature of the Boot Loader and firmware files are not checked.

The signature of the modules is always checked, even when Secure Boot is disabled.

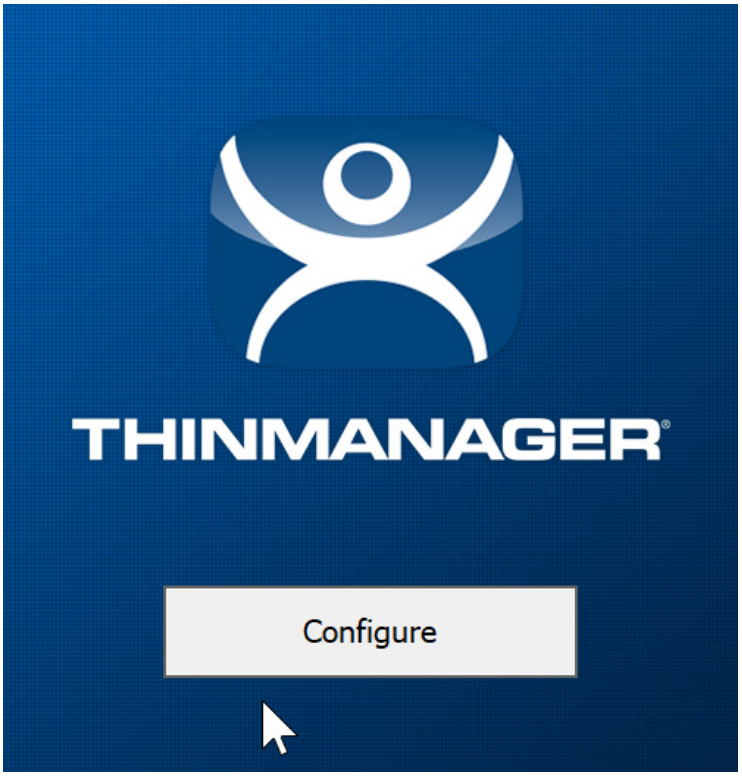
Local WinTMC Configuration

WinTMC is a PC application that allows ThinManager to manage the RDP connections between the PC and Remote Desktop Servers. Also, WinTMC provides enhanced features like failover and Instant Failover, which standard RDP connections lack.

The WinTMC needs to be installed on a PC, then it needs to be configured to point to ThinManager to receive its configuration.

When WinTMC starts, Configure is displayed on the ThinManager splash screen.

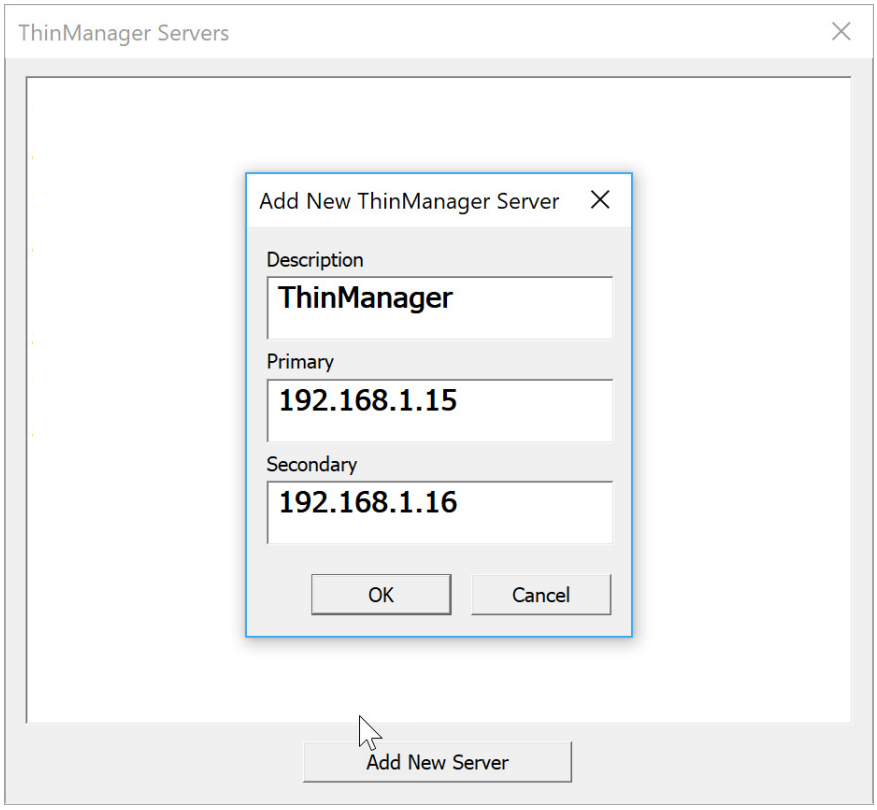
Figure 426 - WinTMC Splash Screen



1. Click Configure to specify the ThinManager Server(s) to use.

   The Add New ThinManager Server dialog box appears.

Figure 427 - 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.

2. Type the IP address or name of your ThinManager Servers in the Enter new ThinManager Server Name or IP Address field and click OK to add them to the Current ThinManager Server list.
3. Click Move Up and Move Down to change the list order of ThinManager Servers with which WinTMC tries to connect.
4. Click Delete to remove unneeded ThinManager Servers.
5. (Optional) Click Set Password to password protect this configuration menu.

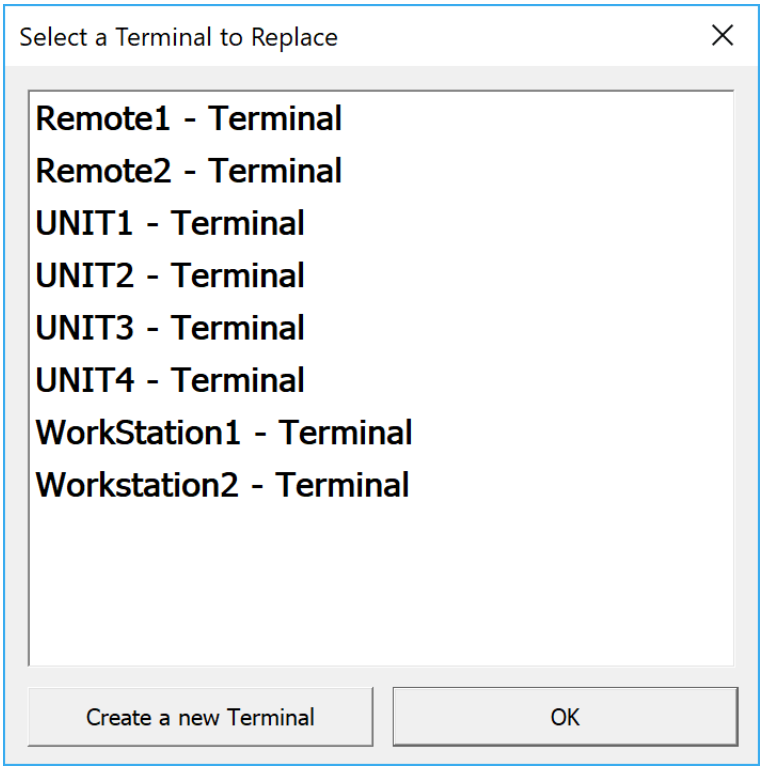
   Once a password is configured, it is required to change the configuration when a user clicks Configure when WinTMC is started.

If OK is clicked without entering a ThinManager Server, an error dialog reminds you to enter a ThinManager Server address.

No ThinManager Server Specified

Once the local configuration is set, WinTMC connects to a ThinManager Server and attempts to retrieve its configuration.

Terminal Replacement Dialog



If the WinTMC PC has not been defined, the user is prompted with a dialog box to allow for the creation of a new configuration or to replace an existing Terminal configuration on the ThinManager Server.

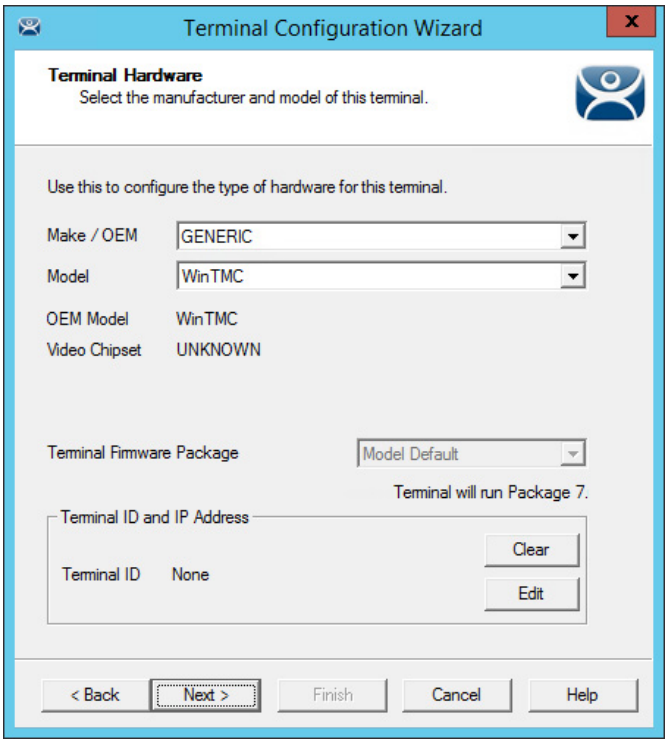
This functionality is similar to that of the create/replacement menu on a Thin Client. Select the thin client configuration you want to assume. Once the WinTMC is assigned a configuration, you do not need to make a selection again.

WinTMC Configuration in ThinManager

To create a WinTMC client in ThinManager using the Terminal Configuration Wizard, follow these steps.

1. Choose GENERIC from the Make/OEM pull-down menu and WinTMC from the Model pull-down menu on the Terminal Hardware page.

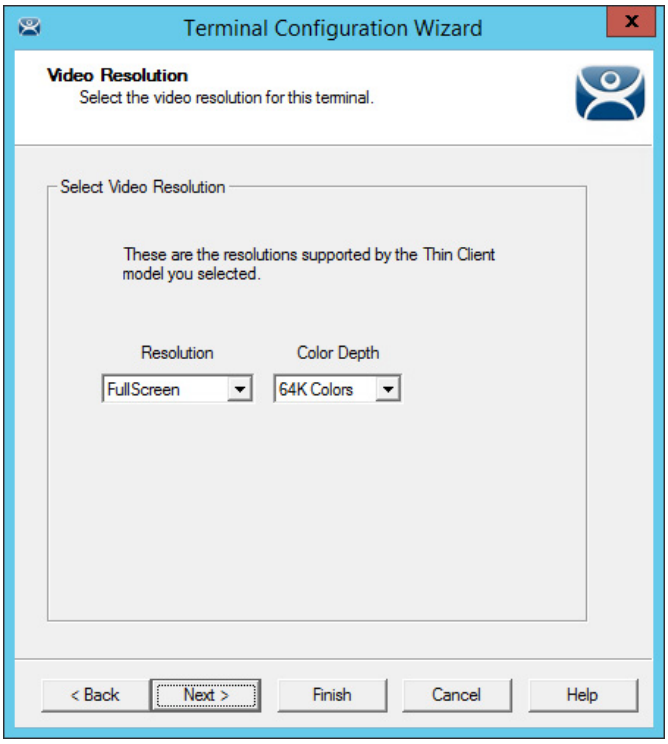
Figure 428 - WinTMC Settings in Terminal Hardware



The Terminal ID populates 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—the Video Resolution page and the WinTMC Settings page.

Figure 429 - Video Resolution for WinTMC

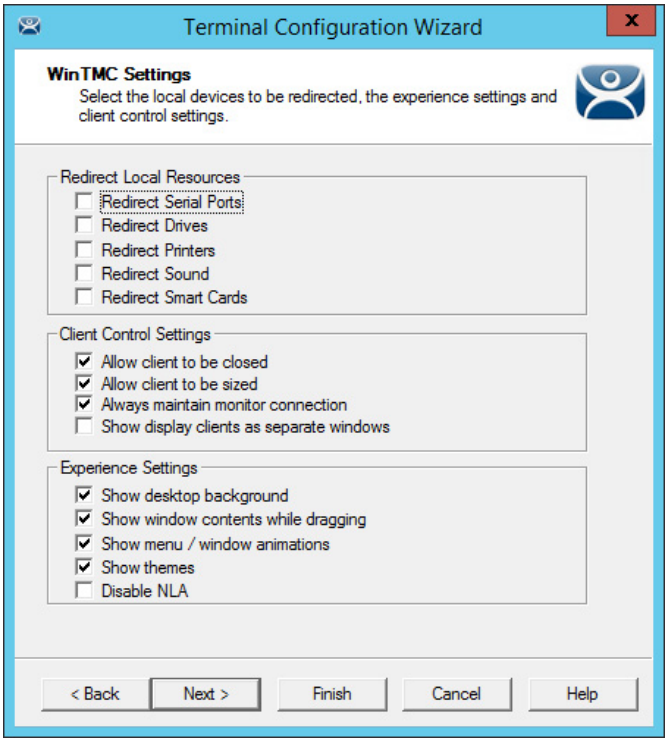


The Video Resolution for WinTMC includes a setting for FullScreen, which populates with whatever resolution the PC client runs.

Also, you may choose from set resolutions.

WinTMC that runs on computers with multiple monitors can run as MultiMonitor WinTMC clients.

Figure 430 - WinTMC Settings



The Terminal Configuration Wizard includes a WinTMC Settings page for WinTMC clients. These settings only apply to connections made by the WinTMC application and include the following.

Setting	Description
Redirect Local Resources	
Redirect Serial Ports	Makes local serial ports available in a session.(1)
Redirect Drives	Makes local drives available in a session.(1)
Redirect Printers	Makes your local printer available in a session.
Redirect Sound	Allows audio played in your session to play locally.(1)
Redirect Smart Cards	Makes your smart card available in a session.(1)
Client Control Settings	
Allow client to be closed	Enables your user to close the client (WinTMC program).
Allow client to be sized	Enables your user to resize the client.
Always maintain monitor connection	Keeps the monitoring connection active when WinTMC is closed to allow shadowing. Clear this checkbox to release the WinTMC license when the WinTMC program is closed but denies shadow access.
Show display clients as separate windows	Displays multiple Display Clients as separate windows rather than in one window shell.
Experience Settings	
Show desktop background	Enables your user to select a Windows Desktop Background. If not selected, the background is a solid color.
Show window contents while dragging	Allows the window contents to be shown while the window is being dragged.
Show menu/window animations	Enables menu/window animations on the client.
Show themes	Enables your user to select a Windows Theme.
Disable NLA	Disables the user of Network Level Authentication for the client.

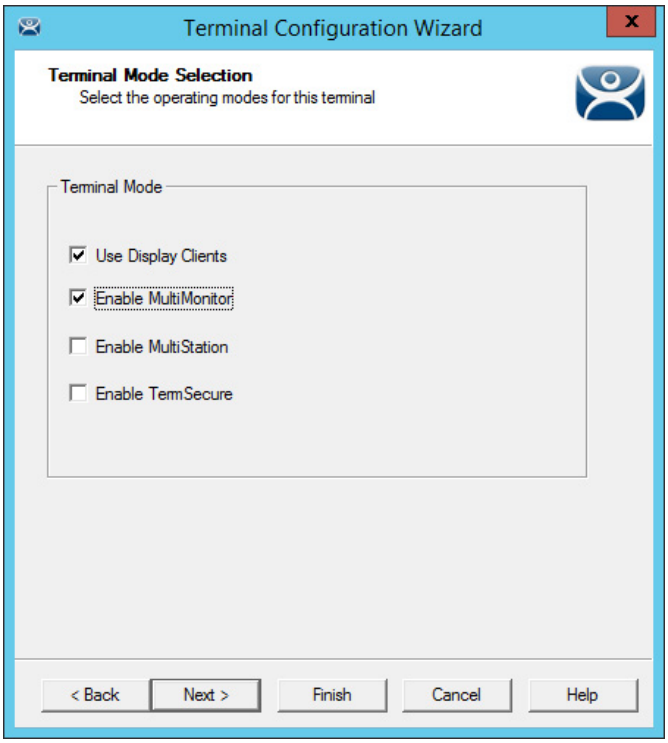
(1) Does not work when you connect to a Remote Desktop Server running Windows 2000 or earlier.

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.

MultiMonitor WinTMC

ThinManager supports MultiMonitor for WinTMC if the PC runs Windows on multiple video cards. If the PC successfully runs multiple monitors on the host OS, then WinTMC can run MultiMonitor on up to five monitors.

Figure 431 - MultiMonitor – Enable MultiMonitor



MultiMonitor requires the use of Display Clients.

1. Check Use Display Clients to enable Enable MultiMonitor.
2. To configure a WinTMC client for MultiMonitor use, check Enable MultiMonitor.
3. Click Next.

The Terminal Configuration Wizard displays the MultiMonitor Video Settings page, Monitor Layout page, and Display Client Selection page as it does for thin clients.

WinTMC Modules

WinTMC clients cannot use the ThinManager modules because they are running Windows locally. Touch drivers, sound drivers, printers, and so on must be installed through the local Windows operating system instead of relying on ThinManager modules.

Mobile Devices

ThinManager offers TMC for Windows for Windows devices, TMC for iOS for iOS devices, and TMC for Android for Android devices. In each of these cases, there remains an underlying OS not managed by ThinManager. Also, ThinManager can boot some x86-based tablets wirelessly, wherein ThinManager not only manages the content delivered to the devices, but also

the underlying OS (which would be the ThinManager firmware). More information about ThinManager Ready Tablets can be found here.

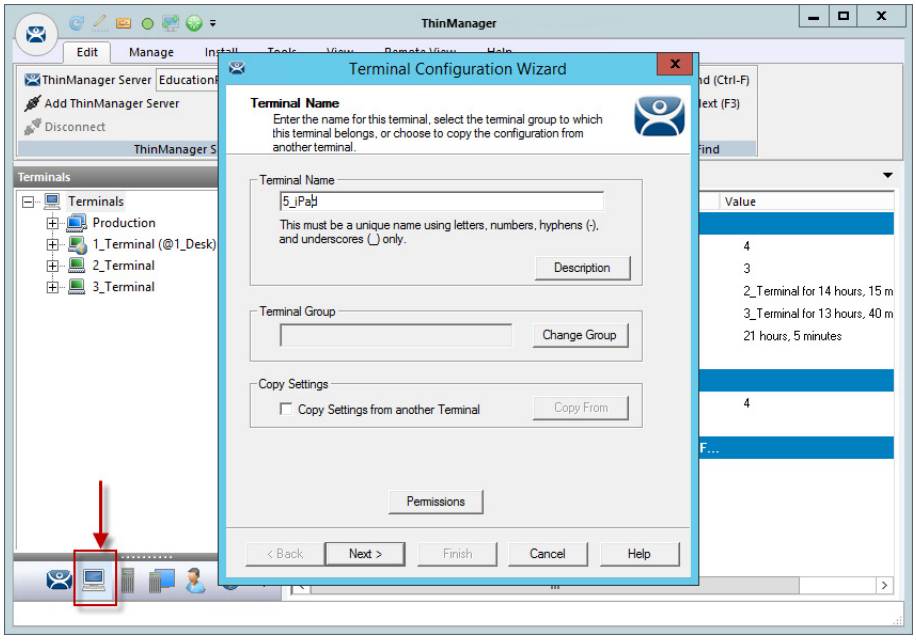
As indicated above, the original Windows application for ThinManager was called WinTMC, and the original iOS application for ThinManager was called iTMC. The new TMC applications are based on the same codebase as TMC for Android, which provide a consistent user experience across these different hardware platforms. We no longer add new features to legacy WinTMC or legacy iTMC, but continue to provide security updates for 2 years beyond the initial release date of TMC for Windows, and TMC for iOS, respectively.

Configure an iOS Device in ThinManager

A configuration needs to be created in ThinManager so that the mobile device can join the system as a Terminal.

1. Open ThinManager and click the Terminal icon to show the Terminals branch of the tree.

Figure 432 - ThinManager Terminal Configuration Wizard



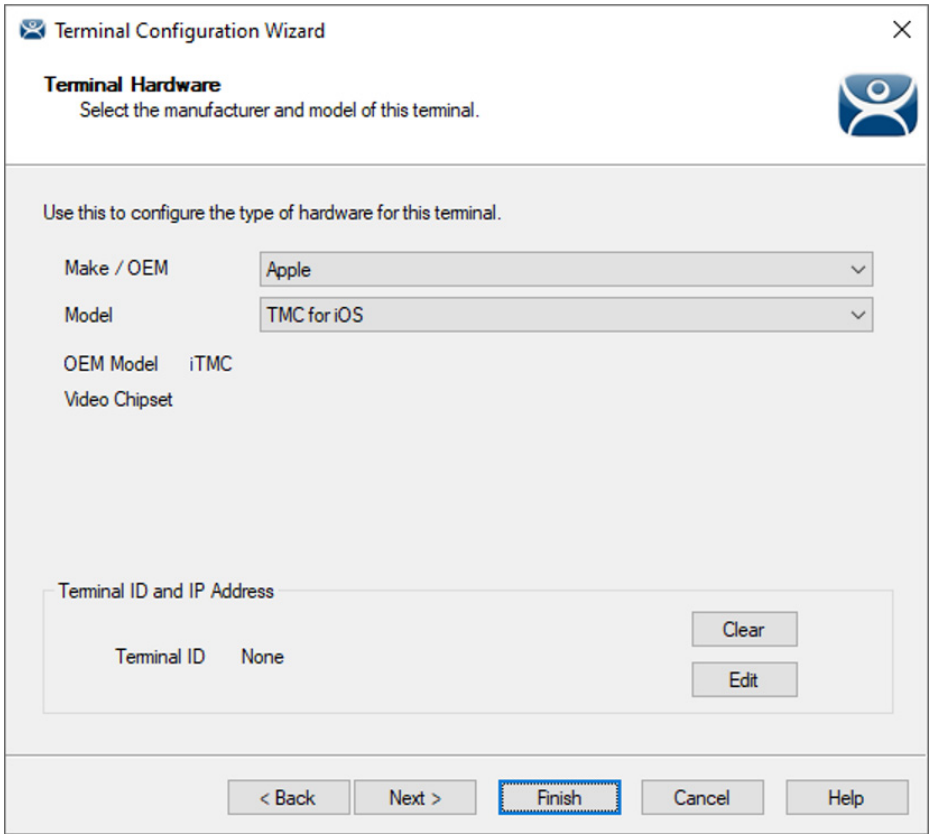
2. Right-click on the Terminals branch and choose Add Terminal.

   The Terminal Configuration wizard appears.

3. Type the name for your mobile device in the Terminal Name field and click Next.

   The Terminal Hardware page appears.

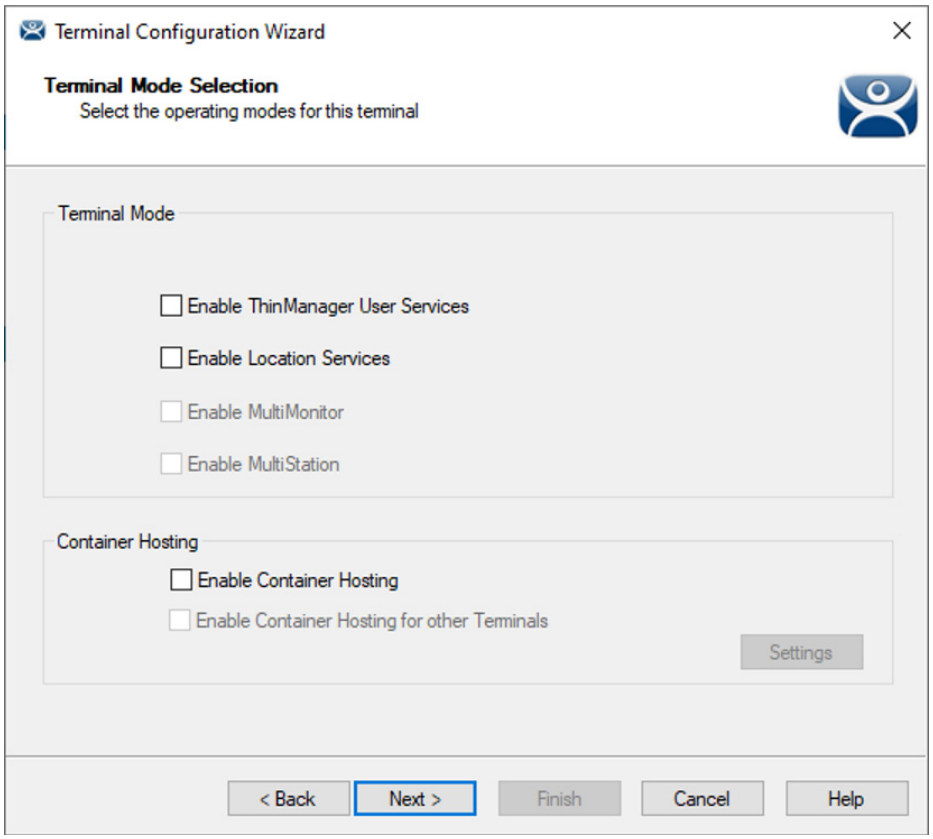
Figure 433 - Terminal Hardware Page



4. Choose Apple/TMC for iOS from the pull-down menus for the Make and Model of the hardware.
5. Click Next.
6. Click Next on the Terminal Options page of the wizard.

   The Terminal Mode Selection page appears.

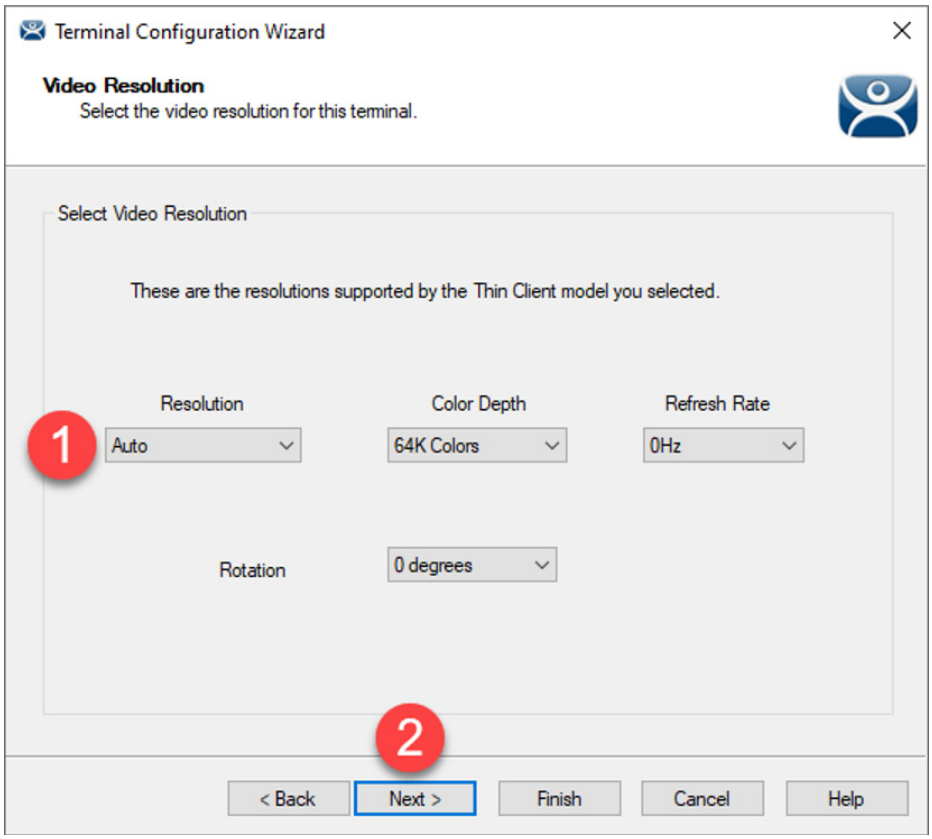
Figure 434 - Terminal Mode Selection Page



An iOS can run as a traditional terminal and have content delivered to it using ThinManager User or Location Services.

7. Check Enable ThinManager User Services and Enable Location Services to control content by user and/or location.
8. Click Next.
9. From the Login Requirements page of the wizard, click Next.
10. From the Video Resolution page of the wizard, select Auto as the Resolution.
11. Click Next.

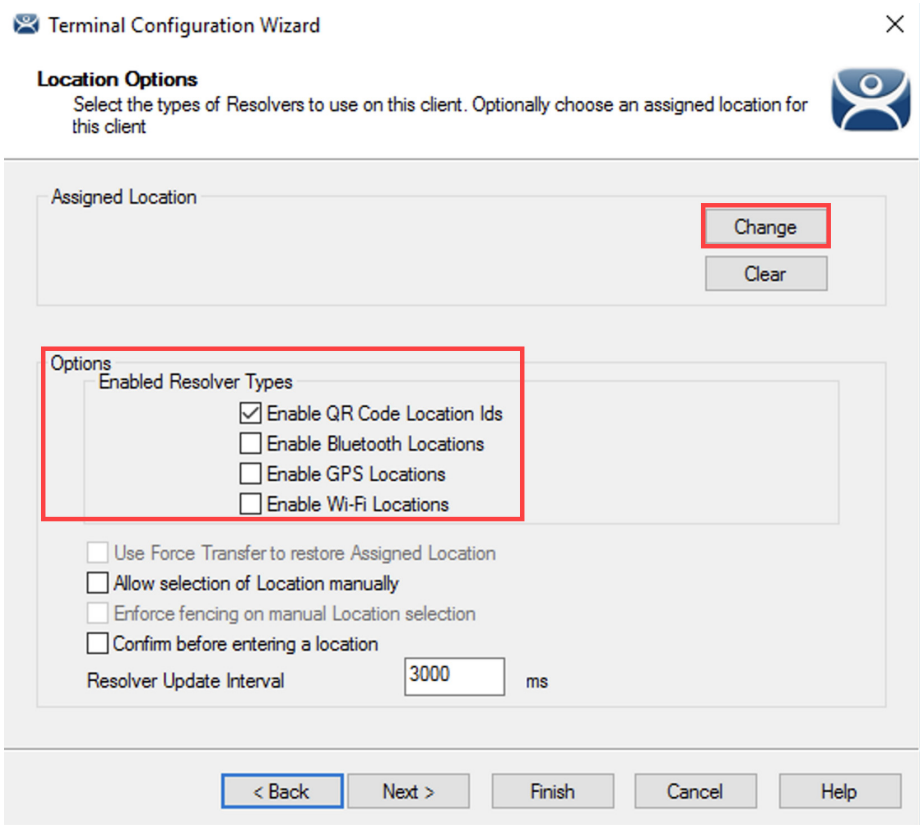
Figure 435 - Video Resolution



12. From the Display Client Selection page of the wizard, select the desired Display Client(s) for your application.
13. From the Terminal Interface Options page of the wizard, click Next.

    The Location Options page appears, which allows you to assign a Location to the iOS device. You may not want to assign a Location to the iOS device but, instead, have it interact with different locations.

Figure 436 - Location Options Page



The Location Options page allows you to enable various Resolver types. Check the ones you want to use from the iOS device.

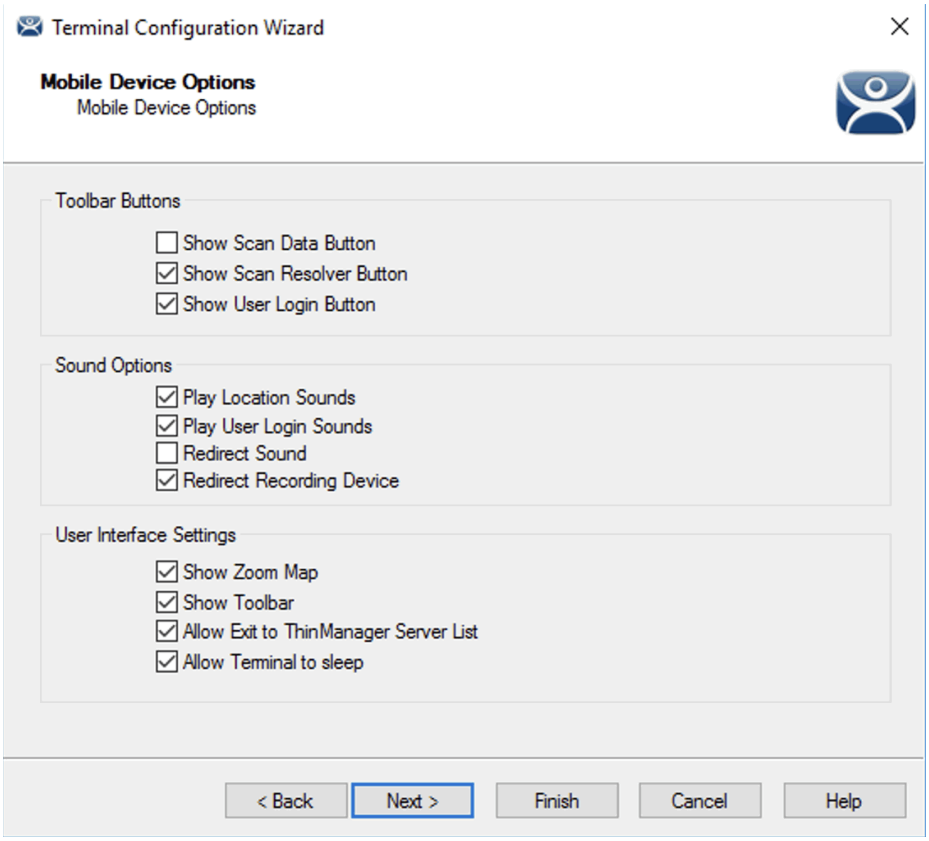
Setting	Description
Enabled Resolver Types	
Enable QR Code Location Ids	Allows the scanning of a QR code to determine the location.
Enable Bluetooth Locations	Allows the use of Bluetooth beacons to determine the location.
Enable GPS Locations	Allows the Global Positioning System of the mobile device to determine the location.
Enable Wi-Fi Locations	Allows the signal strength of Wi-Fi access points to determine the location.

Each method selected requires configuration to associate a location with the Resolver data.

14. Click Next.
15. From the Log In Information page of the wizard, click Next.

    The Mobile Device Options page appears, which has several settings that control the user experience on mobile devices.

Figure 437 - Mobile Device Options



This page allows you to disable features normally displayed in the mobile apps.

16. Complete the Mobile Device Options page per these descriptions.

Setting	Description
Toolbar Buttons	
Show Scan Data Button	Clear this checkbox to hide the Scan Data button.
Show Scan Resolver Button	Clear this checkbox to hide the Scan Resolver button.
Show User Login Button	Clear this checkbox to hide the User Login button.
Sound Options	
Play Location Sounds	Plays a sound when a location is entered.
Play User Login Sounds	Plays a sound when the user logs in as a TermSecure or ThinManager user.
User Interface Settings	
Show Zoom Map	Clear this checkbox to hide the screen map while zooming.
Show Toolbar	Clear this checkbox to hide the app toolbar.
Allow Exit to ThinManager Server List	Clear this checkbox to prevent the user from leaving the app to switch ThinManager Servers.
Allow Terminal to sleep	Clear this checkbox to keep a tablet from going into sleep mode.

17. Complete the wizard as you would for any other thin client.

Configure an iOS Device for ThinManager

The iOS Device needs to have the TMC for iOS application installed. The TMC for iOS application can be downloaded from the Apple App Store® for free.

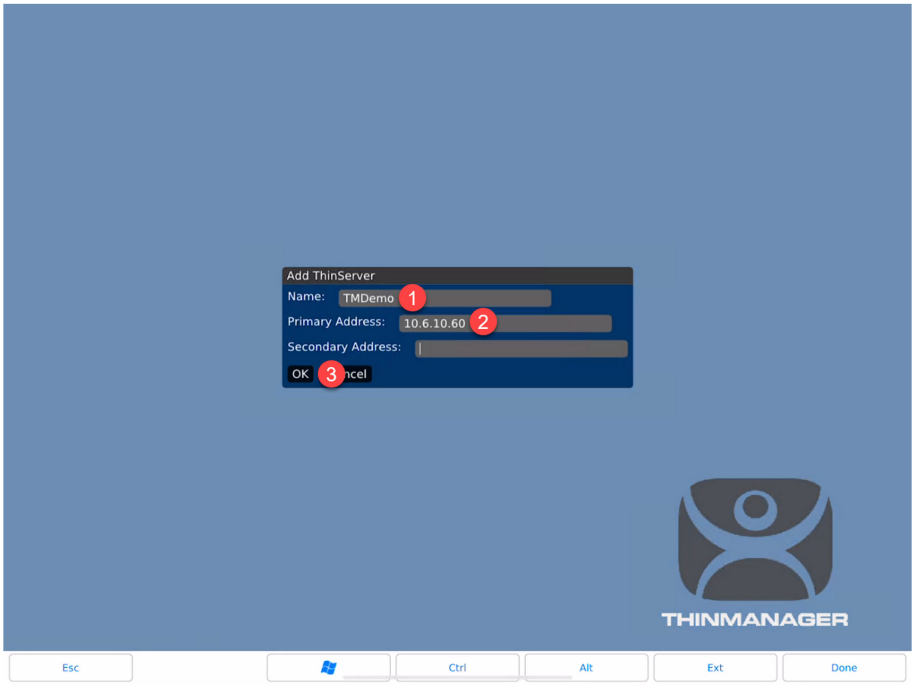
1. Go to the Apple App Store.
2. Type ThinManager Client in the search field.
3. Choose the ThinManager Client (TMC) application and click Open.

   It downloads and installs on your iOS device.

Figure 438 - TMC Icon on iOS Device

4. Press the TMC icon to launch the TMC application.

Figure 439 - Add ThinServer



5. Enter the name of your ThinServer in the Name field.
6. Enter the IP address of your Primary ThinManager server in the Primary Address field.
7. Enter the IP address of your Secondary ThinManager server in the Secondary Address field (if you have one).
8. Click the OK button.

   You are returned to the Main page.

If a message asks if you would like TMC to find and connect to devices on your local network, press Allow.

Figure 440 - Discover and Connect to Devices on Network?

Associate the iOS Device to the Configuration

Once the ThinManager Server is defined on the iOS Device, you must associate the hardware to the TMC for iOS configuration you previously created.

A Pick Replacement page appears, which allows you to choose the newly created Terminal configuration or launch the Terminal Configuration Wizard when you click Create New Terminal.

1. Touch your newly defined Terminal Configuration from the list (TAB01 in the following image).

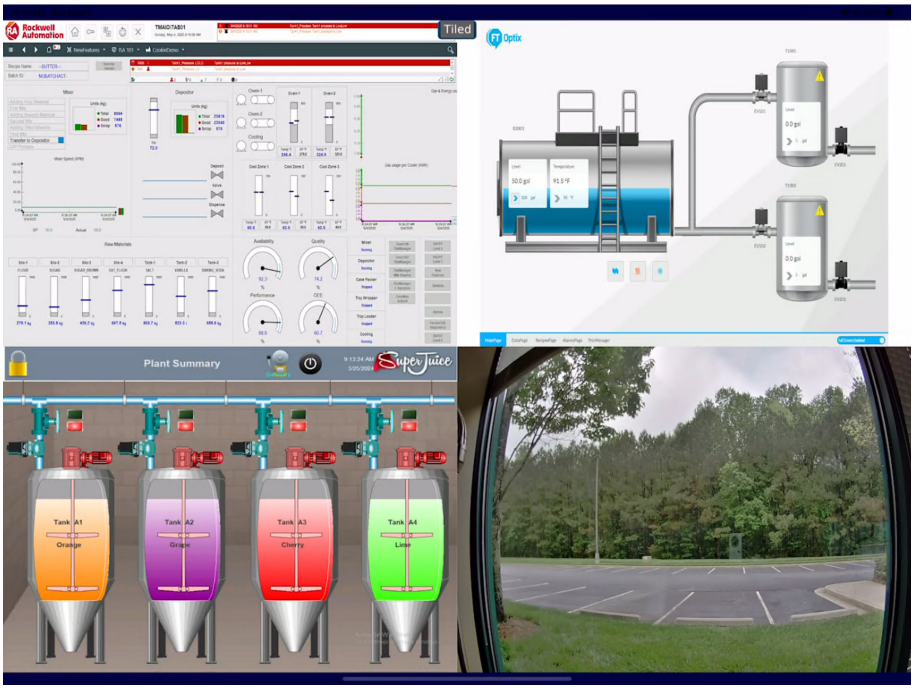
Figure 441 - Pick Replacement

2. If asked to allow TMC to use Bluetooth, touch the Allow button.

Figure 442 - Allow TMC to Use Bluetooth Services

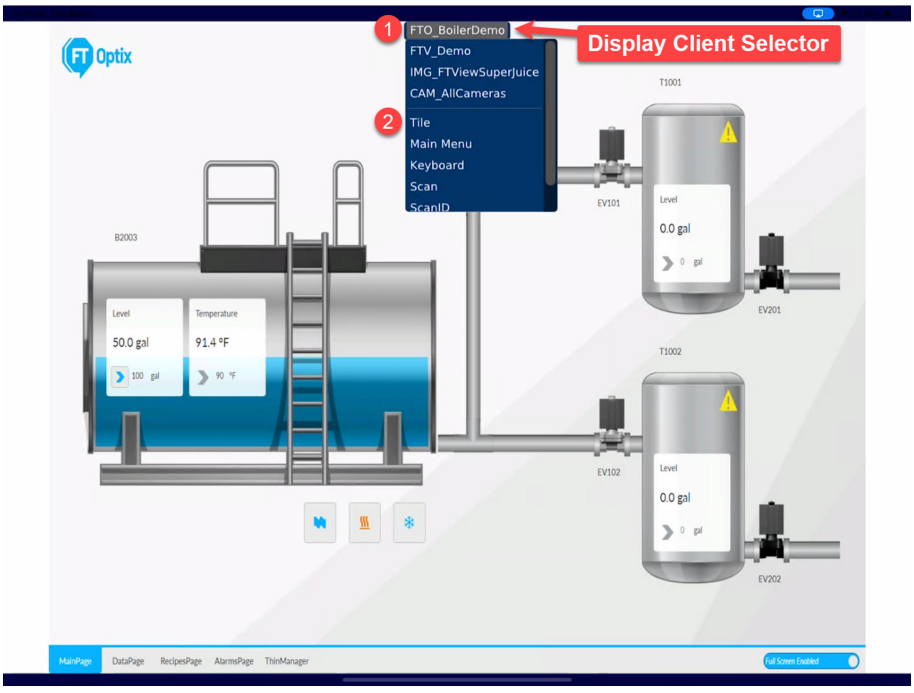
3. In the example below, 4 Display Clients are delivered to the iOS device, which is configured for Tiling Mode. Touch on any of the 4 tiles to bring the selected Display Client to Full Screen.

Figure 443 - Multiple Display Clients on iOS Device



4. To return to Tiling Mode, touch the Display Client Selector at the top of the screen, and select Tile.

Figure 444 - Display Client Selector

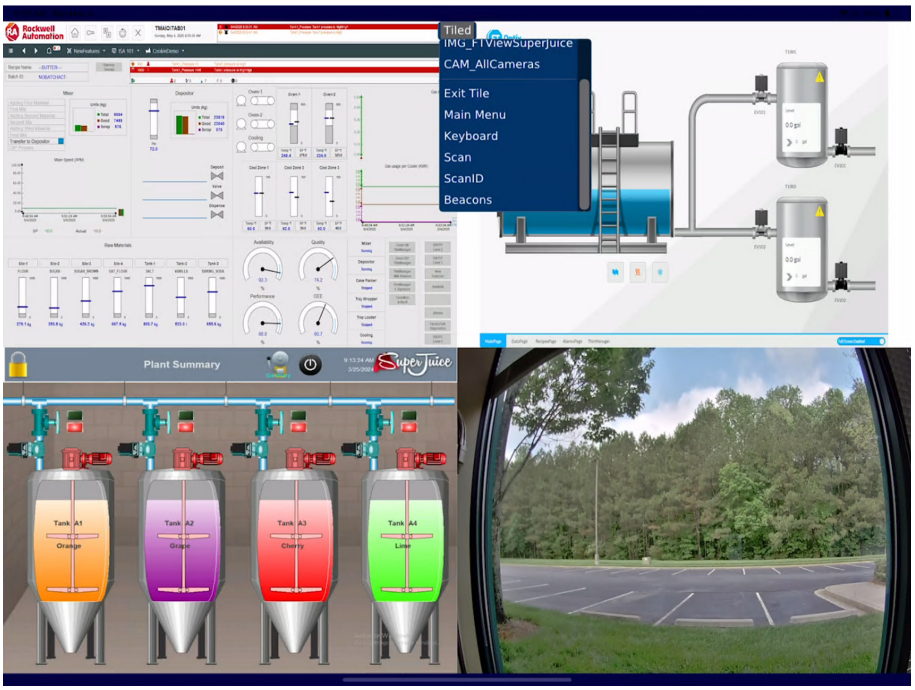


5. From the Display Client Selector, you can select any of the assigned Display Clients, as well as access the Main Menu, Keyboard, Scan, ScanID, and Beacons functions.

Function	Description
Main Menu	Select to open the Main Menu, from which you can LogIn a ThinManager User, manually Select a Location, or Disconnect from ThinManager. The About button provides details about the Terminal, User, Location, as well as the Version. Touch the Disconnect button
Keyboard	The On-screen Keyboard enables you to enter data into your selected Display Client

Function	Description
Scan	Enables you to scan barcodes or QR codes into your select Display Client
ScanID	Enables you to scan QR codes to resolve to defined Locations
Beacons	Enables you to see the signal strength of any configured Bluetooth beacons

Figure 445 - Main Menu



6. Select Main Menu to view the Main Menu, from which you can LogIn a ThinManager User, manually Select a Location, or Disconnect from ThinManager. The About button provides details about the Terminal, User, Location, as well as the Version. Touch the Disconnect button.

Figure 446 - Main Menu

Guided Access on the iOS Device

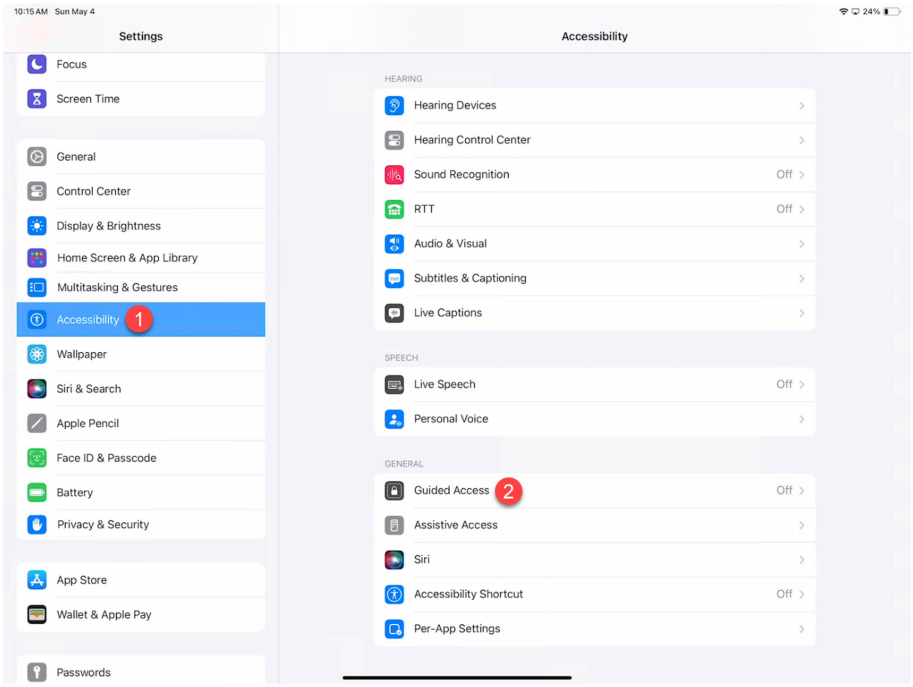
Guided Access is an iOS feature that allows the iOS device to be locked to a single application. Guided Access can help an administrator control the iOS device and limit it to just TMC for iOS.

This section is simply a suggestion for ThinManager users. There are other methods to achieve a similar outcome. Please see Apple documentation for further details on implementation.

To turn on Guided Access, follow these steps.

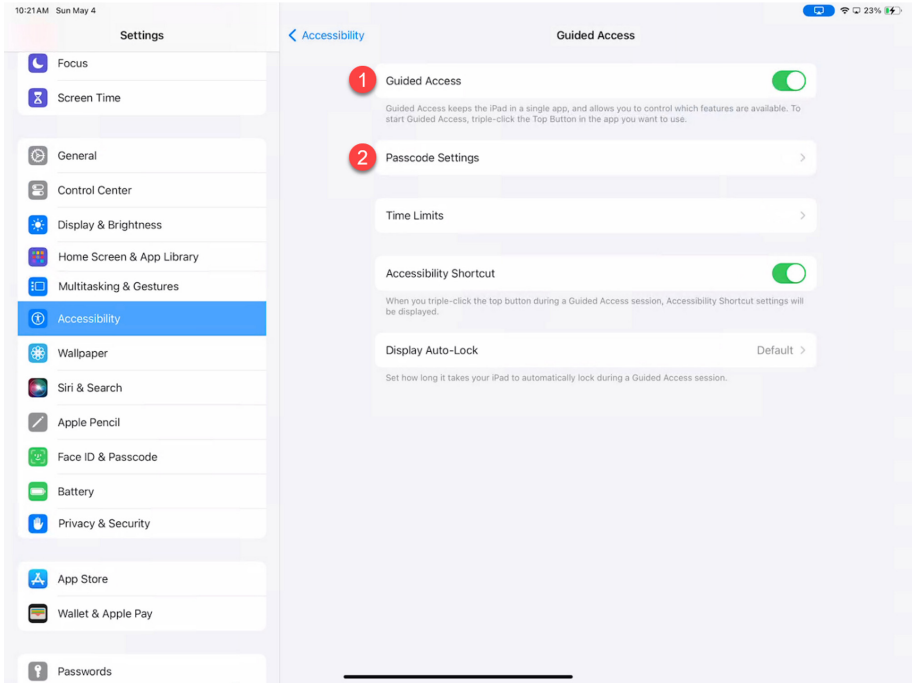
1. Go to Settings on your iOS device and select Accessibility, followed by Guided Access.

Figure 447 - iOS Device Settings



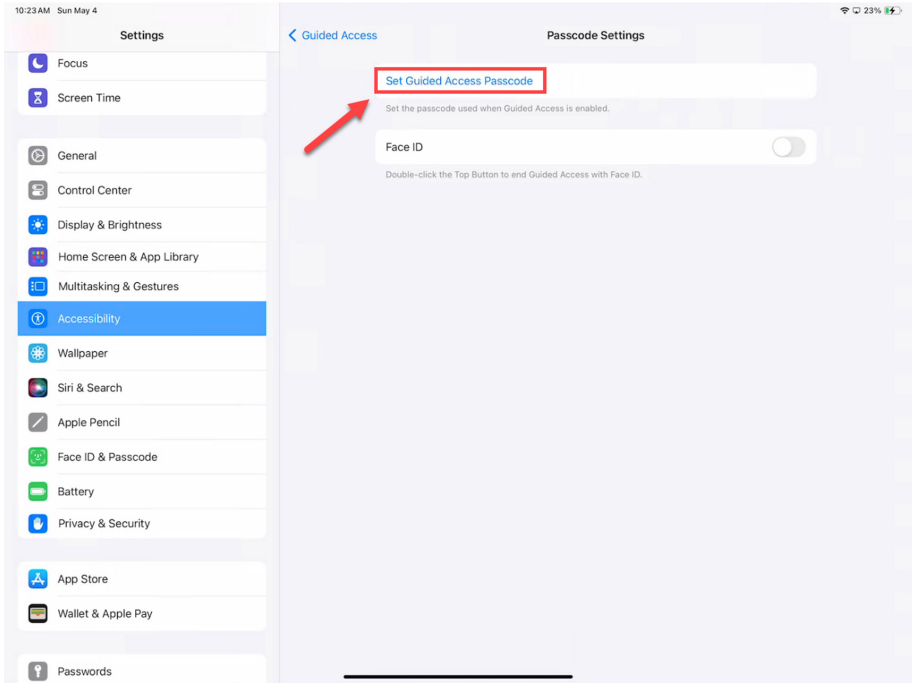
2. Turn on Guided Access, then select Passcode Settings.

Figure 448 - Guided Access and Passcod Settings



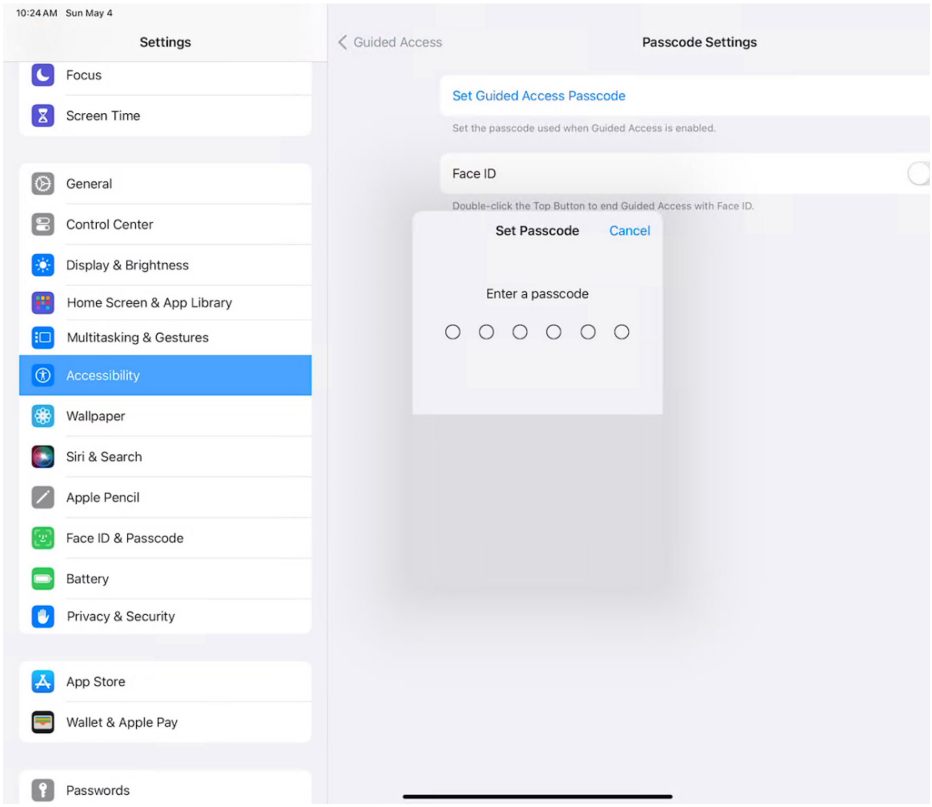
3. Touch the Set Guided Access Passcode button.

Figure 449 - Guided Access Passcode



4. Enter your desired Guided Access passcode and confirm it when prompted.

Figure 450 - Accessibility Settings



How to Use Guided Access.

1. Open TMC for iOS.
2. Depending on the iOS device you have, either press the Top Button (for newer iOS devices) 3 times, or the Home Button (for older iOS devices) 3 times to open the Guided Access control settings. Press Start in the top-right corner.

Figure 451 - Start Guided Access

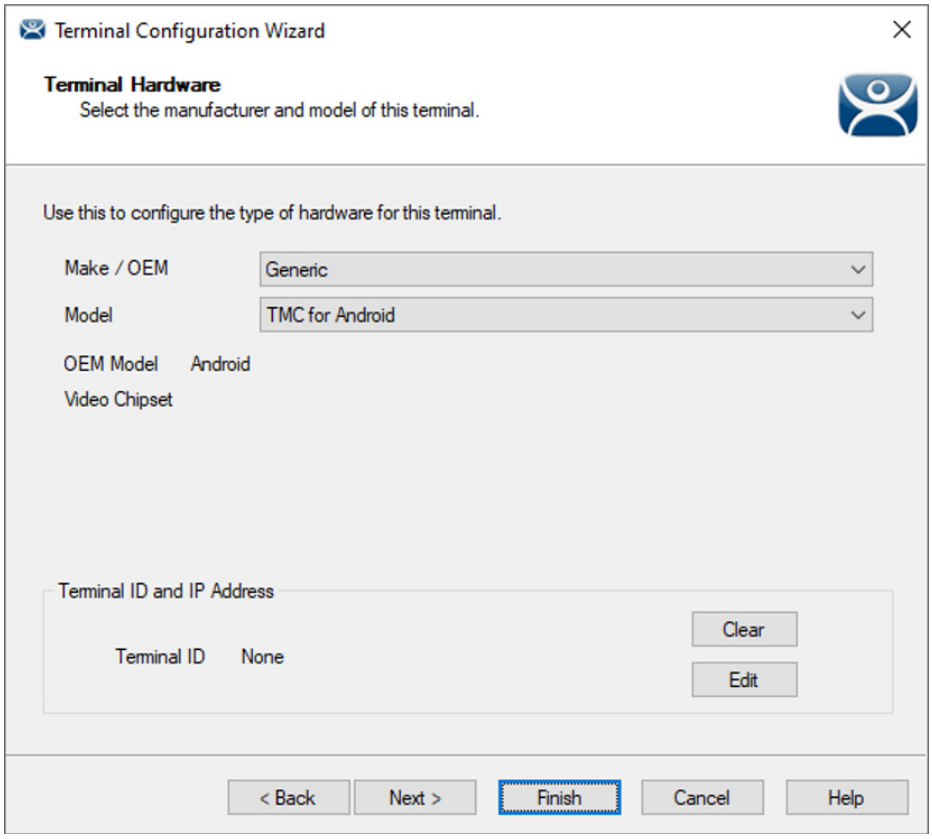
3. To end Guided Access, press either the Top Button (for newer iOS devices) or Home Button (for older iOS devices) 3 times. Enter your Guided Access passcode, and then touch End in the top-left corner.

Figure 452 - End Guided Access

Configure an Android Device

With the new TMC applications, the steps to configure an Android device are identical to the steps presented in the Configure an iOS Device in ThinManager section. However, there is an exception when you select Generic/TMC for Android for the Make and Model to configure the terminal profile in ThinManager.

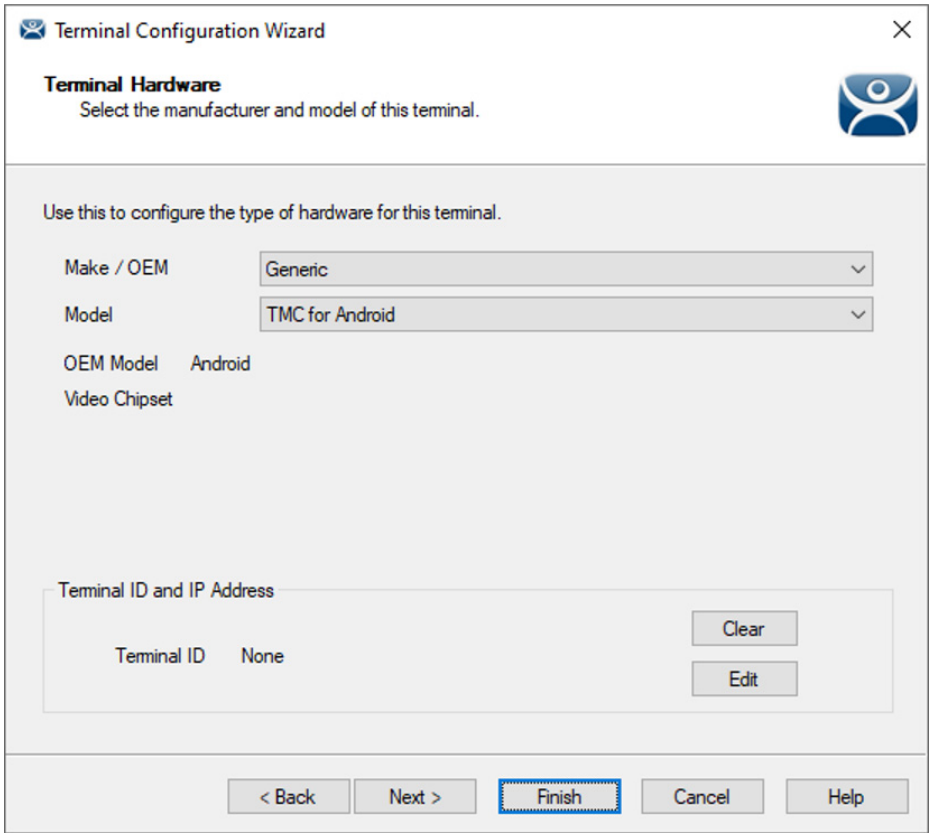
Figure 453 - Terminal Hardware Page



Configure a Windows Device

With the new TMC applications, the steps to configure a Windows device are identical to the steps presented in the Configure an iOS Device in ThinManager section. However, there is an exception when you select Generic/TMC for Windows for the Make and Model when you configure the terminal profile in ThinManager.

Figure 454 - Terminal Hardware Page



ThinManager Users

Introduction

ThinManager User Services grants and denies access to applications based on permissions and membership in Access Groups.

To activate ThinManager User Services, check Enable ThinManager User Services on the Terminal Mode Selection page of the Terminal Configuration Wizard.

See ThinManager User Services Introduction on page 333 for details.

Location Services is Location-based computing. It does not just send an application to a mobile device, but it 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.

To activate Location Services, check Enable Location Services on the Terminal Mode Selection page of the Terminal Configuration Wizard.

See Location Services on page 426 for details.

Location Services has two types of locations: Assigned and Unassigned.

Assigned locations are those that have a Terminal and monitor at the given location, much like traditional computing. Location Services adds additional functions to the location. These functions allow mobile devices to interact with the location and Shadow the Terminal, Clone the applications, or Transfer control of the location to the mobile device.

Unassigned locations are those that lack a permanent Terminal and monitor, and all of the content is sent to the mobile device, which becomes the Terminal.

ThinManager User Services Introduction

ThinManager User Services, formerly TermSecure, is a ThinManager feature that allows users to use a ThinManager-ready thin client to access user-specific or Terminal-specific Display Clients. ThinManager User Services does not replace the Windows login, but adds an additional layer of security and control to it.

ThinManager User Services has two main functions: hiding applications from unauthorized users and deploying applications to a user at any location.

- With Permission Deployed Applications, you can assign a display client to a Terminal and keep it hidden from users until they log in with the correct Permissions. A user with the proper ThinManager User

credentials is able to reveal and access the hidden application.

An example of how to apply this function is to allow a supervisor to initiate a product change in regard to a recipe program. This belongs to the station on the floor, but you want to prevent operators from initiating the change.

- With Roaming User-specific Applications, you can assign Display Clients to a ThinManager user, and they can get access to their applications from any Terminal in the system. This function can be initiated by either manual login or the use of an authentication device.

  Roaming User-specific Applications allow a user to leave one Terminal and log in to a different Terminal and reconnect to their session. Essentially, the session follows the user from Terminal to Terminal.

  An example use for this function includes a quality control worker's ability to retrieve reports assigned to them anywhere they log in.

Permission Deployed Applications are controlled with Permissions, which is covered in Permission-deployed Applications in ThinManager.

Roaming User-specific Applications are controlled when the Display Client is added to the ThinManager User configuration. This is covered in Assign Roaming Display Clients to a ThinManager User on page 355.

The ThinManager User Services section is organized into several sections to walk through the process.

Permission-deployed Applications – See Permission-deployed Applications in ThinManager.

- ThinManager Access Group Creation on page 338
- Create the ThinManager User without a Windows Account on page 347
- Add Access Group to a Display Client on page 341
- Configure Terminals for Location Services on page 343
- Log On to Location Services on page 351

User-specific Applications – See Assign Roaming Display Clients to a ThinManager User on page 355.

- Create the ThinManager User via Active Directory on page 357
- Create login strategies. See Assign Roaming Display Clients to a ThinManager User on page 355
- Add User-specific Display Clients on page 365
- Configure Terminals for Location Services on page 343
- Log On with a ThinManager User Account on page 370

Use of Active Directory to Create ThinManager Users – see Password and Account Management on page 393.

- Batch Create ThinManager Users using Active Directory OU on page 389

Permission-deployed Applications in ThinManager

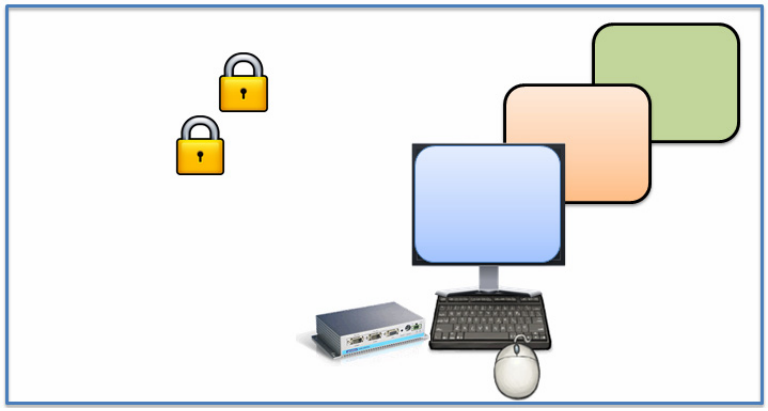
ThinManager User Services can use Access Group Permissions to control access to display clients on a Terminal. Since the display clients belong to the Terminal, they are started with the Terminal's Windows account. The ThinManager user does not need a Windows account to start the session.

The scenario described in this section to explain the concept of Access Groups, Permissions, and ThinManager Users does not have a Windows account tied to it. Window accounts are covered in Create the ThinManager User via Active Directory on page 357.

Permission-deployed Applications Diagrams

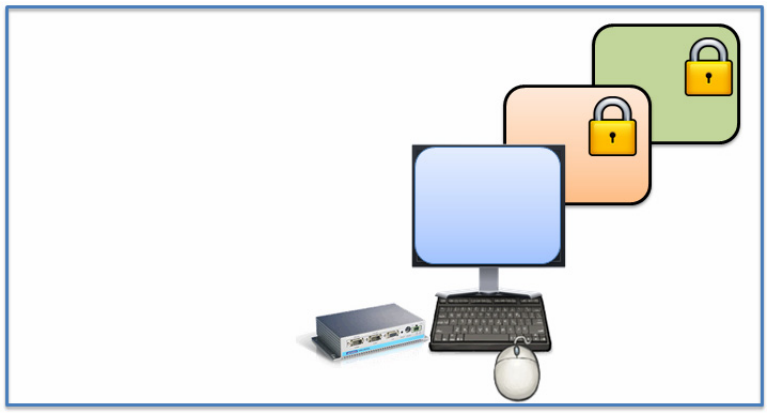
This section is a graphical representation of controlled access to display clients via the Permission tied to Access Groups.

Figure 455 - Create Access Groups



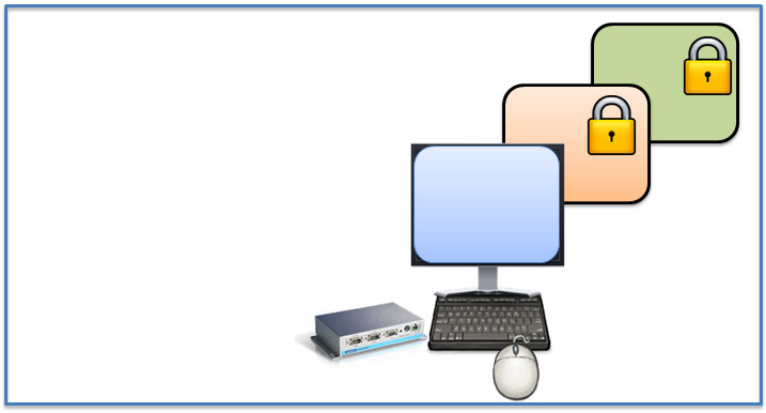
See ThinManager Access Group Creation on page 338.

Figure 456 - Apply Access Groups to Display Clients



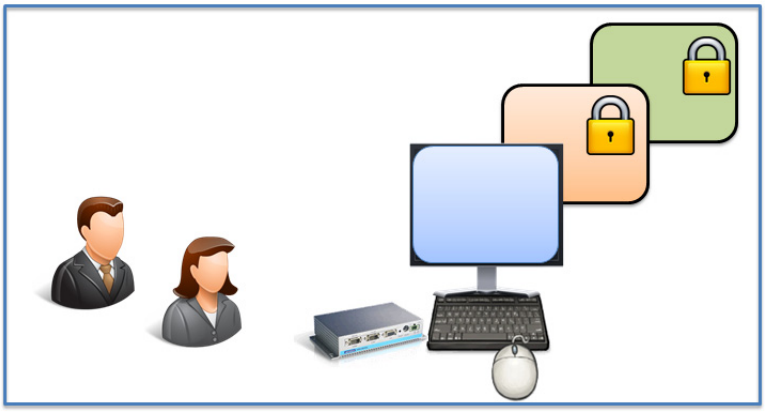
See Add Access Group to a Display Client on page 341.

Figure 457 - Configure Terminals for Location Services



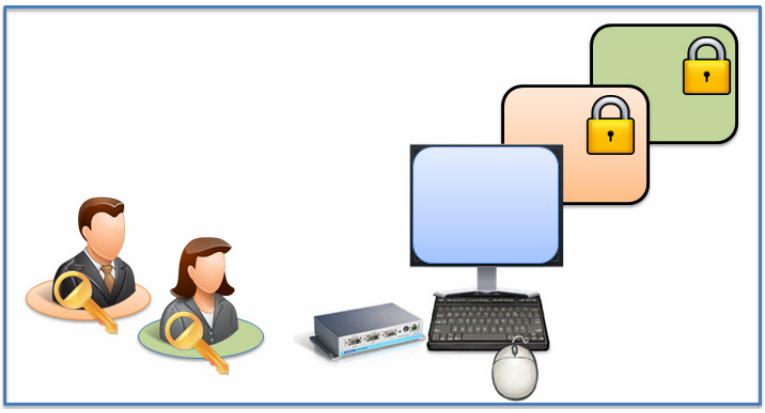
See Configure Terminals for Location Services on page 343.

Figure 458 - Create ThinManager Users



See Create the ThinManager User without a Windows Account on page 347.

Figure 459 - Apply Access Groups to ThinManager Users



See Create the ThinManager User without a Windows Account on page 347.

Figure 460 - Log In with Access Group Permission Unlocks Display Client

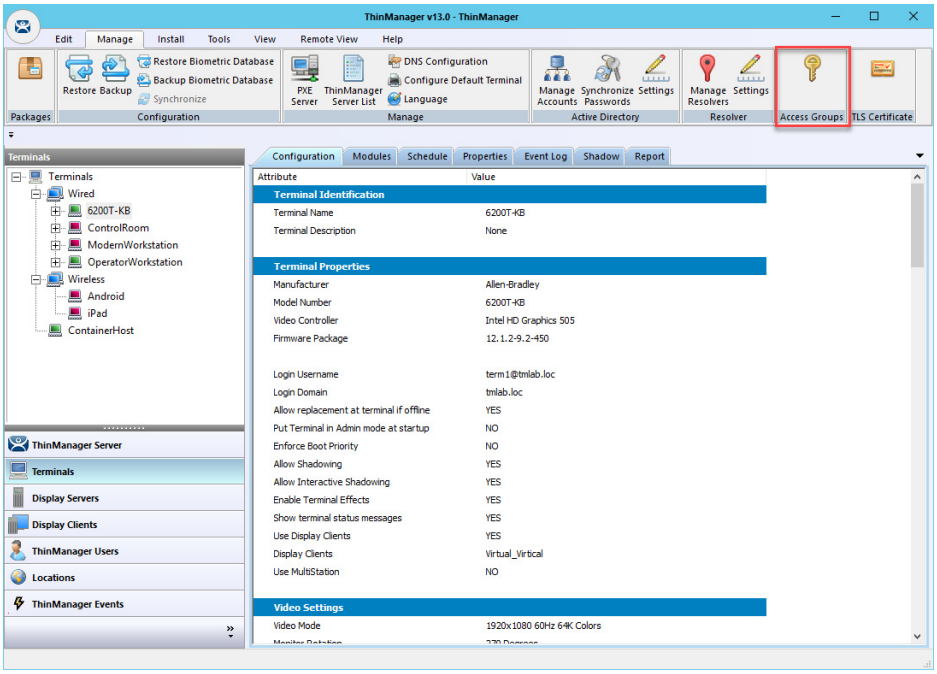
See Log On to Location Services on page 351.

Figure 461 - Different Permissions Grant Access to Different Display Clients

See Log On to Location Services on page 351.

ThinManager Access Group Creation

Figure 462 - Access Groups on ThinManager Menu Bar

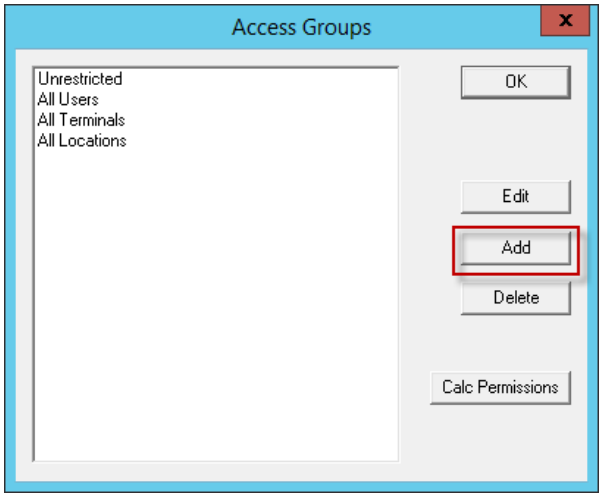


To create a ThinManager Access Group, follow these steps.

1. Choose Manage>Access Groups in the ThinManager menu bar.

   The Access Groups dialog box appears.

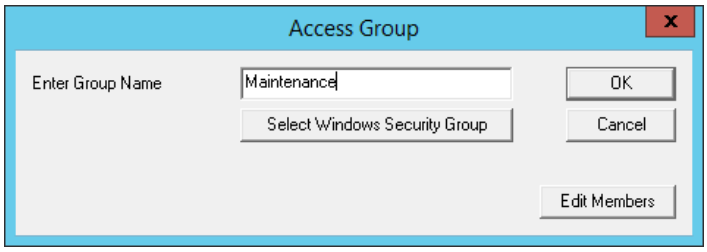
Figure 463 - Access Groups Dialog Box



2. Click Add.

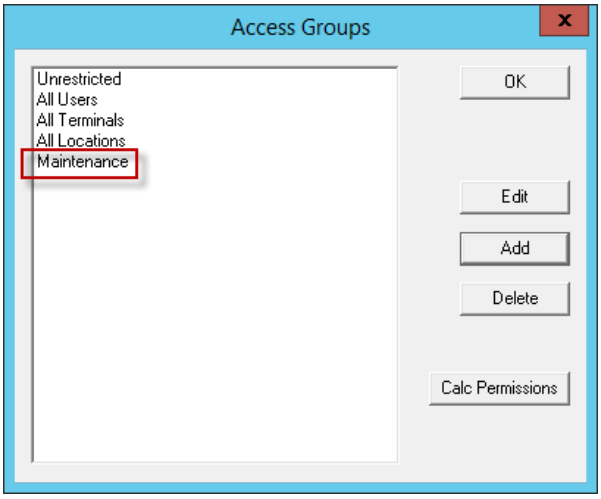
   The Access Group dialog box appears, which lets you define an Access Group.

Figure 464 - Access Group Dialog Box



3. Type a name for your Access Group in the Enter Group Name field and click OK.

Figure 465 - Access Groups Dialog Box



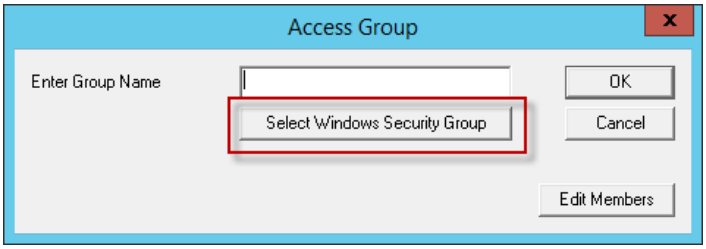
The newly created Access Group appears in the list on the Access Groups dialog box, available for use to grant or deny access to display clients.

Windows Security Groups can be added as Access Groups in a domain.

To add Windows Security Groups as Access Groups, follow these steps.

1. Click Add on the Access Groups dialog box.
2. The Access Group dialog box appears.

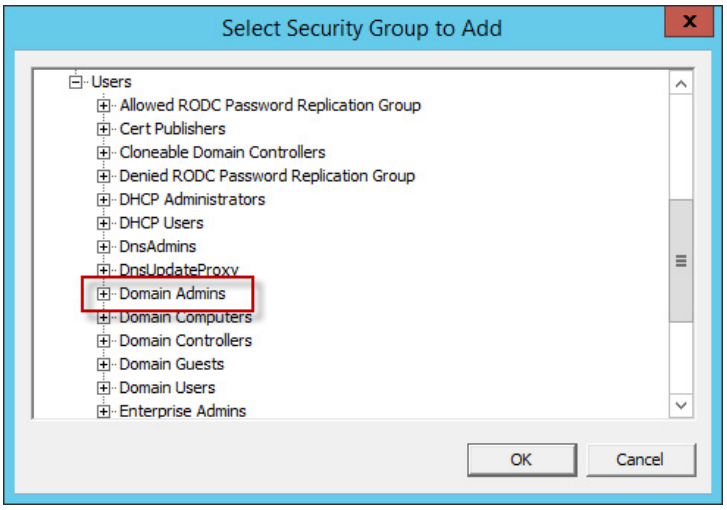
Figure 466 - Access Group Dialog Box



3. Click Select Windows Security Group.

The Select Security Group to Add dialog box appears, which displays the Active Directory tree.

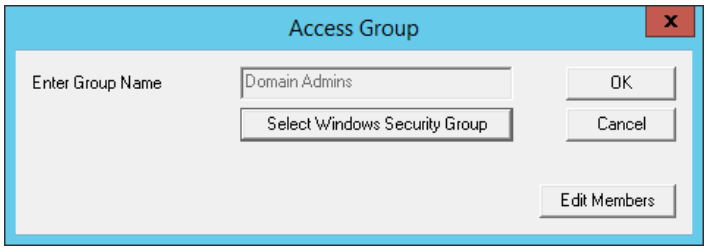
Figure 467 - Select Security Group to Add Dialog Box



4. Highlight the desired Windows group and click OK.

   The Windows security group is populated to the Enter Group Name field of the Access Group dialog box.

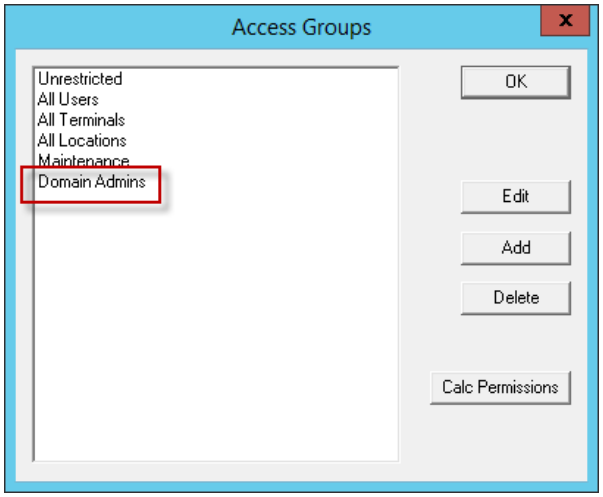
Figure 468 - Access Group Dialog Box



5. Click OK.

   The Windows Security Group is added to the list on the Access Groups dialog box, and it is now available for use to grant or deny access to display clients.

Figure 469 - Windows Security Group as Access Group



Add Access Group to a Display Client

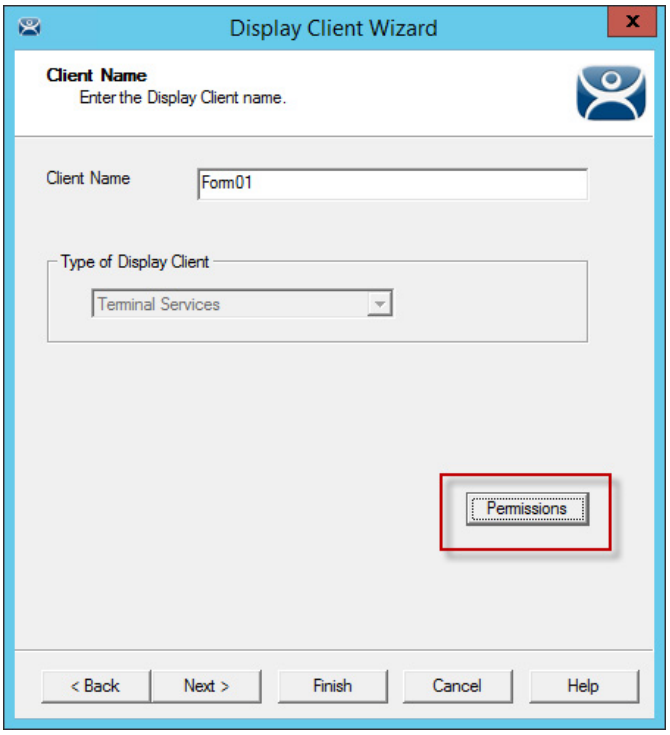
You must add the Access Group to the Display Client that you want to hide from unauthorized users. This example uses Form01 and Form02.

ThinManager Access Group	Display Client	ThinManager User
Maintenance	Form01	Mike, Bob
Supply	Form02	Steve, Bob

1. Double-click on the desired display client in the ThinManager tree.

   The Display Client Wizard appears.

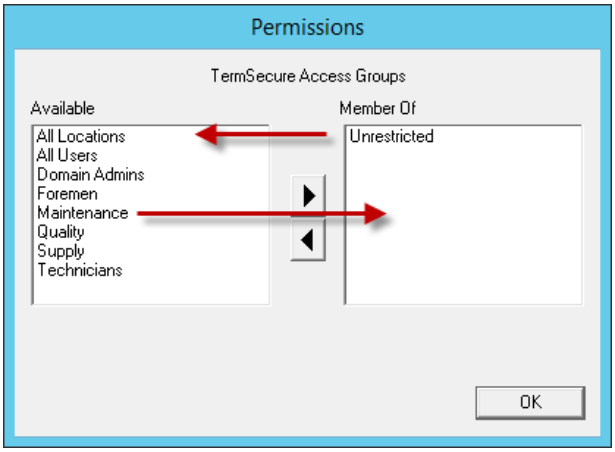
Figure 470 - Client Name Page



2. Click Permissions

   The Permissions dialog box appears.

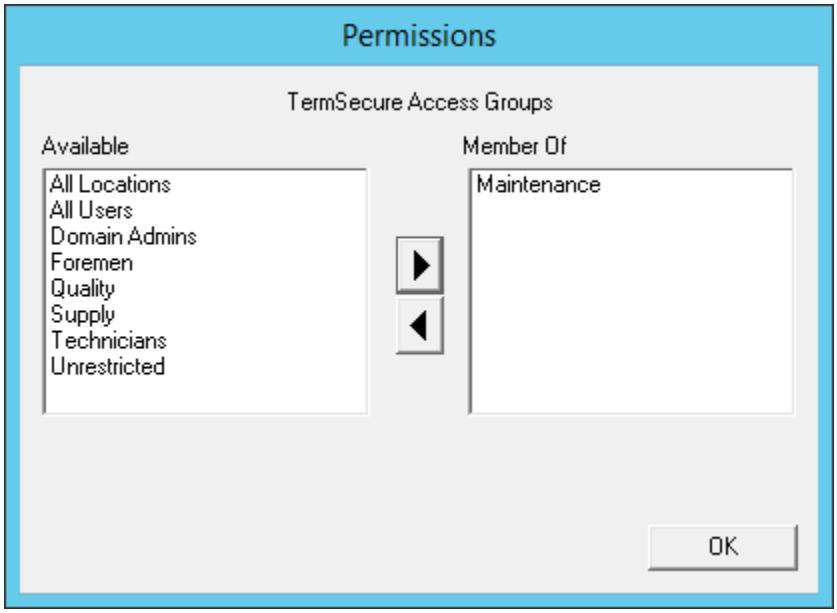
Figure 471 - Display Client with Permissions Dialog Box



Display clients are members of the Unrestricted group by default.

3. Highlight Unrestricted in the Member Of list and click the left arrow to remove it from the list.
4. Highlight the desired Access Group and click the right arrow to add the Access Group to the Member Of list. A display client can have several Relevance Access Groups added to it.

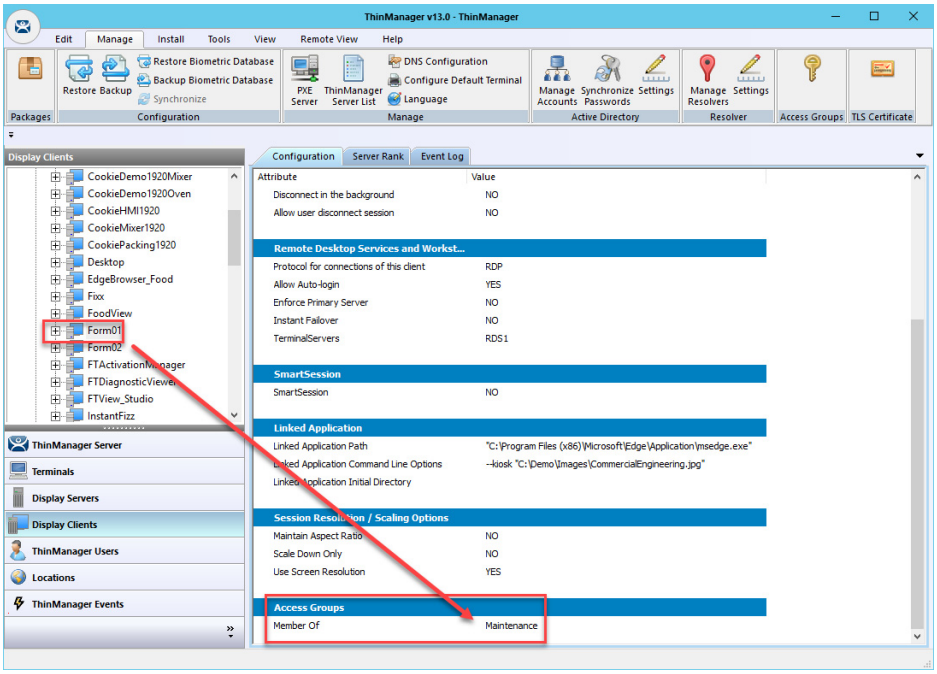
Figure 472 - New Group Membership



The Permissions dialog box shows the Relevance Access Group membership.

5. Click OK to accept the change.
6. On the Client Name page, click Finish to close the Display Client Wizard and accept the changes.

Figure 473 - Display Client Configuration Properties



7. Highlight the display client in the Display Clients tree and click the Configuration tab to quickly view Access Group membership. Scroll

down to the bottom of the Configuration tab to see Access Group membership.

Figure 473 shows that this process was repeated to assign Maintenance to Form01.

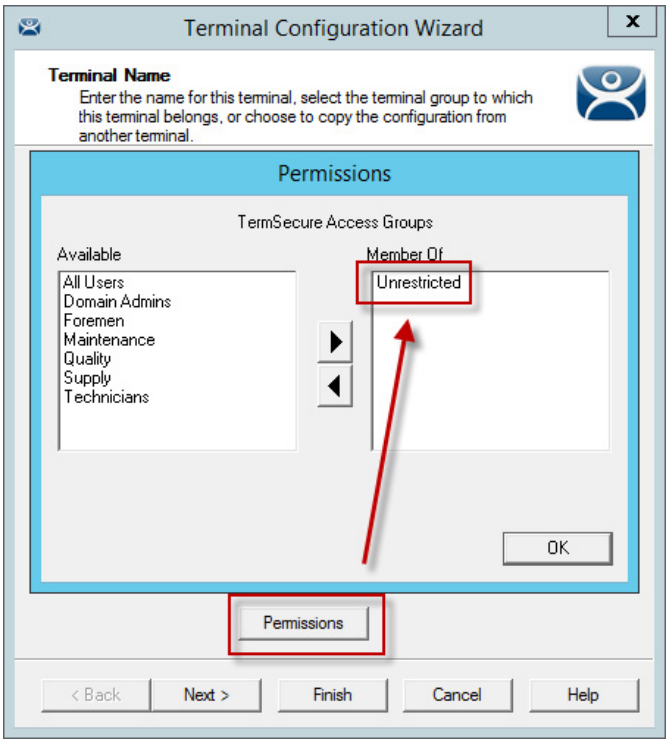
Configure Terminals for Location Services

Each Terminal can be configured to allow ThinManager logins.

1. Double-click on a Terminal in the ThinManager tree.

   The Terminal Configuration Wizard appears.

Figure 474 - Default Terminal Permissions

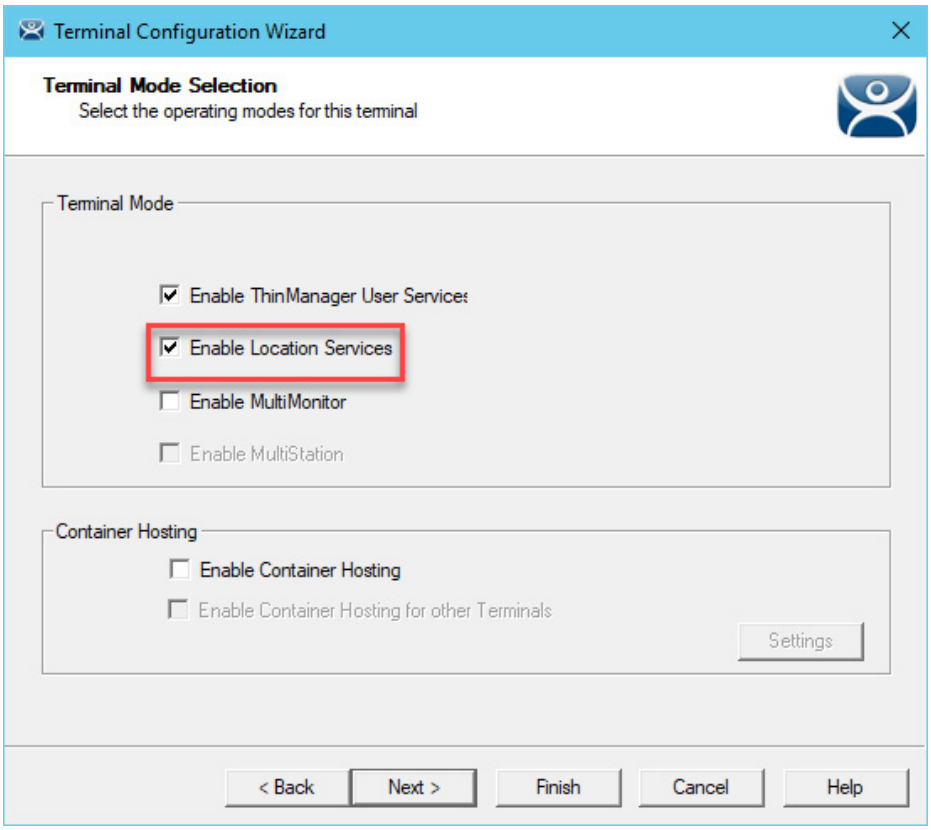


By default, Terminals are members of the Unrestricted Access Group, which allows any user to use the Terminal. Leave it this way unless you want to require a ThinManager login to allow any access at all.

Setting an Access Group in Permissions for a Terminal locks users out of the Terminal until they log in with a ThinManager User account.

Access is configured on the Terminal Mode Selection dialog box.

Figure 475 - Terminal Mode Selection



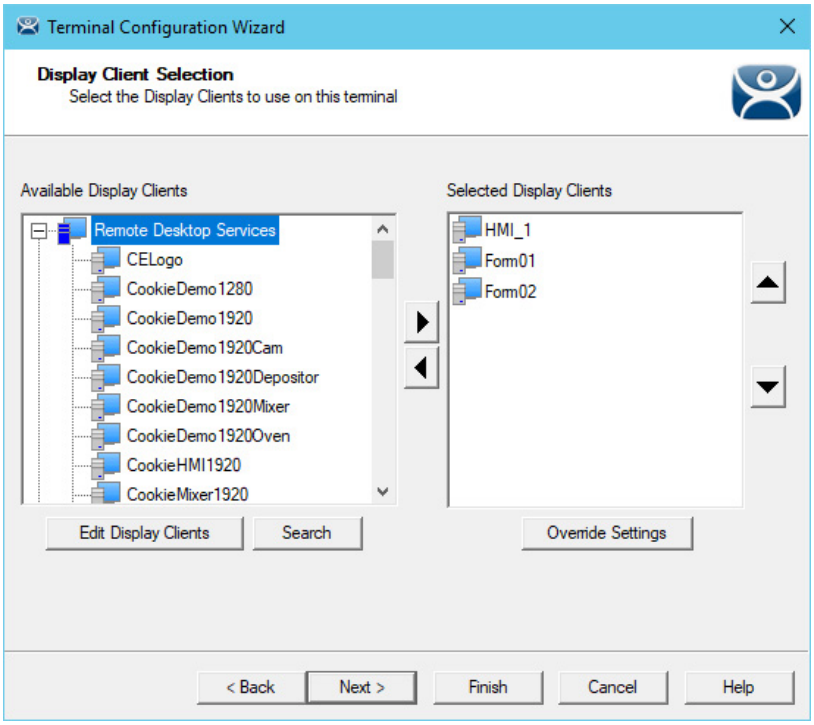
2. Check Enable Location Services to enable Location Services logins on the Terminal.

You must use Display Clients with Location Services.

You may use ThinManager User Services in combination with MultiMonitor and/or Location Services.

3. Click Next until the Display Client Selection page appears.

Figure 476 - Display Client Selection



4. Add the display clients to the Terminal.

   In Figure 476, HMI_1 is Unrestricted, Form01 is restricted to Maintenance, and Form02 is restricted to Supply.

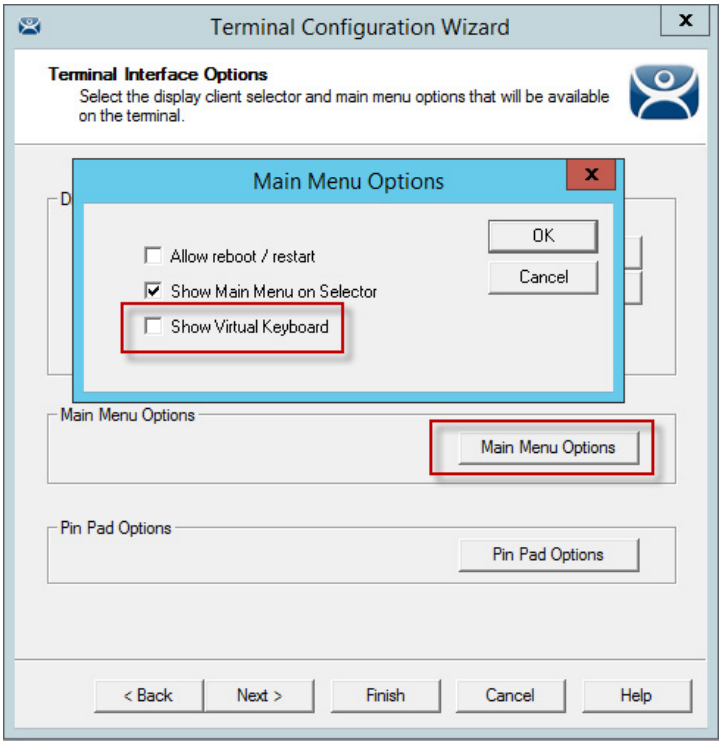
5. Click Next until the Terminal Interface Options page appears.

When Enable Location Services is checked on the Terminal Mode Selection page (see Figure 475 on page 344), a Main Menu Options button is displayed on the Terminal Interface Options page.

6. Click Main Menu Options.

   The Main Menu Options dialog box appears, which configures the Location Services Login Menu.

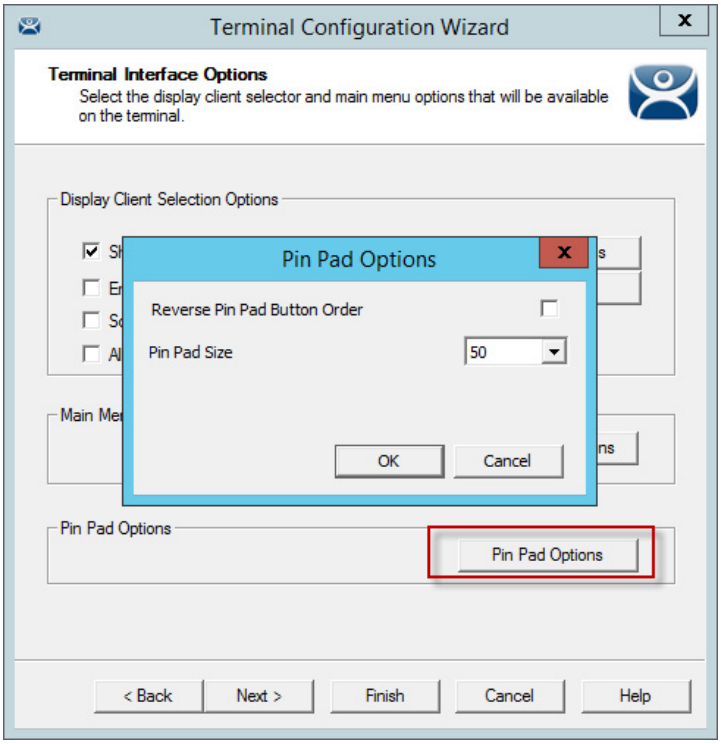
Figure 477 - Terminal Interface Options Page



Setting	Description
Allow reboot/restart	Adds Reboot and Restart to the menu.
Show Main Menu on Selector	Adds the Location Services Main Menu to the Display Client pull-down menu.
Show Virtual Keyboard	Shows a virtual keyboard to the login process. Use to display an on-screen keyboard for touch screens.

7. Click OK to accept the changes.

Figure 478 - Pin Pad Options Dialog Box



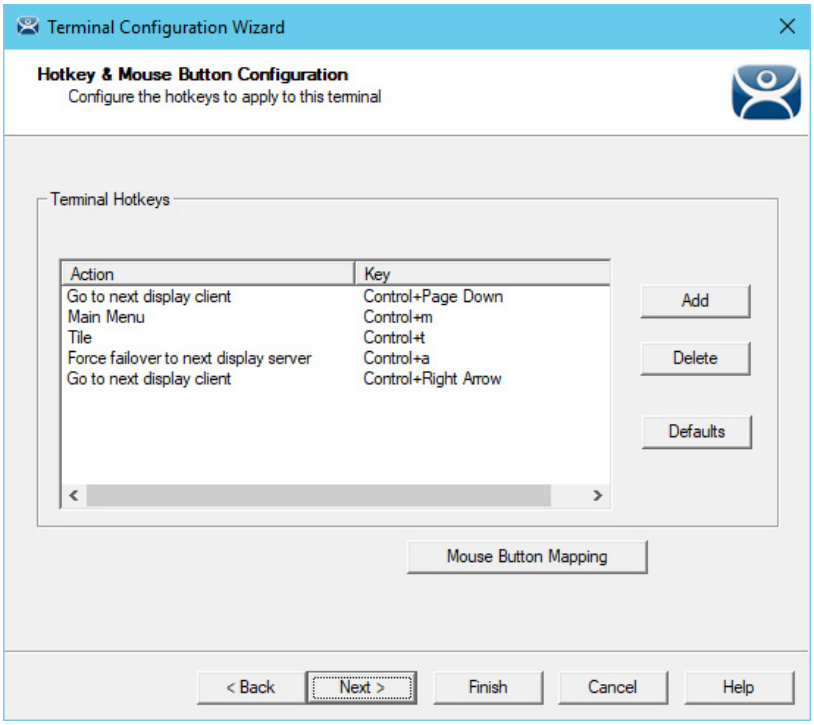
The Pin Pad Options dialog box allows you to configure the PIN pad when using a Personal Identification Number instead of a password.

Setting	Description
Reverse Pin Pad Button Order	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	Sets the size of the PIN pad as a percentage of the screen size.

8. Click Next.

   The Hotkey & Button Configuration page appears.

Figure 479 - Hotkey & Button Configuration Page



When Enable Location Services is checked on the Terminal Mode Selection page (see Figure 475 on page 344), a Main Menu hotkey action is displayed in the Terminal Hotkeys section of the Hotkey & Mouse Button Configuration page. This allows you to set a keyboard hotkey to launch the Location Services menu.

9. Click Finish to apply the changes.
10. Reboot the Terminal after changes are made.

Create the ThinManager User without a Windows Account

The ThinManager User Configuration Wizard is launched from the ThinManager Users branch of the ThinManager tree.

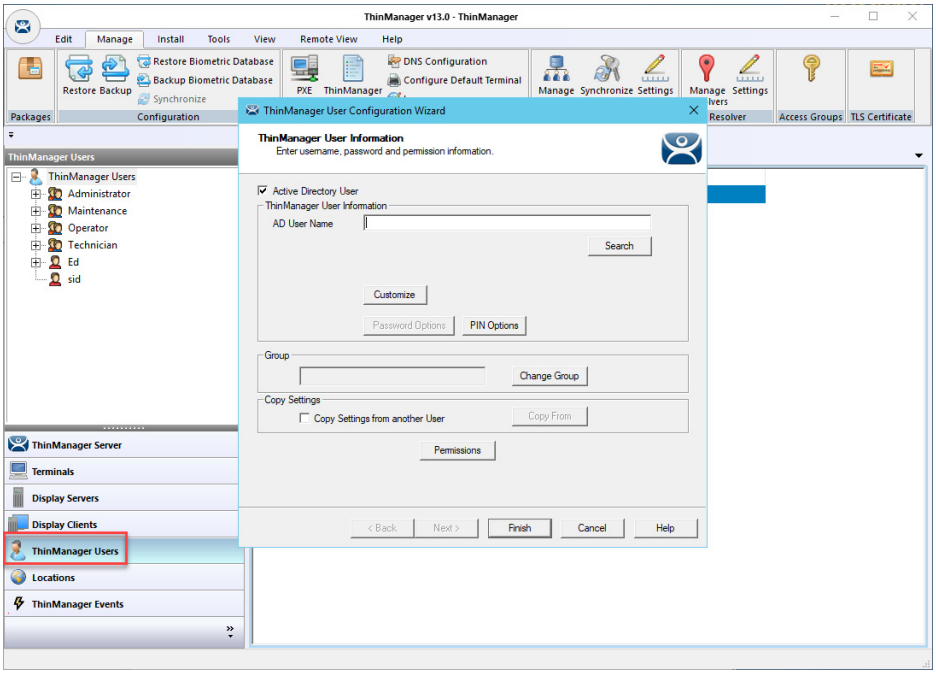
1. Click ThinManager Users at the bottom-left of the ThinManager tree.

   The ThinManager Users tree appears.

2. Right-click on the ThinManager Users branch and choose Add User.

   The ThinManager User Configuration Wizard appears.

Figure 480 - User Branch of the ThinManager Tree



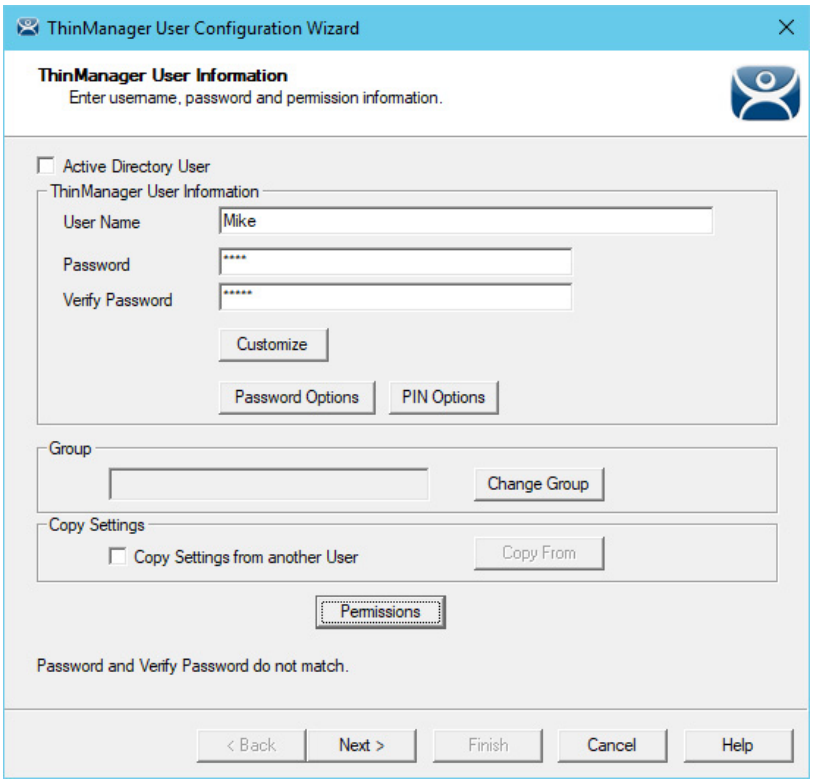
The first page of the ThinManager User Configuration Wizard is the ThinManager User Information page that creates the ThinManager User account.

ThinManager Users with display clients assigned to them must be tied to a Windows account.

If a ThinManager User does not have a display client assigned to them, and they only use the Permissions to access a display client that belongs to the Terminal, then the user does not need a Windows account.

In this scenario, a Windows account is not needed because the display client belongs to the Terminal and is getting logged in with the Terminal's account. A Permission is applied to the user.

Figure 481 - ThinManager User Information Page

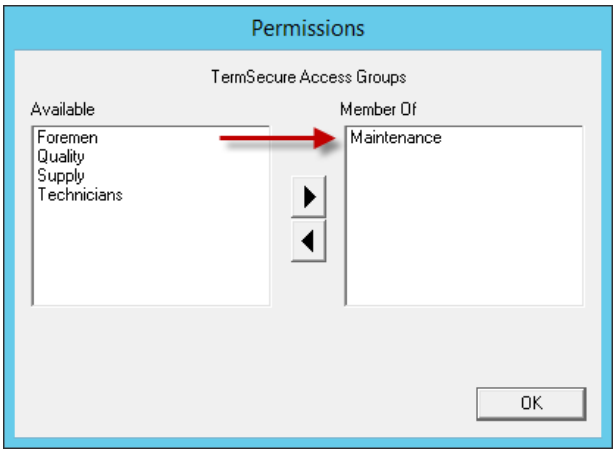


3. To create a ThinManager User that is not an Active Directory user, first, clear the Active Directory User checkbox.
4. Type a name in the User Name field.
5. Type a password into the Password and Verify Password fields.

   A dialog box appears if the passwords do not match.
6. Click Permissions.

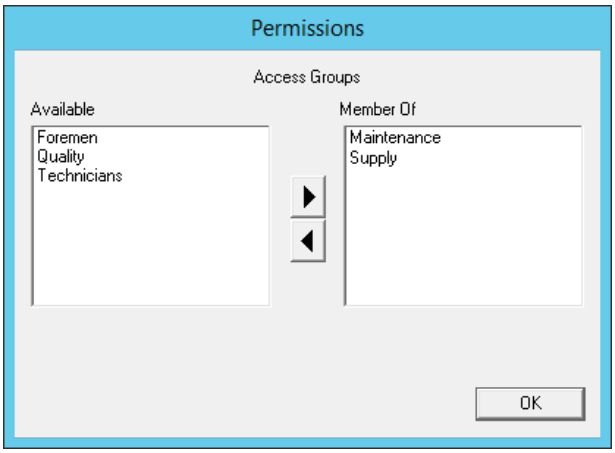
   The Permissions dialog box appears.

Figure 482 - Permissions Dialog Box



7. To add your Relevance Access Group to your created user, double-click on the Access Group in the Available list to move it to the Member Of list.

Figure 483 - Multiple Access Groups



A ThinManager User can be a member in multiple Access Groups.

8. Click OK button to accept the changes.

These are the only settings needed for a ThinManager User to unlock hidden applications: a ThinManager User name and membership in a Relevance Access Group. The wizard has other settings that are described in ThinManager Configuration Wizard on page 362.

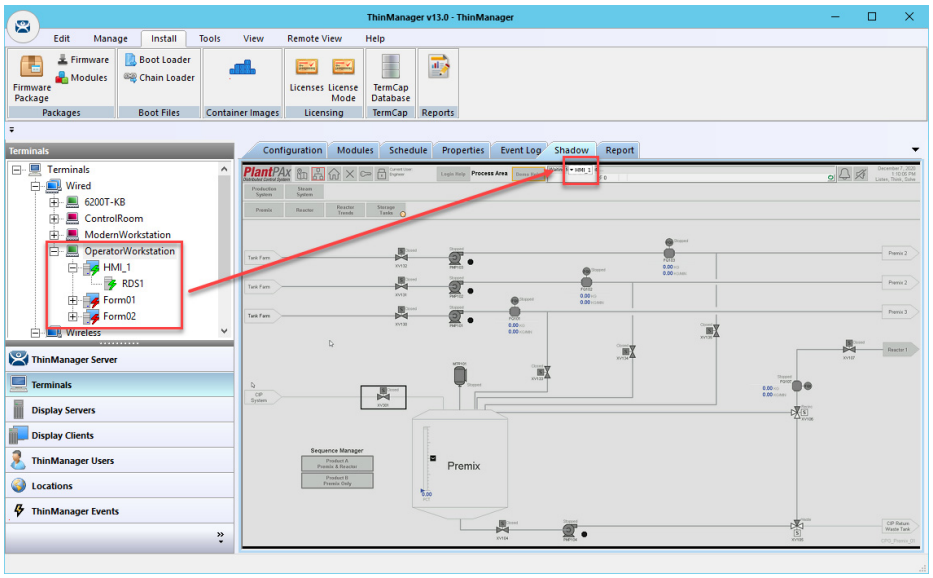
Location Services Results

Use the information in this table to follow the example inFigure 484.

Relevance Access Group	Display Client	ThinManager User
Maintenance	Form01	Mike, Bob
Supervisor	Form02	Steve, Bob

The OperatorWorkstation is using Location Services with the unrestricted HMI_1 display client and the restricted Form01 and Form02 display clients.

Figure 484 - ThinManager Shadow of Thin Client Example



The example in Figure 484 shows the ThinManager tree and the shadowed display of the thin client.

- The Terminals tree shows four display clients assigned to OperatorWorkstation. The lightning bolt indicator for the hidden display clients are red to show that it does not have a connection. Only HMI_1 and RDS1 are visible on the Terminal because they are unrestricted.
- Figure 484 shows the group selector in the shadow and displays the unhidden display client in the selector.

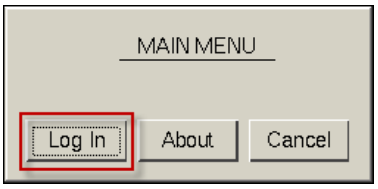
Log On to Location Services

To log in a ThinManager User on a Terminal, follow these steps.

1. Go to a Terminal that has Enable Location Services checked on the Terminal Mode Specification page, see Figure 475 on page 344.
2. Log in one of these ways.
   - Open the display client selector pull-down menu and choose Main Menu.
   - Press the CTRL+m hotkey to launch the Main Menu if the hotkey was activated.

   The Main Menu is displayed on the Terminal.

Figure 485 - Location Services Main Menu

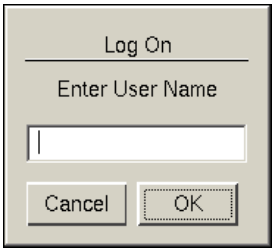


3. Click Log In.

   A virtual keyboard is displayed if Show Virtual Keyboard is checked on the Main Menu Options dialog box when the Terminal for Location Services is configured on the Terminal Interface Options page.

Figure 486 - Location Services Log On Screen with Virtual Keyboard

Figure 487 - Location Services Log On



4. Type your ThinManager user name in the Enter User Name field and click OK.

Figure 488 - Password Dialog Box

5. Type the password in the Enter Password field.
6. Click OK.

Figure 489 - ThinManager with User Logged On

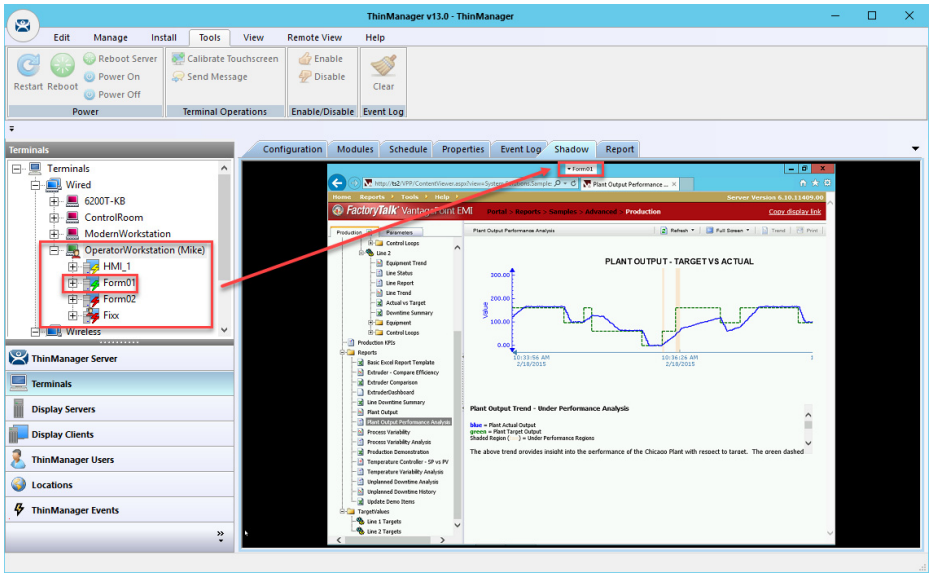
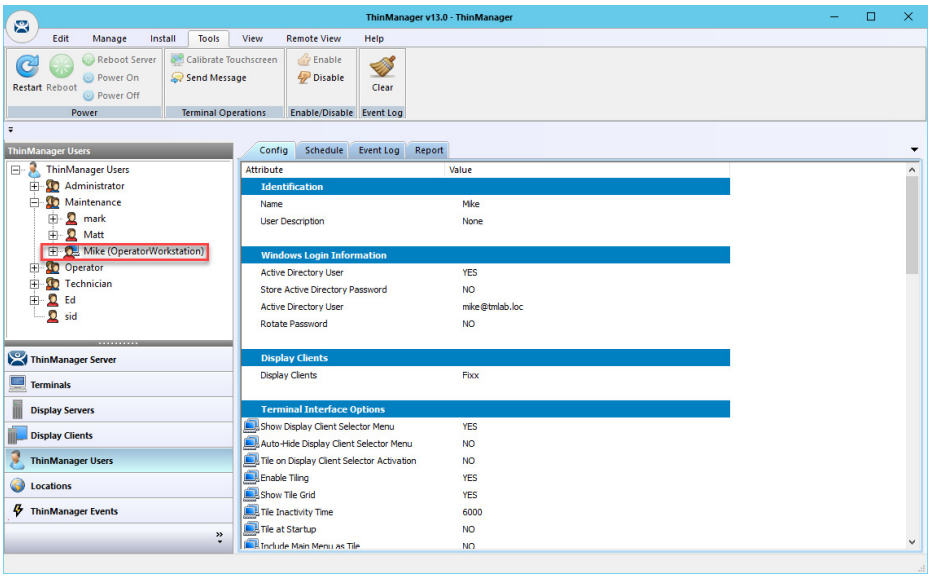


Figure 489 shows ThinManager User, Mike, logged in to the Terminal, his name in parentheses.

Notice that the group selector on the shadowed Terminal now has the hidden display client showing in the pull-down menu. The lightning bolt icon now shows a connection.

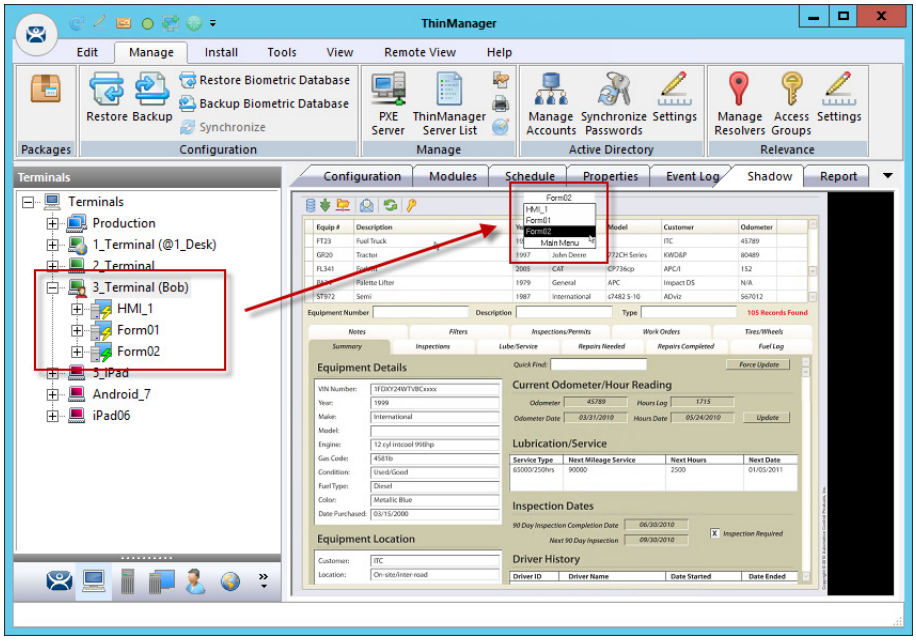
The ThinManager Users tree lists the users.

Figure 490 - ThinManager Users Tree



A user that is logged in to a terminal with Location Services shows a different icon and the name of the terminal into which they are logged. In Figure 490, Mike is logged in to OperatorWorkstation.

Figure 491 - Membership in Multiple ThinManager Access Groups



A ThinManager User can be a member of multiple Location Services Access Groups.

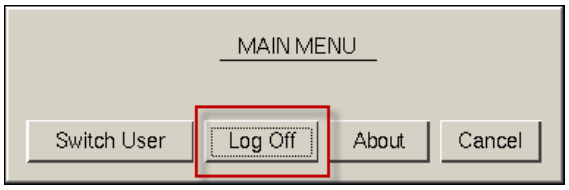
In Figure 491, Bob is a member of both Maintenance and Supply. When he is logged in, the display clients for both Maintenance and Supply are displayed. They are hidden when he logs off.

Log Out of Location Services

The ThinManager User can log out by one of these actions.

- Open the Location Services Main Menu on the Terminal and click Log Off
- Right-click on the ThinManager User in the ThinManager tree and choose Logoff User
- Restart or reboot the Terminal that has a ThinManager User logged in

Figure 492 - Main Menu



Button	Description
Switch User	Logs off the ThinManager User and disconnects any sessions from Display Clients assigned to the user. It opens the Login screen for another ThinManager User.
Log Off	Logs off the ThinManager User, and logs off any sessions from Display Clients assigned to the user, and returns to the Terminal's display.

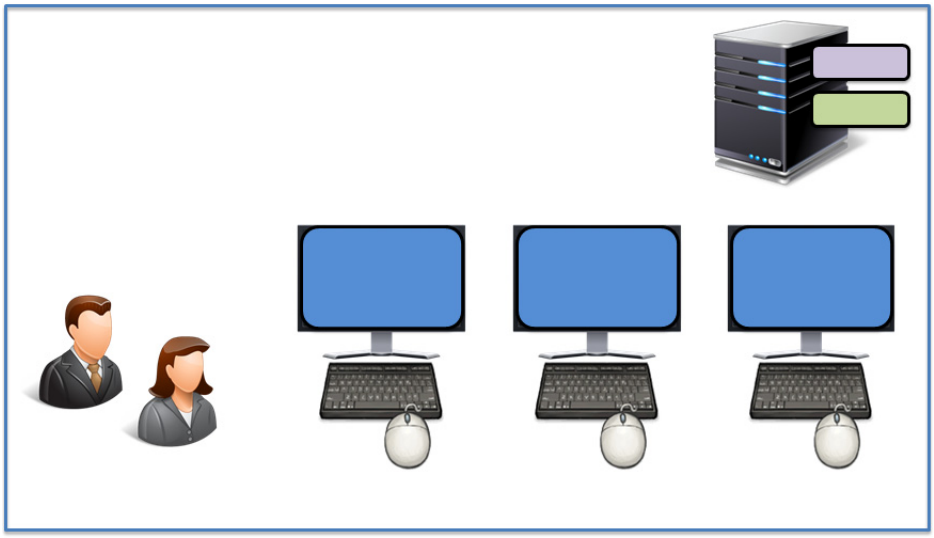
Assign Roaming Display Clients to a ThinManager User

Location Services can assign a user-specific display client to a ThinManager User. This display client is accessible from any Terminal or location that has been configured with ThinManager User Services. ThinManager Users require a valid Windows account since they log in to a Windows session of their own.

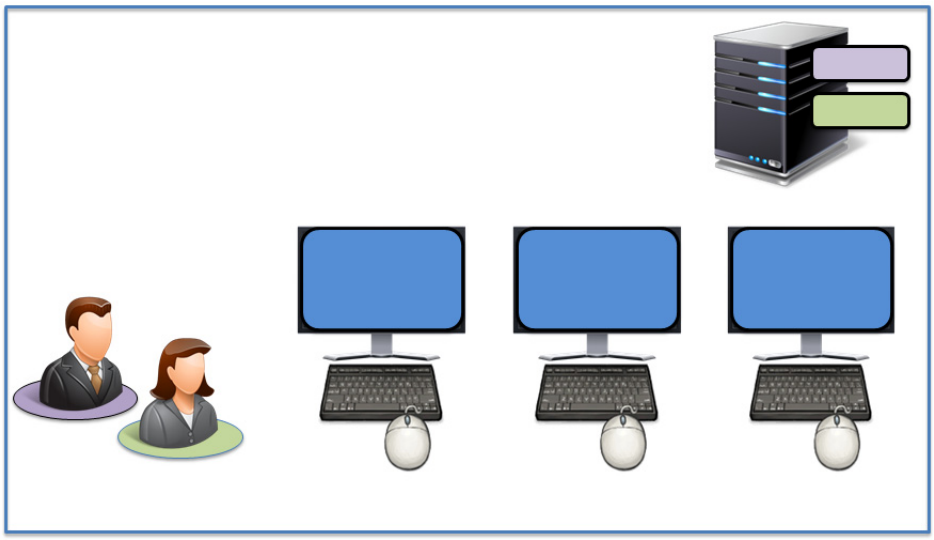
Roaming Display Clients in Location Services Diagrams

The following is a graphical representation of the process to assign user-specific display clients to a ThinManager user to allow the application to follow the user anywhere they need to go.

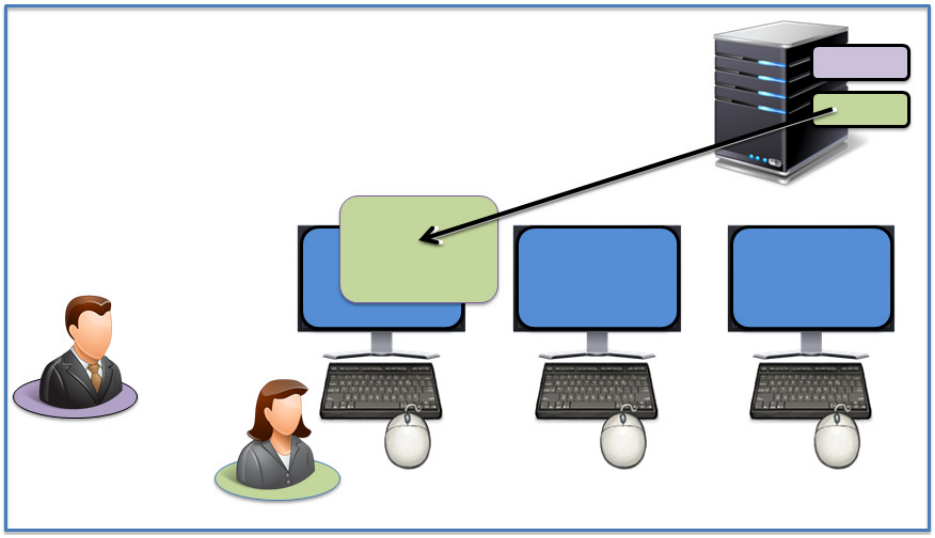
Create ThinManager Users and Display Clients



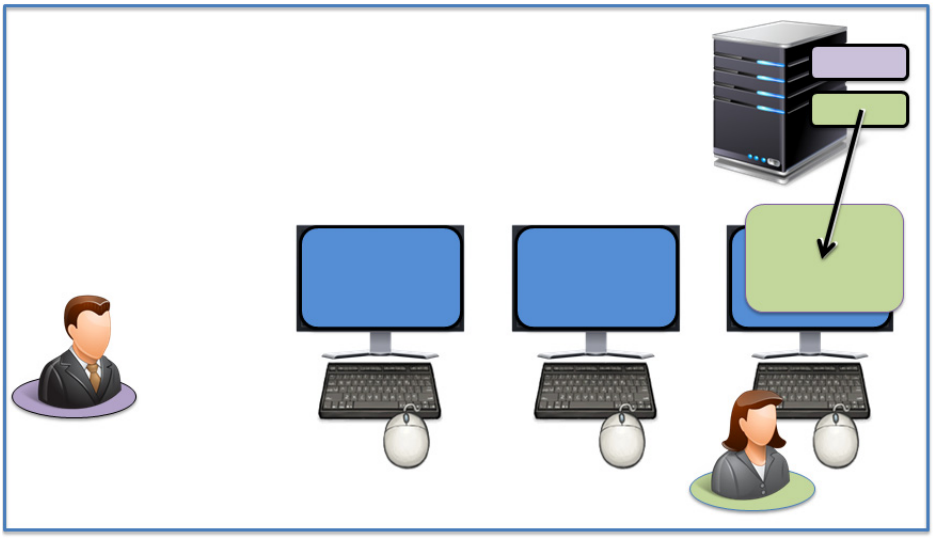
Assign the Display Client to the ThinManager User



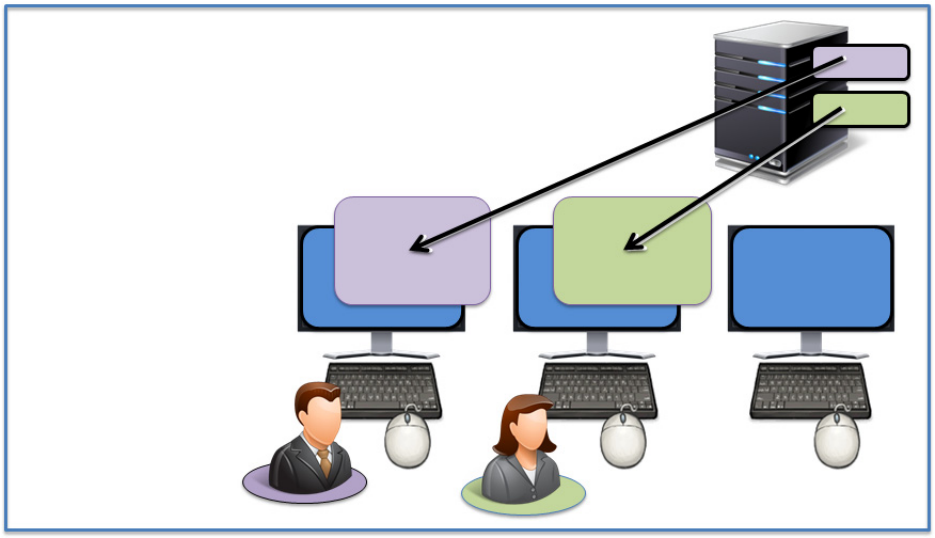
The Display Client is sent to the Terminal where the ThinManager User Logs In



The Display Client follows the ThinManager User



The Display Client Follows the ThinManager User



Create the ThinManager User via Active Directory

ThinManager Active Directory integration allows a ThinManager User to have its Windows user account drawn from the Active Directory. You allow ThinManager to store the password to streamline password management.

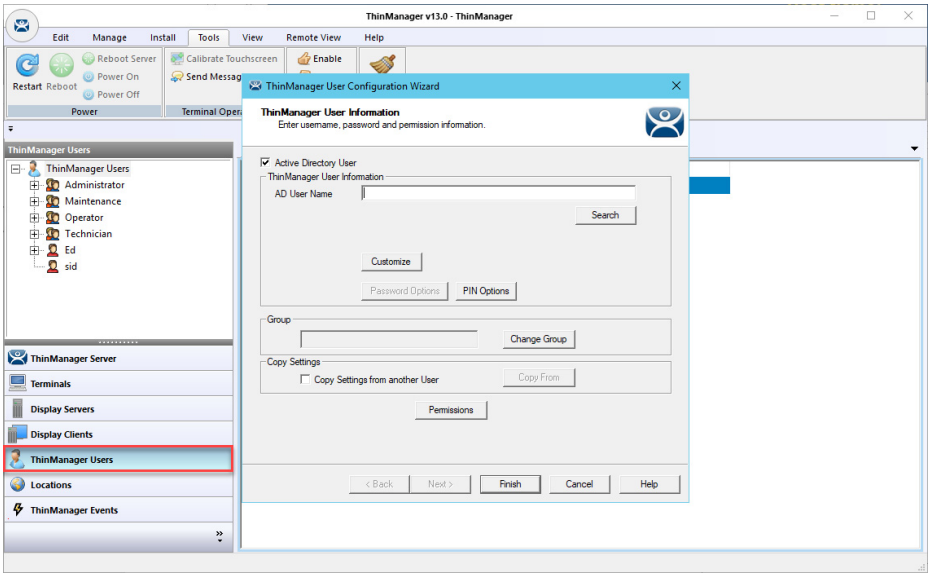
The ThinManager User Configuration Wizard is launched from the ThinManager User branch of the ThinManager tree.

1. Click ThinManager Users near the bottom-left corner of the ThinManager tree.

   The ThinManager Users tree appears.
2. Right-click on the ThinManager Users branch and choose Add User.

   The ThinManager User Configuration Wizard appears.

Figure 493 - User Branch of the ThinManager Tree

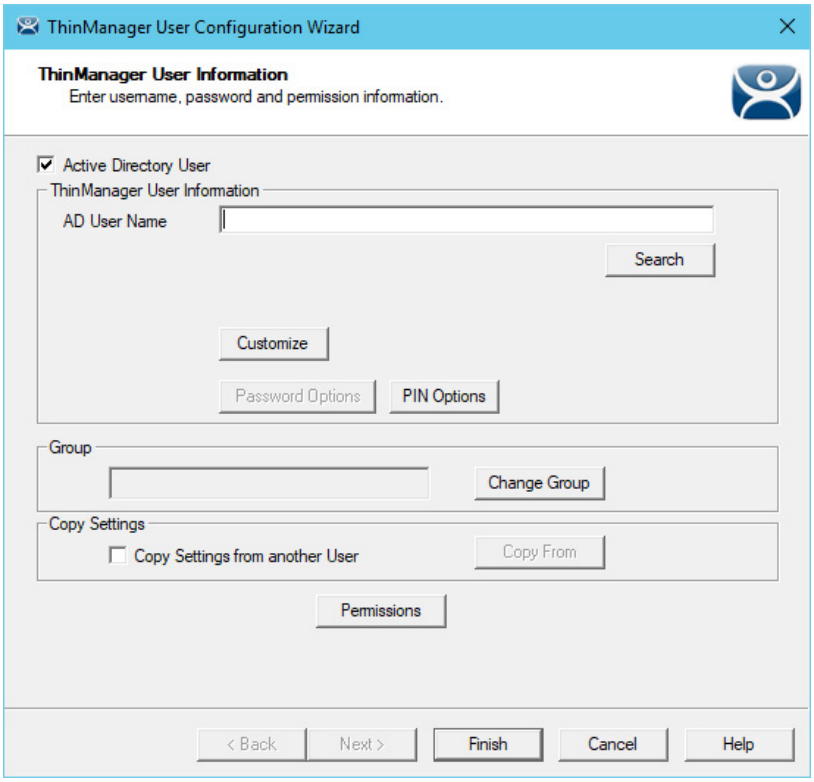


The first page of the ThinManager User Configuration Wizard is the ThinManager User Information page that creates the ThinManager User account.

ThinManager Users that have display clients assigned to them must be tied to a Windows account. If a ThinManager User does not have a display client assigned to it, and it only uses the Permissions to access a display client that belongs to the Terminal, then it does not need a Windows account.

This scenario assigns display clients to the ThinManager User so a valid Windows account is needed.

Figure 494 - ThinManager User Information

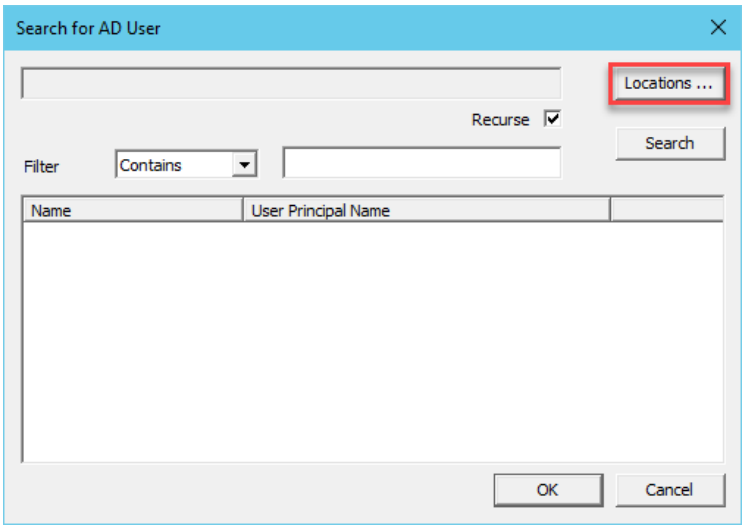


The first page of the ThinManager User Configuration Wizard is the ThinManager User Information page that creates the ThinManager User account.

1. Click Active Directory User, which allows you to draw the user account from the Active Directory.
2. Click Search.

   The Search for AD User dialog box appears, which begins the Active Directory process.

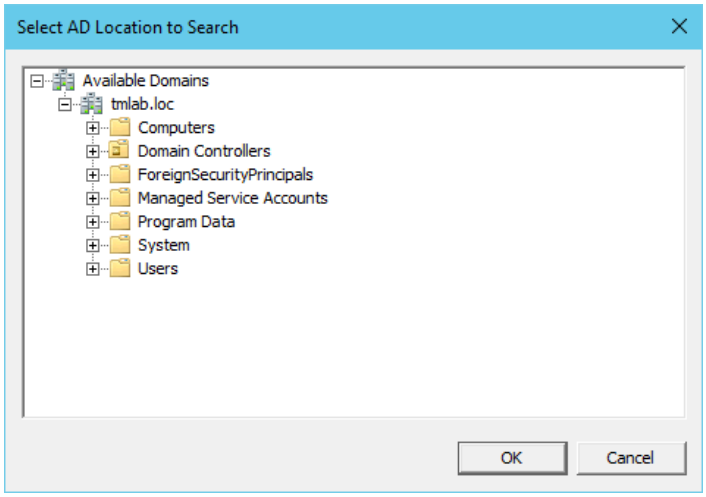
Figure 495 - Search for AD User Dialog Box



3. Click Locations.

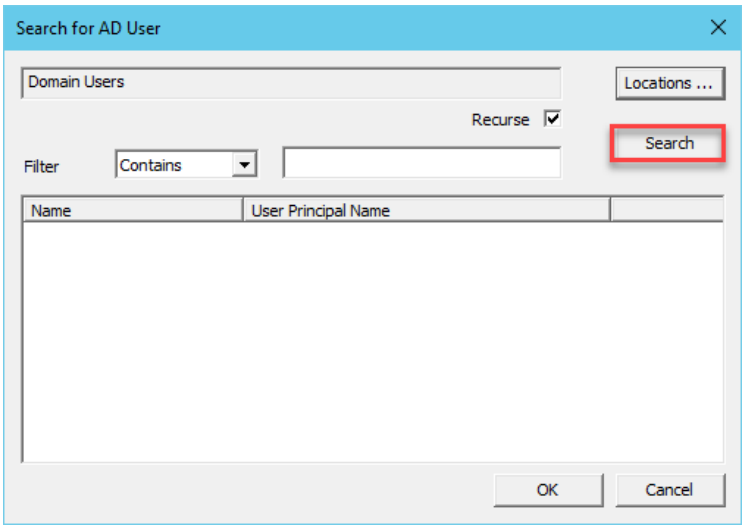
The Select AD Location to Search dialog box appears from which you can choose a location.

Figure 496 - Select AD Location to Search Dialog Box



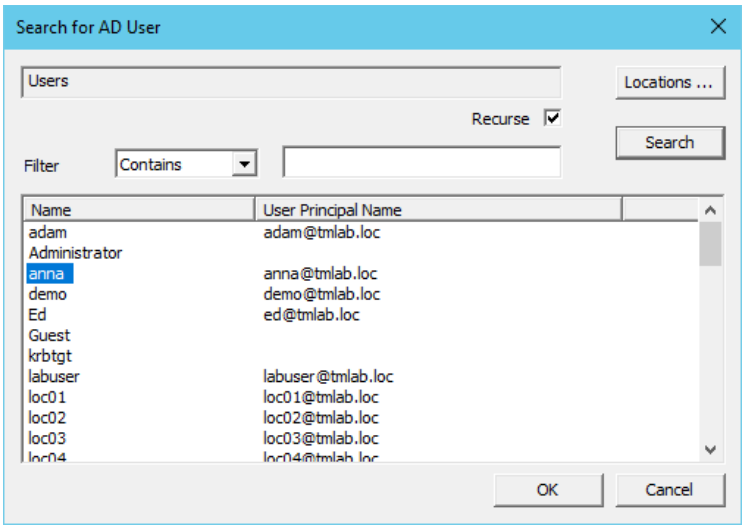
4. Highlight the AD location you want to select the user from and click OK, which populates the location into the Locations field in the Search for AD User dialog box.

Figure 497 - Search for AD User – Location Selected



5. Once the Location has been selected, click Search to populate the user field with users from the highlighted location.

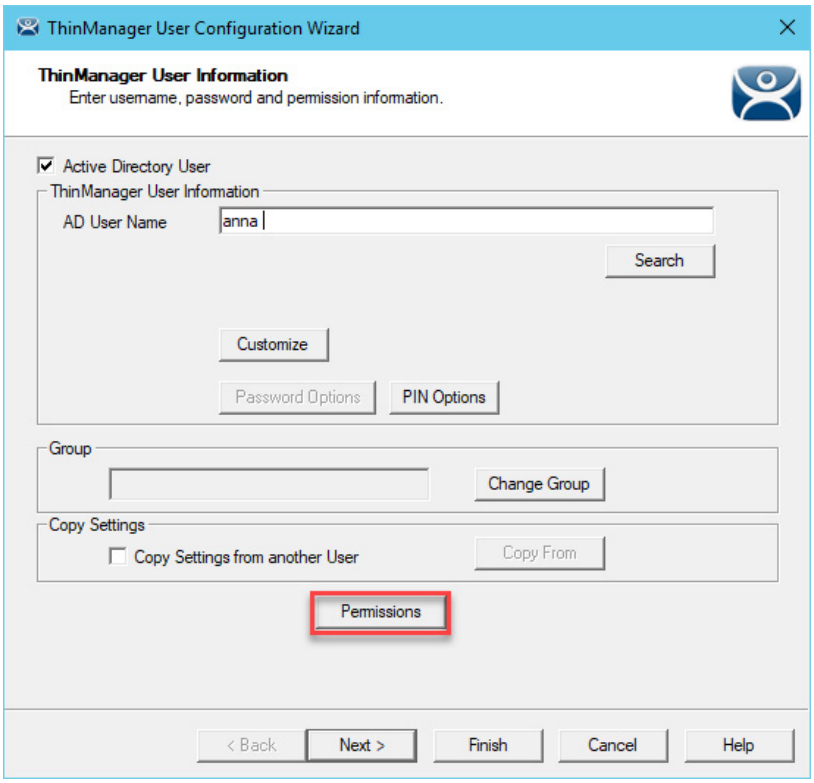
Figure 498 - Search for AD User Dialog Box – Users



6. Highlight the desired user account from the Active Directory members and click OK.

   The user account is populated to the AD User Name field of the ThinManager User Information page. See Figure 499.

Figure 499 - ThinManager User Information



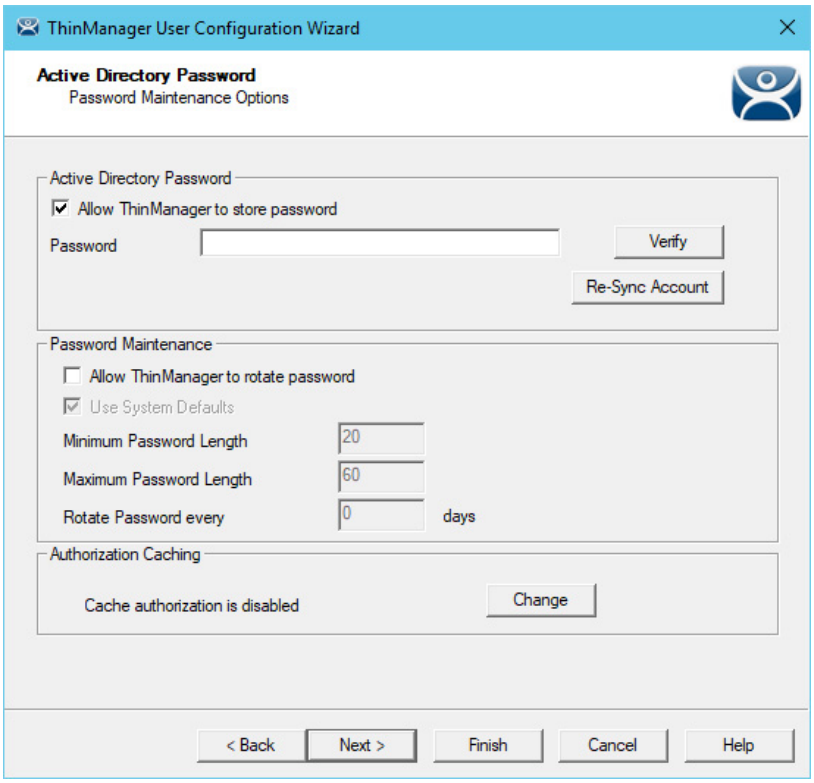
7. Click Permissions to apply membership in Access Groups. See Permission-deployed Applications in ThinManager on page 335.

8. Click Finish if you only need a Permission applied.

Button/Setting	Description
Customize	Launches the User Description dialog box. See ThinManager User Settings for Non-domain Users on page 375.
Password Options	Choose Manage>Active Directory>Settings on the ThinManager menu to configure in the Active Directory System Settings.
Pin Options	Launches the Pin Maintenance Options dialog box. See ThinManager User Settings for Non-domain Users on page 375.
Change Group	Launches the Choose User Group dialog box. See ThinManager User Settings for Non-domain Users on page 375.
Copy Settings from another User	Allows the user to inherit the properties of another user.
Copy From	Opens the Select User dialog box that allow you to select the user from which to inherit properties.

9. Click Next if you want to apply user-specific display clients.

Figure 500 - Active Directory Password Page



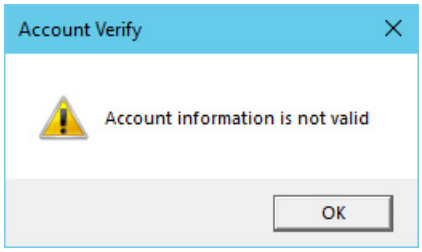
Setting	Description
Active Directory Password	
Allow ThinManager to store password	Allows ThinManager to store the Active Directory password in an encrypted form. Clear the checkbox for ThinManager to require a password each time the session logs on.
Password	Type the password.
Verify	Checks with Active Directory to validate the password.
Re-Sync Account	Sends the typed password to the Active Directory.
Password Maintenance	
Allow ThinManager to rotate password	Check to allow ThinManager to update the Active Directory password per the schedule you set.
Use System Defaults	Uses the system defaults set at Manage>Active Directory>Settings.
Minimum Password Length	Sets the minimum amount of characters the password must contain to be valid.
Maximum Password Length	Sets the maximum amount of characters the password must contain to be valid.
Rotate Password every *n* days	Sets the number of days between scheduled password changes. This setting is propagated from the Password Maintenance Options dialog box when Force User to change password periodically is checked.

If Allow ThinManager to store password is checked, then you can have the Windows password stored in ThinManager, which allows a fingerprint scan to send the Windows password automatically for authentication.

Check Allow ThinManager to store password to use the system defaults, or clear the Use System Defaults checkbox to customize the password settings.

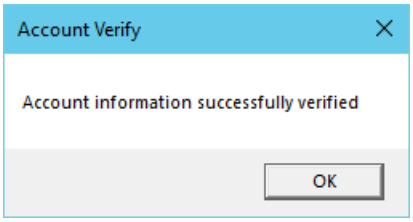
10. Type the user password in the Password field and click Verify to check your password against the Active Directory.
    a. If the password is incorrect, a dialog box appears to indicate account information is not valid.

Figure 501 - Account Verify Dialog - Not Valid



    b. If the password is correct, the dialog box appears to show a positive result.

Figure 502 - Account Verify Dialog - Valid



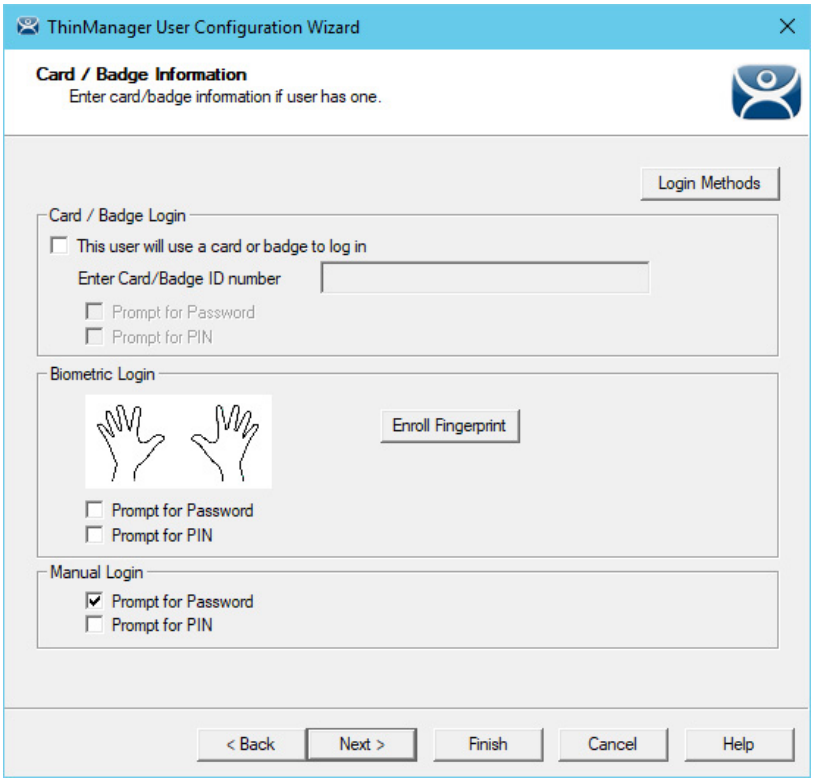
11. Click OK.
12. Click Next on the Active Directory Password page.

    The Card/Badge Information page appears.

ThinManager Configuration Wizard

The next page in the ThinManager User Configuration Wizard is the Card/Badge Information page.

Figure 503 - Card/Badge Information



You can tie a ThinManager User to an 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 406.

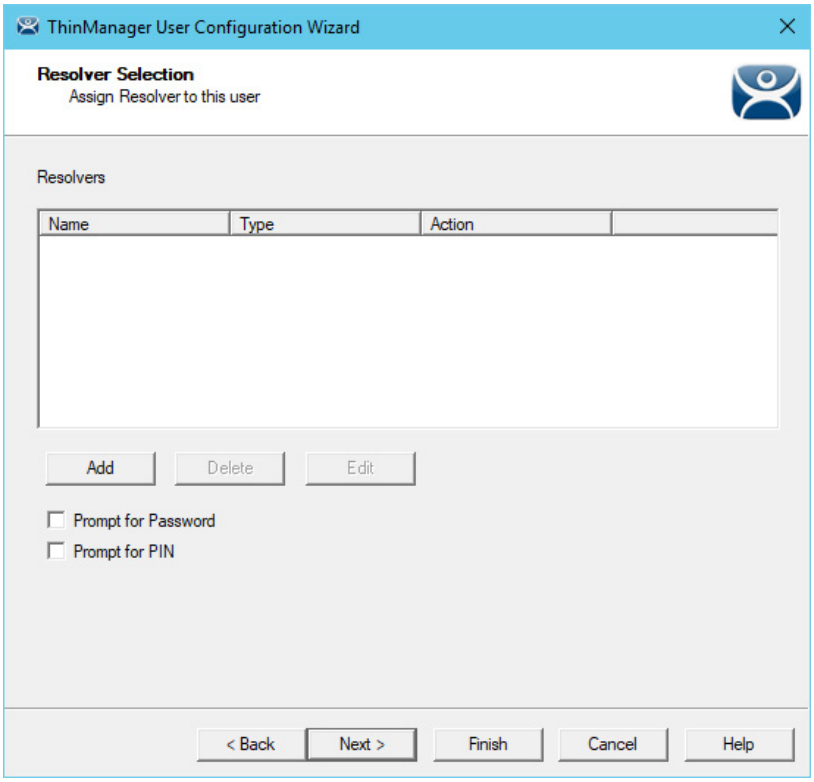
1. Check Prompt for Password or Prompt for Pin, as a secondary credential, for the Card/Badge Login, Biometric Login, or Manual Login.

Setting	Description
Prompt for Password	If checked, requires the user to enter a password.
Prompt for Pin	If checked, requires the user to enter their PIN.

2. Click Next to continue.

   The Resolver Selection page appears.

Figure 504 - Location Resolver



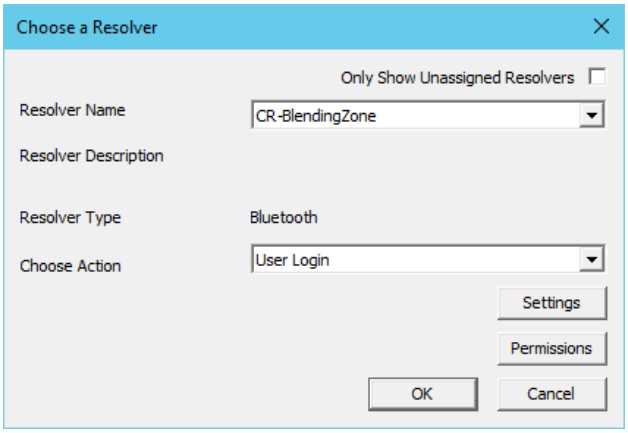
Setting	Description
Prompt for Password	If checked, requires the user to enter a password.
Prompt for Pin	If checked, requires the user to enter their PIN.

ThinManager allows a Resolver to pass the specific user's credentials for a login.

3. Click Add.

   The Choose a Location Services Resolver dialog box appears.

Figure 505 - Choose a Resolver Dialog



4. Choose the resolver from the Resolver Name pull-down menu.
5. Choose User Login from the Choose Action pull-down menu.
6. Click OK to apply the resolver.

The user logs in when the resolver is activated.

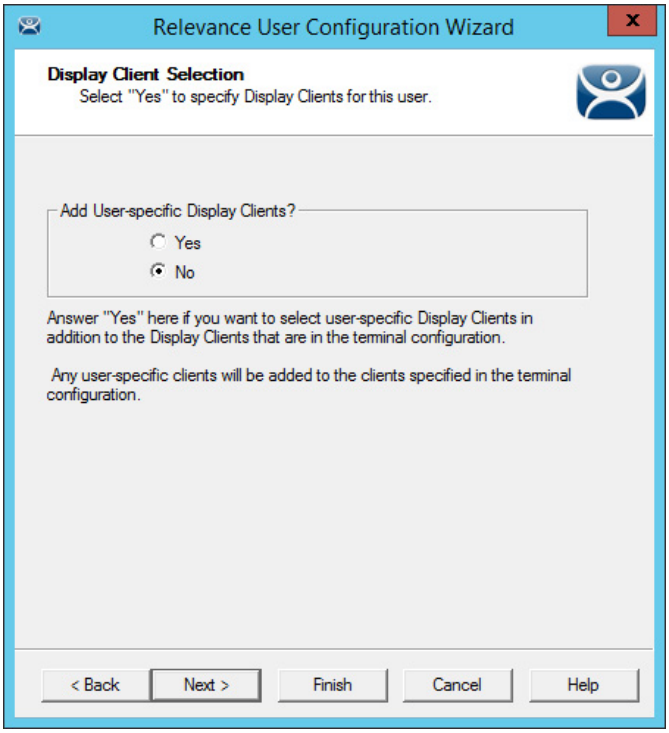
7. Click Next to continue.

The Display Client Selection page appears.

Add User-specific Display Clients

Roaming applications require that display clients are assigned to individuals.

Figure 506 - Display Client Selection Page

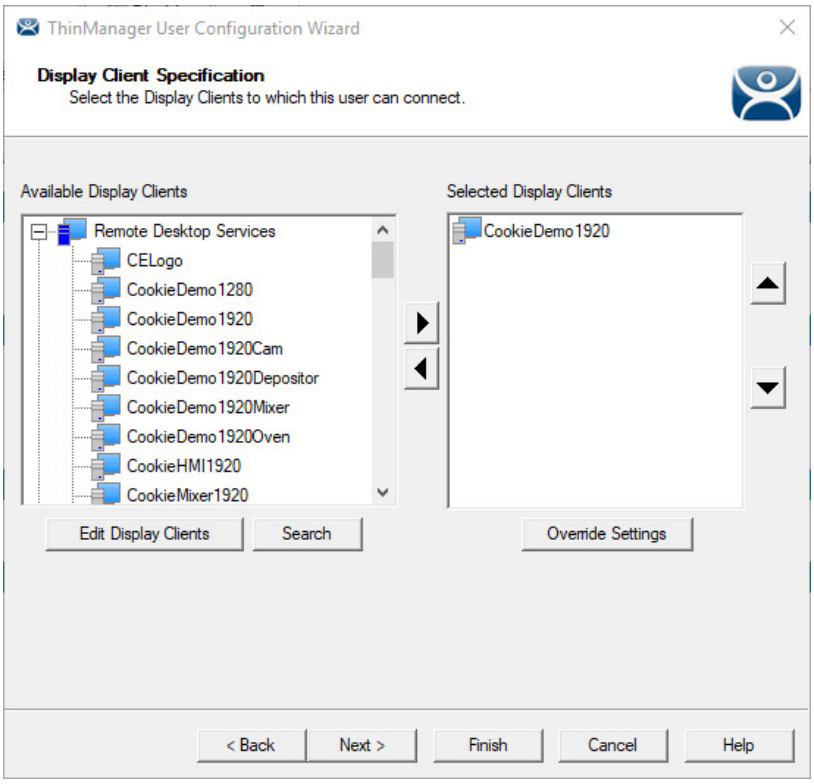


The Display Client Selection page has one setting, Add User-specific Display Clients?

Setting	Description
Yes	User can be assigned display client of their own that they can access from any Terminal that has Location Services enabled. You can also assign the user Permissions to let them access hidden applications.
No	User is able to access display clients that belong to the Terminal they log in to only. Use with Permissions to grant access to applications hidden with Access Group Permissions.

8. Click Next to continue.

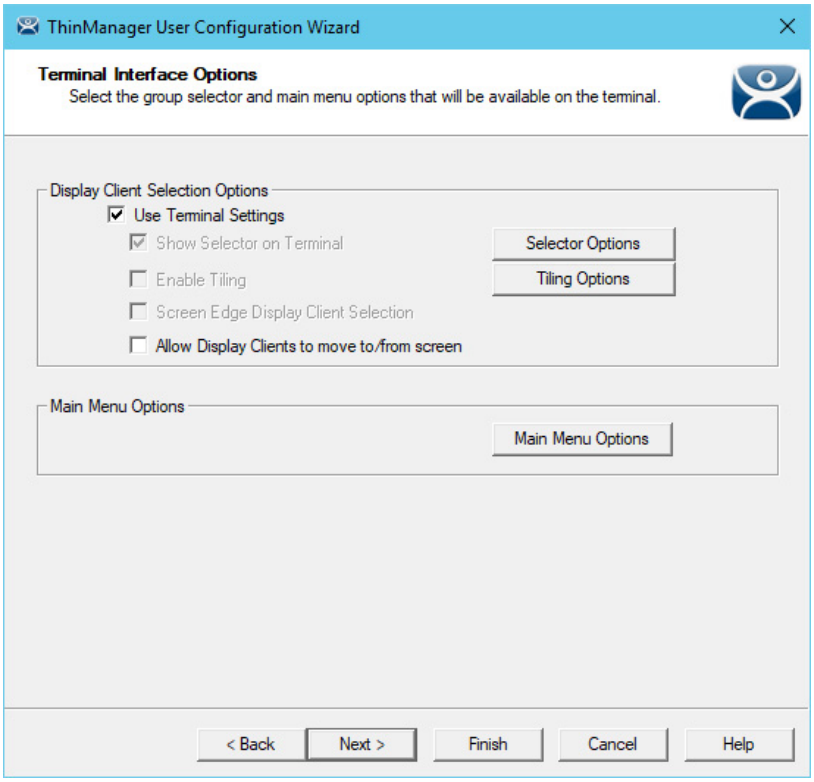
Figure 507 - Display Client Specification Page



The Display Client Specification page allows Display Clients to be assigned to the ThinManager User if Add User-specific Display Clients is set to Yes.

9. Move a Display Client that you want the ThinManager User to use from the Available Display Clients list to the Selected Display Clients list. Use the Right Arrow to move a highlighted Display Client, or double-click a display client to move it.
10. To add a new Display Client, click Edit Display Clients to launch the Display Client Wizard. See Remote Desktop Services Display Clients on page 133 for details.
11. Click Next to continue.

Figure 508 - Terminal Interface Options



The Terminal Interface Options page sets the menus and hotkeys for the ThinManager User so a Terminal using MultiSession needs to have a method to switch between sessions. This is similar to the page in the Terminal Configuration Wizard.

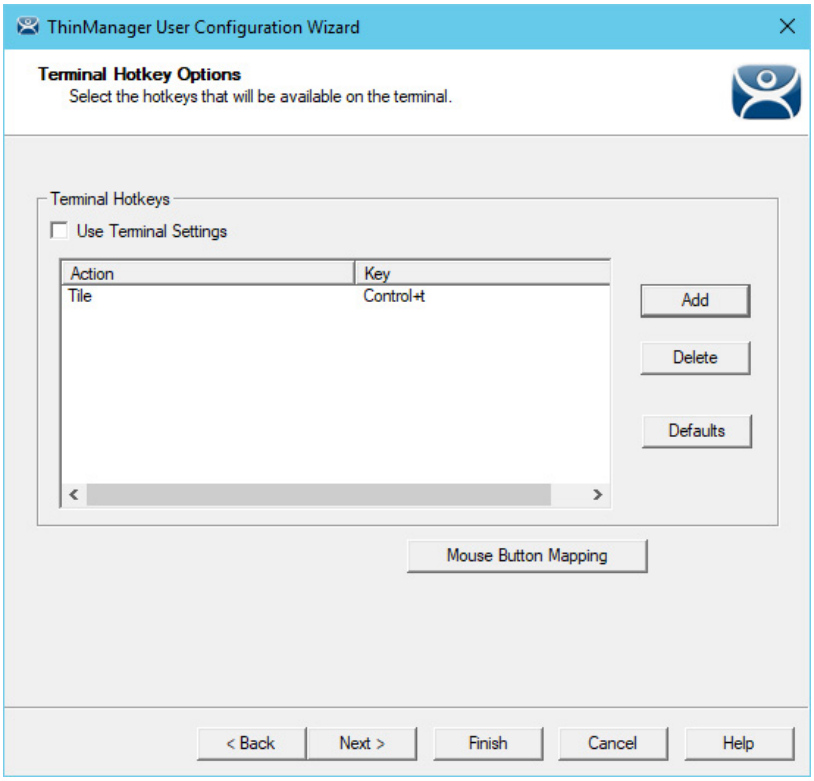
Group Selector Options allow on-screen switching of sessions.

Setting	Description
Use Terminal Settings	Check to let the ThinManager User inherit the properties that are configured for use with the Terminal.
Show Group Selector on Terminal	Check to display an on-screen pull-down menu that can be activated by mouse.
Enable Tiling	Check to allow the sessions to be tiled so that the user can make a visual selection of the desired selection.
Screen Edge Group Selection	Check to activate a feature that switches windows if the mouse is moved off screen.
Allow Display Clients to move to/from screen	Check to give the user the ability to move display clients from screen to screen.
Selector Options	Launches the Group Selector Options dialog box.
Tiling Options	Launches the Tile Options dialog box.
Main Menu Options	Launches the Main Menu Options dialog box, which allows configuration of the Relevance Main Menu.

12. Select the Next button to continue.

    The Terminal Hotkey Options page appears.

Figure 509 - Terminal Hotkey Options



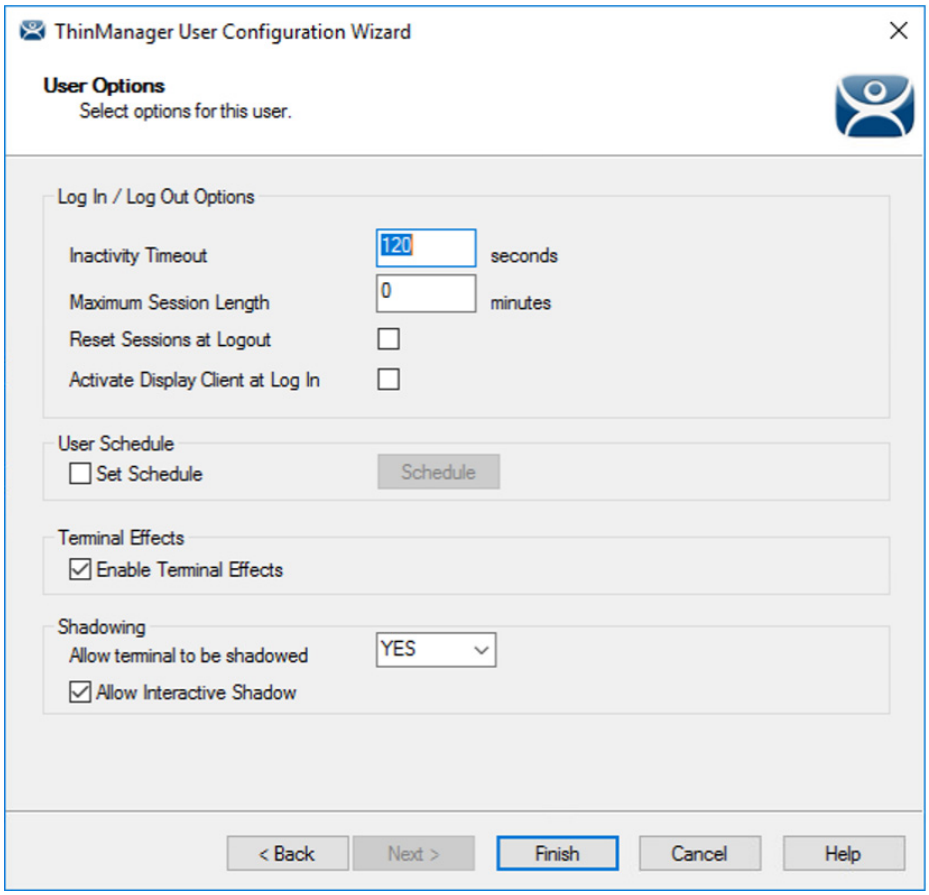
Terminal Hotkeys on the Terminal Hotkey Options page allows the selection of keyboard combinations that allow switching between sessions. This is similar to the page in the Terminal Configuration Wizard.

Setting	Description
Use Terminal Settings	Check to let the ThinManager User inherit the properties that were configured for use with the Terminal. Clear the checkbox to let the user receive the settings as configured for them.
Mouse Button Mapping	Click to open the Mouse Button Mapping dialog box, which allows functions to be assigned to mouse buttons. See Figure 286 on page 212.

13. Click Next to continue.

    The User Options page appears.

Figure 510 - User Options



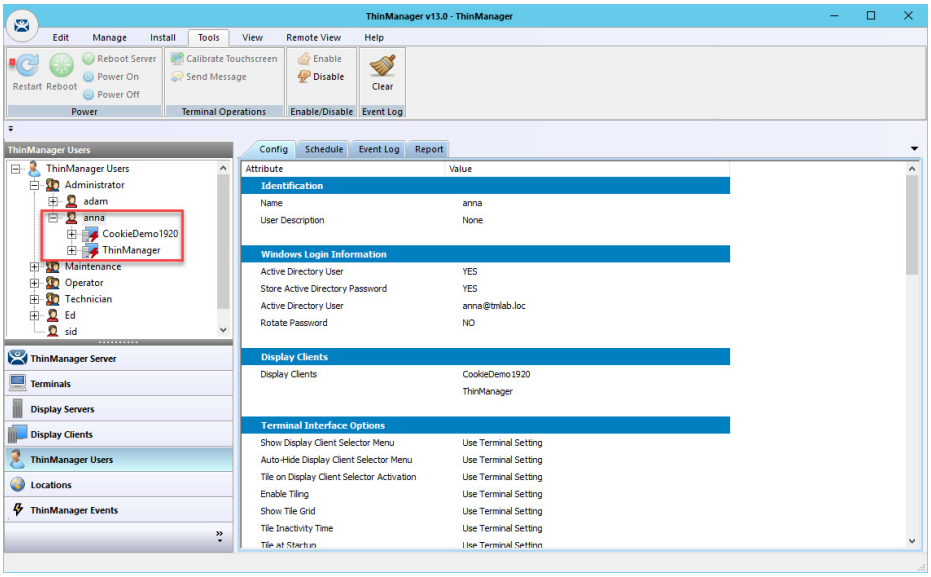
The User Options page has a few options for the user experience.

Setting	Description
Log In/Log Out Options	
Inactivity Timeout	Location Services logs a ThinManager User off of the Terminal after this much inactive time has passed.
Maximum Session Length	Input desired length of time for user to stay logged in to a session before an automatic timeout.
Reset Sessions at Logout	Check to log off a session when the ThinManager User logs off.
Activate User Group at Log In	Check to display the ThinManager User's first Display Client when the user logs in to the Terminal.
User Schedule	
Set Schedule	Check to enable Schedule.
Schedule	Click to launch the Event Schedule dialog box and allow a schedule to be created for Terminal events.
Terminal Effects	
Enable Terminal Effects	Check to allow the use of Terminal Effects, which currently includes sliding Windows and message rollups.
Shadowing	
Allow Terminal to be shadowed	Allows the configuration of these Shadowing Options. • No - Prevents the ThinManager Users from being shadowed. • Ask - Displays a message dialog box that prompts for a positive response before the shadow is allowed. • Warn - Displays a message dialog box, which alerts the Terminal that it is to be shadowed, but does not require a positive response before the shadow is allowed. • Yes - Allows shadow to occur without warning or recipient input.
Allow Interactive Shadow	Allows members with Interactive Shadow privileges to shadow this ThinManager User. Click the Shadow tab on the Details pane to initiate the shadow. Clear this checkbox to prevent shadowing from within ThinManager.

14. Click Finish to complete the configuration.

    The ThinManager User tree shows the display clients assigned to the user.

Figure 511 - ThinManager User with User-Specific Display Clients



Log On with a ThinManager User Account

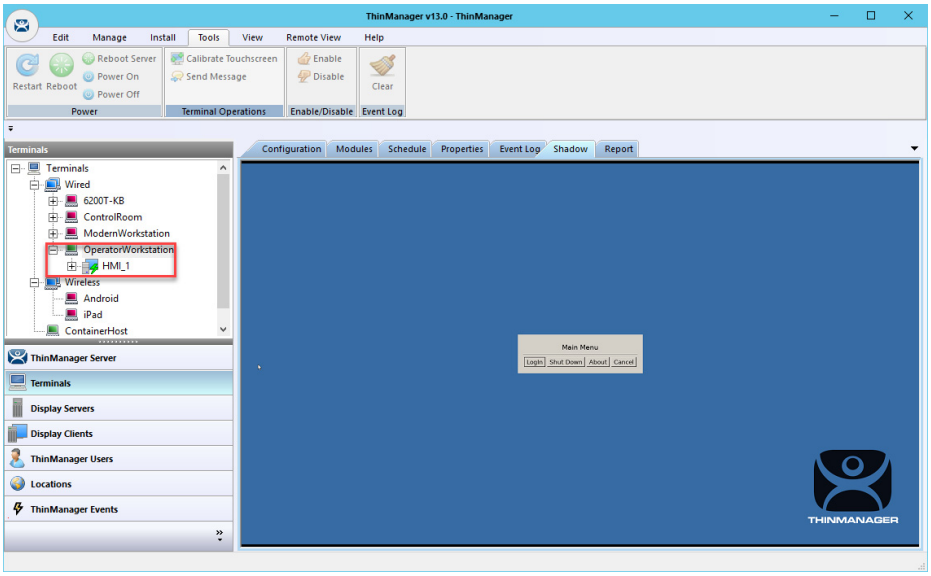
To log in a ThinManager User on a Terminal, go to a Terminal that has Enable Location Services checked on the Terminal Mode Specification page.

Follow these instructions to log in.

1. Open the display client selector pull-down menu and choose Main Menu.
2. Press CTRL+m to launch the Main Menu if the hotkey was checked.

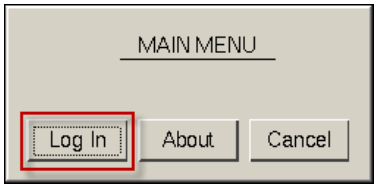
   The Main Menu is displayed on the Terminal.

Figure 512 - ThinManager Console with a Single Display Client on Terminal



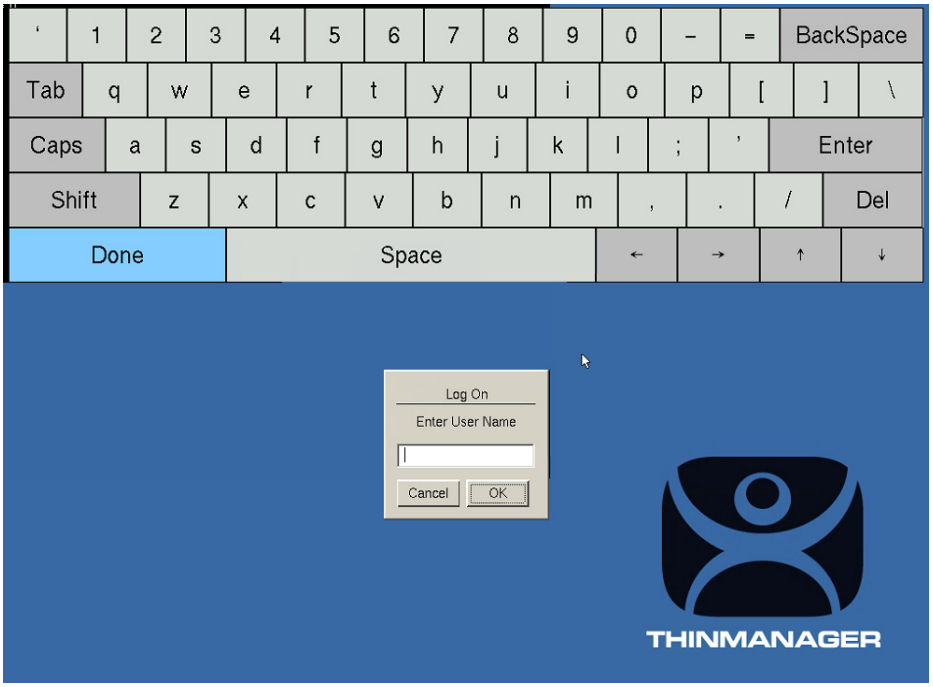
The Terminal tree shows the Terminals and display clients assigned to the Terminals.

Figure 513 - Location Services Main Menu



3. Click Log In on the Main Menu dialog box.

Figure 514 - Location Services Log On Screen with Virtual Keyboard



A virtual keyboard is displayed if Show Virtual Keyboard was checked on the Main Menu Options dialog box when you configured the Terminal for Location Services on the Terminal Interface Options page. See Figure 477 on page 346.

Figure 515 - Location Services Log On Dialog Box

4. Type your ThinManager User Name and click OK.

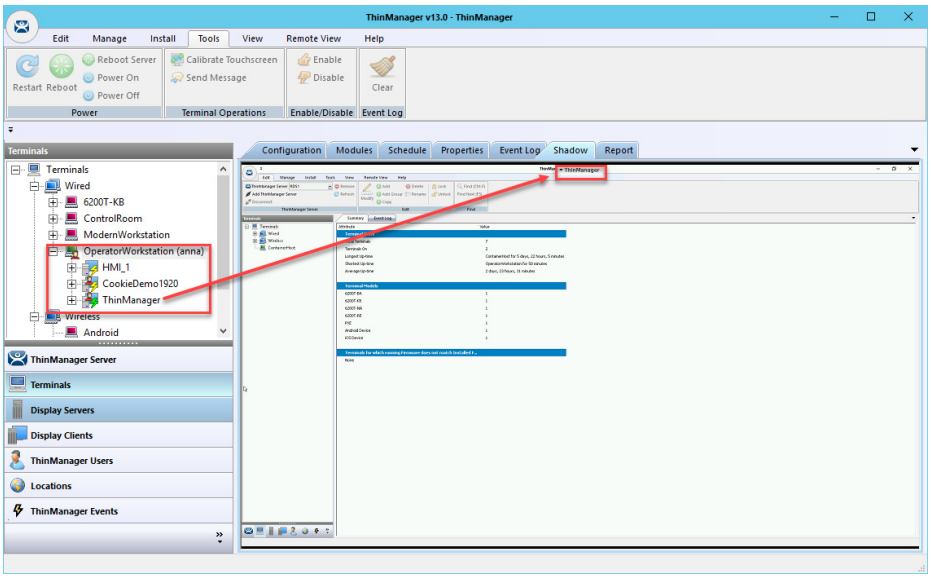
   The Password Dialog box appears.

Figure 516 - Password Dialog

5. Type the password and click OK.

   If the user has valid Windows credentials, the user is logged in.

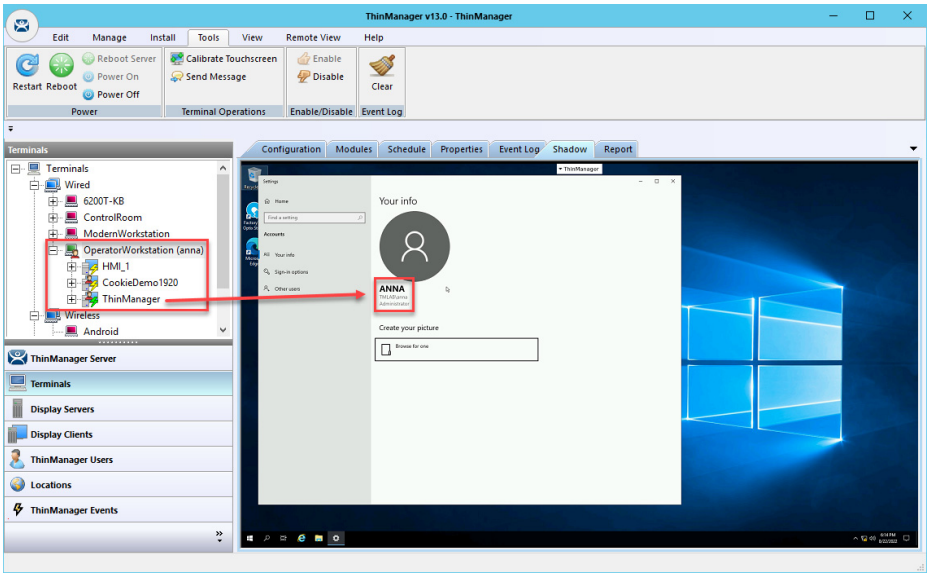
Figure 517 - ThinManager User Logged On



The Terminal displays the name of the ThinManager User in parentheses. Figure 517 shows Anna logged in to the Terminal.

The group selector on the Terminal shows the ThinManager User's display client in the pull-down menu selector. Now, the lightning bolt icon shows a connection.

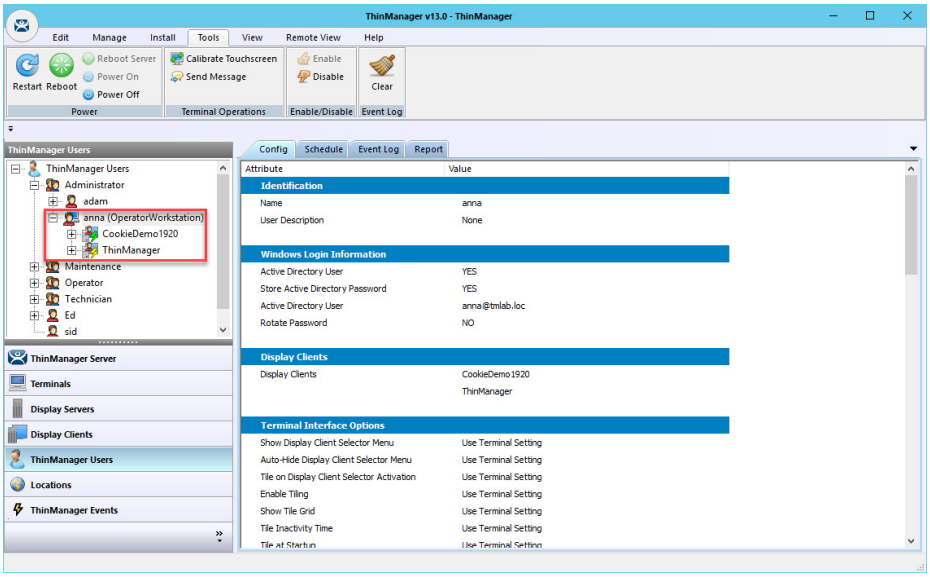
Figure 518 - ThinManager User Logged On



When a ThinManager User logs off from a Terminal, the sessions disconnect by default and remain in an idle state on the Remote Desktop Servers.

If the ThinManager User logs in from another Terminal, then Location Services connects the user to their session, and the sessions are displayed at the new Terminal.

Figure 519 - ThinManager User Tree



The ThinManager Users tree lists the users.

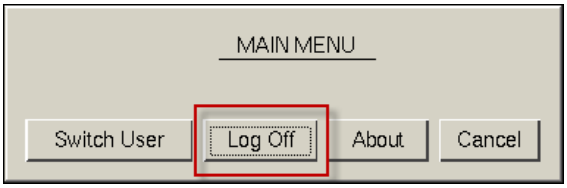
A user that is logged in to a terminal with Location Services shows a different icon as well as the name of the terminal. Adam Brown is logged in to 3_Terminal in Figure 519.

Log Out of Location Services

The ThinManager User can be logged out by one of these methods.

- Open the Location Services Main Menu on the Terminal and click Log Off.
- Right-click on the ThinManager User in the ThinManager tree and choose Logoff User.
- Restart or reboot the Terminal that has a ThinManager User logged in.
- The Inactivity Timeout set on the User Options page is reached.

Figure 520 - Main Menu

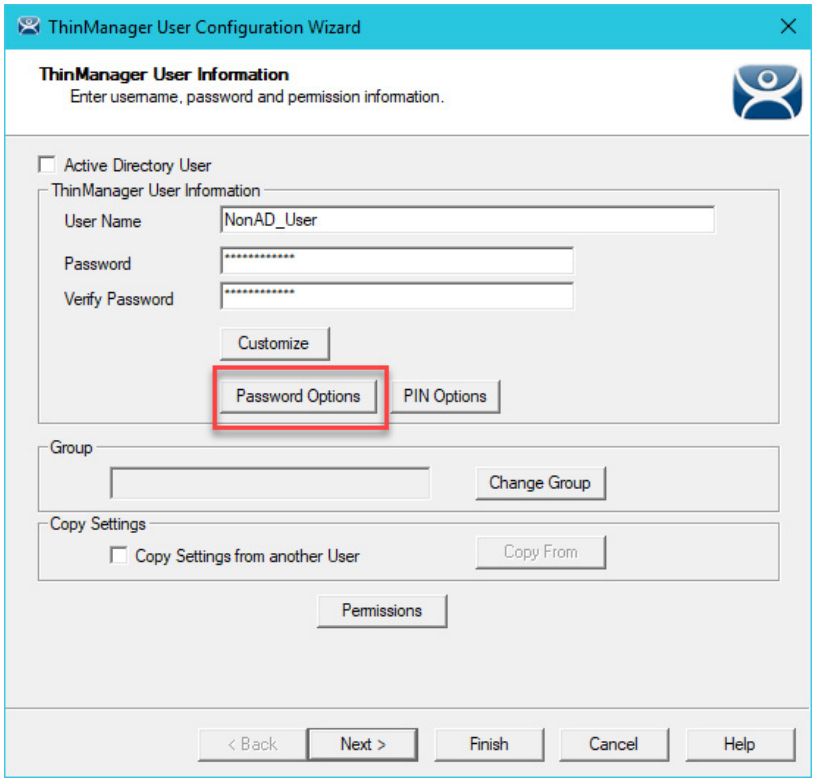


Setting	Description
Switch User	Click to log off the ThinManager User and disconnect any sessions from Display Clients assigned to the user. The Log On dialog box for another ThinManager User appears.
Log Off	Click to log off the ThinManager User and any sessions from Display Clients assigned to the user and return to the Terminal's display.

Roaming Applications for Non-domain Users

Each ThinManager User who has their own display client assigned must be tied to a Windows User account. When a user is created from the Active Directory, the ThinManager User account is the Windows user account. When you create a ThinManager User who is not from the domain, you have a few options to assign the Windows account.

Figure 521 - Non-Active Directory ThinManager User



Clear the Active Directory User checkbox to create a ThinManager User who is not in the Active Directory.

Button	Description
Customize	Click to launch the User Description dialog box.
Password Options	Click to launch the Password Maintenance Options dialog box.
PIN Options	Click to launch the PIN Maintenance Options dialog box.
Change Group	Click to launch the Choose User Group dialog box.
Permissions	Click to launch the Permissions dialog box.

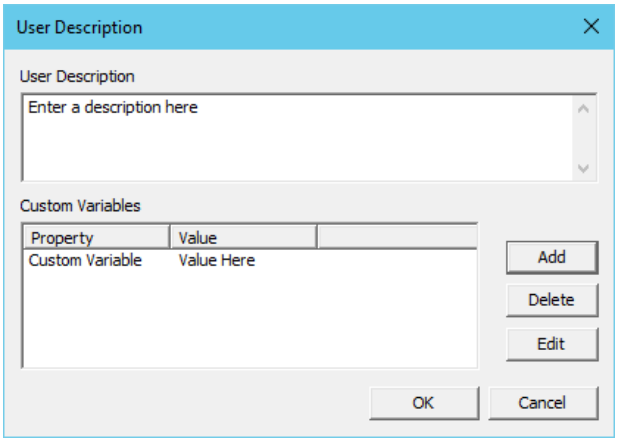
ThinManager User Settings for Non-domain Users

In Figure 521, the ThinManager User Information page has several buttons that configure user settings.

1. Click the Customize button.

   The User Description dialog box appears, which allows a verbose description to be associated with the user account that is displayed in the Configuration detail pane.

Figure 522 - User Description Dialog Box



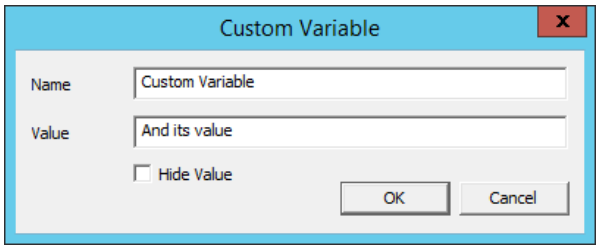
Setting	Description
User Description	Allows you to type a verbose description to be added to the user account.
Add	Click to open the Custom Variables dialog box.

Custom variables allow for the creation of a single display client 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, which allows one display client to do the work of many.

2. Click Add.

   The Custom Variable dialog box appears, which allows you to add a custom variable. A custom variable can be used to pass information to the AppLink display client or to the TermMon ActiveX that you embed in your application.

Figure 523 - Custom Variable Dialog Box

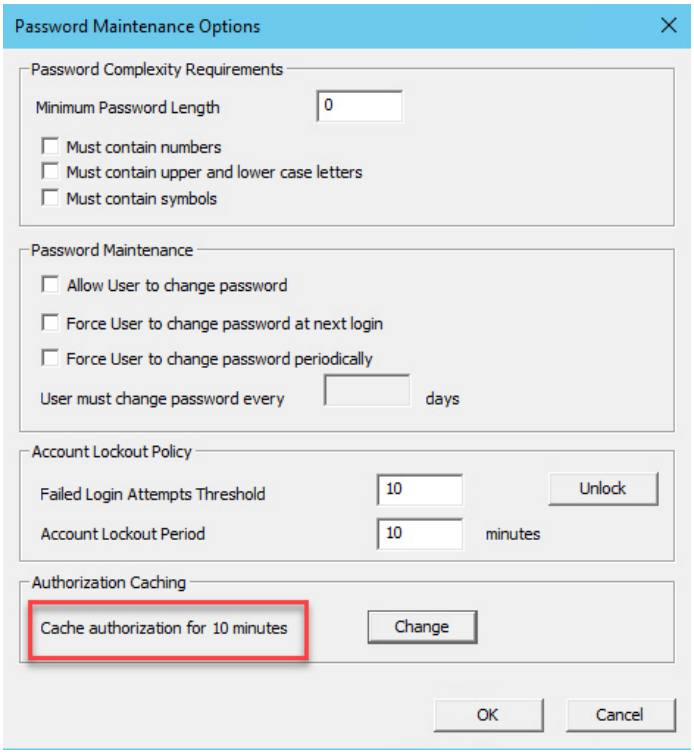


Setting	Description
Name	Type the name of the custom variable.
Value	Type the value or content to be assigned to the custom variable.
Hide Value	Check to obscure the custom variable value. Clear this checkbox to show the value.

3. On the ThinManager User Information page, click Password Options.

   The Password Maintenance Options dialog box appears.

Figure 524 - Password Maintenance Options



The Password Maintenance Options dialog box allows user password configuration.

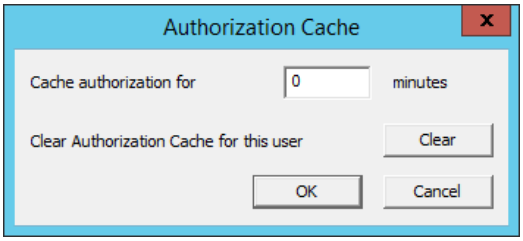
Setting	Description
Password Complexity Requirements	
Minimum Password Length	Type the length requirement.
Must contain numbers	Check to add the number requirement to the password.
Must contain symbols	Check to add the symbol requirement to the password.
Must contain upper and lower case letters	Check to add the mixed-case requirement to the password.
Password Maintenance	
Allow User to change password	Check to allow a user to change the password. Clear the checkbox to prevent a password change by the user.

Setting	Description
Force User to change password at next login	Check to prompt the user to change their password at the next login.
Force User to change password periodically	Check to 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	Type the interval for password changes.
Authorization Caching	
Change	Click to open the Authorization Cache dialog box.

4. Click Change.

   The Authorization Cache dialog box appears.

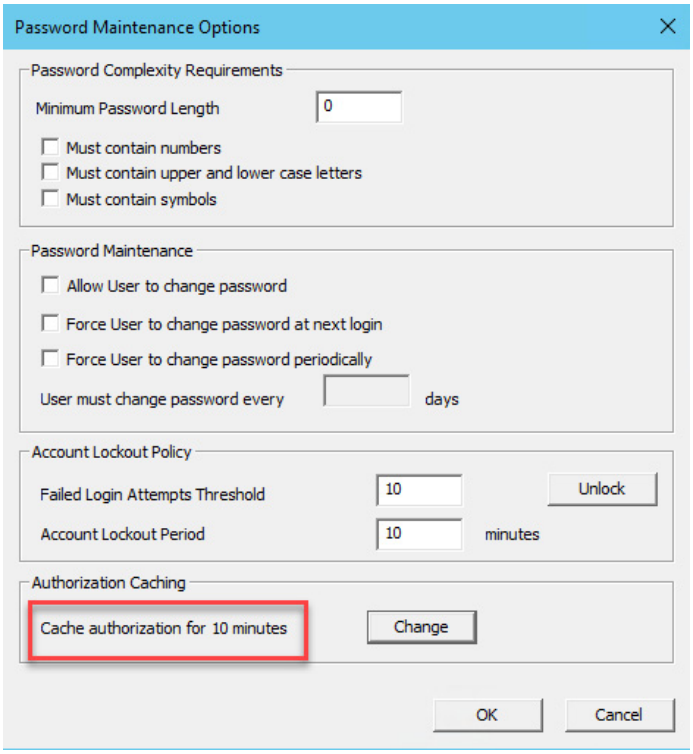
Figure 525 - Authorization Cache Dialog Box



Setting	Description
Cache Authorization for _ minutes	Type the time interval for which the password to be cached. A user enters their password once, and it is cached and provided for the duration.
Clear	Click to remove cache authorization for the user and require the user to enter a password.

When a user has a cached password, the Password Maintenance Options dialog box appears with the cache interval indicated.

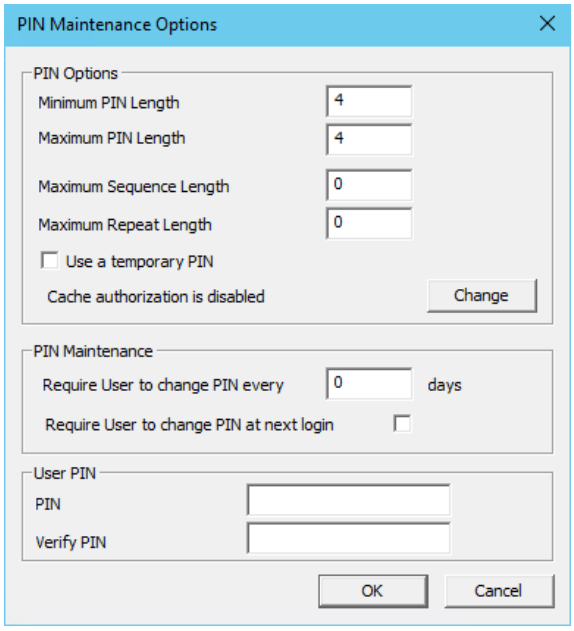
Figure 526 - Password Maintenance Options



5. On the ThinManager User Information page, click PIN Options. See Figure 521 on page 374.

The PIN Maintenance Options dialog box appears, which allows the configuration of a Personal Identification Number, or PIN.

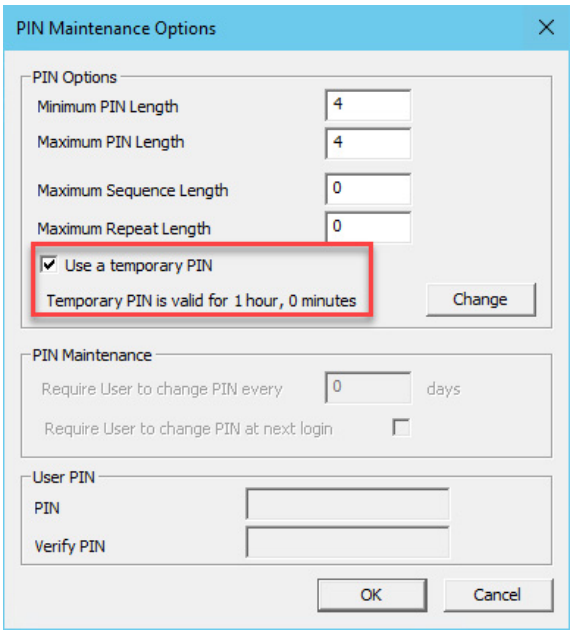
Figure 527 - PIN Maintenance Options



Setting	Description
PIN Options	
Minimum PIN Length	Type the minimum length requirement for the PIN.
Maximum PIN Length	Type the maximum length requirement for the PIN.
Maximum Sequence Length	Type the maximum length allowed for the creation of the PIN.
Maximum Repeat Length	Type the maximum number of times a digit can be repeated in the creation of a PIN.
Use a temporary PIN	Check to allow use of a PIN for the duration set in the Authorization Cache dialog box, which is launched when Change is clicked on the Password Maintenance Options dialog box. See Figure 526.
Change	Click to toggle cache authorization between enabled and disabled.
PIN Maintenance	
Require User to change Pin every __ days	Type the frequency with which the PIN needs set.
Require User to change pin at next login	Check to require the user to create a new PIN the next time they login.
User PIN	
PIN	Type the PIN.
Verify PIN	Type confirmation of the PIN.

The PIN Maintenance Options dialog displays the amount of time for which the Temporary PIN is valid.

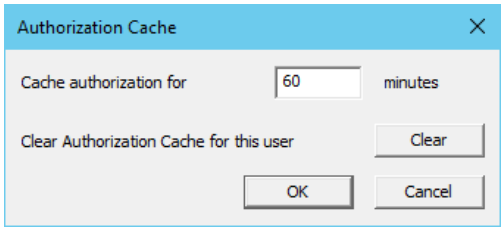
Figure 528 - PIN Maintenance Options



6. Click Change.

The Authorization Cache dialog box appears, where you can set the duration the Temporary Pin.

Figure 529 - Authorization Cache Dialog Box

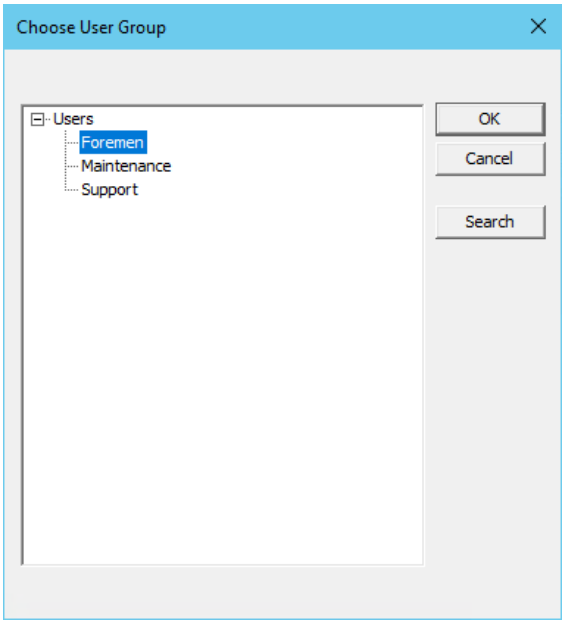


7. Type the Cache authorization duration or click Clear to clear Authorization Cache.

8. On the ThinManager User Information page, click Change Group. See Figure 521 on page 374.

   The Choose User Group dialog box appears, which allows you to select the ThinManager User group in which to nest the user.

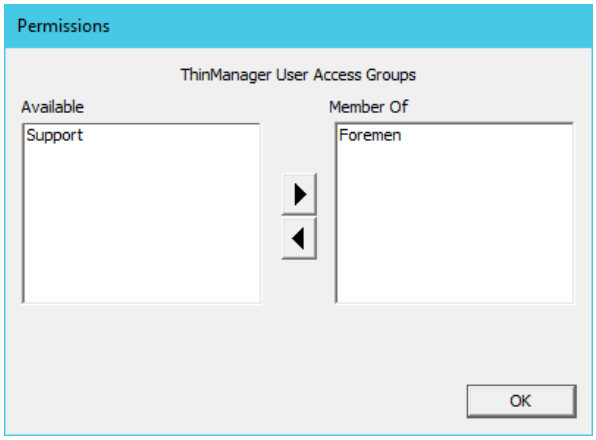
Figure 530 - Choose User Group



9. On the User Information page, click Permissions. See Figure 521 on page 374.

   The Permissions dialog box appear.

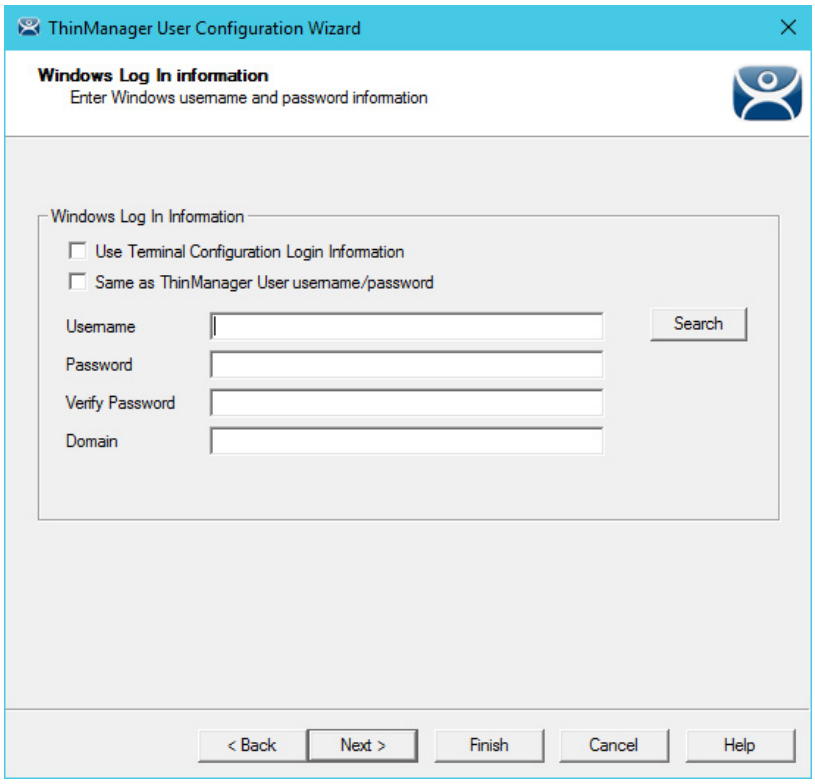
Figure 531 - Permissions Dialog Box



The user can be granted permissions by moving the desired Access Group from the Available list to the Member Of column.

The ThinManager User Configuration Wizard is the same until the Windows Log In information page.

Figure 532 - Windows Log In Information Page



If you chose to assign a display client to the user by selection of the User-specific Display Clients on the Display Client Selection page (see Figure 506 on page 365), then you must provide a Windows account to start the session.

This page is not displayed if the ThinManager User is selected from the Active Directory.

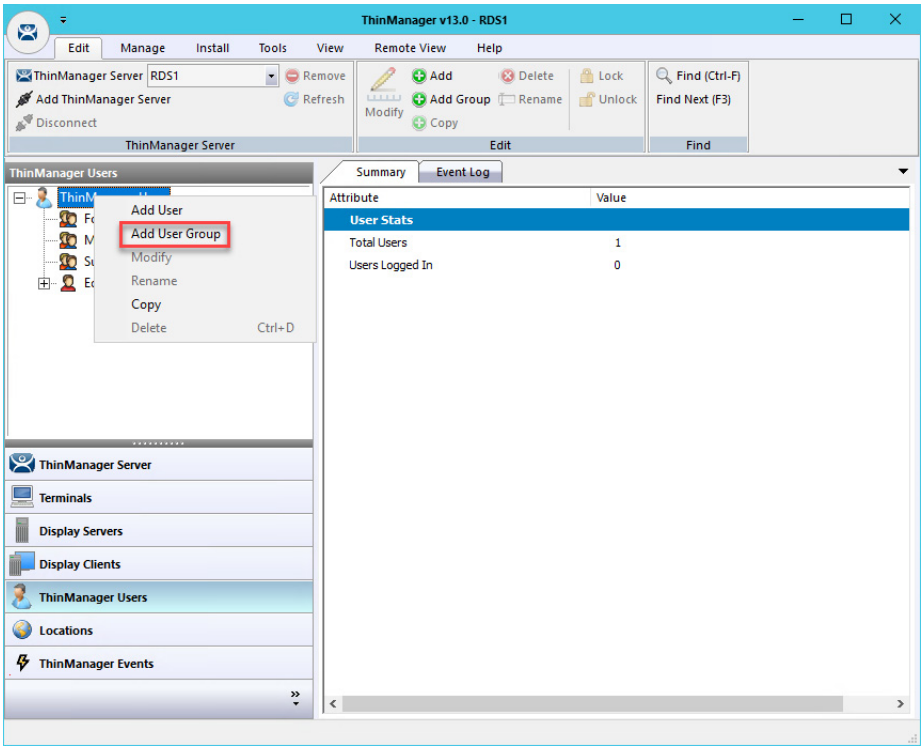
The Windows Log In Information page provides four session log on options.

Setting	Description
Use Terminal Configuration Login Information	Check to use the Terminal's username and password to log on the ThinManager User automatically to the Remote Desktop Server. Since a different account is used at each Terminal, this does not keep a consistent session for the ThinManager User.
Same as ThinManager User username/ password	Check to use the ThinManager User's username and password to log on to the Remote Desktop Server automatically. The ThinManager User username and password must match a Windows User username and password to get authenticated by Windows. If the ThinManager User is selected from the Active Directory, then this is the default behavior.
Use the Username, Password, Verify Password, and Domain fields	The ThinManager User can use an alias username and password to log on to the Remote Desktop Server automatically, which allows you to tie the ThinManager User account to a different Windows account. This allows you to hide the actual Windows account from the user.
Blank Username and Password fields	The ThinManager User can be required to log on to the Remote Desktop Servers manually. To do this, clear the checkboxes and leave the Username, Password, and Domain fields empty. When a ThinManager User logs in with their ThinManager account, they are prompted to enter a valid Windows account and password.

ThinManager User Groups

ThinManager Users can be organized into ThinManager User Groups, just as Terminals can be organized into Terminal Groups. This section shows the configuration of a ThinManager User Group.

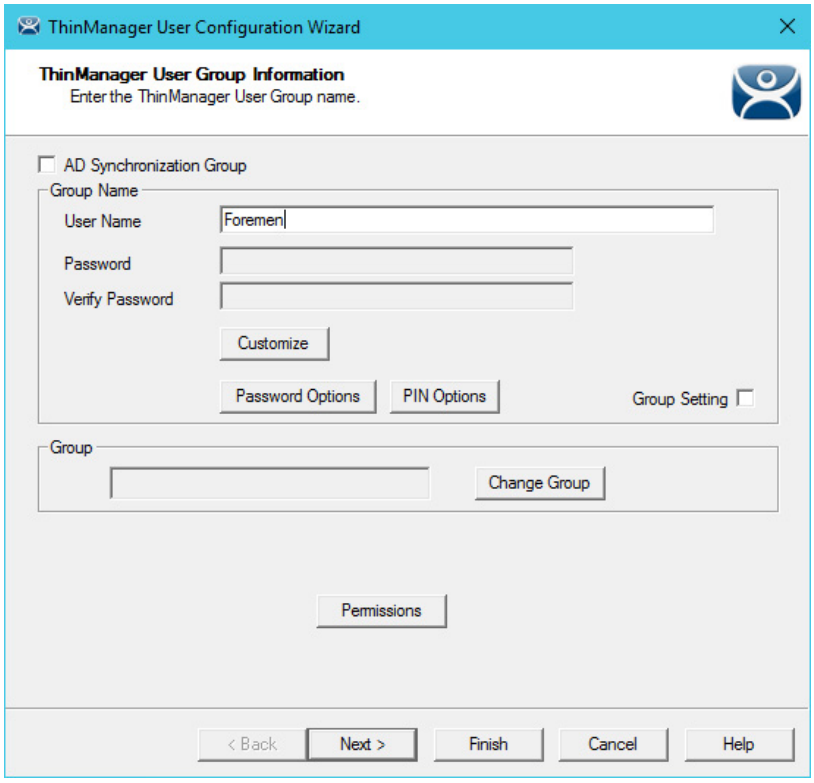
Figure 533 - Add User Group Command



1. Click ThinManager Users at the bottom-left of the ThinManager tree, right-click on the ThinManager Users branch of the tree, and choose Add User Group.

   The ThinManager User Group Information page of the ThinManager User Configuration Wizard appears.

Figure 534 - ThinManager User Group Information Page



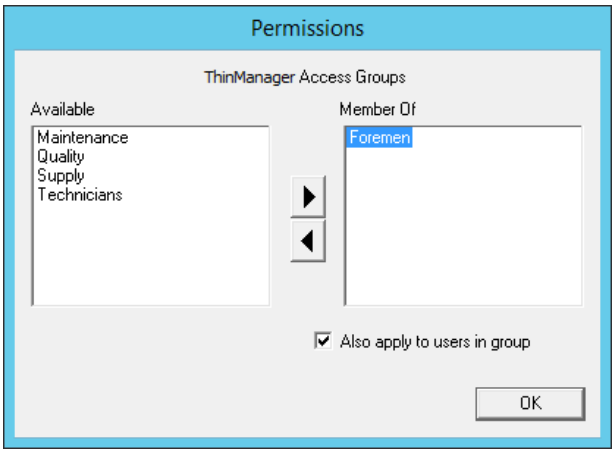
Setting	Description
AD Synchronization Group	Check to access the AD Security Group field.
AD Security Group	Type the name of the Organization Unit to which a user belongs.
Search	Click to select a Security Group to Synchronize.
User Name	Type the user name of your user's login. It can be a unique ThinManager user name, a Windows user name, or one listed in Active Directory.
Password	Type the password for the user. If you are using a Windows account for the ThinManager User, you should use the actual Windows password for automatic login, or leave this field blank for a manual login. If the ThinManager User account is an alias for a Windows account, the password is used as the Location Services password and not the Windows password.
Customize	Click to launch the User Description dialog box and allow custom variables to be applied to the ThinManager User.
Password Options	Click to launch the Password Maintenance Options dialog box, where you can specify password length, complexity, and longevity.
PIN Options	Click to launch the PIN Maintenance Options dialog box, where you can specify the Personal Identification Number length, complexity, and longevity.
Group Setting	Check to apply the setting to all members of the group.
Change Group	Click to launch the Choose User Group dialog box, which allows you to assign the user to a group.
Permissions	Click to apply permissions to the group.

Active Directory Integration allows a Location Services Group to be formed and populated straight from the Active Directory. See Batch Create ThinManager Users using Active Directory OU on page 389.

2. Click Permissions.

   The Permissions dialog box appears.

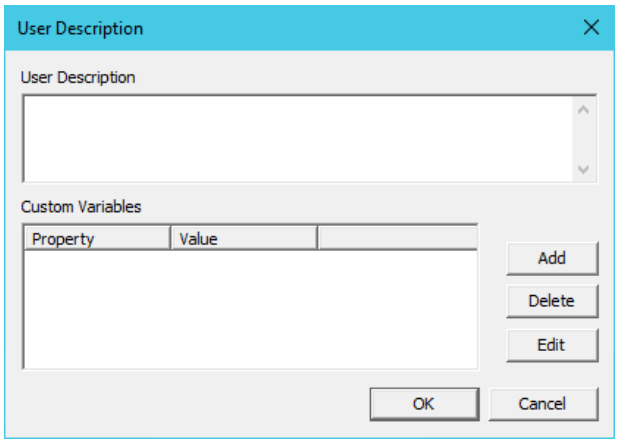
Figure 535 - Permissions Dialog Box



3. Highlight the desired permission in the Available list and click the right-facing arrow to move it to the Member Of list.
4. Highlight the group and check Also apply to users in group, which applies the permission to all group members.
5. Click OK to close and apply.
6. On the ThinManager User Group Information page, click Customize.

   The User Description dialog box appears, which allows a verbose description to be associated with the user account. The description is displayed in the Configuration detail pane.

Figure 536 - User Description Dialog Box

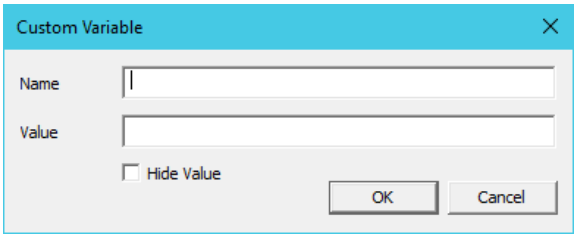


Setting	Description
User Description	Type a description, which is added to the user account. The text field allows a verbose description.
Add	Click to launch the Custom Variable dialog box to add a custom variable.

Custom variables allow a single display client to 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, which allows one display client to do the work of many.

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

Figure 537 - Custom Variable Dialog Box

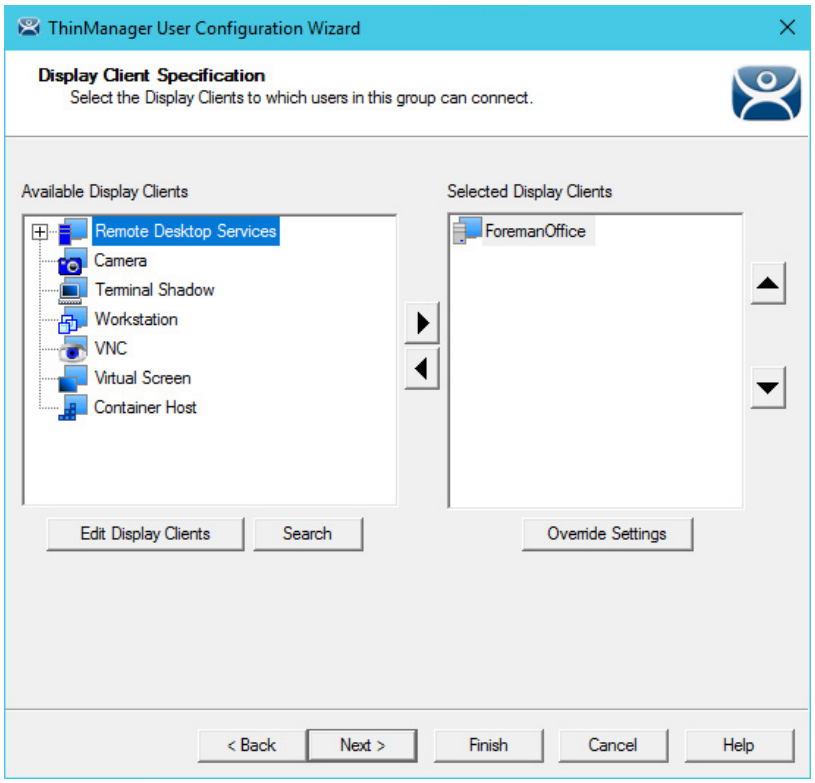


Setting	Description
Name	Type the name of the custom variable.
Value	Type the value or content to assign to the custom variable.
Hide Value	Check to obscure the custom variable value. Clear the checkbox to show the value.
OK	Click to accept the changes and close the dialog box.

7. On the ThinManager User Group Information page, click Next.

   The Display Client Specification page appears.

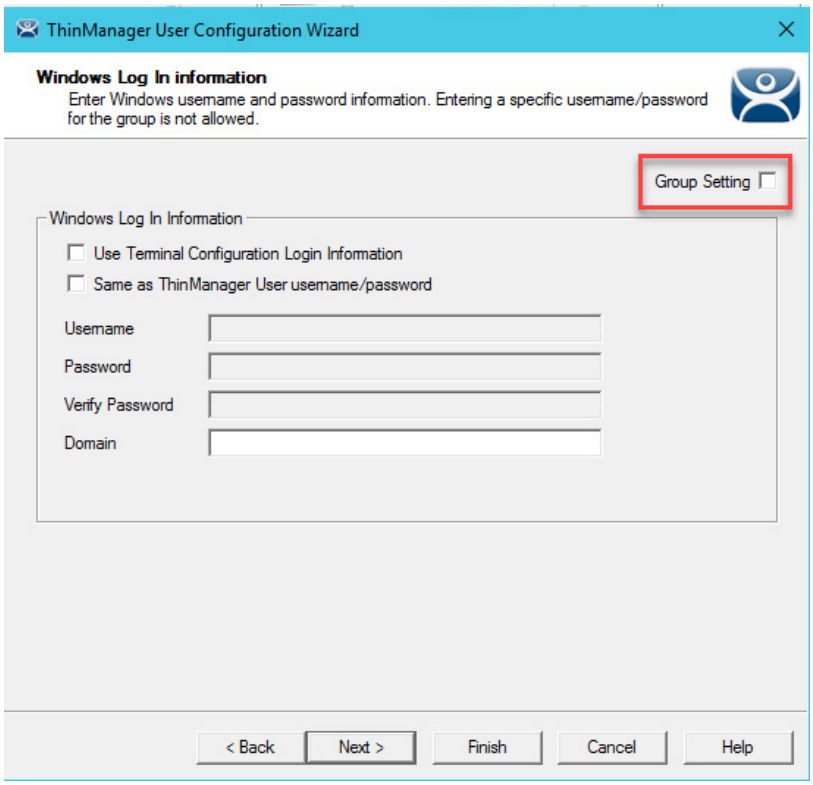
Figure 538 - Display Client Specification Page



8. Double-click the display clients in the Available Display Clients list for the group to move them to the Selected Display Clients list.
9. Click Next to continue the group configuration.

   The Windows Log In Information page appears.

Figure 539 - Windows Log In Information Page



Setting	Description
Group Setting	Check to apply setting to all members of the group.
Use Terminal Configuration Login Information	Check to allow the ThinManager User to use the terminal credentials for the application.
Same as ThinManager User username/password	Check when a Windows account is used for the ThinManager User account.
Username/Password/ Verify Password	These are dimmed because every user needs a unique Windows account. Therefore, a group setting is not allowed.
Domain	Type the domain if domain accounts are used.

The rest of the wizard follows the ThinManager User Configuration Wizard.

10. Click Next to continue or Finish to close and save the settings.

Any member of this group receives the Group Settings. Change a Group Setting and that change affects all members.

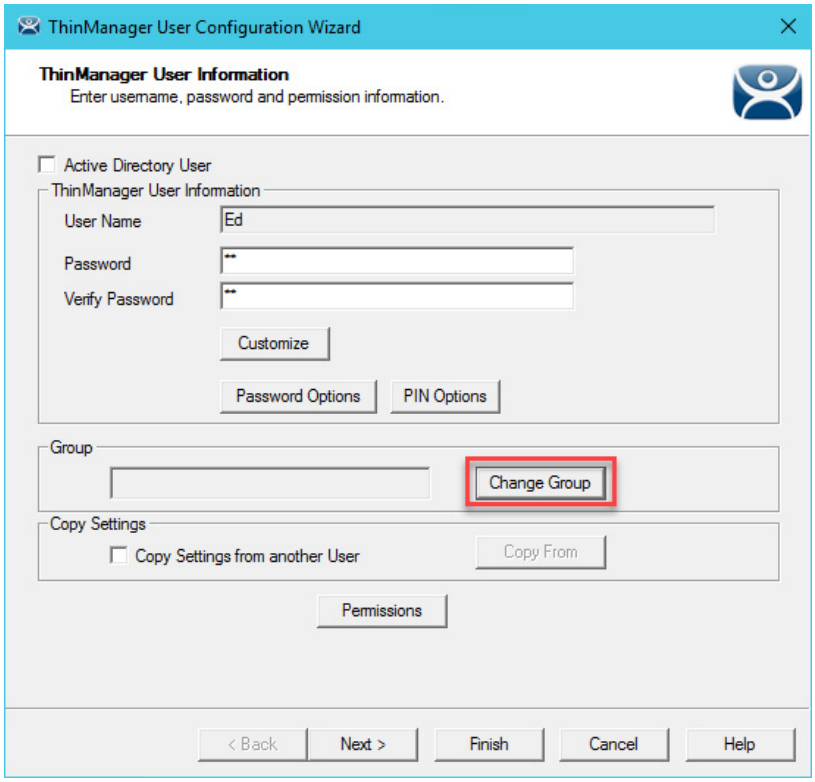
Add a ThinManager User to a ThinManager User Group

ThinManager Users can be added to the ThinManager User Group.

1. Right-click on the ThinManager Users branch in the ThinManager tree and choose Add User.

   The ThinManager User Information page of the ThinManager User Configuration Wizard appears.

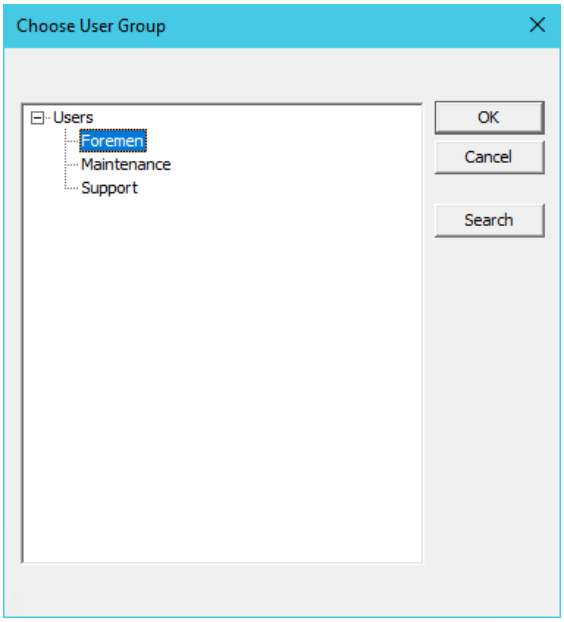
Figure 540 - ThinManager User Information Page



2. Type a name for the ThinManager User in the User Name field.
3. Click Change Group.

   The Choose User Group dialog box appears.

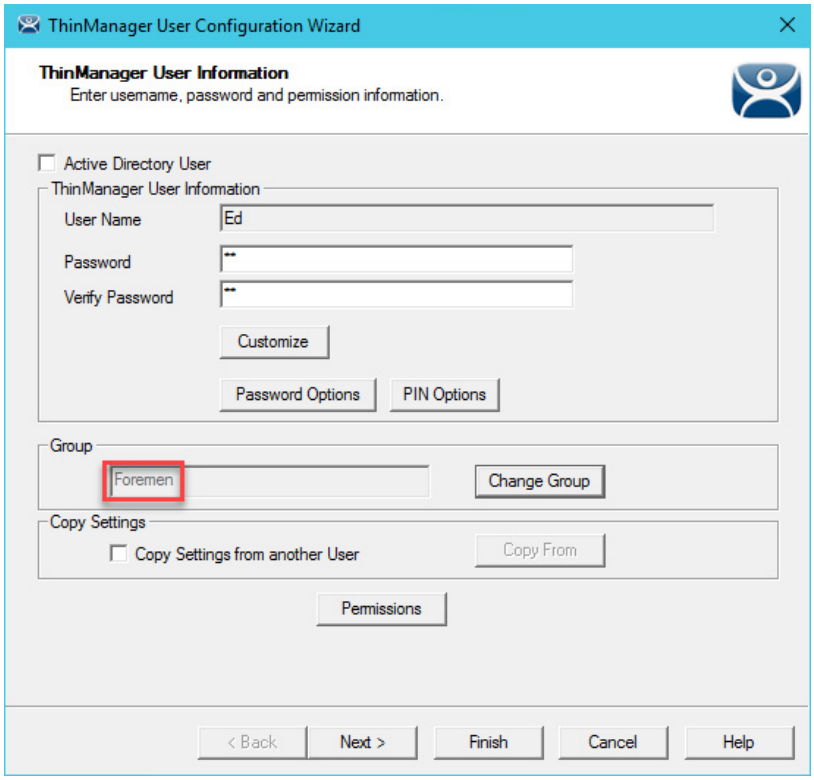
Figure 541 - Choose User Group Dialog Box



4. Highlight your ThinManager User Group and click OK to close the window and accept the changes.

   The ThinManager User Group is displayed in the Group field.

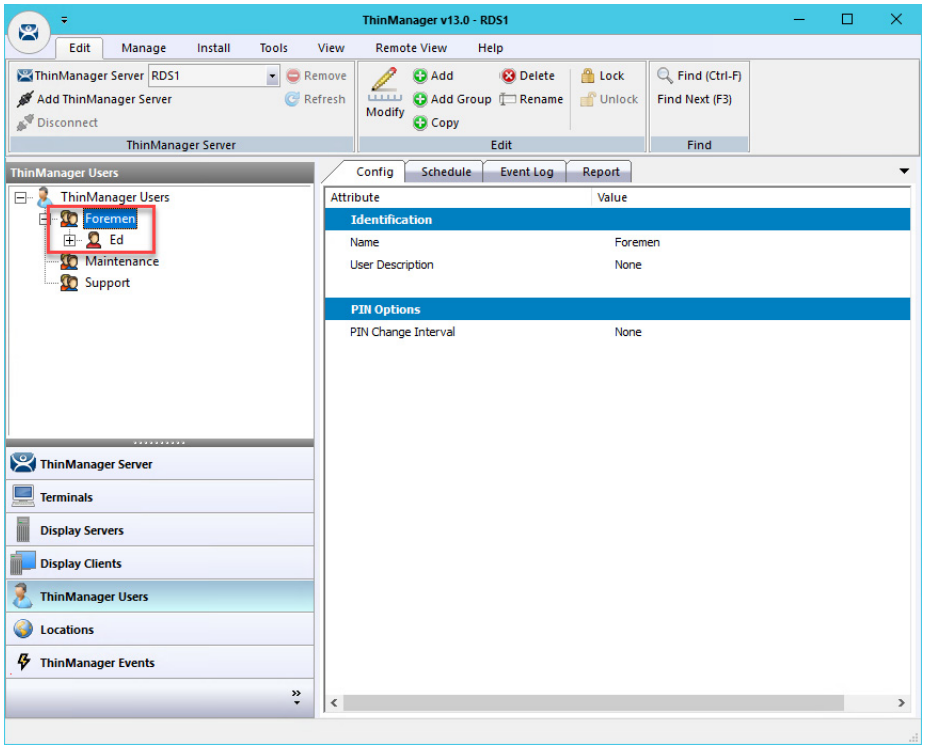
Figure 542 - ThinManager User Group Displayed



5. Click Finish to accept the configuration.

   Once a ThinManager User has joined a group, the user is displayed in the tree under the group.

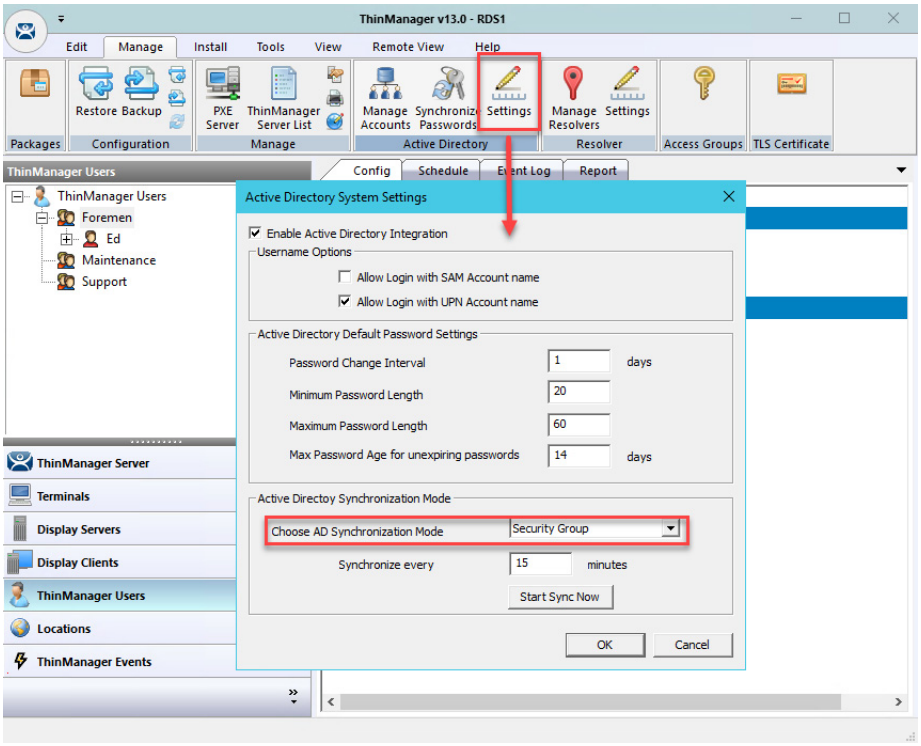
Figure 543 - Group Membership



Batch Create ThinManager Users using Active Directory OU

You can create ThinManager Users in a batch by either selecting one Windows Security Group or multiple Active Directory organizational units (OU). A user can only reside in one OU, but they can be members in multiple Security Groups. Limit users to a single Security Group to prevent duplicate accounts.

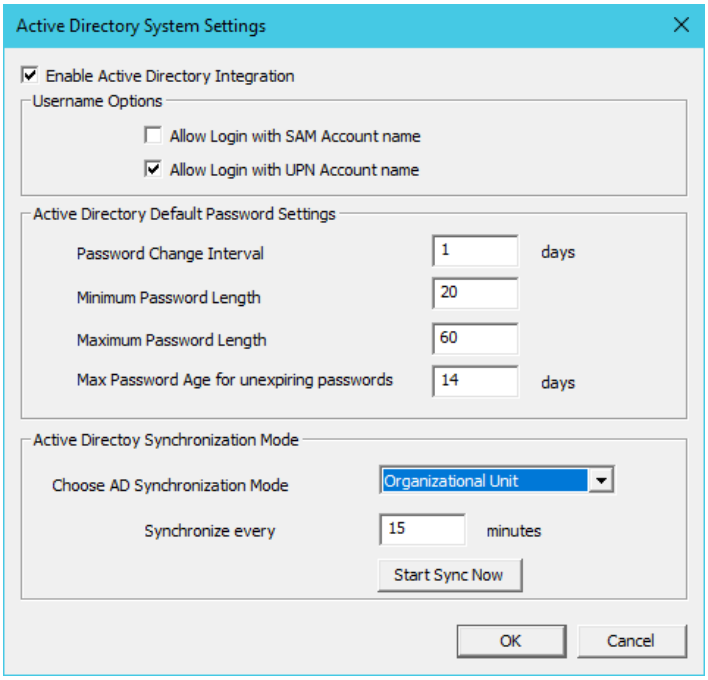
Figure 544 - Active Directory System Settings



1. Choose Manage>Active Directory>Settings.

   The Active Directory System Settings dialog box appears.

Figure 545 - Active Directory System Settings Dialog Box



2. From the Choose AD Synchronization Mode pull-down menu, choose either Organizational Unit or Security Group.

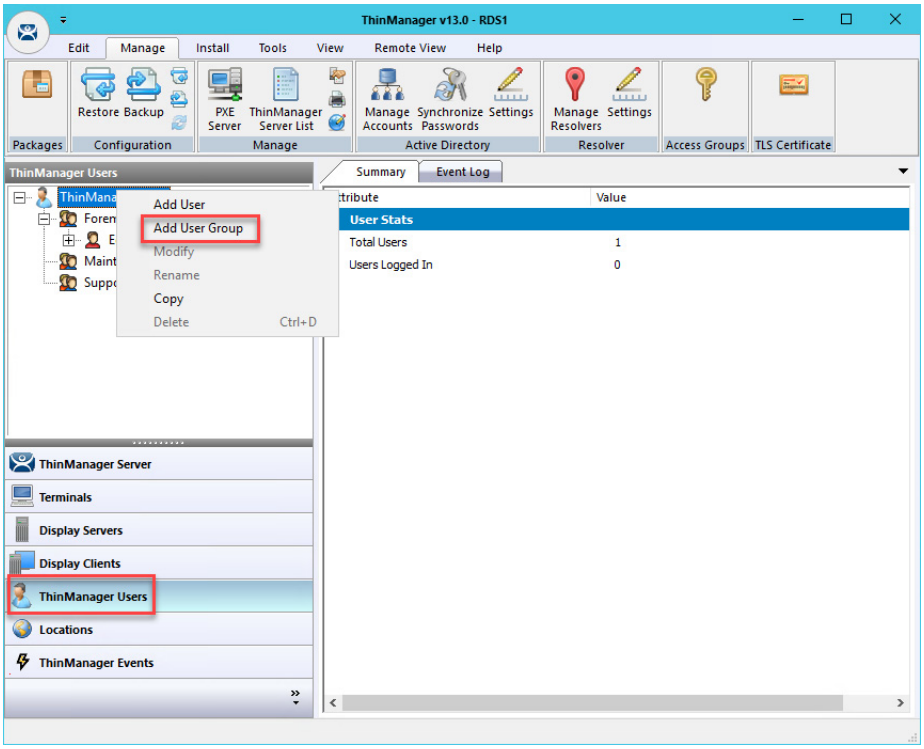
This manual shows the batch creation of ThinManager Users using Active Directory Organizational Units.

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 ThinManager User Group, but you can add many Organizational Units.

3. Click OK to close.

ThinManager User Groups are defined using the ThinManager User Configuration Wizard.

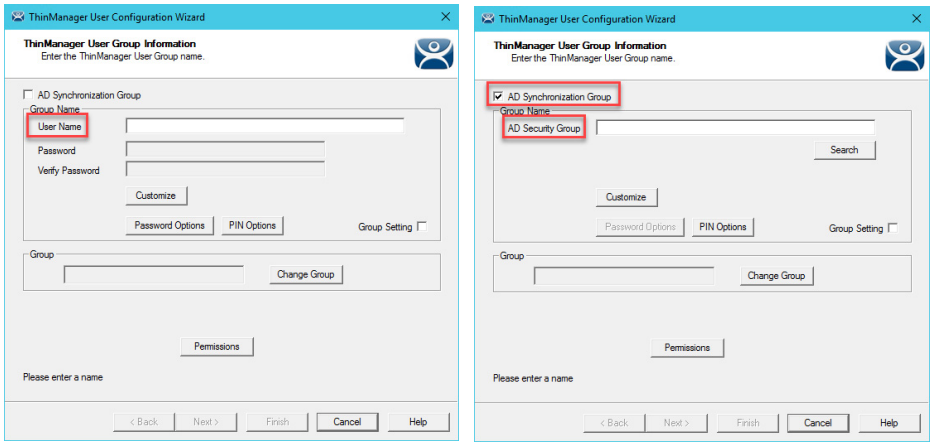
Figure 546 - Add User Group Command



1. Click ThinManager Users at the bottom-left of the ThinManager tree.
2. Right-click on the ThinManager Users branch and click Add User Group.

   The ThinManager User Configuration Wizard for the ThinManager User Group appears.

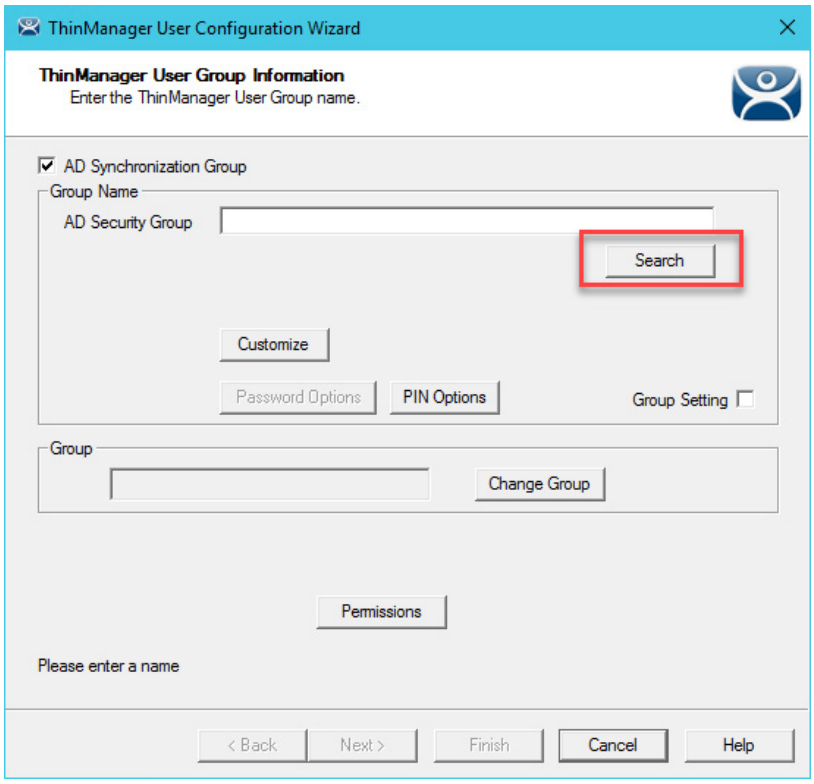
Figure 547 - ThinManager User Group Information Page



3. Check AD Synchronization Group.

   The User Name field becomes an Organizational Unit field.

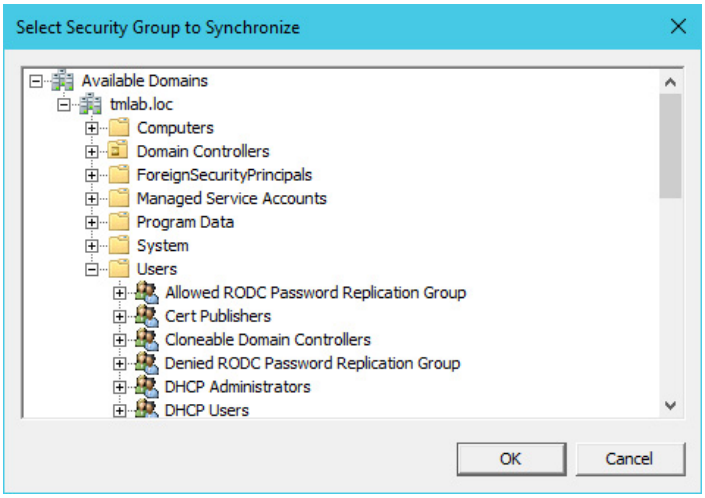
Figure 548 - ThinManager User Group Information Page



4. Click Search.

   The Select AD Location to Search dialog box appears, which lists the Organizational Units for the domain that the ThinManager Server is a member.

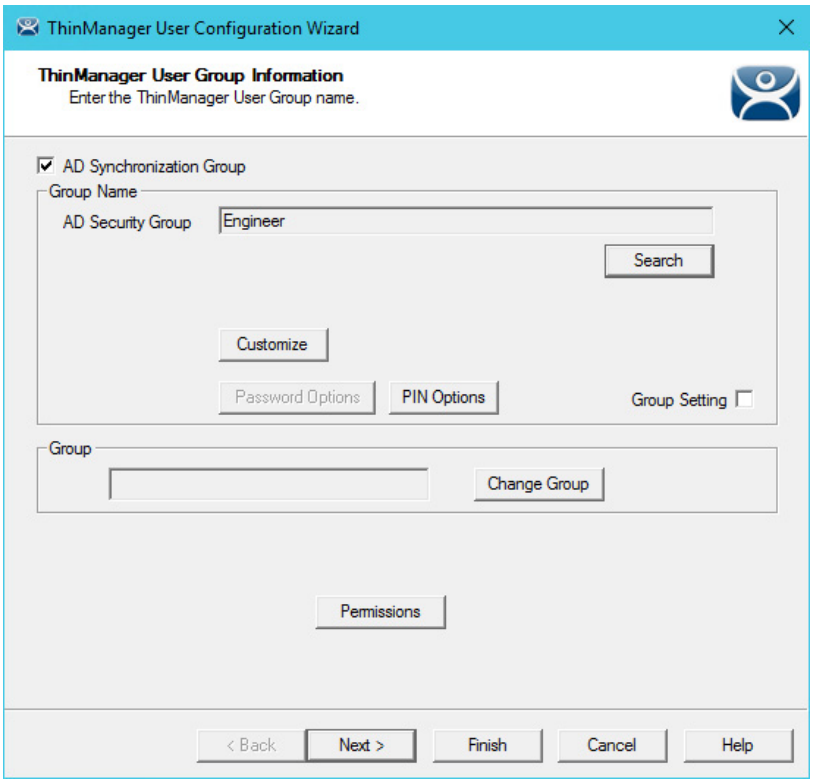
Figure 549 - Select AD Location to Search



5. Highlight the desired Organizational Unit and click OK.

   The ThinManager User Group appears in the Organizational Unit field.

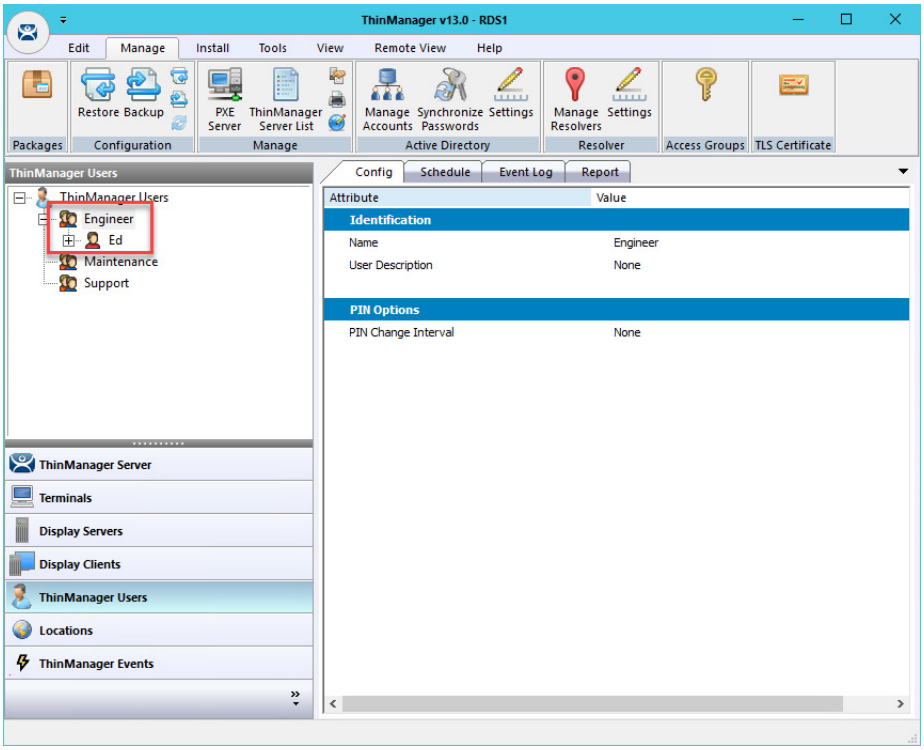
Figure 550 - ThinManager User Group



6. Select Next.
7. Click Finish

   The ThinManager Users Group is created. Depending on the Active Directory size, it may take some time to populate the ThinManager Users group.

Figure 551 - ThinManager Users Group



Once populated, all members of the Organizational Unit appear as members of the ThinManager Users group.

Password and Account Management

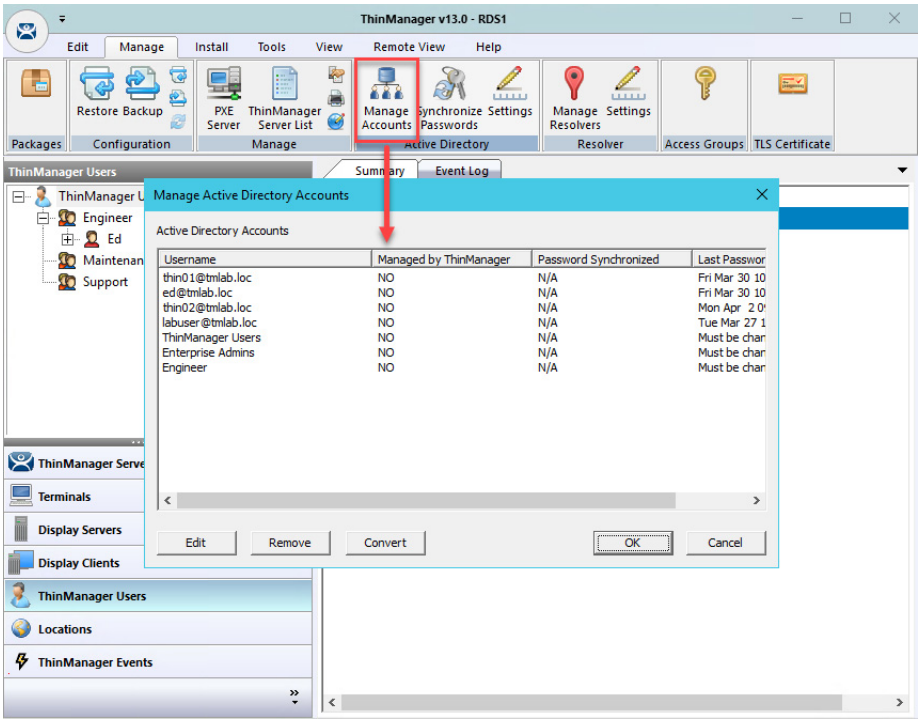
ThinManager has tools to manage domain accounts and passwords.

Active Directory

Manage Accounts Management

The first tool is the Manage Accounts tool.

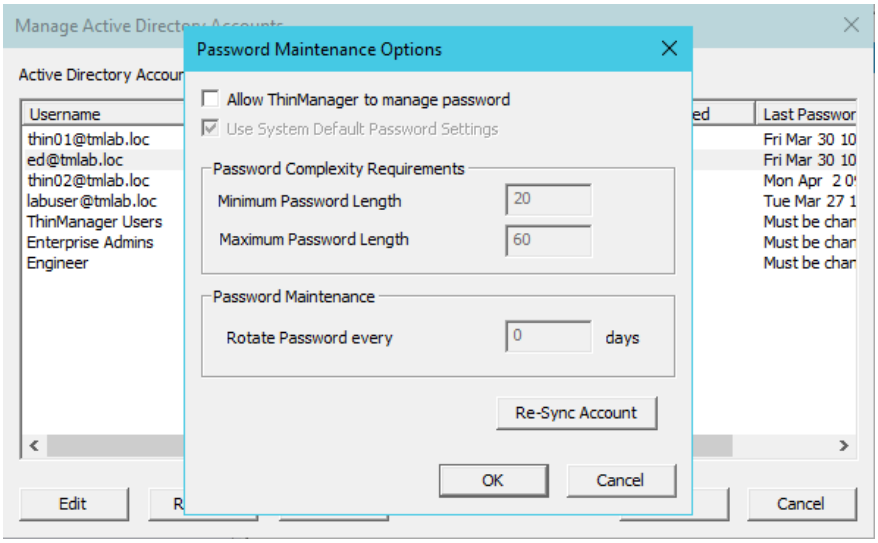
Figure 552 - Manage Active Directory Accounts



1. Choose Manage>Manage Accounts.

   The Manage Active Directory Accounts dialog box appears, which lists all the Active Directory accounts that are referenced in ThinManager.

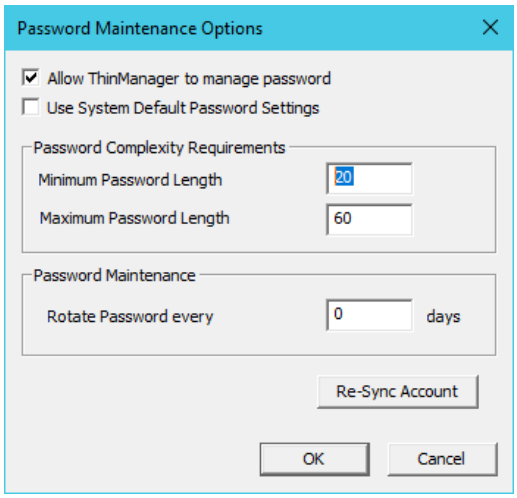
Figure 553 - Password Maintenance Options Dialog Box



2. Double-click on an account.

   The Password Maintenance Options dialog box appears, where you can have ThinManager manage the account's password.

Figure 554 - Password Maintenance Options



3. Check Allow ThinManager to manage password to add the account to the list of managed accounts with which you can use the system defaults.

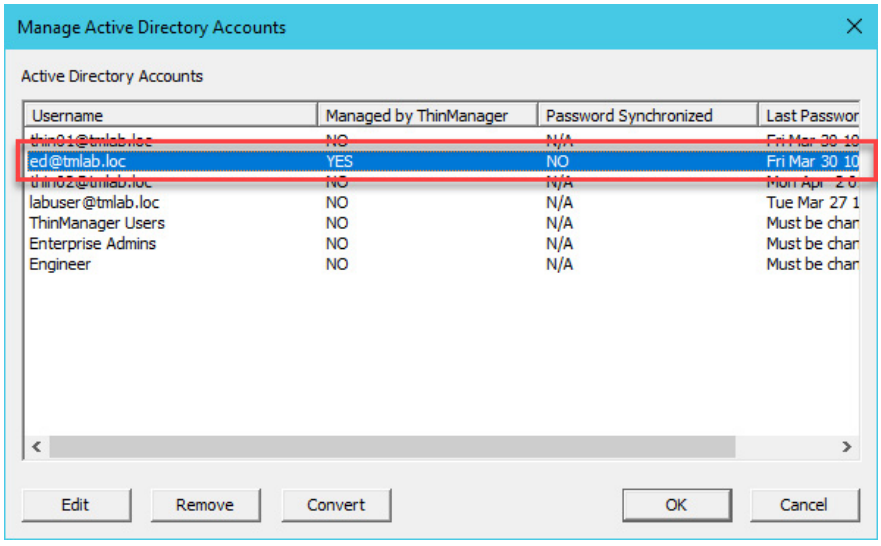
   Clear the Use System Default Password Settings checkbox to customize the password settings.

Setting	Description
Minimum Password Length	The minimum number of characters a password can have.
Maximum Password Length	The maximum number of characters a password can have.
Rotate Password every __ days	The number of days in which the password must be changed.

4. Click OK to accept the changes, or click Cancel to close and not save.

   On the Manage Active Directory Accounts dialog box, the account is displayed as a managed account.

Figure 555 - Manage Active Directory Accounts



Convert Accounts

Domain accounts that were used in previous versions of ThinManager can be converted to a managed account with the Convert function.

Figure 556 - Legacy Domain Log In

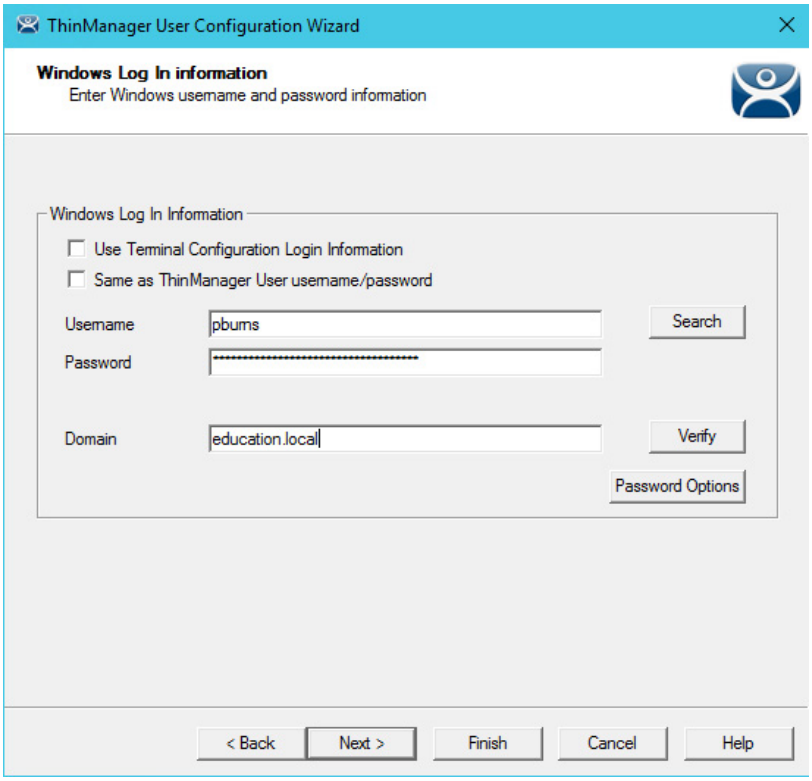
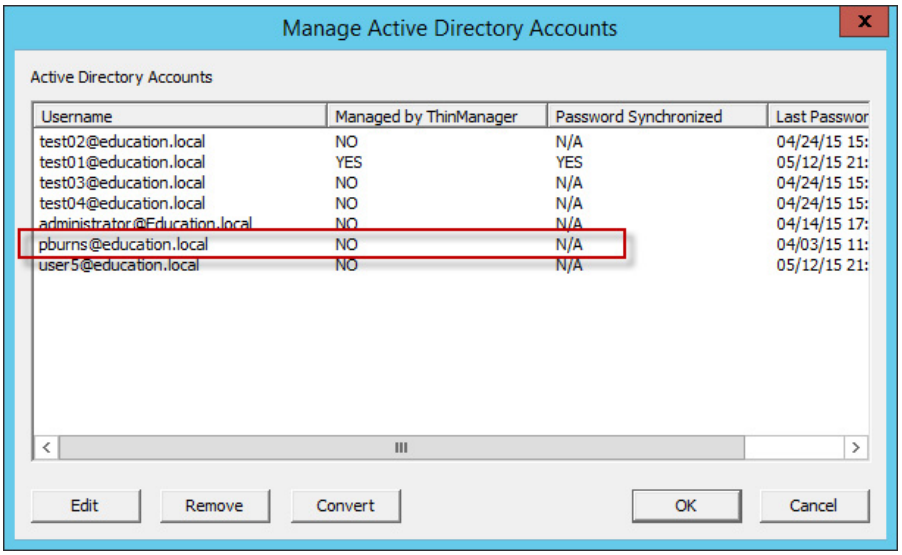


Figure 556 shows a domain account that was entered in an earlier version of ThinManager that did not have Active Directory integration.

Figure 557 - Manage Active Directory Accounts

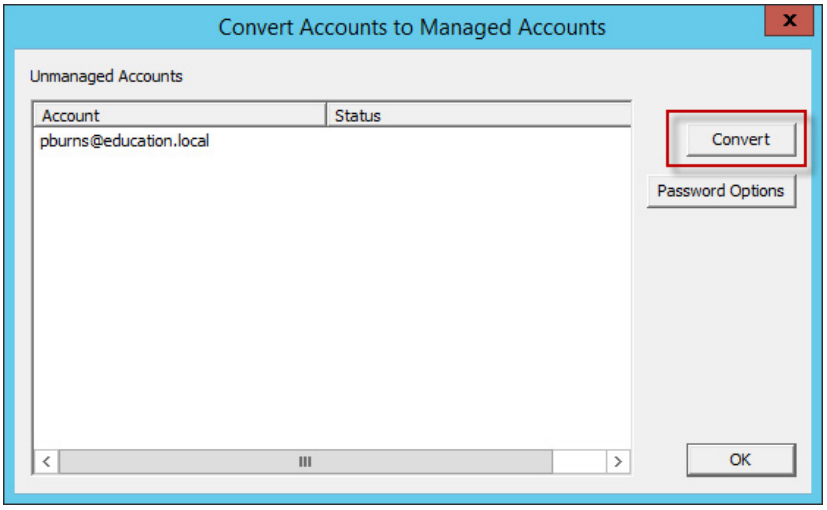


1. Choose Manage>Manage Accounts.

   The Manage Active Directory Accounts dialog box appears.
2. Highlight the legacy account and click Convert.

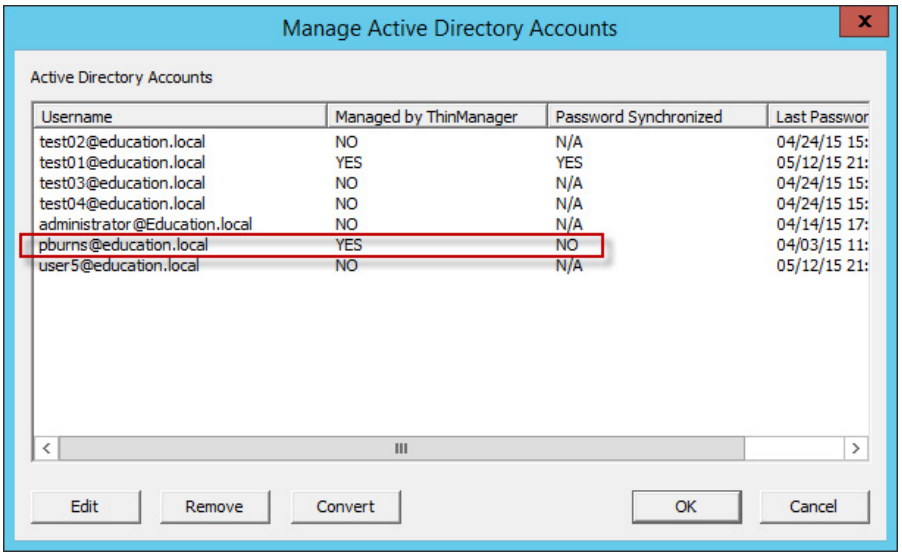
   The Convert Accounts to Managed Accounts dialog box appears.

Figure 558 - Convert Accounts to Managed Accounts



3. Highlight the legacy account and click Convert.
4. The Manage Active Directory Accounts dialog box shows that the account is now managed by ThinManager. See Figure 559.

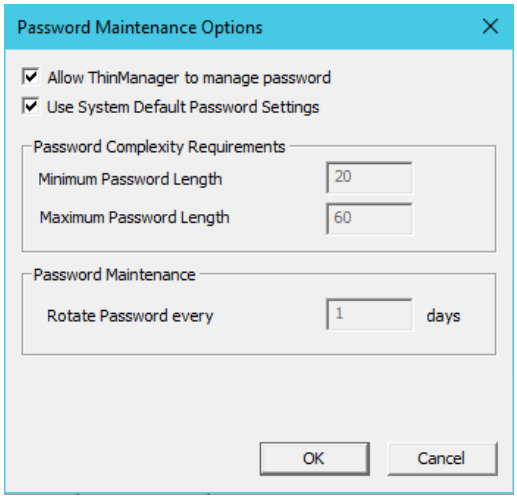
Figure 559 - Manage Active Directory Accounts



5. Double-click on a legacy domain account.

   The Password Maintenance Options dialog box appears for that account.

Figure 560 - Password Maintenance Options



6. Check Allow ThinManager to manage password to add the account to the list of managed accounts with which you can use the system defaults.

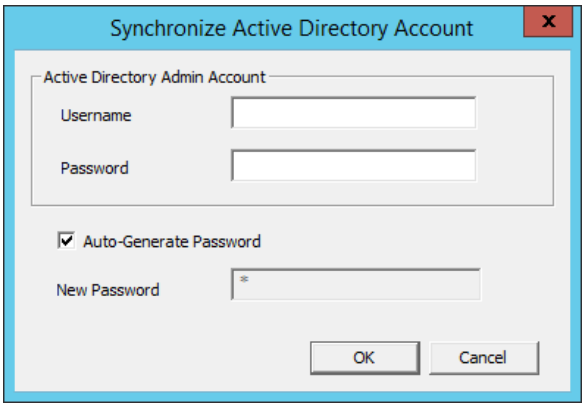
   Clear the Use System Default Password Settings checkbox to customize the password settings.

Setting	Description
Minimum Password Length	The minimum number of characters a password can have.
Maximum Password Length	The maximum number of characters a password can have.
Rotate Password every __ days	The number of days in which the password must be changed.

7. Click OK to accept the changes or click Cancel to not save and close the dialog box.

A Domain Administrator password is required to synchronize the Active Directory account.

Figure 561 - Synchronize Active Directory Account



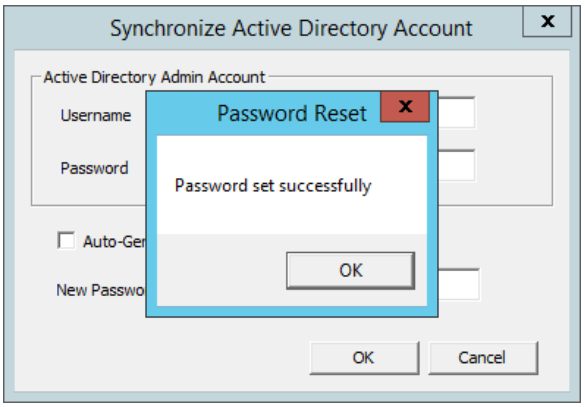
8. Enter domain admin credentials.
9. Check Auto-Generate Password to have ThinManager automatically create a password.

   Clear the Auto-Generate Password checkbox to enter your own password in the New Password field.

10. Click OK to synchronize the password, or click Cancel to not save it and close the dialog box.

An acknowledgment dialog box appears, which indicates a successful synchronization.

Figure 562 - Password Reset Dialog

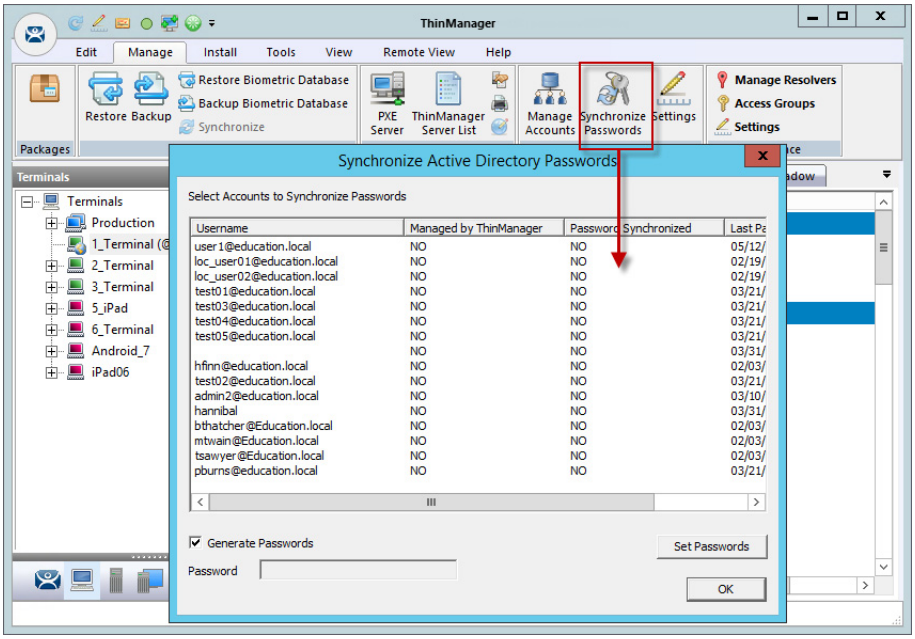


Synchronize Password

1. Choose Manage>Synchronize Passwords.

   The Synchronize Active Directory Passwords dialog box appears, which allows the synchronization of passwords for many accounts at once.

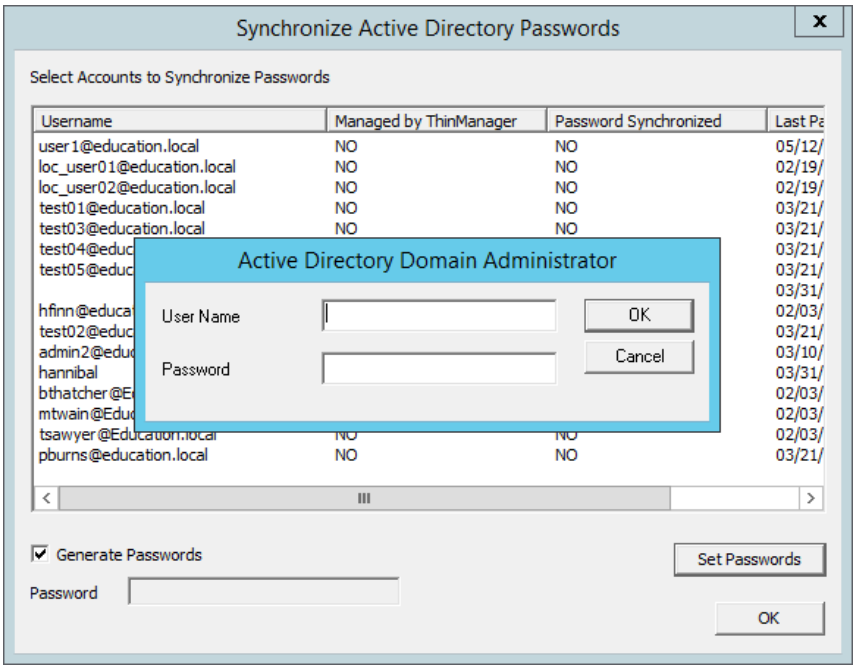
Figure 563 - Synchronize Active Directory Passwords



2. Click Set Passwords.

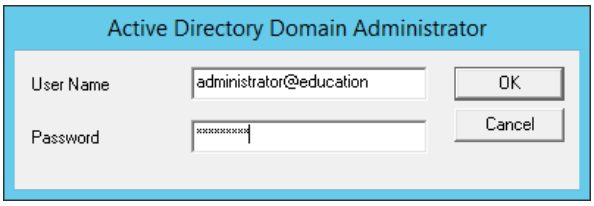
   The Active Directory Domain Administrator dialog box appears.

Figure 564 - Active Directory Domain Administrator Log In



This action requires a Domain Administrator account.

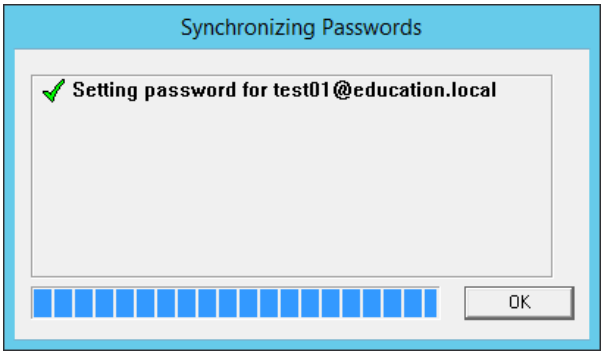
Figure 565 - Active Directory Domain Administrator Log In



3. Type the credentials in the appropriate fields and click OK.

   The Synchronizing Passwords progress dialog appears.

Figure 566 - Synchronizing Passwords



4. Click OK to close the dialog box.

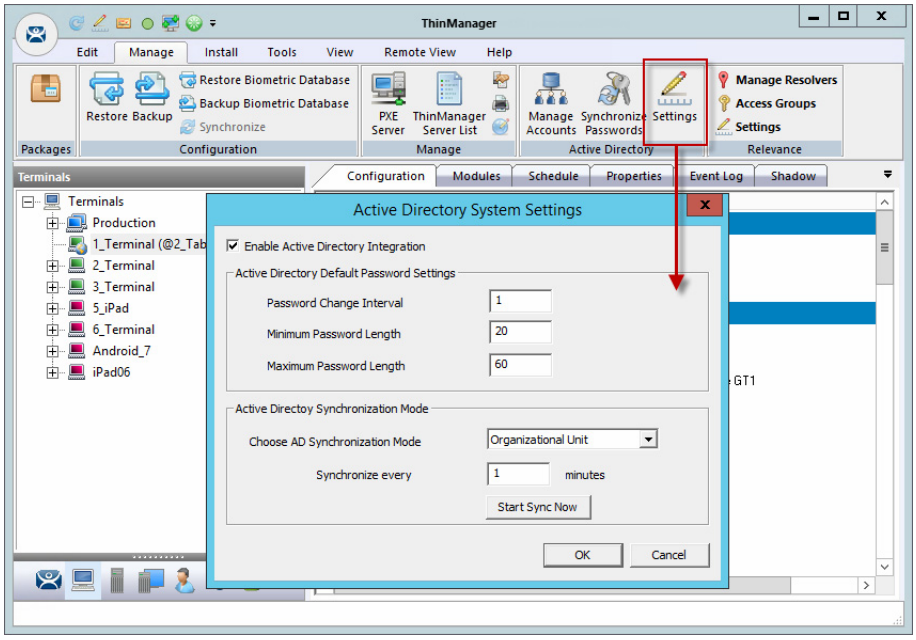
The selected accounts have their passwords synchronized between ThinManager and the Active Directory.

Settings

Choose Manage>Settings (Active Directory).

The Active Directory System Settings dialog box appears, which contains the settings for the passwords.

Figure 567 - Active Directory System Settings



Setting	Description
Password Change Interval	The number of days before the password must be changed.
Minimum Password Length	The minimum number of characters a password can have.
Maximum Password Length	The maximum number of characters a password can have.
Choose AD Synchronization Mode	Use with batch creation of ThinManager Users. You can generate users from one Windows Security Group or multiple Organizational Units.
Synchronize every __ minutes	Type how frequently ThinManager synchronizes with the Active Directory. Password communication is encrypted for security.
Start Sync Now	Manually start the synchronization between the ThinManager Server and the Active Directory.

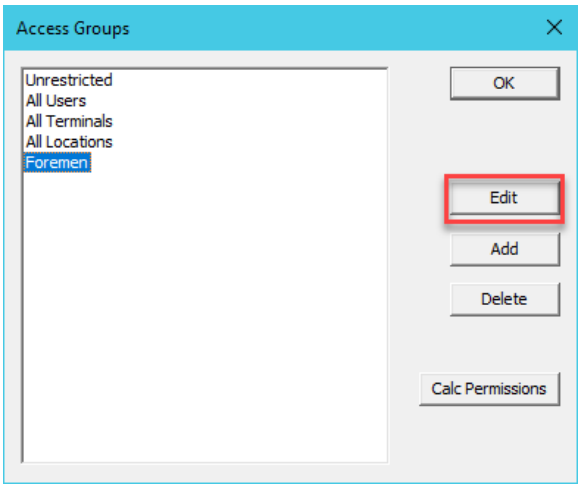
Shortcut Method to Add Access Groups

Quickly add members to Access Groups through the Access Groups Wizard.

1. Choose Manage>Access Groups from the ThinManager menu.

   The Access Groups dialog box appears.

Figure 568 - Access Groups Dialog Box

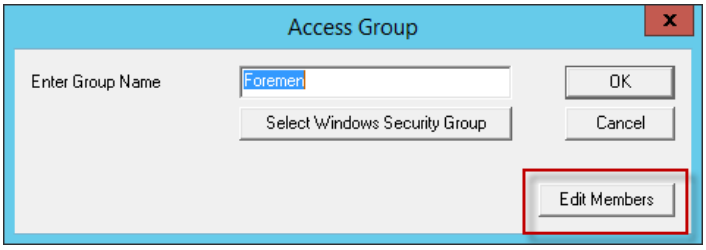


Access groups can be added, deleted, or edited.

2. Highlight the desired Access Group and click Edit.

   The Access Group dialog box appears.

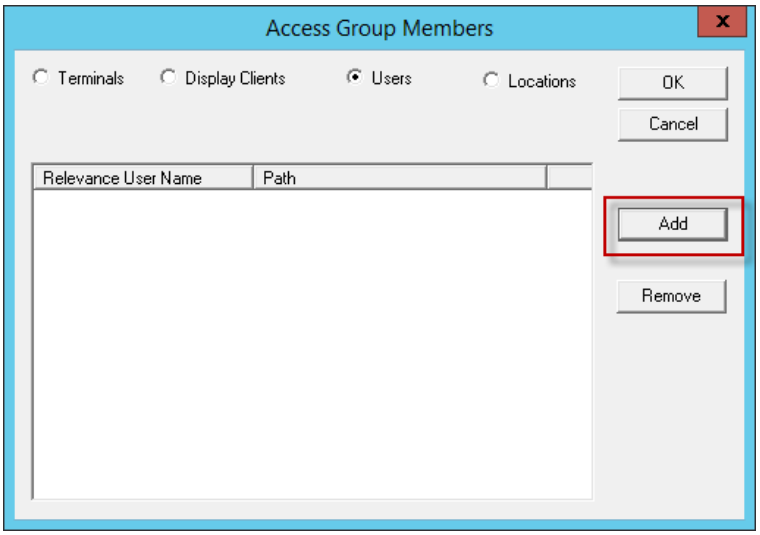
Figure 569 - Access Group Dialog Box



3. Click Edit Members.

   The Access Group Members dialog box appears.

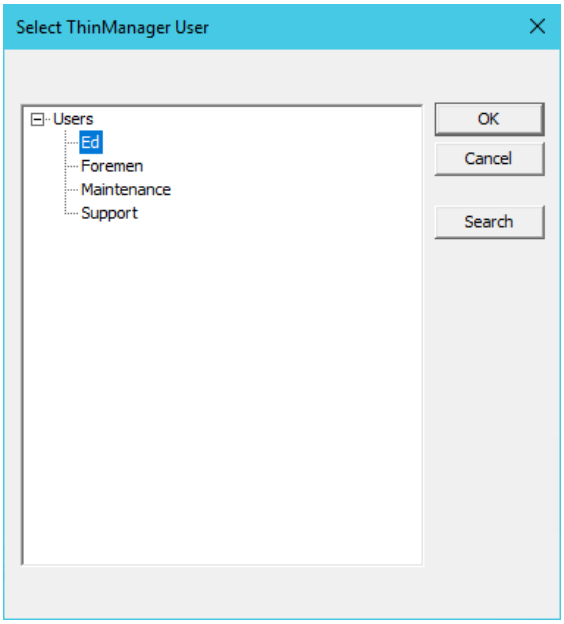
Figure 570 - Access Group Members



4. Click Terminals, Display Clients, or Users to configure that category and click Add.

   The Select ThinManager User dialog box appears with a tree of the configured Users and User groups.

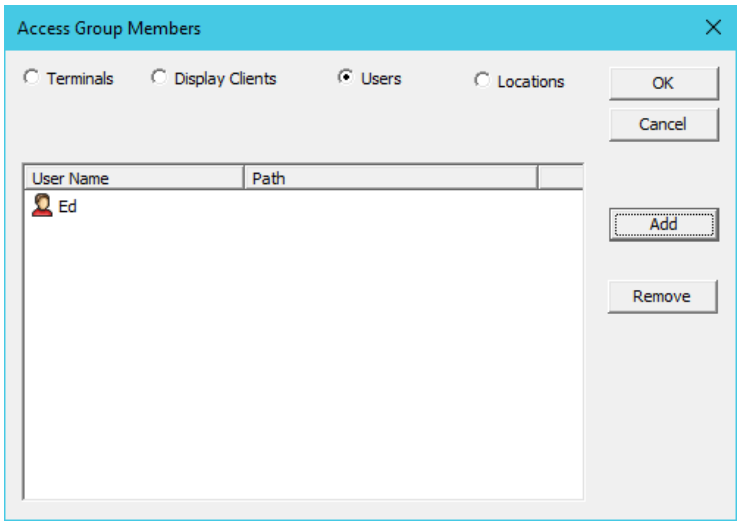
Figure 571 - Select ThinManager User



5. Highlight the desired ThinManager User and click OK for each addition.

   The Access Group Members dialog box shows the members of the Location Services Access Group.

Figure 572 - Access Group Members



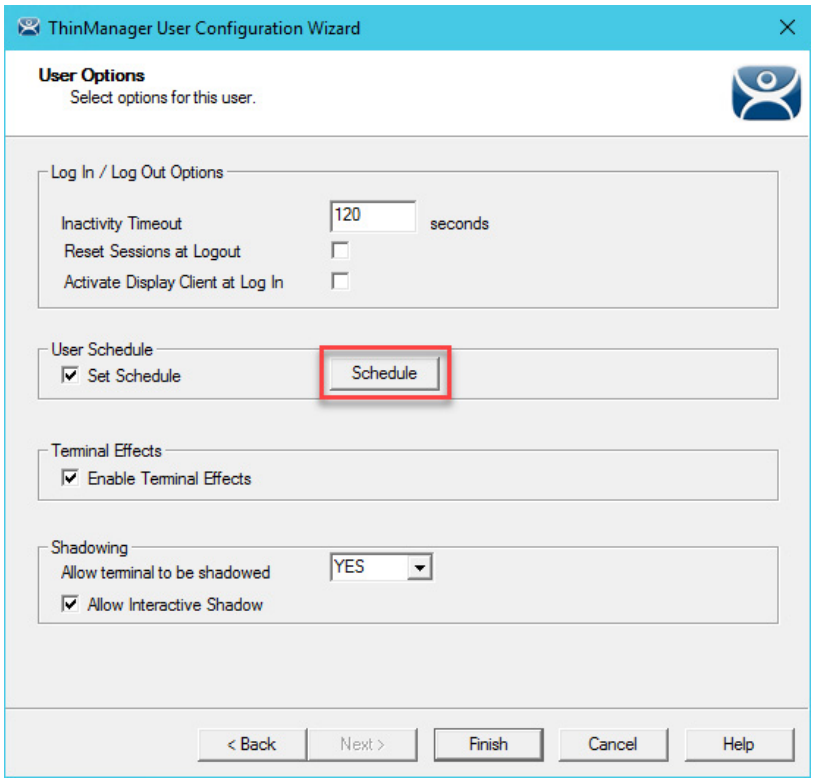
6. Highlight the members of the Access Group and click Remove to remove members.

Display Clients and Users can be added by the same process.

ThinManager User Schedule

ThinManager Users and ThinManager User Groups have a schedule on the User Options page of the ThinManager User Configuration Wizard.

Figure 573 - User Options Page

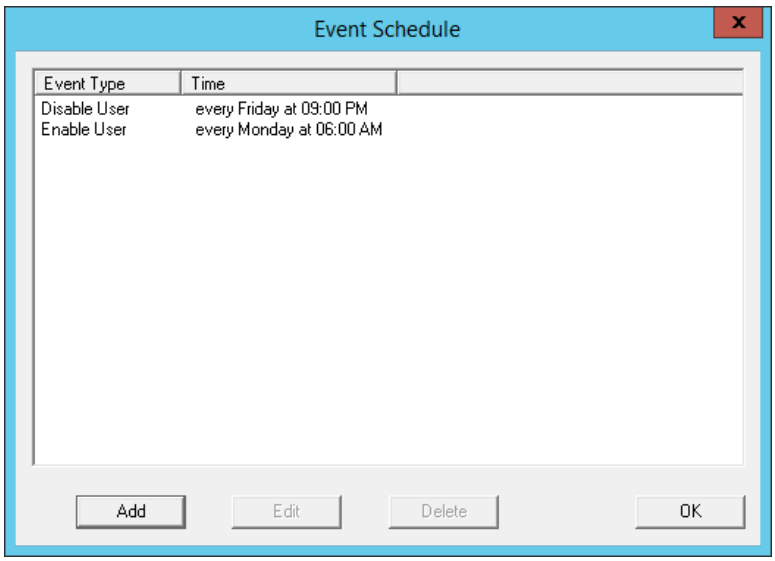


1. Check Set Schedule and click Schedule.

   The Event Schedule dialog box appears, which lists events for the ThinManager User or ThinManager User Group.

The Schedule for ThinManager User Groups feature is the same as for individual ThinManager Users. The advantage of the Schedule for ThinManager User Groups feature is that it allows you to apply scheduled events to a whole group of users rather than the requirements to configure each event for each user.

Figure 574 - Event Schedule



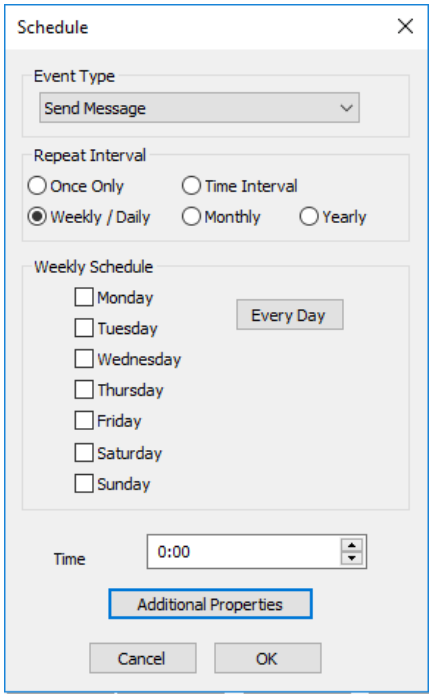
Setting	Description
Add	Launches a Schedule dialog box, which allows an event to be configured.

Setting	Description
Edit	Allows a highlighted event to be changed.
Delete	Removes a highlighted event.
OK	Accepts changes and closes the Event Schedule dialog box.

2. Click Add.

   The Schedule dialog box appears, which has several configuration settings.

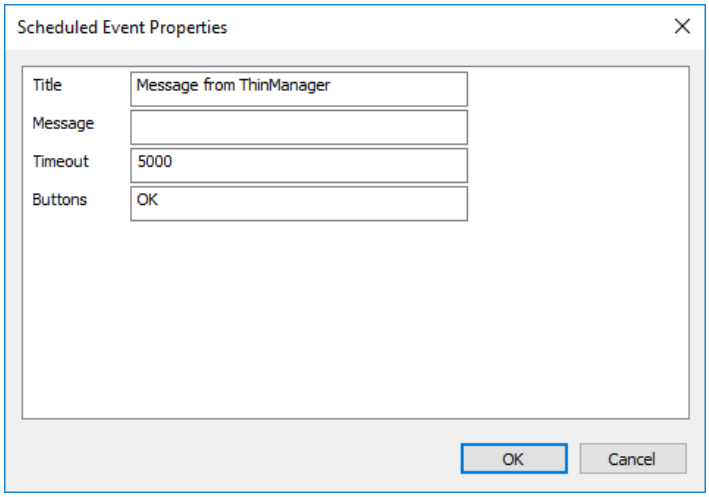
Figure 575 - Schedule Dialog Box



Setting	Description
Event Type	Choose an event from the pull-down menu.
Disable User	Prevents a user login through Location Services, or disconnects a session.
Enable User	Allows a user to become active again.
Send Message	Provides the option to schedule an event to send a dialog message to a terminal via the Additional Properties button, which is propagated by this setting.
Repeat Interval	
Once Only	Shows a Select Date field for the event.
Weekly/Daily	Shows a Weekly Schedule list for the event to run. The Every Day button selects all the days in the list.
Monthly	Shows a Select Day of Month field for the event.
Yearly	Shows a Select Date field for the event.
Time	Allows the selection of the time that the event should occur.
Additional Properties	This button is propagated by the Send Messages Event Type. Click to open the Scheduled Event Properties dialog.

   a. The Scheduled Event Properties dialog opens when Send Message is chosen from the Event Type pull-down menu and the Additional Properties button is clicked. Complete the fields of the dialog box, and then click OK.

Figure 576 - Scheduled Event Properties



Setting	Description
Title	Enter the title for the message.
Message	Enter the message to be sent.
Timeout	Enter the amount of time for message to be sent.
Buttons	Enter the text of the acknowledgment button to be pressed by the user of the terminal that received the message, such as OK.

3. Click OK to close the Schedule dialog box.
4. On the Event Schedule dialog box, click Add to add another event to the Event Schedule or click OK to close the Event Schedule window and return to the Terminal configuration.

Card Readers and Fingerprint Scanners

Card and Badge Configuration for a ThinManager User

ThinManager has the ability to use Prox (proximity) cards for Location Services logins, which requires these actions.

- Add a card reader to the ThinManager-ready thin client
- Add the card reader module to the Terminal configuration
- Associate the card number to the ThinManager User configuration

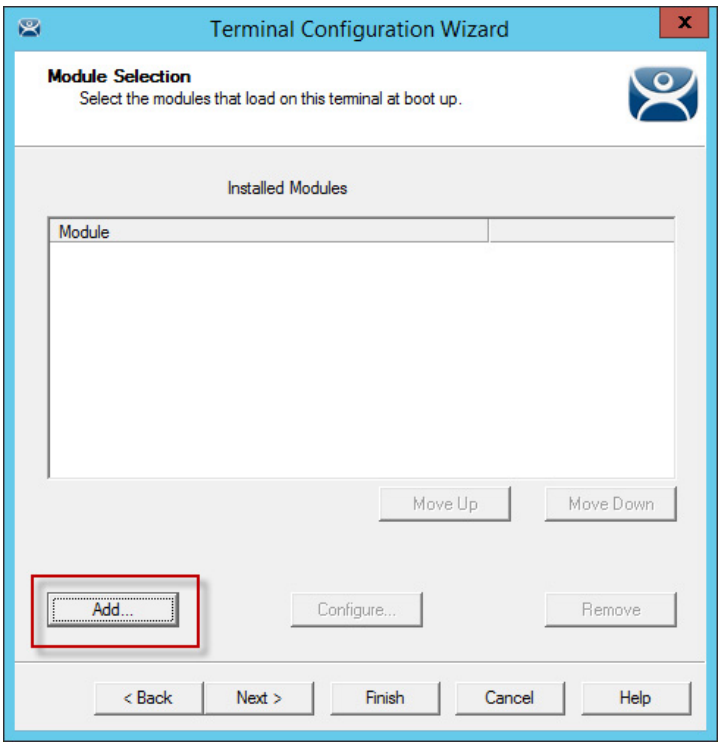
ThinManager has support for the RF Ideas Inc. serial RDR-6081AK2 pcProx card reader and the USB RDR-6081AKU and RDR-80582AK0 pcProx card readers (www.rfideas.com).

Configure a Terminal with the Card Reader Module

1. Double-click on the Terminal in the tree.

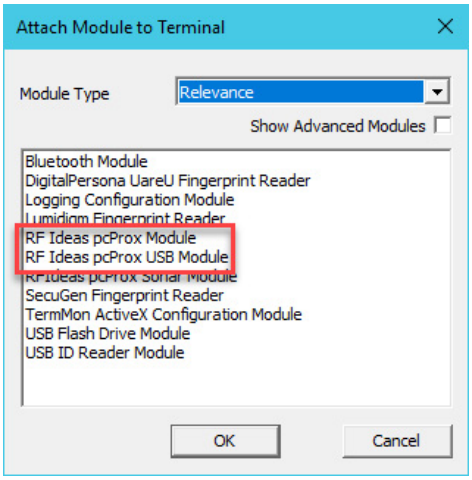
   The Terminal Configuration Wizard appears.
2. Click Next until the Module Selection page appears.

Figure 577 - Module Selection Page



3. Click Add.
4. The Attach Module to Terminal dialog box appears.

Figure 578 - Attach Module to Terminal



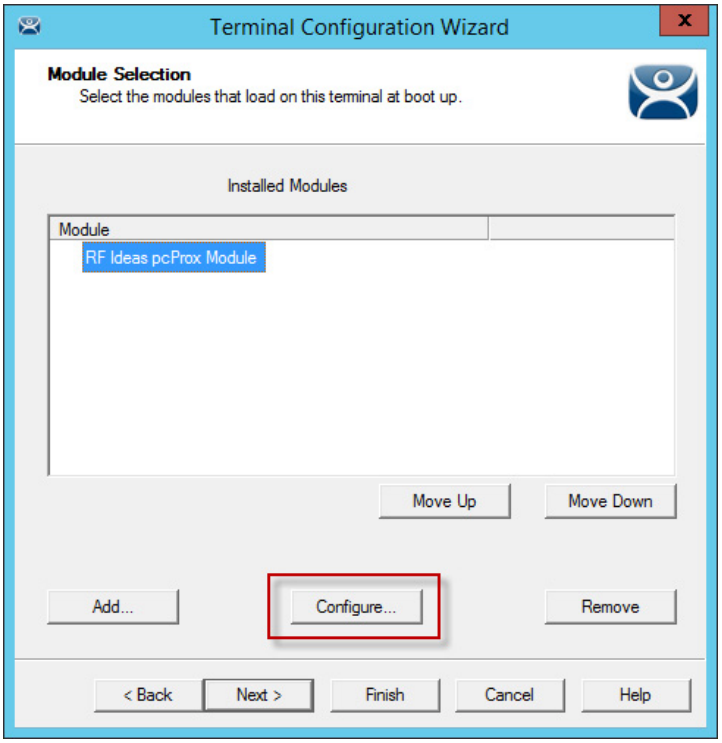
5. Choose Relevance from the Module Type pull-down menu.
6. Highlight an RF Ideas pcProx Module and click OK.

- Use the RF Ideas pcProx Module for serial devices
- Use the RF Ideas pcProx USB Module for USB devices

7. Click OK to attach the module to the Terminal.

The module can be configured once it is attached to a Terminal.

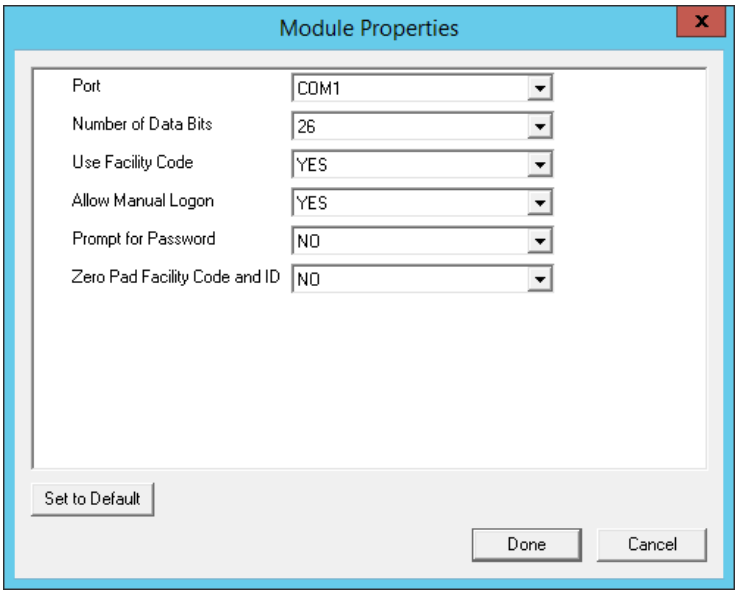
Figure 579 - Module Selection



8. Highlight RF Ideas pcProx Module and click Configure.

   The Module Properties dialog box appears.

Figure 580 - Serial pcProx Card Module Properties



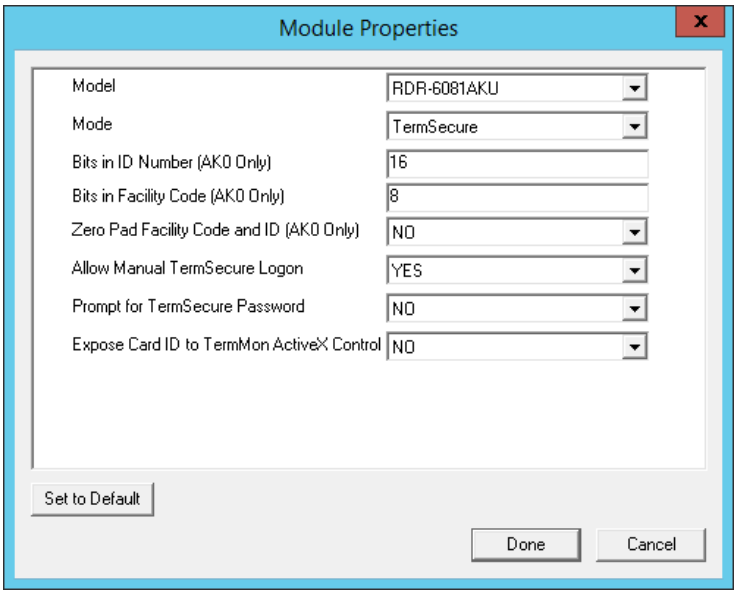
The RF Ideas Serial pcProx Module has parameters that can be configured.

Setting	Description
Port	Choose the port on which the serial RF Ideas pcProx card reader is installed.
Number of Data Bits	Different cards use different numbers of data bits in their format. 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	Set to Yes to add the card's Facility Code to the Card/Badge ID number.

Setting	Description
Allow Manual Logon	Set to Yes to allow a ThinManager User to log in to a Terminal without a ThinManager ID device. Set to No so ThinManager users must use a ThinManager ID device to log in.
Prompt for Password	Set to Yes to require a ThinManager User to enter their password for access even if the password is configured in ThinManager.
Zero Pad Facility Code and ID	Adds a leading 0 to the Facility Code if needed.

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.

Figure 581 - USB pcProx Card Module Properties



The RF Ideas USB pcProx Module has parameters that can be configured.

Setting	Description
Model	Choose from these different USB pcProx card readers. RDR-6081AKU RDR-6011AKU RDR-80582AK0 RDR-80082AK0
Mode	Choose from ThinManager, Wedge, and TermMon modes.
ThinManager Mode	Allows the card to be used with ThinManager as a login device.
Wedge Mode	Allows the data to be sent to the session as a character string.
TermMon Mode	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. 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. Sets the number of data bits of the Facility Code.
Zero Pad Facility Code and ID (AK0 Only)	Adds a leading zero to the Facility Code if needed.
Allow Manual ThinManager Logon	Set to Yes to allow a ThinManager User to log in to a Terminal without a ThinManager ID device. Set to No so ThinManager users must use a ThinManager ID device to log in.
Prompt for ThinManager Password	Set to Yes to require a ThinManager User 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 ThinManager.

To configure a parameter, follow these steps.

1. Highlight the parameter.
2. Change the value.
3. Click Done to accept the changes.

   Once the Terminal has the module added, restart it to apply the changes.
4. On the Module Selection page, click Finish.

   The Terminal Configuration Wizard closes.
5. Right-click on the Terminal in the ThinManager tree and choose Restart.

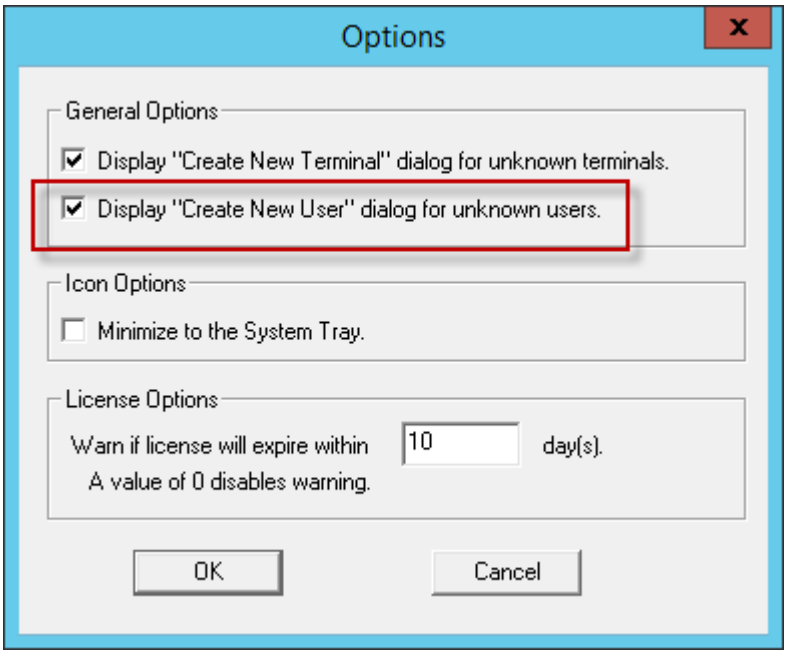
Configure ThinManager for Automatic User Configuration

A card reader can be used to associate cards with ThinManager Users using wizards.

1. Choose View>Options from the ThinManager menu.

   The Options dialog box appears.

Figure 582 - Options Dialog Box



2. Check Display “Create New User” dialog for unknown users.
3. Click OK to accept the change.

   Now, when an unknown ID device (USB key or ID card) is read by a Terminal, the ThinManager User Configuration Wizard appears. Also, when a new ID is scanned or an undefined USB key is inserted, the Enter Card/Badge ID number is automatically populated in the ThinManager User Configuration Wizard.

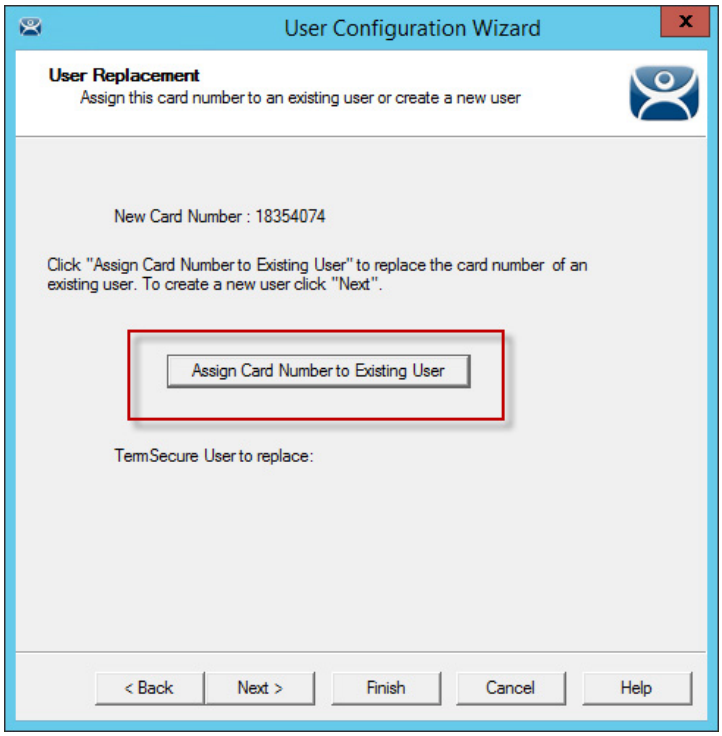
Automatically Apply the Card to a Configuration

Once ThinManager has Display “Create New User” dialog for unknown users checked, a card scanned on a Terminal can be used to associate cards with Location Services.

1. Pass an HID card over the card reader on the Terminal.

   The ThinManager User Configuration Wizard appears.

Figure 583 - Card/Badge Information



Once the card reader has scanned an unknown Prox card, a ThinManager User Configuration Wizard is launched, associated with the new card number.

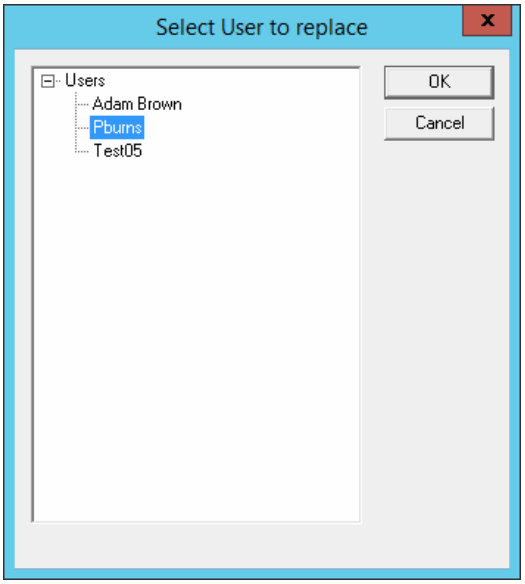
2. Click Assign Card Number to Existing User.

   The ThinManager User Replacement page appears.

3. Click Next if you want to create a new ThinManager User for this card instead of associating it with a previously created ThinManager User.

The User Replacement Page allows you to select an existing ThinManager User with whom to associate the card.

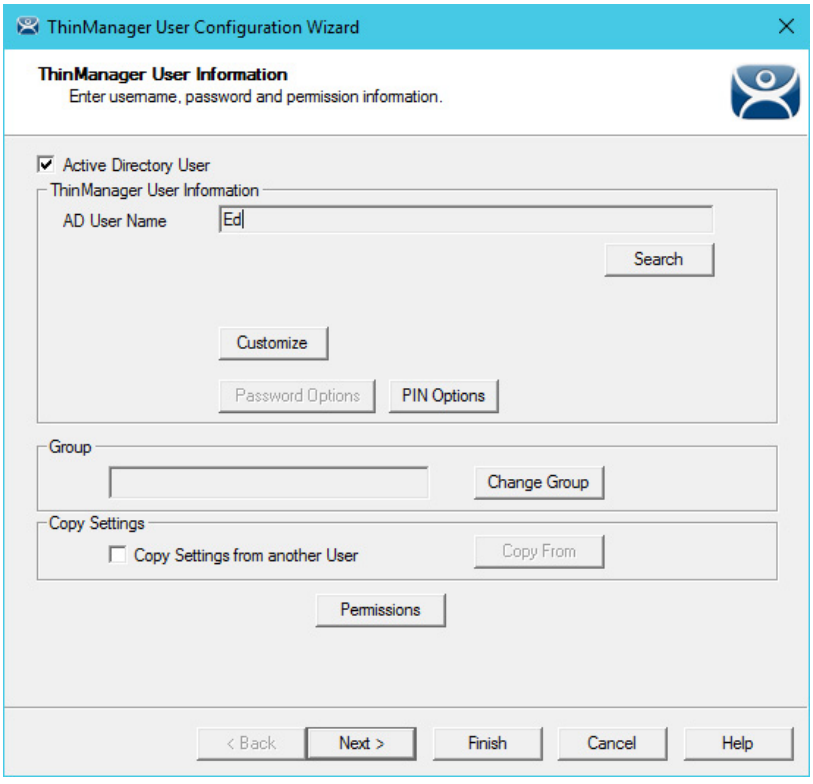
Figure 584 - User Replacement Dialog Box



4. Select a ThinManager User from the tree and click OK.

   The ThinManager User Information page for the selected user appears.

Figure 585 - ThinManager User Configuration Wizard



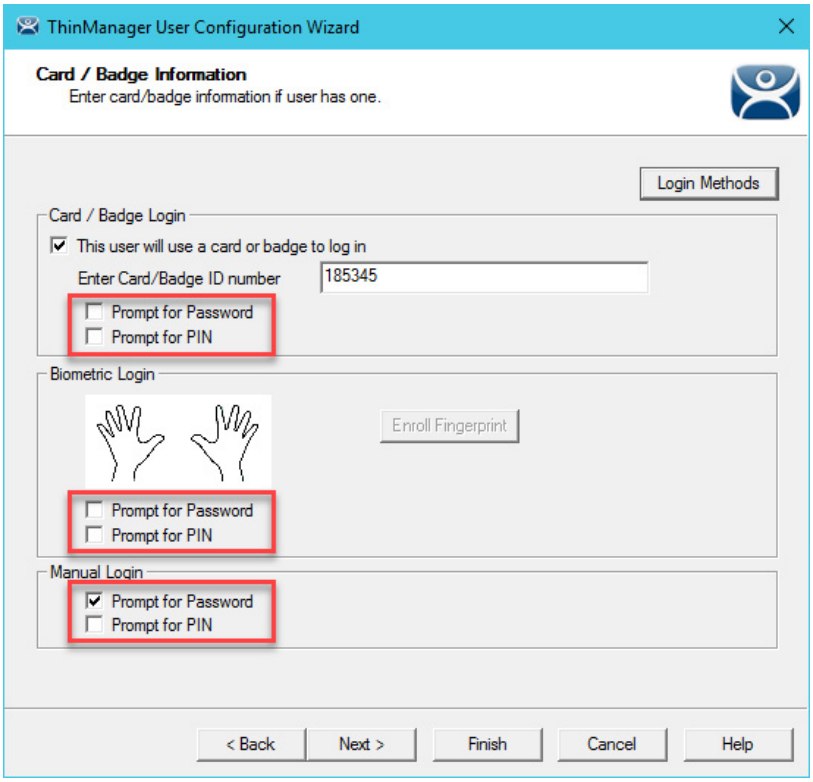
The Password and Permissions can be modified at this time if it is not an Active Directory user.

5. Click Next.

The Card/Badge Information page appears with This user will use a card or badge to log in checked.

The serial number of the HID card is populated to the Enter Card/Badge ID number field.

Figure 586 - Card/Badge Information Page



Check Prompt for Password or Prompt for Pin for the Card/Badge Login, the Biometric Login, or a Manual Login to require a secondary credential.

Setting	Description
Prompt for Password	Check to require the user to enter their password
Prompt for Pin	Check to require the user to enter their PIN

6. Click Finish to accept the changes.

   The card can now be used to log in at terminals configured with card readers.

Manually Apply the Card to a Configuration

Although the easiest method to assign a card or badge is automatic as described in the previous section, ThinManager can be configured for manual entry.

To configure a terminal to allow a device, follow these instructions.

1. In the Options dialog box, see Figure 582 on page 410, clear the Display "Create New User" dialog for unknown users checkbox to manually complete the Enter Card/Badge ID number field. You can find the Card/Badge ID number in the event log.
2. Turn the ThinManager User Event Log on in the ThinManager Server Configuration Wizard. See Event Log on page 414 for more information.

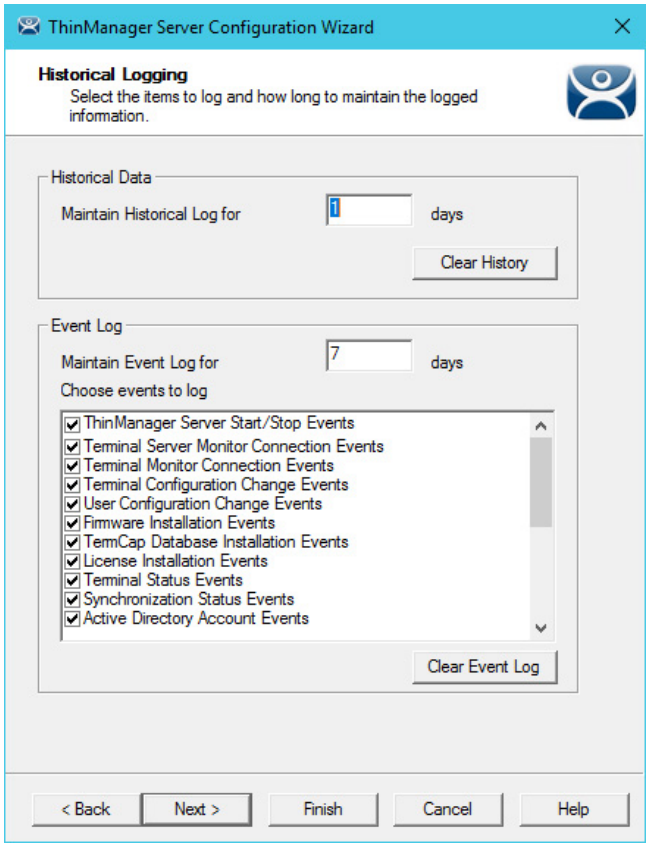
3. Have the appropriate hardware on the terminal, either a USB or Serial ProxCard reader.
4. Add the appropriate module.
5. Use the device once to have the device's identifier entered to the event log.
6. Open the ThinManager User Configuration Wizard and enter the ID number to tie the ThinManager User to the device.
7. Log in with the ID device.

Event Log

The Event Log is configured in the ThinManager Server Configuration Wizard.

1. Click the ThinManager Server icon to access the ThinManager Server branch of the ThinManager tree.
2. Double-click on the ThinManager Server icon or choose Edit>Modify from the menu to open the ThinManager Server Configuration Wizard.
3. Click Next until the Historical Logging page appears.

Figure 587 - Historical Logging Page



All events can be selected to be logged, but the ThinManager User Configuration changes checkbox is critical to the ThinManager Device detection.

4. Check ThinManager User Configuration changes and click Finish.

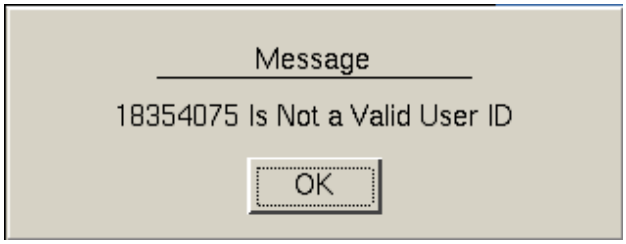
Device Identifier Number

Next, the HID card needs to be scanned to help find the ID number.

1. Pass the HID card over the pcProx Card scanner attached to a terminal.

   A ThinManager dialog box is displayed.

Figure 588 - ThinManager Dialog Box



The ID device does not work; so, the Terminal sends a message with the ID device's identifier number.

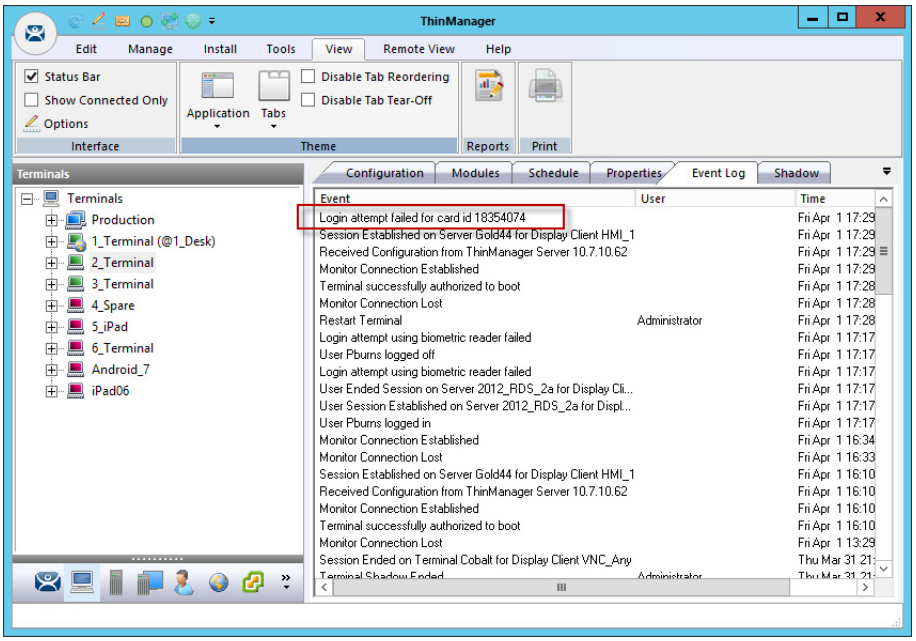
2. Record the number displayed.

   This number is also entered in the event log if the Terminal Events are checked in the ThinManager Server Configuration Wizard.

3. Open ThinManager.
4. Highlight the Terminal in the tree and click the Event Log tab.

   The ID for the device is entered in the log.

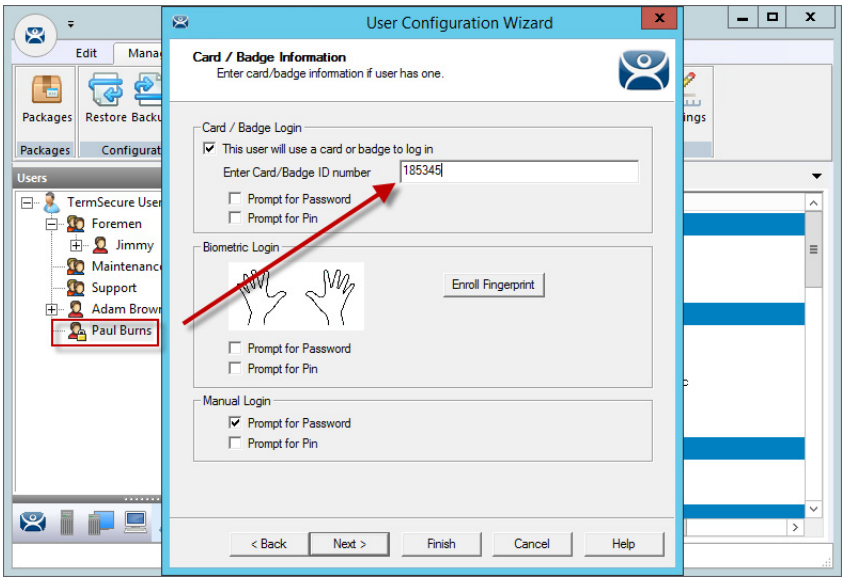
Figure 589 - ThinManager Event Log



Next, the ID number needs to be associated with the ThinManager User.

5. Open the ThinManager User Configuration Wizard for the user you want to associate with that ID card.
6. Click Next until the Card/Badge Information page appears.

Figure 590 - Card/Badge Information Page



7. In the Card/Badge Login section, check This user will use a card or badge to log in.
8. Type the ID Identifier from the earlier steps into the Enter Card/Badge ID number field.

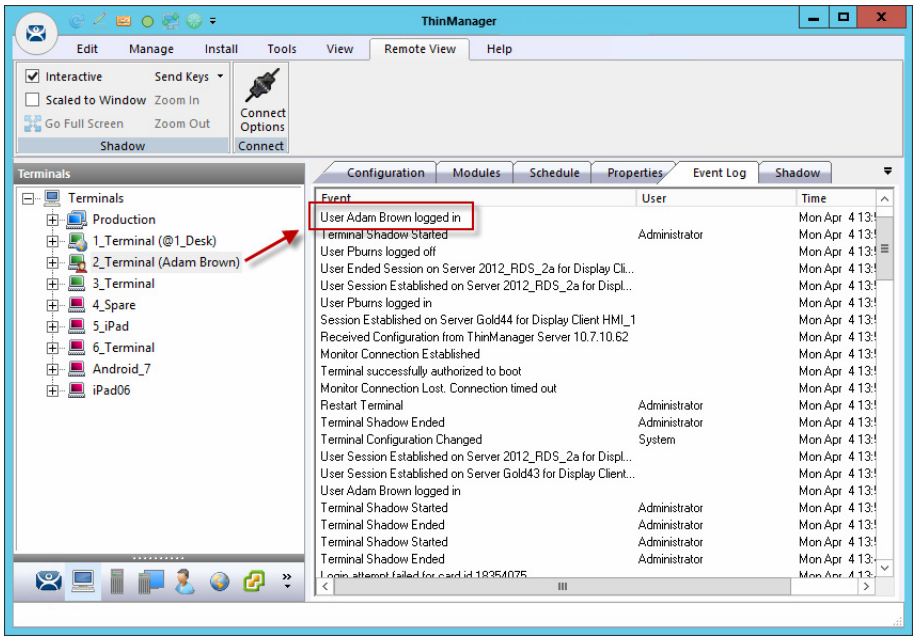
Check Prompt for Password or Prompt for Pin for the Card/Badge Login, the Biometric Login, or a Manual Login to require a secondary credential.

Setting	Description
Prompt for Password	Check to require the user to enter their password.
Prompt for Pin	Check to require the user to enter their PIN.

Now, the Terminal is configured, the ID device is identified, and the ThinManager User is configured to use the device.

9. Click Finish to complete the configuration.

Figure 591 - Event Log



10. Rescan the card that now is associated with a ThinManager User account.

The Event Log shows the results of the successful login. The terminal has the ThinManager User added to its icon in the tree, while the ThinManager User icon shows the name of the terminal into which it is logged.

Fingerprint Reader

ThinManager supports the DigitalPersona UareU models 4500 and 5160 fingerprint readers as biometric readers. These can be used as identifiers for ThinManager.

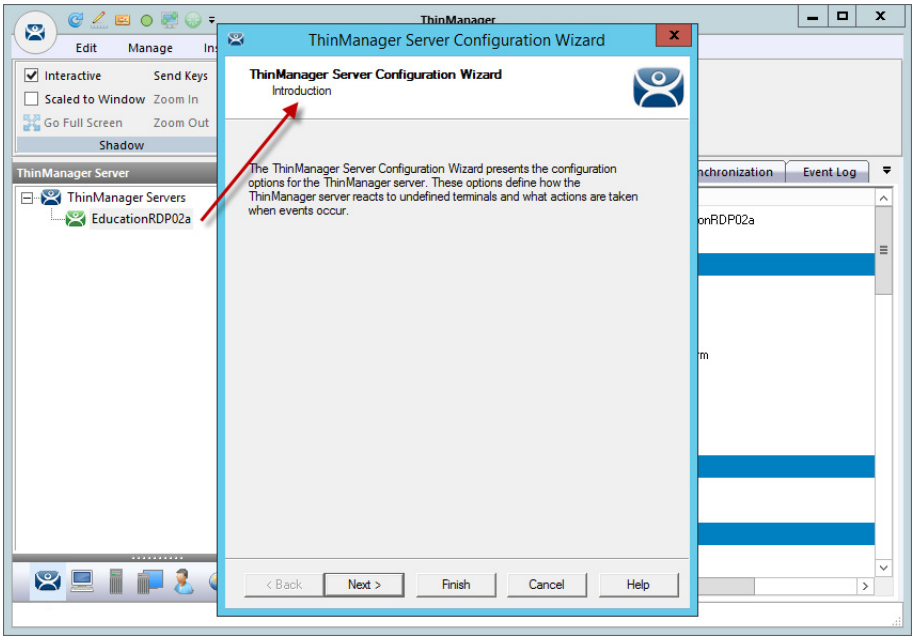
These are the requirements for the DigitalPersona UareU model 4500 fingerprint scanner.

- Activation in the ThinManager Server Configuration Wizard
- The unit is plugged into a terminal and the DigitalPersona UareU Fingerprint Reader module added to the terminal
- The user fingerprint scanned in ThinManager to associate a user with the fingerprint

Fingerprint Reader in ThinManager

The DigitalPersona UareU fingerprint reader must be activated in the ThinManager Server Configuration Wizard.

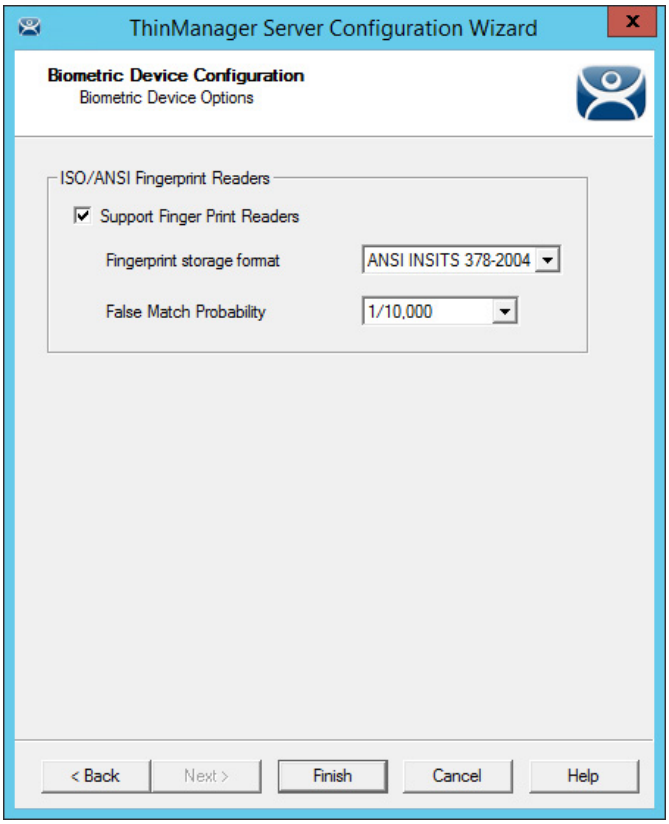
Figure 592 - ThinManager Server Configuration Wizard



1. Double-click on the ThinManager Server icon in the ThinManager branch of the ThinManager Server tree.

   The ThinManager Server Configuration Wizard appears.
2. Click Next until the Biometric Device Configuration page appears.

Figure 593 - Biometric Device Configuration Page



Setting	Description
Support Finger Print Readers	Check to enable the use of readers
Fingerprint storage format	Choose the data format you plan to use from the pull-down menu • ISO IEC 19794_2_2005 • ANSI INSITS 378_2004
False Match Probability	Sets the sensitivity of the read. 1/100 is less sensitive than 1/1,000,000

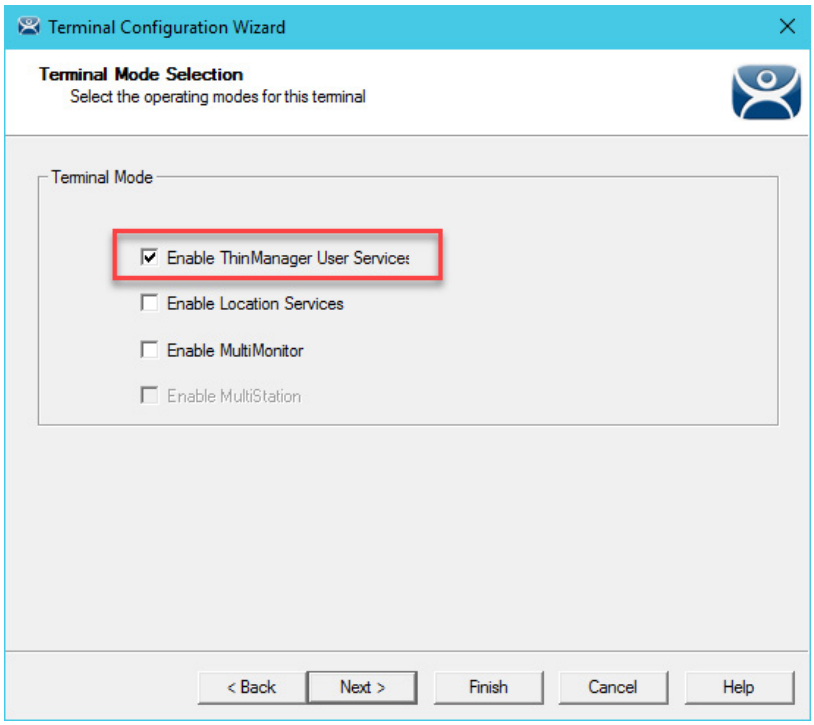
3. Click Finish to accept the changes.

Fingerprint Reader on the Terminal

You must add the DigitalPersona UareU Fingerprint Module to a Terminal if you plan to plug a DigitalPersona UareU fingerprint reader into the terminal.

1. Double-click on the terminal icon in the terminal branch of the ThinManager Server tree to open the Terminal Configuration Wizard.

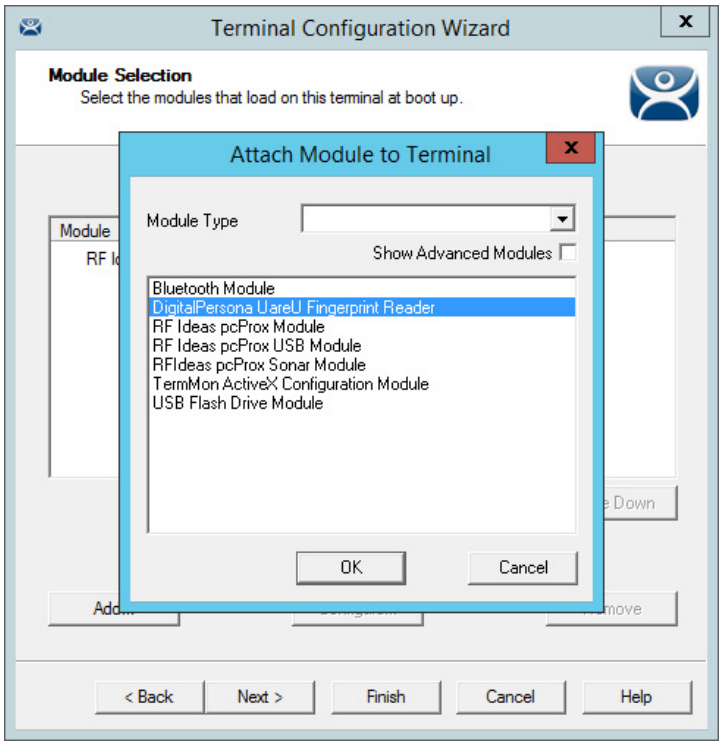
Figure 594 - Terminal Mode Selection Page



2. Click Next until the Terminal Mode Selection page of the Terminal Configuration Wizard appears.
3. Check Enable ThinManager User Services to make the fingerprint reader work with ThinManager.
4. Click Next until the Module Selection page appears.
5. Click Add on the Module Selection page.

   The Attach Module to Terminal dialog box appears.

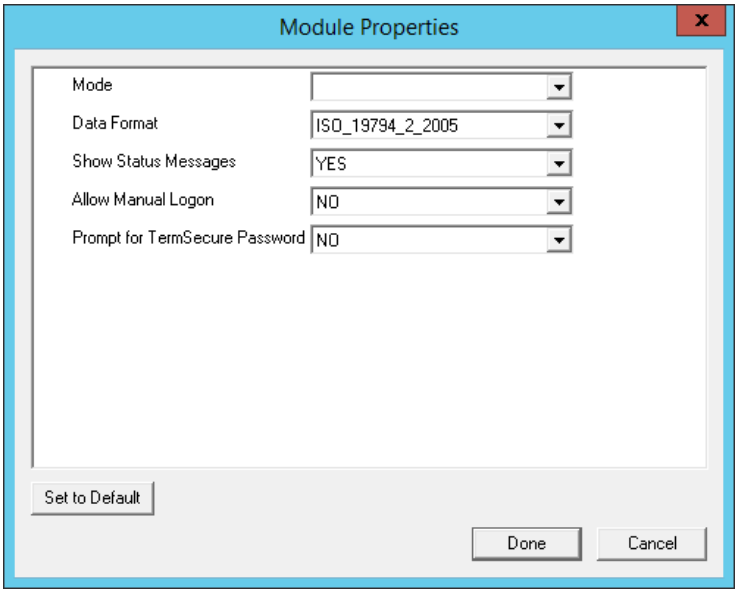
Figure 595 - Attach Module to Terminal



6. Choose Location Services from the Module Type pull-down menu, highlight the DigitalPersona UareU Fingerprint Reader module, and click OK to add the module to the Terminal.
7. On the Module Selection page, highlight the DigitalPersona UareU Fingerprint Reader module and click Configure.

   The Module Properties dialog box appears.

Figure 596 - DigitalPersona UareU Fingerprint Reader Module Properties



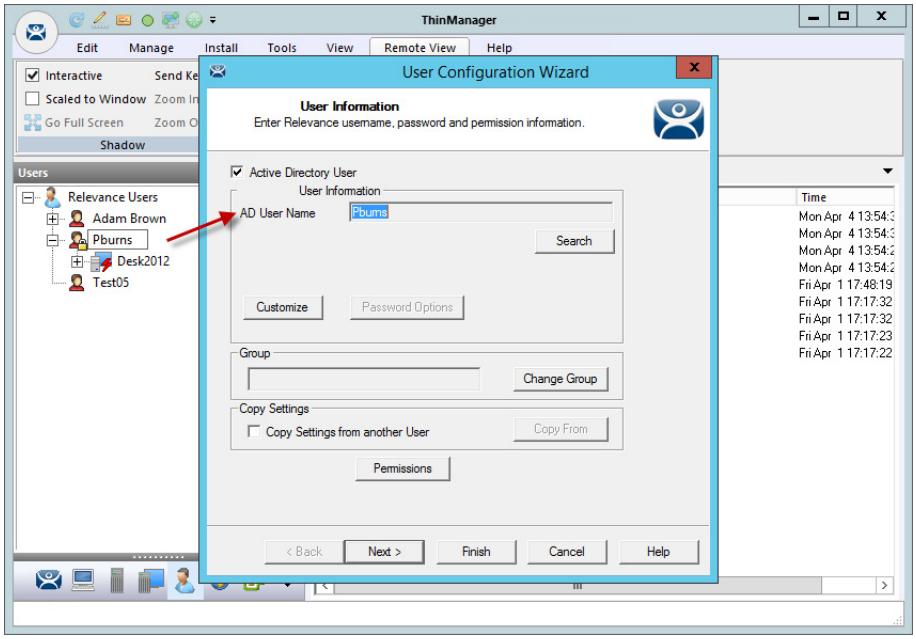
The DigitalPersona UareU Fingerprint Reader module has several configurable settings.

Setting	Description
Mode	Allows you to choose the Mode
ThinManager	Used to identify a ThinManager User
TermMon	Sends the fingerprint data to the TermMon ActiveX
TermMon Lookup	Allows the TermMon ActiveX to identify the user without the need for them to log in
Data Format	Sets the data format for the fingerprint reader. It should match the configuration in the ThinManager Server Configuration Wizard. These are the data formats. • ISO_19794_2_2005 • ANSI_378_2004 • DigitalPersona
Show Status Messages	Set to YES to show a brief message in the upper-right corner of the Terminal for each fingerprint reader event
Allow Manual Logon	Set to NO so that a user must use the fingerprint reader to log on. Set to YES to use the fingerprint scanner or log on manually.
Prompt for ThinManager Password	Set to YES for the user to be required to enter a password in addition to the fingerprint scan. Set to NO so the fingerprint scan is enough to allow a log on.

Fingerprint Reader for the ThinManager User

Fingerprint data is associated with a user in the ThinManager User Configuration Wizard.

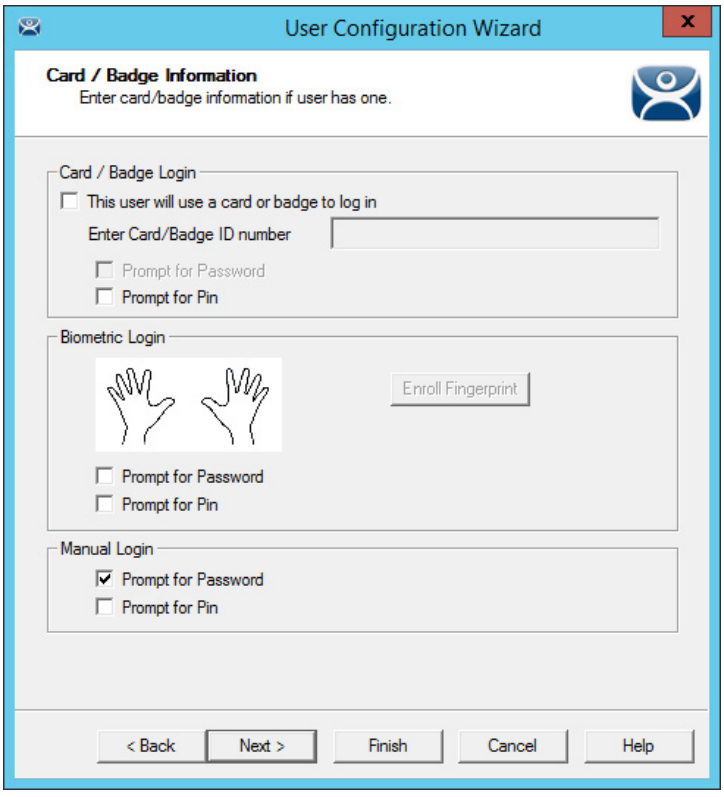
Figure 597 - ThinManager User Configuration Wizard



1. Open the ThinManager Users branch of the ThinManager tree and double-click on the ThinManager User whose fingerprints you want to register.

   The ThinManager User Configuration Wizard appears.

Figure 598 - Card/Badge Information Page



Setting	Description
Prompt for Password	Check to require the user to enter a password
Prompt for Pin	Check to require the user to enter a PIN

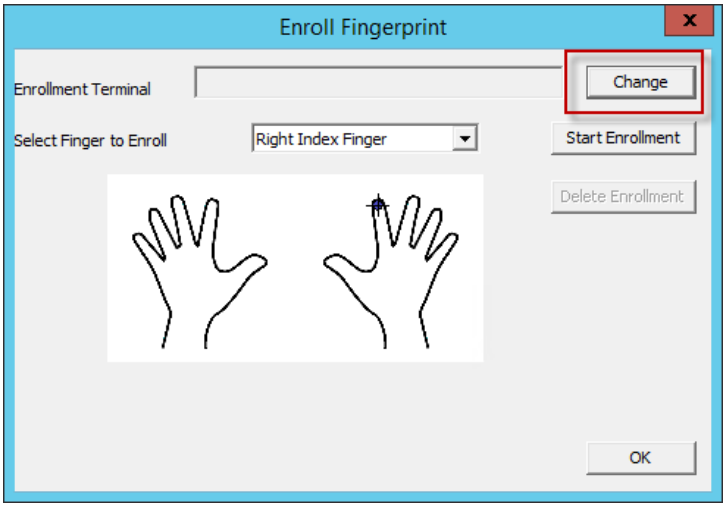
Check Prompt for Password or Prompt for Pin for the Card/Badge Login, the Biometric Login, or a Manual Login to require a secondary credential.

The Card/Badge Information page has an Enroll Fingerprint button that begins the registration process.

1. Click Enroll Fingerprint.

   The Enroll Fingerprint dialog box appears.

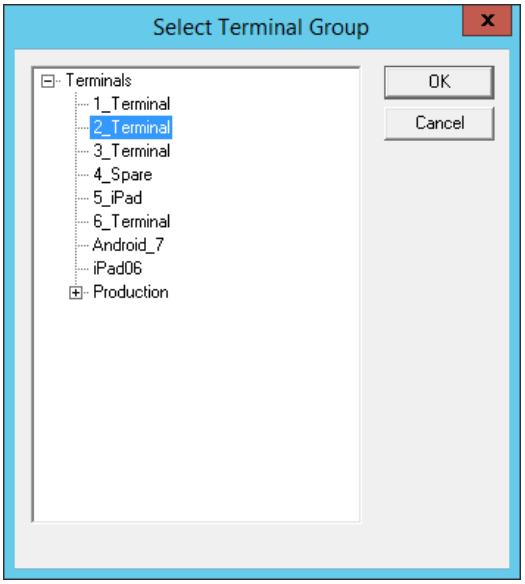
Figure 599 - Enroll Fingerprint



2. Click Change.

   The Select Terminal Group dialog box appears, where you can select the Terminal that has the fingerprint scanner to use for registration.

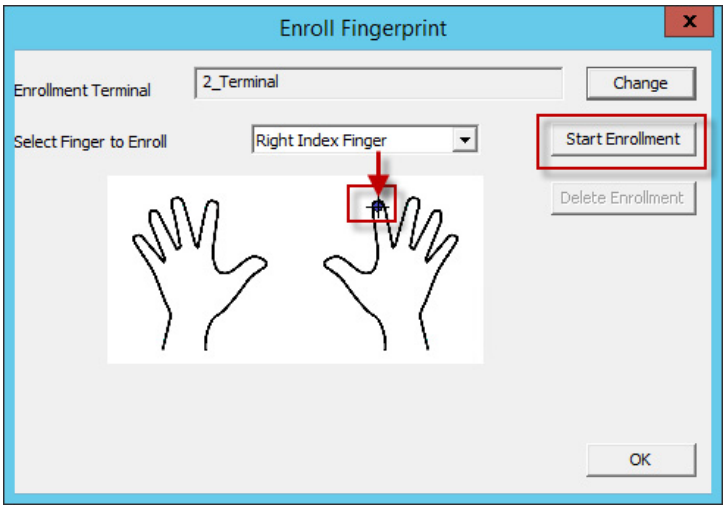
Figure 600 - Select Terminal Group Dialog Box



3. Highlight the terminal that has the fingerprint scanner to use for registration and click OK.

   Now, this terminal is registered as the Enrollment Terminal in the Enroll Fingerprint dialog box.

Figure 601 - Enroll Fingerprint



4. Choose the finger you want to enroll in the Select Finger to Enroll pull-down menu.

   A crosshair appears on the finger chosen.

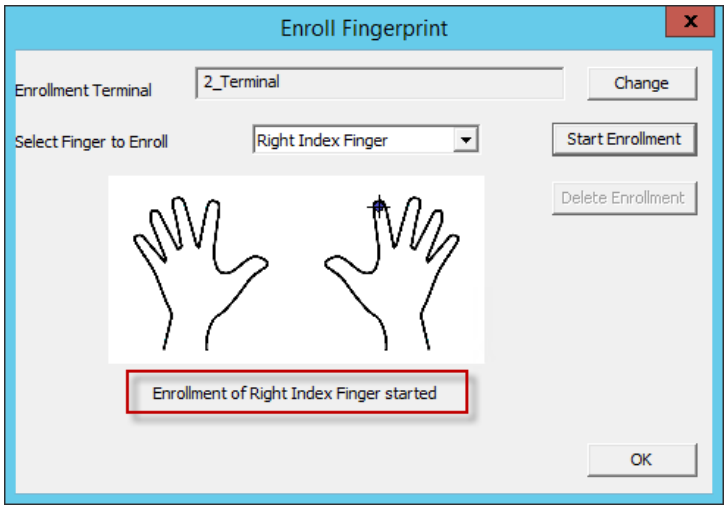
5. Click Start Enrollment.

The enrollment requires four scans of the fingerprint.

6. Place the finger on the scanner.

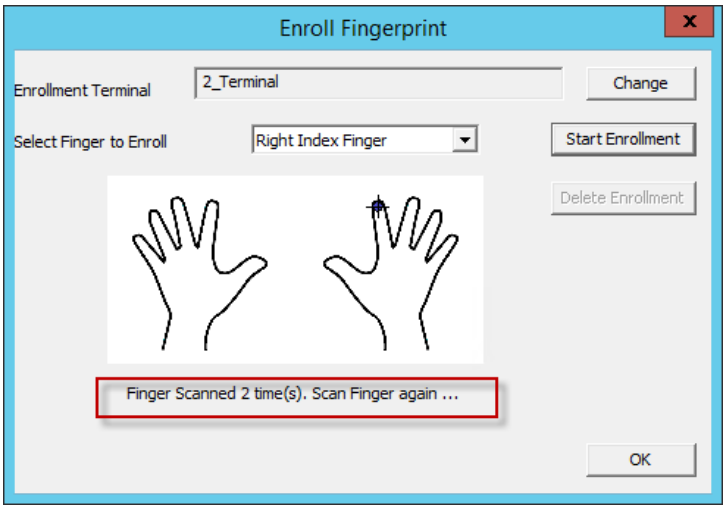
   The blue light should turn red, and then back to blue. Leave the finger on the scanner until the red light turns off.

Figure 602 - Enrollment Started



A status message indicates progress.

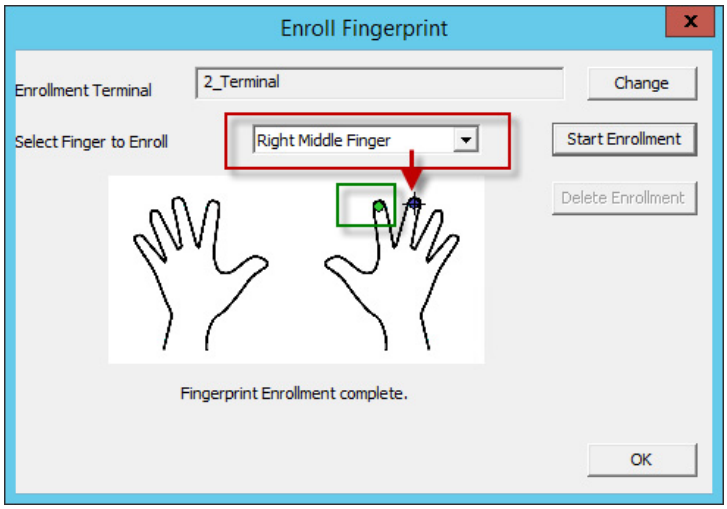
Figure 603 - Scan Status



The enrollment requires four scans of the fingerprint.

7. Repeat until complete.

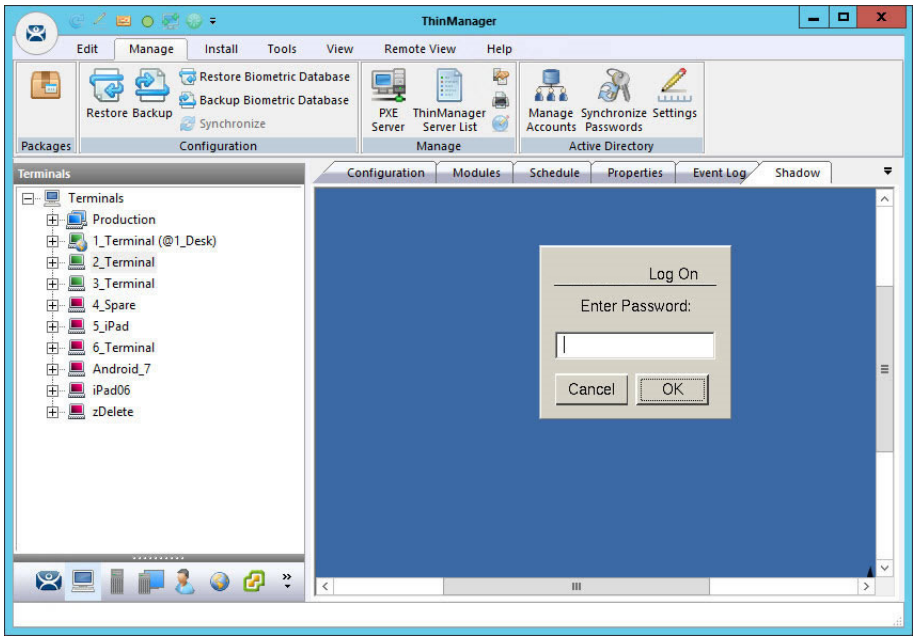
Figure 604 - Enroll New Finger



Once the finger has been scanned and enrolled, the scanned finger appears green in the Enroll Fingerprint dialog box.

8. Choose a new finger from the Select Finger to Enroll pull-down menu.

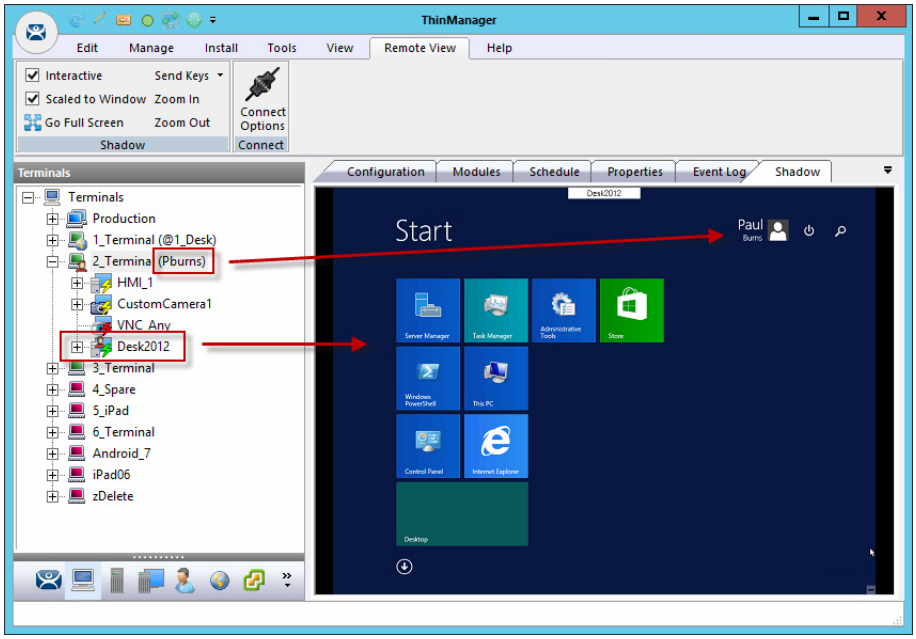
Figure 605 - Shadow of a Terminal Scan



If Prompt for Password was checked on the Card/Badge Information page, then a dialog box appears with a request for the Windows password for the Windows account. See Figure 598 on page 421.

Figure 606 on page 425 shows a ThinManager User logged in to a terminal that uses a DigitalPersona UareU Fingerprint Reader.

Figure 606 - Shadow of a Terminal Scan



The Terminals icon shows a user logged in, it names the user, and the Desktop2012 application shows a user login to show that display client was assigned through the ThinManager User.

Location Services

Location Services is mobile computing based on location. It does not just send an application to a mobile device, but it 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.

Location Services is the *how* to provide *what* you need, *where* and *when* you need it.

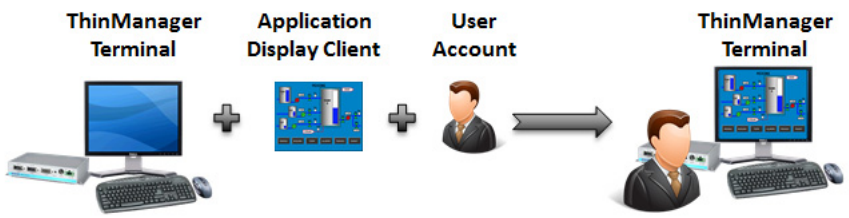
There are two types of locations in Location Services: Assigned and Unassigned.

Assigned locations are those that have a terminal and monitor at the given location, much like traditional computing. Location Services adds functions to the location that allow mobile devices to interact with it. These interactions include Shadow the terminal, Clone the applications, or Transfer the control of the location to the mobile device.

Unassigned locations are those that lack a permanent terminal and monitor, and all of the content is sent to the mobile device.

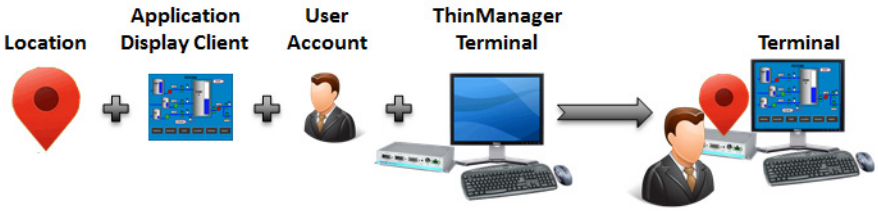
In ThinManager, to deploy applications, define a terminal and configure it with applications and a user account, which allows the operator to access needed applications. See Figure 607 on page 426.

Figure 607 - ThinManager Deployment



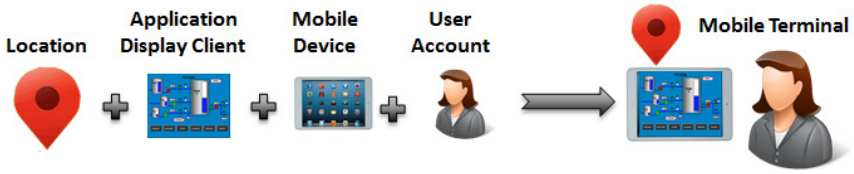
The Location Services method starts with location creation. The application, user account, and terminal are added to the location. See Figure 608.

Figure 608 - Assigned Location



Location Services can deploy applications to locations without terminals. Your mobile device becomes the terminal. See Figure 609 on page 427.

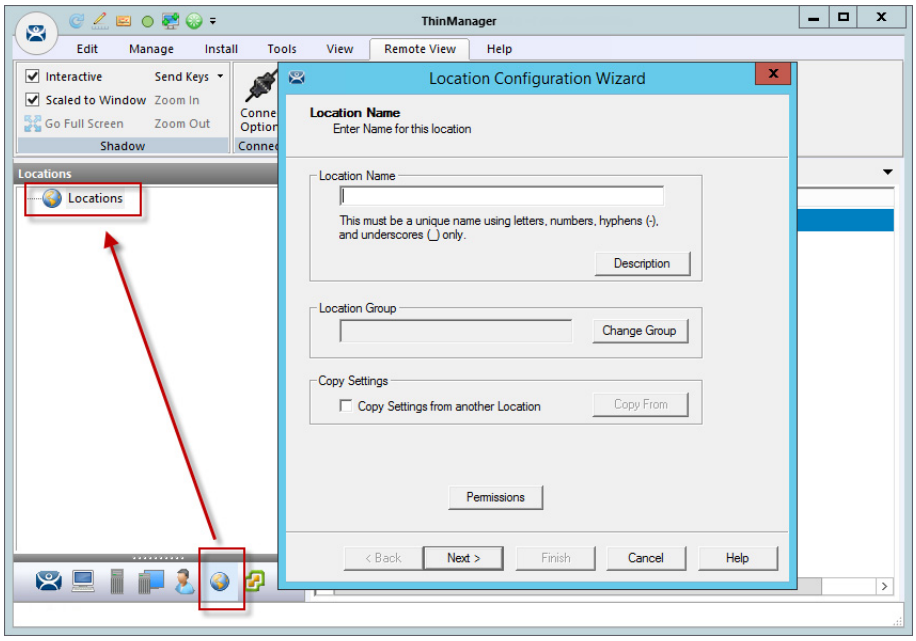
Figure 609 - Unassigned Location



Create 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 is then be assigned to the terminal.

Figure 610 - Location Configuration Wizard

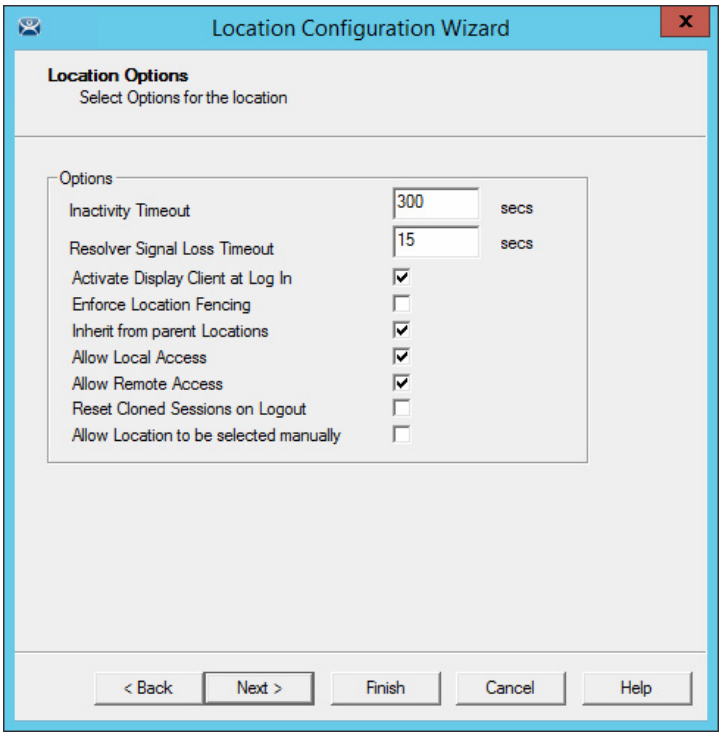


1. Click the Locations (globe) icon in the Tree Selector at the bottom of the tree to open the Locations branch.
2. Right-click on the Locations branch and choose Add Location.

   The Location Configuration Wizard appears.
3. Type the Location Name in the field.
4. Click Next to continue.

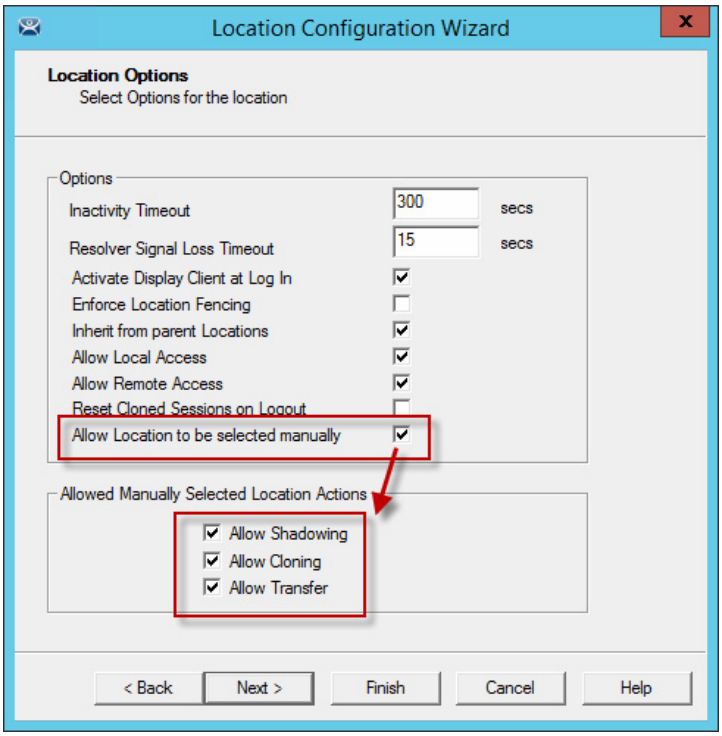
The Location Options page has several configurable options that control the remote access.

Figure 611 - Location Options Page



Setting	Description
Inactivity Timeout	Time interval in which a ThinManager user is logged off for inactivity.
Resolver Signal Loss Timeout	Time interval before a ThinManager user is logged off due to lack of a signal.
Activate Display Client at Log In	Check to bring the display client to the forefront when the ThinManager user logs in.
Enforce Location Fencing	Check to control access in an area with nested locations. If local fencing is enforced, the user must be within the fence to access the sub-locations.
Inherit from parent Locations	Check to allow nested sub-locations to inherit the parent display clients.
Allow Local Access	Check to allow a ThinManager user to access the location from that location. Clear this checkbox to allow remote access only.
Allow Remote Access	Check to allow a ThinManager user to access the location from a remote site. Clear this checkbox to allow access at the location only.
Reset Cloned Sessions on Logout	Check to close any cloned sessions once they are disconnected.
Allow Location to be selected manually	Check to allow a location to be selected manually and dynamically reveal settings under Allowed Manually Selected Location Actions. Clear this checkbox to require the ThinManager user to use a Resolver like QR Codes, Wi-Fi, or Bluetooth™ to initiate the location access.

Figure 612 - Location Options Page

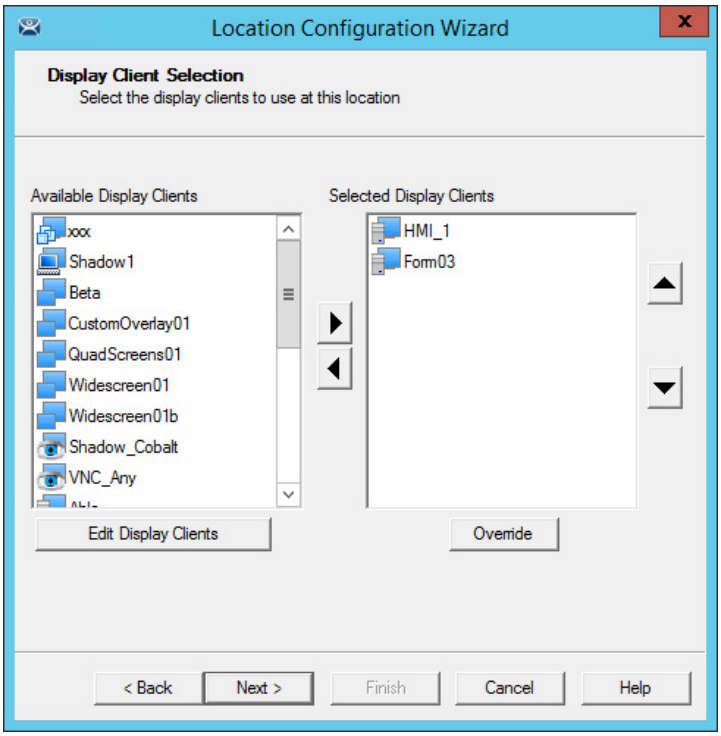


These are the actions you can select manually. You can allow all or none. The defaults are fine, but you have the option to customize the settings as needed.

Setting	Description
Allow Shadowing	Check to allow a duplicate of the display to be shown on mobile device.
Allow Cloning	Check to allow the user to launch the same applications as the location but using their Windows account.
Allow Transfer	Check to allow the display to be moved from the location to the mobile device.

5. Choose the manual connections of your choice. Cleared checkboxes are not available in the manual selection menu.

Figure 613 - Remote Desktop Server Selection

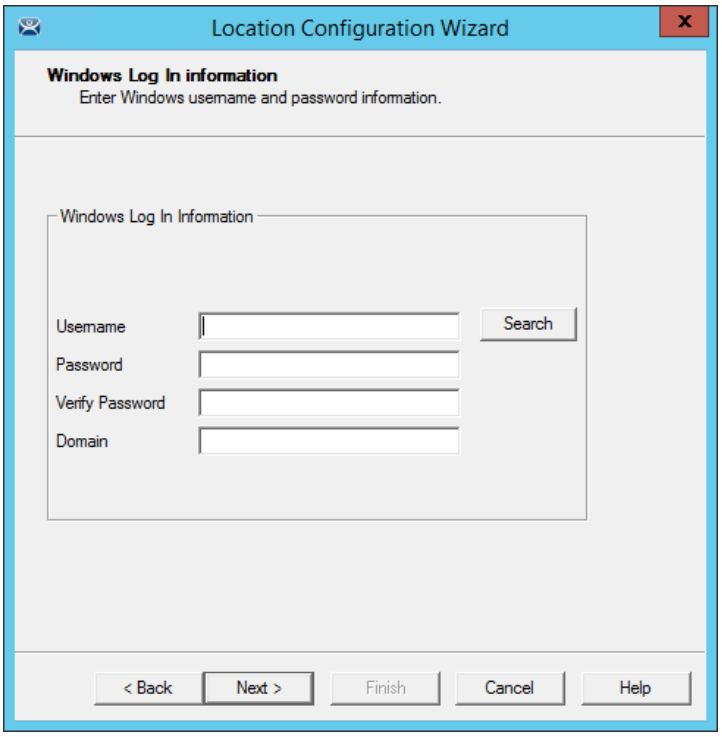


6. Select the display clients you want displayed on the Location.
7. Click Override.

   The Override Settings dialog box appears, which allows you to add a different user name to a highlighted display client.
8. Apply the desired display clients to the location and click Next to continue.

A location with a display client requires a Windows username.

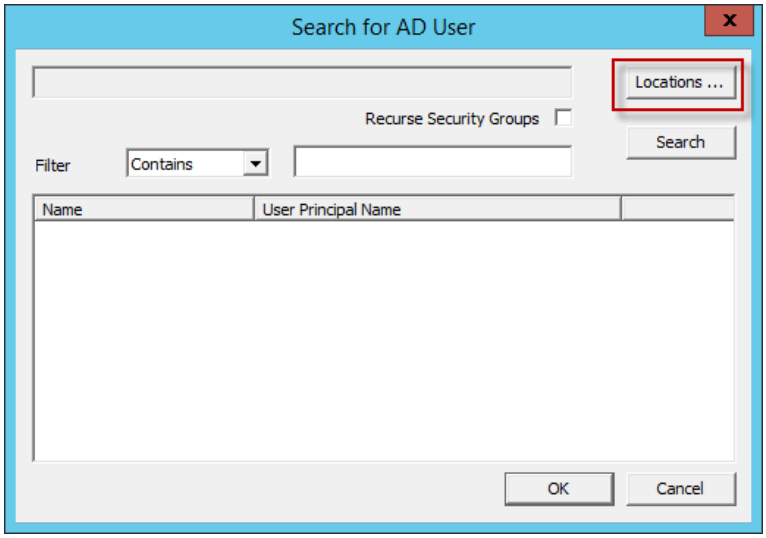
Figure 614 - Windows Log In Information



Setting	Description
Username	Type a valid Windows username.
Password	Type the password.
Verify Password	Type the password.
Domain	Click Search and the Search for AD User dialog box appears.

The Search for AD User window allows you to reference users from the Active Directory.

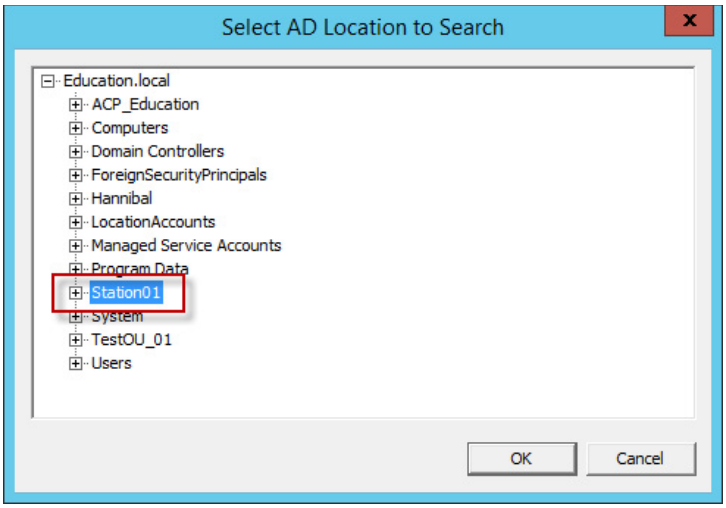
Figure 615 - Search for AD User



9. Click Locations.

   The Select AD Location to Search dialog box appears, where you can choose users.

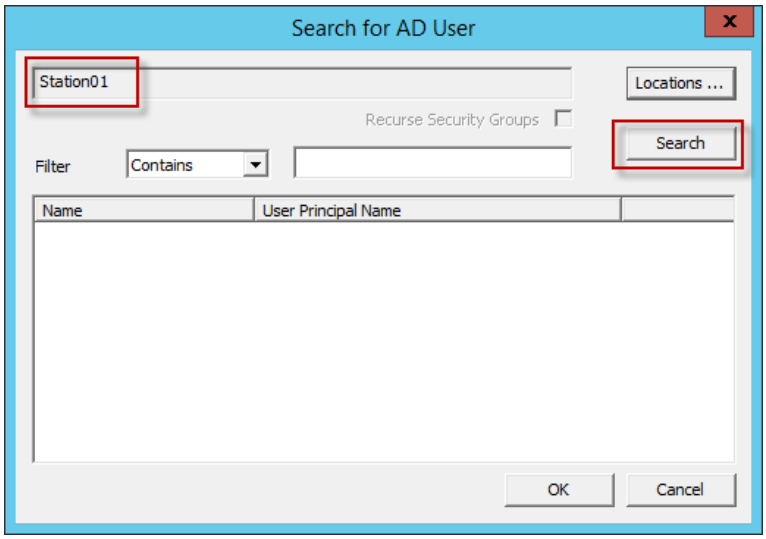
Figure 616 - Select AD Location to Search



10. Highlight the domain branch you want to use and click OK.

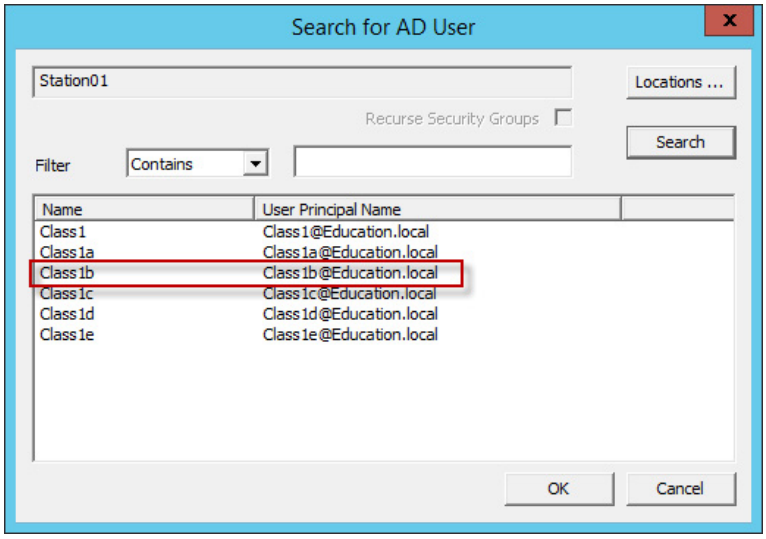
    The Location for the search is added.

Search for AD User



11. Click Search to fetch the user accounts and populate the Search for AD User dialog box.

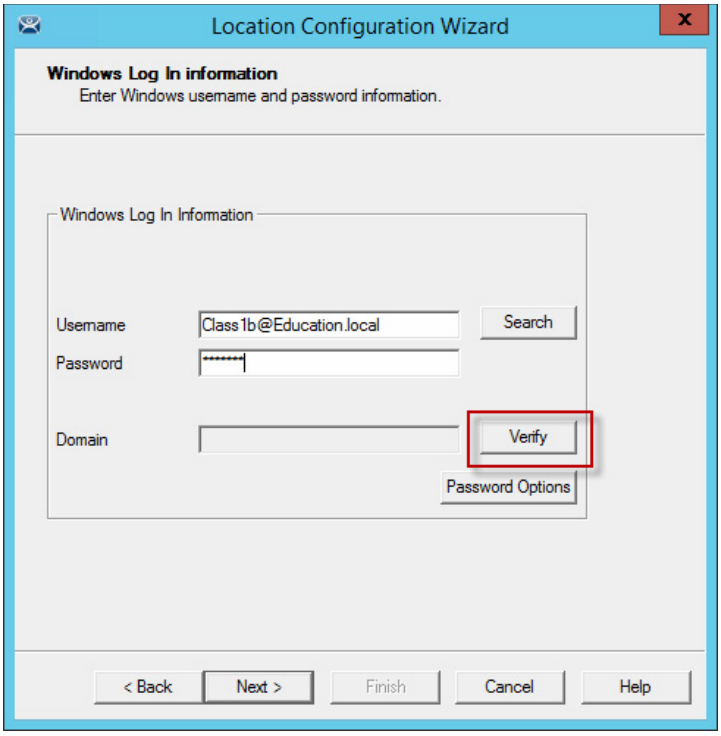
Figure 617 - Populated Search for AD User



12. Highlight the domain user you want and click OK.

    This references the user for the terminal log in account. The Location is now configured to use an Active Directory user account.

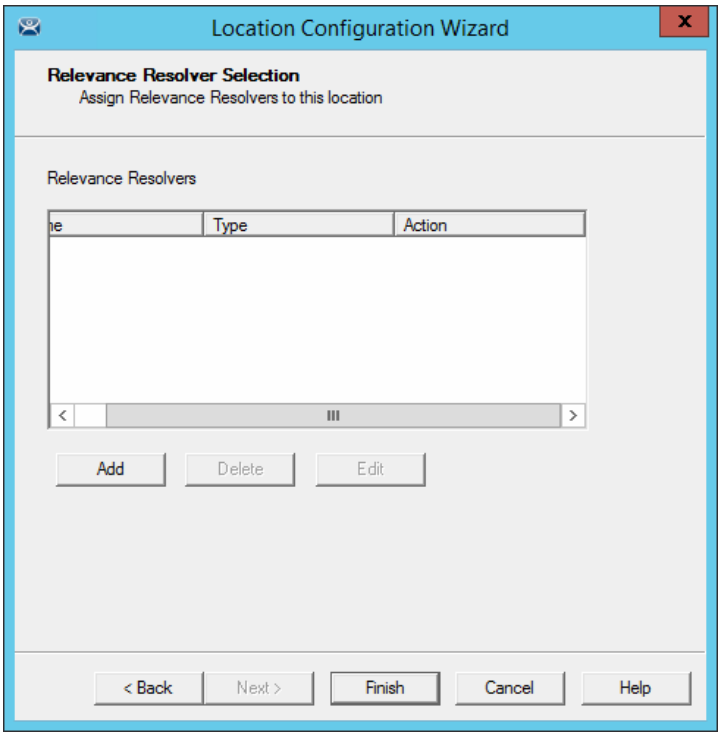
Figure 618 - Windows Log In Information Page



13. Select Next to continue.

    The Location Services Resolver Selection page appears, which allows the association of Resolvers to the location.

Figure 619 - Location Services Resolver Selection Page

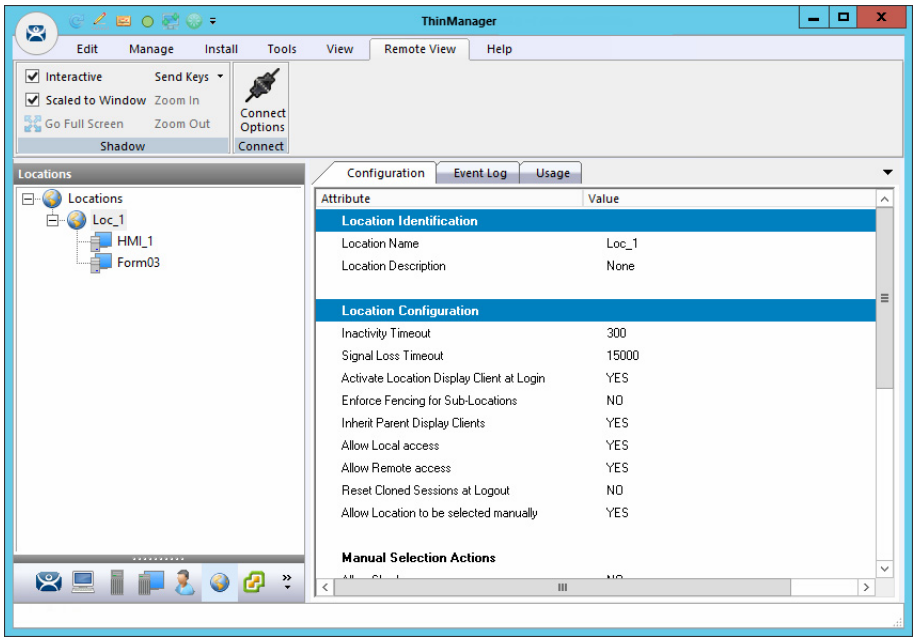


These are the Resolvers.

- QR Codes
- Bluetooth® Beacons
- Wi-Fi Access Points
- GPS

14. Click Finish to create the Location.

Figure 620 - Location with Assigned Display Clients



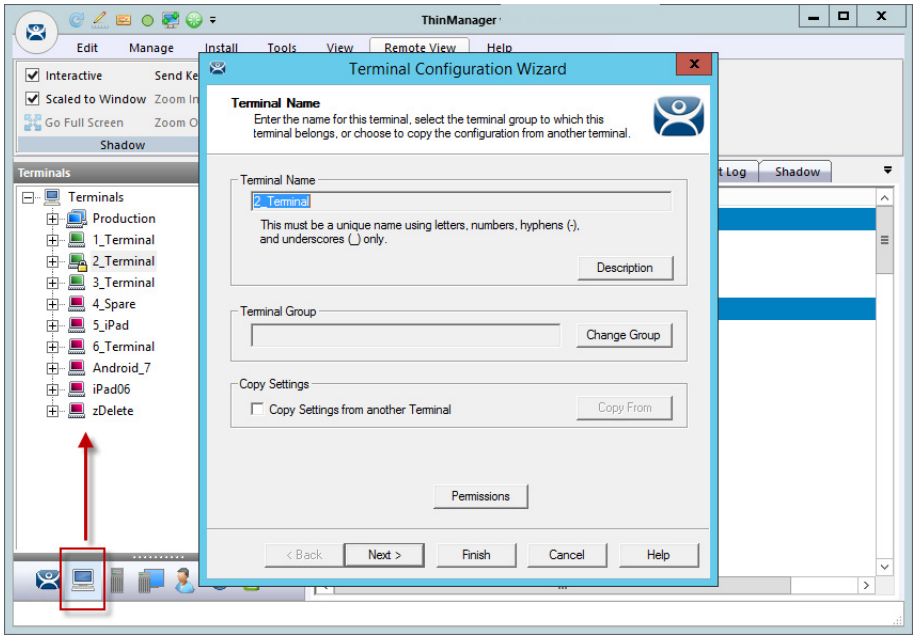
The Location tree shows the created Locations and the display clients assigned to it.

Add a Location to a Terminal

Now, the newly created location must be attached to a Terminal.

These instructions show how to add a Location to an already configured Terminal. You can create the Terminal from scratch and add the location as you configure the Terminal.

Figure 621 - Terminal Configuration Wizard

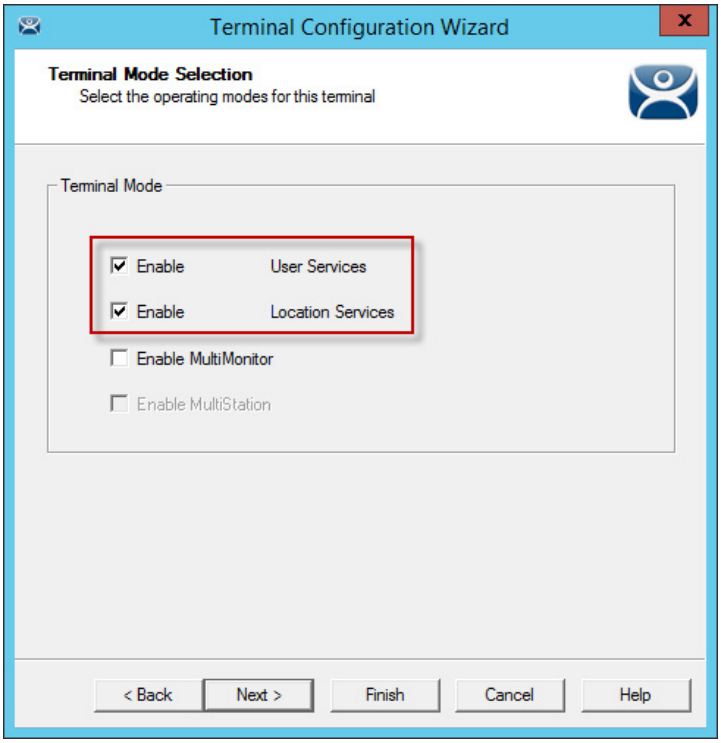


1. Click the Terminal icon on the Tree Selector at the bottom of the tree.

   The Terminals branch appears.
2. Double-click a Terminal or right-click and choose Modify.

   The Terminal Configuration Wizard appears.

Figure 622 - Terminal Mode Selection Page

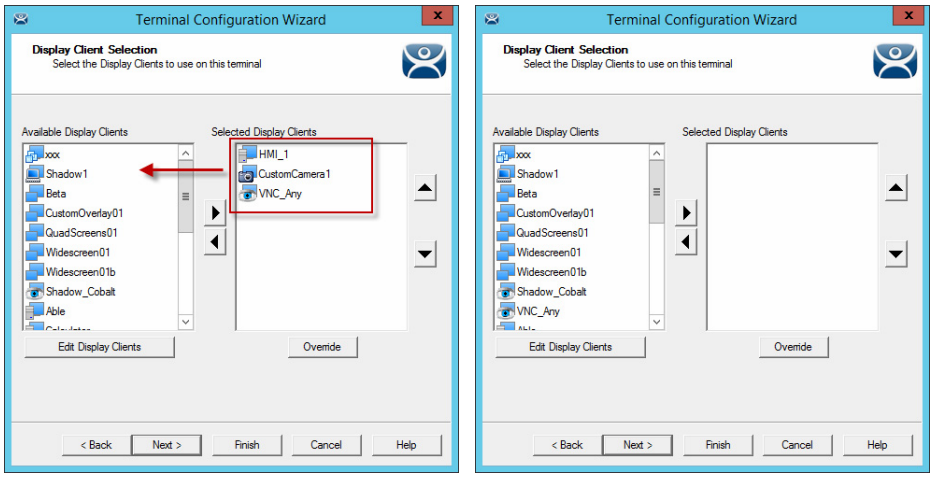


3. Click Next until the Terminal Mode Selection page appears. There are ThinManager User and Location Services checkboxes.

Setting	Description
Enable ThinManager User Services	Check to use the ThinManager User Access to control access to applications.
Enable Location Services	Check to allow the Terminal to use Locations in its configuration.

4. Check Enable Location Services to use Locations.
5. Click Next to navigate to the Display Client Selection page.

Figure 623 - Remove Display Clients on the Display Client Selection Page



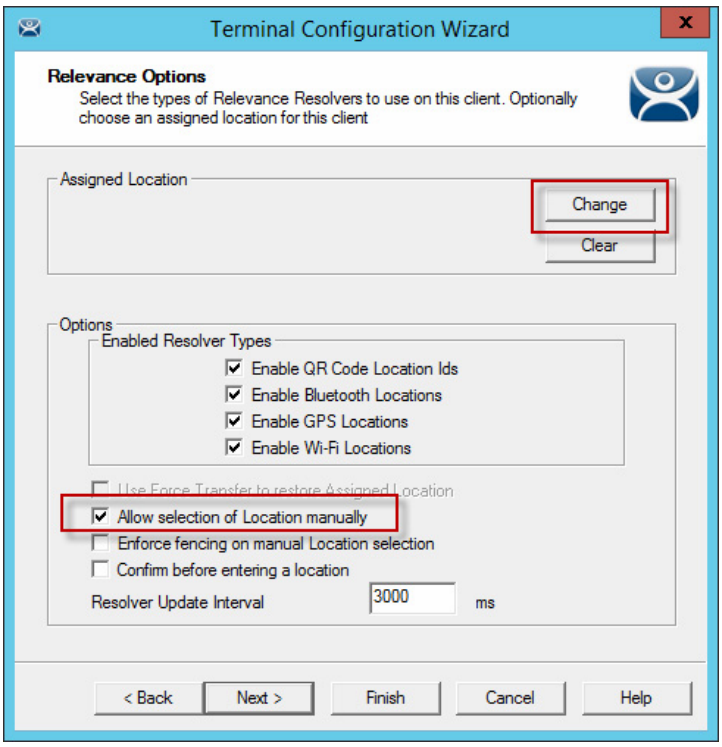
6. Highlight the display clients that already exist in the Selected Display Clients list and click the left arrow to remove them from a Terminal that already exists.

   Leave the Selected Display Clients list blank if you want to configure a new terminal.

The user accesses the display clients through the location, not the Terminal.

7. Click Next and continue to the Location Services Options page.

Figure 624 - Location Services Options Page



Choose Options prior to a Location. Once the Location is assigned, Options are locked. Click Clear to clear the Location if you need to change an option, and then reassign the Location.

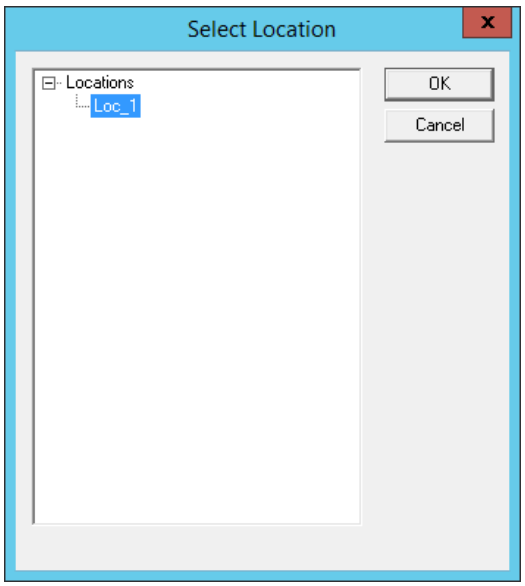
Options	Description
Use Force Transfer to restore Assigned Location	Check to allow the operator to take a transferred session back without the need to wait for the other device to approve of the transfer.
Allow selection of Location manually	Check to let the user manually select the location from a menu on the mobile device. Clear the checkbox so the user must use a Resolver.
Enforce fencing on manual Location selection	Check to enforce the fencing on a location during manual selection.
Confirm before entering a location	Check so you are notified as you enter a fence and asks for an acknowledgment.
Enable Resolver Types	Location Services has several methods to resolve the location to allow specific applications to get sent to specific locations.
Enable QR Code Location Ids	Check to allow the scanning of a QR code to determine the location.
Enable Bluetooth Locations	Check to allow the use of Bluetooth beacons to determine the location.
Enable GPS Locations	Check to allow the Global Positioning System of the mobile device to determine the location.
Enable Wi-Fi Locations	Check to allow the signal strength of Wi-Fi access points to determine the location.

Each method selected requires configuration to associate a location with the Resolver data.

8. Click Change.

   The Select Location dialog box appears with the created Locations displayed in the Selection Location tree.

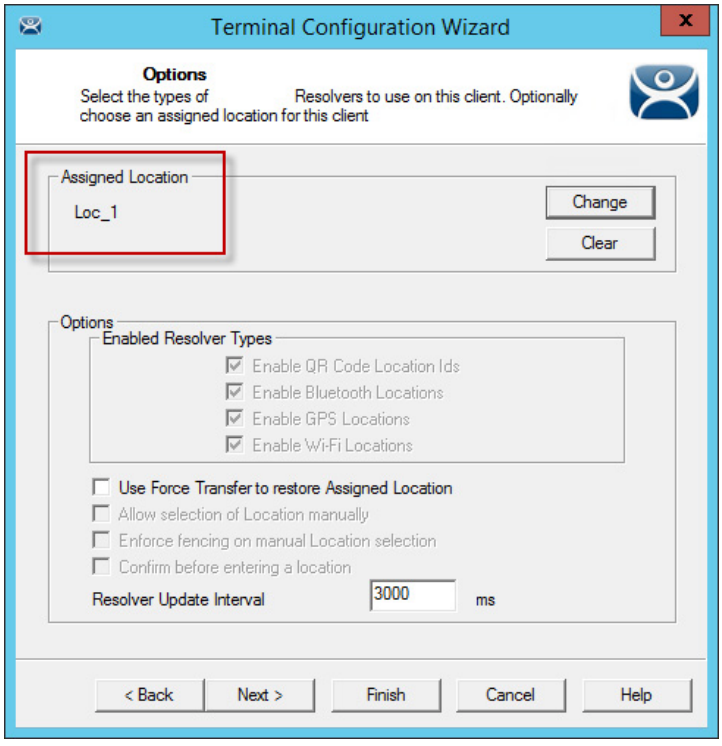
Figure 625 - Select Location Dialog Box



9. Highlight the desired Location and click OK.

   The Location is displayed in the Assigned Location field once it is assigned to the Terminal.

Figure 626 - Location Assigned

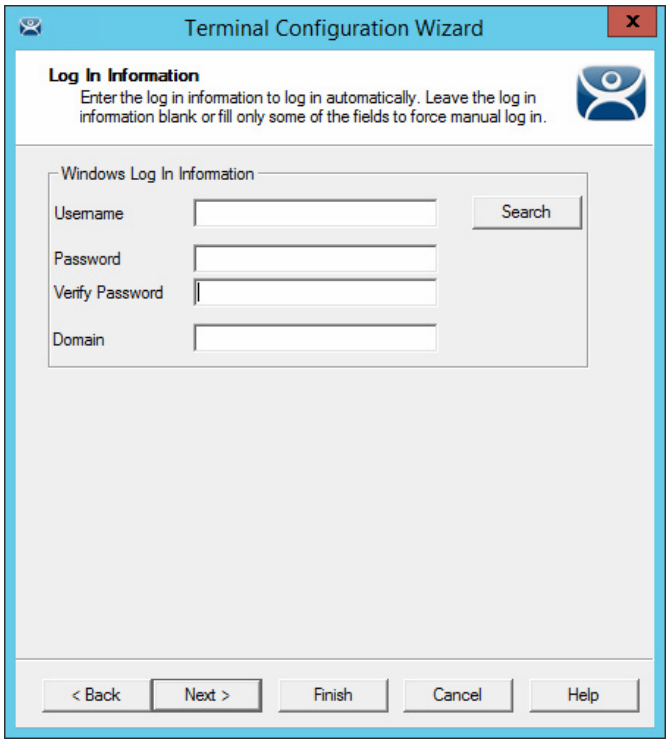


Once the Location is assigned, the Options are locked.

If you need to change an option, click Clear, change the option, and then reassign the Location.

10. Once the location is assigned, click Next until the Log In Information page appears.

Figure 627 - Log In Information Page



Typically, a preconfigured Terminal is assigned a user account to allow it to log in to the servers. However, this is not needed now because it uses the user account assigned to the location.

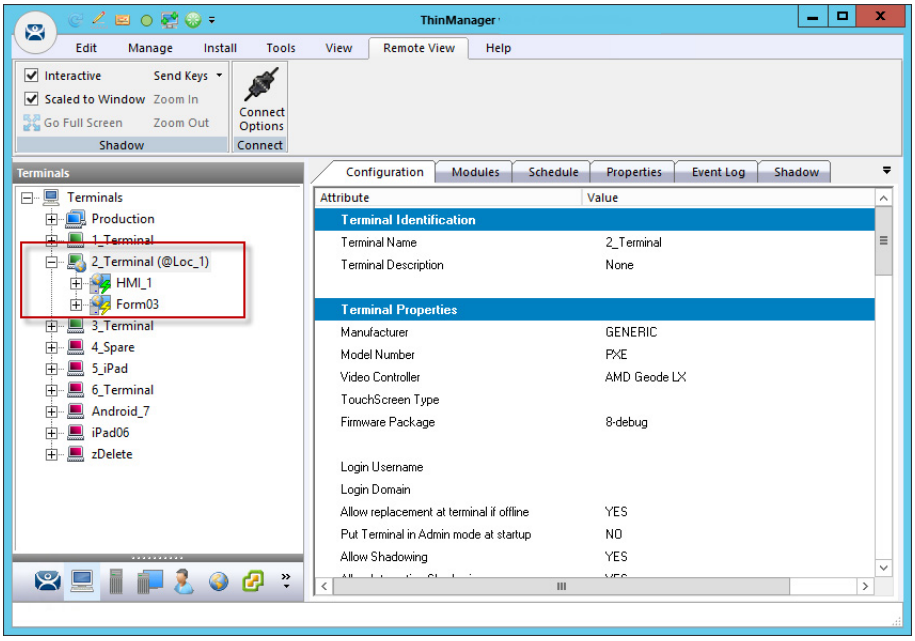
11. Leave the Username and Password fields blank.
12. Once the Username is cleared, click Finish to complete the wizard.

Once the wizard is closed, you must restart the Terminal to load the changes.

13. Right-click on the Terminal in the tree and choose Restart Terminal to load the new configuration.

    The application now runs on the location that is assigned to the Terminal.

Figure 628 - Locations on Terminals in Terminal Tree



The tree shows location icons to show which display clients are from the location.

In Figure 628, the terminal 2_Terminal is using location Loc_1.

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 Location Services makes is when a mobile device interacts with the location.

Mobile Device Interactions with Location Services

When you add a location to a Terminal, it does not seem like it makes any difference. The application runs the same on the Terminal versus a location on a Terminal. The difference is the mobile-device interaction a user can have with that location.

Configuration of mobile devices is covered in Mobile Devices on page 315.

ThinManager uses Resolvers to define the location.

- Manual Selection – allows user to select the location manually from a menu on the mobile device
- QR Code – can be created to define a location
- Bluetooth – allows the use of Bluetooth beacons to determine the location
- GPS – allows the Global Positioning System of the mobile device to determine the location
- Wi-Fi – allows the signal strength of Wi-Fi access points to determine the location
- iBeacon – the Apple® Inc. version of Bluetooth

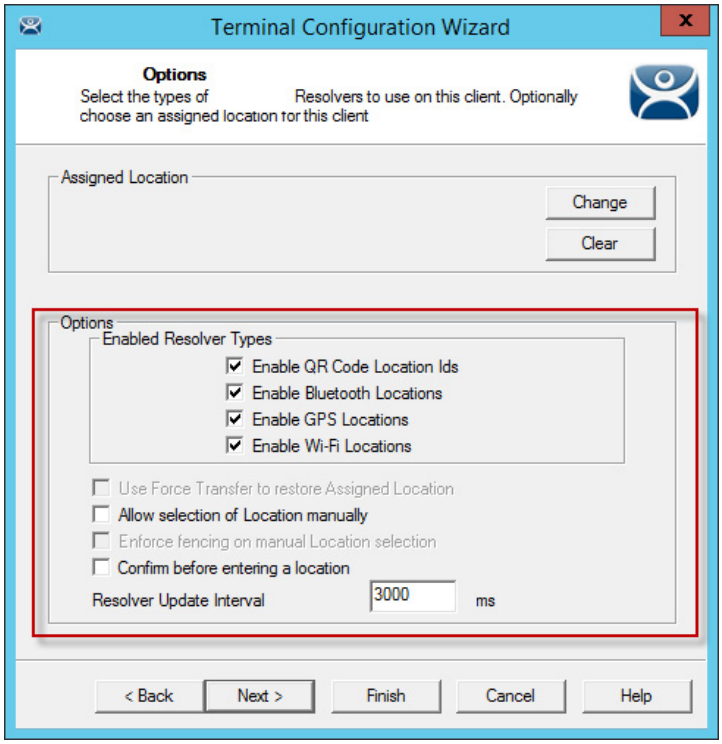
Resolvers are identified and marked using the mobile device; so, it is important to configure a mobile device to identify the resolvers in Location Services.

- 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 website at http://downloads.thinmanager.com/

Two pages of the Terminal Configuration Wizard enable mobile devices.

The first page that covers interaction with a Location is the Location Services Options page, which lets you select which Resolver methods you want to use. These are listed in the Enable Resolver Types section.

Figure 629 - Location Services Options



1. Check the Resolvers you want to use and Allow selection of Location manually.

   Each method selected requires configuration to associate a location with the Resolver data.

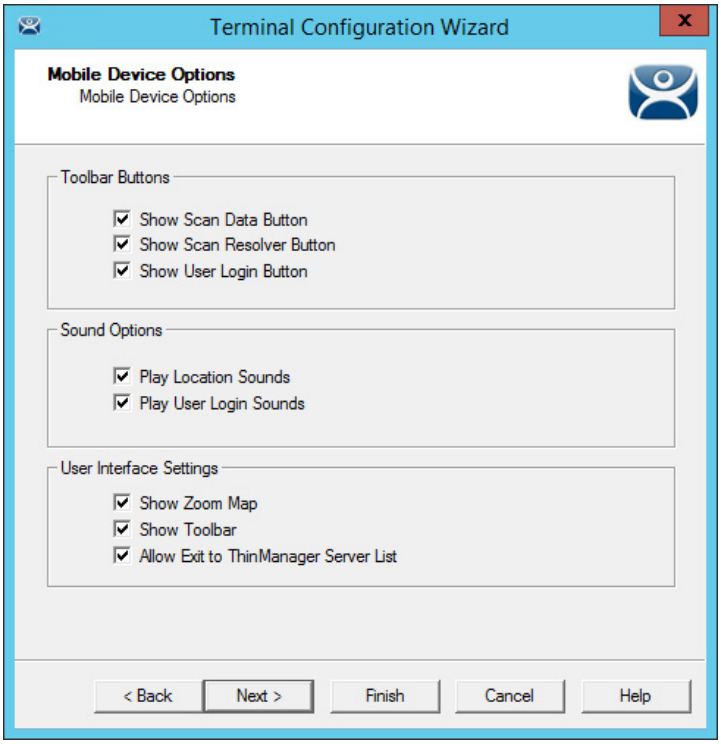
These are the Options.

Options	Description
Use Force Transfer to restore Assigned Location	Check to allow the operator to take a transferred session back without the need to wait for the other device to approve of the transfer.
Allow selection of Location manually	Check to let the user manually select the location from a menu on the mobile device. Clear the checkbox so the user must use a Resolver.
Enforce fencing on manual Location selection	Check to enforce the fencing on a location during manual selection.
Confirm before entering a location	Check so you are notified as you enter a fence and asks for an acknowledgment.
Enable Resolver Types	Location Services has several methods to resolve the location to allow specific applications to get sent to specific locations.

Options	Description
Enable QR Code Location Ids	Check to allow the scanning of a QR code to determine the location.
Enable Bluetooth Locations	Check to allow the use of Bluetooth beacons to determine the location.
Enable GPS Locations	Check to allow the Global Positioning System of the mobile device to determine the location.
Enable Wi-Fi Locations	Check to allow the signal strength of Wi-Fi access points to determine the location.

2. Click Next to navigate to the Mobile Device Options page, which has several settings that control the user experience on mobile devices. This page allows you to disable features normally displayed in the mobile applications.

Figure 630 - Mobile Device Options



Options	Description
Toolbar Buttons	
Show Scan Data Button	Clear this checkbox to hide the Scan Data button.
Show Scan Resolver Button	Clear this checkbox to hide the Scan Resolver button.
Show User Login Button	Clear this checkbox to hide the User Login button.
Sound Options	
Play Location Sounds	Check to play a sound when a location is entered.
Play User Login Sounds	Check to play a sound when the user logs in as a TermSecure or ThinManager user.
User Interface Settings	
Show Zoom Map	Clear to hide the screen map while zoomed in.
Show Toolbar	Clear to hide the app toolbar.
Allow Exit to ThinManager Server List	Clear to prevent the user from leaving the app to switch ThinManager Servers.

3. Click Finish to complete the configuration of the mobile Terminal.

Locations

Unassigned Locations

Location Services allows you to deploy applications to mobile devices not tethered to a physical location. You can create a location, deploy applications to it, and access these applications 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.

Create an Unassigned Location

Figure 631 on page 444 uses GPS so that when the mobile user enters the area, the appropriate applications are delivered to the user.

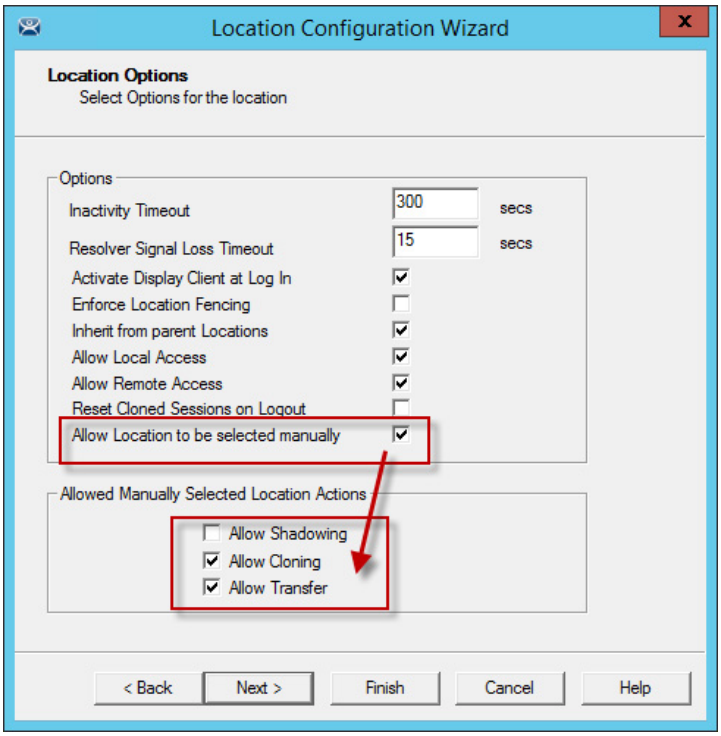
1. Click the Locations icon in the Tree Selector.

   The Locations branch of the tree appears.
2. Right-click on the Locations branch and choose Add Location.

   The Location Configuration Wizard appears, opened at the Location Name page.
3. Type a Location Name and click Next.

   The Location Options page appears.

Figure 631 - Location Options Page



The Location Options page has several configurable options that control the remote access.

Option	Description
Inactivity Timeout	Type a time interval (in seconds) after which an inactive ThinManager user logged off.
Resolver Signal Loss Timeout	Type a time interval (in seconds) before a ThinManager user is logged off due to lack of a signal.
Activate Display Client at Log In	Check to bring the display client to the forefront when the ThinManager user logs in.
Enforce Location Fencing	Check to control access in an area with nested locations. If local fencing is enforced, the user must be within the fence to access the sub-locations.
Inherit from parent Locations	Check to allow nested sub-locations to inherit the parent display clients.
Allow Local Access	Check to allow a ThinManager user to access the location from that location. Clear this checkox to allow remote access only.
Allow Remote Access	Check to allow a ThinManager user to access the location from a remote site. Clear this checkbox to allow access at the location only.
Reset Cloned Sessions on Logout	Check to close any cloned sessions once they are disconnected.
Allow Location to be selected manually(1)	Check to allow a location to be selected manually. Clear this checkbox to require the ThinManager user to use a Resolver like QR Codes, Wi-Fi, or Bluetooth® to initiate the location access. When checked, the following options dynamically appear.
Allow Manually Selected Location Actions	Check the actions you can manually select. You can allow all, or none.
Allow Shadowing	This option is not supported in Unassigned Locations as there is no Terminal to shadow.
Allow Cloning	Check to allow the user to launch the same applications as the location, but use the Windows account of the mobile device.
Allow Transfer	Check to allow the display to be shown on the mobile device with the Windows account of the Unassigned Location.

(1) This option lets you manually choose the location from the mobile device. Clear the checkbox to rely on another resolver, like QR code or Bluetooth, to choose the location.

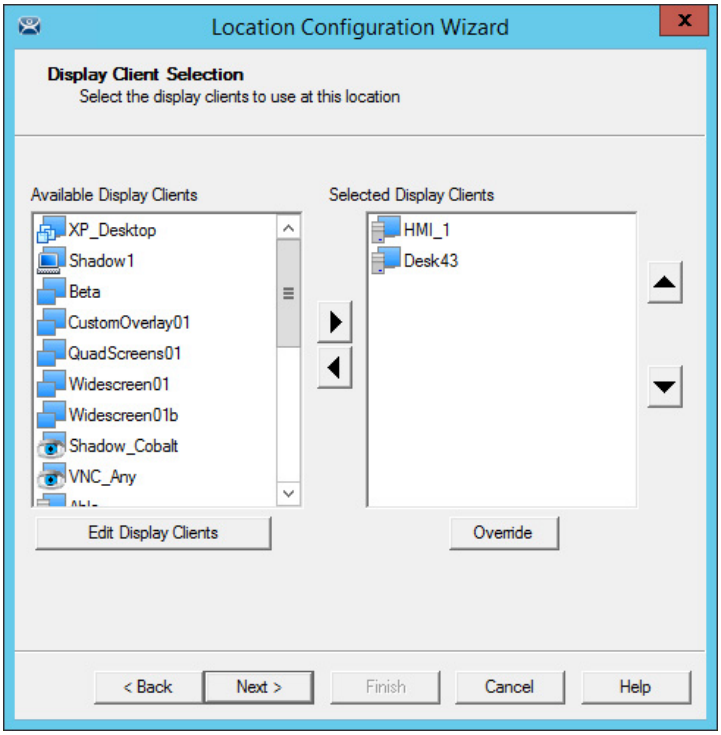
Unassigned Locations do not support Shadow. Therefore, the Allow Shadowing checkbox is clear in Figure 631 on page 444. Allow Cloning and

Allow Transfer are checked in Figure 631 on page 444. The defaults are fine, but you have the option to customize the settings as needed.

4. Click Next to continue.

   The Display Client Selection page appears.

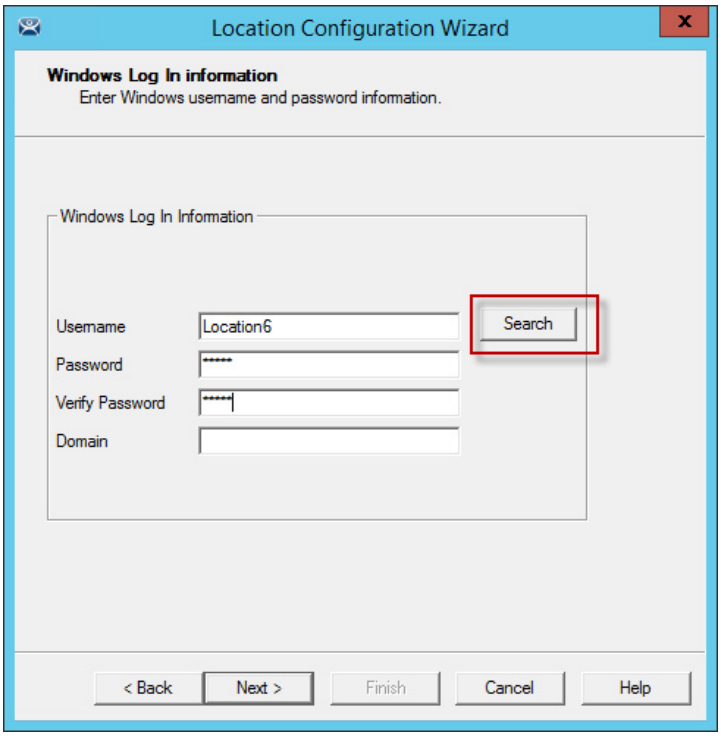
Figure 632 - Display Client Selection Page



5. Add the display clients you want on the Remote Desktop Server Selection page.
6. Click Next to continue.

   The Windows Log In Information page appears.

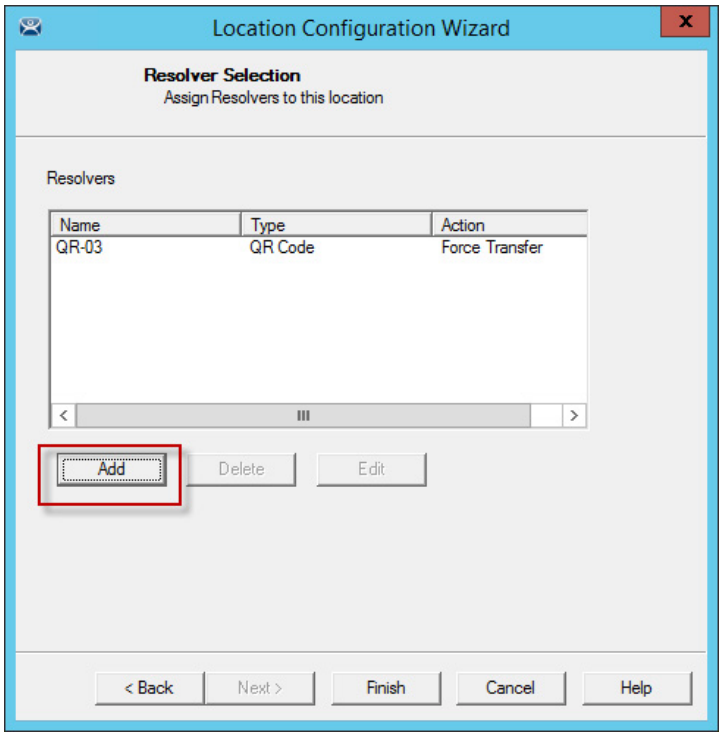
Figure 633 - Windows Log In Information Page



7. Type a Windows user account into the Username field.
8. Click Search to use an Active Directory user as described in Search for Active Directory User on page 257.
9. Click Next to continue.

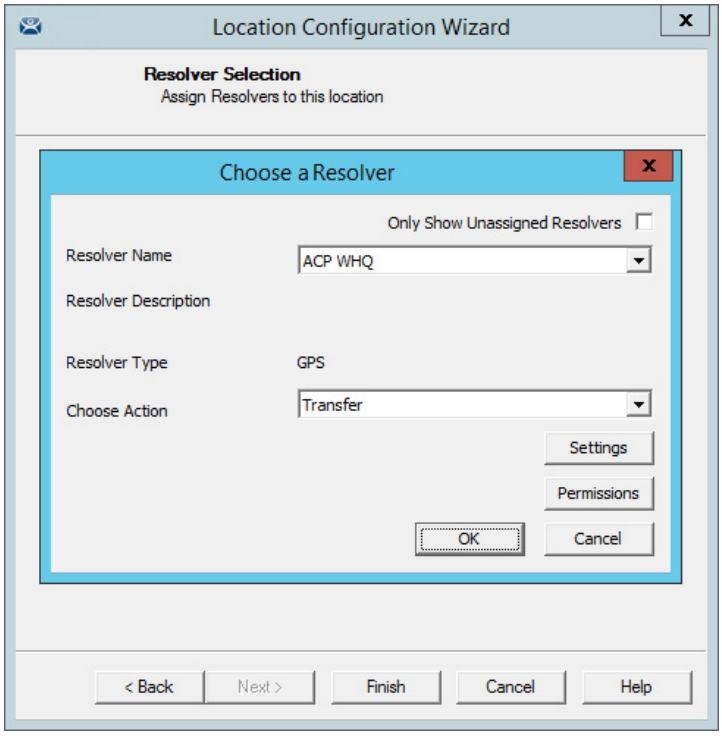
   The Resolver Selection page appears.

Figure 634 - Resolver Selection Page



10. Click Add to add the resolver on the Resolver Selection page and add an action.

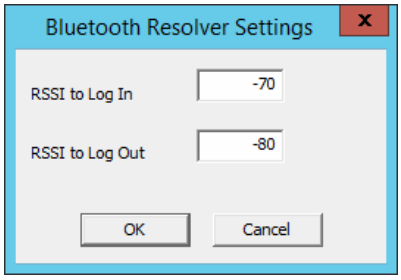
Figure 635 - Choose a Resolver Page



11. Choose a resolver from the Resolver Name pull-down menu.
12. Choose the action from the Choose Action pull-down menu.
13. Click OK to accept the configuration.

There is a Settings button for the resolvers.

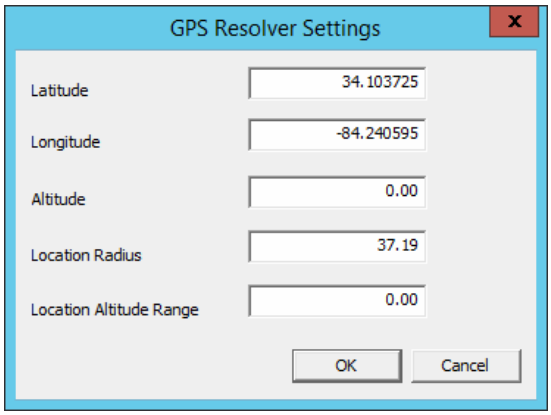
Figure 636 - Bluetooth Resolver Settings



Option	Description
RSSI to Log In	A relative value that determines when a device automatically logs on.
RSSI to Log Out	A relative value that determines when a device automatically logs out.

The Bluetooth Resolver Settings dialog box shows 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 through the subtraction of 10 from the RSSI to Log In value.

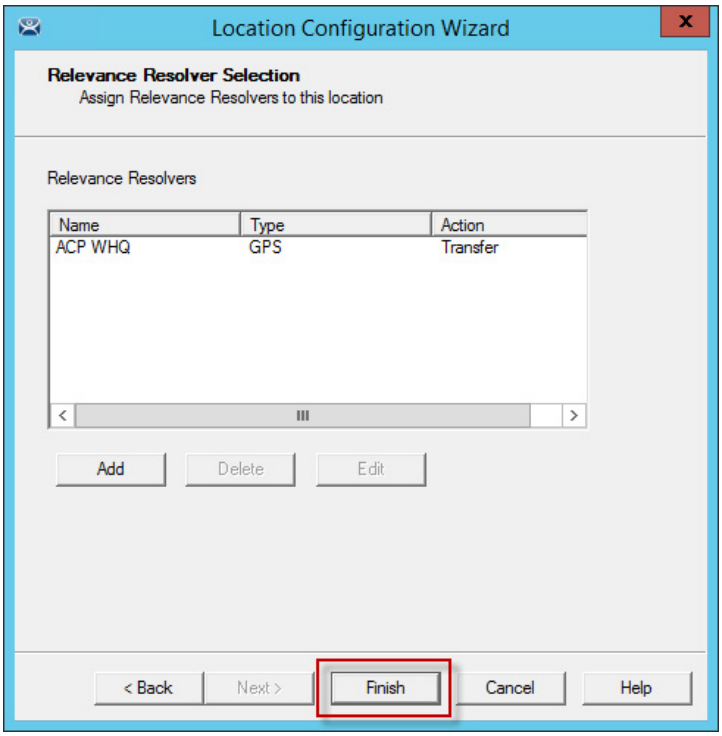
Figure 637 - GPS Settings



Option	Description
Latitude	The Fractional Latitudinal Coordinate in Degrees.
Longitude	The Fractional Longitudinal Coordinate in Degrees.
Altitude	The altitude trigger of the GPS Point.
Location Radius	The trigger Radius of the GPS Point in meters.
Location Altitude Range	The range along the Z-axis, in meters, that the mobile device is supposed to enter to be considered active at the location.

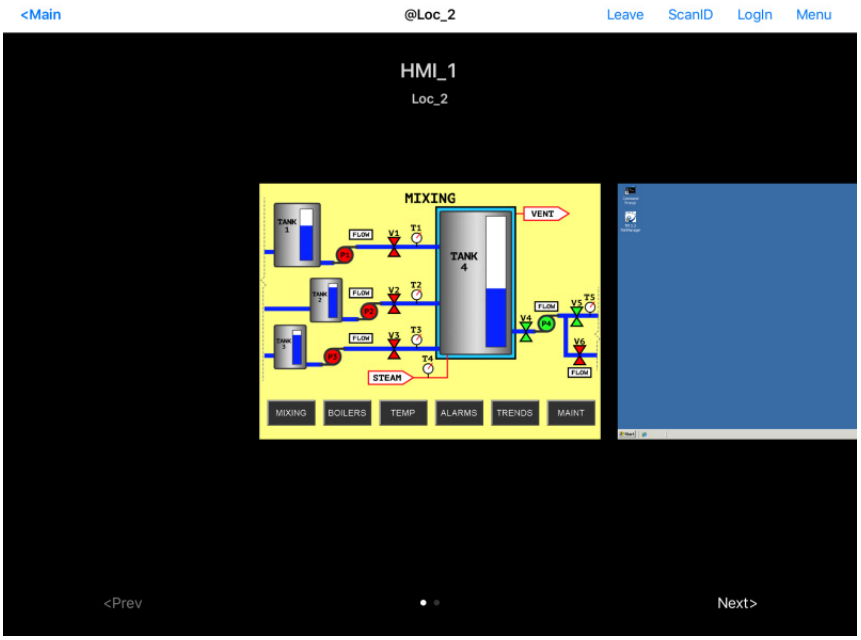
The GPS Resolver Settings dialog box shows the Latitude, Longitude, and Altitude that was measured when the GPS was registered. The Location Radius and Location Altitude Range are added automatically.

Figure 638 - Selected Resolver



14. Once a resolver is added, click Finish to close the wizard and accept the configuration.

Figure 639 - Display Clients Launched by GPS



15. Launch the iTMC client.

The display clients appear on the mobile device once the resolver is triggered, either by a QR code or bar code scan, or entry within the range of the Bluetooth beacons, Wi-Fi area, or GPS zone.

This allows you to deploy applications without deploying permanent Terminal hardware.

Fencing and Sub-Locations

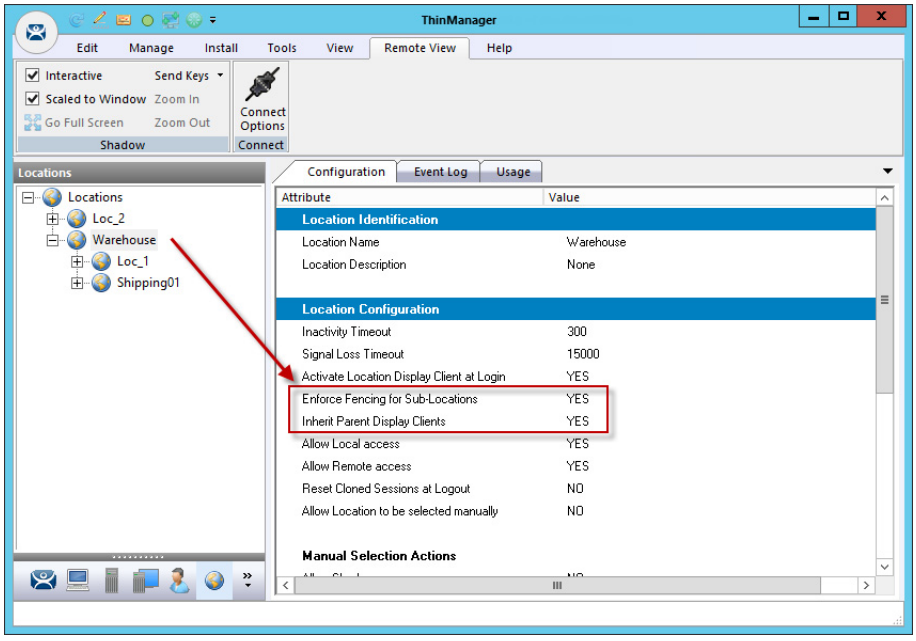
Fencing is a hierarchy that allows you to nest locations within locations, which can be useful for organization and allow control of access.

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 is 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. For example, a worker cannot 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 run the application and leave the Fence, then the application is no longer transmitted.

Fencing is best initiated by Bluetooth beacons, Wi-Fi Access Points, or GPS.

Figure 640 - Location Using Fencing



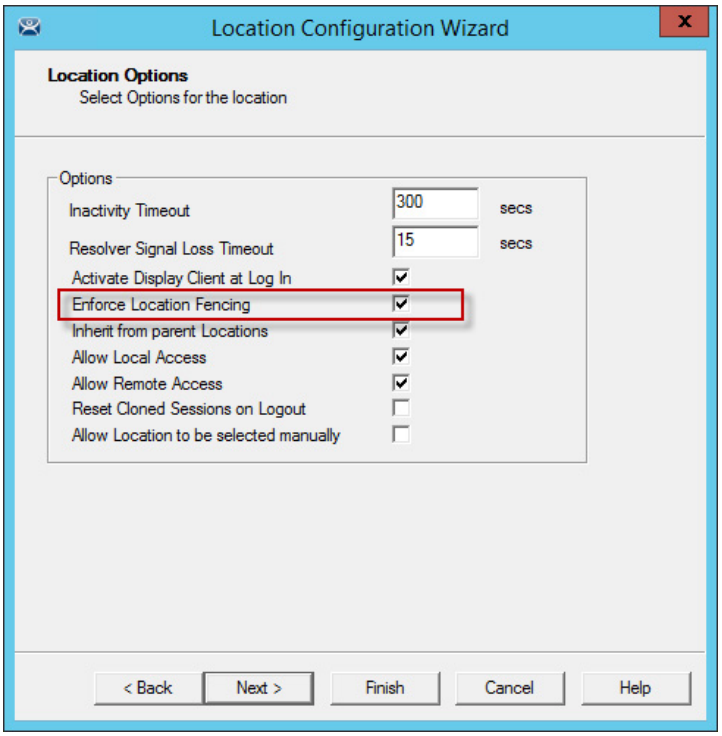
In Figure 640, the Warehouse location was created as the parent group with Fencing Enforced. You have to enter the Warehouse location before you are allowed to access the Loc_1 or Shipping01 locations and applications.

Parent Locations

A Fence needs a parent location that authenticates a high-level location, which must be resolved before the child sub-locations can become active.

The parent location can be configured without display clients and actions, which merely provides proof of location. The applications and actions are delivered by the child sub-locations.

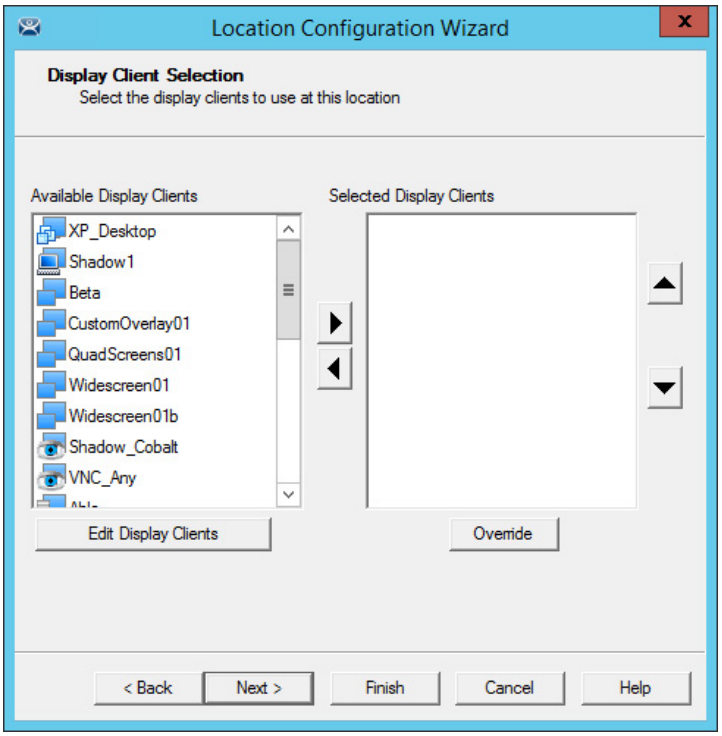
Figure 641 - Location Options for Parent Location



The Warehouse parent location has Enforce Location Fencing enabled.

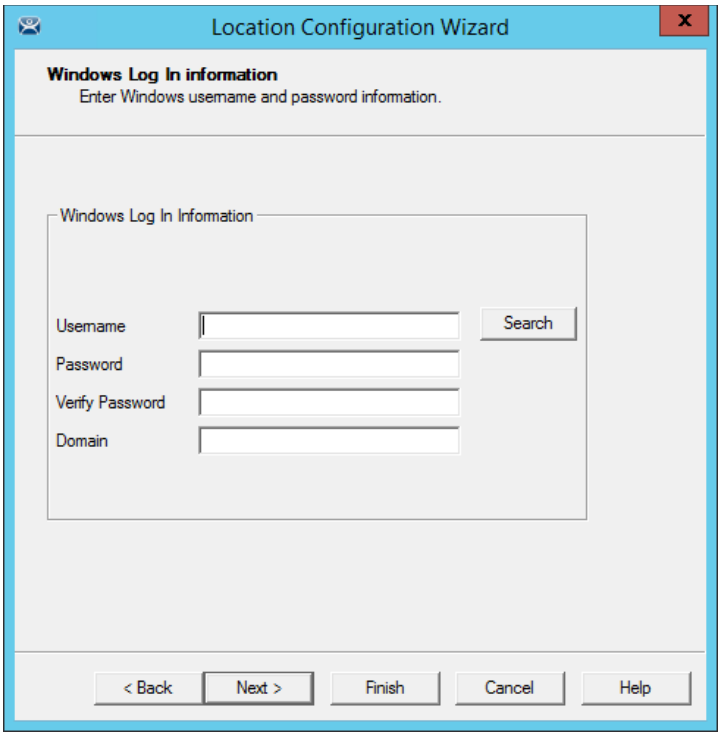
A user must authenticate to the Warehouse location before the child sub-locations can be accessed.

Figure 642 - Display Client Selection



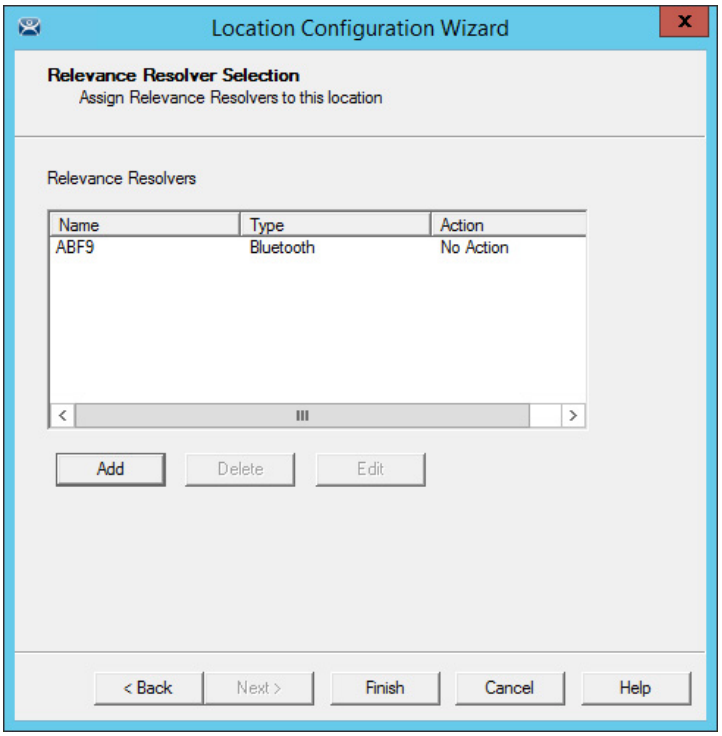
The Warehouse parent location is not assigned display clients. It is used only for authentication so display clients are left off the location.

Figure 643 - Windows Log In Information Page



The Warehouse parent location is not assigned a Windows user account because it has no display clients of its own.

Figure 644 - Relevance Resolver Selection Page



The Warehouse parent location is assigned the ABF9 Bluetooth resolver, which has no action listed because the intent is not to launch a program or initiate an action other than to identify the user in the parent location.

A user must be on the range of the ABF9 Bluetooth beacon to access the sub-locations.

A GPS location or Wi-Fi Access Point could be used instead.

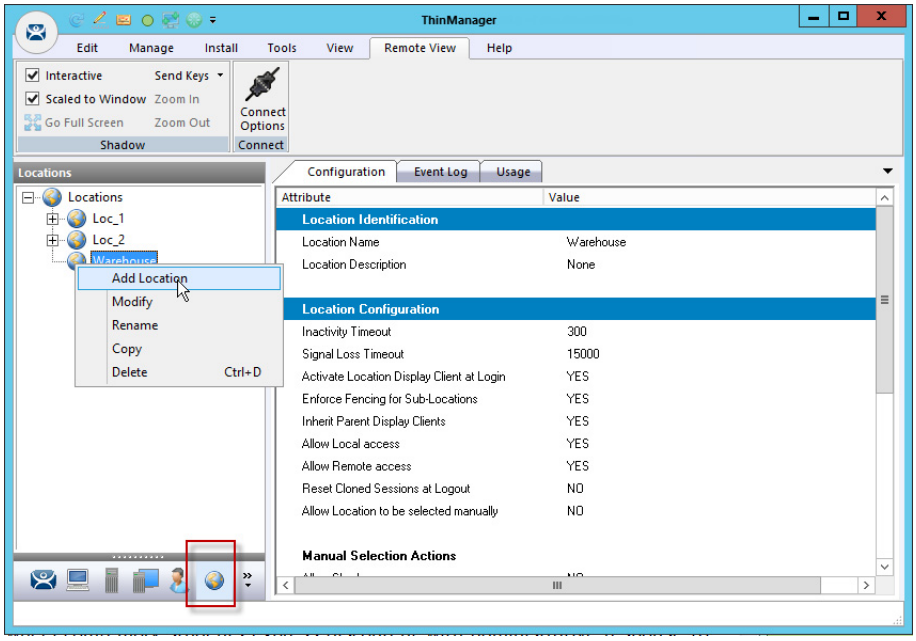
Child Sub-locations

Sub-locations that are nested under a parent location must resolve the parent location before it can initiate the action of the sub-location.

These two methods can create a sub-location.

This is the first method to create a sub-location.

Figure 645 - Location Right-click Menu



1. Right-click on the parent location and choose Add Location.

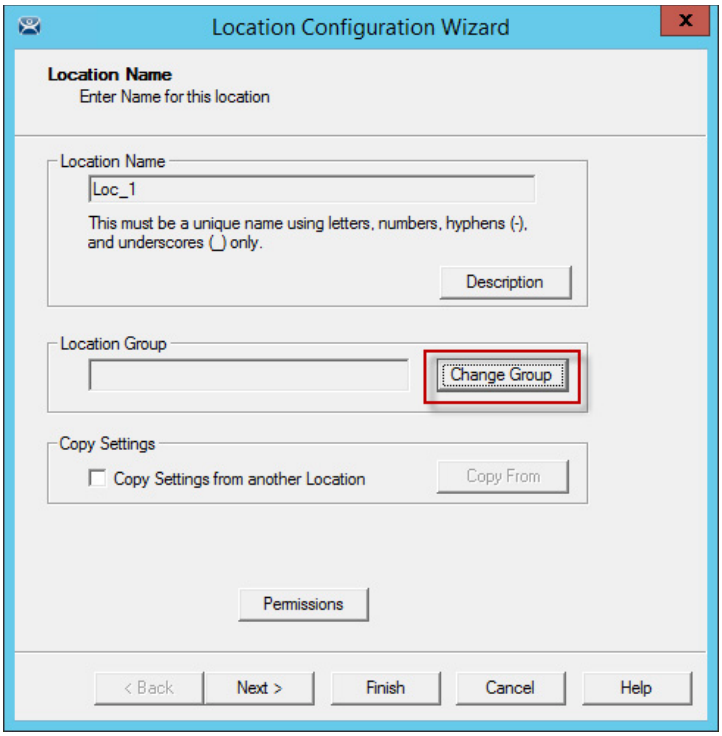
   The Location Configuration Wizard appears with the created location nested under the parent location.

The second method to create a sub-location is to add an existing location to the location.

1. Double-click on a location in the Location branch of the ThinManager tree.

   The Location Configuration Wizard appears.

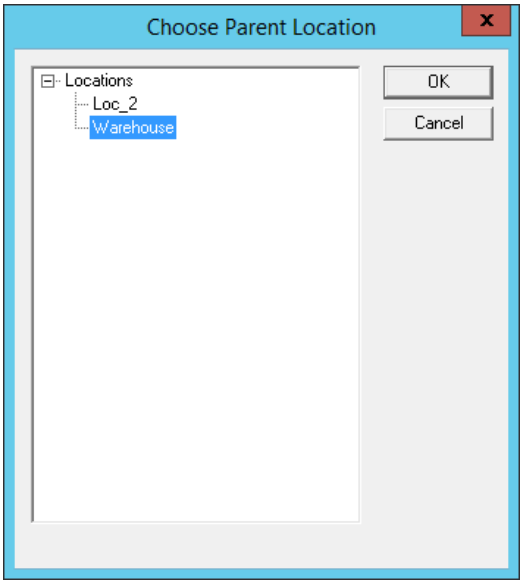
Figure 646 - Location Name Page



2. Click Change Group.

   The Choose Parent Location dialog box appears.

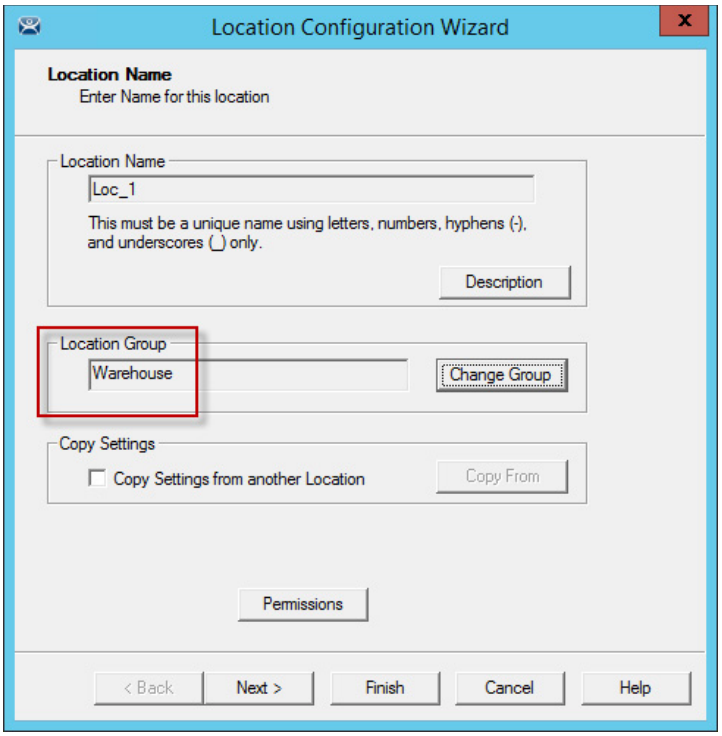
Figure 647 - Choose Parent Location



3. Highlight the desired parent location and select OK. In this example, the Warehouse location is used.

   The Location Name page appears, with the highlighted parent location displayed as the Location Group.

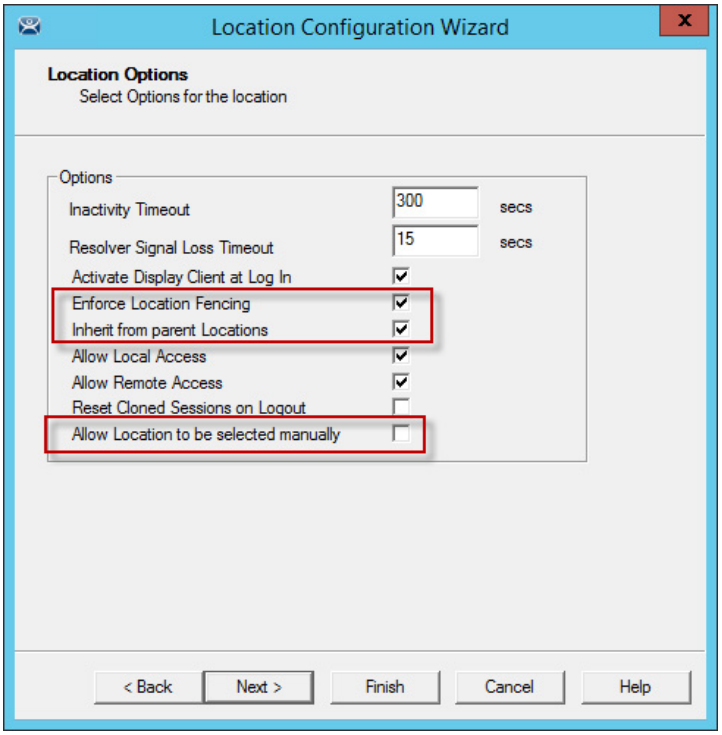
Figure 648 - Location Name Page



4. Click Finish to accept the change.

   The open location becomes a child sub-location.

Figure 649 - Location Options for Sub-location

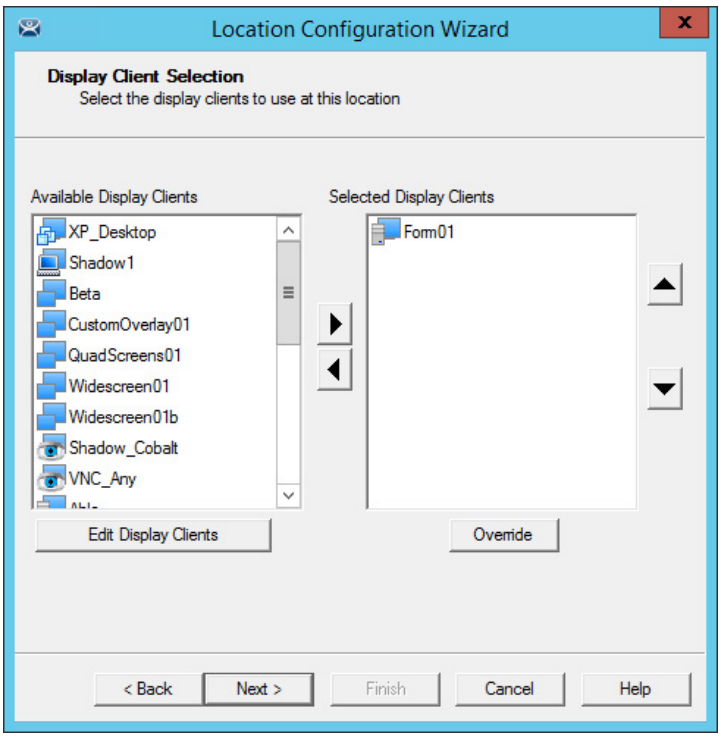


This sub-location is configured to Inherit from parent Locations.

If they had sub-locations of their own, they could have the Enforce Location Fencing applied.

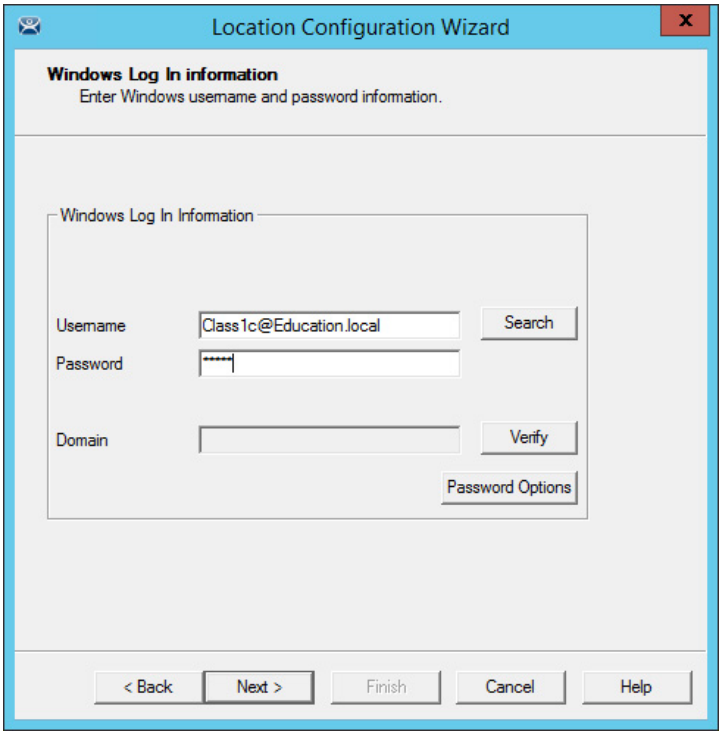
5. Check Inherit from parent Locations to inherit the applications applied to the parent location.
6. Clear the Allow Location to be selected manually checkbox to make the user use the resolvers at the location to initiate the application or action.

Figure 650 - Display Client Selection Page



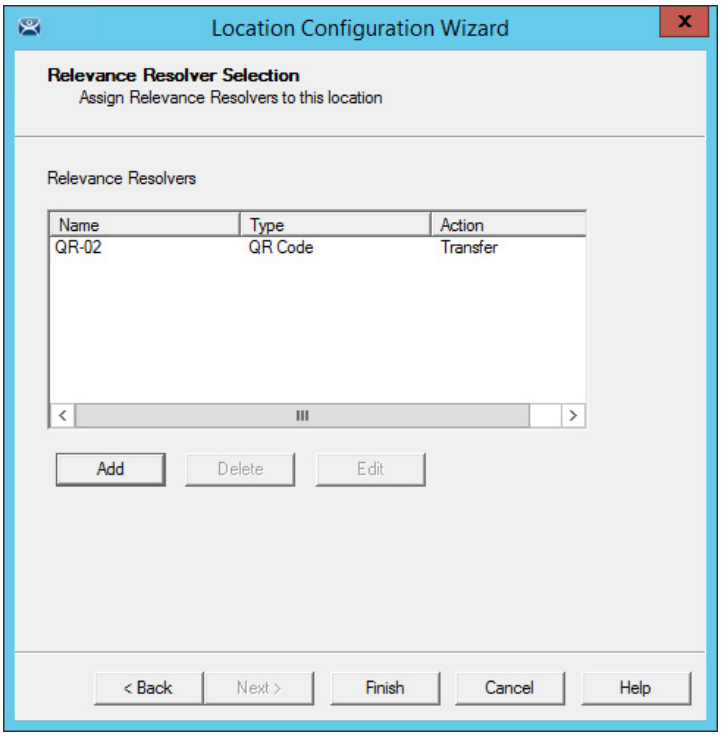
7. Add the desired display clients to the sub-location that the user accesses when connected.

Figure 651 - Windows Log In Information Page



The sub-location needs a user account if it has a display client added. You can use domain accounts or non-domain accounts.

Figure 652 - Relevance Resolvers Selection for Sub-locations



The sub-locations can use any resolver—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 Add Actions to Resolver Codes on page 46 for details on how to add the Relevance Resolvers to a Location.

ThinManager 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. Follow these steps to control user access.

1. Create Access Groups. See ThinManager Access Group Creation on page 338.
2. Apply to Applications or actions. See Add Access Group to a Display Client on page 341.
3. Apply to location. See Add Actions to Resolver Codes on page 46.
4. Create ThinManager Users. See Create the ThinManager User via Active Directory on page 357.
5. Apply Permissions. See Add Actions to Resolver Codes on page 46.
6. Log in to the location to access applications. See Interact with the Location on page 518.

Figure 653 - 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.

Figure 654 - User Access to Display Clients via Permissions

As each person scans the Resolver, they get the application that matches their access group.

Figure 655 - User Access to Display Clients via Permissions

The same Resolver delivers different content, based on Permissions.

Create a Location with Restricted Applications

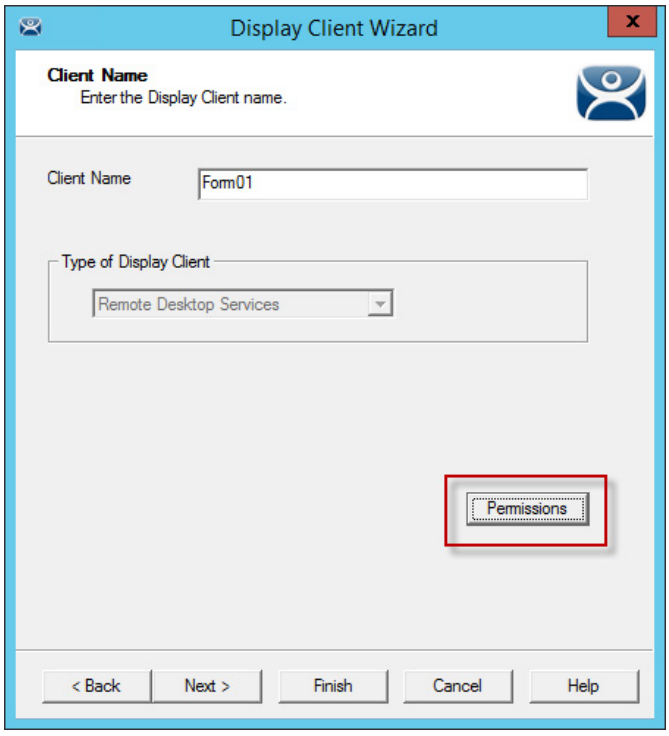
Access Group permissions grant or deny access to display clients so that a user must log on with an account that has permission to access the application.

Use Permissions to Restrict an Application

1. Double-click on the display client with the application you want to restrict in the Display Client tree.

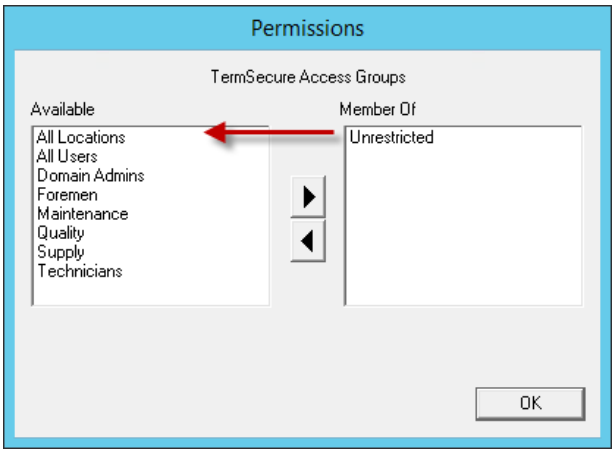
   The Client Name page of the Display Client Wizard appears, where permissions are applied to the display client.

Figure 656 - Client Name Page



2. Click Permissions.
3. The Permissions dialog box appears.

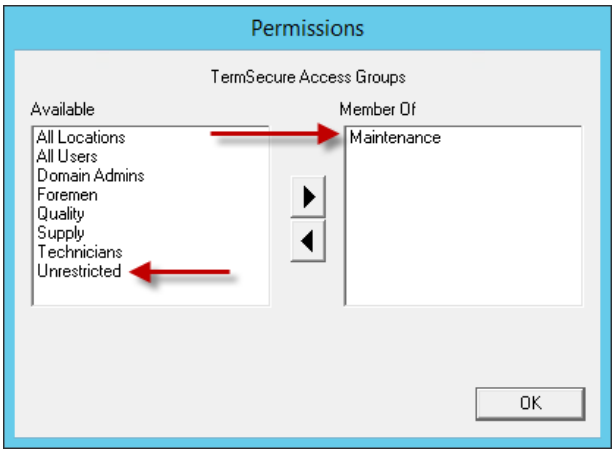
Figure 657 - Permissions Dialog Box



4. Move Unrestricted from the Member Of list to the Available list.

IMPORTANT If Unrestricted is not removed, then anyone can still access the application.

Figure 658 - Permissions



5. Move the desired Access Group to the Member Of list.
6. Click OK to close the window.
7. On the Client Name page, click Finish.

Add a Restricted Application to a Location

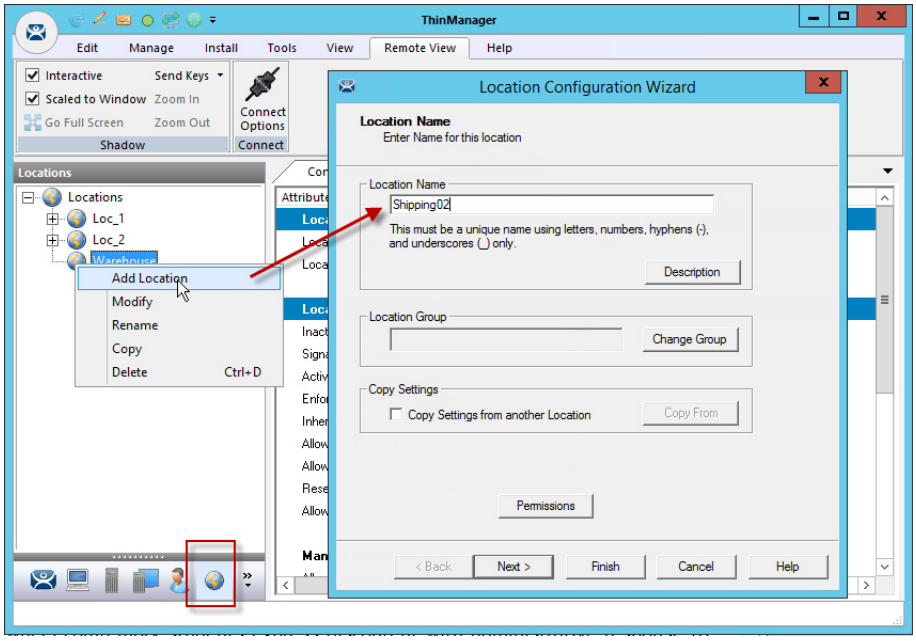
You can apply ThinManager User Services to Location Services and have applications on Locations that are restricted by membership in Access Groups.

To create a Location with the restricted display client, follow these steps.

1. Click the Locations icon on the Tree Selector to open the Locations tree and create a Location.
2. Right-click on the Locations branch and choose Add Location.

   The Location Configuration Wizard appears.

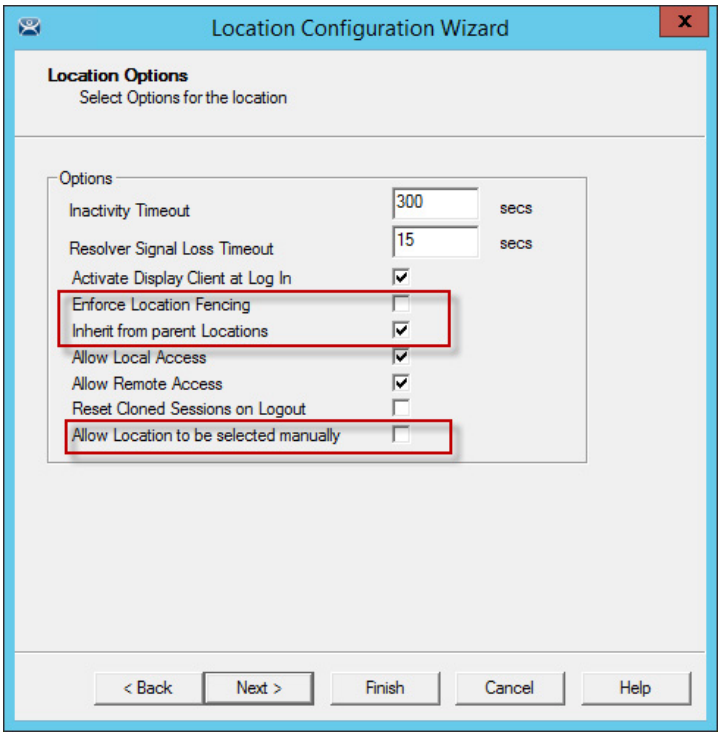
Figure 659 - Location Configuration Wizard



3. Type a Location Name and click Next.

   The Location Options page appears.

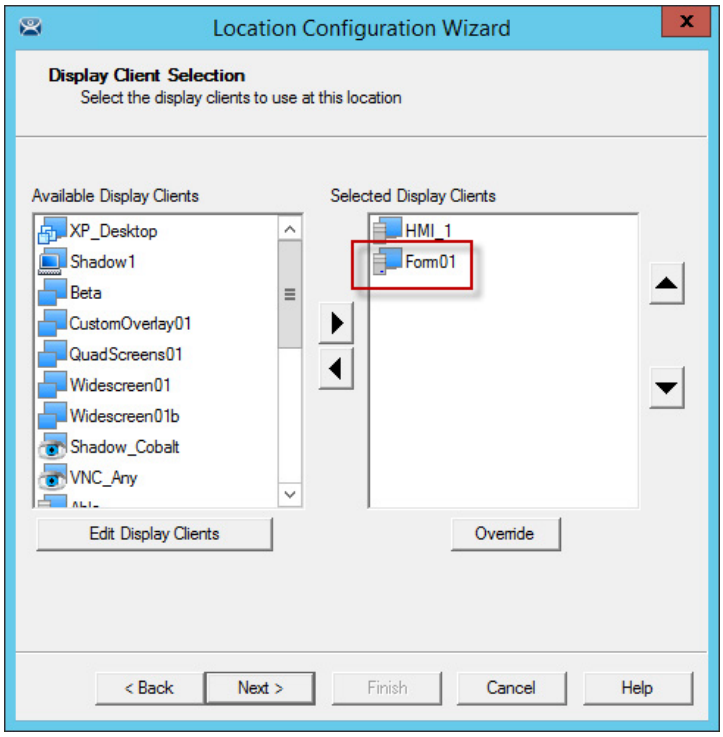
Figure 660 - Location Options



4. Choose your options.
5. Clear the Leave the Allow Location to be selected manually checkbox to force the user to use a resolver to access the applications.
6. Click Next to continue.

   The Display Client Selection page appears.

Figure 661 - Display Client Selection Page



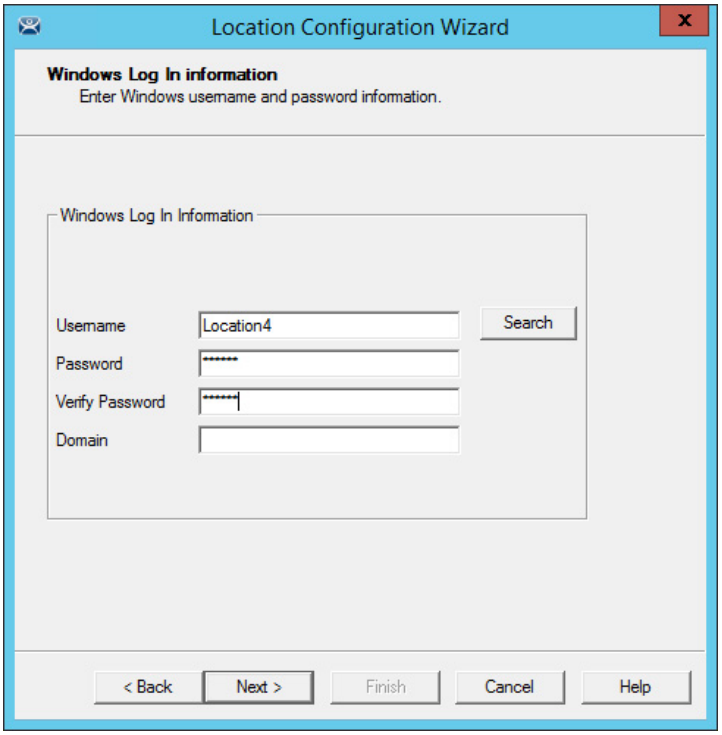
7. Add the desired display clients to the Selected Display Client list on the Display Client Selection page.

8. 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 Use Permissions to Restrict an Application on page 458.
9. Click Next to continue.

   The Windows Log In Information page appears.

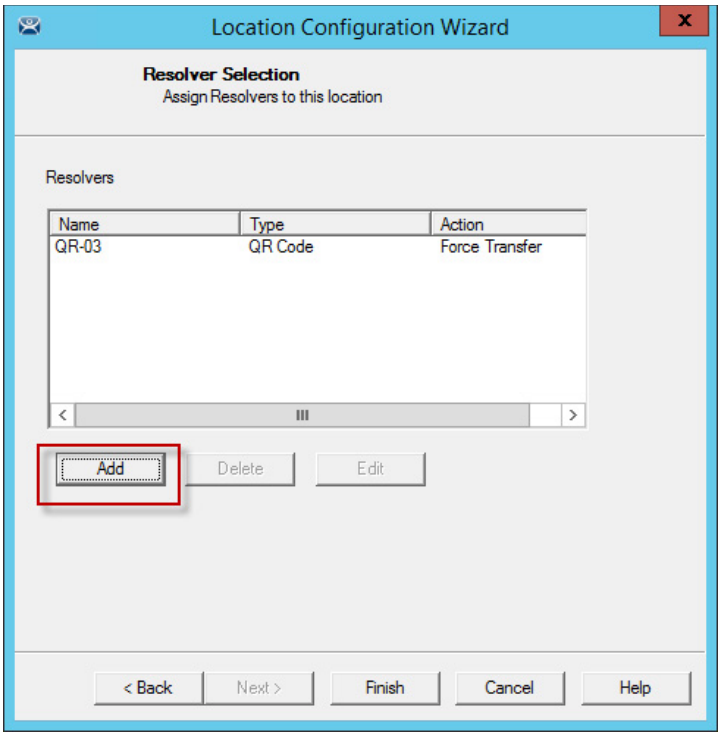
A location with display clients requires a valid Windows user account, which can be a domain or non-domain account.

Figure 662 - Windows Log In Information Page



10. Click Search for a domain account or type one into the Username field and type the Password.
11. Click Next to continue.

Figure 663 - Relevance Resolver Selection



12. Click Add.

    The Choose a Relevance Resolver dialog box appears.
13. Choose your action, Forced Transfer in this case.
14. Click Finish.

    The location is created and the wizard closes.

Put It Together

Figure 664 shows 1_Terminal at the Shipping02 location. It has two display client applications:

- HMI_1 is unrestricted and is visible to anyone accessing the location
- Form01 is restricted to members of the Maintenance access group

Figure 664 - Shadowed Location

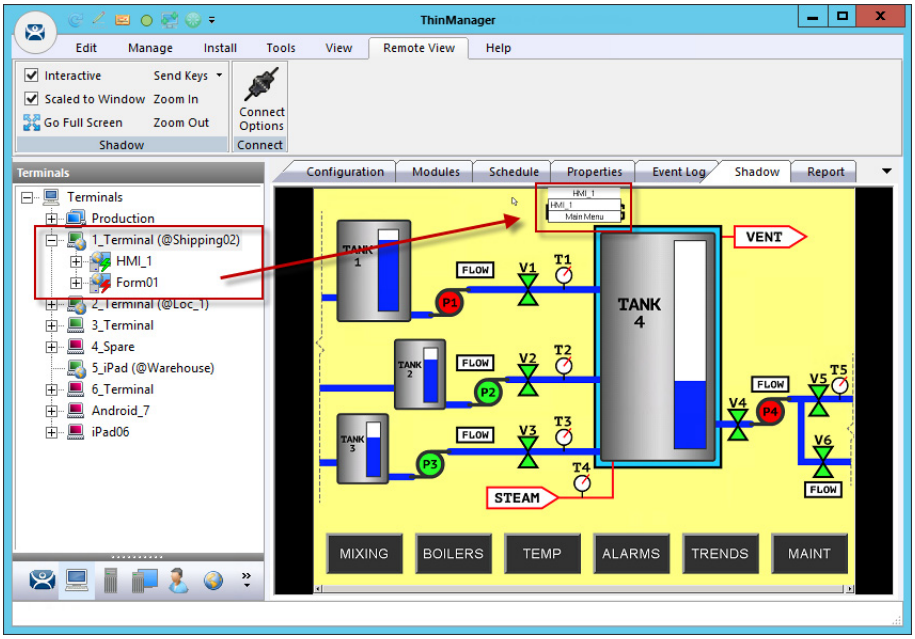
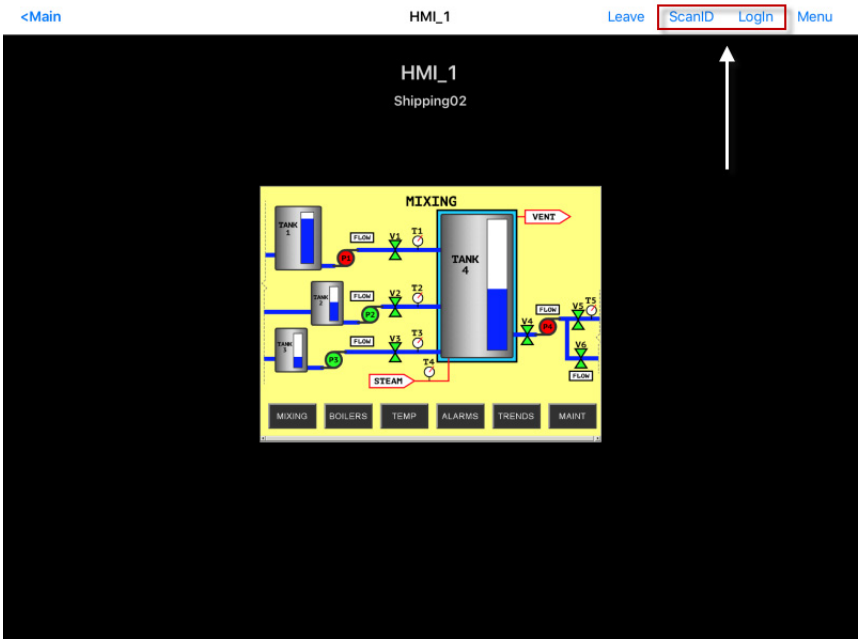


Figure 664 shows the location with the HMI_1 application operational. Form01 is not operational because no Maintenance user is logged in.

Figure 665 - Mobile Transfer of the Location



When the mobile user transfers the location, they have access to the unrestricted HMI_New application only.

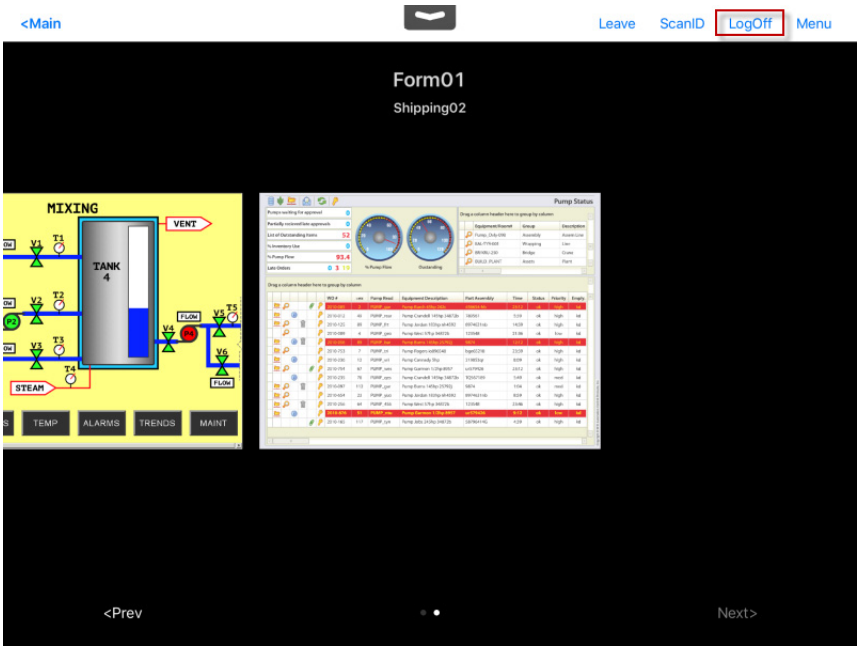
1. Click ScanID to scan a QR code resolver.
2. Click Login.

   The Login prompt appears, which allows the ThinManager user to login.

Figure 666 - ThinManager User/ThinManager User Login Prompt

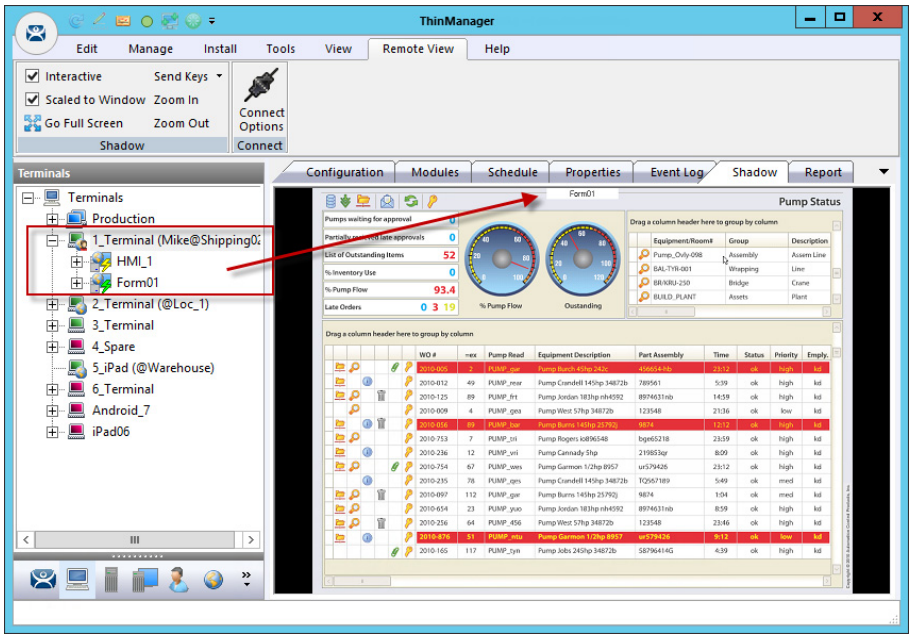
3. Login with the ThinManager User account that is a member of the proper access group.

Figure 667 - ThinManager User Account Accesses Application



Once the ThinManager User logs in, the user has access to the hidden restricted application. Figure 667 shows both locations on the mobile device.

Figure 668 - ThinManager Tree



Once the ThinManager user is logged on with the correct Permissions from the access group membership, the hidden application is revealed.

One QR Code, Multiple Actions

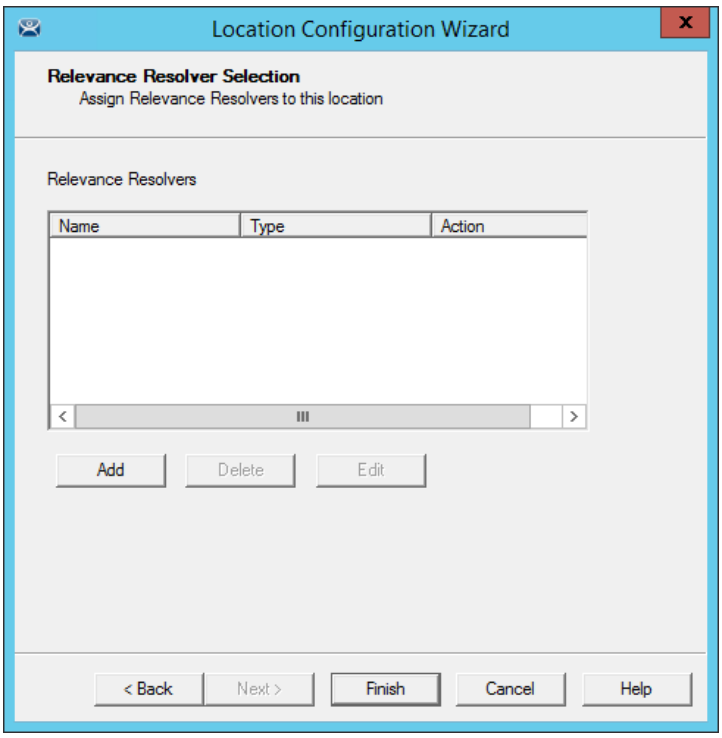
The previous section covered the use of a Relevance Access Group to hide a display client application from the public with the use of Access Groups. This section cover the use of access groups to provide different actions.

Instead of using a different resolver for every action, you can use a single resolver and Access Groups to provide different actions. The example that follows uses a QR code as the resolver.

1. Click the Locations globe icon on the Tree Selector at the bottom of the tree to open the Locations branch.
2. Double-click the Terminal or right-click on the Terminal and choose Modify.

   The Location Configuration Wizard appears.
3. Click Next until the Relevance Resolver Selection page appears.

Figure 669 - Relevance Resolver Selection Page

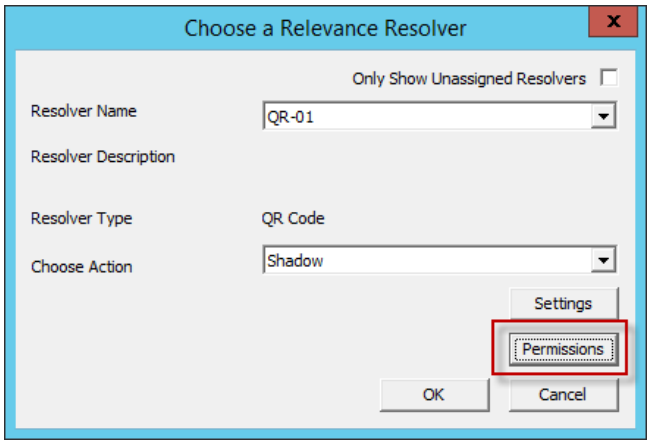


4. Click Add.

   The Choose a Relevance Resolver dialog box appears.

   Add the same resolver to the location as many times as you have actions and access groups you want to involve.

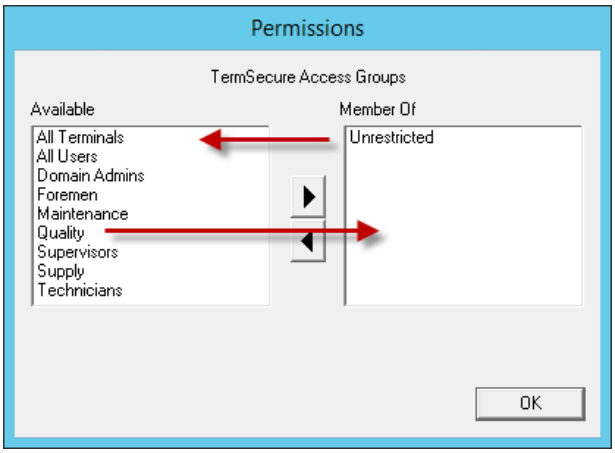
Figure 670 - Choose a Relevance Resolver



5. Choose a different action from the Choose Action pull-down each time you add it.
6. Click Permissions to add the Access Group to the action.

   The Permissions dialog box appears.

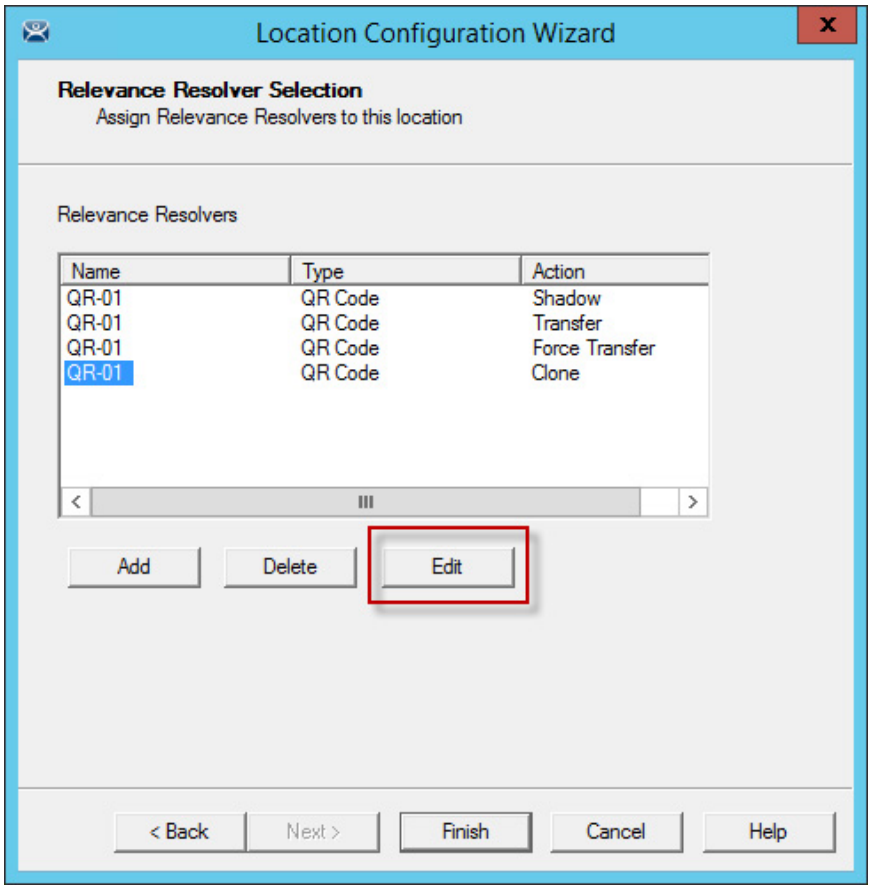
Figure 671 - Permissions Dialog Box



7. Remove the Unrestricted group from the Member Of list and add the desired access group from the Available list group; Quality in this example.
8. Click OK to finish.

You can also edit the permissions

Figure 672 - Edit Button on the Relevance Resolver Selection Page



1. Highlight a resolver and click Edit.

   The Choose a Relevance Resolver dialog box appears, within which the Permissions button resides.

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 are able to shadow the location and leave control with the operator.

If a Maintenance member scans QR-01, they transfer the application to their mobile device once the operator allows it.

If a Foreman scans the QR-01 code, they 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 clone the application and run it with their own Windows account.

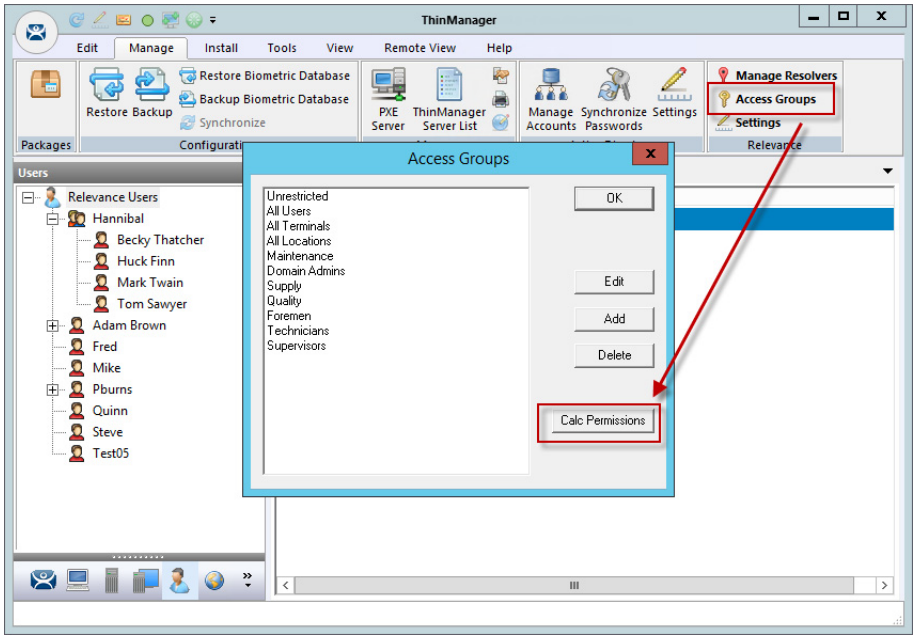
Calculate Permissions

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.

1. Choose Manage>Access Groups.

   The Access Groups dialog box appears.

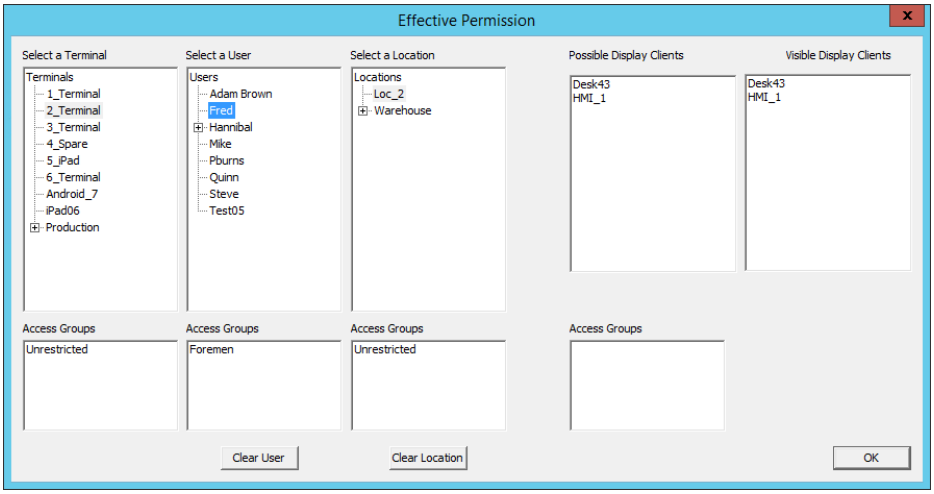
Figure 673 - Access Groups Dialog Box



2. Click Calc Permissions.

   The Effective Permission dialog box appears.

Figure 674 - Effective Permission Dialog Box



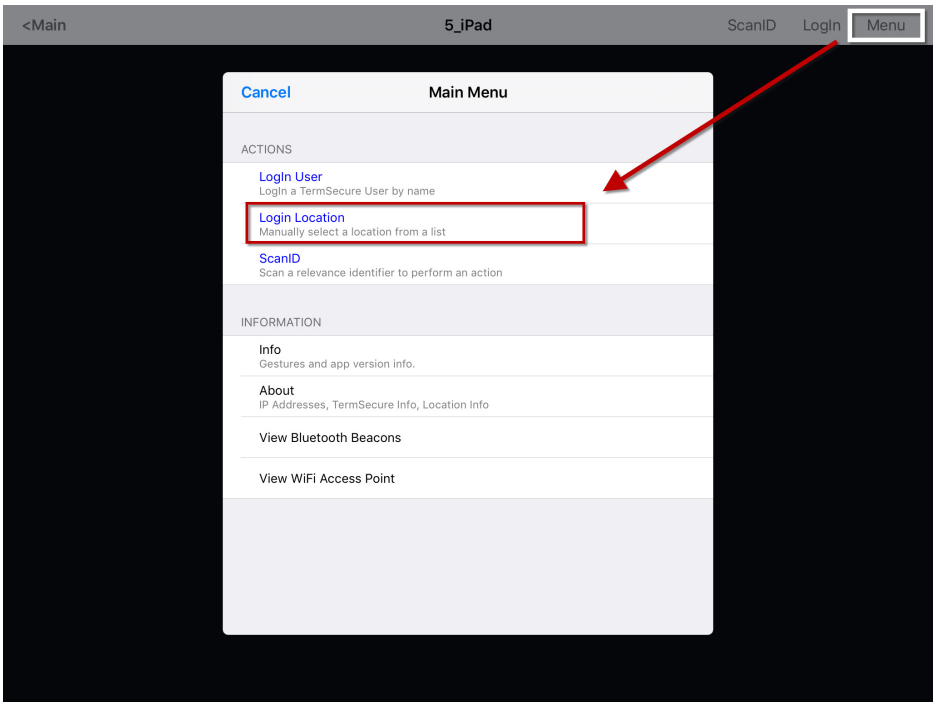
3. Highlight members of selection lists to show the display clients that are visible in the Visible Display Clients column.
4. Click Clear User and Clear Location to clear the fields and test another combination.
5. Click OK to close the dialog box.

Manual Interaction with Locations

A mobile device can connect to a Location and manually interact with the applications.

1. Connect the mobile device to the ThinServer and connect as shown in Mobile Devices on page 315.

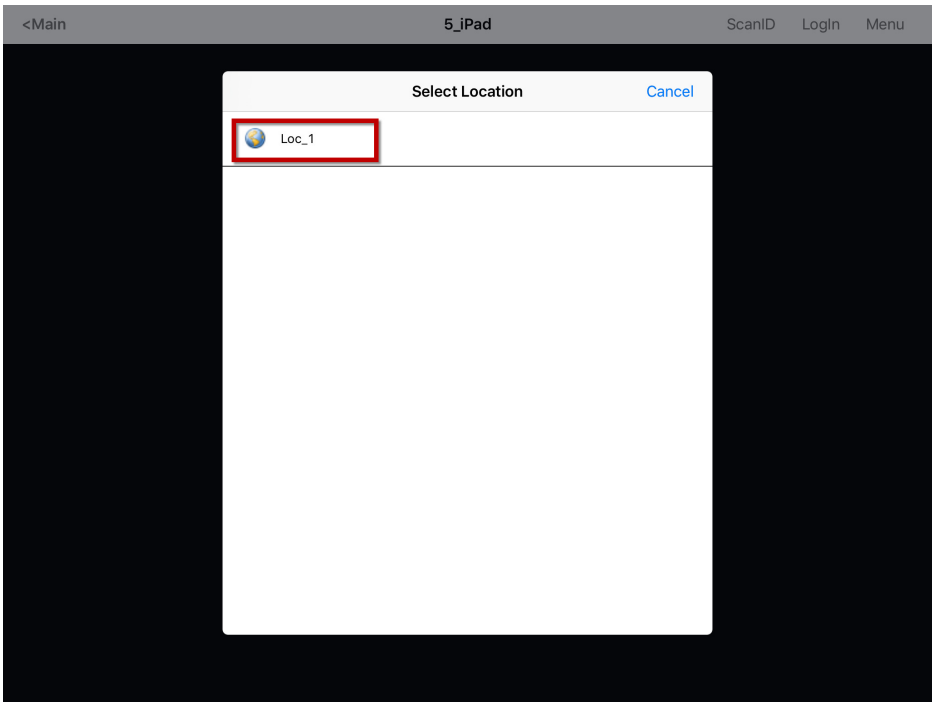
Figure 675 - Main Menu on a Mobile Device



2. Launch the Main Menu from the mobile device menu bar.
3. Press Login Location, which manually connects to a Location.

   The Select Location dialog box appears, which lists all Locations that are allowed to have a manual configuration. In Figure 676 on page 472, only one Location is created.

Figure 676 - Select Location



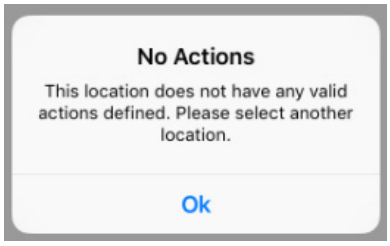
4. Press the Location.

   The Select Action dialog box appears.

   If a No Actions dialog box appears, it indicates one of two possibilities.

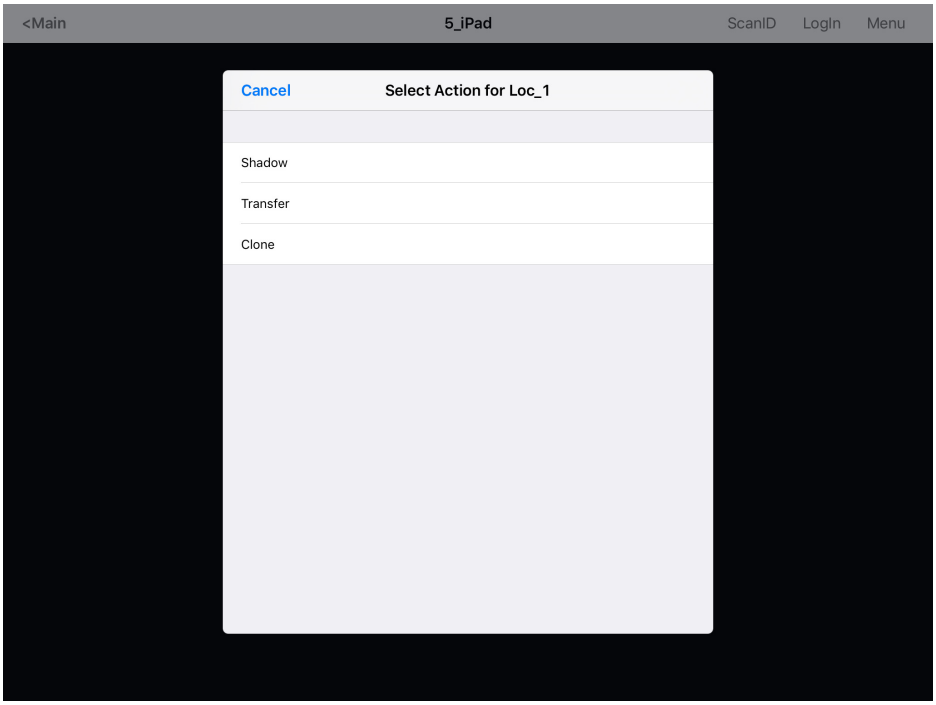
   - There were no Actions checked on the Location Options page of the Location Configuration Wizard
   - A Relevance Permission was applied, and the user is not a member of a permitted access group

Figure 677 - No Actions Error



   a. If the No Actions dialog box appears, click Ok to close it and select another location.

Figure 678 - Actions for Manual Interaction



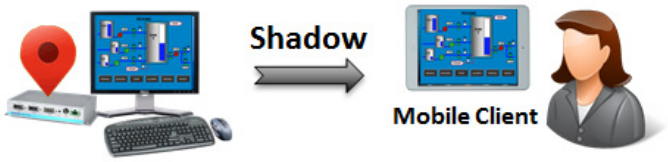
There are three manual interactions between a mobile device and a location.

Interaction	Description
Shadow	Duplicates the graphic output of the Location screen and sends it to the mobile device.
Transfer	Sends the graphic output of the location to the mobile device instead of the location. Requires the operator to manually allow the transfer.
Clone	Creates a duplicate session for the mobile device using the configuration of the location and the user credentials of the mobile device.

Shadow

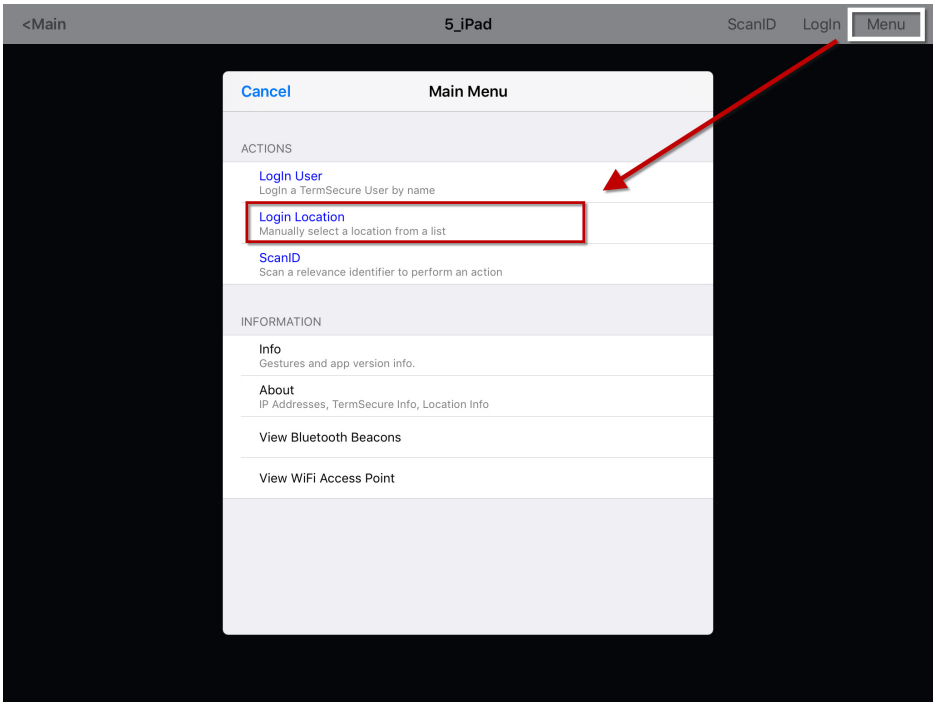
Shadow duplicates the graphic output of the location and sends it to the mobile device.

Figure 679 - Shadow



The Shadow feature allows the mobile user to see and interact with the exact display as the location.

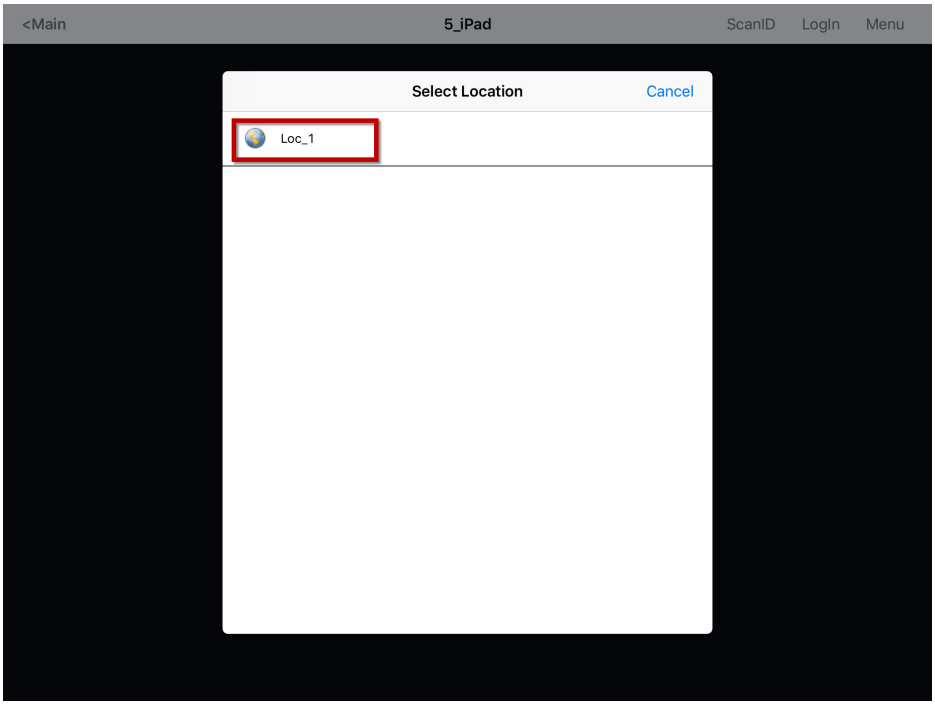
Figure 680 - Main Menu



1. Open the mobile program, select your ThinManager Server, and press Menu in the upper-right corner to launch the Main Menu dialog box.
2. Press Login Location on the menu.

   The Select Location dialog box appears.

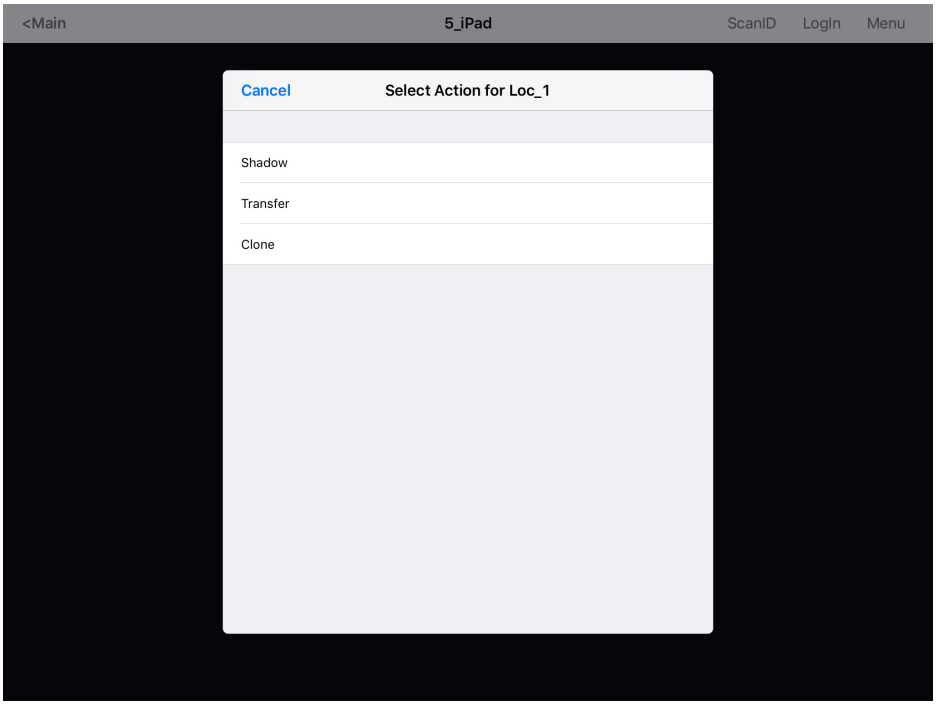
Figure 681 - Select Location Menu



3. Press a Location.

   The Select Action dialog box appears, which list the actions allowed at the location.

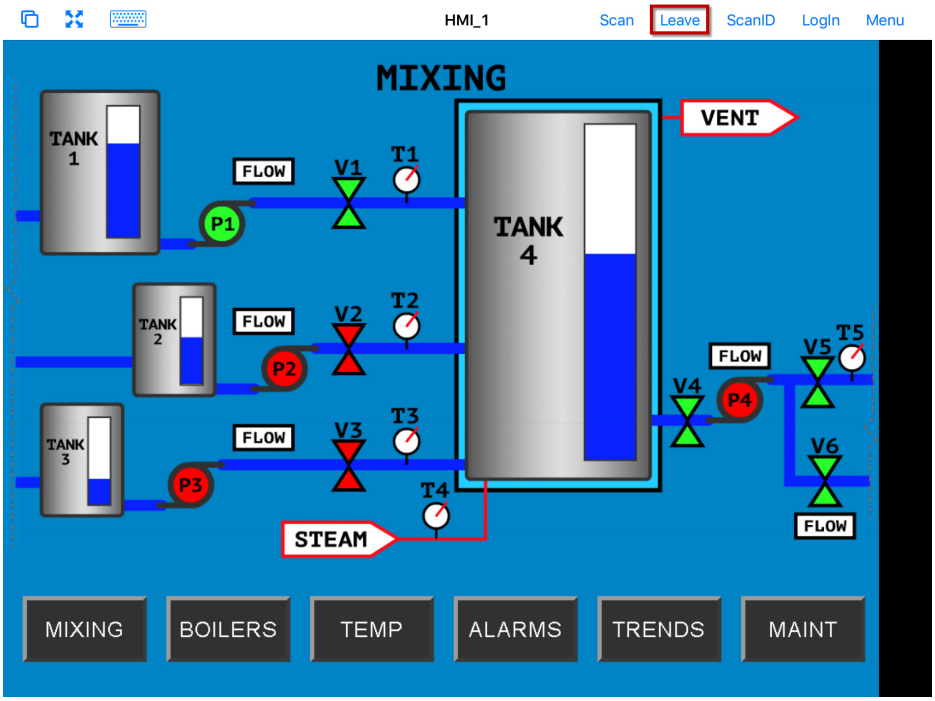
Figure 682 - Select Action Dialog Box



4. Press Shadow to connect and shadow the Location.

Figure 683 shows the shadow of the location.

Figure 683 - iTMC Shadowing Location



The shadow only shows one display client window when you shadow the location and receive the current graphic output from the location.

5. Press Leave to end the shadow.

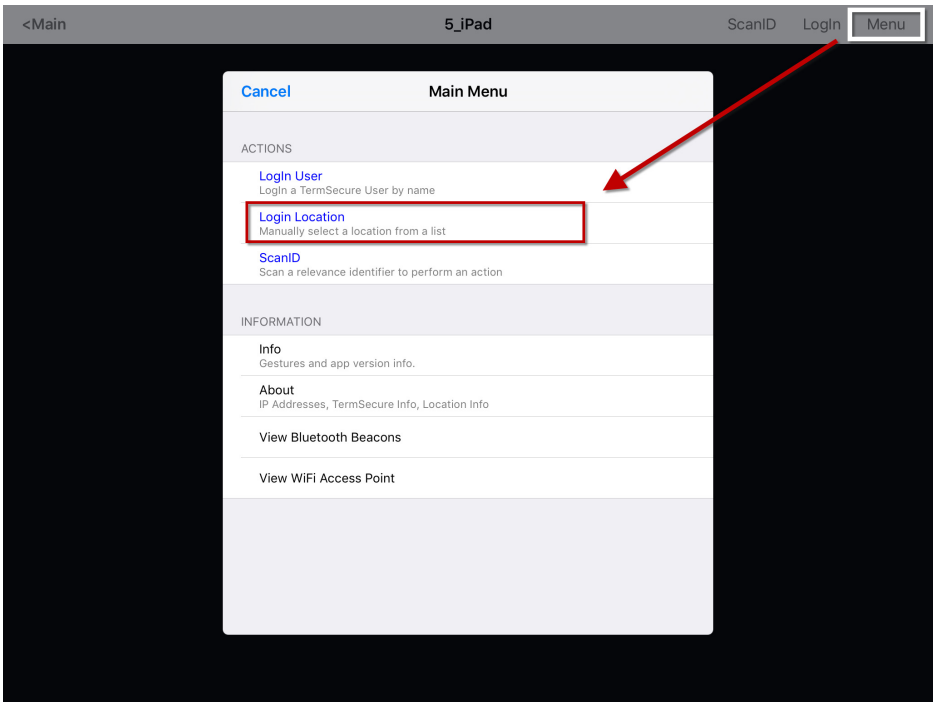
Transfer

Transfer is similar to Shadow except that the user must allow the transfer at the location, which prevents someone from taking the session while the operator is busy with a process. Also, it allows a mobile user to take sole control of the location.

Figure 684 - Transfer

1. Open the mobile program, select your ThinManager Server, and press Menu in the upper-right corner to launch the Main Menu dialog box.

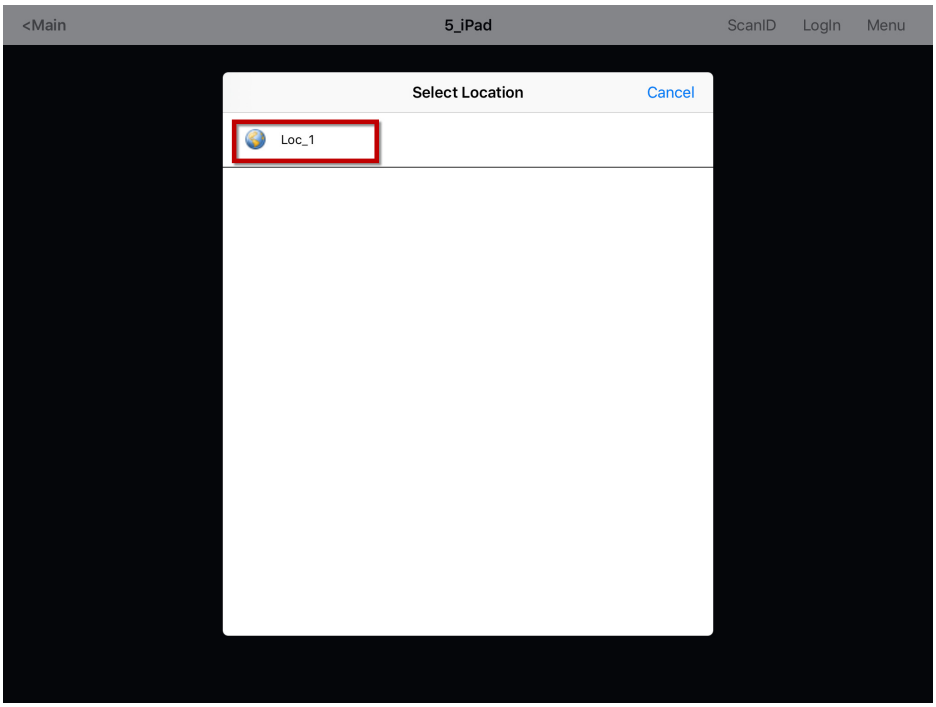
Figure 685 - Main Menu on a Mobile Device



2. In the Main Menu, press Login Location.

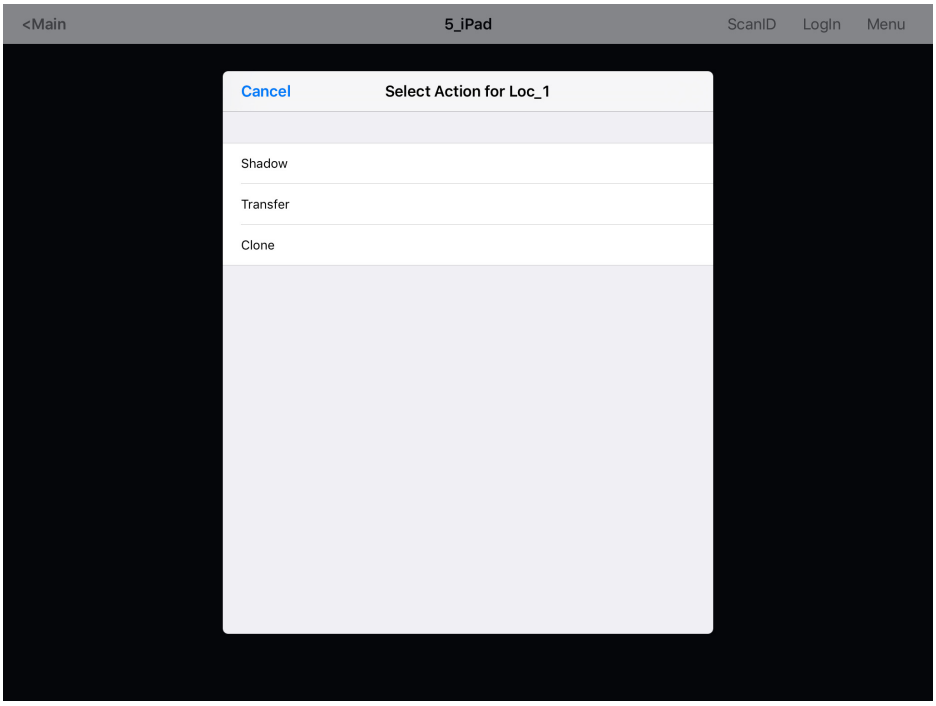
   The Select Location dialog box appears, where you can manually connect to a Location. It lists all Locations that are allowed to have a manual configuration. Figure 686 on page 477 shows only one Location was created.

Figure 686 - Select Location



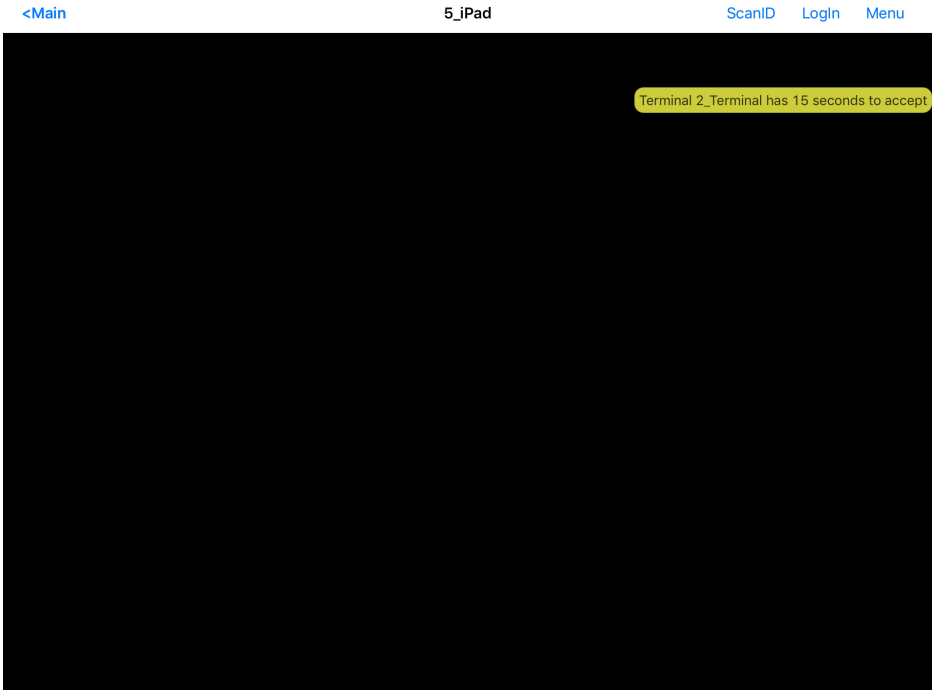
3. Press Location to open the Select Action dialog box.

Figure 687 - Actions for Manual Interaction



4. Press Transfer from the Select Action dialog box.

Figure 688 - Wait for Transfer Permission Message

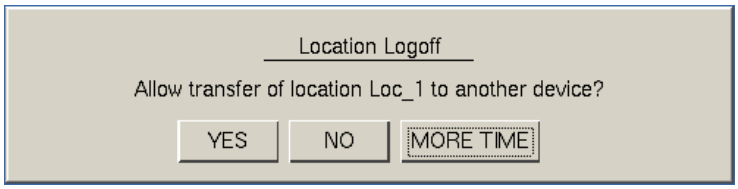


The user of the location must allow the transfer. This communication prevents the mobile user from taking the session while the local user is performing a task.

Transfer at the Location

A dialog box is displayed at the location to allow the transfer.

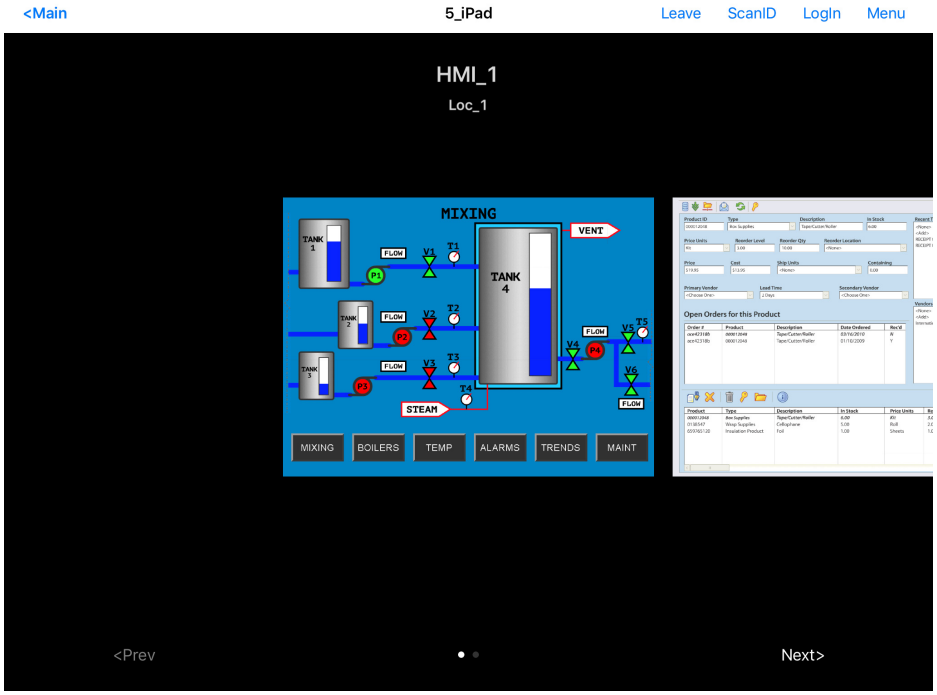
Figure 689 - Location Logoff Dialog Box



1. The local user must press YES to allow the transfer.

   The mobile client is allowed to display the location display.

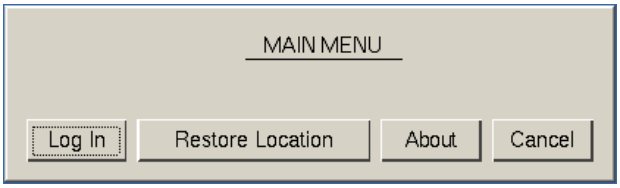
Figure 690 - Transferred Location Display



The Transfer shows all the display clients on the location instead of just the display output of the location.

2. The location display can be restored from the client or the location.
   - Press Leave on the client menu to restore the display to the location.
   - Also, you can press Restore Location at the location to restore the display.

Figure 691 - Main Menu at the Location

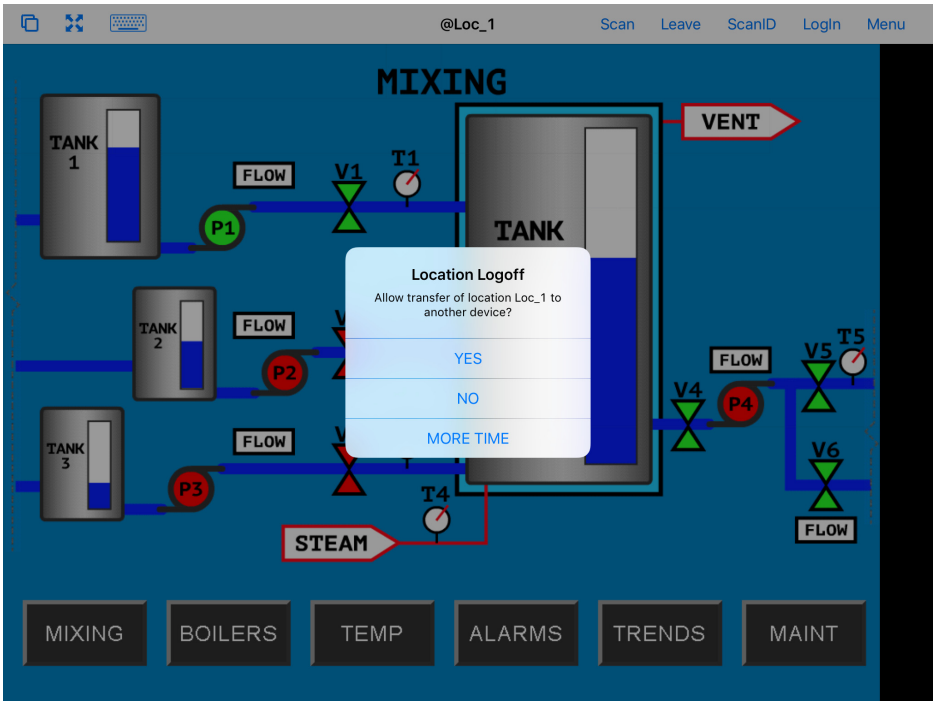


The Location displays the Main Menu during the transfer.

3. Press Restore Location to return the session.

   A dialog box appears on the mobile client to warn the mobile user that the transfer ends soon.

Figure 692 - Location Logoff Dialog



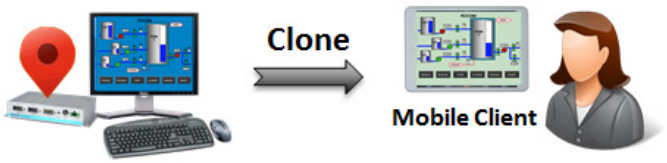
4. Press YES to allow the transfer back to the original location, NO to refuse the restoration, or MORE TIME to delay the restoration.

The amount of time that an operator has to acknowledge and allow the transfer can be set on the Relevance Setting dialog box. See Bluetooth Beacons on page 490 for details.

Clone

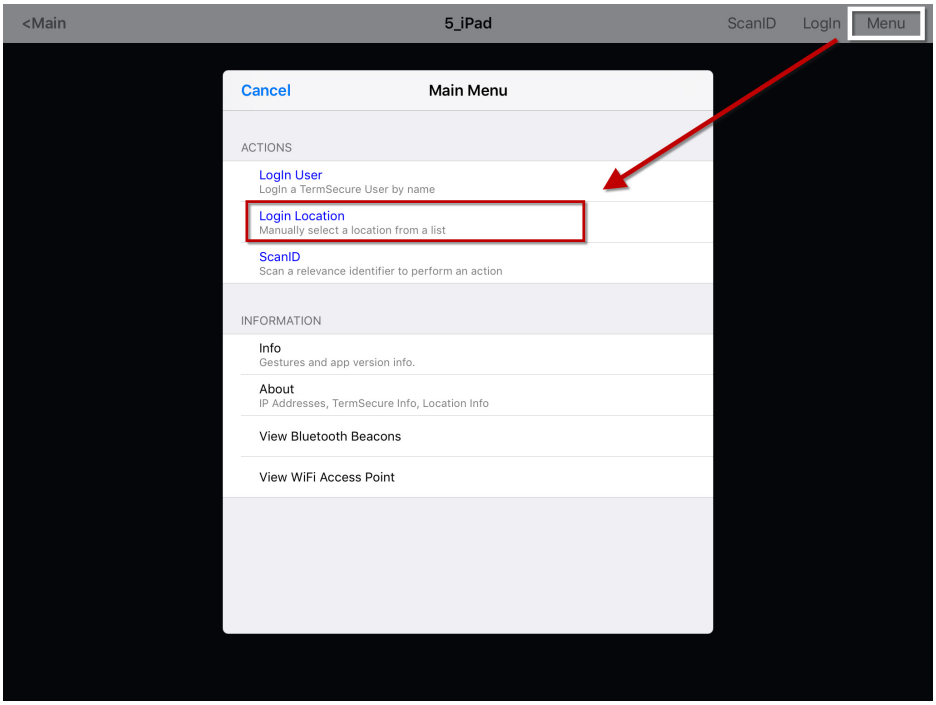
Clone duplicates the display clients of the location on the mobile device, but the sessions are created with the mobile device Windows user account.

Figure 693 - Clone



Session creation with the mobile device Windows user account allows a mobile user to get the HMI or other software and have independence from the user at the location.

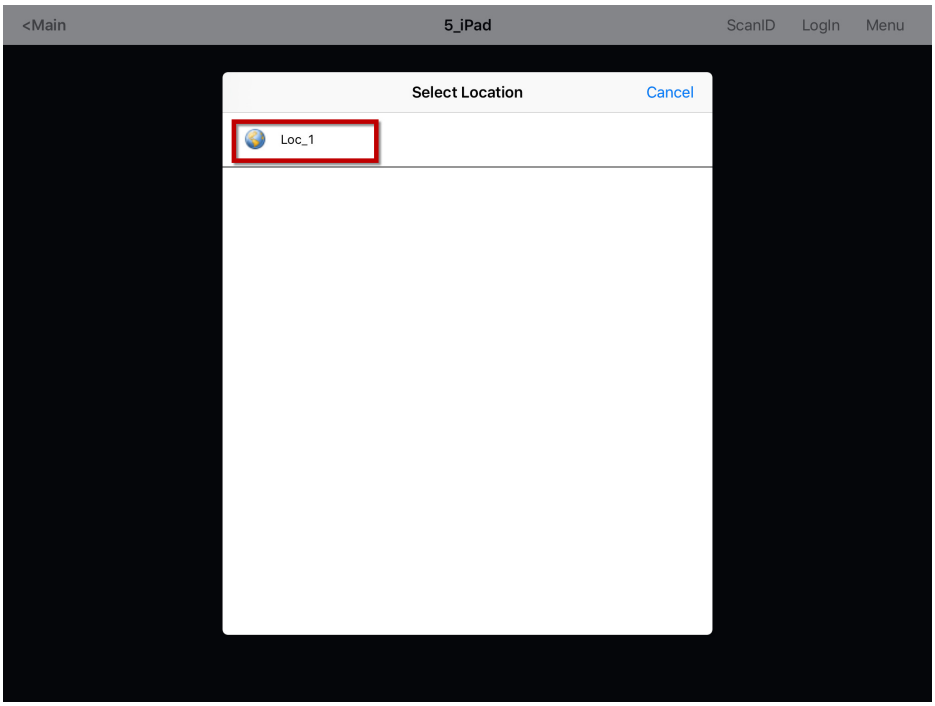
Figure 694 - Main Menu on a Mobile Device



1. Press Login Location.

   The Select Location dialog box appears, which lists all Locations that are allowed to have a manual configuration.

Figure 695 - Select Location

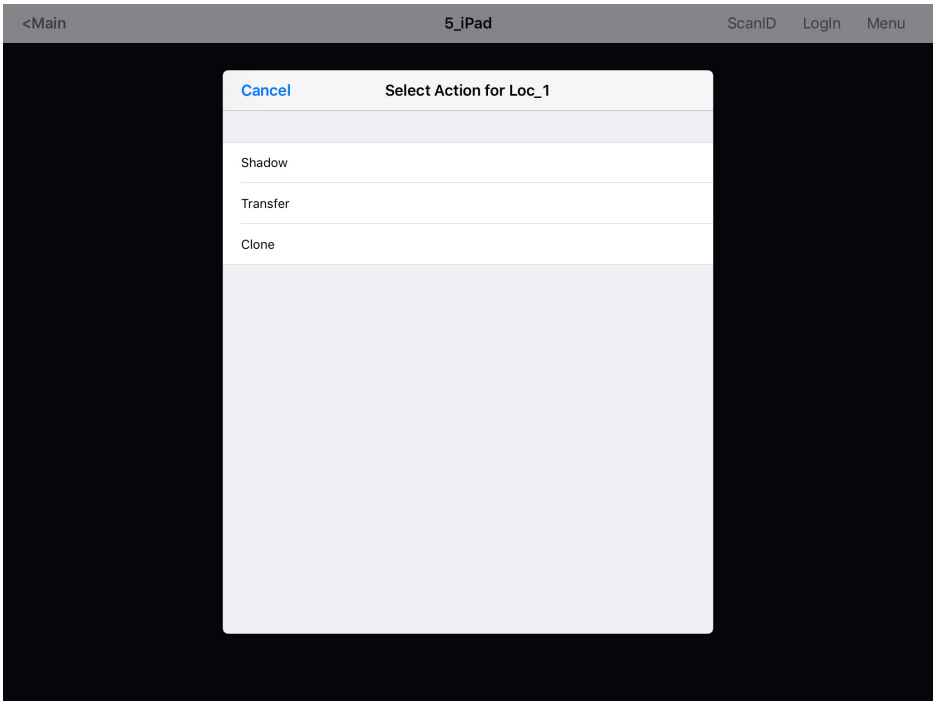


In Figure 695, only one Location was created.

2. Press the Location.

   The Select Action dialog box for the Location appears.

Figure 696 - Actions for Manual Interaction



3. Press Clone.

   The mobile device launches copies of the location's display clients, but uses the mobile device login.

Figure 697 - Cloned Session

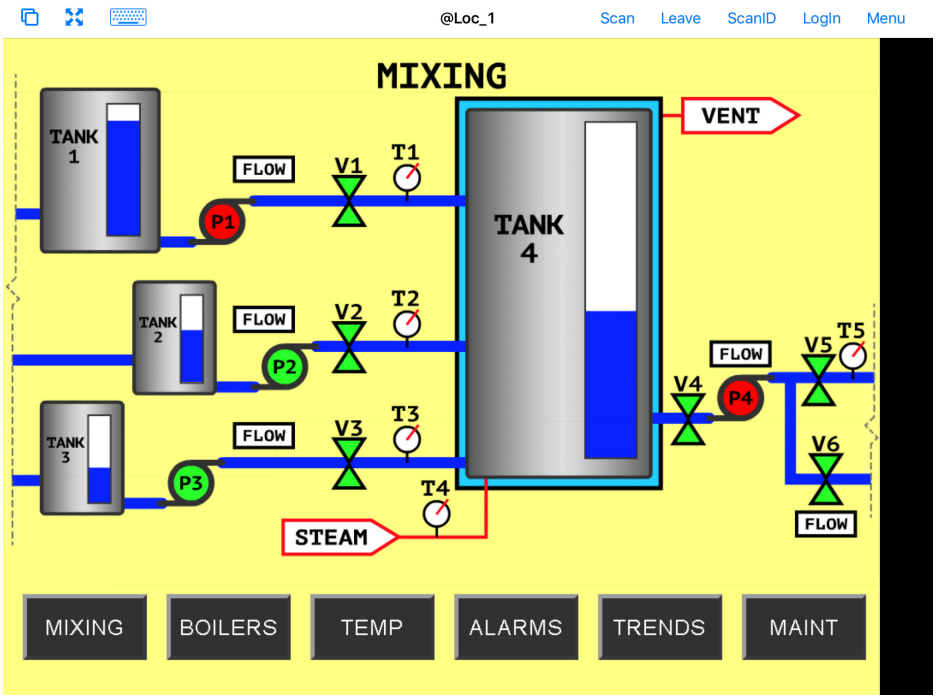


Figure 697 shows a session running the same application, but with a different set of credentials.

4. Press Leave near the top-right corner to close the mobile client.

Addition of Resolver Codes with Mobile Device

Resolvers can help a mobile device know what location it is in. These can be configured to tell the mobile device what action to take.

These are Resolvers.

- 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 can use Permissions to 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 can require presence in an area covered by a Bluetooth beacon or GPS site before a QR code can be scanned, which can prevent a user's departure from an area with a critical process. The Fence prevents the use of the application outside of the assigned areas.

QR Codes

Quick Response (QR) Codes can store text, numeral data, and URLs. QR Codes can be read quickly and easily. There are many programs which generate them, which include free sites on the web.

QR Codes provide pinpoint location as you need to be at the QR Code to read it, which allows 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 449 for details.

The iTMC and aTMC programs use the built-in camera as a scanner to read the QR Codes.

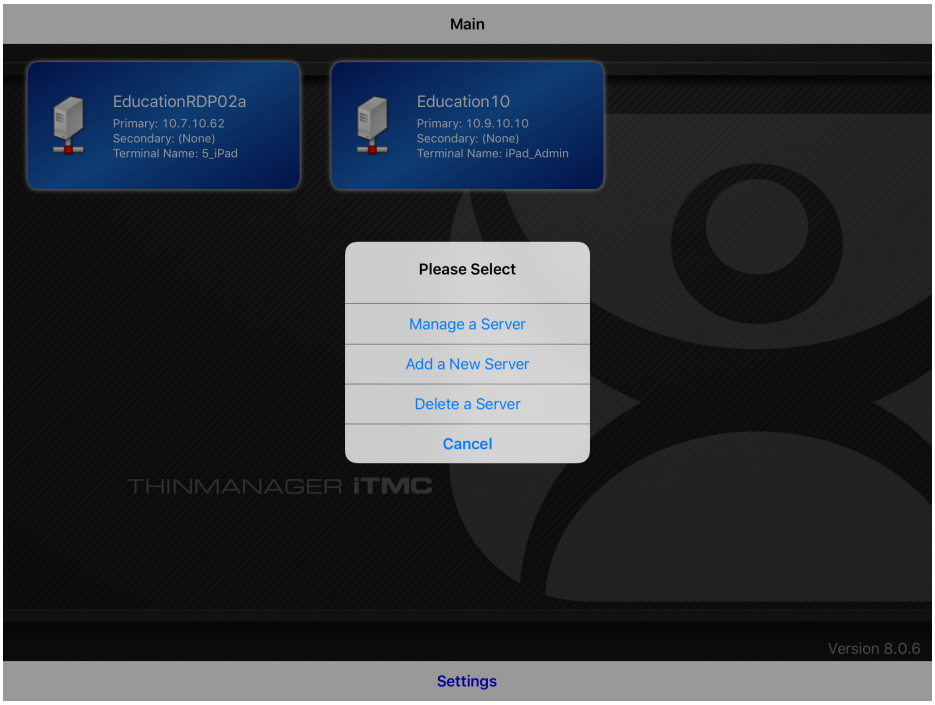
Register QR Codes with an iPad

QR codes must be registered with a mobile device.

1. Open the iTMC program on the iPad®.
2. Press Settings at the bottom-center to launch the Settings dialog box.

   A selection menu appears.

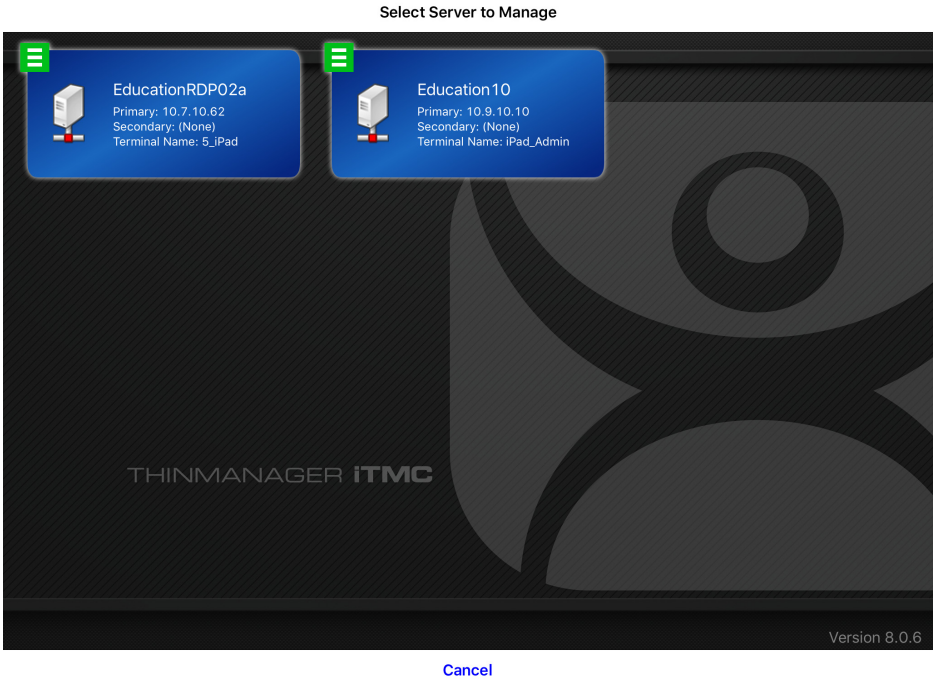
Figure 698 - iPad Settings Menu



3. Press Manage a Server.

   The Select Server to Manage screen appears.

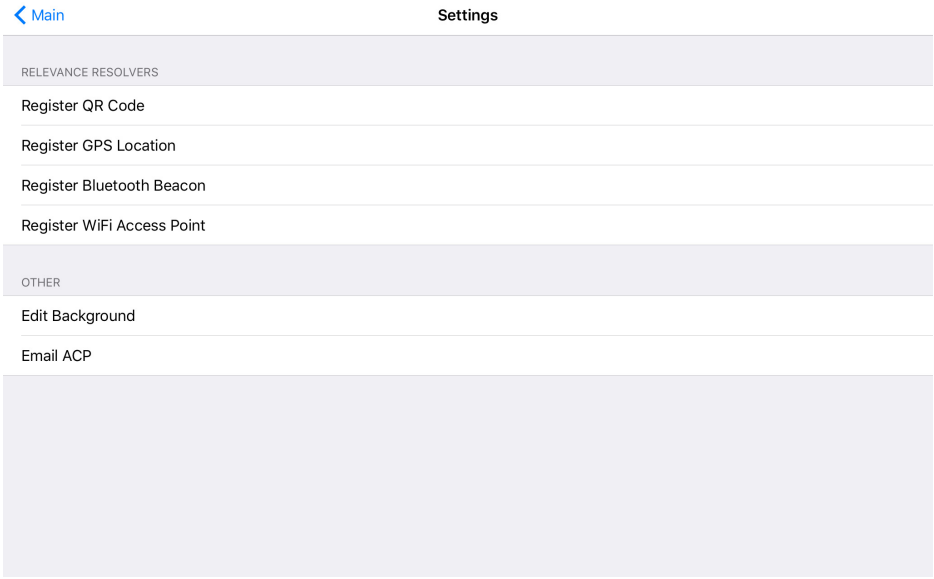
Figure 699 - Select Server to Manage Screen



4. Press the ThinManager Server to which you want to apply the QR Codes.

   The iTMC Settings page appears, which has the links to register the various resolvers.

Figure 700 - iTMC Settings Page



5. Press Register QR Code, which opens the camera to scan and register the QR Code.

Figure 701 - Scan New QR Code

6. Point the camera at the QR Code. Once the QR Code is framed in the window, it reads the code and registers it.

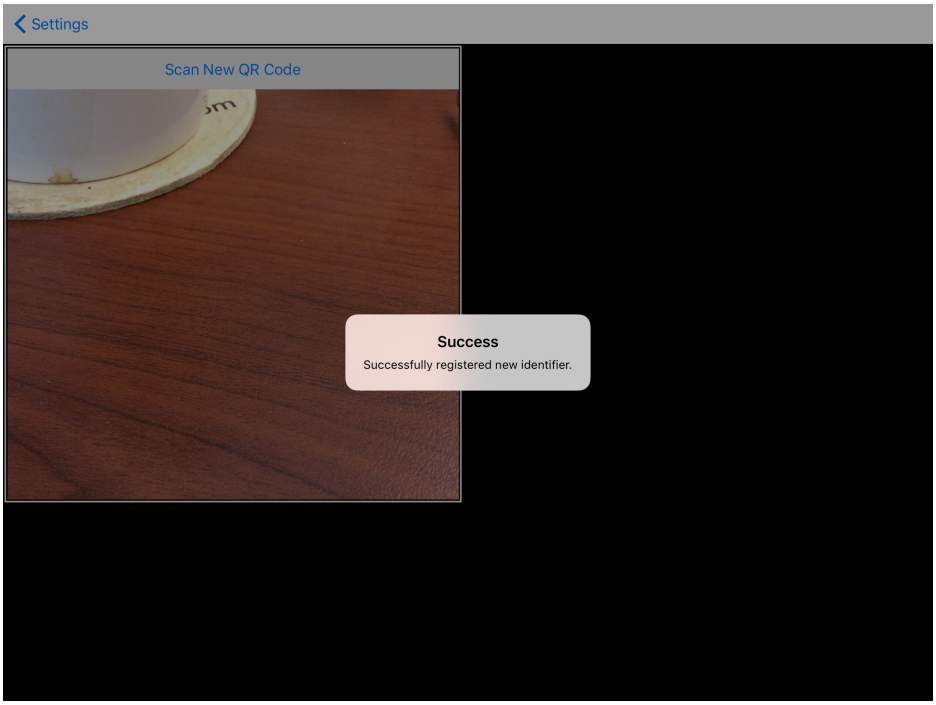
   Once the iTMC program reads the QR code, it asks you to name it.

Figure 702 - Enter Description for QR Code

7. Type a description in the Enter Description dialog box.
8. Click OK.

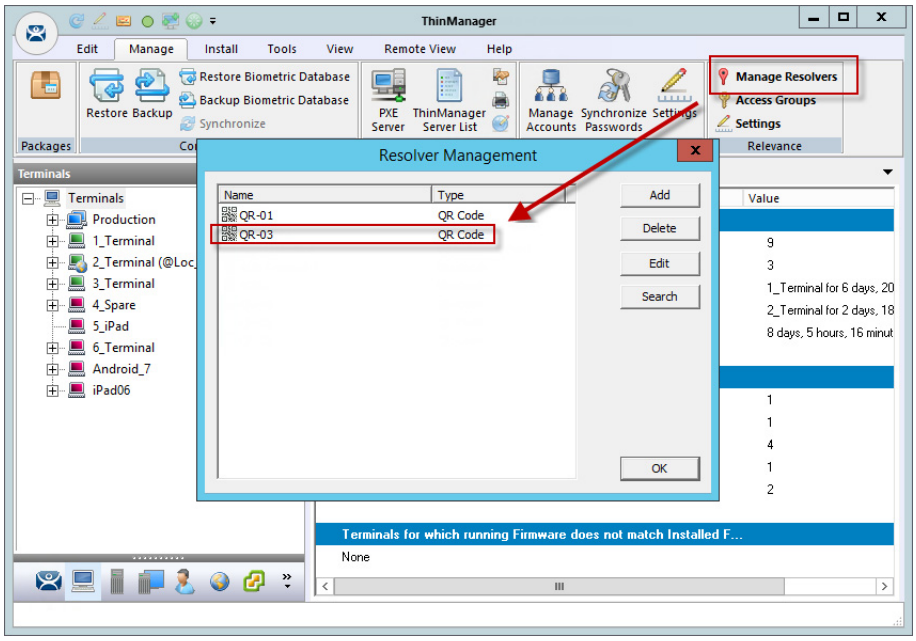
   The iTMC program confirms a successful registration.

Figure 703 - Successful Registration Confirmation



The Resolvers are listed in the Resolver Management dialog box.

Figure 704 - QR Code in Resolver Management Dialog Box



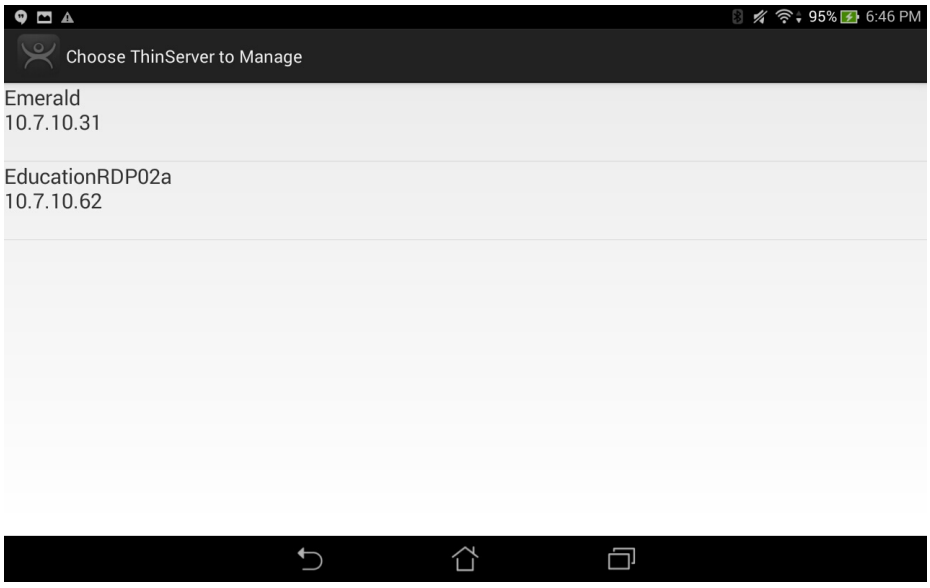
9. Choose Manage>Manage Resolvers from the ThinManager menu bar to open the Resolver Management dialog box.

Register QR Codes with an Android Device

QR codes need to be registered with a mobile device.

1. Open the aTMC program on the Android device.

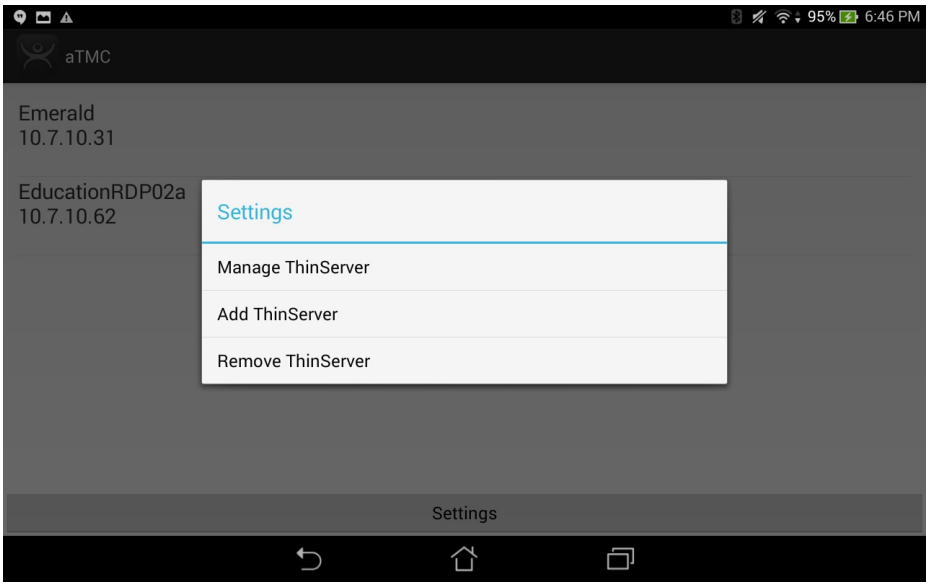
Figure 705 - aTMC Home Screen



2. Press Settings on the bottom.

   The Settings dialog box appears.

Figure 706 - Settings Menu



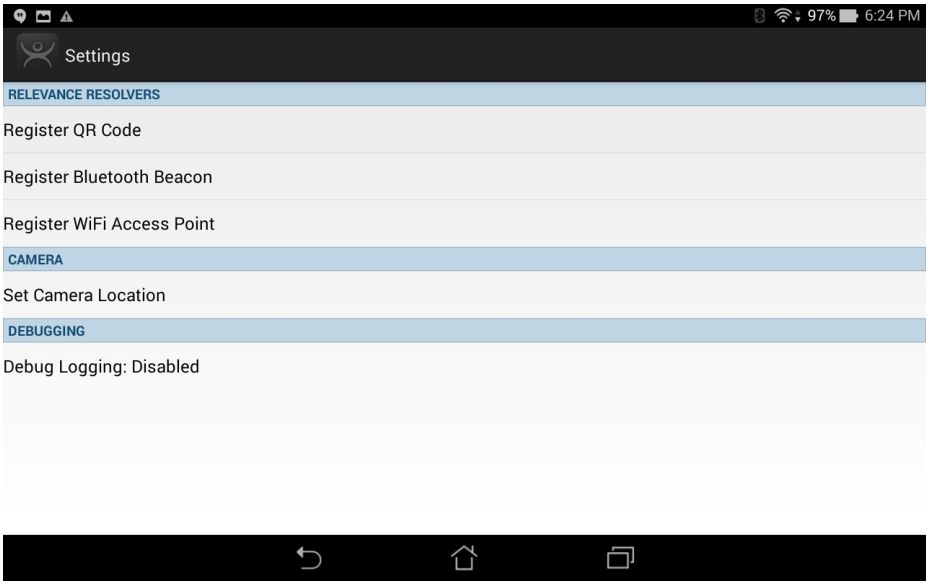
3. The Setting menu provides these choices.

Setting	Description
Manage ThinServer	Press to open the Settings Menu and register resolvers.
Add ThinServer	Press to open the Add New ThinServer page, which lets you define a new ThinManager Server.
Remove ThinServer	Press to allow you to delete a defined ThinManager Server.

If you have multiple ThinManager Servers defined, you must select the ThinManager Server to which you want to apply the QR codes.

The Settings page contains the links to register the various resolvers.

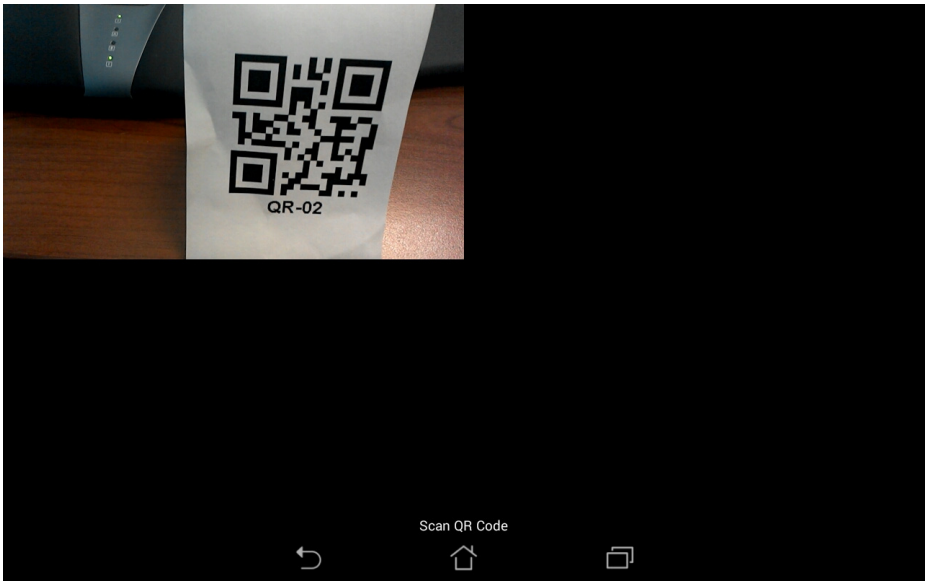
Figure 707 - aTMC Settings Page



4. Press Register QR Code.

   The camera opens to scan and register the QR Code.

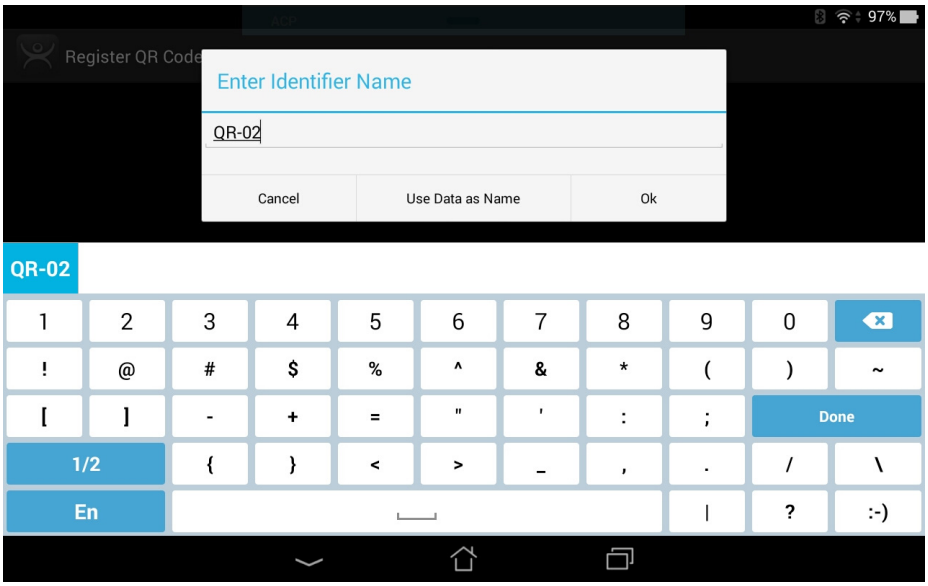
Figure 708 - Scan New QR Code



5. Point the camera at the QR Code. Once it is framed in the window, it reads the code and registers it.

   Once the aTMC program reads the QR code, it asks you to name it.

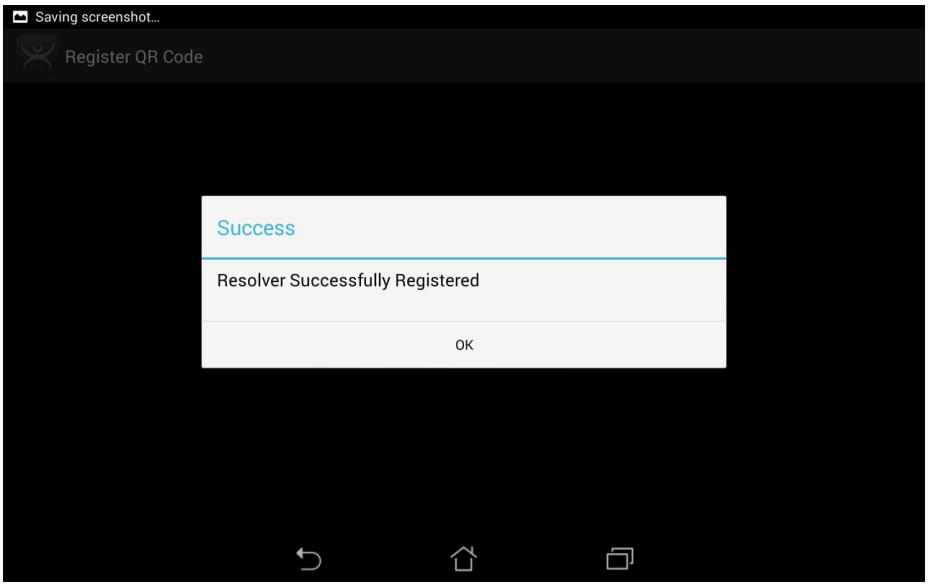
Figure 709 - Enter Description for QR Code



6. Type the name for the Resolver in Enter Identifier Name dialog box.
7. Click Ok.

   The aTMC program confirms a successful registration.

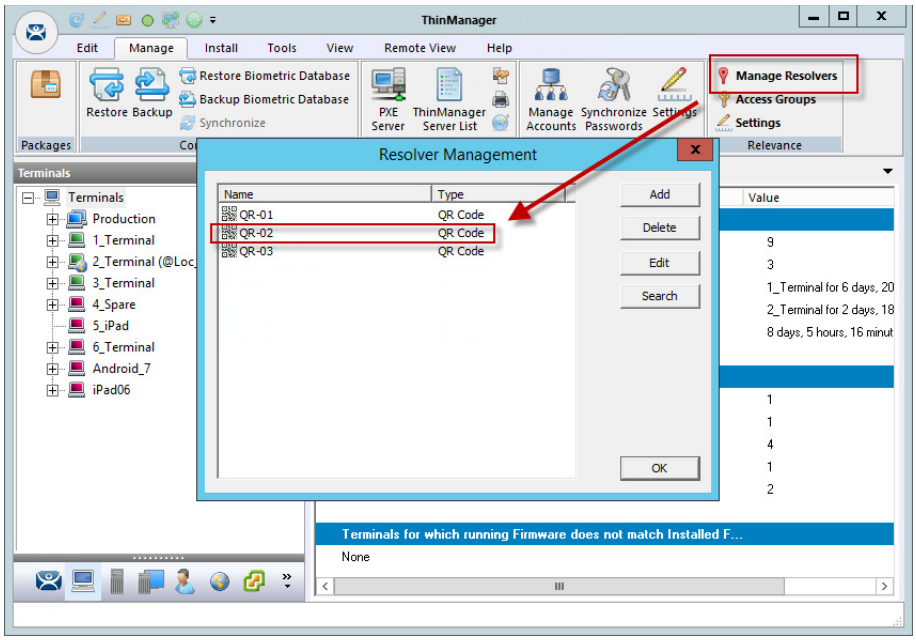
Figure 710 - Successful Registration Confirmation



8. Click OK.

   The Resolvers are listed in the Resolver Management dialog box.

Figure 711 - QR Code in Resolver Management



9. Choose Manage>Manage Resolvers from the ThinManager menu bar to open the Resolver Management dialog box.

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 must support Bluetooth Version 4.0 or later. In the case of an iPad, this is any iPad (regular, Mini, or Air) that uses the Lightning connector.

Relevance can use Bluetooth beacons as location resolvers. These must be Low Energy Bluetooth beacons that provide a unique name in the Advertising Packet.

See Fencing and Sub-Locations on page 449 for details.

To add new beacons to the system, you can use the mobile device to find 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 automatically adds 10 to this number for the exit point. You can adjust these in ThinManager in the Manage Resolvers section.

Here is how to define a Bluetooth beacon with a mobile device.

1. Place the Bluetooth beacons in the locations you want.
2. Launch the iTMC or aTMC program and press Settings.
3. Press Register Bluetooth Beacon command under the Relevance Resolvers section. If you have more than one ThinManager Server defined, you must pick the ThinManager Server on which you want the Bluetooth beacons registered.
4. Choose the desired Bluetooth beacon from the generated list.
5. Type a name and press Register.
6. Choose Manage>Manage IDs.

   The Resolver Management dialog box appears, in which the Bluetooth beacon is registered and entered.

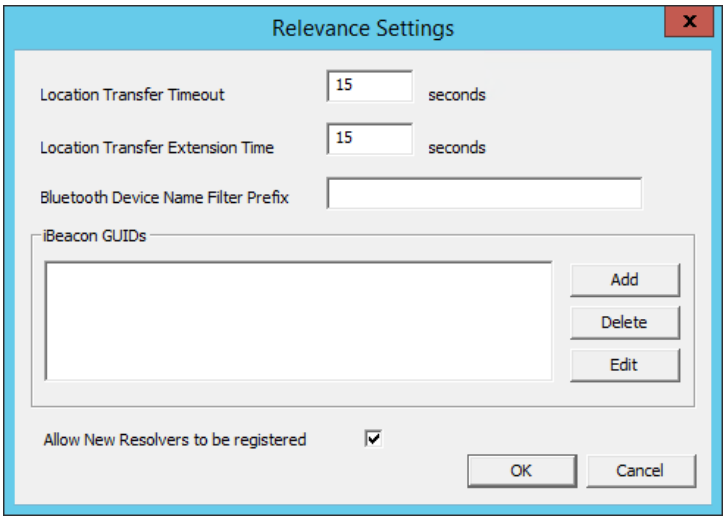
Relevance Settings

The Relevance Settings dialog box has some settings that can affect Bluetooth beacons.

1. Choose Manage>Relevance Settings on the ThinManager menu bar.

   The Relevance Settings dialog box appears.

Figure 712 - Relevance Settings



These are the settings available in the Relevance Settings dialog box.

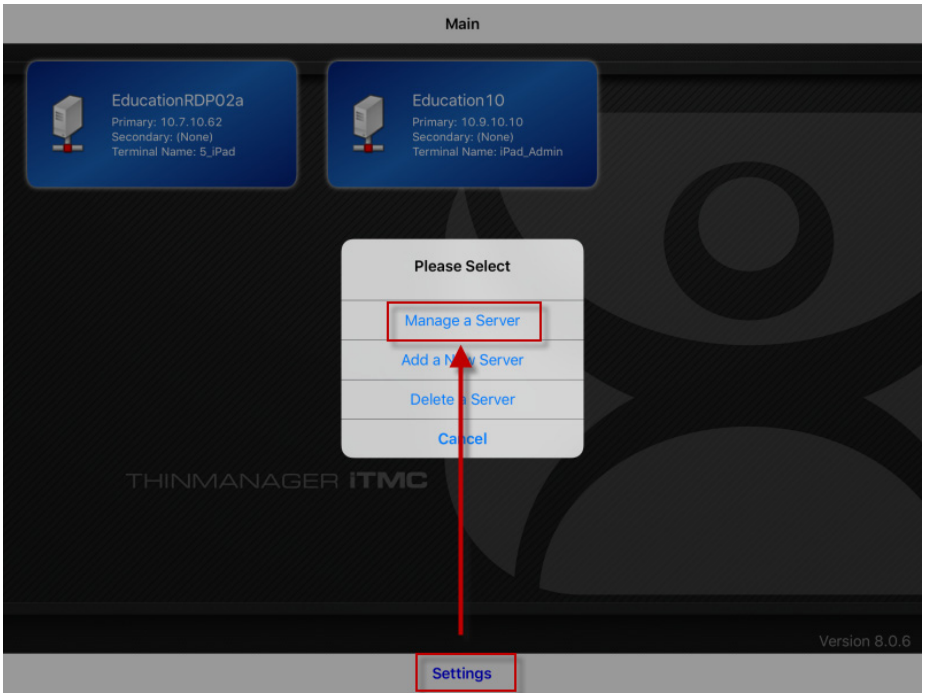
Setting	Description
Location Transfer Timeout	Sets the time that an operator has to acknowledge and allow a Transfer. See Transfer on page 476.
Location Transfer Extension Time	Sets the interval of extra wait time that a refused transfer allows.
Bluetooth Device Name Filter Prefix	Enter a name in this field to limit the display of Bluetooth devices that have that prefix, which is helpful because ThinManager Bluetooth devices have an ACP prefix.
iBeacon GUIDs	Shows the registered iBeacons.
Add	Click to open the Enter iBeacon GUID dialog box, which allows definition of a new iBeacon.
Delete	Click to delete a highlighted iBeacon from the list.
Edit	Click to edit a highlighted iBeacon in the Enter iBeacon GUID dialog box.
Allow New Resolvers to be registered	Allows new resolvers. Clear this checkbox to prevent the addition of Bluetooth beacons by unauthorized users.

Bluetooth Beacons Defined on an iPad

Define a Bluetooth beacon similarly to how you define a QR code.

1. Open the iTMC program on the iPad.

Figure 713 - ThinManager iTMC Program



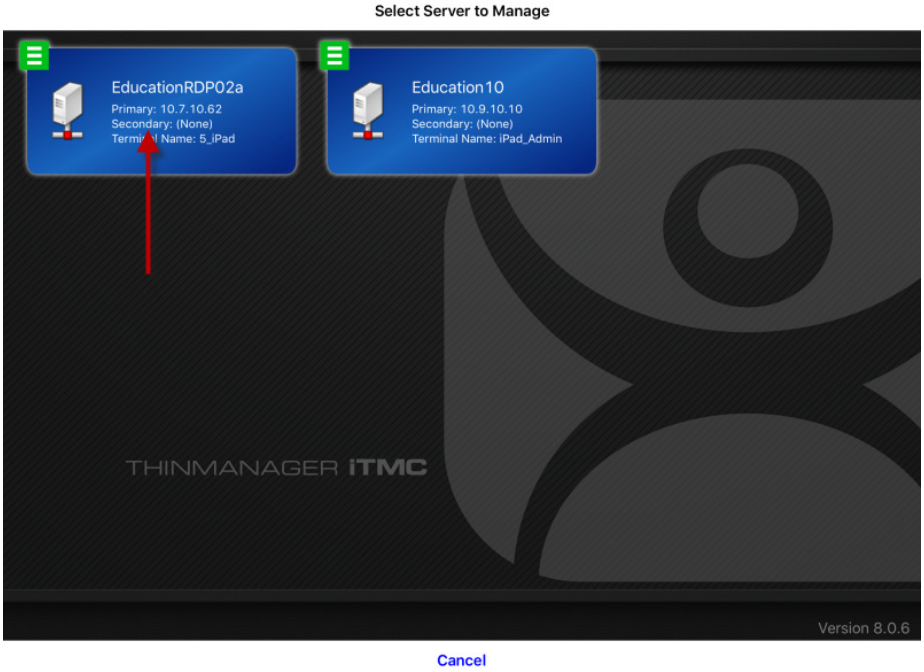
2. Press Settings on the bottom of the screen.

   The Settings menu dialog box appears.

3. Press Manage a Server.

   The Select Server to Manage screen appears.

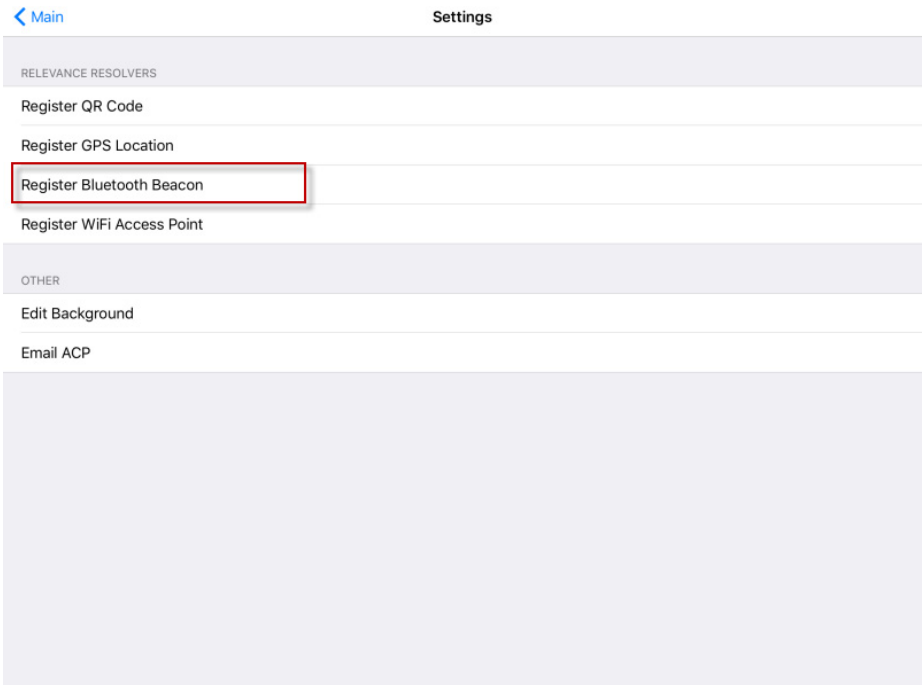
Figure 714 - Select Configuration



4. Press the ThinManager Server on which you want to register the Bluetooth beacon.

   The Settings page appears.

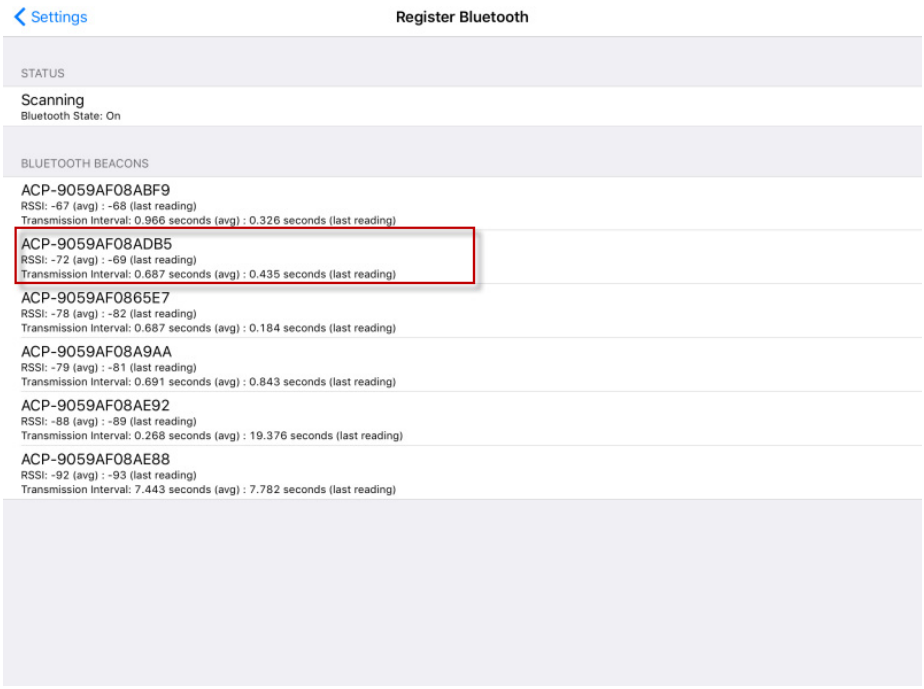
Figure 715 - Register Bluetooth Beacon Command on the Settings Page



5. Press Register Bluetooth Beacon on the Settings page.

   The Register Bluetooth page appears, which lists the Bluetooth beacons the mobile device finds.

Figure 716 - Available Bluetooth Beacons



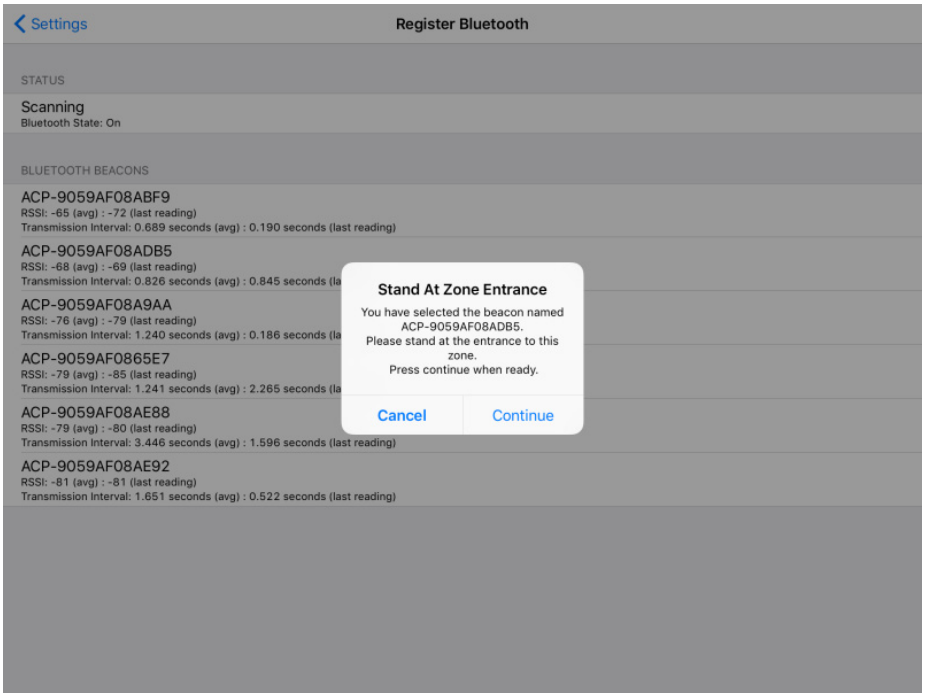
6. Press the desired Bluetooth beacon.

ACP-9059AF08ADB5 was chosen in Figure 716.

This ThinManager Server is using ACP as a filter in the Relevance Settings dialog box to limit the number of Bluetooth beacons shown. See Bluetooth Beacons on page 490 for details.

The mobile device prompts you to go to the location that you want as the entrance point for the zone.

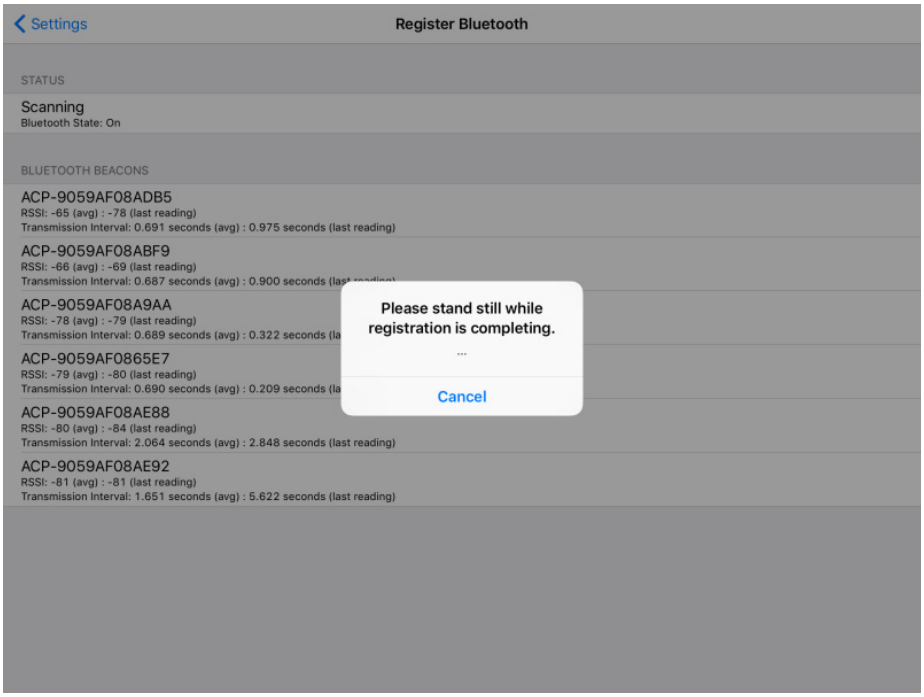
Figure 717 - Stand At Zone Entrance Dialog



7. Press Continue.

It can take a few seconds to allow the device to read the signal strength to create the resolver data.

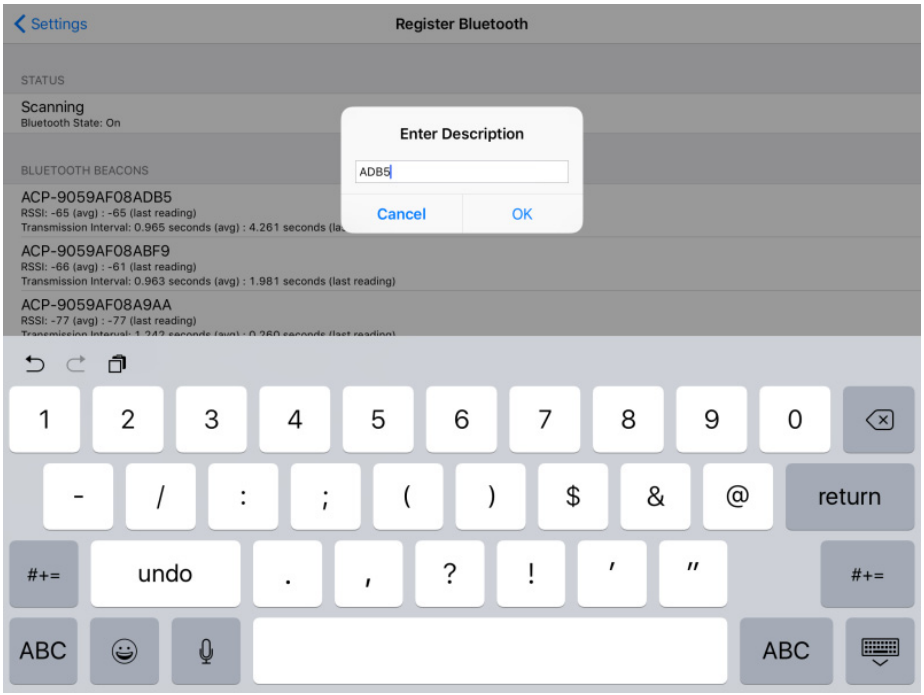
Figure 718 - Stand Still Message



8. Do not move around while the device registers.

Once the data is collected and the Bluetooth beacon is registered, you are prompted to name the location.

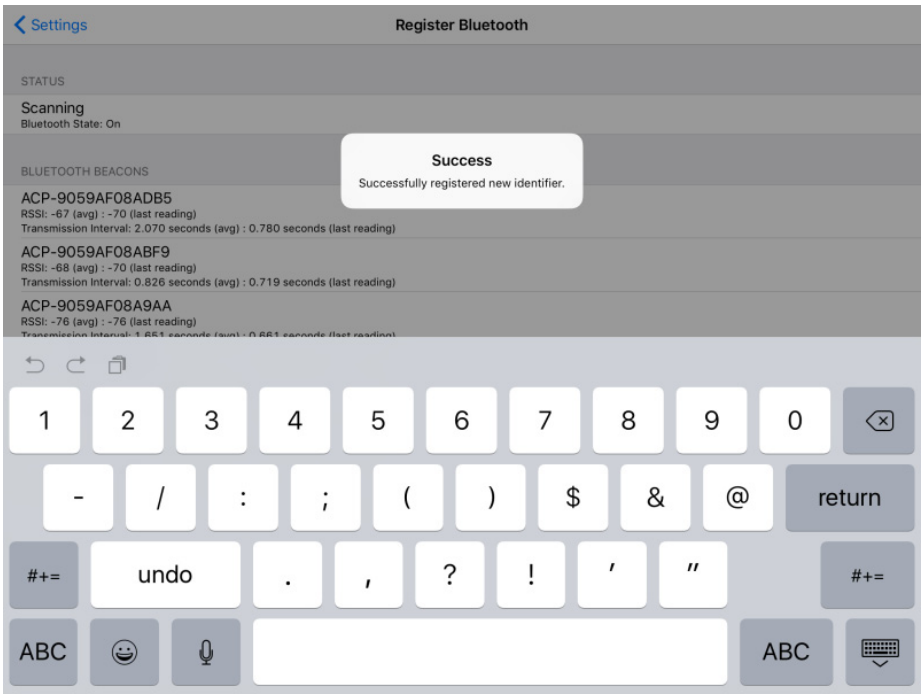
Figure 719 - Enter Location Description



9. Type a Description and click OK.

   The program confirms successful Bluetooth registrations.

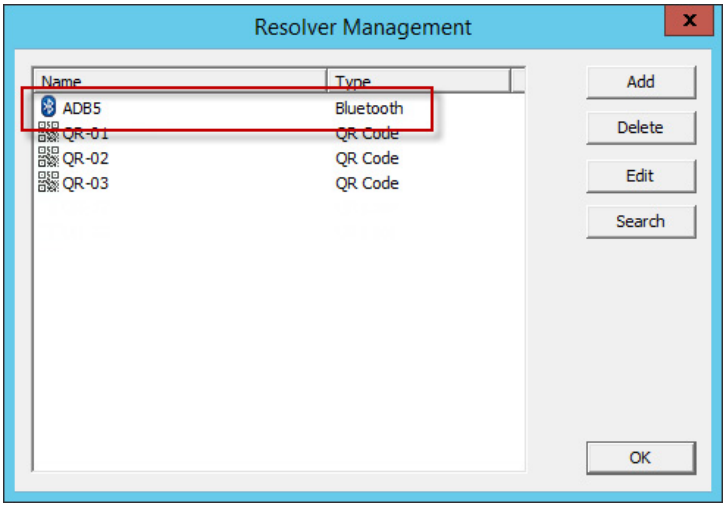
Figure 720 - Success Dialog Box



10. Choose Manage>Manage IDs.

    The Resolver Management dialog box appears, where the QR Code is registered and entered.

Figure 721 - Resolver Management

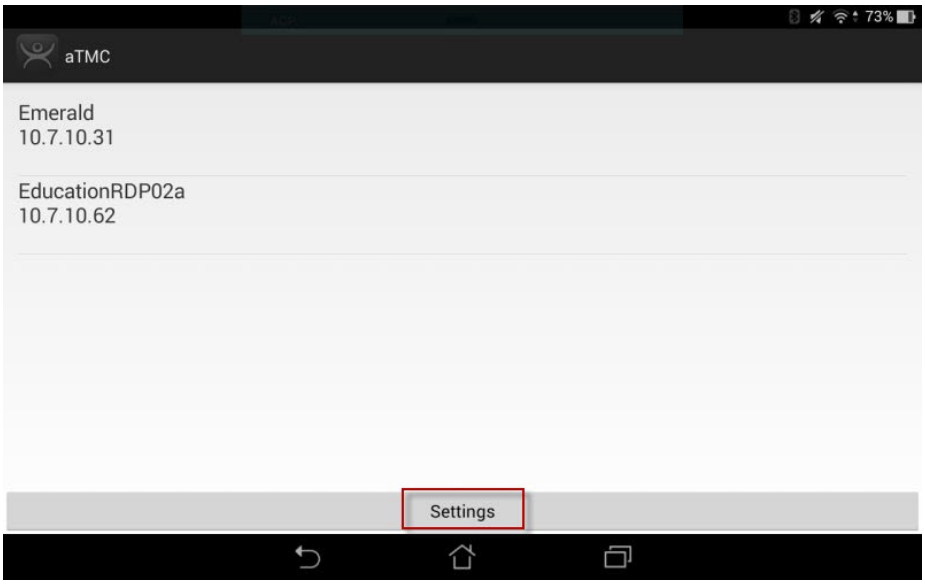


Bluetooth Beacons Defined on an Android

This is the procedure defines a Bluetooth beacon with an Android tablet.

1. Open the aTMC program on the Android tablet.

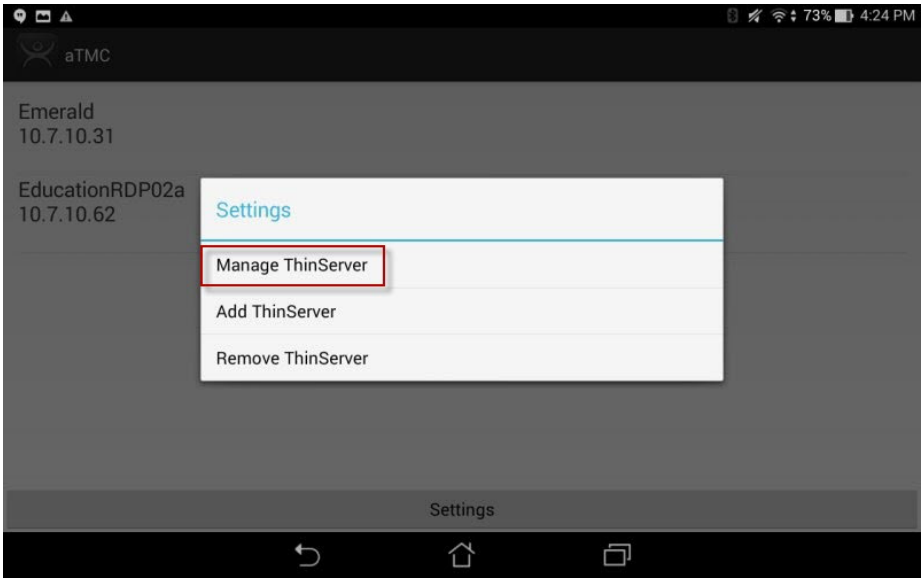
Figure 722 - ThinManager aTMC Program



2. Press Settings on the bottom.

   The Settings dialog box appears.

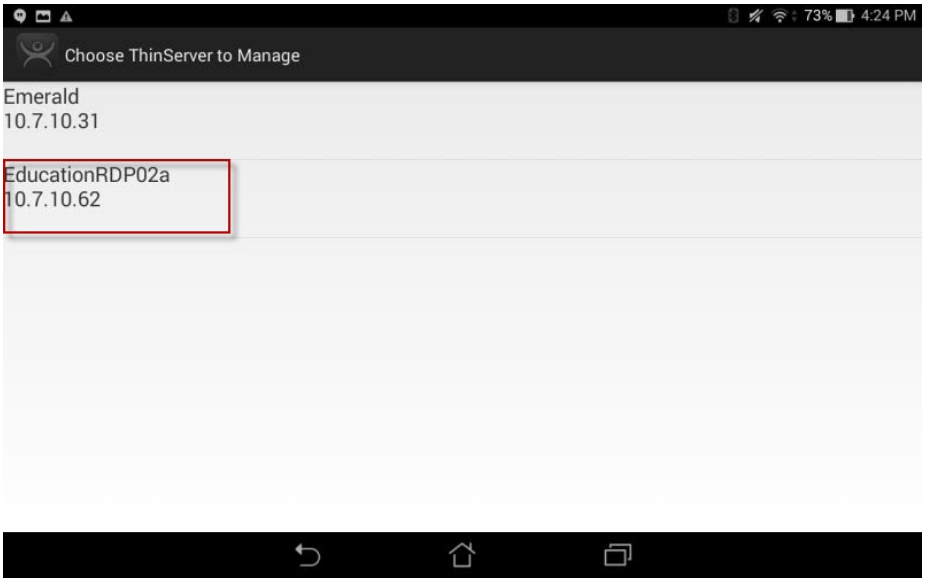
Figure 723 - Settings Menu



3. Press Manage ThinServer.

   The Choose ThinServer to Manage page appears.

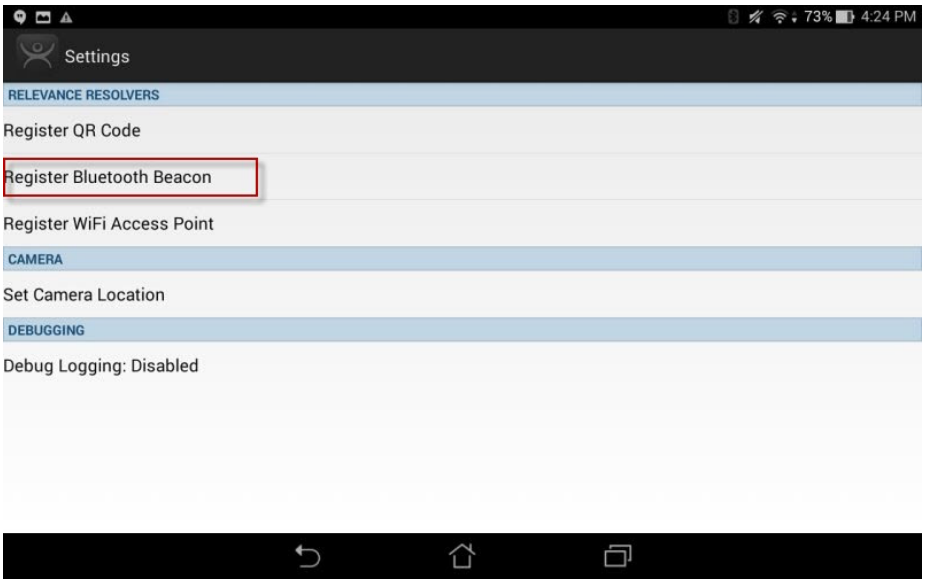
Figure 724 - Select Configuration



4. Press the ThinManager Server on which you want to register the Bluetooth beacon.

   The Settings page appears.

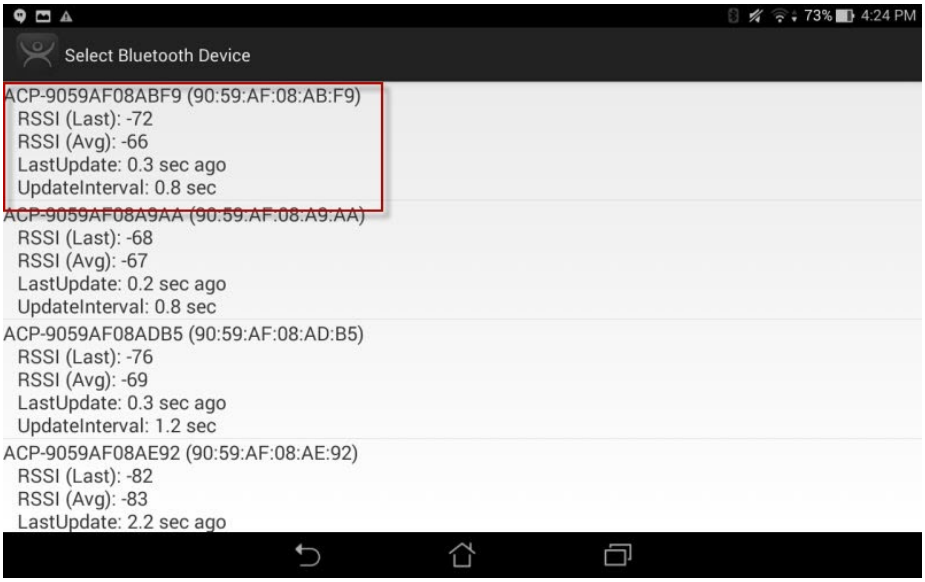
Figure 725 - Register Bluetooth Beacon Command



5. Press Register Bluetooth Beacon.

   The Bluetooth beacons that the mobile device finds are listed on the Register Bluetooth page.

Figure 726 - Available Bluetooth Beacons



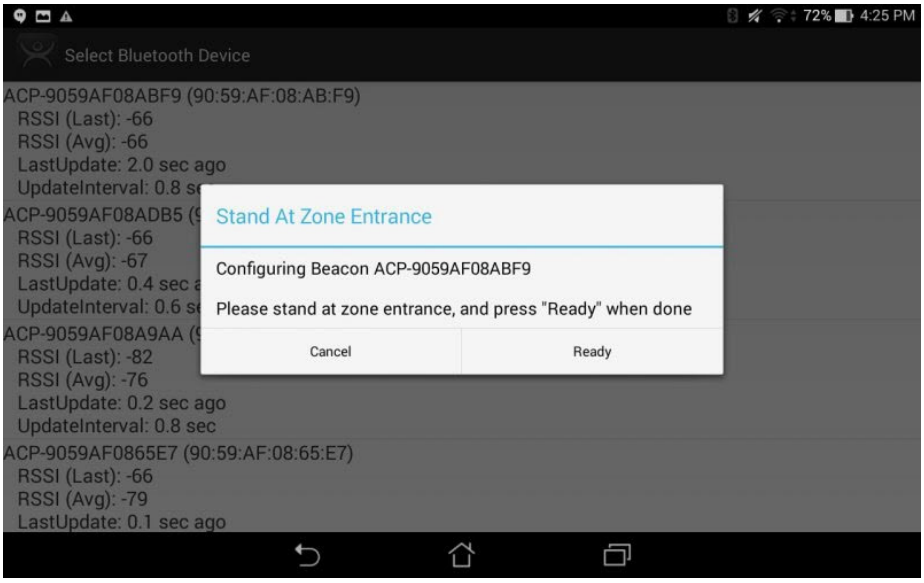
6. Press the desired Bluetooth beacon.

   In Figure 726, ACP-9059AF08ABF9 was selected.

This ThinManager Server is using ACP as a filter in the Relevance Settings dialog box. See Bluetooth Beacons on page 490 for details.

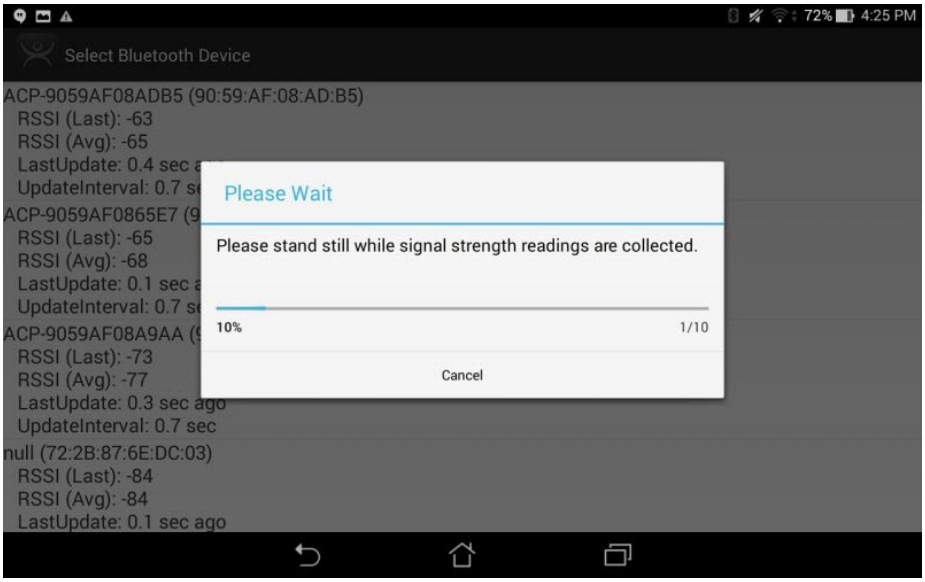
The mobile device prompts you to go to the location that you want as the entrance point for the zone.

Figure 727 - Stand At Zone Entrance Dialog Box



7. Press Ready.

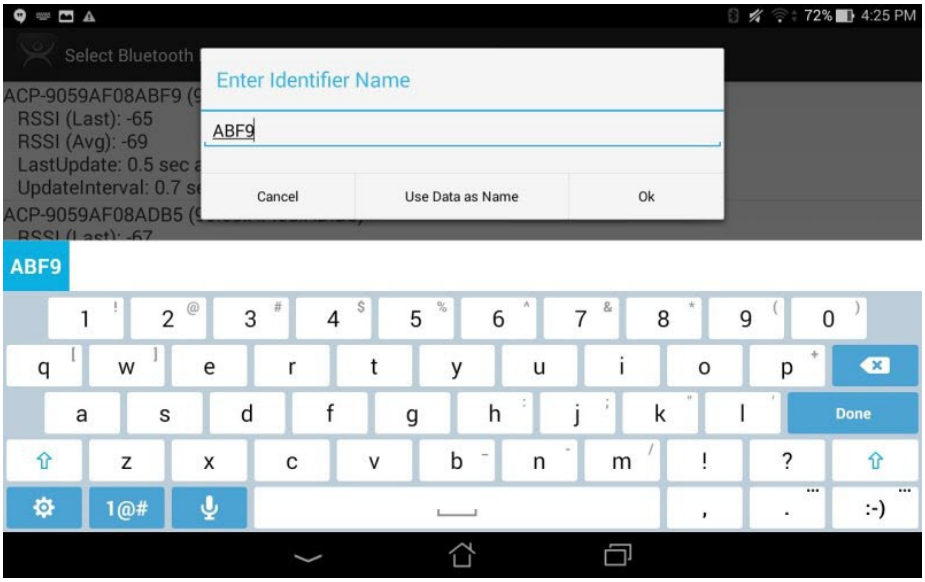
Figure 728 - Please Wait Message



It can take a few seconds to allow the device to read the signal strength to create the resolver data.

Once the data is collected and the Bluetooth beacon is registered, you are prompted to name the location.

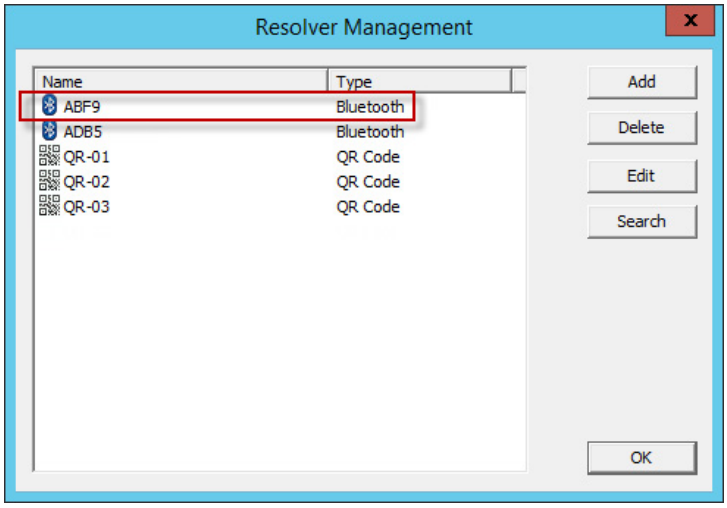
Figure 729 - Enter Location Description



8. Type a Name for the location and click Ok.
9. Choose Manage>Manage IDs.

   The Resolver Management dialog box appears with the Bluetooth beacon displayed.

Figure 730 - Resolver Management Dialog Box



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 gives you access to functions in that area.

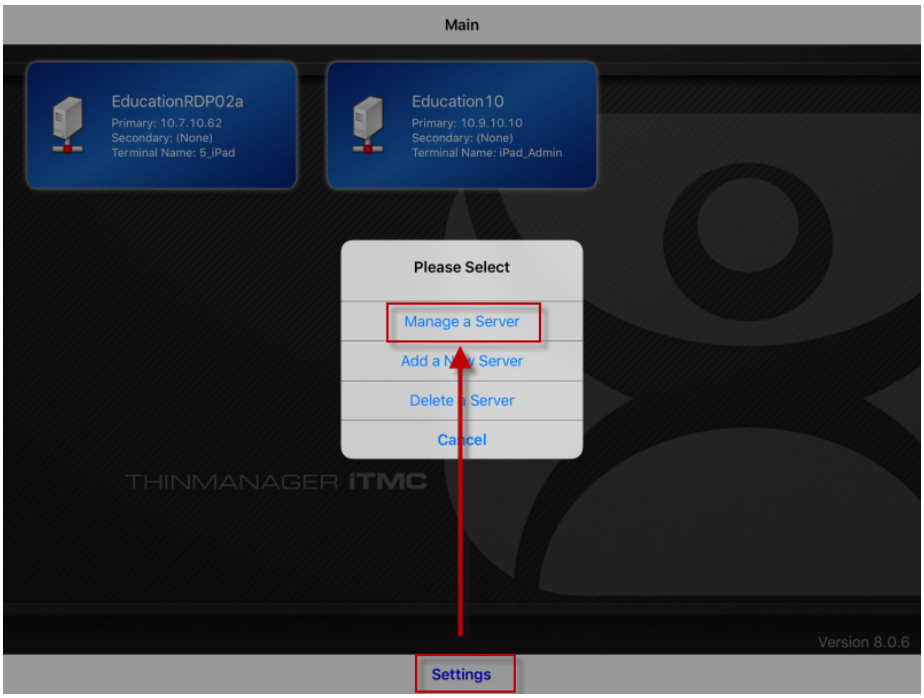
See Fencing and Sub-Locations on page 449 for details.

iPad-defined Wi-Fi Access Points

The Wi-Fi resolver is defined like a Bluetooth beacon.

1. Open the iTMC program on the iPad.

Figure 731 - ThinManager iTMC Program

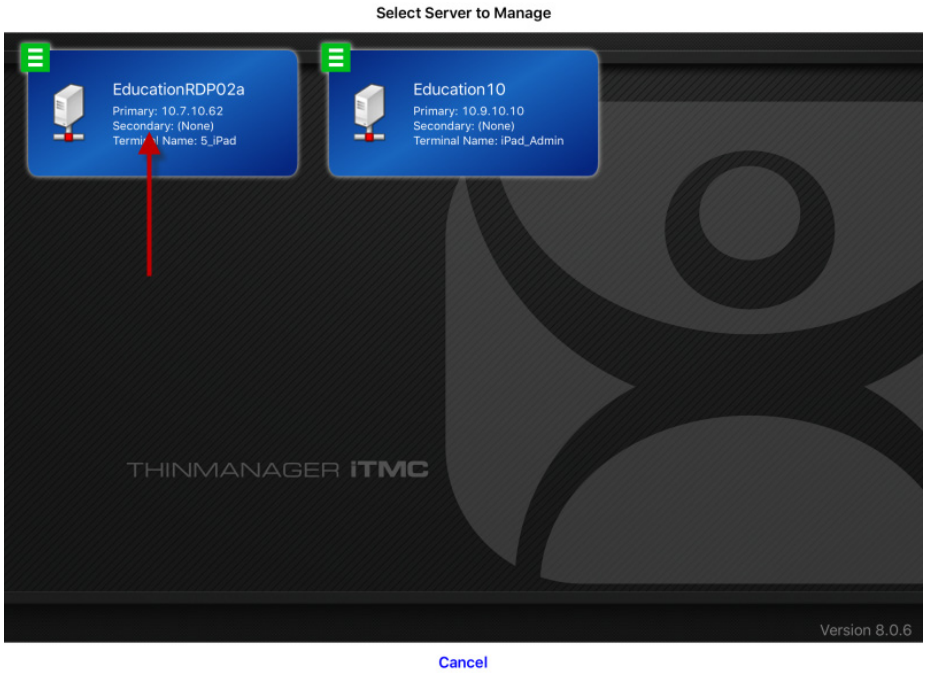


2. Press Settings on the bottom.

   The Settings menu dialog box appears.
3. Press Manage a Server.

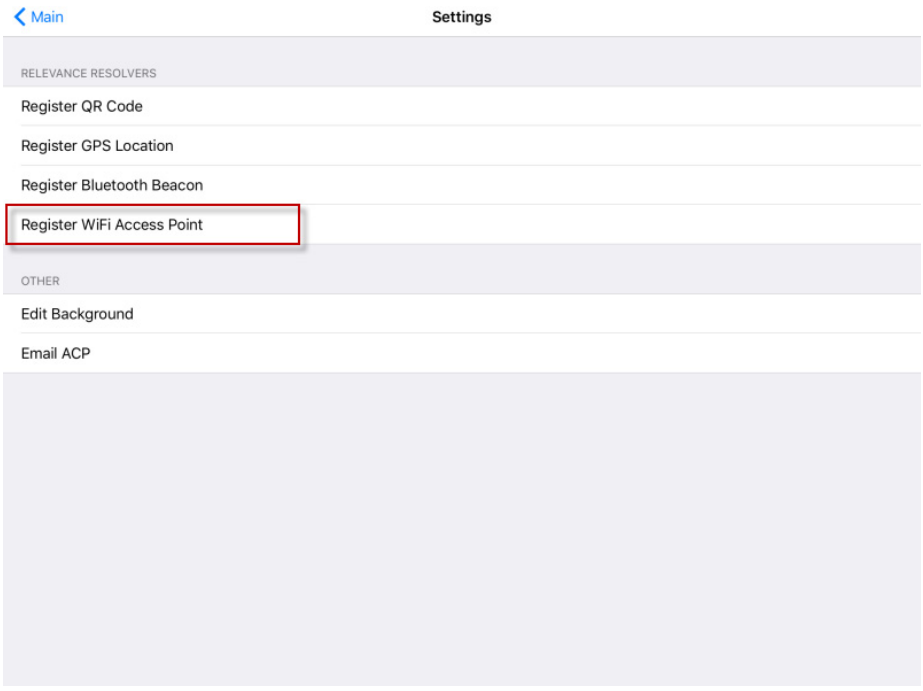
   The Select Server to Manage page appears.

Figure 732 - Select Configuration



4. Press the ThinManager Server on which you want to register the Wi-Fi resolver.

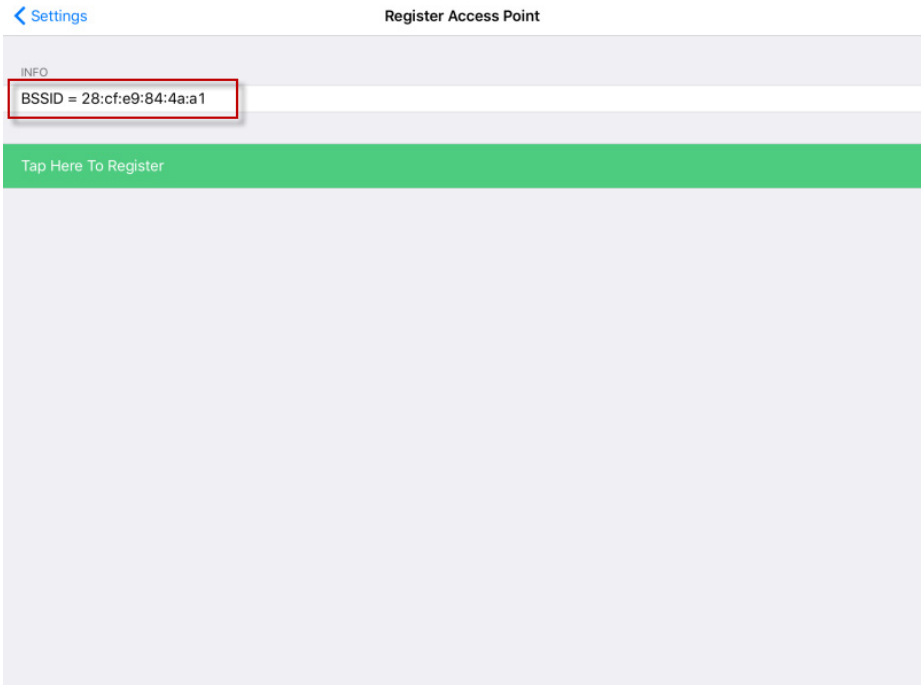
Figure 733 - Settings Page of iTMC



5. Press Register WiFi Access Point.

The Register Access Point page appears.

Figure 734 - Available Wi-Fi Access Points

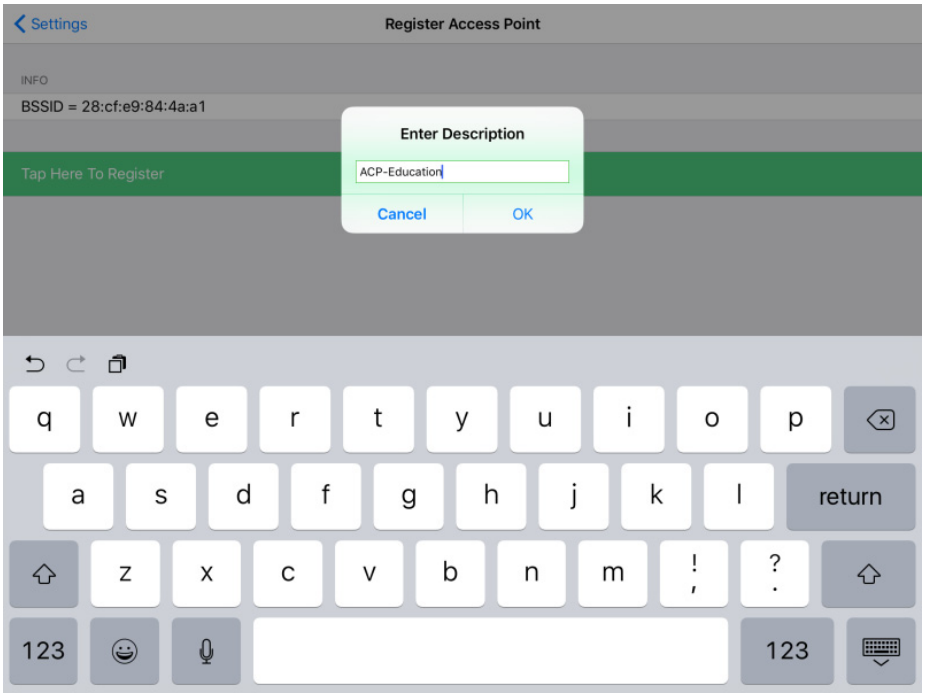


The mobile device allows you to register the Wi-Fi Access Point you are connected to and list it on the Register Access Points page.

6. Press the access point.

   Once the data is collected and the Wi-Fi access point is registered, you are prompted to name the location.

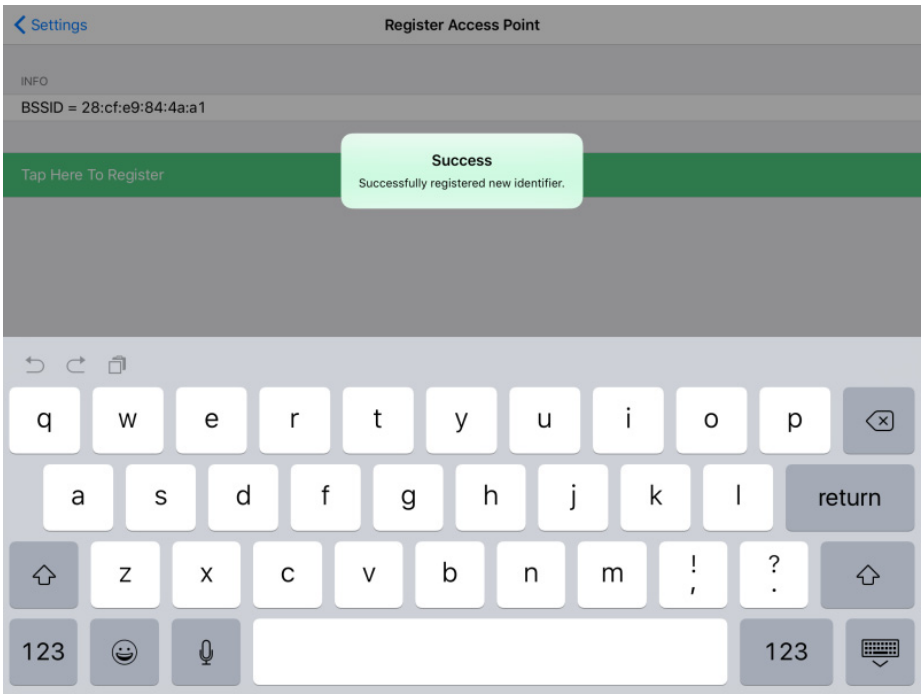
Figure 735 - Enter Location Description



7. Type a description and click OK.

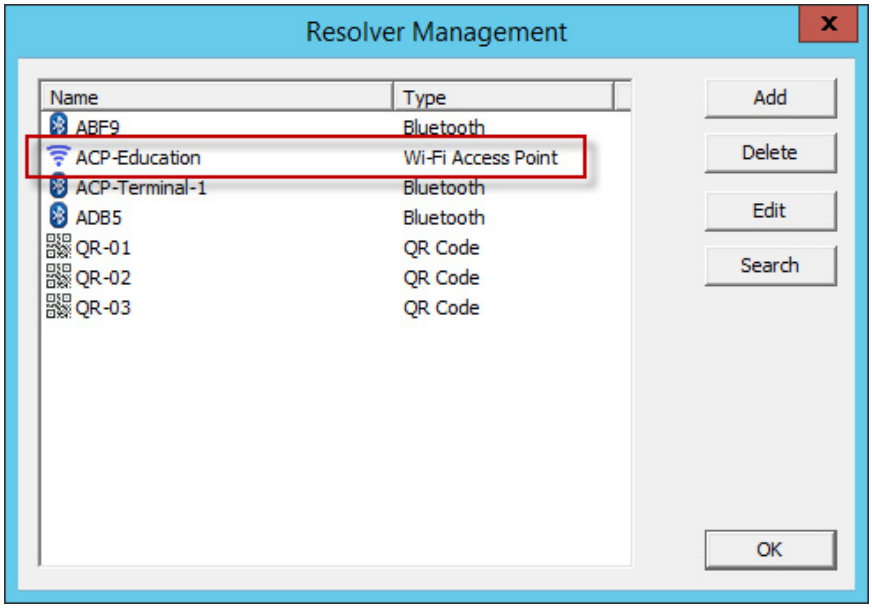
The program confirms successful Wi-Fi registrations with a Success dialog box.

Figure 736 - Success Dialog



8. Choose Manage>Manage IDs.

   The Resolver Management dialog box appears with the Wi-Fi resolver is registered and entered.

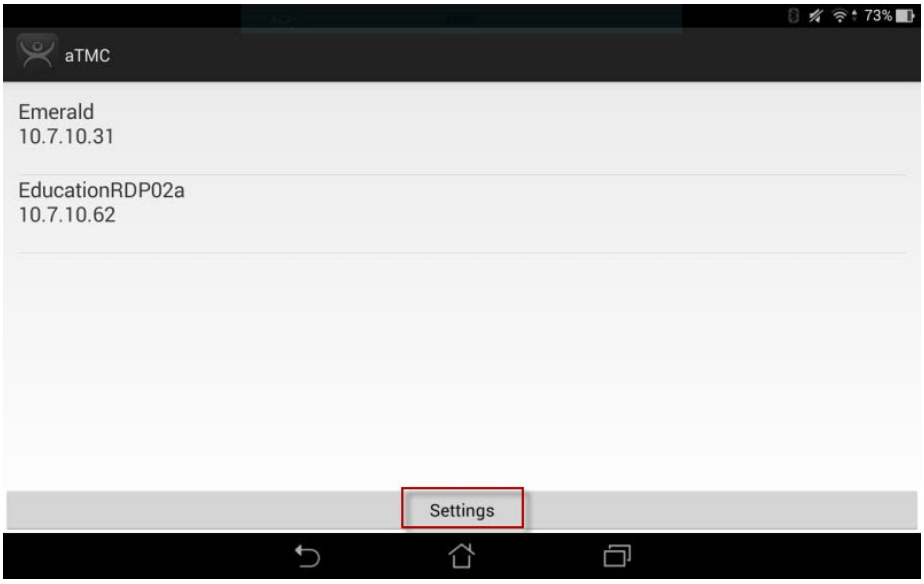


Android-defined Wi-Fi Access Points

Wi-Fi access points are defined and registered like the Bluetooth beacon.

1. Open the aTMC program on the Android tablet.

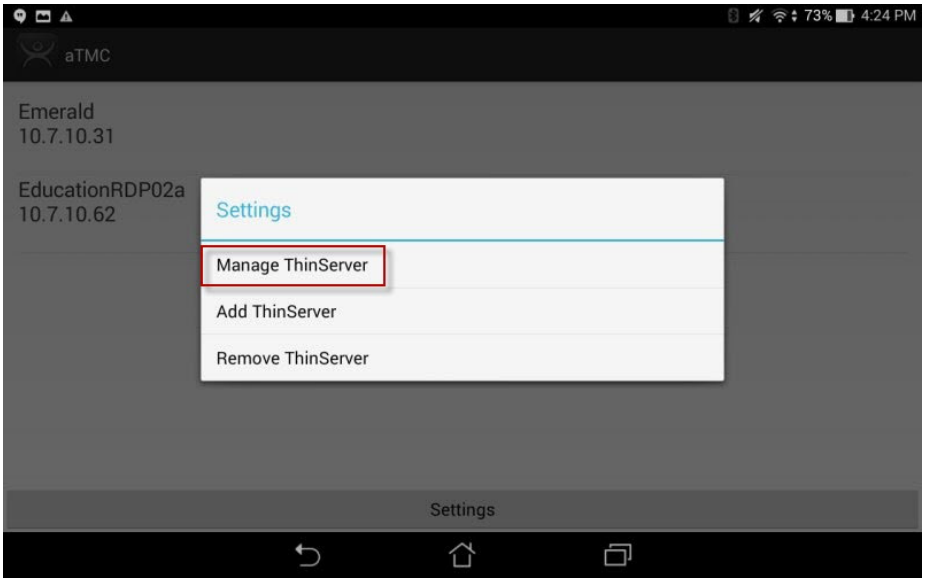
Figure 737 - ThinManager aTMC Program



2. Press Settings on the bottom.

   The Settings page appears.

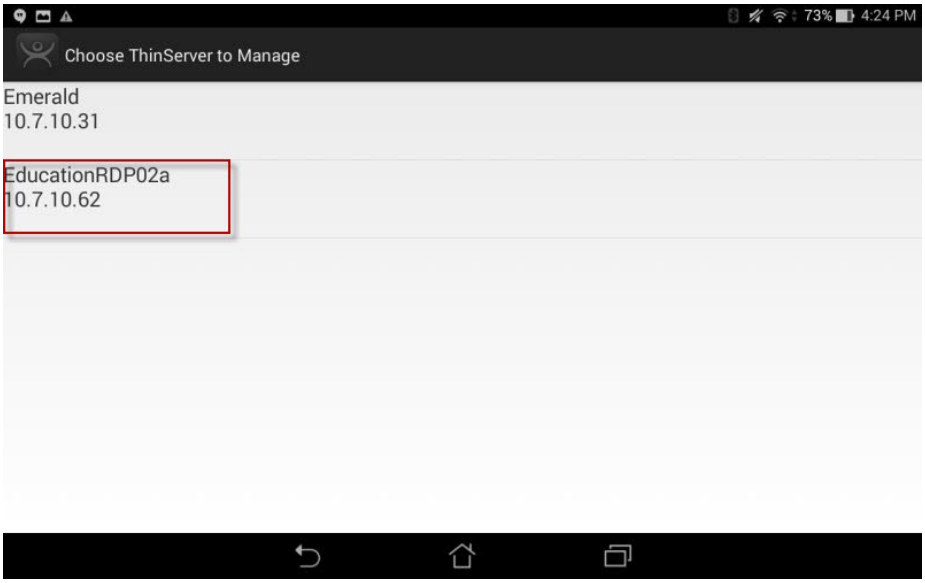
Figure 738 - Settings Menu



3. Press Manage ThinServer.

   The Choose ThinServer to Manage page appears.

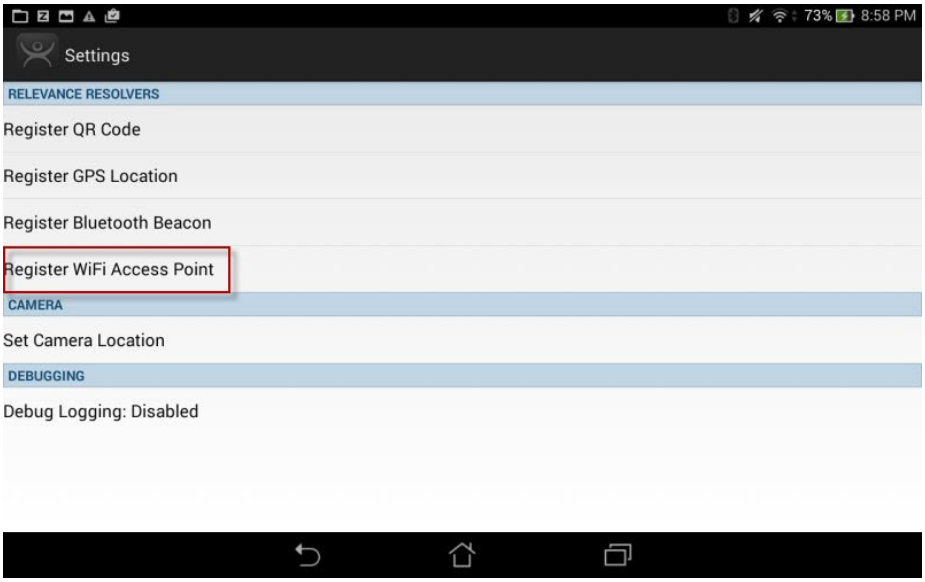
Figure 739 - Select Configuration



4. Press the ThinManager Server with which you want to register the Wi-Fi network.

   The Settings page appears.

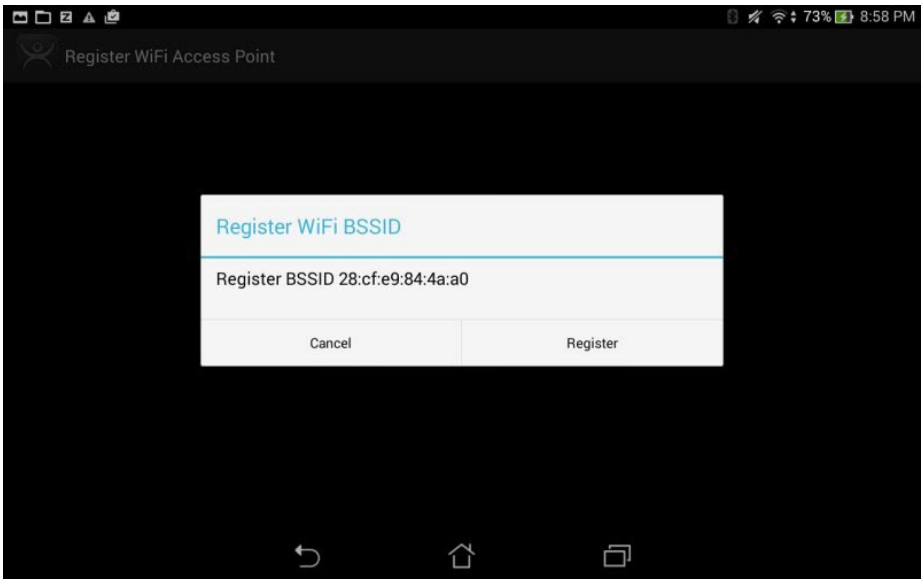
Figure 740 - Register Bluetooth Beacon Command



5. Press Register Wi-Fi Access Point on the Settings page.

   The Register WiFi BSSID dialog box appears.

Figure 741 - Register Configuration

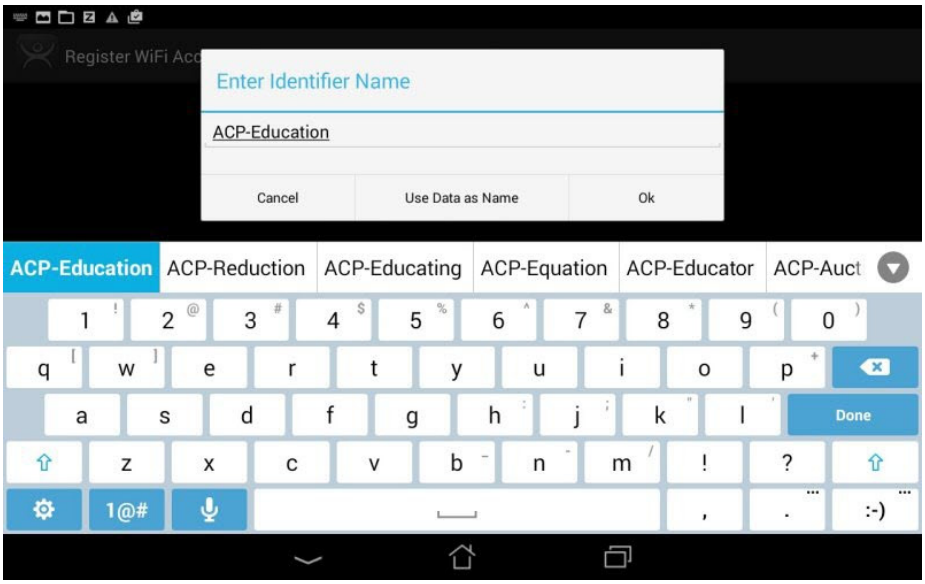


The ThinManager Server lets you register the wireless network to which you are connected.

6. Press Register.

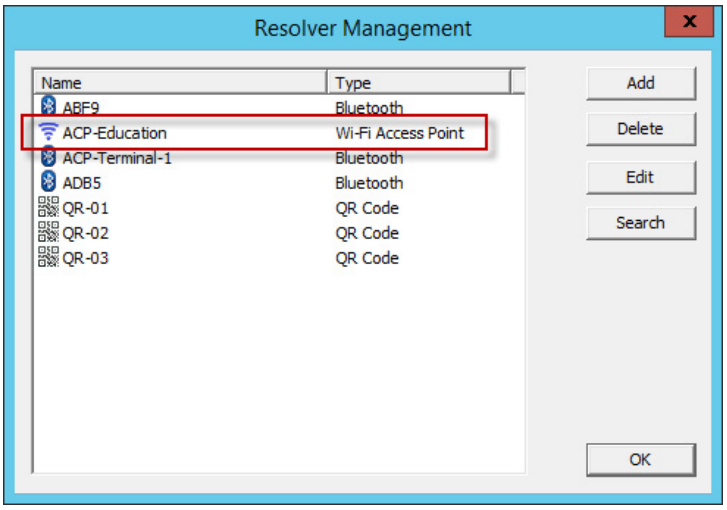
   Once the Wi-Fi access point is identified, you are prompted to name the location.

Figure 742 - Enter Location Description



7. Type a Name for the Wi-Fi access point and press Ok to finish the registration process.

Figure 743 - Resolver Management Dialog Box



8. Choose Manage>Manage IDs.

   The Resolver Management dialog box appears, where the Wi-Fi access point is registered and entered.

GPS

Relevance can use the Global Positioning System, or GPS, as a location resolver. The mobile program uses the built-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. Set it 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 gives 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 can also use it for finer resolution of individual buildings, tanks, pump jacks, or other smaller outdoor areas.

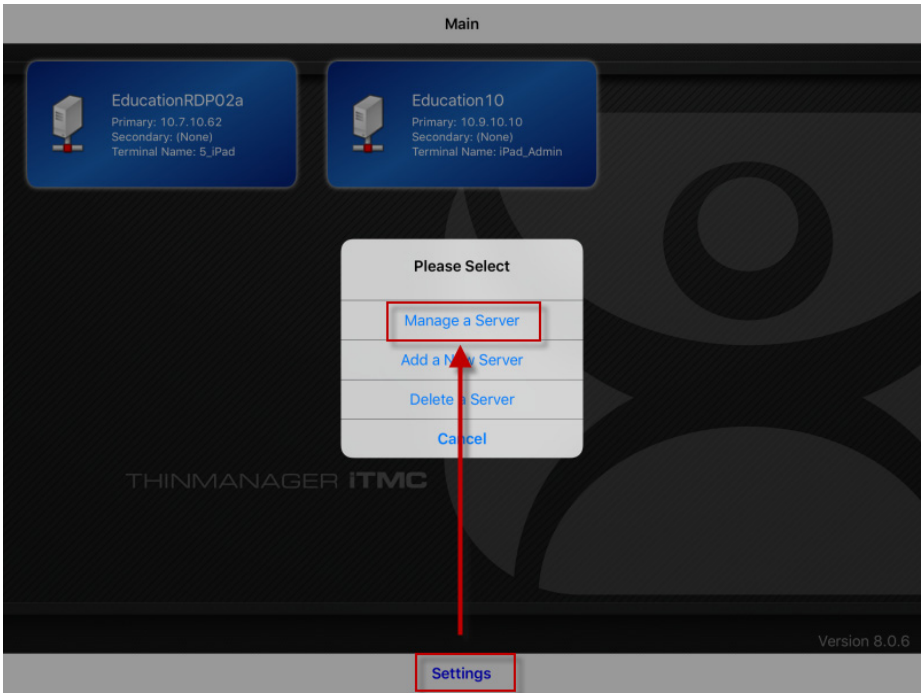
As you assign these types of resolvers, it is best to avoid overlap of GPS areas.

iPad-Registered GPS

Define a GPS location similarly to how you define a Bluetooth beacon.

1. Open the iTMC program on the iPad.

Figure 744 - ThinManager iTMC Program



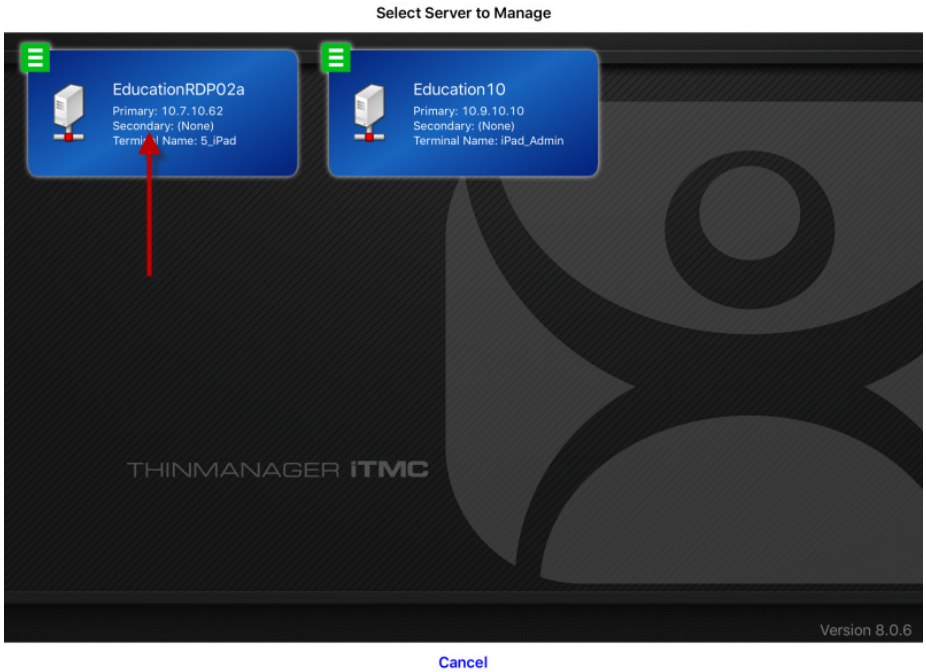
2. Press Settings on the bottom.

   The Settings menu dialog box appears.

3. Press Manage a Server.

   The Select Server to Manage page appears.

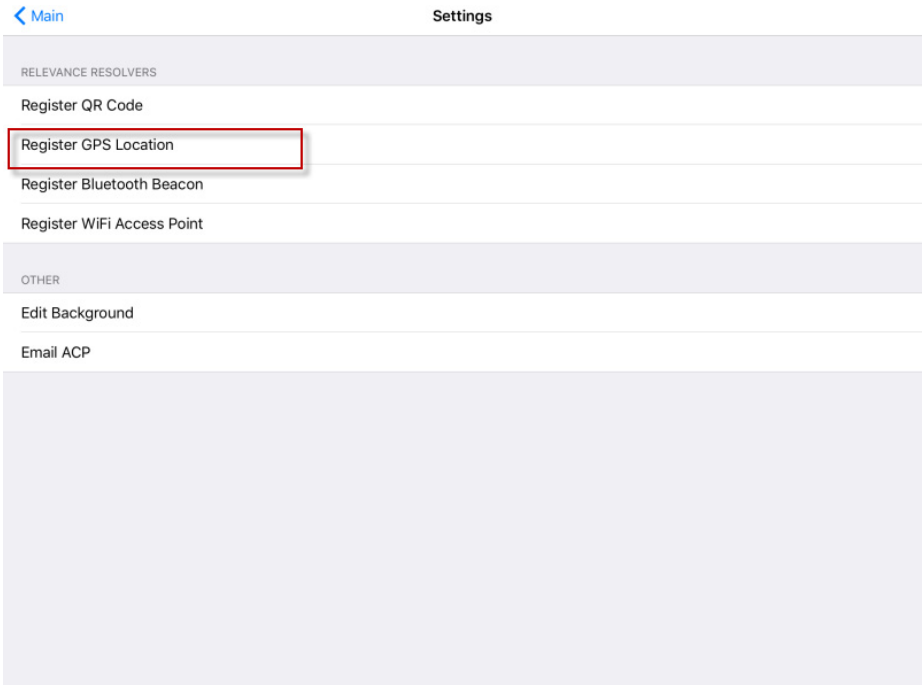
Figure 745 - Select Configuration



4. Press the ThinManager Server on which you want to register the GPS location.

   The Settings page appears.

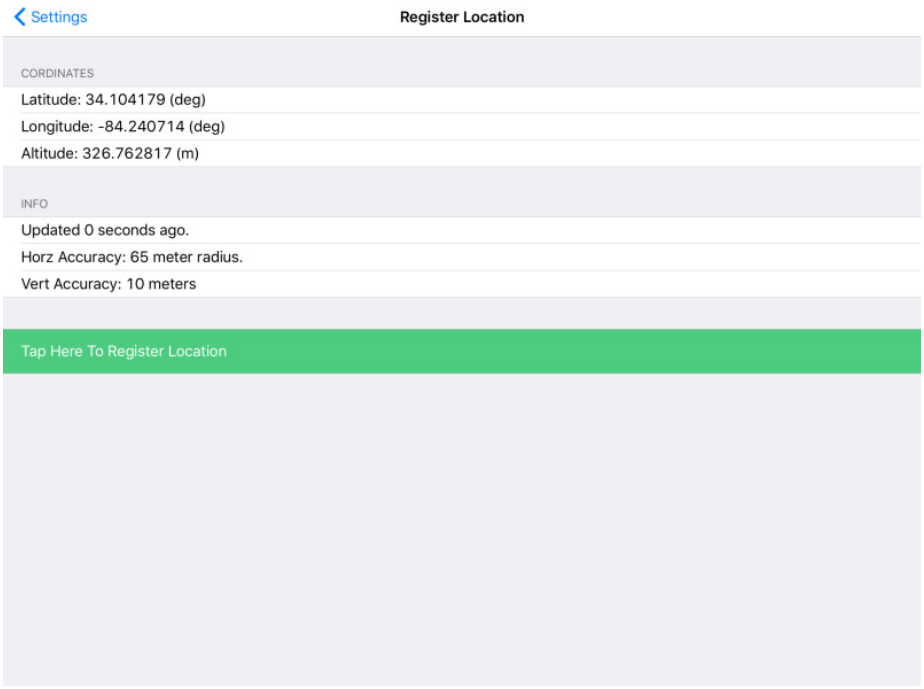
Figure 746 - Register GPS Location



5. Press Register GPS Location.

   The Register Location page appears with the GPS listed on it after the mobile device finds it.

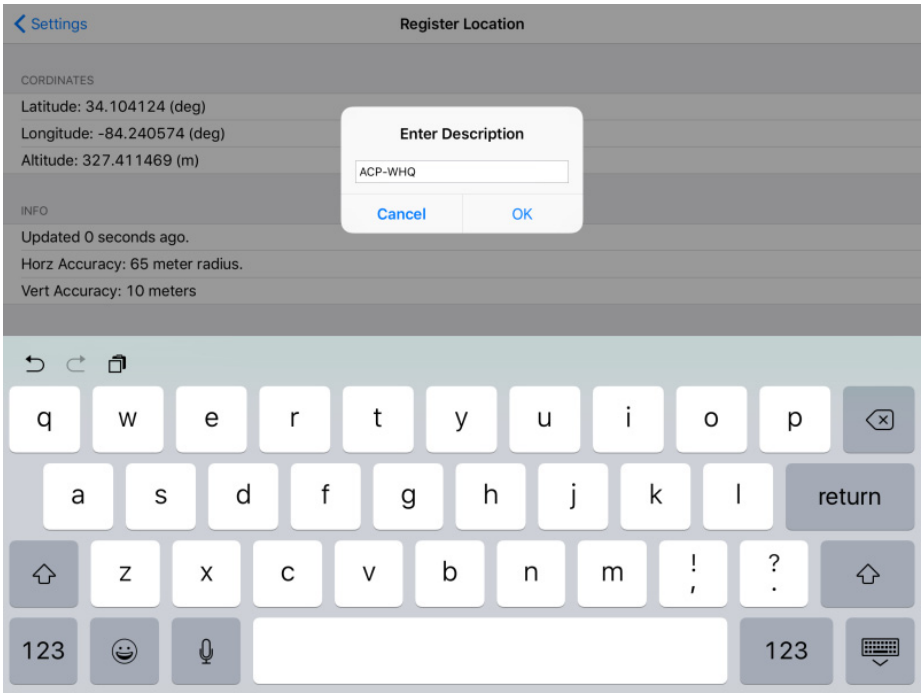
Figure 747 - Available GPS Location



6. Press Tap Here To Register Location.

   Once the data is collected and the GPS location registered, you are prompted to name the location.

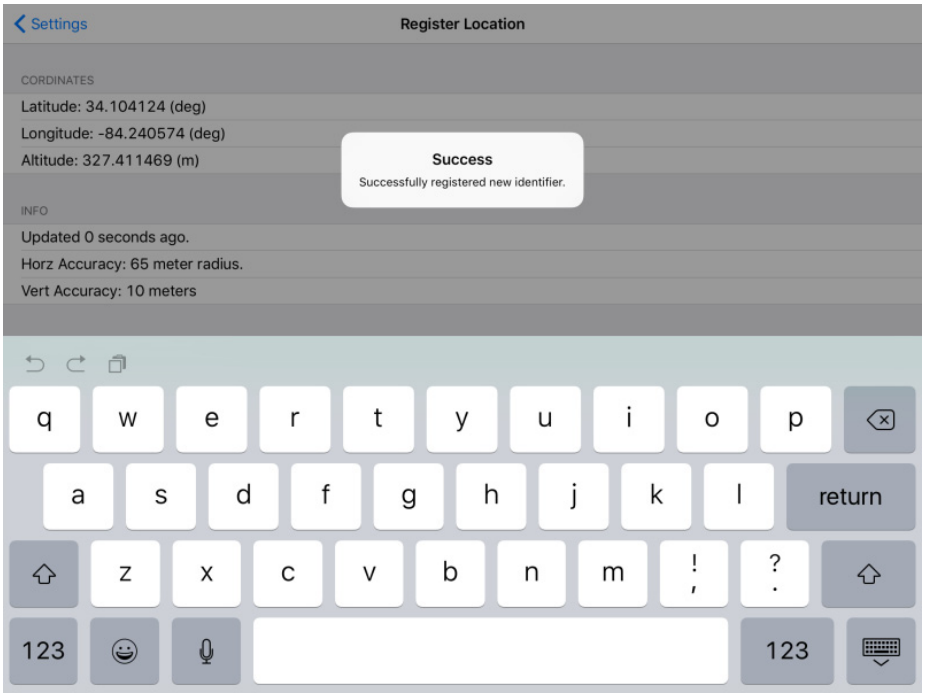
Figure 748 - Enter Location Description



7. Type the Location Description.

   The program confirms a successful GPS location registration.

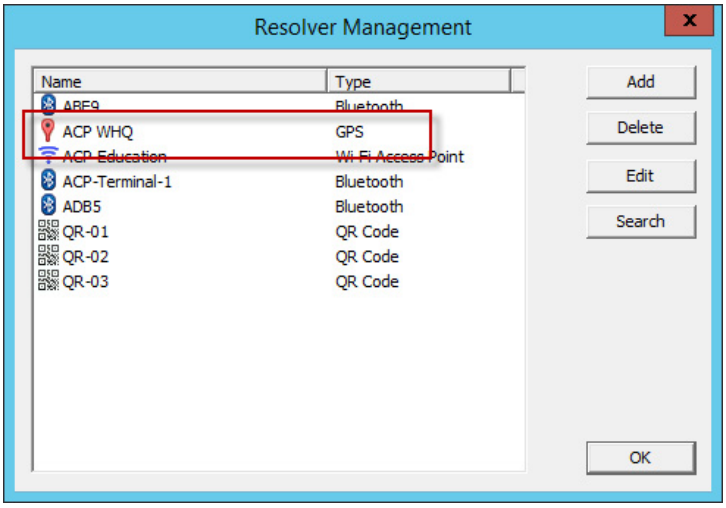
Figure 749 - Success Dialog



8. Choose Manage>Manage IDs.

   The Resolver Management dialog box appears with the registered GPS location displayed.

Figure 750 - Resolver Management

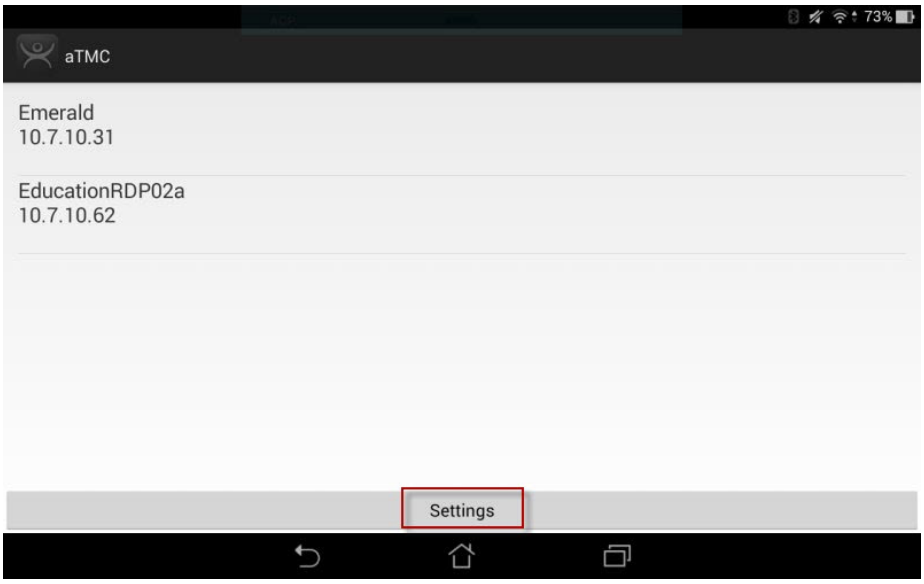


Android-registered GPS

GPS locations are defined and registered like the Bluetooth beacon.

1. Open the aTMC program on the tablet.

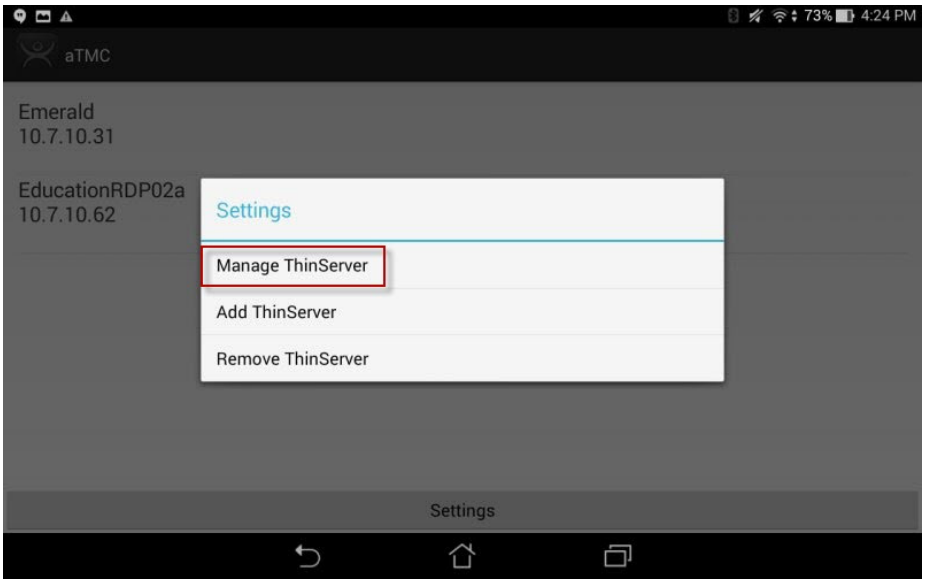
Figure 751 - ThinManager aTMC Program



2. Press Settings on the bottom of the page.

   The Settings dialog box appears.

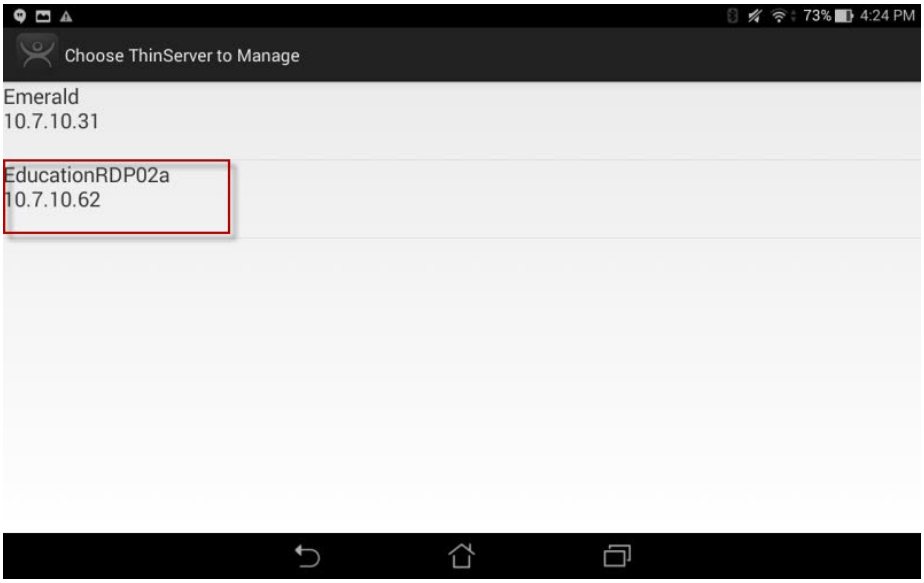
Figure 752 - Settings Menu



3. Press Manage ThinServer.

   The Choose ThinServer to Manage page appears.

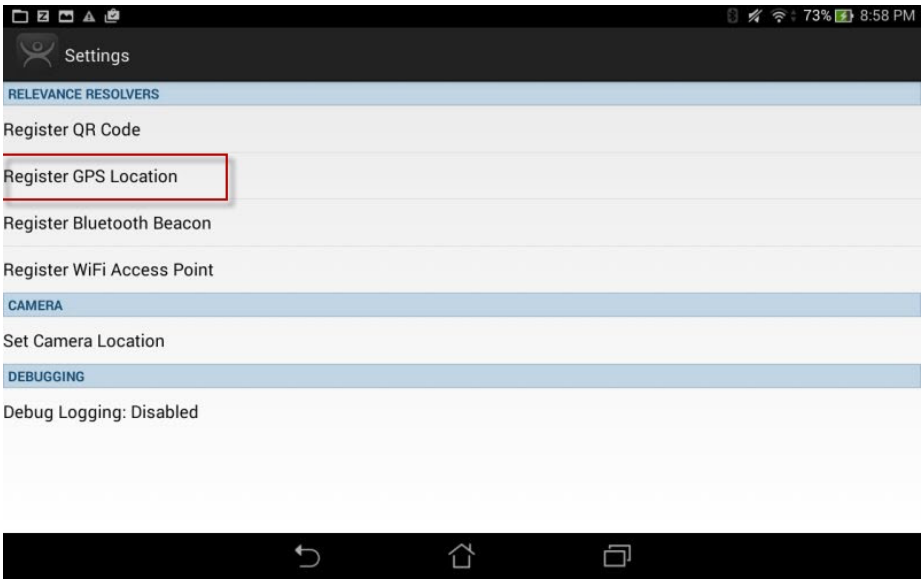
Figure 753 - Select Configuration



4. Press the ThinManager Server with which you want to register the GPS locations.

   The Settings page appears.

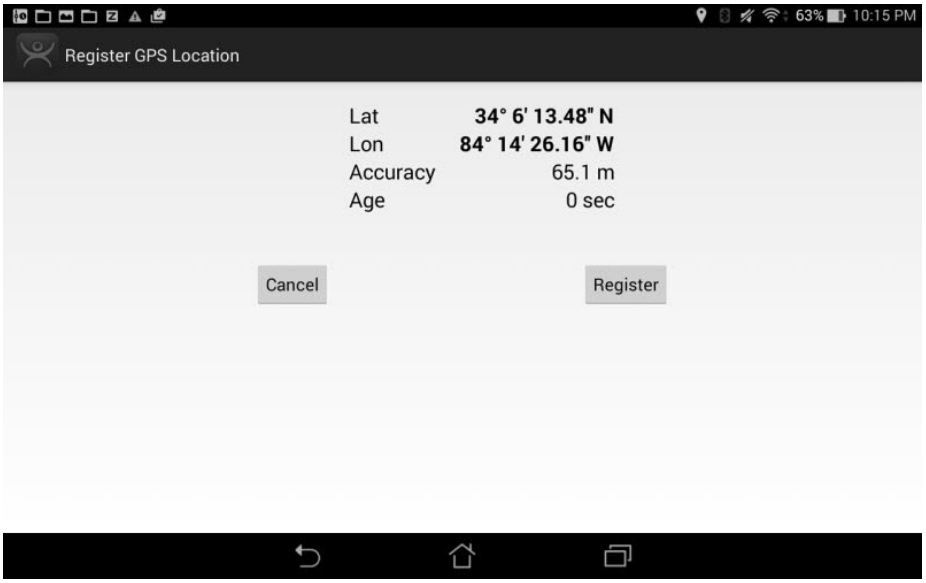
Figure 754 - Register GPS Location



5. Press Register GPS Location.

   The Register GPS Location page appears.

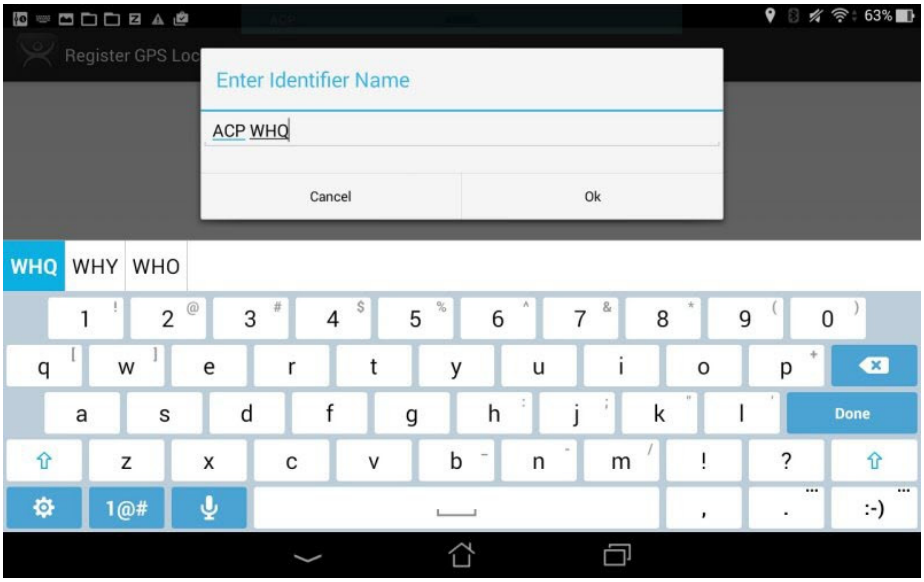
Figure 755 - Register GPS Location



6. Press Register.

   Once the GPS location is identified, you are prompted to name the location.

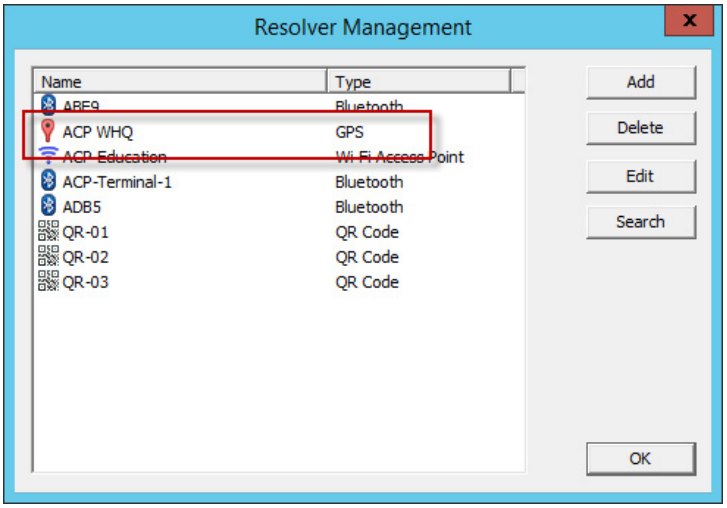
Figure 756 - Enter Location Description



7. Type the Name of the GPS location and press OK to finish the registration process.
8. Choose Manage>Manage IDs.

   The GPS location is registered and entered in the Resolver Management dialog box.

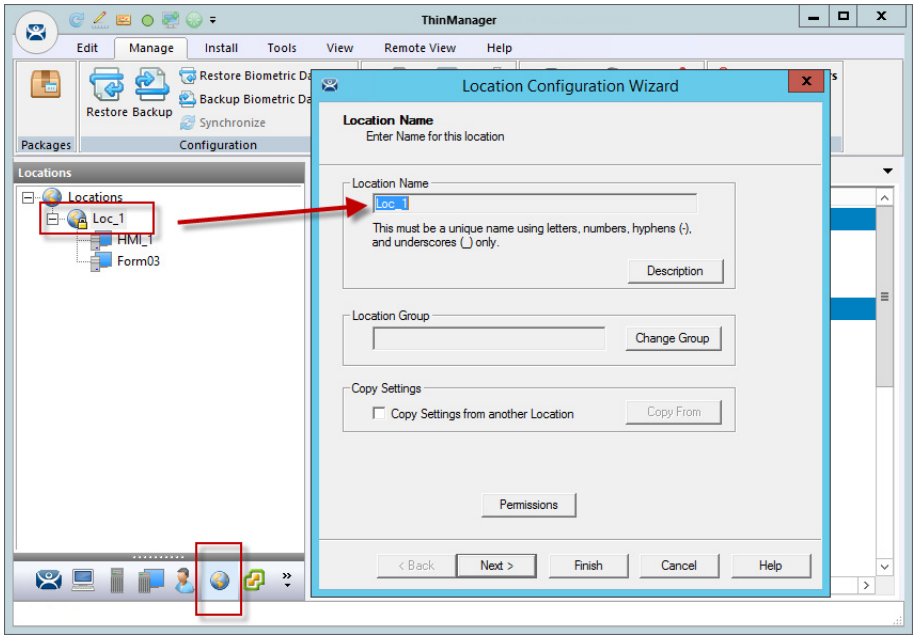
Figure 757 - Resolver Management



Add Actions to Resolver Codes

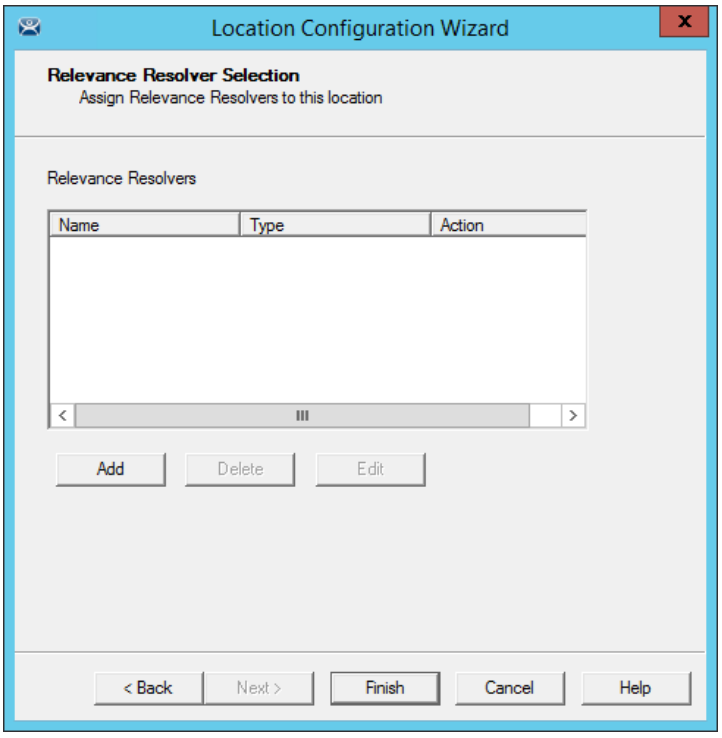
Resolvers can be applied to a location and have an action associated with them so that when a resolver is used, a particular action is launched.

Figure 758 - Location Configuration Wizard



1. Click the Locations icon at the bottom of the ThinManager tree.
2. Double-click a location to open the Location Configuration Wizard.

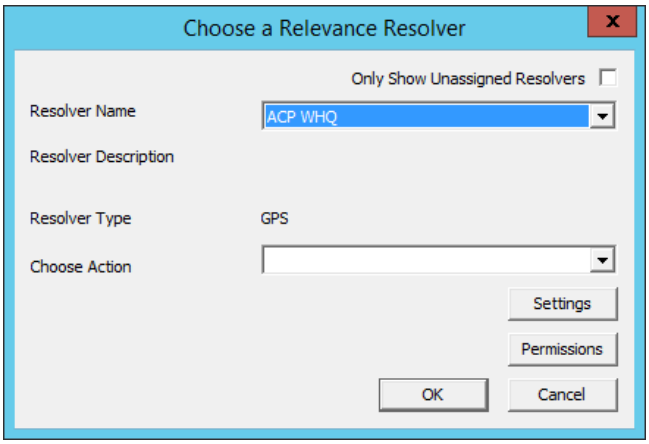
Figure 759 - Relevance Resolver Selection Page



3. Click Next until the Relevance Resolver Selection page appears.
4. Click Add.

   The Choose a Relevance Resolver dialog box appears, which has a pull-down menu that lets you select which resolver to configure.

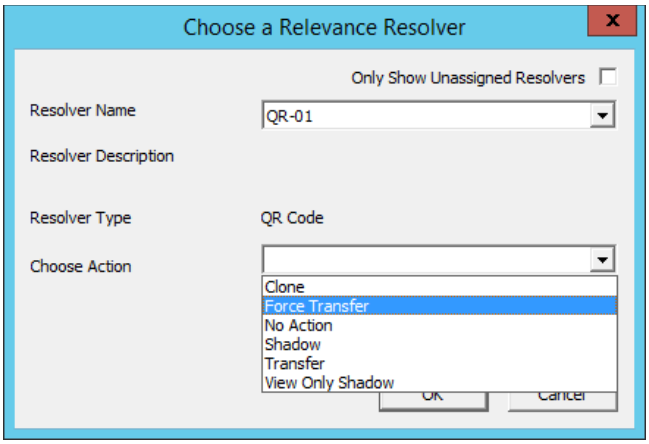
Figure 760 - Choose a Relevance ID



5. Check Only Show Unassigned Resolvers to limit the list to unassigned resolvers, which prevents duplication.
6. Choose a resolver from the Resolver Name pull-down menu.

   The Resolver Type indicates whether it is a QR code, Bluetooth beacon, GPS, or Wi-Fi resolver.

Figure 761 - Choose Action Selection



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

Action	Description
Clone	Creates a new duplicate session using the mobile device Windows account.
Force Transfer	Automatically diverts the location graphic to the mobile device.
No Action	Initiates no new action.
Shadow	Provides an interactive shadow on the mobile device.
Transfer	Diverts the location graphic to the mobile device after operator input.
View Only Shadow	Provides a shadow without allowance of any input from the mobile device.

Each location can have several Relevance IDs with different actions.

Figure 762 - Relevance ID Selection Page

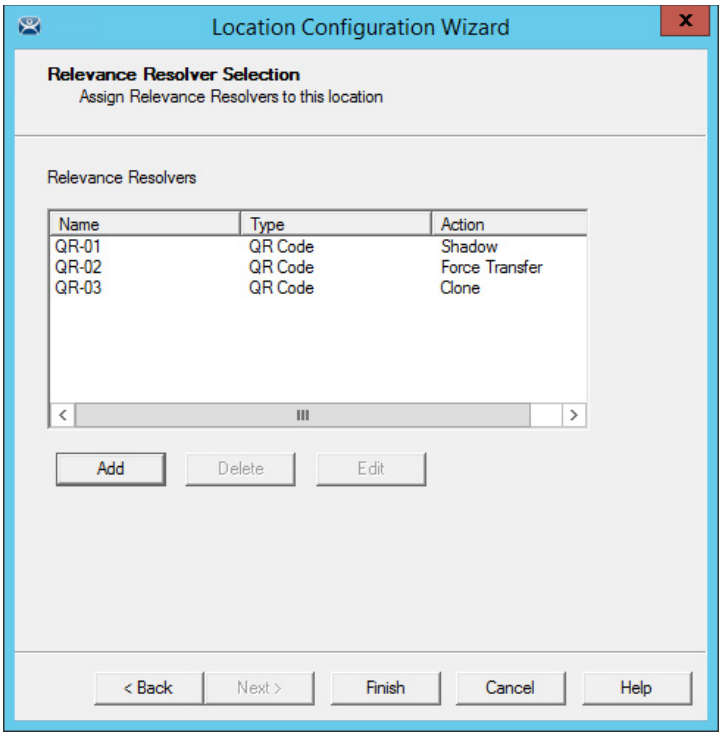


Figure 762 shows a location with three QR codes, each with their own action. Scan a code to initiate the associated action.

Table 3 - QR Code Resolver Actions

QR Code Resolver	Action
QR-01	Shadow
QR-02	Force Transfer
QR-03	Clone

Normally, you use a single QR code and use Permissions to deploy the different functions. Table 3 is just a simplified example to show the concept of different actions. See One QR Code, Multiple Actions on page 466.

Interact with the Location

The iTMC client can be used to interact with the location by a scan of the four resolvers configured with different actions in the previous example.

The iTMC screen has a menu bar at the top with several command buttons.

Figure 763 - iTMC Menu Bar

These are the button descriptions from right to left.

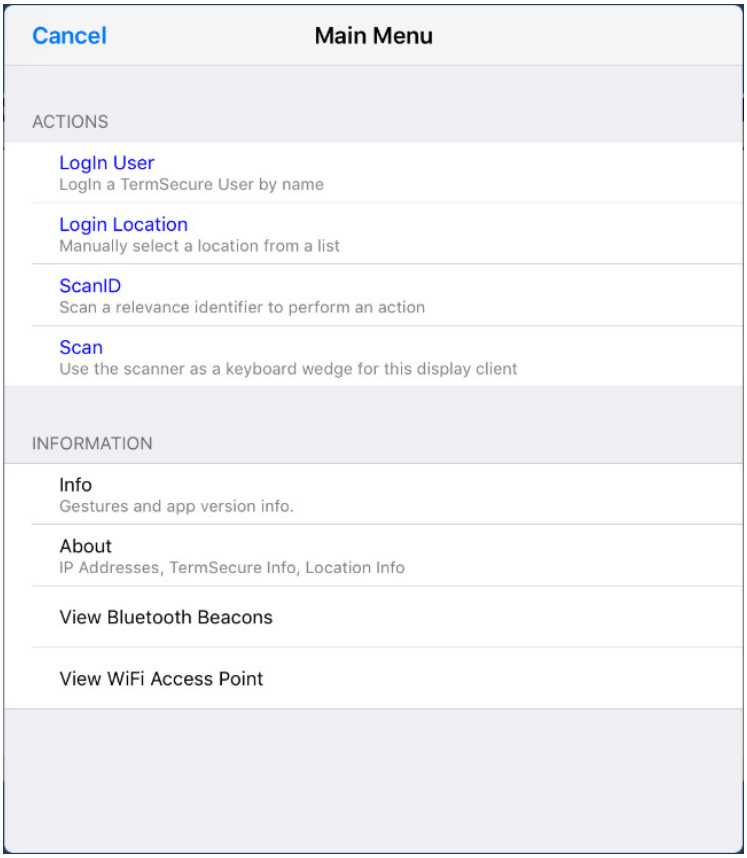
Button	Description
Switch (cascaded square)	Press to switch between two or more Display Clients.
Full Screen (four-arrow icon)	Press to make the display client full screen. Touch the screen with three fingers to restore the view.
Keyboard	Press to launch an on-screen keyboard.
Name	The center space displays the name of the Terminal, ThinManager user, or display client per the state of the Terminal.

Button	Description
Leave	Press to end the action that was initiated by the original scan.
Scan	Press to allow the scan window to act as a keyboard wedge to pull data into the session.
Scan ID	Press to open the Scan Identified window to scan QR codes to resolve a location or action.
Login	Press to open the Relevance login dialog box to allow you to log in with a ThinManager user name.
Menu	Press to launch the Main Menu screen.

1. Press Main Menu.

   The Main Menu appears.

Figure 764 - Main Menu



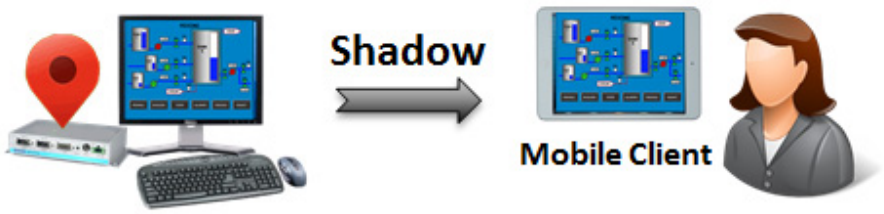
The Main Menu has a variety of functions. The state of the application determines what is displayed.

Function	Description
ACTIONS	
Login User	Press to launch a dialog box to log in as a ThinManager user.
Login Location	Press to manually select a location.
Scan ID	Press to open the Scan Identified window to scan QR codes to resolve a location or action.
Scan	Press to allow the scan window to act as a keyboard wedge to pull data into the session.
INFORMATION	
Info	Provides version numbers and lists gestures to navigate the program.
About	Launches a dialog box with user, location, and network information.
View Bluetooth Beacons	Lists the Bluetooth beacons within range and their signal strength.
View WiFi Access Point	Lists the BSSID of the Wi-Fi network to which you are connected.
Hide Map When Zoomed	Normally, when the screen is zoomed, a map is provided so you can determine the part of the screen that is viewed. This feature hides the map during a zoom.

Shadow

A Shadow duplicates the graphic output of the location and sends it to the mobile device. The mobile user sees the exact display as the location. See Figure 765 on page 520.

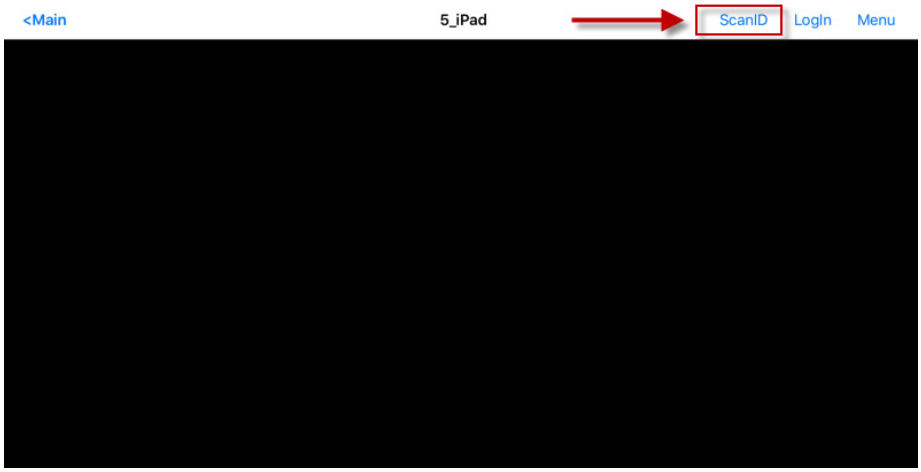
Figure 765 - Shadow



1. Launch the iTMC application.
2. Select your ThinManager Server on the configuration screen to run your iPad as a Terminal.

   The Main Screen has a menu bar at the top with Main, ScanID, Login, and Menu.

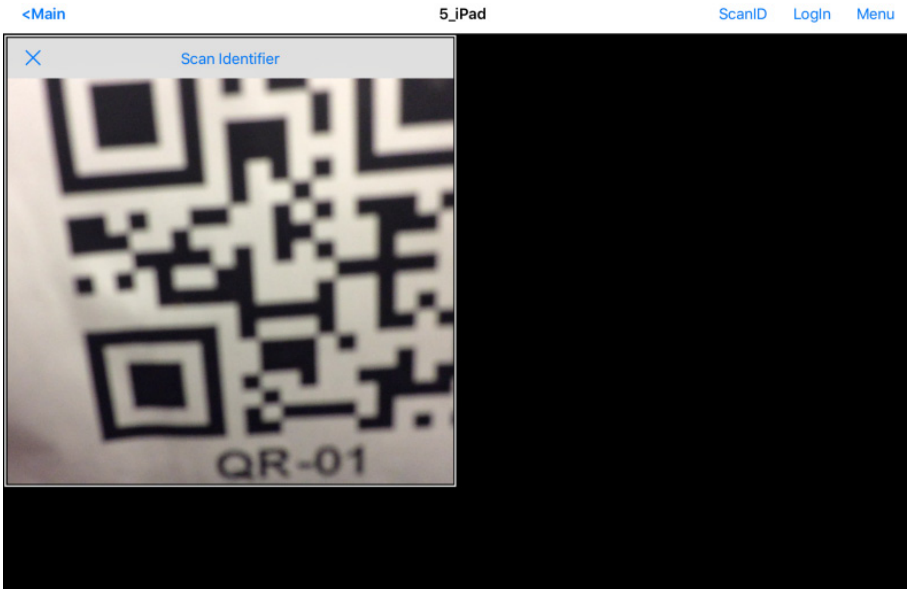
Figure 766 - ThinManager iTMC Main Screen



3. Press ScanID in the upper-right of the menu bar.

   The Scan Identifier screen, which is the onboard camera, appears.

Figure 767 - Scan Identifier



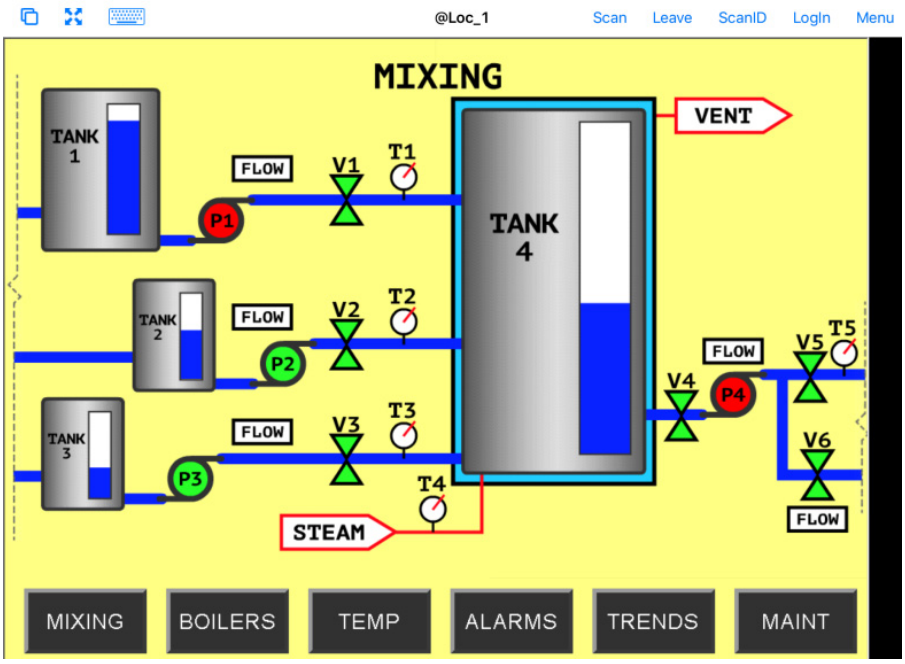
4. Position the camera over the resolver code.

   The device reads the code and acts on it.

The image of the QR code is blurry because it registers and closes as soon as it is in focus.

The iTMC client now shadows the location because the resolver had the shadow action applied to it.

Figure 768 - Shadowed Session on iTMC Client



5. Press Leave to end the Shadow action.

Forced Transfer

Transfer sends the graphic output of the location to the mobile device instead of the location. Transfer can be done automatically with Forced Transfer or set to require the operator to manually allow the transfer.

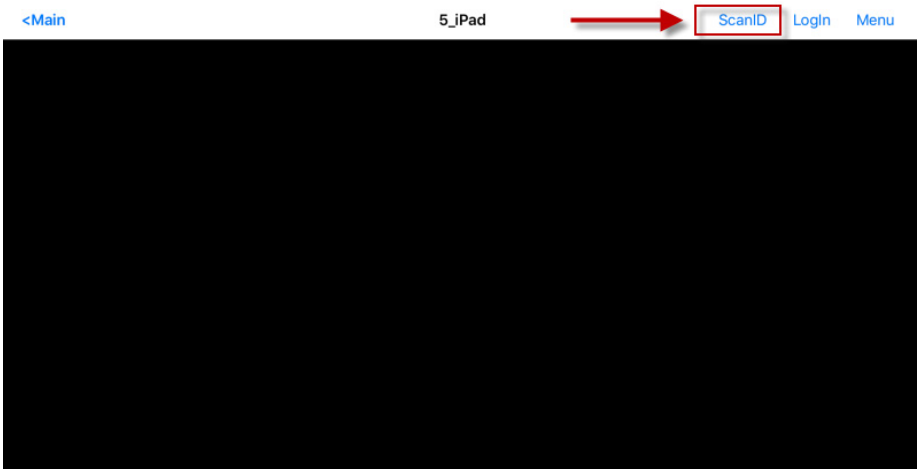
Forced Transfer takes control without operator input, which prevents someone from taking the session while the operator is busy with a process. It also allows a mobile user to take sole control of the location.

Figure 769 - Forced Transfer

1. Launch the iTMC application.
2. Select your ThinManager Server on the configuration screen to run your iPad as a Terminal.

The Main Screen has a menu bar at the top with Main, ScanID, Login, and Menu.

Figure 770 - ThinManager iTMC Main Screen



3. Press ScanID near the upper-right corner.

   The Scan Identifier screen, which is the onboard camera, appears.

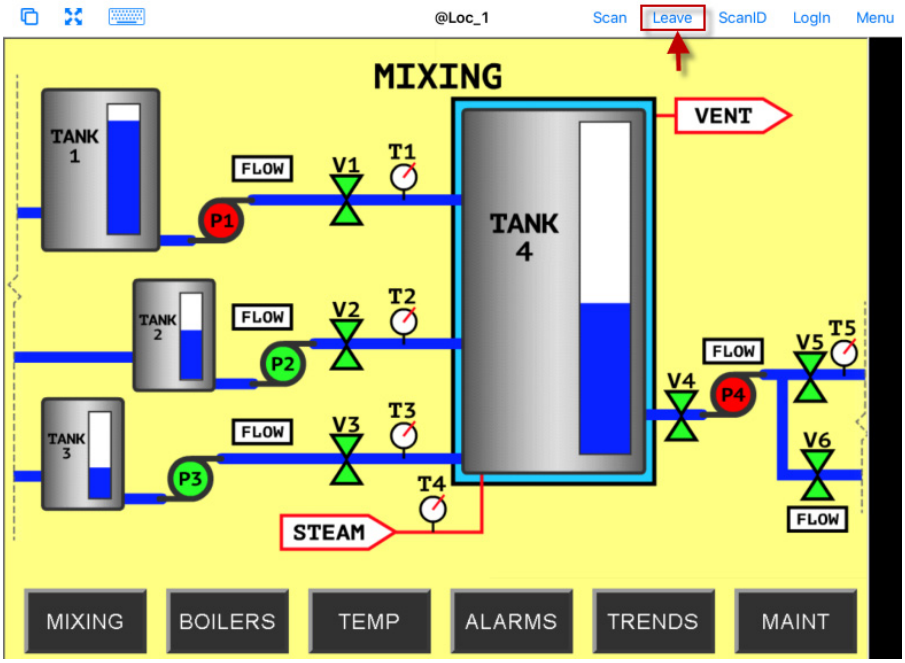
Figure 771 - Scan Identifier

4. Scan the resolver associated with Forced Transfer. The display is ported to the mobile device.

The image of the QR code is blurry because it registers and closes as soon as it is in focus.

The display from the location is moved to the mobile device.

Figure 772 - Transfer on the Mobile Device



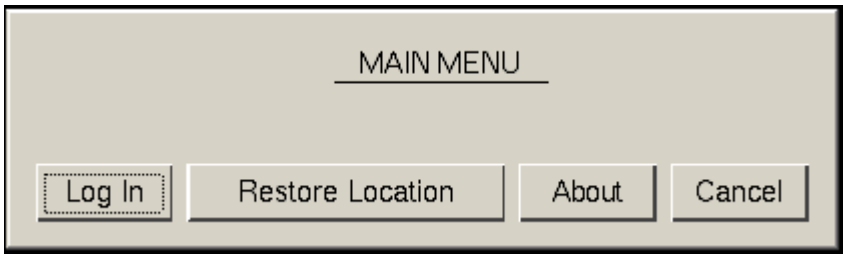
When the action of the resolver is Forced Transfer, the display at the location is automatically transferred to the scanning iTMC client.

Figure 773 - Forced Transfer at Location

5. Press Leave in the top menu bar or Leave Location on the Main Menu to end the transfer.

   A message box is displayed on the client to explain that the display is transferred.

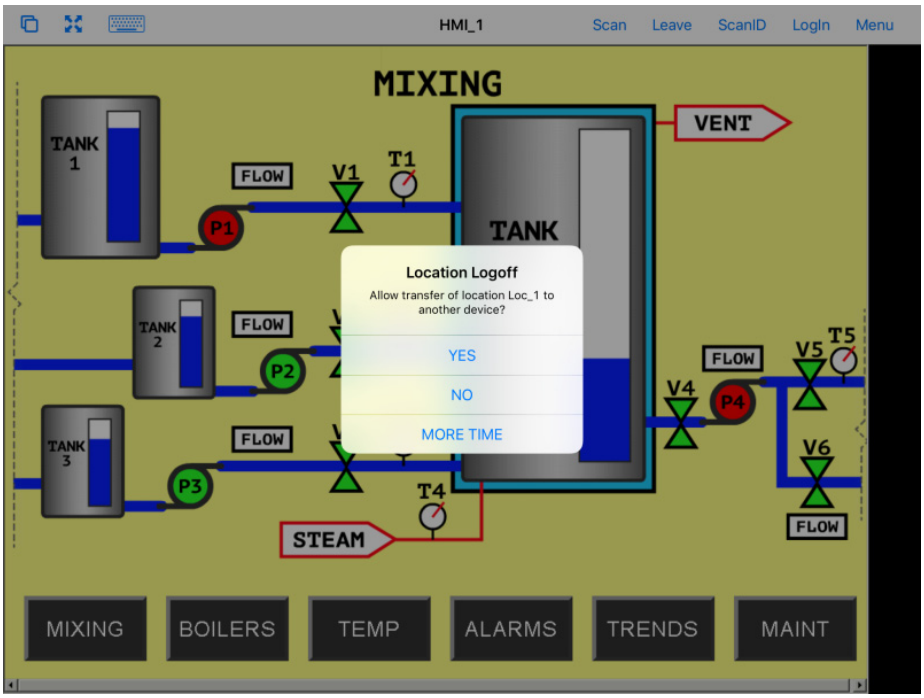
Figure 774 - Main Menu at the Location



6. If you want to recall the display, go to the location and press Restore Location.

   The iTMC client displays a Location Logoff dialog box when a restoration request is initiated.

Figure 775 - Location Logoff Dialog Box



Setting	Description
Yes	Press to allow the restoration of the display.
No	Press to refuse the restoration of the display.
More Time	Press to send a request to the location for more time. The location gets a message with Yes and No, which provides the power to allow more time or end the transfer.

Transfer

Transfer sends the graphic output of the location to the mobile device instead of the location. Transfer can be done automatically with Forced Transfer or set to require the operator to manually allow the transfer.

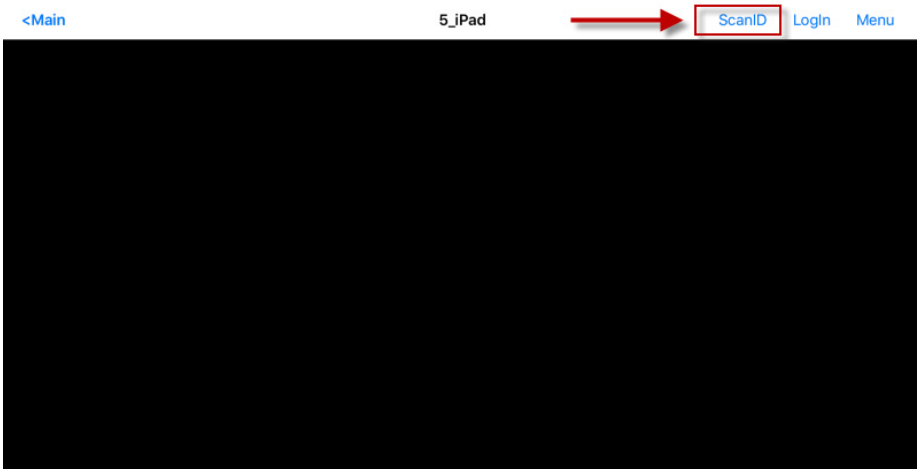
Transfer requires operator input to allow the transfer, which prevents someone from taking the session while the operator is busy with a process. Also, it allows a mobile user to take sole control of the location.

Figure 776 - Transfer

1. Launch the iTMC application.
2. Select your ThinManager Server on the configuration screen to run your iPad as a Terminal.

The Main Screen has a menu bar at the top with Main, ScanID, Login, and Menu.

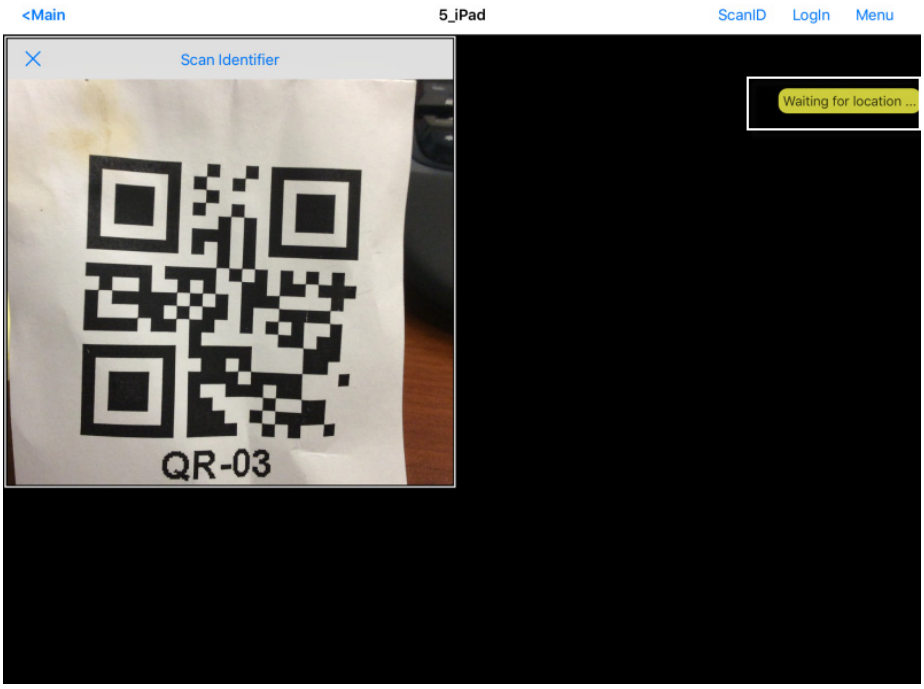
Figure 777 - ThinManager iTMC Main Screen



3. Press ScanID in the right part of the menu bar.

   The Scan Identifier screen, which is the onboard camera, appears.

Figure 778 - Scan Identifier



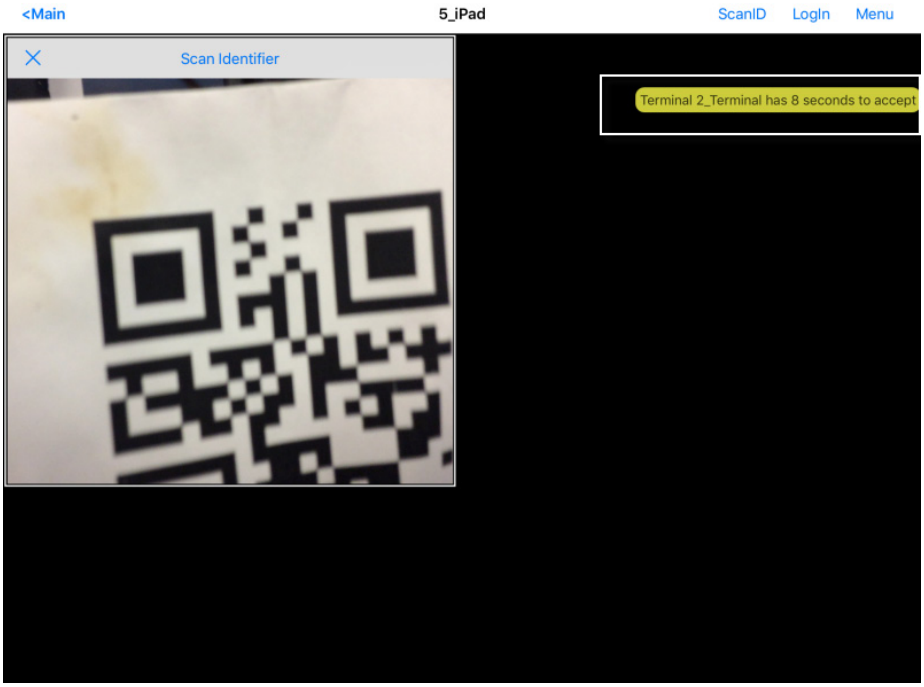
4. Scan the resolver associated with Transfer.

   A request for transfer is sent to the location.

   The image of the QR code is blurry because it registers and closes as soon as it is in focus.

   A message is sent to the mobile device, which tells it that the location must respond.

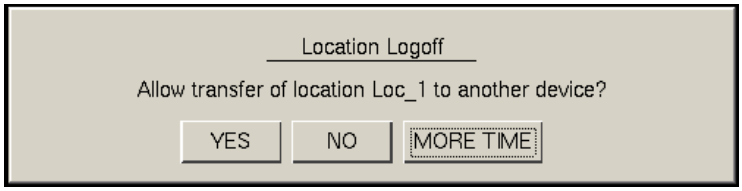
Figure 779 - Transfer Notification



The scan initiates the transfer—this is not a forced transfer, but a manual transfer—which requires confirmation at the location.

The operator at the location is shown a dialog box that requires approval to transfer.

Figure 780 - Location Logoff Dialog Box

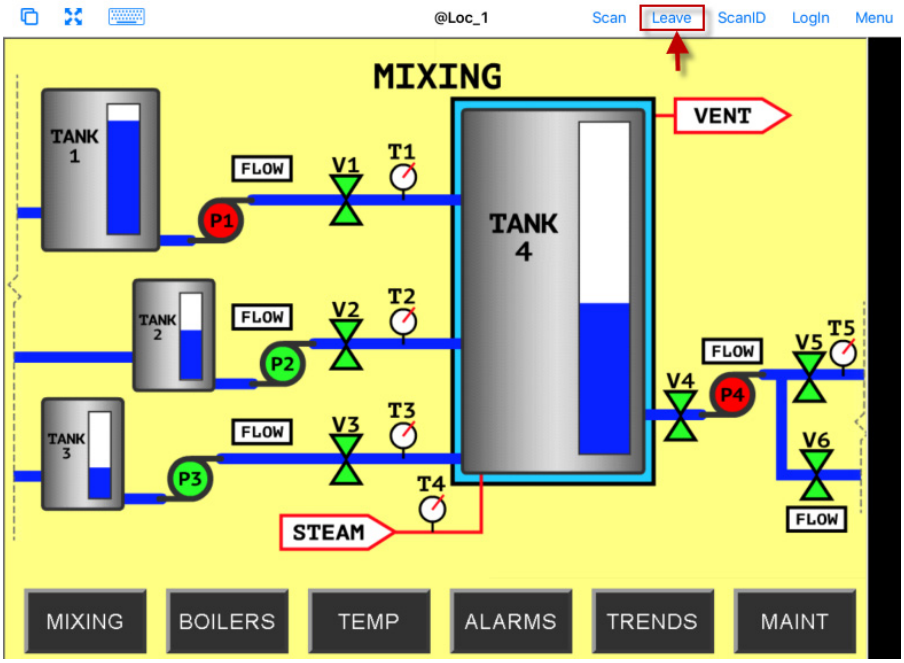


5. The operator at the location clicks Yes to allow the transfer.

   The iTMC client is allowed to show the location display, which is moved from the location to the mobile device.

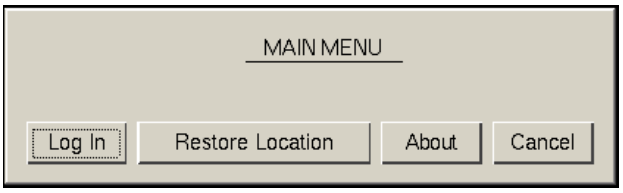
   The location display can be restored from the iTMC client or the location.

Figure 781 - Transfer on the Mobile Device



6. Press Leave on the iTMC client menu to restore the display to the location.

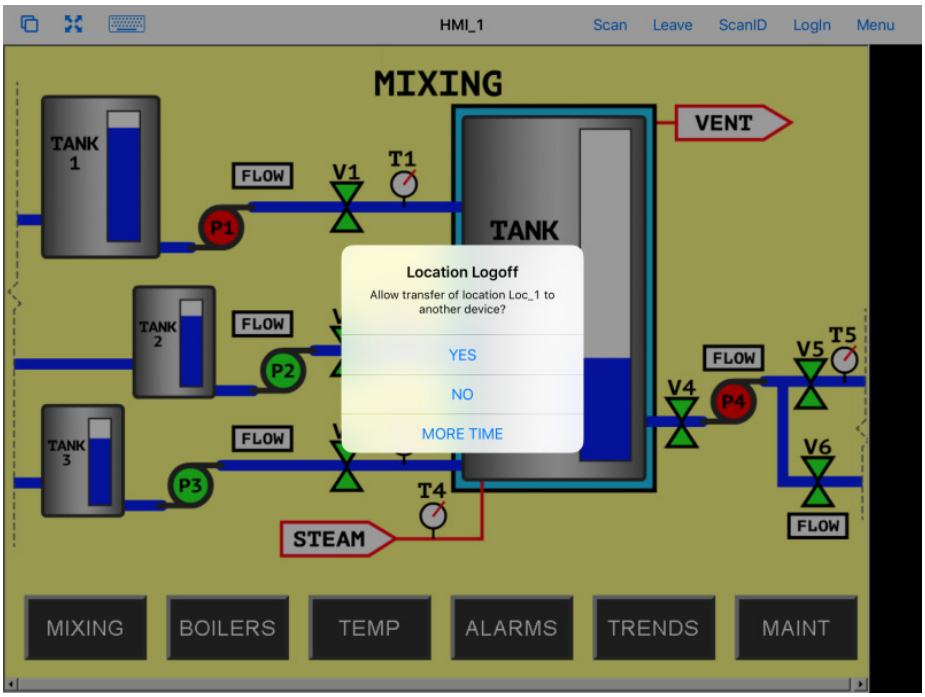
Figure 782 - Main Menu at the Location



   a. Alternatively, the operator at the Location, can click Restore Location on the Main Menu to restore the display.

   On the iTMC client, the Location Logoff dialog box appears, which asks whether to transfer location display to another device.

Figure 783 - Location Logoff on the Mobile Device

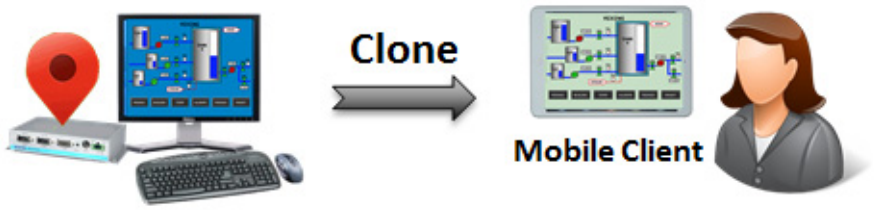


7. On to the iTMC client, press Yes to allow the transfer to the location.

Clone

Clone duplicates the display clients of the location on the mobile device, but the sessions are created with the mobile device Windows user account.

Figure 784 - Clone

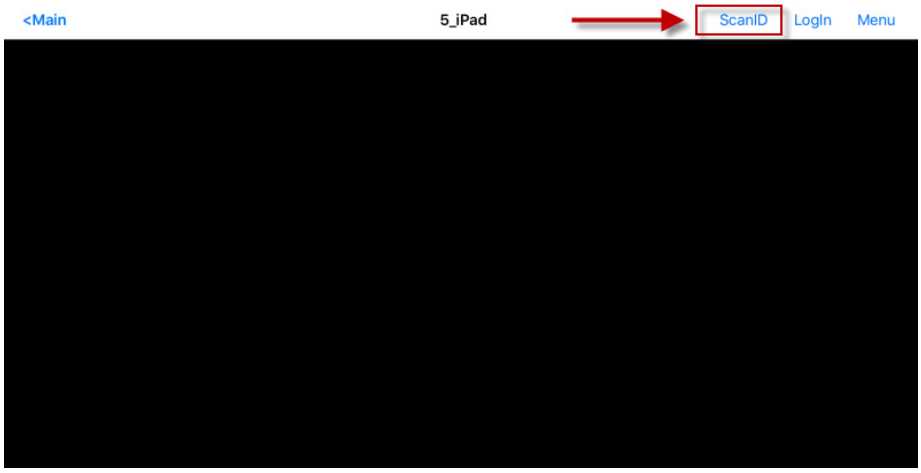


Clone allows a mobile user to get the HMI or other software and have independence from the user at the location.

1. Launch the iTMC application.
2. Select your ThinManager Server on the configuration screen to run your iPad as a Terminal.

The Main Screen has a menu bar at the top with Main, ScanID, Login, and Menu.

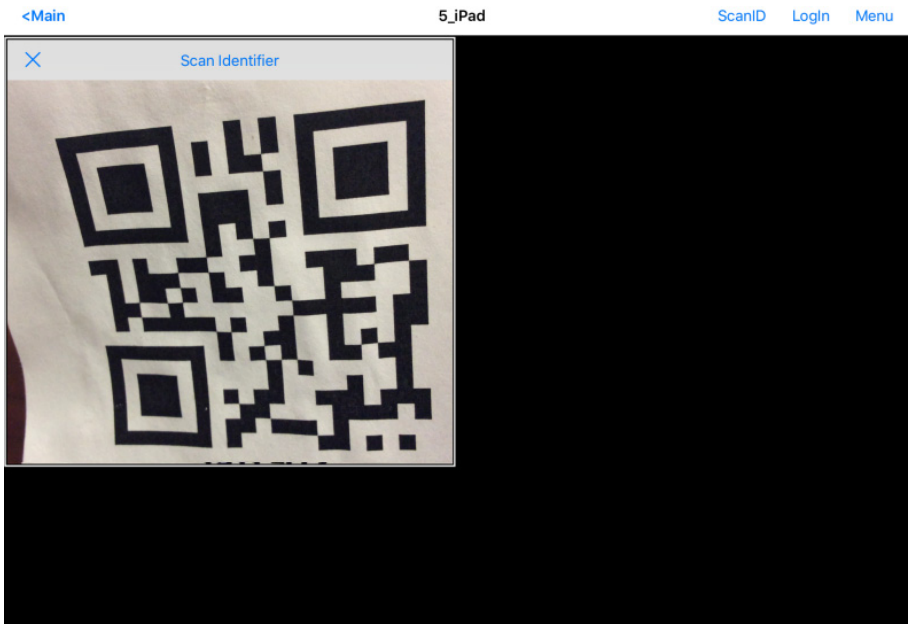
Figure 785 - ThinManager iTMC Main Screen



3. Press ScanID on the right side of the menu bar.

   The Scan Identifier screen, which is the onboard camera, appears.

Figure 786 - Scan Identifier



4. Scan the resolver associated with Clone.

   Relevance launches the display clients used at the location on the mobile device, but uses the mobile device account. Clone gives a mobile user the same applications as the location, but with an independent session instead of a shared as in Shadow. Clone does not take the session as in Transfer and Forced Transfer.

Figure 787 - Cloned Session

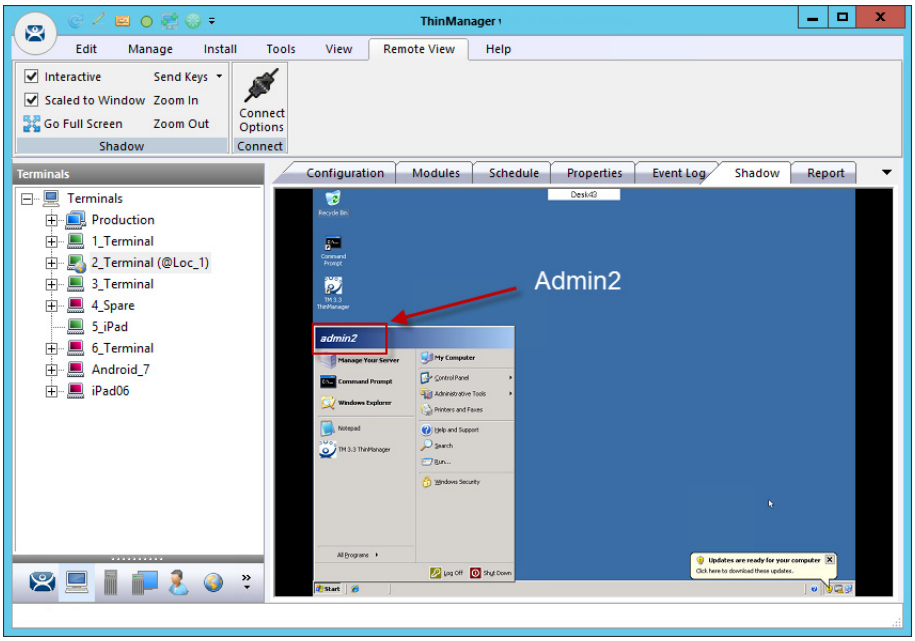
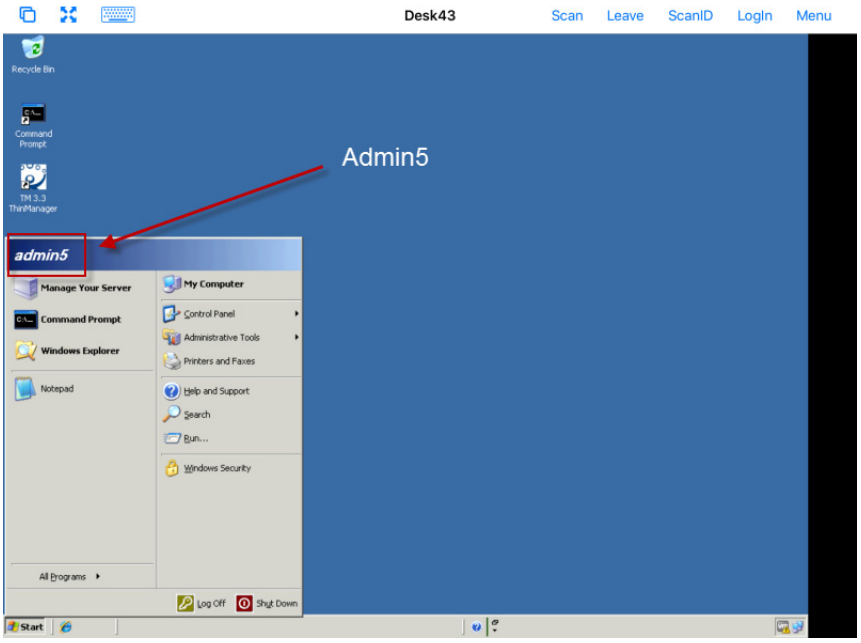


Figure 787 is a shadow from ThinManager that shows the Terminal logged in as Admin2.

Figure 788 - Cloned Session



Clone duplicates the sessions on the location, but creates the sessions with the Windows user account of the mobile device.

Figure 788 shows the iPad clone of the 2_Terminal, which runs the same applications, but logs in with the Windows account of the iPad, which is Admin5.

Notes:

Events

ThinManager Events ensure relevant visual content is presented, or ThinManager administrative tasks are completed, subsequent to an occurrence of an external source. The Event source can be any software that uses ActiveX and is defined in the ThinManager Event Property Wizard with simple logic. ThinManager Events provide the ability to Add, Remove, Switch, or Tile a Display Client on a Terminal based on an Event or multiple Events. It also allows the ability to add or remove permissions of a specific Access Group on a Terminal based on an Event or multiple Events. Also, expressions of various Events can be grouped if needed.

ThinManager Events can be accessed from the ThinManager Events tree.

Create a ThinManager Event

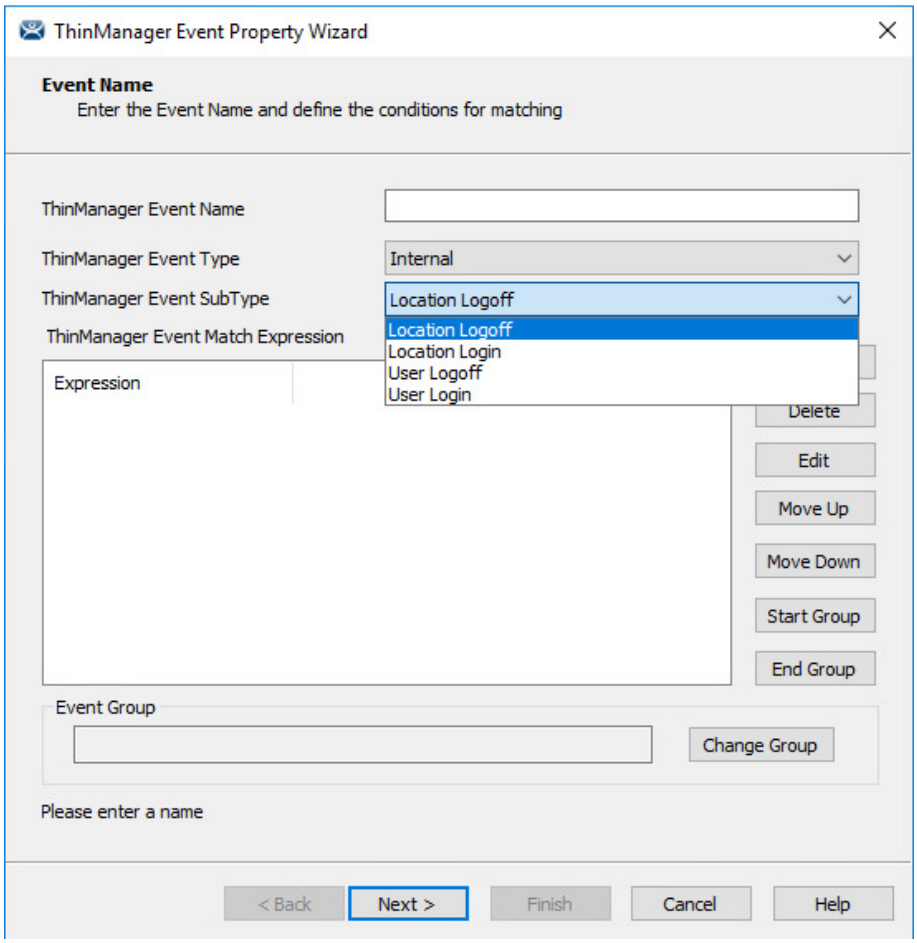
Follow these steps to create a ThinManager Event.

These steps are not inclusive and may require additional VBA or other configuration in the external software (source of Event).

1. Right-click on ThinManager Event > Add Event.

   The ThinManager Event Property Wizard appears, opened to the Event Name page.

Figure 789 - Event Name Page

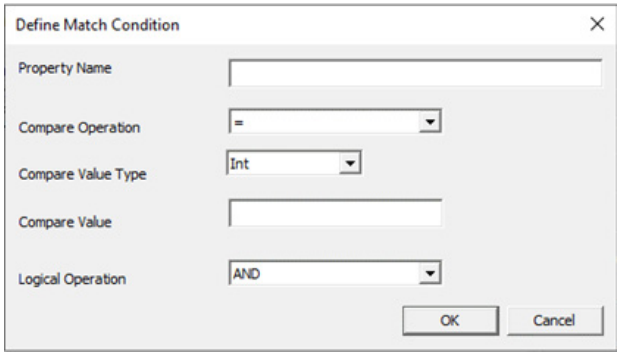


Fields	Description
ThinManager Event Name	This is an organizational name only. It does not impact the operation of the event.
ThinManager Event Type	Specifies the type of event. Select Generic for all events except for ThinManager Logix PinPoint events, which uses PinPoint as the ThinManager Event Type; select Internal to propagate the ThinManager Event SubType pull-down menu.
ThinManager Event SubType	Choose from Location Logoff, Location Login, User Logoff, or User Login.
Event Group	This is the group in which the event is nested. Blank means it is nested at the root of the ThinManager Events tree. Otherwise, the name in this field is the name of the group in which the event is nested.
Buttons	
Add	Opens the Define Match Condition page to create a new Match Expression
Delete	After the undesired Expression is selected, this action permanently removes it
Edit	After an Expression is selected, the Define Match Condition page appears, where modifications can be made
Move Up	Changes the presentation order of an Expression
Move Down	Changes the presentation order of an Expression
Start Group	Denotes the start of a Group of Expressions
End Group	Denotes the end of a Group of Expressions
Change Group	Launches the ThinManager Events tree, from which to select a group in which to nest the event.

2. Enter a ThinManager Event Name.
3. Click Add.

The Define Match Condition Wizard appears.

Figure 790 - Define Match Condition



Fields	Description
Property Name	This value should match the value of a User Defined Variable that originated from whichever host has the Termon ActiveX embedded and enabled
Compare Operation	Shows the comparison functions used against the Property Name value in text field of the page. Operations include: • = (equal) • != (not equal) • > (greater than) • < (less than) • begins with • contains • matches pattern
Compare Value Type	Select the type of value to use in the Compare Value field: Int, Real, or String
Compare Value	This value is used to compare against the Property Name value
Logical Operation	Use to combine or create a larger Expression

Define Match Condition is the Expression created for the Event.

4. Enter the Property Name.

The Property Name must match the user-defined variable of the external software that uses ActiveX (source of Event).

5. Set the Compare Operation, Compare Value Type, Compare Value, and Logical Operation based on desired outcome.

The Logical Operation field is only relevant when multiple expressions are combined.

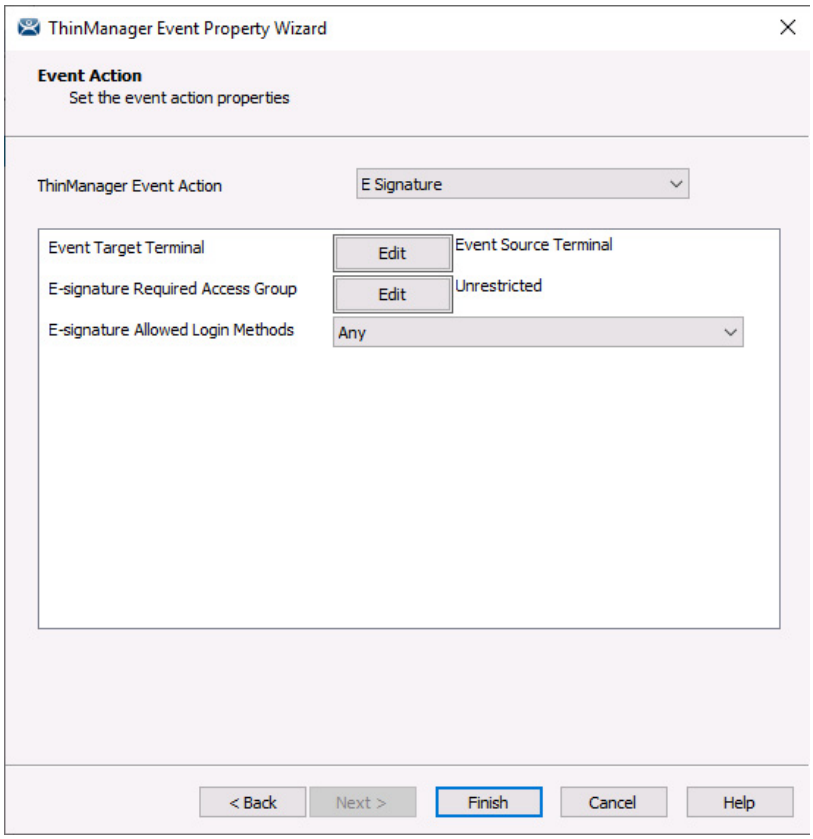
6. Click OK.

   The Define Match Condition Wizard closes, and you are returned to the ThinManager Event Property Wizard.

7. Click Next.

   The Event Action page appears.

Figure 791 - Event Action Page



Fields	Description
ThinManager Event Action	The list of actions that can be applied to a terminal based on the Match Expression(s) applied in the Event Name page of the ThinManager Event Property Wizard. When a desired action is selected, additional parameters are presented that need to be defined.
Buttons	
Edit	Opens a window to edit a specific parameter for the specified **ThinManager Event Action**. Some of these parameters include the **Event Target Terminal**, **Event Target Display Client List**, **Event Target Access Group**, **E-signature required Access Group**, and **E-signature Allowed Login Methods**.

8. From the pull-down menu, select the ThinManager Event Action to occur when the set logical expression is executed.
9. Click Edit for the available parameters based on the Event Action.
10. Click Finish.

    When the Event expression is true, the set ThinManager Event Action occurs. No additional terminal or user configuration is necessary.

For more information about the uses of the various ThinManager Event Actions and their associated fields, see the ThinManager Events White Paper found at https://thinmanager.com/paper/files/TMEvents.PDF.

Packages

Firmware, Packages, and Modules

Firmware is the basic operating system that thin clients run. It is downloaded and expanded into memory, where it serves as an operation system.

Modules bring additional functionality to the thin client such as touch screen integration, keyboard, and sound.

Packages contain a version of firmware and the modules that belong with it.

In the past, ThinManager made all of the firmware changes backward 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 are 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 by default to a thin client, or you can override the setting and run a different package.

This is particularly helpful in validated systems. If new hardware is purchased that requires 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.

Update Packages and Files

ThinManager allows updates of Packages. Also, you can update just the firmware or specific modules if needed.

Firmware and modules get updated automatically during Service Pack upgrades. This section shows how to update firmware and modules without an update to a Service Pack.

1. Download new components from the ThinManager web site at http://downloads.thinmanager.com/ .
2. Choose Install>Firmware Package from the ThinManager menu bar.

   A file browser appears, which allows you to install a `*.pkg` file.
3. Choose Install>Firmware.

   A file browser appears, which allows you to install a `*.fw` file. Also, you can use this command to load a new version of the legacy `firmware.acp` firmware file
4. Choose Install>Module.

   A file browser appears, which allows you to install a `*.mod` file.

ThinManager uses a Boot Loader and a Chain Loader during PXE boot.

5. Choose Install>Boot Loader.

   A file browser appears, which allows you to install a `*.bin` file.
6. Choose Install>Chain Loader.

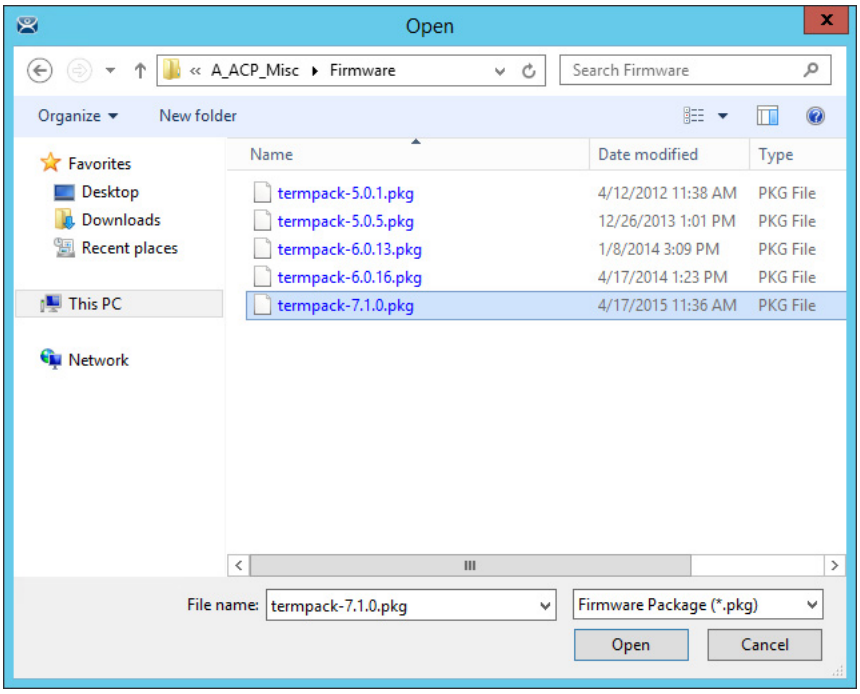
   A file browser appears, which allows you to install a `*.bin` file.

ThinManager uses a Terminal Capabilities Database, or TermCap, to aid in configuring the thin clients.

7. Choose Install>TermCap Database.

   A file browser appears, which allows you to install a `*.db` file.

Figure 792 - Package Installation



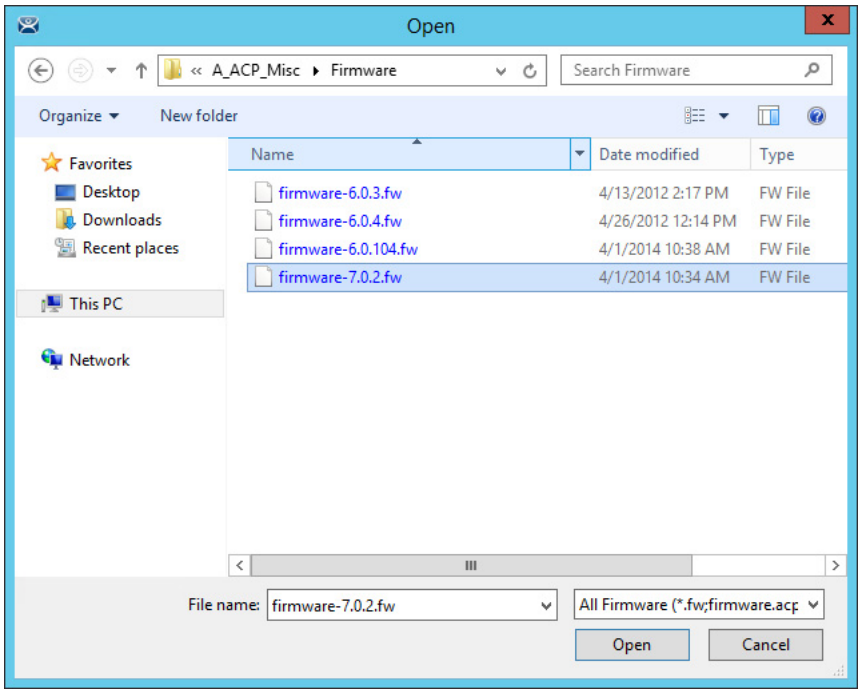
8. Choose Install>Firmware Package.

   A file browser appears, which allows you to install a `*.pkg` file.

Figure 792 shows a folder with three firmware package versions.

9. Highlight the desired firmware package and click Open.

Figure 793 - Firmware Installation



10. Choose Install>Firmware.

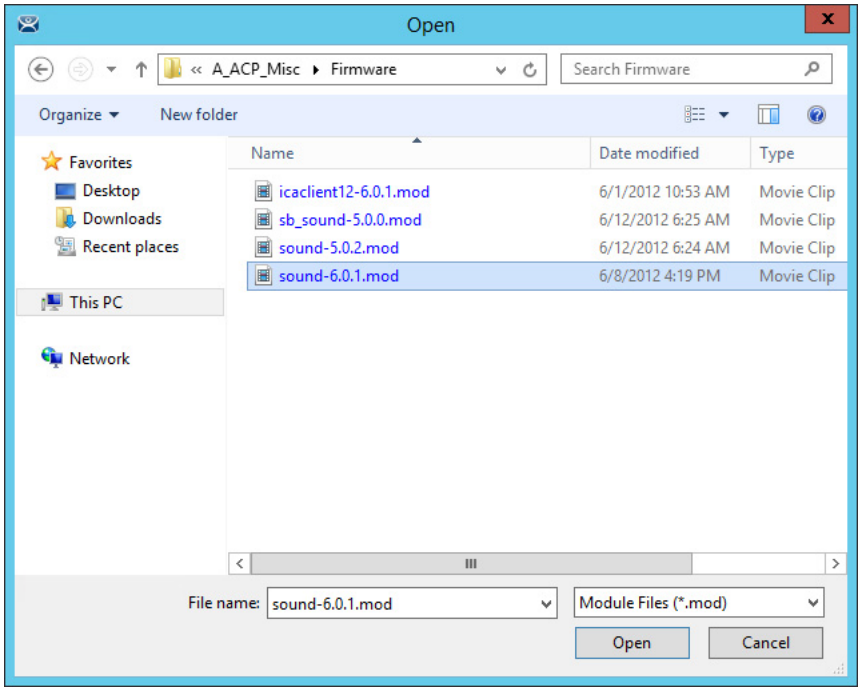
    A file browser appears, which allows you to install a `*.fw` file.

    a. Also, use this command to load a new version of the legacy `firmware.acp` firmware file.

Figure 793 on page 539 shows a folder with several versions of firmware.

11. Highlight the desired firmware and click Open.

Figure 794 - Module Installation



12. Choose Install>Module.

    A file browser appears, which allows you to install a `*.mod` file.

Figure 794 shows a folder with two sound modules.

13. Highlight the desired module and click Open.

Customizing Packages

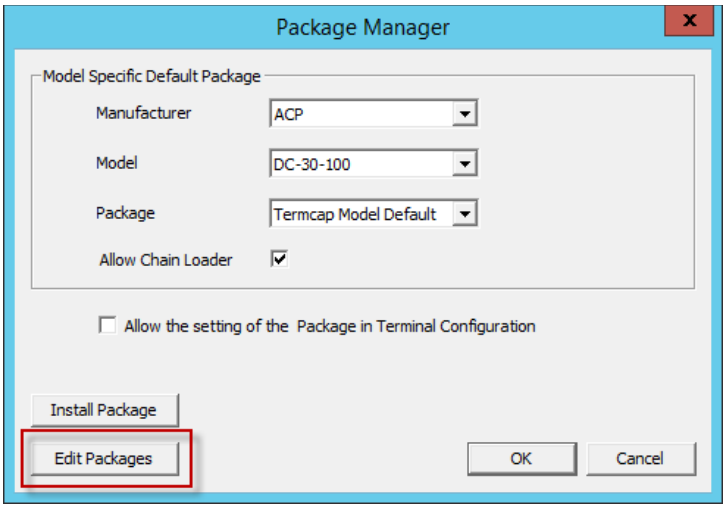
ThinManager allows you to run different packages on different models or individual Terminals. You can modify a package by copying it and making changes to it.

Modules and packages are normally updated with service packs and releases. You can download updated modules at http://downloads.thinmanager.com/ when needed.

1. Choose Manage>Packages.

   The Package Manager appears.

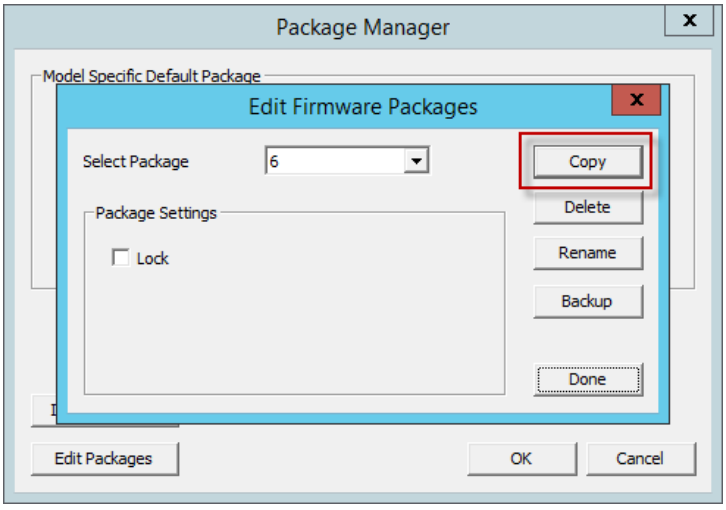
Figure 795 - Package Manager



2. Click Edit Packages.

   The Edit Firmware Packages dialog box appears.

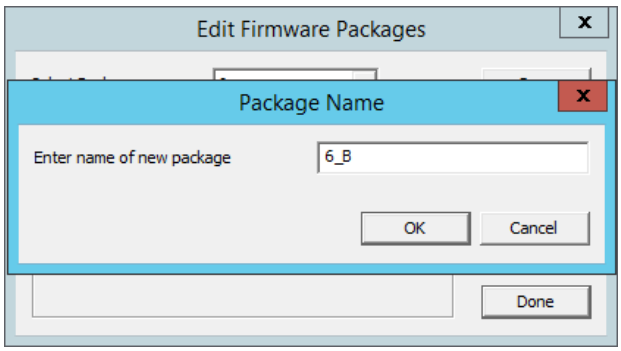
Figure 796 - Edit Firmware Packages Dialog Box



3. Choose the package version you want from the Select Package pull-down menu to modify in the Select Package dialog box and click Copy.

   The Package Name dialog box appears.

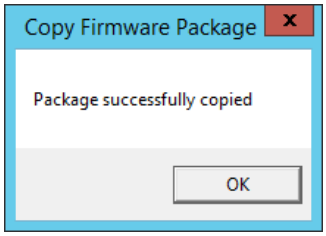
Figure 797 - Package Name Dialog Box



4. Type a name for the new package in the Enter name of new package field.

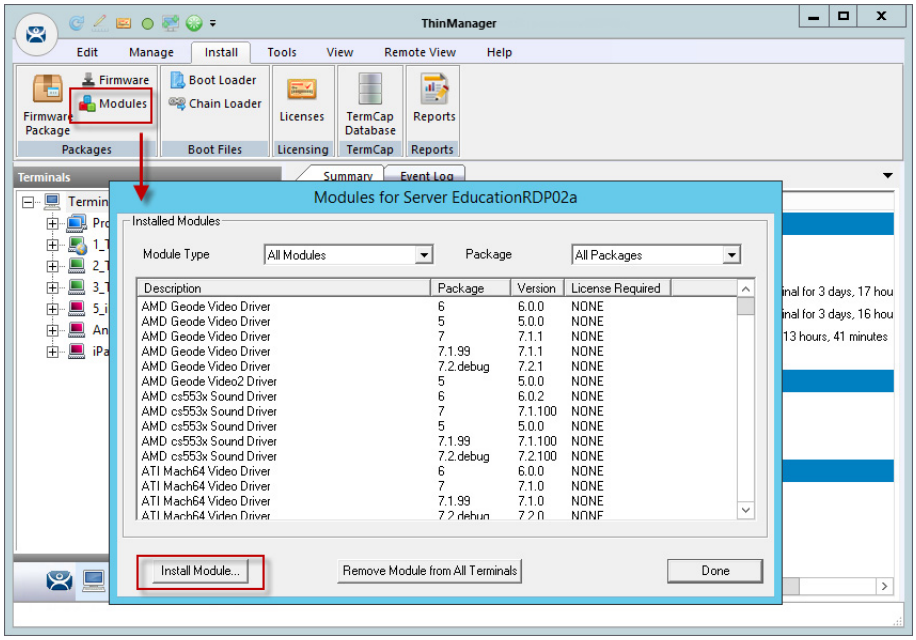
Success is confirmed in the Copy Firmware Package dialog box.

Figure 798 - Success Dialog



5. Click OK.
6. Click Done on the Edit Firmware Packages and OK on the Package Manager dialog boxes.

Figure 799 - Modules Dialog Box

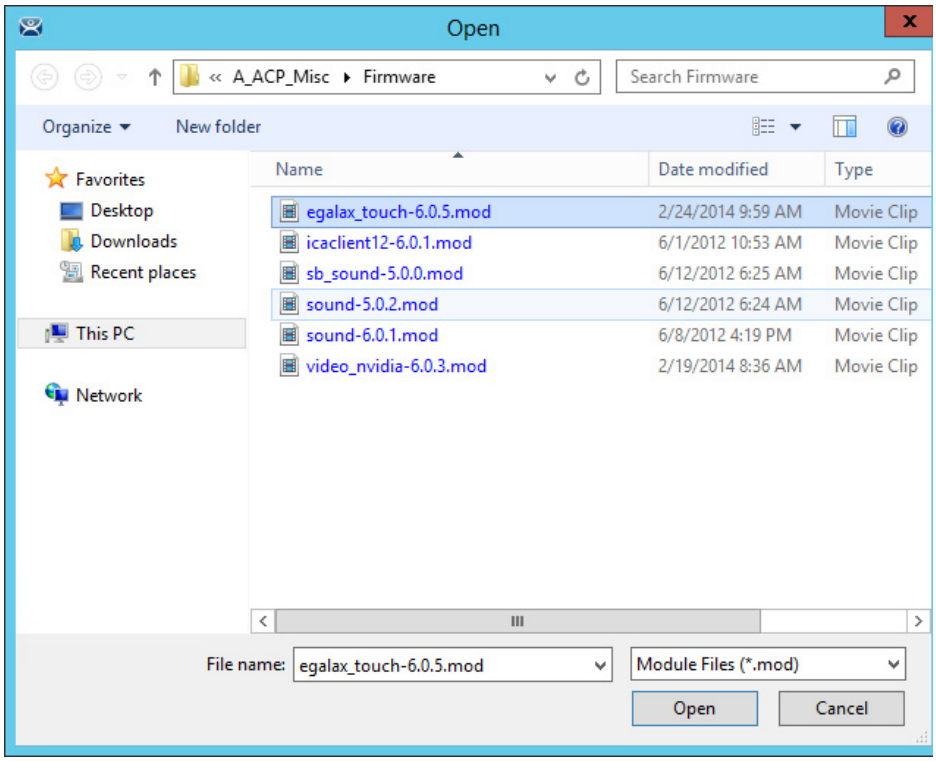


7. Choose Install>Modules.

   The Modules dialog box for that server appears.
8. Click Install Module.

   A file browser appears, which you can use to navigate to your downloaded modules.

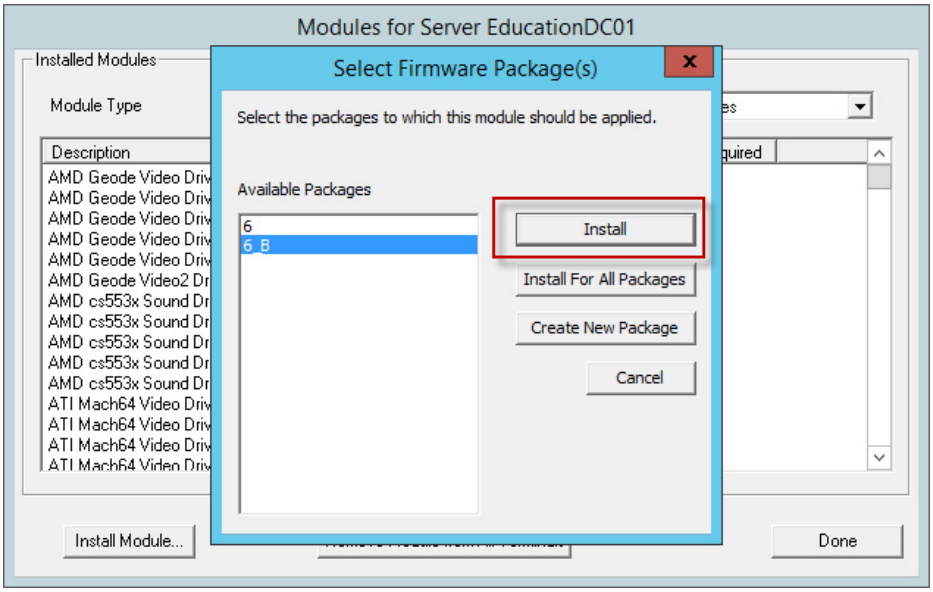
Figure 800 - File Browser



9. Highlight the needed module and click Open.

   A dialog box appears, which allows the selection of a package you want to add the module.

Figure 801 - Select Firmware Package Dialog Box



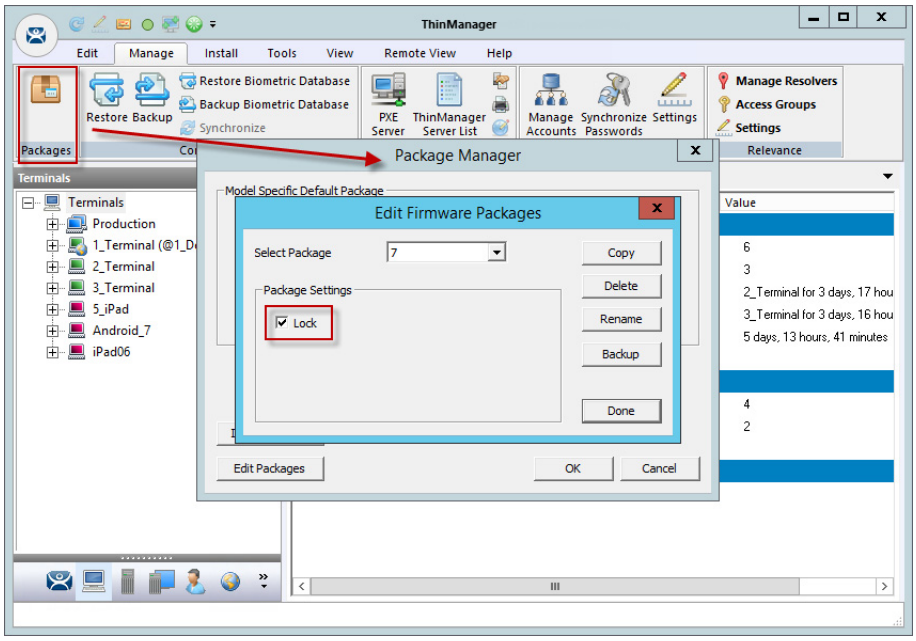
10. Highlight your copied module and click Install.

    The new module is added to that package.

11. Click Done on the Modules dialog box to finish.

You can lock a package on the Edit Firmware Packages window.

Figure 802 - Edit Firmware Packages Dialog Box



12. Choose Manage>Packages on the ThinManager menu bar.

    The Package Manager dialog box appears.

13. Click Edit Packages.

    The Edit Firmware Packages dialog box appears.

14. Choose the package from the Select Package pull-down menu and check Lock.

    The package is locked.

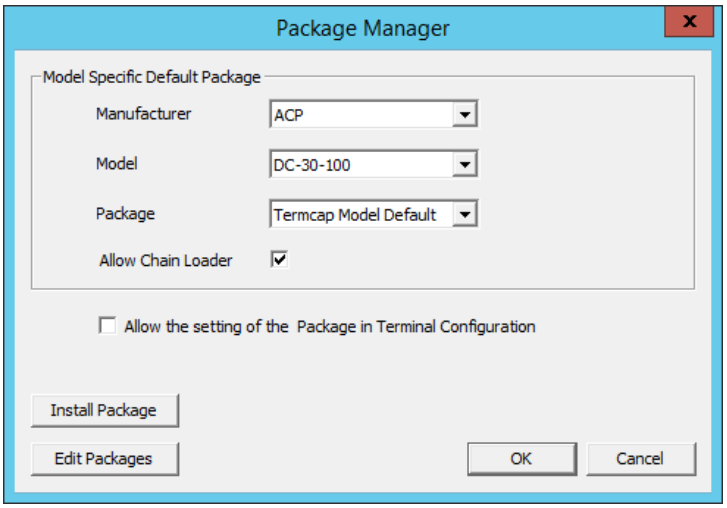
Configure Packages for a Model of Thin Client

ThinManager allows you to change the package for all units of a make and model.

1. Choose Manage>Packages.

   The Package Manager dialog box appears.

Figure 803 - Package Manager



2. Choose your Manufacturer and Model from the pull-down menus.
3. Choose the Package you want from the pull-down.

   This becomes the Model Default.
4. Click OK.

   The Package Manager dialog box closes.

Older makes and models have fewer options than newer, more powerful makes and models.

Figure 804 - ACP DC-30-100 Firmware

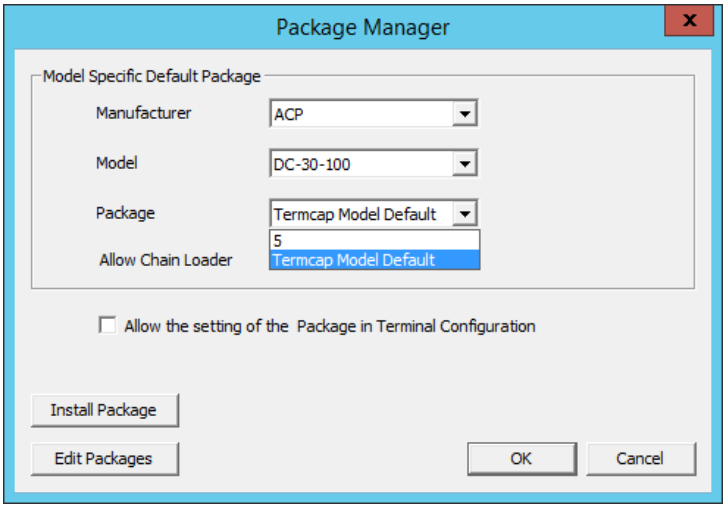


Figure 804 provides an example of limited package availability for the DC-30-100, an older model, as it can only run package 5. This is set in the TermCap as the default package.

Figure 805 - ACP TC3500 Firmware

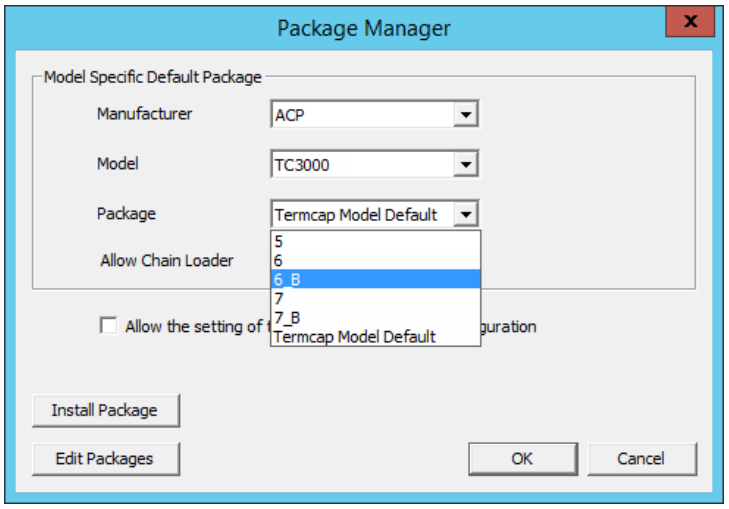
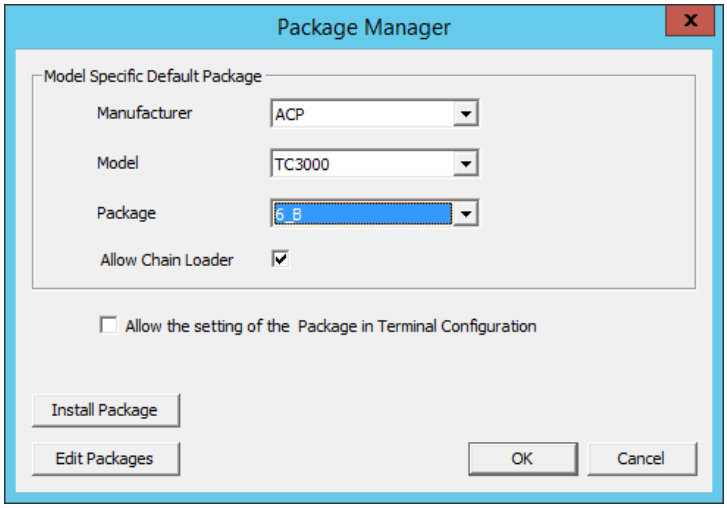


Figure 805 shows package options for the more recent ACP TC3000, which can run several versions of firmware and custom firmware.

Figure 806 - New Default Firmware



The firmware package chosen from the Package pull-down menu sets that firmware as the default to run on any Terminal of that make and model.

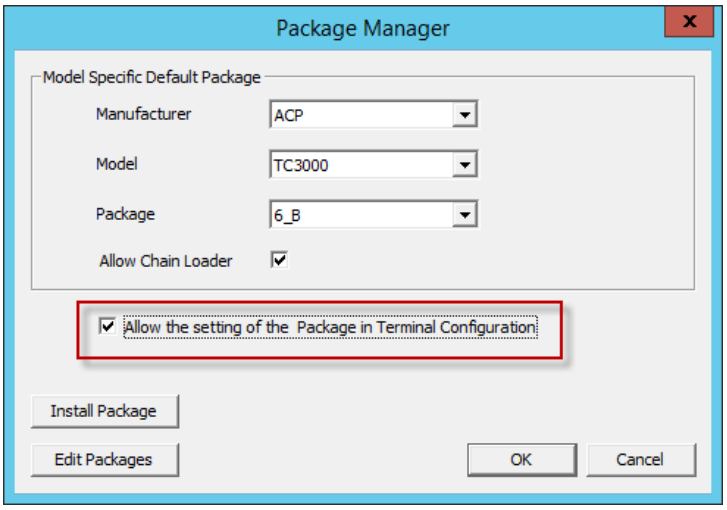
Configure Packages for an Individual Thin Client

Packages can be changed for an entire series of thin clients or for an individual thin client. This change is done in the Package Manager dialog box.

1. Choose Manage>Packages.

   The Package Manager dialog box appears.

Figure 807 - Package Manager

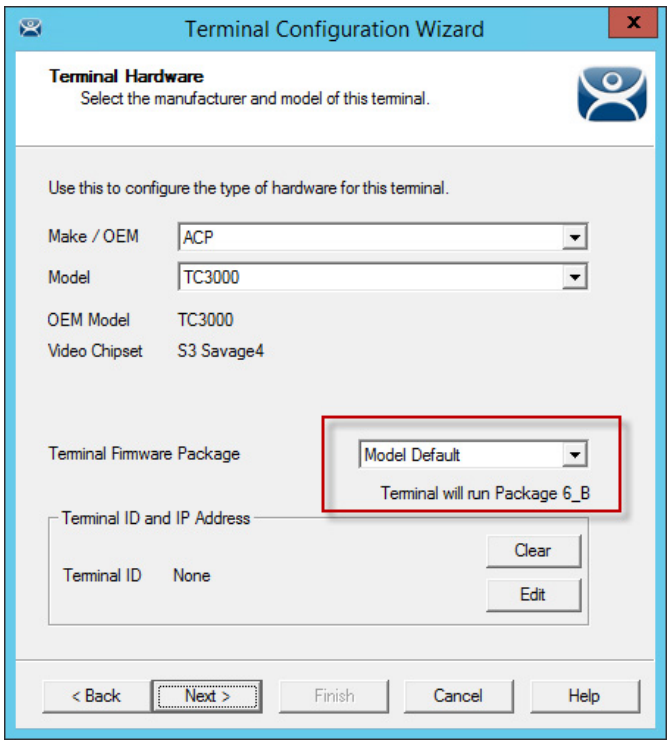


2. Check Allow the setting of the Package in Terminal Configuration, which allows you to override an individual thin client's package setting.
3. Click OK.

   The Package Manager dialog box closes.
4. Double-click on the Terminal in the Terminal branch of the ThinManager tree.

   The Terminal Configuration Wizard appears.
5. Click Next until the Terminal Hardware page appears.

Figure 808 - Terminal Firmware Package Setting

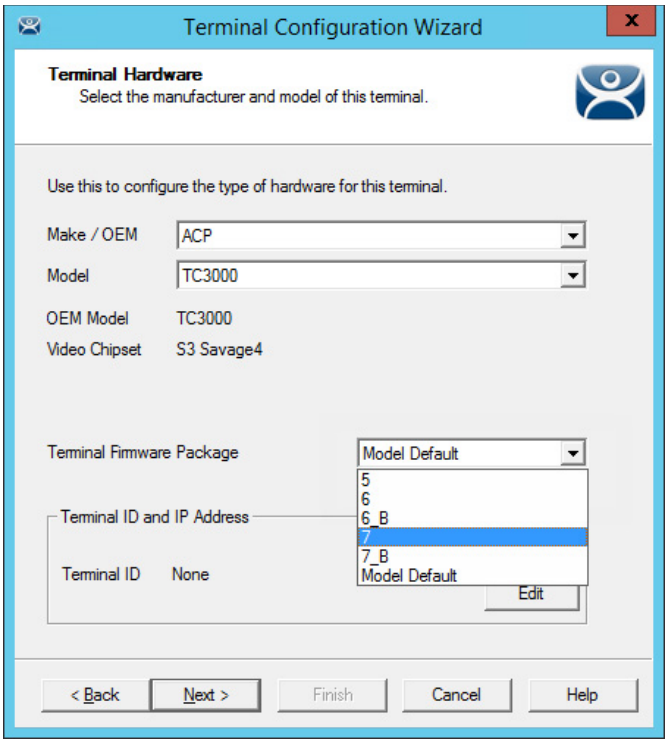


The Terminal Firmware Package pull-down menu allows you to pick a different package to run once you allow individual firmware on the Package Manager dialog box.

Figure 808 on page 547 shows that Package 6_b that was used in the previous example.

Once the firmware setting is allowed on the Package Manager dialog box, it appears in the Terminal Firmware Package pull-down menu on the Terminal Hardware page, which allows you to choose it for that individual Terminal.

Figure 809 - New Terminal Firmware Package Setting



6. Choose the Terminal Firmware Package from the pull-down menu.
7. Click Finish.

   The Terminal Configuration Wizard closes.
8. Highlight the Terminal in the ThinManager Servers tree and choose Tools>Reboot from the ThinManager menu.

   The Terminal reboots, and the ThinManager splash screen for that firmware is displayed.

Modules

Modules are components and drivers for the Terminals that are not 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 follow, the types and modules include the following.

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 covers the details of a dozen modules. The first covers the general steps with the Key Block Module. The other modules cover the individual configuration.

Module List

ICA* - see ICA Modules on page 554.

- Citrix ICA UseAlternateAddress Module
- Citrix ICA wfclient.ini Extension Module
- Citrix Receiver Version 13.3

Keyboard – See Keyboard Modules on page 555.

- 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 Controller Module
- Share Keyboard and Mouse Follower Module

Language - See Language Modules on page 558.

- Language Selection Module

Local Storage - See Local Storage Modules on page 558.

- USB Flash Drive Module
- USB Memory Card Reader Module (Package 5 only)
- Boot Assist (Package 9.4 and newer, specific ASEM hardware only)

Miscellaneous - See Miscellaneous Modules on page 566.

- Add Serial Port
- Bluetooth® Module
- Firmware Update Module
- Generic USB Redirection Module (requires FreeRDP 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 on page 572.

- Locate Pointer Module
- Mouse Configuration
- Serial Mouse Driver
- Share Keyboard and Mouse Controller Module
- Share Keyboard and Mouse Follower Module

Network - See Network Modules on page 573.

- Domain Name System Module
- Network Time Protocol Module
- Second Network Module
- Third Network Module

RDP - See RDP Modules on page 575.

- FreeRDP Client Module*
- Nymi Band Module
- RDP Experience Module
- RDP Port Module
- RDP Serial Port Redirection Module
- RDP Session IP Module
- Smart Cart Module

Relevance - See Relevance Modules on page 576.

- Bluetooth Module
- DigitalPersona UareU Fingerprint Reader
- Logging Configuration Module
- Lumidigm Fingerprint Reader
- RF Ideas pcProx Module
- RF Ideas pcProx USB Module
- RF Ideas pcProx Sonar Module
- SecuGen Fingerprint Reader
- TermMon ActiveX Configuration Module
- USB Flash Drive Module

- USB ID Reader Module

Screen Saver - See Screen Saver Modules on page 584.

- MultiSession Screen Saver Module
- Screen Saver Module

Sound - See Sound Modules on page 586.

- 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 on page 588.

- 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 MultiTouch Screen Driver*
- USB Touch Screen Driver
- Xycom 33XX Touch Screen Driver (Package 5 only)
- Zytronic Touch Screen Driver

Video Driver - See Video Driver Modules on page 591.

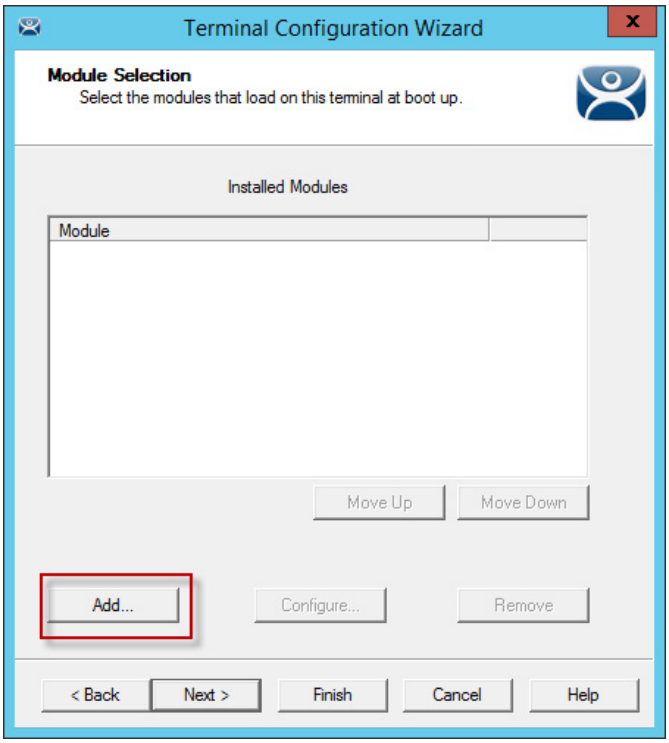
- Advanced Video Configuration Module
- Core Video Module*
- Custom Video Mode Module
- Monitor Configuration Module

Add a Module

1. Double-click on your Terminal.

   The Terminal Configuration Wizard appears.
2. Click Next until the Module Selection page appears.

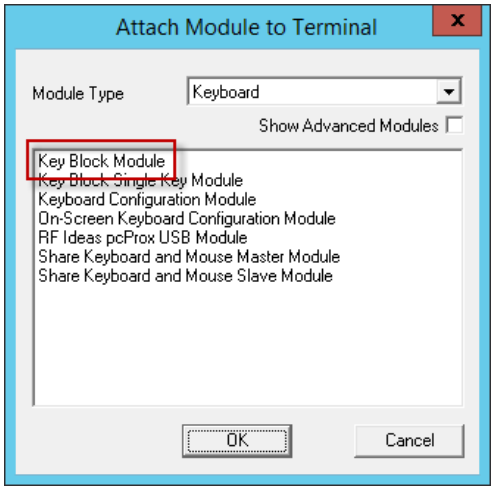
Figure 810 - Module Selection Page



3. Click Add.

   The Attach Module to Terminal dialog box appears.

Figure 811 - Attach Module to Terminal Window



Modules can be viewed by category or as a whole.

4. Choose a module category from the Module Type pull-down menu.
5. Highlight a module and click OK.

Figure 812 - Key Block Module

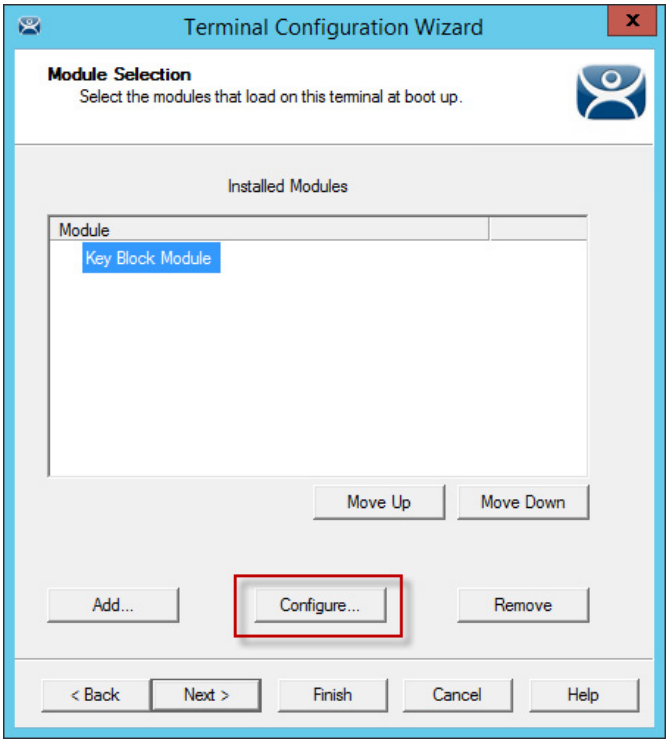


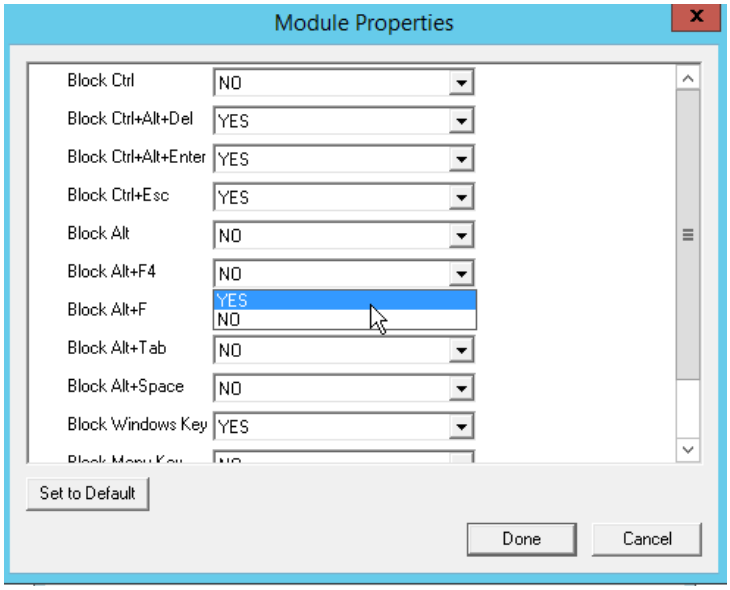
Figure 812 shows the Key Block Module in the Installed Modules pane.

The Key Block Module has configurable settings.

6. Highlight the Key Block Module and click Configure.

   The Module Properties dialog box appears, in which settings can be configured.

Figure 813 - Module Properties



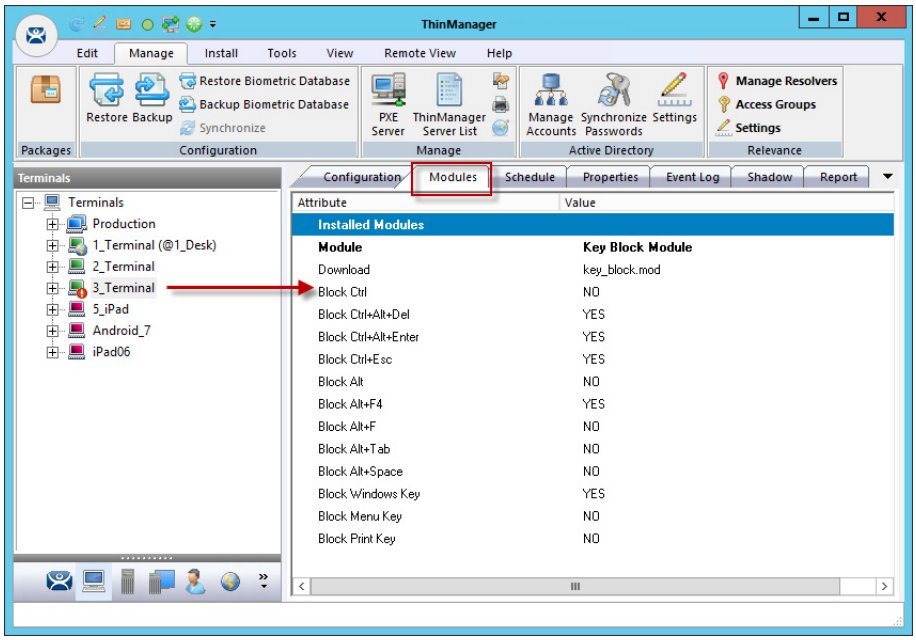
7. Use the pull-down menu to change a parameter or type a new setting.

   By default CTRL+ALT+DEL, CTRL+ALT+ESC, and CTRL+ESC are blocked.

a. To change other key combinations, change the respective pull-down value to Yes.

8. Click Done to close the Module Properties dialog box.

Figure 814 - Modules Tab for a Terminal



The module and settings are displayed on the Modules tab when the Terminal is highlighted.

The 3_Terminal shows the red Configuration Indicator icon to indicate that the configuration changed when the module was added, but it has yet to be restarted to load the new configuration.

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.

ICA Modules

ICA Modules are advanced modules for advanced users of the ICA client communication protocol.

Citrix ICA UseAlternateAddress Module

The Citrix ICA UseAlternateAddress Module is used by advanced Citrix users to specify connections to Citrix Servers.

Configuration includes Use Alternate Address, Browser Protocol, and HttpBrowser Addresses.

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.

Keyboard Modules

Keyboard Modules are modules used to control or alter keyboard behavior.

Key Block Module

The Key Block module traps certain keystrokes and prevents them from being sent to the Remote Desktop Server for processing.

Key combinations to be blocked can be configured by in the Module Properties. To launch Module Properties, follow these steps.

1. Highlight the module on the Module Selection page and click Configure.

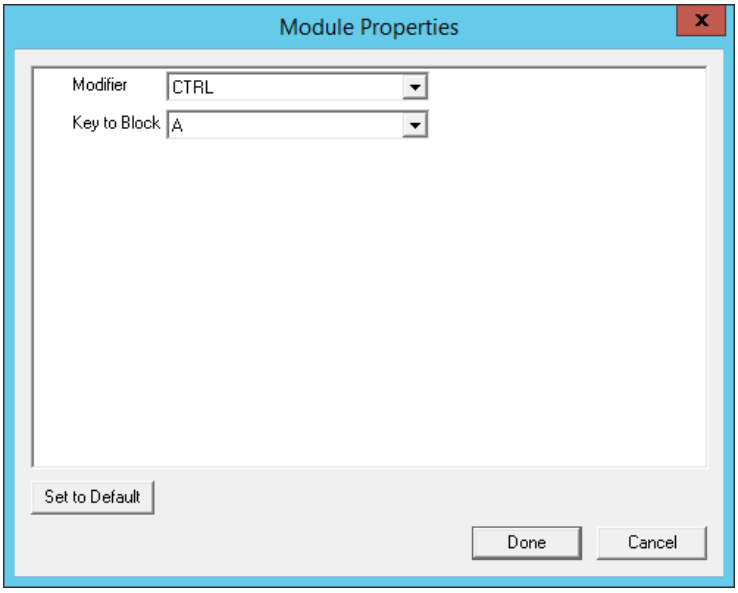
   A Module Properties dialog box appears.
2. Choose the parameter to change in the Module Properties dialog box and choose the Value in the pull-down menu.

The key combinations that have a value of YES are blocked from reaching the Remote Desktop Server.

Key Block Single Key Module

The Key Block Single Key Module lets you block a single key combination from being sent from the Terminal to the session.

Figure 815 - Key Block Single Key Module Properties



Add and configure the Key Block Single Key Module to block a single set of key combinations.

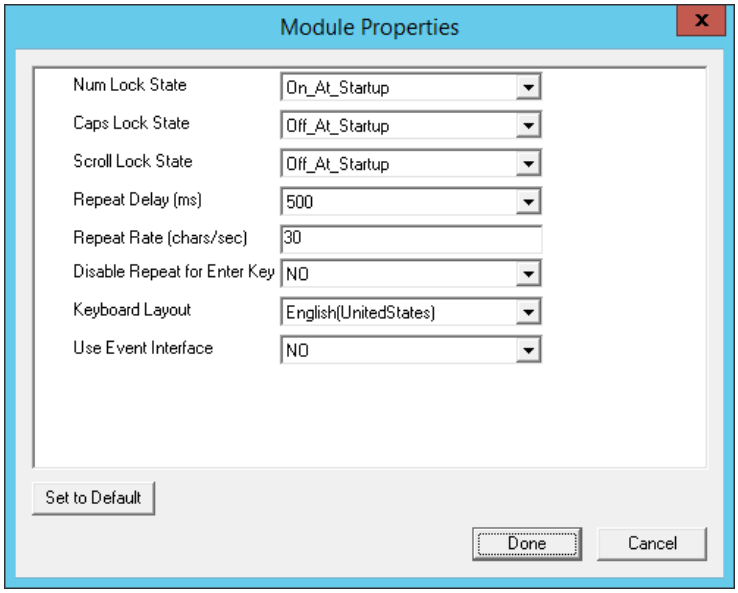
You can set ALL, CTRL, ALT, or CTRL+ALT as the modifier key(s) and set A-Z, F1-F12, and ESC, Tab, Backspace, and so on as the key to block.

If you have multiple keys to block, add the Key Block Single Key Module once for each combination and configure them accordingly.

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.

Figure 816 - Keyboard Configuration Module Properties



The Keyboard Configuration parameters include the following.

Parameters	Description
Num Lock State	Allows the Number Lock to be set to On at startup, Off at startup, always On, or always Off.
Cap Lock State	Allows the Caps Lock to be set to On at startup, Off at startup, always On, or always Off.
Scroll Lock State	Allows the Scroll Lock to be set to On at startup, Off at startup, always On, or always Off.
Repeat Delay (ms)	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 sends only one keystroke even if the key is held down.
Repeat Rate (char/sec)	Sets the number of characters per second that a held down key sends.
Disable Repeat for Enter Key	When set to Yes, it prevents the Enter key from repeating if it is held down.
Keyboard Layout	Allows the thin client to use keyboards other than the default English (United States) keyboard map.

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.

Parameters	Description
Show Keypad	Adds the keypad to the display.
Show Function Keys	Adds the function keys to the display.
Show Control Key	Adds the Control key to the display.
Show Alt Key	Adds the ALT key to the display.
Num Lock State	Turns the numbers lock on or off on launch.
Inactivity Timeout (seconds)	Sets the duration of the idle time that closes the keyboard.
Keyboard Scale Percentage	Sets the width of the keyboard as a percentage of the screen.
Font Size	Sets the font size of the keys.

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. These include 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.

These are the parameters.

Parameters	Description
Mode	Allows the device to be used in TermSecure Mode, Wedge, or TermMon mode.
TermSecure	Sends data to ThinManager for use with TermSecure.
Wedge	Sends data straight to the session as a keyboard wedge.
TermMon	Sends data to the TermMon ActiveX that you embed in your application.
Allow Manual TermSecure Login	When set to Yes, allows a ThinManager user to log in to 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	When set to Yes, requires a TermSecure user to enter their password for access even if the password is configured in ThinManager.

See Card and Badge Configuration for a ThinManager User on page 406 for details.

Share Keyboard and Mouse Module

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).

Share Keyboard and Mouse has a Controller module that is added to the controlling Terminal and a Follower module that is added to the dependent Terminals.

Share Keyboard and Mouse allows you to place several monitors connected to thin clients, side-by-side or top-to-bottom. The Share Keyboard and Mouse Controller module is loaded on the center thin client.

1. Add the IP addresses of the secondary follower thin clients to configure it.

The other Terminals receive the Share Keyboard and Mouse Follower module.

2. Once the Share Keyboard and Mouse Controller Module is added to a Terminal, highlight it in the Installed Module dialog box and click Configure.

   These are the configuration settings.

Setting	Description
Left Terminal IP Address	Enter the correct IP address for the Follower Terminal on the left of the Controller Terminal, if used, and click Set.
Right Terminal IP Address	Enter the correct IP address for the Follower Terminal on the right of the Controller Terminal, if used, and click Set.
Top Terminal IP Address	Enter the correct IP address for the Follower Terminal on the top of the Controller Terminal, if used, and click Set.
Bottom Terminal IP Address	Enter the correct IP address for the Follower Terminal on the bottom of the Controller Terminal, if used, and click Set.
Allow Interactive Shadow of Controller	Normally, a Terminal with the controller module loaded is blocked from interactive shadow. If you want to allow interactive shadowing on the Controller, highlight the Allow Interactive Shadow of Controller parameter, choose Yes from the Value pull-down menu, and click Set.
Controller IP Address	Enter the IP address of the Controller Terminal and click Set to allow the follower module to be configured to connect to a specified Controller.

The Share Keyboard and Mouse Follower module is loaded on the secondary thin clients using the same methods in which other modules are loaded.

3. Click Done when finished.

Once the ThinManager Enabled thin clients are booted, the mouse on the controller thin client can be moved seamlessly into the other desktops. The keyboard is active on whatever screen the mouse pointer is present.

This feature allows an operator to have control of several displays with only one keyboard and mouse. The mouse movement is seamless, which allows access to displays without switching.

A Controller Share Keyboard and Mouse session cannot be interactively shadowed in ThinManager unless it is configured to allow it.

The keyboards and mice for the follower thin clients can be left attached but stowed away until a multi-user configuration is needed.

Language Modules

The Language modules allow different languages to be used by the terminal.

Language Selection Module

The Language Selection Module sets the language on the terminal. You can use the Keyboard Configuration module to set the keyboard language and set the language in the session.

Local Storage Modules

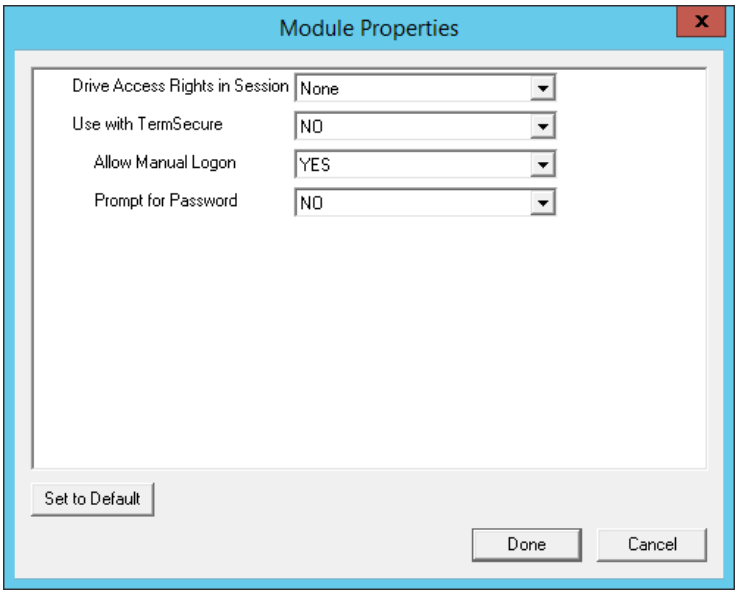
The Local Storage modules allow the use of USB ports on thin clients. By default, the USB ports are not active for security reasons.

USB Flash Drive Module

By default, USB ports are disabled in the ThinManager system. You can use the USB ports for keyboards and mice, but not USB flash drives. For USB flash drives, you need to allow the port to be used with the USB Flash Drive Module.

Also, the USB port works with a device that functions as a keyboard wedge.

Figure 817 - USB Flash Drive Module Properties



The USB Flash Drive Module has several parameters.

Parameter	Description
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 • None sets the flash drive to access only the unique serial number to make it usable as a TermSecure ID device
Use with TermSecure	• YES allows the device to be a TermSecure identifier • NO in conjunction with a ReadWrite Access Rights allows the device to be used as a remote storage drive
Allow Manual Login	• Yes allows a ThinManager user to log in to a Terminal without a TermSecureID device • No requires TermSecure users to use a TermSecure ID device to log in
Prompt for Password	Yes requires a ThinManager User to enter their password for access even if the password is configured in ThinManager.

USB does not map to the session like serial does. If you want to add a USB device that requires a driver to be installed, such as a printer, you can use an IP-to-USB converter that allows you to address the device and mount the drives from the session.

USB Memory Card Reader Module

The USB Memory Card Reader Module allows USB card readers to connect to a Terminal.

These are the USB Memory Card Reader Module parameters.

Parameter	Description
Number of Slots in Reader	Sets the number of slots that the card reader uses.
Read Only Access	• Yes limits the user to reading the card. • No allows the user to read and write to the card.

BootAssist

BootAssist provides the ability to leverage the on-board storage of a thin client to optionally cache the Firmware, Terminal Profile, and/or Container Images and Applications. This enables the thin client to boot even if it could not reach a configured ThinServer.

With ThinManager 14.1, cached Container Images still require a connection to ThinServer in order to launch properly, even if they are cached on local storage.

The BootAssist Module has several parameters.

Parameter	Description
Storage Device	Allows the user to specify a storage device to use for caching other than the default defined in the TermCap database. In almost all cases, it is recommended to leave this setting as Default.
Cache Firmware	• YES stores the terminal's assigned firmware package on the thin client's local storage • NO does not store the terminal's assigned firmware package on the thin client's local storage
Cache Terminal Profile	• YES stores the terminal's configuration profile on the thin client's local storage • NO does not store the terminal's configuration profile on the thin client's local storage
Cache Container Images	• YES stores any configured Docker Container Images on the thin client's local storage • NO does not store any configured Docker Container Images on the thin client's local storage
Allow Container Local Storage	• YES enables the storage of configured Container Applications on the thin client's local storage (set per Container Host Display Client) • NO disables the storage of configured Container Applications on the thin client's local storage

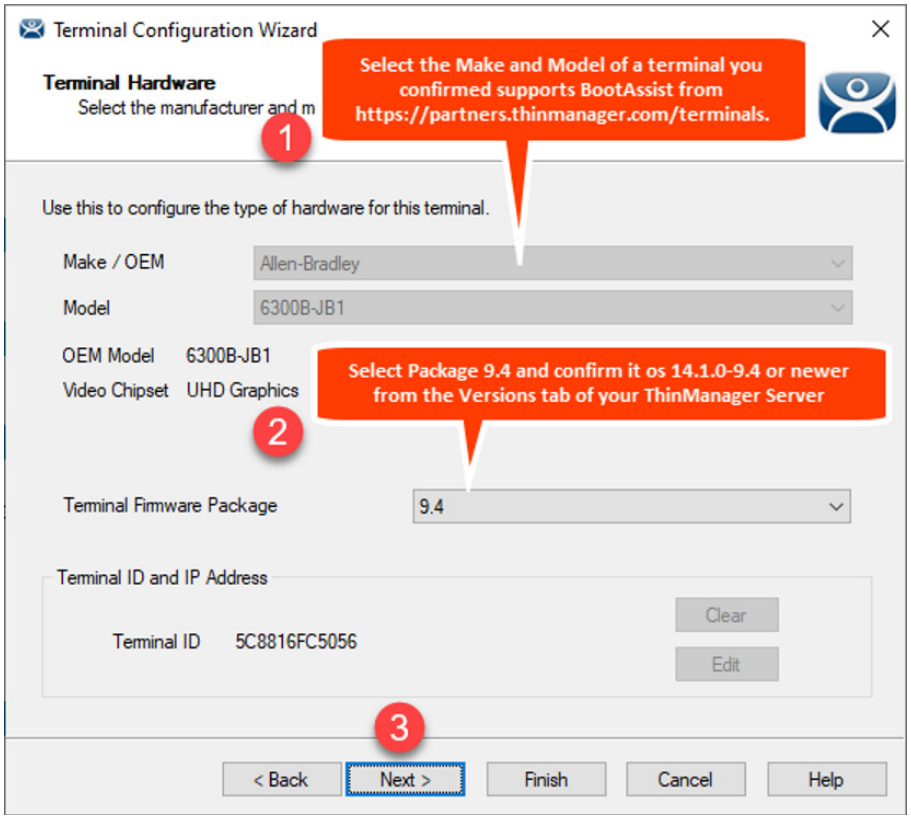
In order to utilize the BootAssist module, you need the following:

1. A thin client that supports BootAssist. Please refer to https://partners.thinmanager.com/terminals, and then filter for BootAssist.
2. The thin client must include on-board storage (the minimum available from the device manufacturer is sufficient).
3. The thin client must include a Trusted Platform Module (TPM), and it must be enabled in BIOS. This is required in order to encrypt what is being cached on the thin client.
4. Firmware package of 14.1.0-9.4 or newer.
5. TermCap2 database 14.1.137 or newer.
6. A redundant ThinManager license (if you intend to boot your thin client when ThinServer is unreachable).

Here are the steps to deploy BootAssist:

1. Create a new terminal or modify an existing terminal.
2. Within the Terminal Configuration Wizard, navigate to the Terminal Hardware page and make sure you have package 9.4 (or newer) selected.

Figure 818 - Terminal Hardware page

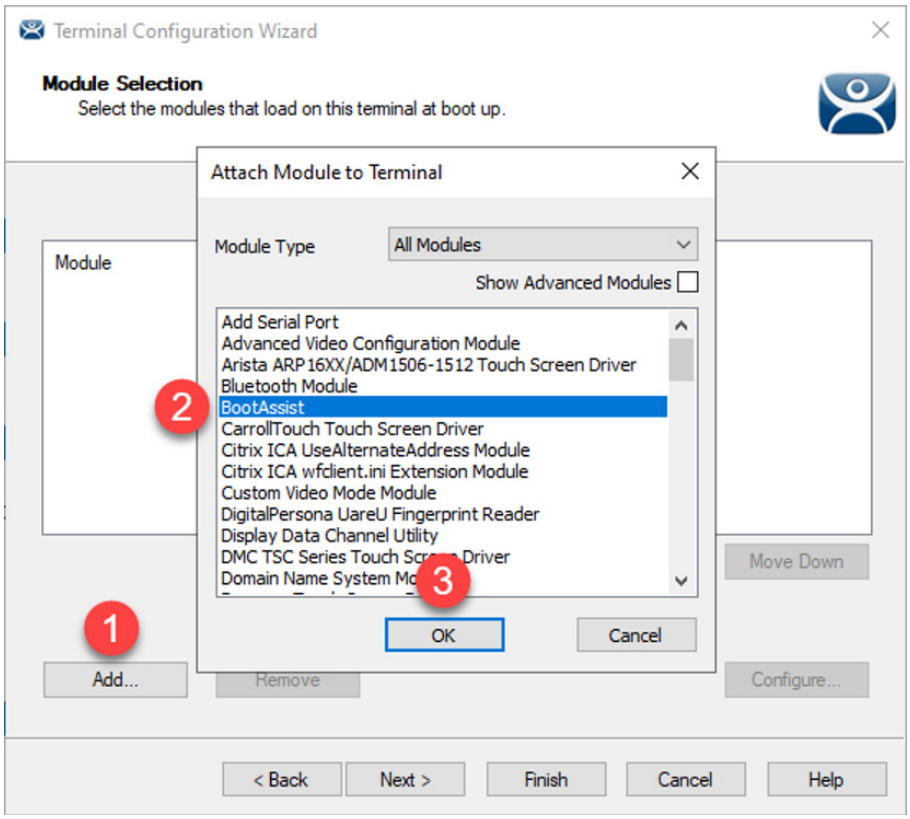


To confirm your specific package version, click the ThinManager Server icon in the button bar, then highlight your ThinManager Server from the ThinManager Servers tree; finally, select the Versions tab. Check that your Package 9.4 is 14.1.0-9.4 or newer.

If you need to change the firmware package assigned to your terminal and the Terminal Firmware Package pull-down menu is disabled in the Terminal Configuration Wizard, go to the Manage ribbon, and then click the Packages icon. From the Package Manager window, you can: (a) check Allow the setting of the Package in Terminal Configuration (which enables the Terminal Firmware Package pull-down menu in the Terminal Configuration Wizard), and/or (b) assign a different Package to the Manufacturer and Model that you are using in your application (NOTE: this changes the Package used by all terminals configured for the selected Manufacturer and Model).

3. Advance through the Terminal Configuration Wizard until you reach the Module Selection page. Click Add. Select BootAssist, and then click OK.

Figure 819 - Attach Module to Terminal window



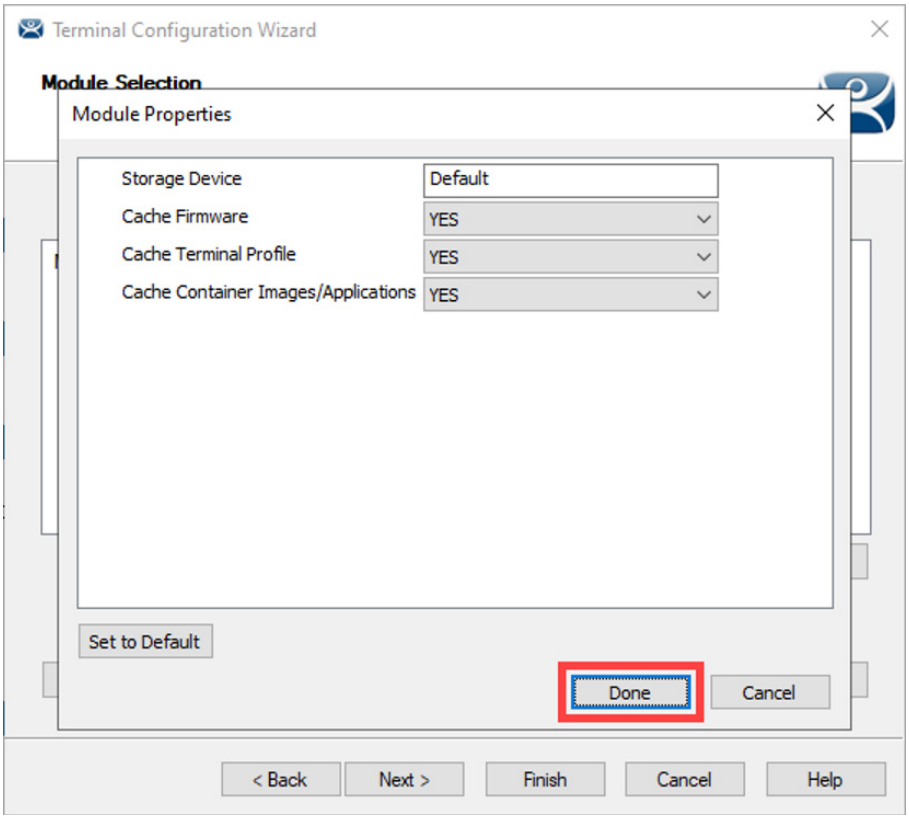
If the BootAssist module is not visible from the module list, make sure you:

- are running ThinManager 14.1 or newer
- have selected a Make/Model that supports BootAssist
- have selected firmware package 9.4 and confirmed it is 14.1.0-9.4 or newer
- have a TermCap2 database that is 14.1.137 or newer

If BootAssist is not visible still, visit downloads.thinmanager.com and see if there is an updated TermCap2 database available. If so, download it, install it, and try again.

4. Double-click the BootAssist module to configure it. Click Done, and then click Finish. Reboot the terminal to apply the changes.

Figure 820 - Module Properties window



During the next boot cycle, notice the message *Firmware caching has been enabled. Rebooting.*

Figure 821 - ThinManager Rebooting

The terminal proceeds with an automatic reboot to cache what was configured in the BootAssist module. During the subsequent boot sequence, you should see the message *Detecting Boot Device*, and the terminal reboots.

Figure 822 - Detecting Boot Device

5. To further test BootAssist functionality, stop and disable the ThinServer service on your Primary and Secondary ThinManager Servers; then, physically reboot the terminal. With BootAssist enabled and ThinServer unavailable, the terminal fails to get its configuration from ThinServer twice; but, ultimately, boots from what is cached on the local storage.

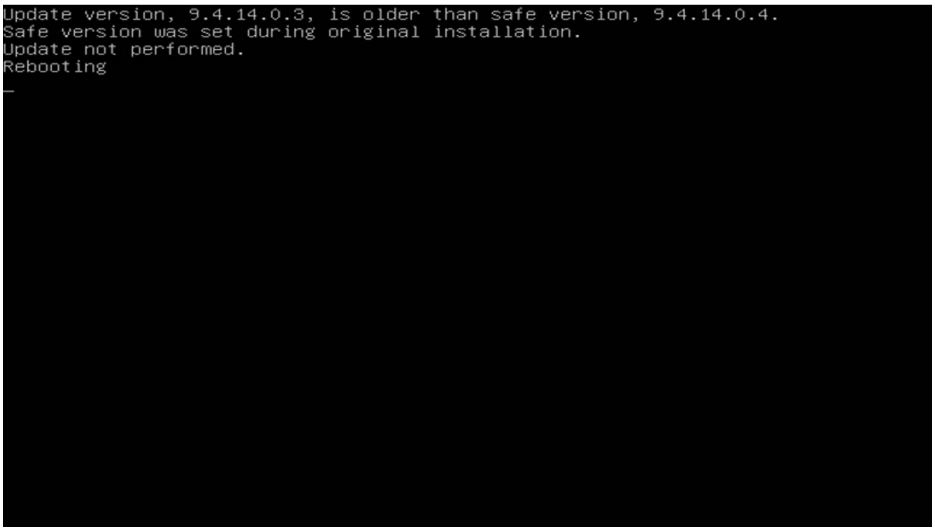
Figure 823 - Failed Configuration Message

Figure 824 - Termporary License Expiration Warning

When BootAssist is used to boot the terminal without ThinServer, it starts using a temporary license for 30 days. In other words, BootAssist can be used to boot a terminal without ThinServer for a total of 30 days.

The first firmware package you cache with BootAssist on a terminal becomes the Safe Version. If you need to assign a firmware package version older than the Safe Version, BootAssist does not permit you to do so.

Figure 825 - BootAssist Message: Update Not Performed



In order to assign a firmware package older than the Safe Version, follow these steps:

1. Return to the Terminal Configuration Wizard and navigate to the Terminal Hardware page.
2. Select the original firmware package used with BootAssist from the Terminal Firmware Package pull-down menu.
3. Navigate to the Module Selection page.
4. Double-click the BootAssist module.
5. Set the Cache Firmware property to NO. Click Done, and then click Finish.
6. Reboot the terminal.

7. Once the terminal is rebooted, return to the Terminal Hardware page of the Terminal Configuration Wizard.
8. Select the desired firmware package to use now with BootAssist from the Terminal Firmware Package pull-down menu.
9. Navigate to the Module Selection page.
10. Double-click the BootAssist module.
11. Set the Cache Firmware property to YES. Click Done, and then click Finish.
12. Reboot the terminal.

As indicated earlier, BootAssist requires a ThinManager Redundancy license if you need the thin client to boot when ThinServer is unreachable. BootAssist is not intended to circumvent ThinManager Redundancy. ThinManager Redundancy is still the primary recommendation for deployments that require high availability. For ThinManager Activation (TMA), BootAssist just needs to validate that you have a Redundant license available. For FactoryTalk Activation (FTA), BootAssist requires your Primary and Secondary ThinManager Servers to be synchronized in order to validate that you have a Redundant license available.

As noted in Chapter 5, to deploy an Optix application to a thin client requires some special considerations. While BootAssist does provide the ability to cache the new Optix Container Image and an associated Optix Application, it does not provide a method to persist any Optix-related data captured during runtime. Each time you reboot a terminal configured with BootAssist to cache the Optix Container Image and an Optix Application, it unzips the original Optix Application imported into ThinManager and runs it within the Optix Container Image. Therefore, if your Optix application requires DataStores that persist across thin client reboots, you need to utilize either an ODBC database and/or a Remote InfluxDB database for this data.

Removal of the BootAssist module is a two-step process.

1. Set all caching settings in the BootAssist module to NO and reboot the terminal.
2. Once the terminal has rebooted, remove the BootAssist module from the terminal and reboot the terminal again.

Miscellaneous Modules

These are modules that do not fit into other categories.

Add Serial Port

The Add Serial Port Module is used only to configure the serial ports of daughter boards that add additional serial ports to Terminals.

1. Add a module for each additional serial port.

   Each module lets the user configure one additional port.

These are the Add Serial Port Module parameters.

Parameter	Description
Port Number	Set to the port number of the new port.
Port Address	Set to the port address of the new port.
IRQ	Set to the IRQ of the new port.
UART	Set to the chipset type for the new port.

Barcode Configuration Module

This module sets the protocols that a tablet uses to scan barcodes.

Bluetooth Module

See the Relevance Modules on page 576 for more information.

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 does not have to download the entire firmware at boot. Instead, the unit can boot locally and download just the configuration to save bandwidth. This is most commonly used with units that 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.

The firmware download can vary depending on the bandwidth of the connection and the size of the update. It is recommended that updates be done over a wired LAN versus a wireless connection.

The Firmware Update module has three configurable parameters.

Parameter	Description
Confirm at Terminal	• Yes prompts the operator to choose between an immediate firmware update or an update at the next Terminal boot. • No causes the firmware download to take place immediately.
Force Update	Yes forces the Terminal to always download the firmware for an update. Ordinarily, a stored firmware Terminal with the Firmware Update module checks firmware version numbers at boot and only downloads a new firmware if the versions are different.
Disable Update	Prevents the download and flash of a new firmware if it is installed. This allows the administrator to select the time of update instead of an automatic update.

The module downloads firmware when it detects a different firmware. Since this only happens 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 updates when the firmware is different, it tries to update the firmware if you boot it from a ThinManager server with older firmware.

Firmware Update Program

Once the new firmware is downloaded, an update program runs on the Terminal to rewrite the new firmware to the storage. The program displays a warning, which state that the Terminal must not be reset or powered off during the process, which usually takes around 30 seconds. If you ignore the

warning, the stored firmware can be corrupted; so, it is important to leave the Terminal alone for that time period.

IMPORTANT The Terminal must not be reset or powered off during the brief period that the update program writes the firmware to the firmware storage device. It is recommended that you update firmware over a wired LAN versus a wireless connection.

Stored Firmware Terminal Configuration

A stored firmware Terminal loads the firmware locally before it connects to the ThinManager server. The stored firmware Terminals have a setup program that allows configuration of the connection.

1. Press any key to enter the program when prompted during the boot process.

   A setup screen is displayed.
2. Save or discard changes before the boot process resumes.

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 versus using the legacy "Individual Remote Desktop Servers," the module is hidden from view unless Show Advanced Modules is checked.

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 displayed immediately, which eliminates any downtime due to Remote Desktop Server failure. See Instant Failover on page 164 for details.

The Instant Failover Module is used only with Terminals that use Individual Remote Desktop Servers. Terminals using Display Clients have Instant Failover checked in order to use it. (See Figure 177 on page 136).
Do not use the Instant Failover module while using Display Clients.

The Instant Failover function requires an Instant Failover license for each Terminal that uses it.

Instant Failover Configuration with Use of 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 behind the primary session. There is an option that allows one to switch between sessions with a hot key.

Parameter	Description
Hot Key Session Switching	Set to Enabled for the hotkey combination to toggling between sessions.
Hotkey Combination is CTRL+	The value of the hotkey is defaulted to CTRL+F9, but it can be assigned to any function key.

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 to which the client connects.
2. Add the Local Print Module to the thin client as described in Add a Module on page 552.
3. Configure the Print Driver Name parameter in the module to contain the print driver's 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.
   a. Choose Start>Settings>Printers to launch the Printer Property page for a printer and choose the appropriate printer.

      The Printer Queue dialog box appears.

   b. Choose Printer>Properties to launch the Printer Properties page.

      The Advanced tab on the Printer Properties page contains the Print Driver name.

   c. Type the Print Driver name into the appropriate field on the Local Print Module.

When printing from the client, the printer is displayed as Printer/username/session number.

MultiStation Configuration Module

The MultiStation Configuration Module allows you to specify how many keyboards and mice are at each station.

The settings include these.

Setting	Description
Station Number	Specifies the station number to configure.
Number of Keyboards	Sets the number of keyboards at the selected station.
Number of Mice	Sets the number of mice at the selected station.

MultiStation is supported on firmware platform versions 6.0 through 9.0. Firmware platform 9.1 and later leverage a different Linux kernel in which MultiStation is not technically viable. Therefore, MultiStation is not supported on firmware platform versions 9.1 or earlier. The MultiStation checkbox is not available in ThinManager when newer firmware packages are selected. The recommendation to accomplish the same outcome of MultiStation is to either:

- use thin client hardware that support firmware versions 9.0 or earlier, or
- use more thin client hardware for the additional independent stations needed

Redundant Ethernet Module

Adding the Redundant Ethernet Module to a Terminal with dual network ports allows the Terminal to use the second port as a backup. The Terminal has 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 boots from the first available network port and downloads the configuration. If the first network path fails, it seamlessly switches to the backup port to prevent interruption of service.

Terminal Shadow Module

This module needs to be installed in ThinManager, but it is not applied to a Terminal. A Terminal automatically downloads this module if it is needed.

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 Modules section.

See TermMon ActiveX Configuration on page 583 for details.

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.

1. Highlight the Time Zone parameter to activate the Value pull-down menu that contains time zones.
2. Click Set to accept the changes.
3. Allow time zone redirection in the Group Policy Console of the Windows Remote Desktop Servers.

   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.

See Microsoft documentation for information on Group Policy.

TMTerm DLL Configuration Module

The TMTerm DLL Configuration module is used to communicate with the Terminal sessions from another Terminal or computer.

Setting	Description
Allow Connections from	• 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)	Allows you to list the IP addresses of computers authorized to retrieve the TermMon data. Separate multiple computer IP addresses with a comma.

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.

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 and later.

See Display Client Override for the current method of User Override.

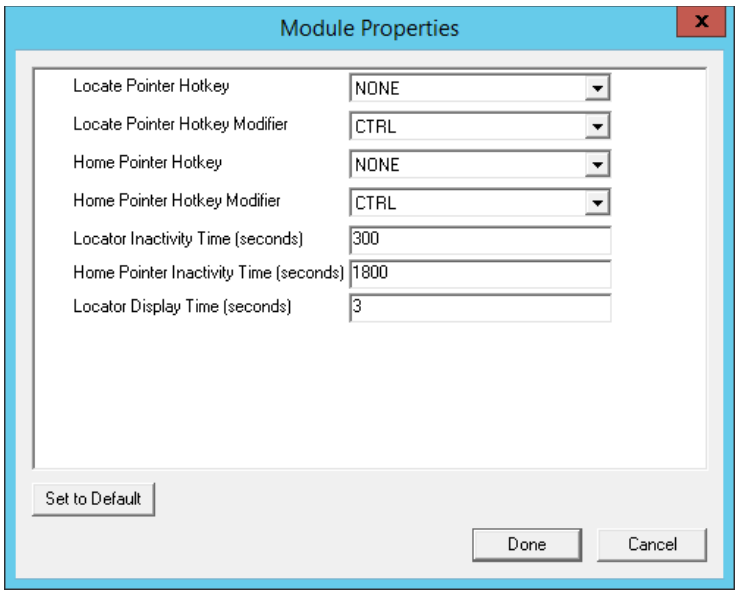
Mouse Modules

Mouse Modules can configure mouse functions in the ThinManager system.

Locate Pointer Module

The Locate Pointer Module adds a large crosshair to the cursor when it becomes active after being idle, which allows you to see its location quickly. This feature is particularly helpful in a MultiMonitor system.

Figure 826 - Locate Pointer Module



The settings include these.

Setting	Description
Locate Pointer Hotkey	Allows you to set a hotkey to make the cursor appear.
Locate Pointer Hotkey Modifier	Allows you to set the modifier key to activate the hotkey to show the pointer cursor.
Home Pointer Hotkey	Allows you to set a hotkey that moves the cursor to the center of the main screen.
Home Pointer Hotkey Modifier	Allows you to set the modifier key that moves the cursor to the center of the main screen.
Locate Inactivity Time (seconds)	Sets the length of the idle time before the locate pointer cursor is activated.
Home Pointer Inactivity Time (seconds)	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)	The length of time that the locate pointer crosshair cursor is displayed when activated.

Mouse Configuration Module

The Mouse Configuration Module allows USB or PS/2 mice to be configured and allows the use of two mice. These are the Mouse configuration settings.

Setting	Description
Primary Mouse Type	Allows both a PS/2 mouse and USB mouse to be used on a Terminal. Define which mouse is considered the primary mouse.
Mouse Protocol	Allows the selection of different protocols used by the mouse.
Scroll Mouse	When set to Yes, allows a scroll mouse to function on a Terminal.
Acceleration Multiplier	Allows the mouse movement to be slowed down or sped up.

Setting	Description
Acceleration Threshold (pixels)	The number of pixels a mouse must move before the acceleration multiplier takes effect.
Left Button	Disables the left mouse button when set to Disabled.
Right Button	Disables the right mouse button when set to Disabled.
Scroll Button	Disables the scroll button when set to Disabled.
Scroll Wheel	Disables the scroll wheel when set to Disabled.

1. To change a parameter, highlight the parameter and choose a new value from the Value pull-down menu.
2. Click Set to accept the new parameter value.

PS/2 Mouse Module

The PS/2 Mouse Module is the predecessor 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.

Setting	Description
Primary Mouse Type	Allows both a PS/2 mouse and USB mouse to be used on a Terminal. Define which mouse is considered the primary mouse.
Scroll Mouse	When set to Yes, allows a scroll mouse to function on a Terminal.
Acceleration Multiplier	Allows the mouse movement to be slowed down or sped up.
Acceleration Threshold (pixels)	The number of pixels a mouse must move before the acceleration multiplier takes effect.

Serial Mouse Driver

The Serial Mouse Driver allows a serial mouse to be used with thin clients.

Setting	Description
Mouse Type	Defines what type of mouse is used.
Serial Port	Set this value to the serial port number used for the mouse.

Share Keyboard and Mouse Modules

See Share Keyboard and Mouse Modules on page 573.

The Share Keyboard and Mouse Master module is licensed for each master thin client. The Share Keyboard and Mouse Follower module is free. Each controller module can have 1...4 follower units. Future releases expand the number of replicas that the master can control.

Network Modules

Domain Name System Module

The Domain Name System Module allows you to specify a DNS server for a Terminal without the need to turn on DNS for the entire ThinManager Server system.

Network Time Protocol Module

The Network Time Protocol (NTP) Module provides a way to sync the time of the terminal with a central time server. This module may be useful if you are hosting Docker Container applications that require time-stamping.

Setting	Description
NTP Server Address	Primary NTP Server Address
NTP Server Address	Primary NTP Server Address

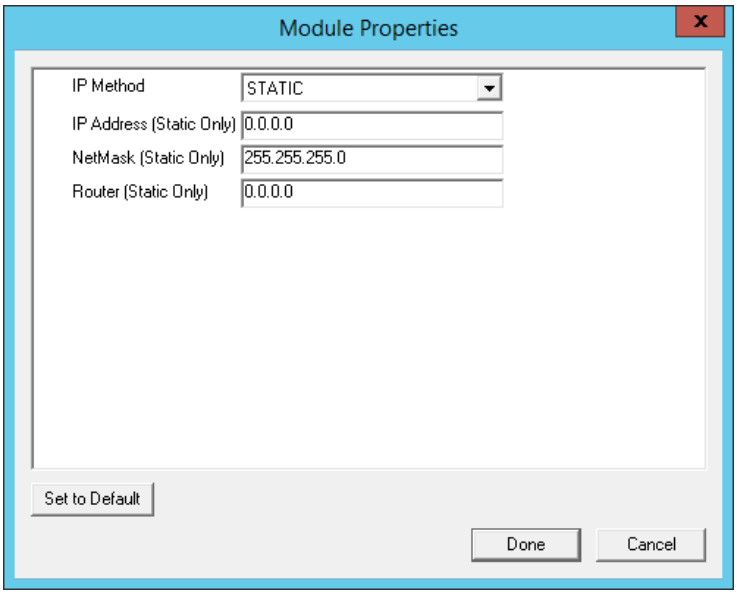
Second Network Module

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 always boots from the first port; but once booted, it enables the second port and allows communication on both networks. This is useful for separating IP camera bandwidth from the process control network, for example.

Figure 827 - Second Network Module



The settings include these.

Setting	Description
IP Method	Allows the second port to use DHCP or a static IP.
IP Address (Static Only)	Allows the second port to be assigned a static IP address.
NetMask (Static Only)	Allows the second port to be assigned a subnet mask.
Router (Static Only)	Allows the second port to be assigned a router.

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.

These are the Third Network Module parameters.

Parameter	Description
IP Method	Allows you to choose a static IP or use DHCP.
IP Address (Static Only)	Allows you to set a static IP address if Static was the chosen IP method.
NetMask (Static Only)	Allows you to set a NetMask if Status was the chosen IP method.
Router (Static Only)	Allows you to set a static IP address for a router if Static was the chosen IP method.

RDP Modules

RDP Experience Module

The RDP Experience Module allows a session to add features when connected to a Windows 2003 Remote Desktop Server with RDP.

These are the RDP Experience Module parameters.

Parameter	Description
Allow Desktop Background	If set to Yes, allows a Terminal to show a desktop background.
Show Window Contents While Dragging	If set to Yes, allows a Terminal to show window contents while dragging.
Allow Menu and Window Animation	If set to Yes, allows a Terminal to show window and menu animations.
Allow Themes	If set to Yes, allows a Terminal to show a desktop theme.
Allow Font Smoothing	If set to Yes, uses the Microsoft font smoothing in the session.
Duplicate Server Connect Delay (seconds)	Adds a delay when a Terminal is creating multiple connections to a Remote Desktop Server and, normally, displays an error message that the server is busy. Add a delay to possibly minimize that error message.
Enable Network Level Authentication	Allows you to turn off NLA (Network Level Authentication) for that Terminal.
Use Hardware Scaling When Available	If set to Yes, uses the local video hardware for scaling.

Enable RDP Experience in Windows Group Policy Editor in order to use these features. See Microsoft documentation for details.

RDP Port Module

The RDP Port Module allows the port that RDP uses to communicate to the Remote Desktop Server with to be changed from the default 3389.

- Type the new port number for RDP in the RDP Server Port Number (decimal) field.

RDP Serial Port Redirection Module

The use of serial ports on a thin client presents a paradox: the session runs 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 looks 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 maps the remote ports on the Terminal to the local ports in the session. If the session references COM Port 1, it is sent to the Terminal COM Port 1.

The RDP Serial Port Redirection Module has no configuration. Add it to map the remote COM Ports.

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.

Setting	Description
Group Name	Specifies the Display Client to use.
Session IP Address	The IP address to use as the alias.
Session IP Address for Instant Failover	The IP address to use for a backup session if the Display Client is configured to use Instant Failover.

Smart Card Module

The Smart Card module must be added to use a Smart Card Reader and Smart Cards.

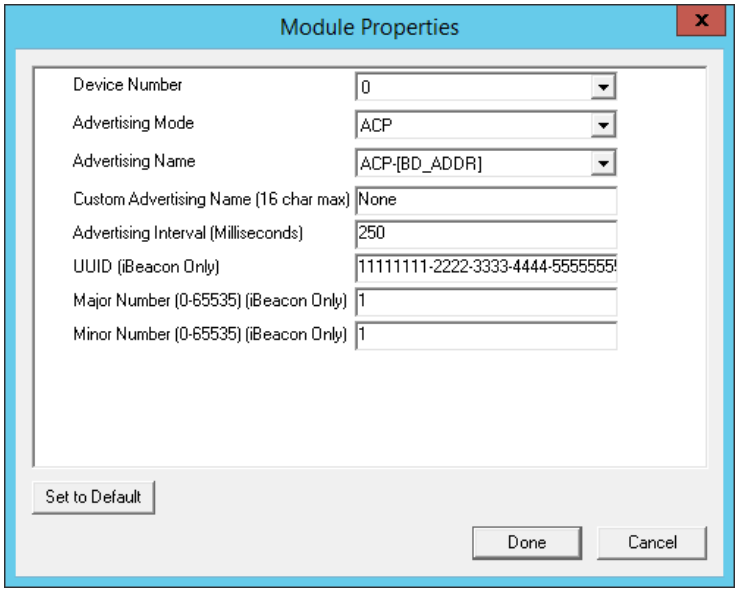
Network Level Authentication (NLA) must be disabled on the Remote Desktop Servers to use a smart card as a login device. It can be left enabled if you are using the smart card to send information to the active session.

Relevance Modules

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 does not require batteries. The Bluetooth module allows you to configure the USB adapter.

Figure 828 - Bluetooth Module



The Bluetooth Module has several settings.

Setting	Description
Device Number	Add this module for each device added and assign each device a different number. ThinManager sorts out which is which.
Advertising Mode	Allows you to set the transmission mode of the USB adapter.
ACP	Sets the adapter to transmit in the ACP protocol.
iBeacon	Sets the adapter to transmit in the iBeacon protocol. You must assign a UUID, a major number, and a minor number.
Disabled	Stops the transmission from the adapter.
Advertising Name	Allows you to choose which naming convention is used to identify the Bluetooth USB adapter.
ACP-{BD_ADDR}	Transmits the Bluetooth address of the USB adapter with the "ACP-" prefix.
ACP-{Terminal Name}	Transmits the Terminal name of the client that hosts the USB adapter with the "ACP-" prefix.
BD-Address	Transmits the Bluetooth address of the USB adapter.
Terminal Name	Transmits the Terminal name of the client that hosts the USB adapter.
Custom	Allows you to set a custom advertising name in the Custom Advertising Name (16 char max) field.
Custom Advertising Name (16 char max)	Allows you to set a Custom Advertising Name if Custom is chosen in the Advertising Name pull-down menu. You are limited to 16 characters.
Advertising Interval (Milliseconds)	Sets the frequency of the Bluetooth signal.
UUID (iBeacon Only)	Each iBeacon has a Universally Unique Identifier (UUID). Allows you to associate your iBeacon to the Terminal if iBeacon was chosen from the Advertising Mode pull-down menu.
Major Number (0-65535) (iBeacon Only)	Allows you to add the iBeacon major number for registration.
Minor Number (0-65535) (iBeacon Only)	Allows you to add the iBeacon minor number for registration.

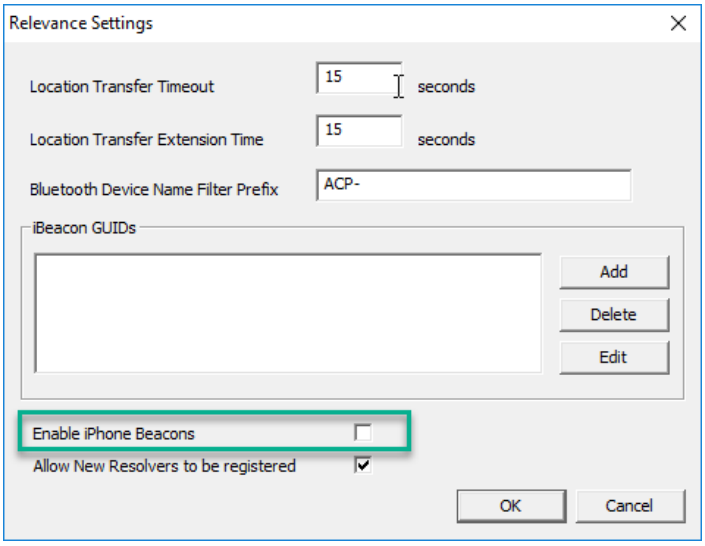
iBeacon USB adapters normally have a UUID, a major number, and a minor number assigned to them. These must be added to the Bluetooth Module in the appropriate fields.

ThinManager® with Relevance® filters Bluetooth adapters by default and only shows Bluetooth beacons with the ACP prefix. If you use the BD-Address, Terminal Name, or Custom advertising names you must turn off the ACP filter, which is done in the Relevance Settings dialog box.

1. From the ThinManager menu bar, choose Manage>Relevance>Settings.

   The Relevance Settings dialog box appears.

Figure 829 - Relevance Settings Dialog Box



Setting	Description
Location Transfer Timeout (seconds)	The amount of time an operator has to allow a session to transfer during a normal Transfer.
Location Transfer Extension Time (seconds)	The amount of time that a transfer can wait when user selects More Time during a transfer.
Bluetooth Device Name Filter Prefix	Allows you to filter Bluetooth beacons by their prefix.
iBeacon GUIDs	Lists the registered iBeacon devices.
Enable iPhone Beacons	Check to allow the ThinManager Beacon application on an iPhone to work as a beacon to identify the location of the ThinManager user. This setting tells the client application (iTMC or aTMC) to look for devices that run ThinManager Beacon, which a free iPhone application available from the App Store®.
Allow New Resolvers to be registered	Check to allow new resolvers to be added. Clear this checkbox to prevent the addition of new resolvers unless an administrator re-enables this setting.

2. Clear or change the Bluetooth Device Name Prefix if you use the BD-Address, Terminal Name, or Custom advertising names.

The iTMC application can show the Bluetooth beacons it is receiving.

3. Click Menu in the upper-right corner of the iTMC menu bar.

   The Main Menu appears.

4. Click View Bluetooth Beacons to see the Bluetooth beacons.

Figure 830 - Bluetooth Beacons in iTMC Application

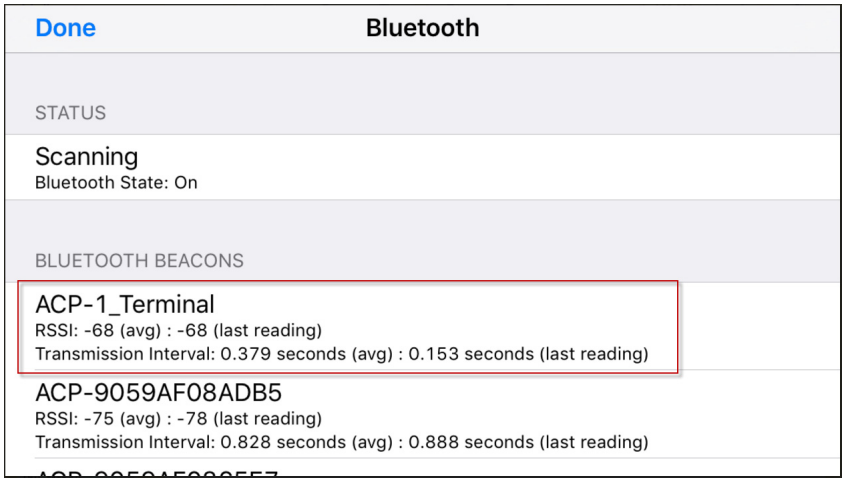


Figure 830 on page 579 shows a beacon using the ACP-{Terminal Name} advertising name.

iPhone Beacon

To use your iPhone as a beacon, follow these steps.

1. Choose Manage>Relevance>Settings.

   The Relevance Settings dialog box appears.
2. Check Enable iPhone Beacons.
3. Launch the ThinManager Beacon app on your iPhone.

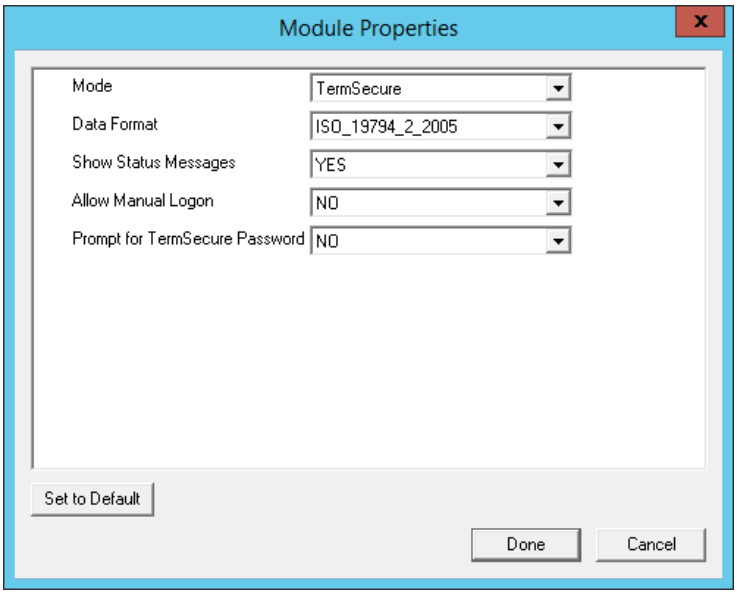
   The ThinManager Beacon app is available at the App Store. Once the app is turned on, the iPhone can be used as a beacon.

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 417 for more details.

Figure 831 - DigitalPersona UareU Fingerprint Reader Module



The DigitalPersona UareU Module has several settings.

Setting	Description
Mode	Allows you to use the reader with TermSecure, TermMon ActiveX, or as a TermMon Lookup device.
Data Format	Allows you to choose the data format used by the biometric reader.
Show Status Messages	Displays activity messages in the upper-right corner of the Terminal.
Allow Manual Logon	Can be set to No to require access only through the biometric device.
Prompt for TermSecure Password	Set to Yes to require a password in addition to fingerprint scan.

RF Ideas pcProx Modules

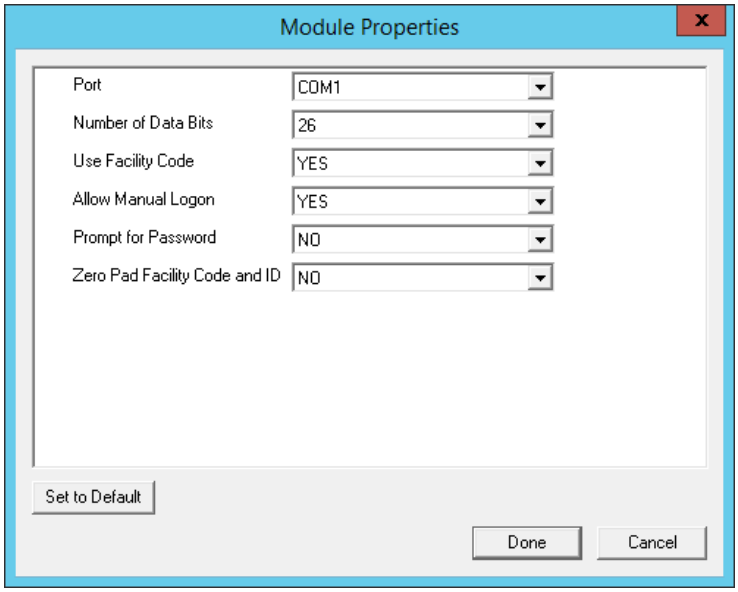
On the Biometric Device Configuration page of the ThinManager Server Configuration Wizard, check Support Finger Print Readers to use a fingerprint scanner. Set the data format here, as well.

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.

Serial RF Ideas pcProx Module

This module is used with the RFIdeas pcProx Enroll Series 81 readers like RDR-xx81AKx.

Figure 832 - RF Ideas pcProx Module Parameters



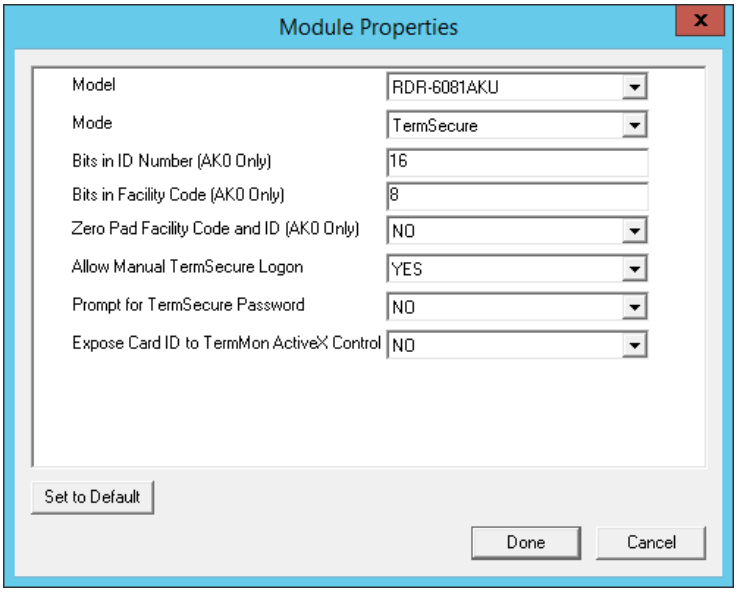
These are the parameters.

Parameter	Description
Port	Choose the port on which the RF Ideas pcProx card reader is installed.
Number of Data Bits	As 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	Set to Yes to require the addition of the card's Facility Code to the Card/Badge ID number.
Allow Manual Login	• Yes allows a ThinManager user to log in to a Terminal without a TermSecure ID device. • No requires TermSecure users to use a TermSecure ID device to log in.
Prompt for Password	Set to Yes to require a TermSecure user to enter their password for access even if the password is configured in ThinManager.
Zero Pad Facility Code and ID	Adds a zero to the number string. This is rarely needed.

USB RF Ideas pcProx USB Module

This module is used with the RDR-6081AKU, RDR-80582AK0, and RDR-80082AK0 USB RFIdeas pcProx readers.

Figure 833 - RF Ideas pcProx USB Module



These are the RF Ideas USB pcProx Module parameters.

Parameter	Description
Model	Allows you to choose between the RDR-6081AKU, RDR-80582AK0, and RDR-80082AK0 USB pcProx card reader.
Mode	• TermSecure Mode allows the card to be used with TermSecure as a login device • Wedge Mode allows the data to be sent to the session as a character string • TermMon Mode allows the data to be sent to the TermMon ActiveX
Bits in ID Number (AK0 Only)	As 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)	As 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)	Adds a leading 0 to the Facility Code if needed.
Allow Manual TermSecure Login	• Yes allows a ThinManager user to log in to a Terminal without a TermSecure ID device. • No requires TermSecure users to use a TermSecure ID device to log in.
Prompt for TermSecure Password	Set to Yes to require a TermSecure user 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 ThinManager User identifier.

To configure a parameter, follow these steps.

1. Highlight the parameter.
2. Change the value.
3. Click Set to apply the new value.
4. Click Done to accept the changes.

Once the Terminal has the module added, it needs to be restarted for the changes to take effect.

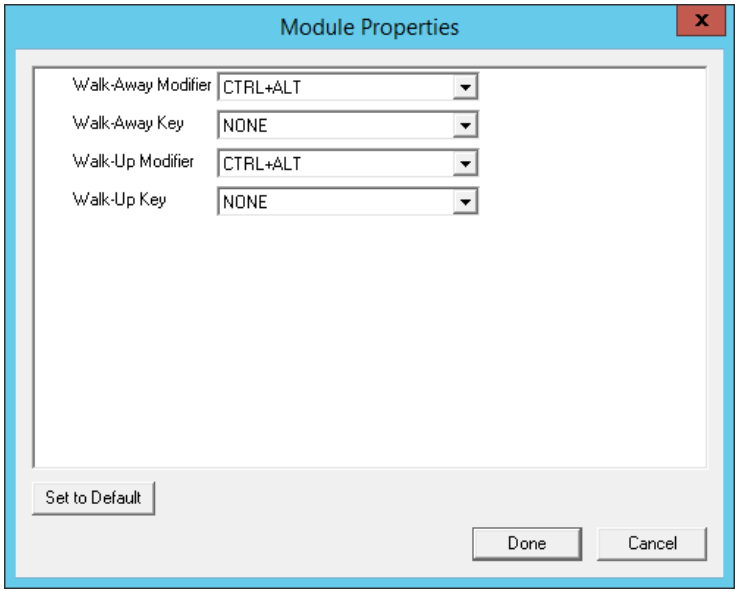
5. Click Finish to close the Terminal Configuration Wizard.
6. Right-click on the Terminal in the ThinManager tree and choose Restart.

RFIdeas pcProx Sonar Module

RF Ideas has a sonar device that can be a pointer to the operator. It becomes active when a ThinManager User logs on and measures the time for a sonar

echo. If the user walks away without logging off, the sonar detects the absence because of the increase in the time interval of the echo.

Figure 834 - RFIdeas pcProx Sonar Module



Parameter	Description
Walk-Away Modifier	Allow you to use a key combination to trigger to turn off the sonar.
Walk-Away Key	
Walk-Up Modifier	Allow you to use a key combination to turn on the sonar.
Walk-Up Key	

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.

Parameter	Description
Allow ActiveX Connections	• Yes allows the ActiveX control to function. • No prevents any ActiveX communication to the Terminal, which includes the default Remote Desktop Server to Terminal access.
Only Allow Connections from Session	• Yes allows other Remote Desktop Server sessions and PCs to communicate to the Terminal with the ActiveX functions. • No restricts communication to that between the Terminal and a session on the Remote Desktop Server belonging to the Terminal, provided that Allow ActiveX Connections is set to Yes.

See Registering the Control on page 731 of the ThinManager for Relevance 11.2 User Manual for details.

USB Flash Drive Module

The USB Flash Drive Module can be used to allow USB flash drives to be used as TermSecure ID devices.

See Figure on page 559 in Local Storage Modules for details.

Wavetrend Tag Reader (Package 5 Only)

The Wavetrend Tag Reader Module allows a Terminal to use Wavetrend RFID cards as TermSecure ID cards. This logs in a user through TermSecure when they approach the Terminal and logs them out when they leave the area. The distance required to log in and log out isconfigurable in the module.

These are the parameters.

Parameter	Description
Port	Specifies which COM Port the reader is attached to as the WaveTrend Tag Reader Module connects to a thin client through the serial port.
Use Vendor Code	When set to YES, the vendor code is included as part of the identifier number.
Allow Manual Login	• YES allows a ThinManager User to use the hotkey to initiate logins, or the device. • NO forces a ThinManager User to use a device to login.
Prompt for Password	• NO allows the device to login without a password. • YES forces every ThinManager 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 required to register as “Entered.”
Exit Sensitivity	The number of reads below the Exit Signal Strength required to register as “Exited.”

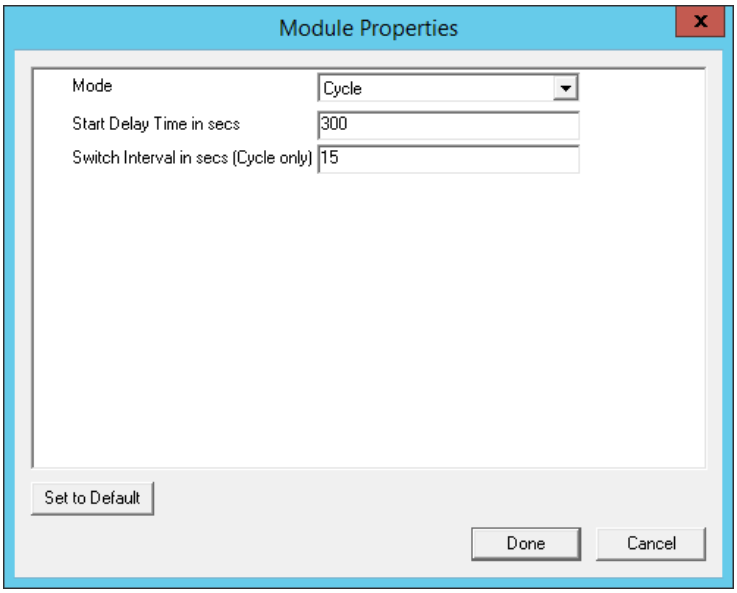
Screen Saver Modules

The use of ThinManager Screen Savers is recommended 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.

MultiSession Screen Saver Module

The MultiSession Screen Saver Module is a screen saver that allows the different sessions of a MultiSession client to cycle.

Figure 835 - 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.

These are the parameters.

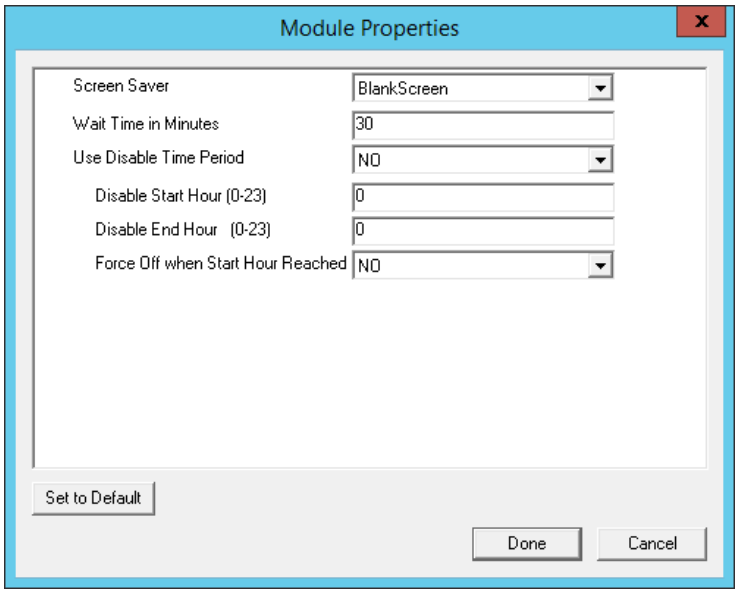
Parameter	Description
Mode	• Cycle switches between all active sessions on the Terminal. • GotoFirstGroup switches the Terminal to the main session when it is inactive.
Start Delay Time in secs	The number of seconds of inactivity that the Terminal allows before the screen saver starts.
Switch Interval in secs (Cycle mode only)	The number of seconds the Terminal displays each session when using the Cycle mode.

Screen Saver Module

Screen Saver Module loads a screen saver on the client. The screen saver runs 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 disables the screen saver during working hours so that the screen is visible during those hours.

Figure 836 - Screen Saver Module



The Screen Saver Module configuration includes these parameters.

Parameter	Description
Screen Saver	The graphic displayed when the screen saver is active.
Wait Time in Minutes	The length of time that the Terminal must 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 can be used to prevent the screen saver from running during normal business hours.
Disable Start Time (0-23)	Sets the start of the disabled time block. 0 is Midnight and 23 is 11:00 p.m.
Disable End Time (0-23)	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	Set to Yes to turn the screen saver off when the Disable End Time is reached.

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.

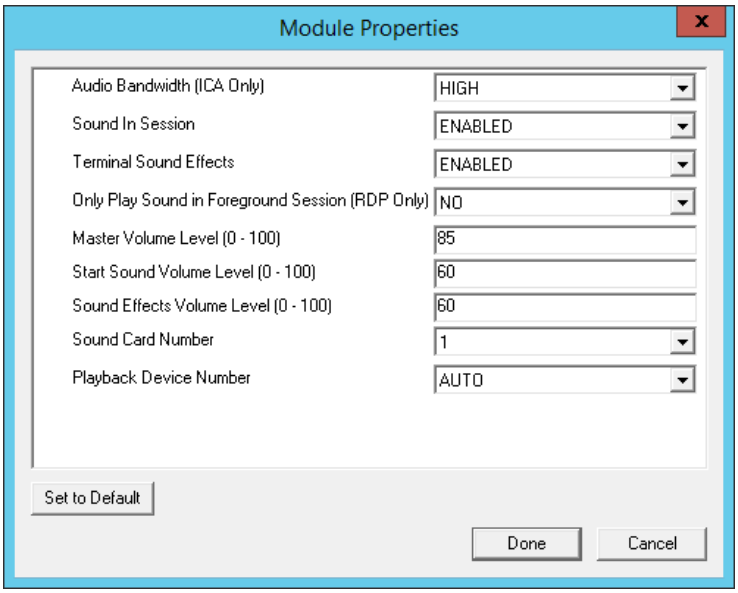
- Hardware with a Line Out/Speaker plug
- Amplified speaker(s)
- Universal Sound Driver Module

1. Plug the speaker(s) into the Line Out plug on the Terminal.
2. Add the module.
3. Connect to the Remote Desktop Server.

Universal Sound Driver

The Universal Sound Driver Module activates 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.

Figure 837 - Universal Sound Driver Properties



The Universal Sound Module has several settings.

Setting	Description
Audio Bandwidth (ICA Only)	Set to Low, Medium, or High bandwidth when using Citrix ICA.
Sound in Session	• Enabled allows sound generated within the session to be played through the Terminal. • Disabled turns off the session sounds, but system sounds are generated during TermSecure login for audio feedback during the login process.
Terminal Sound Effects	Set to Enabled to allow Terminal sound effects like TermSecure login sounds on the Terminal.
Only Play sound in Foreground Session	Turns off the sound in background sessions when using MultiSession.
Master Volume Level (0-100)	Sets the master volume for the Terminal.
Start Sound Volume Level (0-100)	Sets the master volume for the Terminal.
Sound Effects Volume Level (0-100)	Sets the level for sound effects on the Terminal.
Sound Card Number	Lets you specify which sound card to use if you have multiple sound cards.
Playback Device Number	Lets you choose the playback device output of the sound card.

TermSecure Modules

There is a legacy category for TermSecure that was superseded by the Relevance category.

The modules in the TermSecure list are identical to the modules in the Relevance list. See Relevance Modules on page 576.

These are the modules.

- 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)

Touch Screen

ThinManager supports over a dozen serial touch screen controllers and a universal USB driver. You must add the proper driver for the controller. Some manufacturers are not consistent and use different controllers for different product lines.

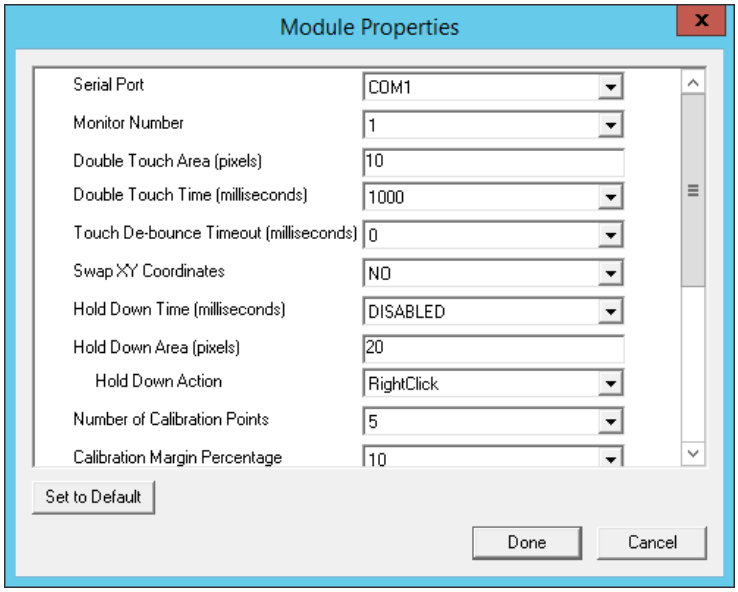
Serial Drivers

Each serial touch screen has a specific touch driver based on the touch controller of the monitor. You must add the appropriate driver that matches the touch controller.

- 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

The touch controller is the important component. Many manufacturers make touch screen monitors, but fewer make the controller. You need the module that matches the controller.

Figure 838 - Serial Touch Screen Driver



Some, but not all, touch screen modules have parameters that can be modified, which may include these.

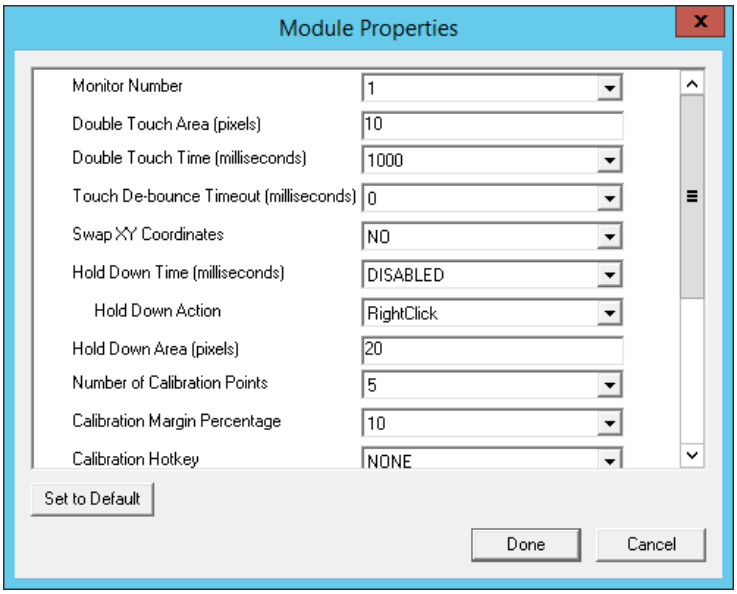
Parameter	Description
Connection	
Serial Port	Sets the COM port that a serial touch screen is connected to.
Baud Rate	Sets the speed used for communication between the Terminal and the touch screen on some serial touch screens.
Monitor Number	Used to specify which monitor in a MultiMonitor scheme uses for the touch screen. MultiMonitor thin clients with multiple touch screens need a module loaded for each touch screen used.
Touch Settings	
Double Touch Area (pixels)	Sets the size of the area that a second touch registers as a double-touch.
Double Touch Time (milliseconds)	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 corrects the orientation.
Hold Down Time (milliseconds)	When enabled, initiates the Hold Down Action when the touch is held for the configured time
Hold Down Action	Sets the action that a long touch initiates, includes Right-Click and OnBoard Keyboard.
Hold Down Area (pixels)	Sets the size of the area that a second touch registers as a right-click.
Calibration	
Number of Calibration Point	Sets the number of calibration points that the calibration program uses during the calibration process.
Calibration Margin Percentage	Sets the distance from the edge of the screen at which calibration points are displayed.
Calibration Hotkey	Allows a function key to be set as a hotkey so that the calibration can be launched from a keyboard.
Calibration Hotkey Modifier	Adds CTRL or ALT to the hotkey to launch the calibration from the keyboard, if desired.
Calibration Hold Down Time (seconds)	When enabled, launches the calibration program when the screen is touched and held for the assigned number of seconds. Cannot be used with the Right-Click Hold Time.
Clean Time	Sets an idle time before the calibration to allow you to clean and wash a touch screen. The calibration waits until you are done touching the screen while cleaning.
Calibration (entered automatically)	Set automatically by machine. These are the values set during the calibration process.

Parameter	Description
Miscellaneous	
Hide Mouse Cursor	Hides the mouse cursor if a mouse is not present.
Orientation (entered automatically)	Set automatically by machine. Used at the direction of Tech Support in error correction.

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.

Figure 839 - USB Touch Screen Module



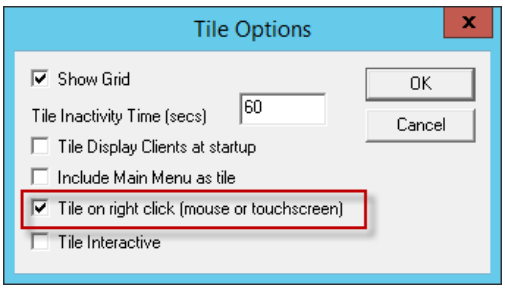
Some, but not all, touch screen modules have parameters that can be modified, including these.

Parameter	Description
Connection	
Monitor Number	Used to specify which monitor in a MultiMonitor scheme uses for the touch screen. MultiMonitor thin clients with multiple touch screens need a module loaded for each touch screen used.
Touch Settings	
Double Touch Area (pixels)	Sets the size of the area that a second touch registers as a double-touch.
Double Touch Time (milliseconds)	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 corrects the orientation.
Hold Down Time (milliseconds)	When enabled, initiates the Hold Down Action when the touch is held for the configured time.
Hold Down Action	Sets the action that a long touch initiates, includes Right-Click and OnBoard Keyboard.
Hold Down Area (pixels)	Sets the size of the area that a second touch registers as a right-click.
Calibration	
Number of Calibration Point	Sets the number of calibration points that the calibration program uses during the calibration process.
Calibration Margin Percentage	Sets the distance from the edge of the screen at which calibration points are displayed.

Parameter	Description
Calibration Hotkey	Allows a function key to be set as a hotkey so that the calibration can be launched from a keyboard.
Calibration Hotkey Modifier	Adds CTRL or ALT to the hotkey to launch the calibration from the keyboard, if desired.
Calibration Hold Down Time (seconds)	When enabled, launches the calibration program when the screen is touched and held for the assigned number of seconds. Cannot be used with the Right-Click Hold Time.
Clean Time	Sets an idle time before the calibration to allow you to clean and wash a touch screen. The calibration waits until you are done touching the screen while cleaning.
Calibration (entered automatically)	Set automatically by machine. These are the values set during the calibration process.
Miscellaneous	
Hide Mouse Cursor	Hides the mouse cursor if a mouse is not present.
Orientation (entered automatically)	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. Check Tile on right click setting, in the Tile Options dialog box, to allow a user to switch screens on a touch screen without a keyboard or mouse.

Figure 840 - Tile Options



The Tile Options dialog box appears when Tiling Options is clicked on the Terminal Interface Options page of the Terminal Configuration Wizard.

USB MultiTouch Screen Driver

The USB MultiTouch Screen Driver is an Advanced Module. Therefore, it is only available when the Show Advanced Modules checkbox is selected. Additionally, the USB MultiTouch Screen Driver requires the FreeRDP Module, which is also an Advanced Module.

Currently, MultiTouch calibration is not available; so, this driver initially only works with touch screens that support absolute coordinates.

It should also be noted that the USB MultiTouch Screen Driver only works with RDS Display Clients. Therefore, the application delivered within the RDS Session must support MultiTouch (i.e., MultiTouch Screen Driver is not currently supported with Container Host Display Clients.

Video Driver Modules

The method of downloading video drivers was changed in ThinManager 3.0. In previous versions, all video drivers were contained in the firmware and were downloaded at boot. In ThinManager 3.0, the video was split out of the firmware and each thin client only downloads the video driver that it needs.

One does not need to add the video module to the Terminal, but must only have the video module installed in ThinManager to make it available. As each Terminal connects to ThinManager, it downloads the correct module.

These modules are normally installed with ThinManager.

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 nontraditional 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.

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.

Parameter	Description
Monitor 1 Connection Type	Allows you to choose the connection type of your first monitor.
Monitor 2 Connection Type	Allows you to choose the connection type of your second monitor.
Monitor 3 Connection Type	Allows you to choose the connection type of your thirde monitor.
Monitor 4 Connection Type	Allows you to choose the connection type of your fourth monitor.
Monitor 5 Connection Type	Allows you to choose the connection type of your fifth monitor.
Enable TwinView for nVidia Adapters	Enables TwinView.

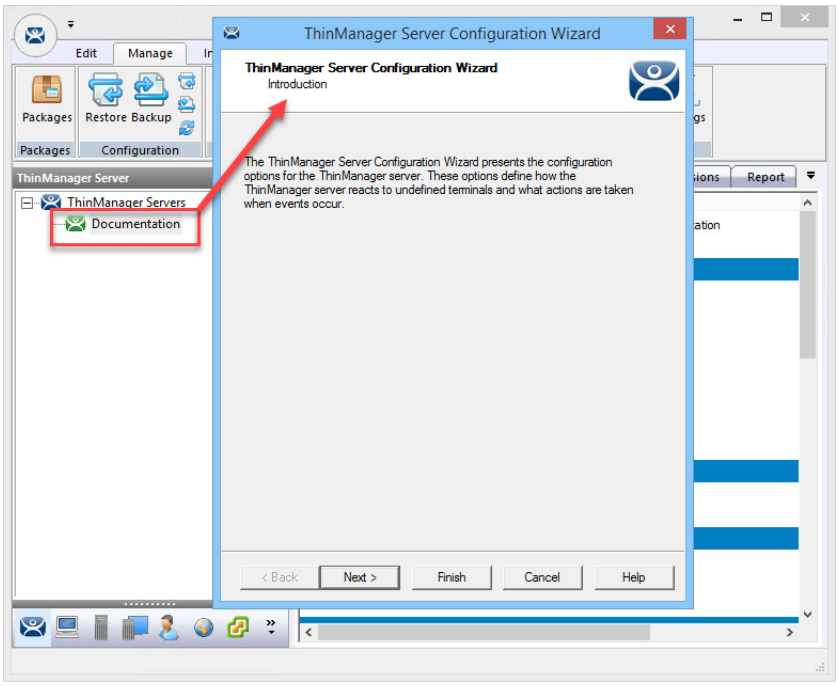
ThinManager Server Configuration Wizard

The ThinManager Server Configuration Wizard allows the configuration of global ThinManager settings. It can be launched one of these ways.

- Choose Edit>Modify while the ThinMan icon is highlighted in the ThinManager tree
- Double-click on the ThinManager icon in the ThinManager tree
- Right-click the ThinMan icon and choose Modify

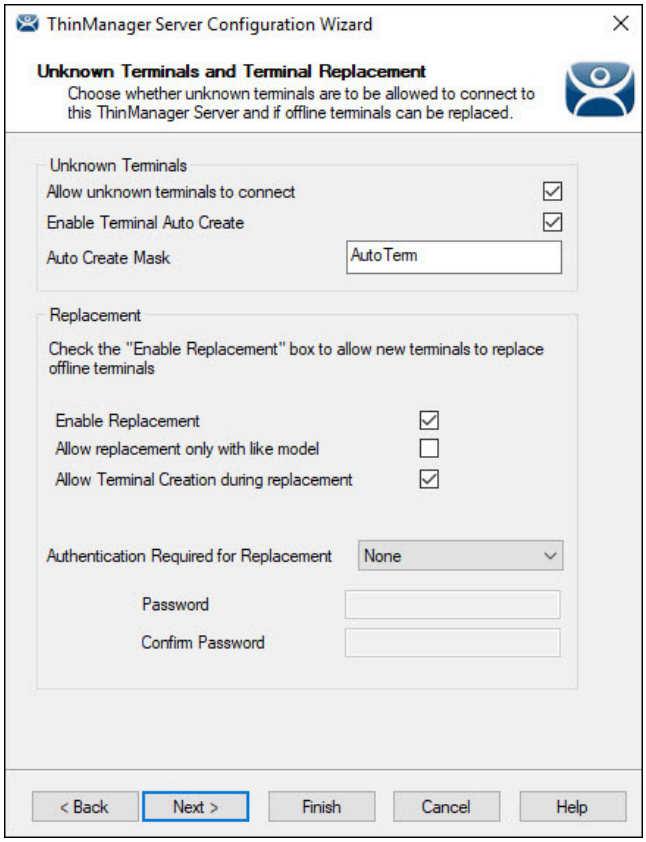
Introduction Page

Figure 841 - ThinManager Server Configuration Wizard



Unknown Terminals and Terminal Replacement Page

Figure 842 - Unknown Terminals and Terminal Replacement



1. Complete the Unknown Terminals and Terminal Replacement page per the following descriptions.

Setting	Description
Unknown Terminals	
Allow unknown terminals to connect	Allows the addition of new Terminals to the ThinManager Server. Clear this checkbox to prevent replacements and new Terminals.
Enable Terminal Auto Create	Allows the auto-creation of an array of terminals as described in Auto-Creation of Terminals.
Auto Create Mask	The base name used in the array of terminals when using Auto-Creation of Terminals.
Replacement	
Enable Replacement	Allows the newly booted terminals to replace an existing entry in ThinManager.
Allow replacement only with like model	Allows the newly booted terminal to replace an existing terminal only if the new and previous hardware models are the same.
Allow Terminal Creation during replacement	Allows user to create a new terminals and configuration upon booting.
Authentication Required for Replacement	Controls replacement authorization.
None	Allows a Terminal to be added without authentication.
ThinManager Password	Allows you to set a password so that only authorized personnel can add Terminals to the ThinManager Server. Check to enable the password fields and allow the addition of a password.
Windows Account	Requires that the replacer enter their Windows account on the Terminal as it is being replaced. ThinManager checks and allows the replacement if the replacer is a member of a Windows Security Group that has the Allow Terminal Replacement task granted.
Password	These are the fields to enter a password needed to allow replacement if ThinManager Password is selected from the Authentication Required for Replacement pull-down menu.
Confirm Password	

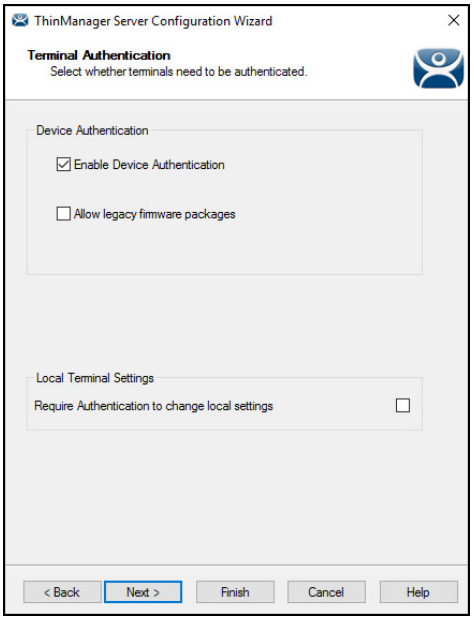
These terminal settings allow greater security when thin clients are added or replaced. Require a password to control who adds Terminals. Use auto-creation to help with some large deployments.

2. Click Next to continue, Finish to save and close, or Cancel to close and not save.

   The Terminal Authentication page appears, which sets device authentication when a terminal boots and configures whether a user can change local terminal settings.

Terminal Authentication Page

Figure 843 - Terminal Authentication



Complete the Terminal Authentication page per the following descriptions.

Setting	Description
Device Authentication	
Enable Device Authentication	When enabled (recommended), it requires Device Authentication for all terminals. No further configuration is required. Clear this setting to not require device authentication for any terminal.
Allow legacy firmware packages	Allows the user to bypass Device Authentication for unsupported versions of firmware. Leave this option's checkbox clear (recommended).
Local Terminal Settings	
Require Authentication to change local Settings	When enabled, authentication is required in order to change local terminal settings.

Device Authentication

Device Authentication is another step in the boot process that requires firmware versions 13.2.0 or later. It helps prevent MAC address spoofing when terminals boot, as well as prevents a terminal profile with potentially sensitive data from being used on an unauthorized terminal.

It identifies the terminal by using one of the following methods:

- A windows-based username and password with the Allow Terminal Replacement permission listed in the ThinManager Security Group
- A generated key pair on the device's Trusted Platform Module (TPM) chip

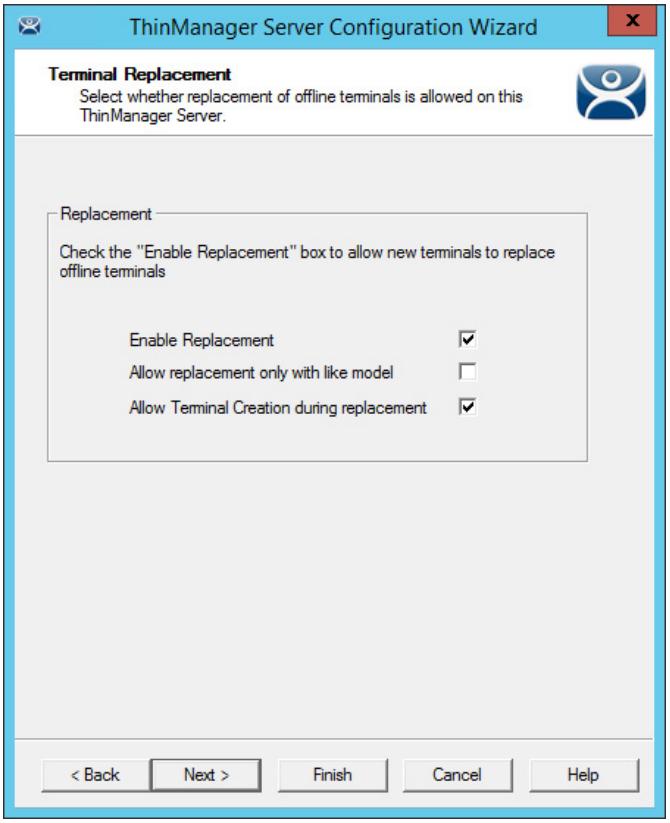
The first time a terminal connects, the user is prompted to provide valid Windows user credentials. If authentication fails, the terminal does not boot. If authentication succeeds, the process continues depending on whether the terminal has a TPM chip.

For terminals with a TPM chip, a key is generated by the TPM of the device. The terminal returns the public key, which is what the ThinManager server uses to identify the device to the ThinManager server.

For terminals that do not have a TPM chip onboard, the user is prompted for a username and password every time that device boots.

Terminal Replacement Page

Figure 844 - Terminal Replacement



Terminals that are turned on cannot be replaced until they are turned off.

1. Complete the Terminal Replacement page per these descriptions.

Setting	Description
Enable Replacement	Gives global permission for Terminals to be replaced. Clear this checkbox to prevent the appearance of all Terminals in the replacement list when a new Terminal is added, which makes Create New Terminal the only option. Also, this feature is available for the Group and Terminal level on the first page of the wizard. However, if this checkbox is cleared in the ThinManager Server Configuration Wizard, it has no effect in a Terminal Configuration Wizard when it is checked.
Allow replacement only with like model	Prevents the replacement of a Terminal with a different model to prevent configuration changes. For example, only a PXE can replace a PXE, or only an Android can replace an Android.
Allow Terminal Creation during replacement	Normally, a Terminal displays the Create New Terminal option during replacement. Clear this checkbox to remove that option and only allow a Terminal replacement, not a new configuration.

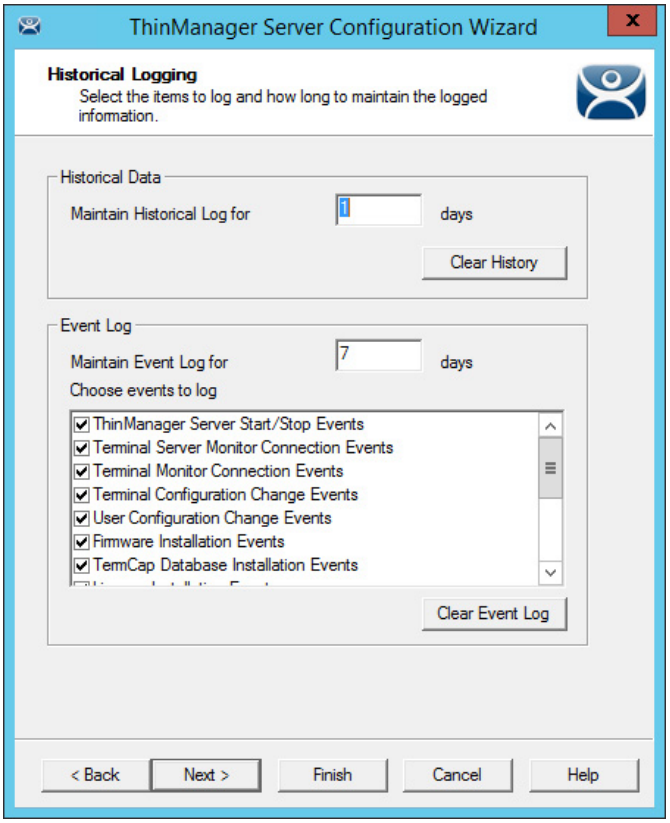
Clear the checkbox to prevent the appearance of all Terminals in the replacement list when a new Terminal is added, which makes Create New Terminal the only option.

2. Click Next to continue, Finish to save and close, or Cancel to close and not save.

   The Historical Logging page appears, which adjusts the Historical Data setting to determine the length of time logs are maintained.

Historical Logging Page

Figure 845 - Historical Logging



1. Complete the Historical Logging page per these descriptions.

Setting	Description
Maintain Historical Log for X days	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	Determines how long the event log is kept.
Choose events to log	Determines which events are stored in the log.
Buttons	
Clear History	Erases the Historical log.
Clear Event Log	Erases the Event log.

By default, Remote Desktop Server events and ThinManager User events are not collected. Add these as well as other event logs to use as a tool when troubleshooting.

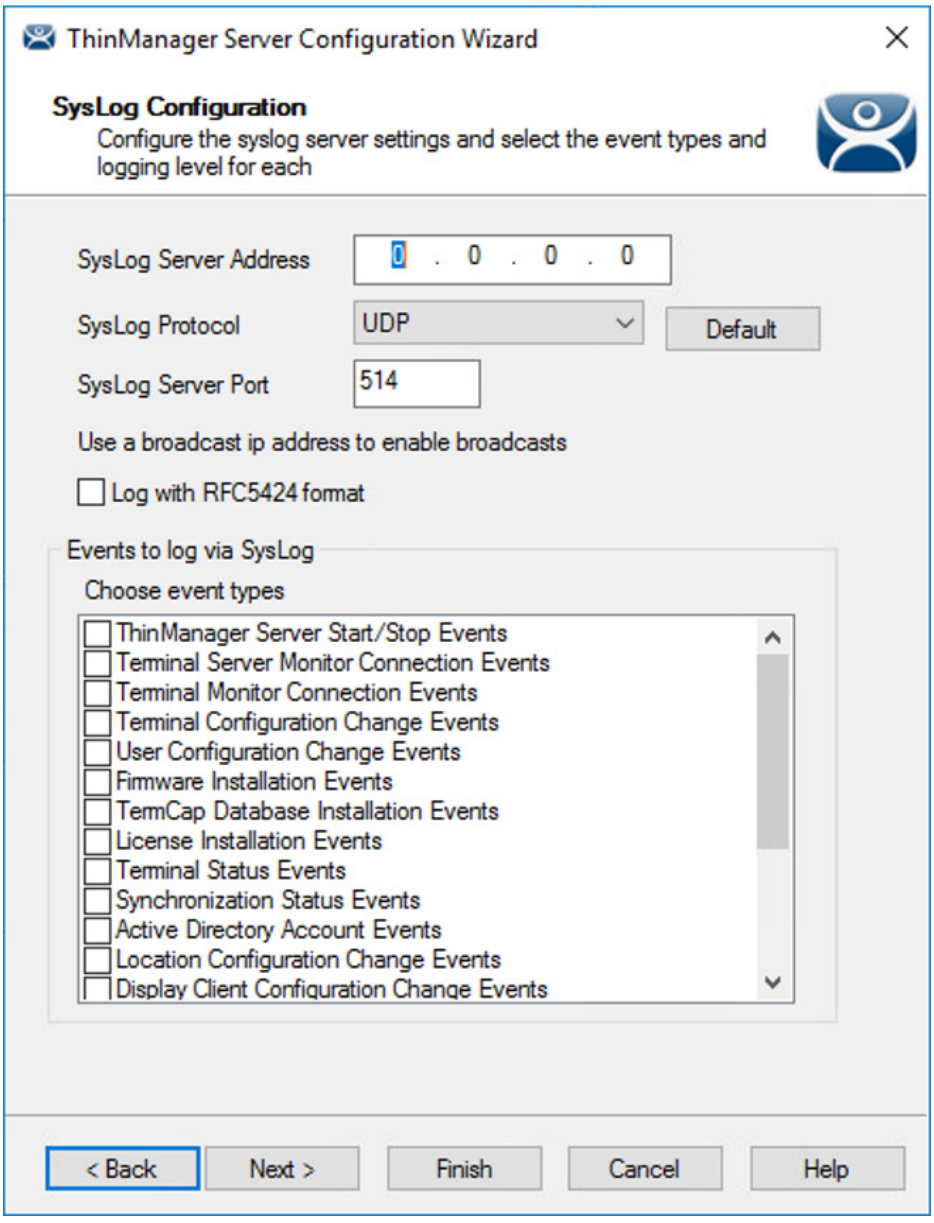
2. Click the Event Log tab to show the events for the highlighted tree icon.

SysLog Configuration Page

ThinManager Events, which were previously only found within the ThinManager interface's Event Logging tab, can now be viewed in SysLog Servers when using SysLog Compatible Reporting. For example, you can log events to the Application log of Windows Event Viewer and view the logs there that have a source of ThinServer. This allows users to view ThinManager events sorted among other Windows logging events.

The SysLog Configuration option is in the ThinManager Server Configuration Wizard.

Figure 846 - SysLog Configuration

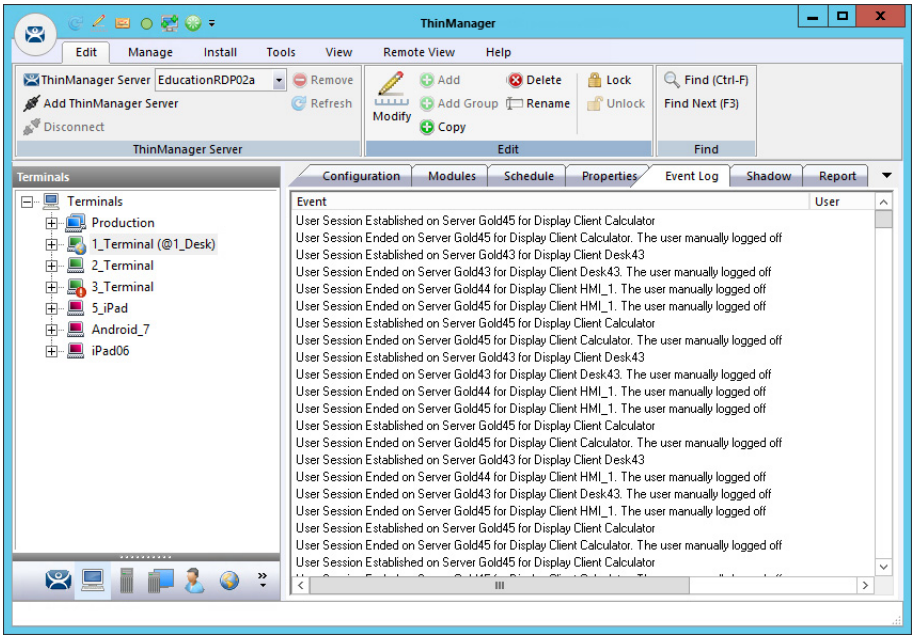


Setting	Description
SysLog Server Address	Enter the designated SysLog Server IP Address.
SysLog Protocol	From the pull-down menu, choose the appropriate SysLog protocol used. The options are TCP, TLS encrypted TCP, and UDP.
Default	Click to automatically populate the SysLog Server Port field with the standard port per the selected protocol.

Setting	Description
SysLog Server Port	If the SysLog Server Port deviates from the standard, it may be manually entered here. Otherwise, click Default after choosing the SysLog Protocol to automatically populate the standard port.
Log with RFC424 format	Check to send data to SysLog in RFC5424 format. Clear to send in the previously supported format.
Choose event type	By default, events are not configured for SysLog. Therefore, you must choose which events are to appear in SysLog.

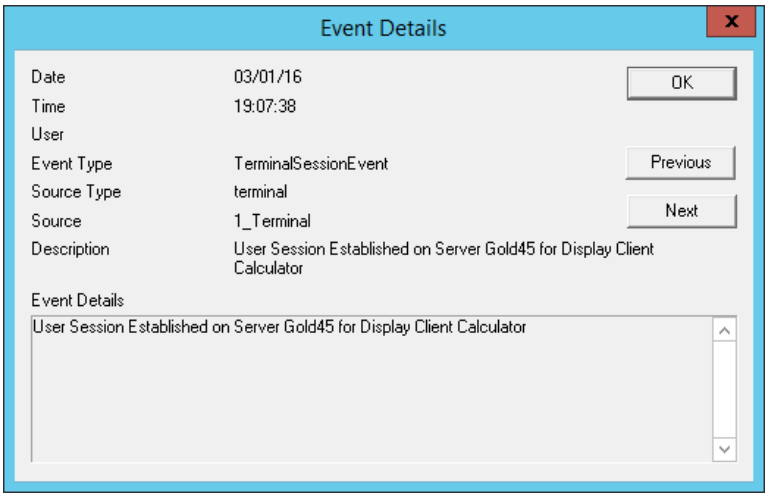
Event Log Tab

Figure 847 - Event Log Tab



3. Double-click on an event to view its details in the Event Details dialog box.

Figure 848 - Event Details

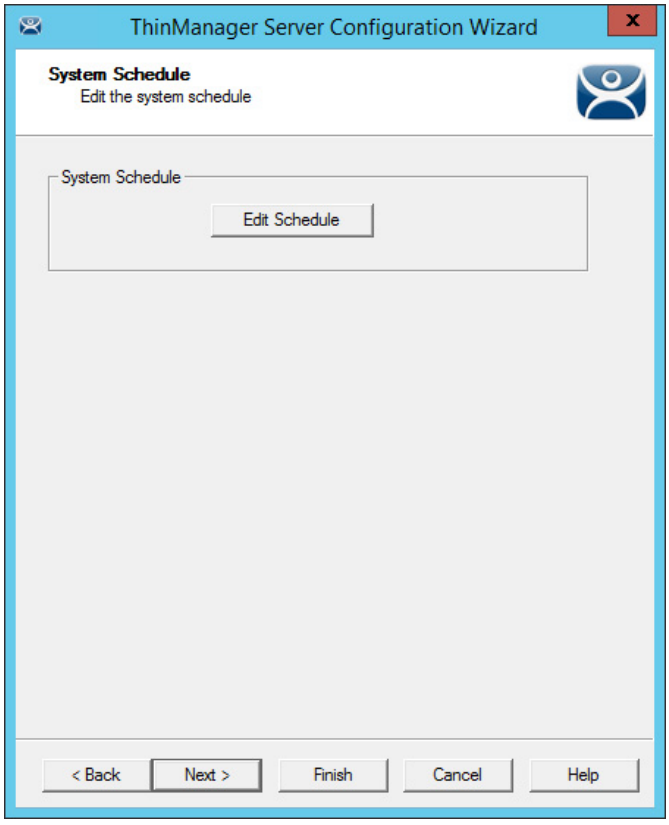


4. Click OK or Cancel to close.
5. Click Next to continue, Finish to save and close, or Cancel to close and not save.

   The System Schedule page appears, allows schedules to be setup for ThinManager and the ThinManager system.

System Schedule Page

Figure 849 - System Schedule



1. Click Edit Schedule to create a System Schedule to automate backups, reports, and actions. This serves as a great troubleshooting tool, also.

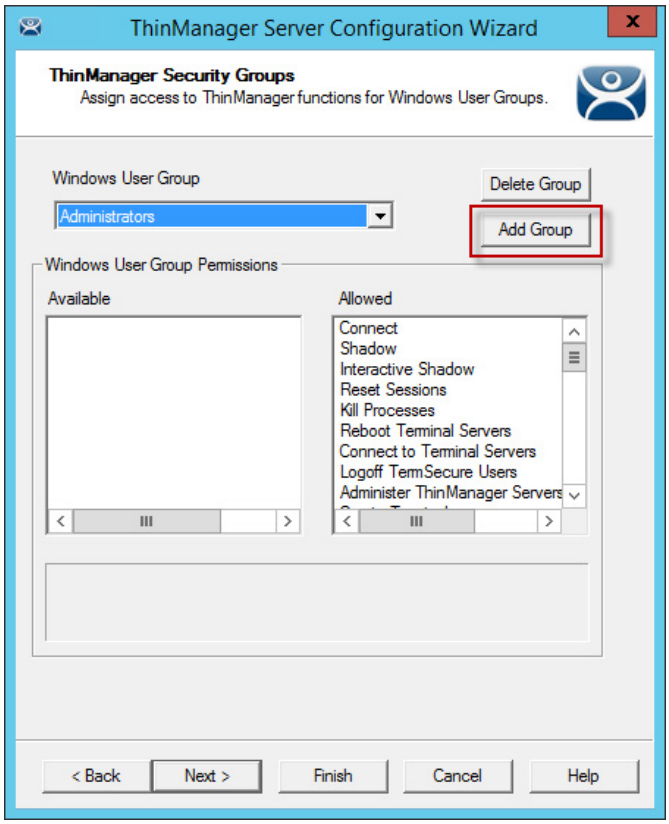
Button	Description
Edit Schedule	Launches the Event Schedule dialog box. See Scheduling on page 643 for details.

2. Click Next to continue, Finish to save and close, or Cancel to close and not save.

   The ThinManager Security Groups page appears, where access to ThinManager can be assigned to Windows User Groups. 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.

Security Groups Page

Figure 850 - ThinManager Security Groups



Setting	Description
Windows User Group	Shows the group that is being configured.
Field	
Available	Shows the ThinManager functions that are available to the Windows group displayed in the Windows User Group dialog box. Double-click these functions to add them to the Allowed list.
Allowed	Shows the ThinManager functions that are granted to the Windows group displayed in the Windows User Group dialog box. Double-click these functions to remove them from the Allowed list.
Button	
Delete Group	Removes the highlighted group in the Windows User Group dialog box.
Add Group	Launches the New Window Group dialog box where a new Windows group can be added to the configuration.

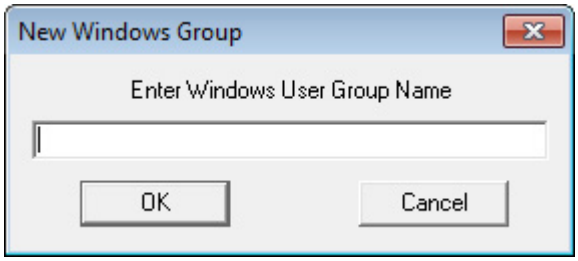
ThinManager allows different levels of access and functionality based on standard Windows groups. By default, only members of the Windows Administrator group have the ability to connect to ThinManager and use the application. The ThinManager Security Groups allows other Windows groups to be granted privileges in ThinManager.

ThinManager comes with privileges predefined for six groups. Each of these groups (except Administrators) must be created on the domain controller or in the Local Users and Groups on the Computer Management console. Members must be added before they can be used.

Windows User Group	Description
Administrators	The Microsoft-defined Administrators group is given all privileges by default in ThinManager. Double-click a Windows User Group Permission to move it from the Allowed list to the Available list and deny particular permissions.
ThinManager Administrators	Provides full permission to do anything within ThinManager. This includes the power to log off 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 cannot be removed from the Allowed list and are dimmed.
ThinManager Interactive Shadow Users	Members of this group can interactively shadow a Terminal.
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 they cannot interact with the session.
ThinManager Shadow Users	Members of this group can shadow a Terminal, but not interactively.
ThinManager Users	This is a view-only permission. They cannot log off sessions, kill processes, send messages, restart Terminals, or calibrate touch screens. ThinManager Users cannot shadow a Terminal.

1. Click Add Group in a non-domain ThinManager Server to launch the New Windows Group dialog box, which allows the configuration of additional Windows User Groups.

Figure 851 - New Windows User Group



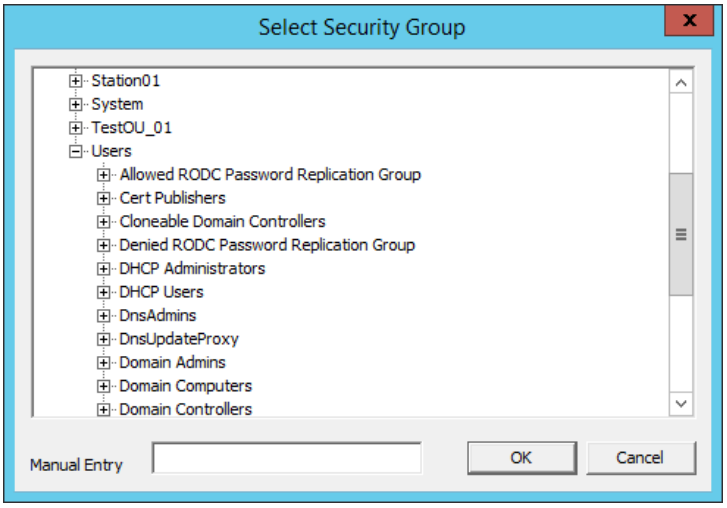
2. Type a Windows Group name in the Enter Windows User Group Name field of the New Windows Group dialog box and click OK to add the Windows User Group to the pull-down menu.

This does not create the user group on any servers, it just adds the name of a group that exists to the list that ThinManager maintains.

3. Click Add Group in a domain ThinManager Server

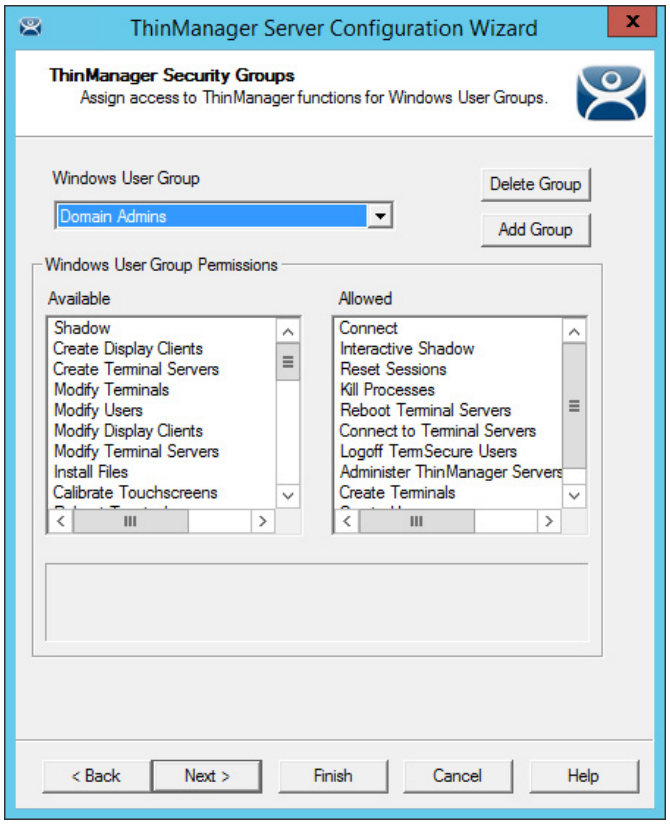
   The Select Security Group dialog box appears, which allows you to add Active Directory groups and configure their permissions in ThinManager.

Figure 852 - New Windows User Group Dialog Box



4. Type a local Windows User Group into the Manual Entry field and click OK.

Figure 853 - ThinManager Security Groups Page



5. On the ThinManager Security Groups page, choose the group from the Windows Users Group pull-down menu.
6. Double-click a function in the Available list of the Windows User Group Permissions section to grant that permission to the group. Members of the Windows User Group have the selected permissions at their next login.

Although ThinManager has Windows User Groups preconfigured with privileges, these groups were not created on the Remote Desktop Servers. These are merely templates for groups that can be created.

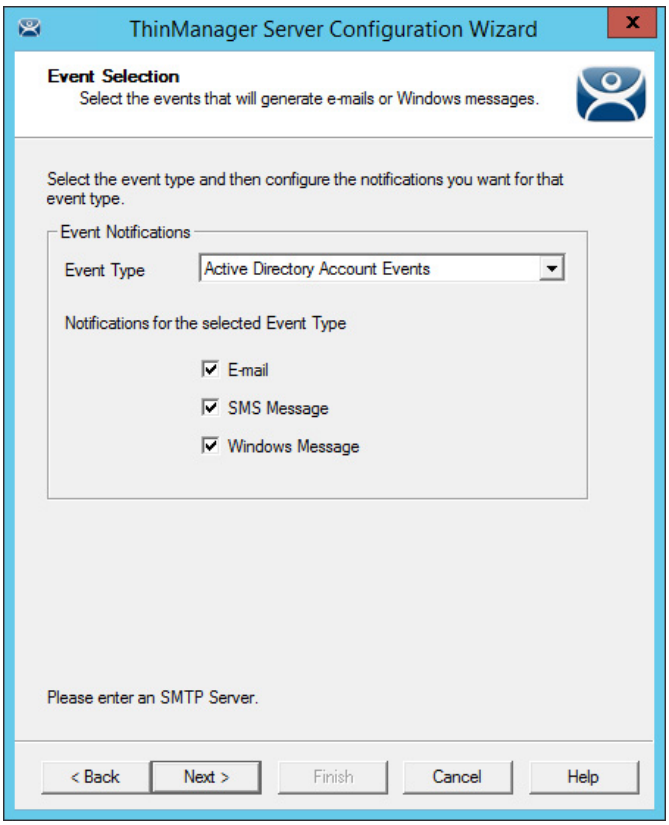
a. If you need a new Windows group, create the Windows User Group using standard Microsoft methods.

The ThinServer service may need to be stopped and restarted to load the new ThinManager Security Group settings.

7. Click Next to continue the ThinManager Server Configuration Wizard, Finish to save and close, or Cancel to close and not save.

Event Selection Page

Figure 854 - Event Selection



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.

These are the settings for Event Selection page.

Windows User Group	Description
Event Type	Lists the events that can trigger a message. Choose the desired event and notification type. You can choose multiple events.
Email	Check to send an e-mail message when that event occurs. The e-mail must be set up on the next page of the wizard.
SMS Message	Check to send an SMS message when that event occurs. The SMS Messaging system must be defined on the next page of the wizard.
Windows Messages	Check to send a message to a Terminal when that event occurs. The Terminal must be defined on the next page of the wizard.

Information about these events can be useful. The event must be checked to add the notification.

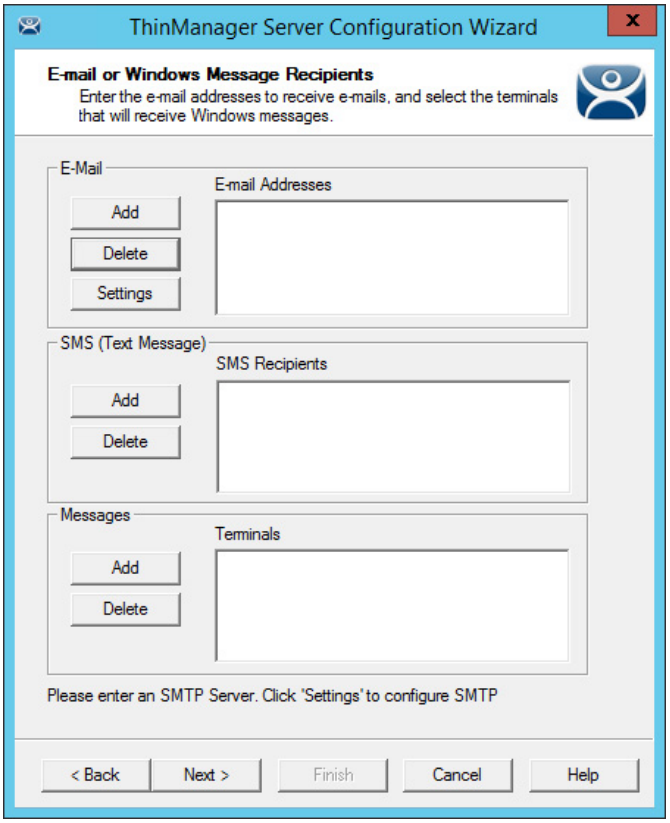
The ThinManager Server Stop/Start, Remote Desktop Server Monitor Connection, and Terminal Monitor Connection events can indicate the failure of the ThinManager Server, Remote Desktop Server, or Terminal.

It can be useful to share information on configuration changes, firmware, TermCap, or license installation when management is shared among a group.

1. Send an e-mail to all group members to keep them informed of all changes.
2. Click Next to continue, Finish to save and close, or Cancel to close and not save.

Email or Windows Messaging Recipients Page

Figure 855 - Email or Windows Messaging Recipients Page

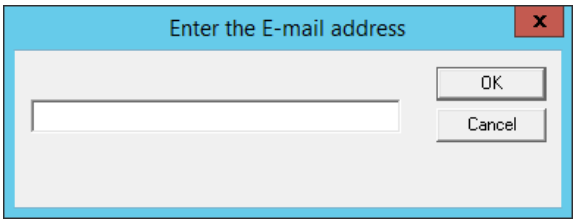


This page defines which users are notified of event changes from the Event Selection page.

Windows User Group	Description
Fields	
E-Mail Addresses	ThinManager sends an e-mail message to the addresses in this text box when an event is chosen on the Event Select page.
SMS Recipients	ThinManager sends an SMS message to the addresses in this text box when an event is chosen on the Event Select page.
Terminals	ThinManager sends a message to the Terminals in this text box when an event is chosen on the Event Select page.
E-mail Buttons	
Add	Click to make the Enter the E-mail address dialog box appear, where you can type an e-mail address.
Delete	Click to delete a highlighted e-mail address from the E-mail Addresses list.
Settings	Click to make the Email Server Settings dialog box appear, where you can configure the e-mail settings in the Email Server Settings dialog box.

Windows User Group	Description
SMS (Text Message)	
Add	Opens the SMS Message Recipient dialog box to add a phone number to the distribution list.
Delete	Deletes a highlighted number from the SMS Recipients list.

Figure 856 - Enter the E-mail Address Window

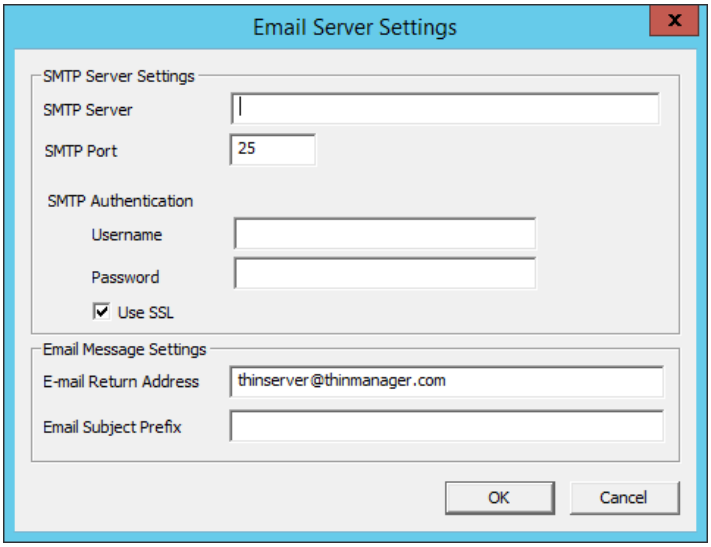


1. Click Add in the E-mail section.

   The Enter the E-mail Address dialog box appears, where you can add an e-mail address to the notification list.
2. Click OK to accept the setting or click Cancel to close the dialog box and not save.
3. Click Settings in the E-mail section of the Email or Windows Message Recipients page.

   The Email Server Settings dialog box appears, which allows you to configure the SMTP mail server.

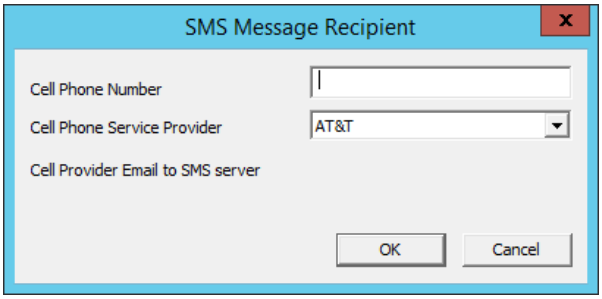
Figure 857 - E-mail Server Settings Window



SMTP Sever Settings	Description
SMTP Server	Type the name of the SMTP Server.
SMTP Port	Type the number of the SMTP Port.
SMTP Authentication	
Username	Type the Username to allow the use of authentication for the connection to the SMTP server.
Password	Type the Password to allow the use of authentication for the connection to the SMTP server.
Use SSL	Check to allow the use of the SSL (Secure Socket Layer) to communicate with the SMTP server.
Email Message Settings	
Email Return Address	Allows you to configure a sender account for replies.
Email Subject Prefix	Allows you to configure a subject line for emails.

4. Click OK to accept the setting or click Cancel to close without saving.

Figure 858 - SMS Message Recipient

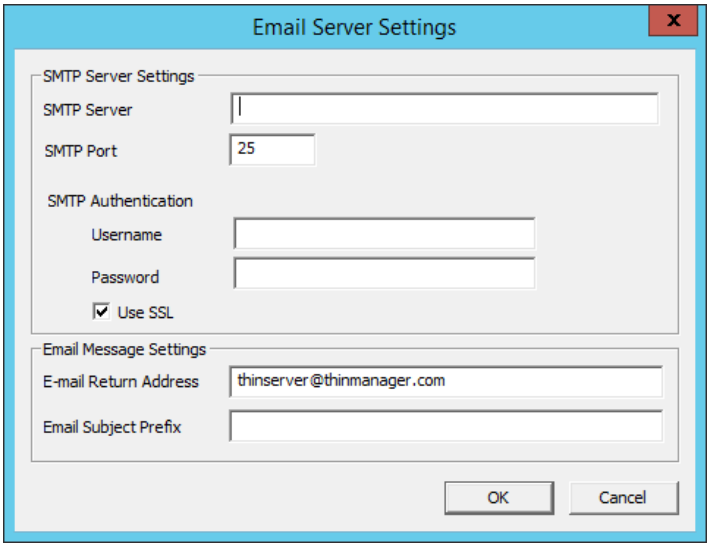


The SMS Message Recipient dialog box allows you to add a phone number to the SMS distribution list.

Setting	Description
Cell Phone Number	Type a phone number.
Cell Phone Service Provider	Allows you to specify what network the cell phone uses. Each service provider uses a unique account; so, the correct account is important.

5. Click OK to accept the setting or Cancel to close without saving.

Figure 859 - Select Terminal

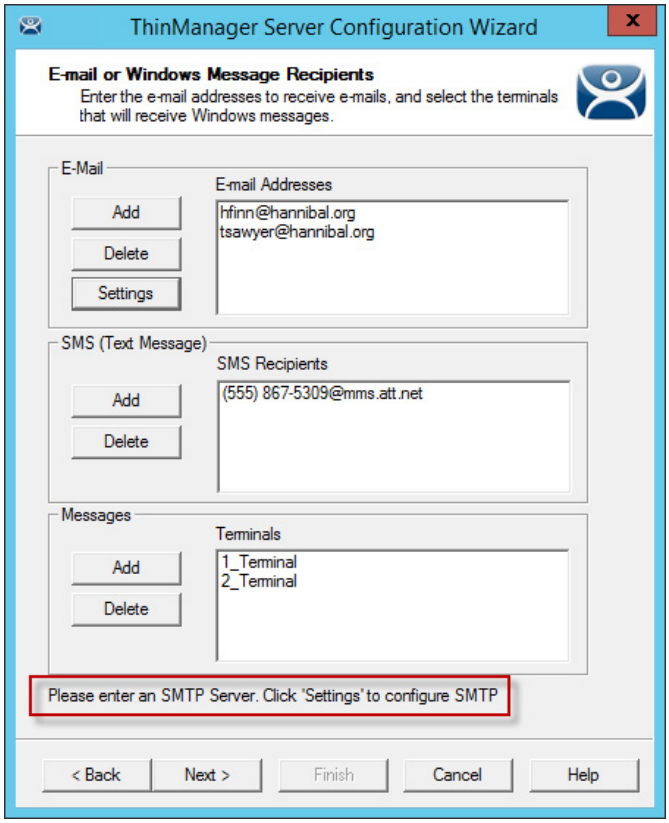


The Select Terminal dialog box lists the Terminals configured on the ThinManager Server.

6. Highlight the desired Terminal and click OK.

Figure 860 shows the Email or Windows Messaging Recipients page populated with different recipients.

Figure 860 - Email or Windows Messaging Recipients Page



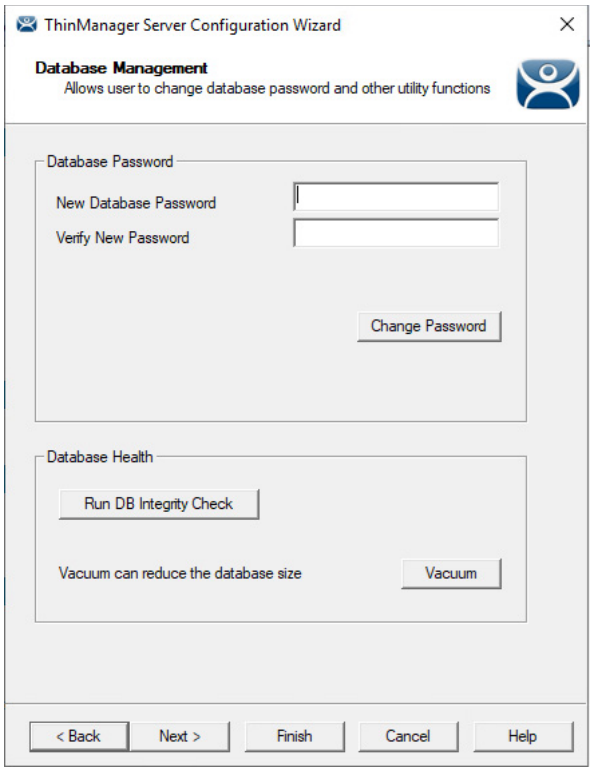
In Figure 860, the SMTP server was not set up properly and an error message was displayed as a reminder.

7. Click Next to continue, Finish to save and close, or Cancel to close and not save.

Database Management Page

1. Navigate to the Database Management page of the ThinManager Server Configuration Wizard. See ThinManager Server Configuration Wizard on page 593 for more information on how to open the wizard.

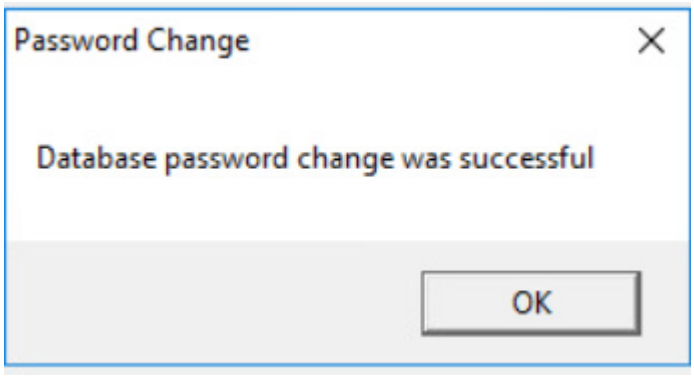
Figure 861 - Database Management Page



2. Type the new password in the New Database Password and Verify New Password fields.
3. Click Change Password to commit the changes.

   A dialog box confirms the database password change was successful.

Figure 862 - Successful Database Password Change dialog

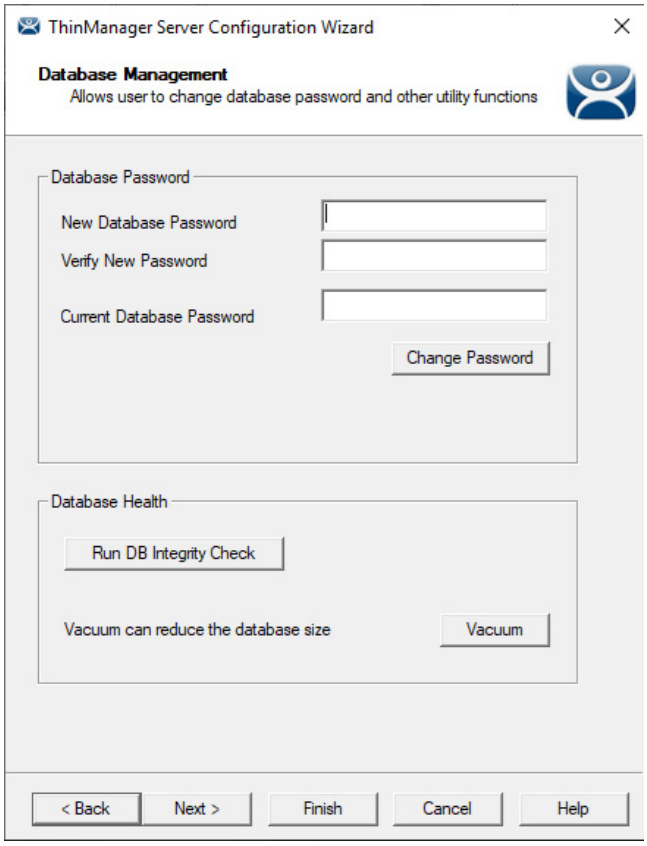


4. Click OK.

   The database password is changed.

User accounts without the Administer ThinManager Servers security role can change the running database password. However, they are prompted to enter the current database password. See Figure 863 on page 611.

Figure 863 - Current Database Password and Integrity Check



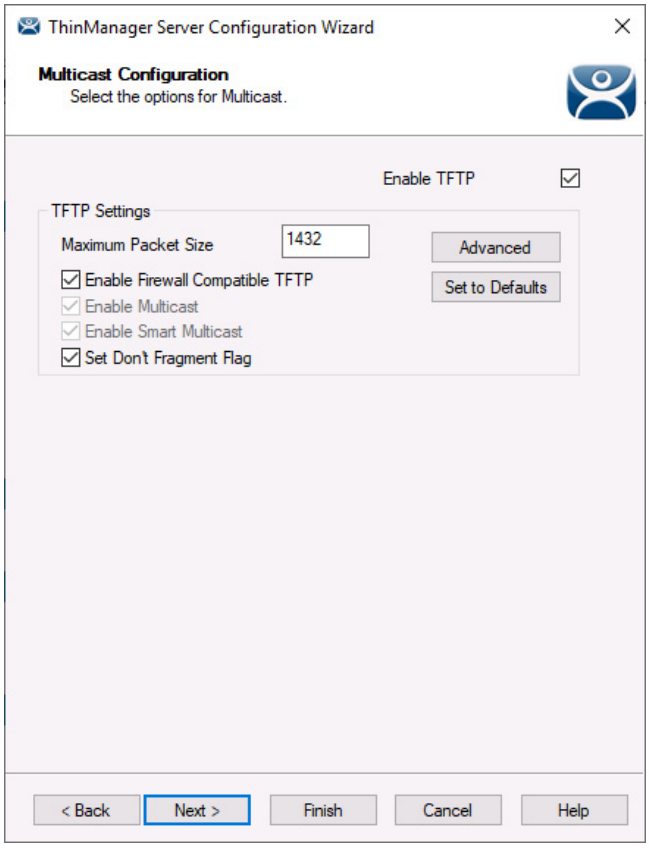
IMPORTANT Backups are still unrecoverable if the password is lost.

5. Click Run DB Integrity Check to run an integrity check on the configuration database.

Contact Technical Support if any errors result from the integrity check.

6. Click Vacuum to compress the running database, which is useful prior to database exportation or major database change.
7. Click Finish to exit the wizard, or click Next to proceed to the Multicast Configuration page.

Figure 864 - Multicast Configuration Page



1. Configure TFTP Settings, if required, based on network infrastructure for the following properties.

Setting	Description
Enable TFTP	Check to enable firmware delivery via TFTP (Trivial File Transfer Protocol) to terminals. Clear this checkbox to disable this option and force firmware delivery via HTTPS (Hypertext Transfer Protocol Secure), which is the default delivery mechanism for ThinManager firmware even if TFTP is enabled. The ThinManager server uses the HTTPS port that is configured on the HTTPS Server Settings page of the ThinManager Server Configuration Wizard, see HTTPS Server Settings Page on page 614 for more information. If the HTTPS port is not open and allowed through the firewall, the ThinManager server attempts to deliver the firmware to the terminal via TFTP if this option is enabled.
Maximum Packet Size	Allows the firmware download packet size to be changed, if needed.
Enable Firewall Compatible TFTP	Enables the firewall friendly TFTP to be used to send firmware to the thin client. This setting makes it easier to get through a firewall.
Enable Multicast	Check to enable multicast.
Enable Smart Multicast	Check to enable Smart Multicast.
Set Don't Fragment Flag	Check to tell the switch to keep the packets together instead of breaking them into fragments. This setting adds the Don't Fragment header in the network packets used to deliver firmware to the thin clients. Network hardware, such as switches and routers, will not break these packets apart. Checked by default because the thin client cannot rejoin fragmented packets.
Advanced	Click to display the advanced settings.
Set to Defaults	Click to return the settings back to the defaults.

You may need to change the settings if there is a conflict with another multicast server on the network.

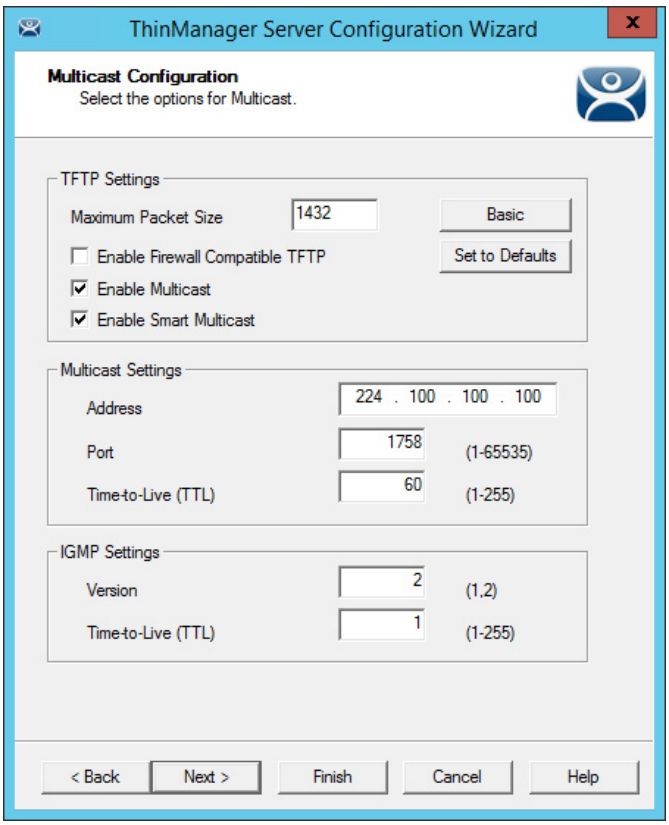
Multicast provides the ability for an unlimited number of Terminals to boot simultaneously from the same data stream. This feature reduces the amount of network traffic and the load on the ThinManager Server when multiple Terminals boot concurrently. Multicast is especially useful for low-bandwidth connections and highly utilized networks.

Smart Multicast allows the Terminal firmware to be sent directly to the Terminal while a single Terminal boots. If additional Terminals request the Terminal firmware at this time, the firmware is multicast so that all Terminals can receive the firmware from a single data stream. If Smart Multicast is disabled, the firmware is always 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.

When a ThinManager error check determines that a Terminal's multicast download failed, the firmware download is switched to unicast. The thin client continues to try to use multicast at each boot, but uses unicast if multicast continues to fail.

Figure 865 - Advanced Multicast Options



Changing the multicast settings is beneficial if there is a conflict with another multicast server on the network.

Setting	Description
Multicast Settings	
Address	IP address used for Multicast transmissions.
Port	Destination port used for Multicast transmissions.
Time-to-Live (TTL)	Maximum number of router hops for Multicast packets. Set to 255 to allow for unlimited hops.
IGMP Settings	Internet Group Management Protocol
Version	Sets the IGMP version for use with multicast-capable routers.
Time-to-Live (TTL)	Sets the time-to-live value for IGMP packets.

2. Click Next to continue, Finish to save and close, or Cancel to close and not save.

HTTPS Server Settings Page

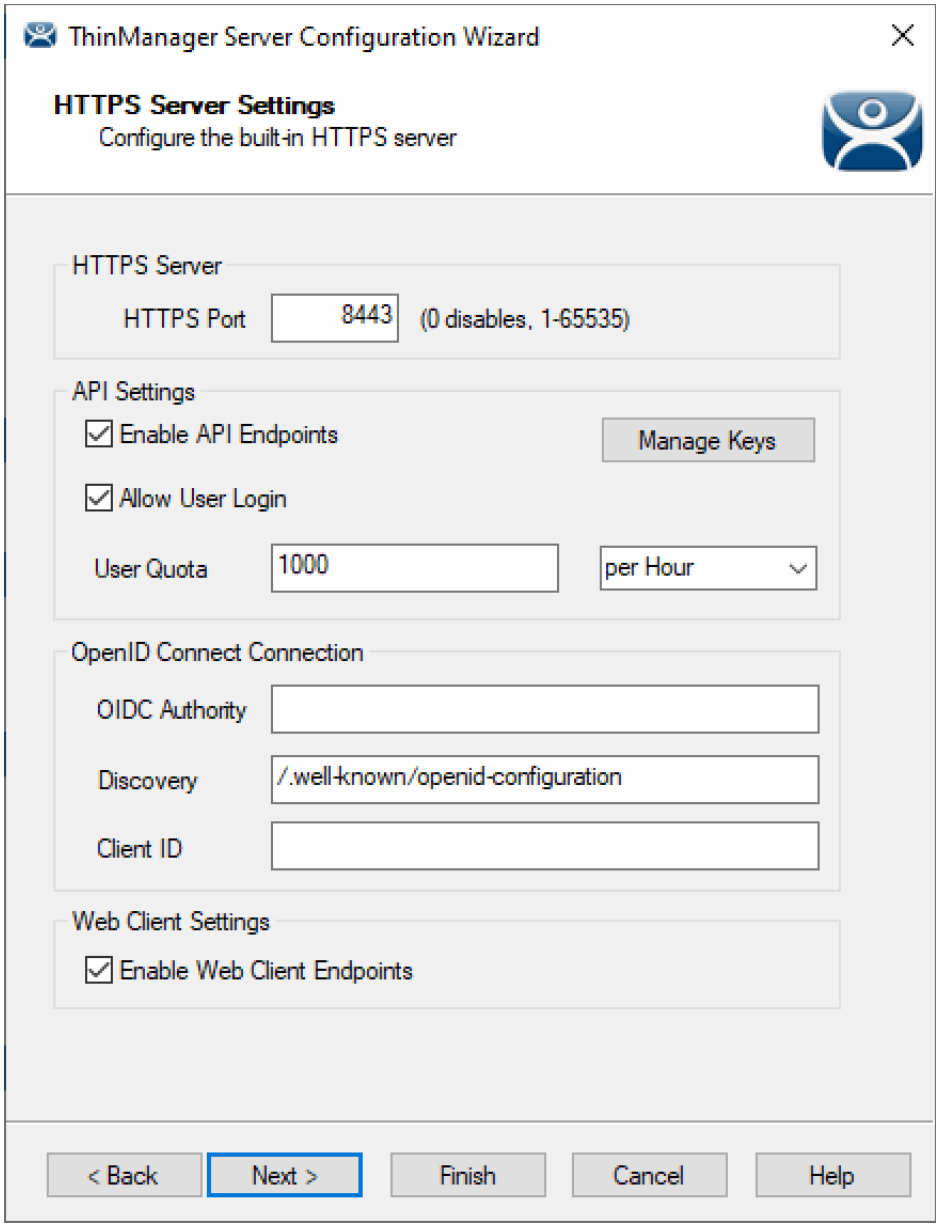
The HTTPS Server Settings page is used to set the HTTPS port for ThinServer and API settings. By default, the HTTPS port is enabled and set to Port 8443. This port is used to deliver some modules after the firmware delivery and is used to access the API. If set to 0, modules will be delivered via UDP 69 and UDP 4900 and the API will not be accessible.

To use the API, Enable API Endpoints must be checked. This is in addition to setting the HTTPS Port to a valid number. API end point documentation is intended to be accessed via a web browser and can be found at https://[thinserverhostIP]:[HTTPS port]/api/documentation. For example, to connect with the default port when ThinServer is installed on the local host, navigate to https://localhost:8443/api/documentation. The API supports GET, POST, PUT, and DELETE methods.

For more information on the API, see page [insert page here in Ch. 4 ThinManager® System]

See API on page 60 for more details.

Figure 866 - HTTPS Server Settings Page



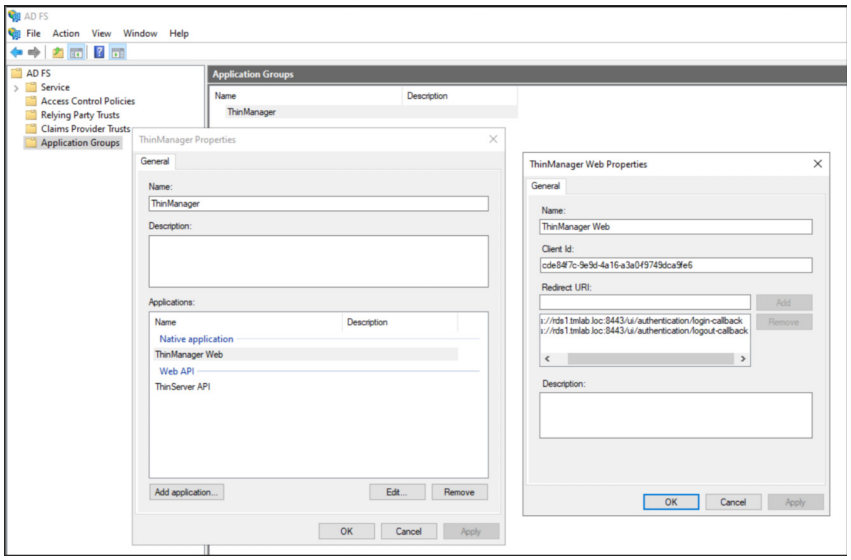
Setting	Description
HTTPS Server	
HTTPS Port	This sets the TCP port which the HTTPS server will run on for access to the API.
API Settings	
Enable API Endpoints	Enabling this settings allows for an entry point to communicate with the HTTPS server. Without enabling this setting, the API cannot be utilized.
Allow User Login	This setting allows for User API Keys to be generated using the Login API endpoint. The ThinManager API allows for application keys and user keys to be generated. When enabled, users can generate their own API key from the login endpoint. API User keys are inherited from the users group membership role as defined in ThinManager Security Groups.
User Quota (time and unit)	Sets the number of times a user can use an user API key to authenticate a method on an endpoint for the specified rolling duration.
OpenID Connect Connection	
OIDC Authority	This server address URL connects to the OIDC provider.
Discovery	Sets the path to the OpenID configuration.

Setting	Description
Client ID	Sets the OpenID client application's specific ID.
Web Client Settings	
Enable Web Client Endpoints	Check to activate the ThinManager Web UI and make it available to users. This is a global setting for this ThinServer, but permissions can be used in the same way to secure users or group actions.
Button	
Manage Keys	Launches the Manage API Keys wizard which allows for API keys to be created, edited, or deleted. The Manage Keys wizard will manage both application and user API keys.

To effect changes to the OpenID Connect Connection or Web Client Settings, restart the ThinManager server via a restart of the ThinServer service or a toggle of the Enable API Endpoints checkbox.

An Open ID Connect (OIDC) service can be used to add Single Sign-on functionality for the ThinManager Web API and the Web UI. While it is beyond the scope of this manual to provide guidance on your OIDC configuration, some guidance for an on-premise solution can be found in Figure 850. For on-premise Active Directory deployments, a Microsoft Active Directory Federated Service (ADFS) role can be added to a member server on your domain.

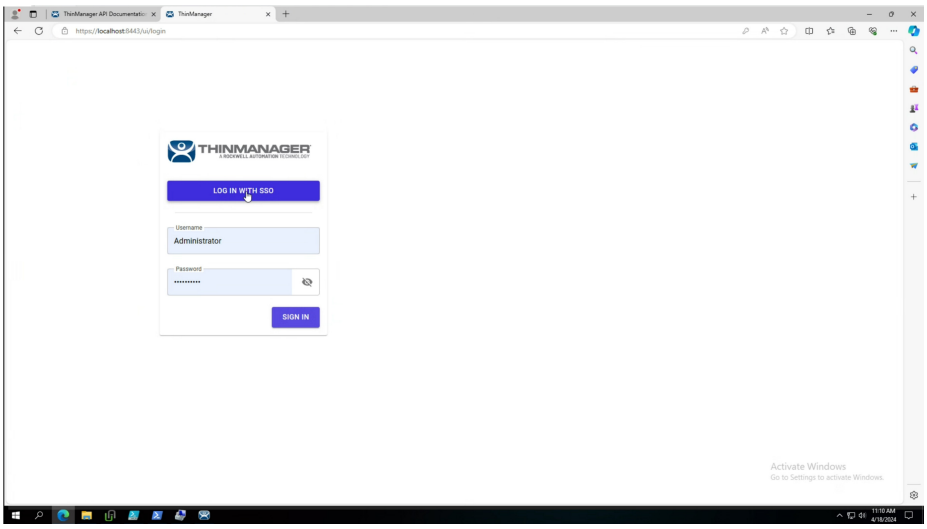
Figure 867 - ThinManager Web Properties - within the ADFS



Setting	Description
ThinManager Properties	
Name	Enter the name to reference for your ADFS configuration.
ThinManager Properties	
Client ID	Enter your ADFS client ID.
Redirect URI	Set the login/logout-callback paths

After ADFS configuration is complete, go to ThinManager Web UI, where a new LOG IN WITH SSO button appears.

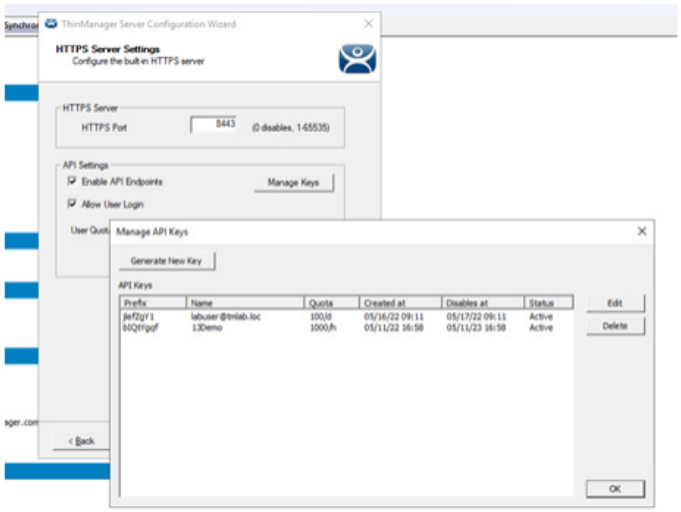
Figure 868 - ThinManager Web UI with Single Sign-on (SSO) Available



Why Change from Default Settings?

The API for ThinServer is not enabled by default, and must be enabled to communicate with any of the endpoints. When enabled, only application keys are enabled without enabling user keys. User keys allow users to self-generate a key to authenticate their use of the API for the endpoints which their ThinManager Security Group would allow them to configure.

Figure 869 - Manage API Keys Dialog



Importance of Page: This page allows an administrator to view all user and application API keys that have been created in the system. User keys will be named with a Windows username and application keys will be named with a logical name given by the administrator during creation. The prefix of each key will be shown to help identify the key but cannot be used alone for authentication. The full key value is required for endpoint authentication. Application key values cannot be retrieved after their creation. A key can be created, modified, or deleted from this page. This page also displays

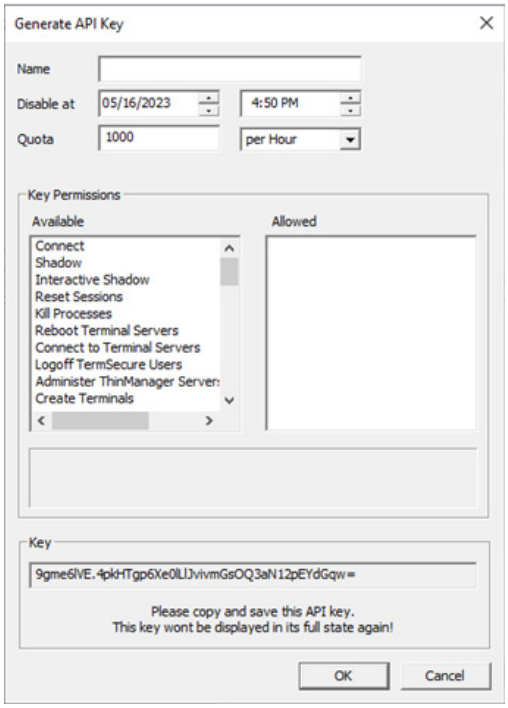
information such as create date, rolling usage quota, create date, disable date, and status.

Button	Description
Generate New Key	Launches a page to create a new application API key.
Enable API Endpoints	Enabling this settings allows for an entry point to communicate with the HTTPS server. Without enabling this setting, the API cannot be utilized.
Edit	After one of the listed API keys is selected press this button to launch the Edit API Key page, where the permissions, quota, and disable date are modified.
Delete	Press to delete the selected PI key.

Why change from default settings?

API Keys are required to access the API endpoints. Users who no longer have access to the API endpoints can have their key disabled or deleted. Keys which need a more or less restrictive access to the API can be modified with the appropriate permissions.

Figure 870 - Generate API Key



Importance of Page: API keys provide access for authentication to communicate with API endpoints. If this page was accessed from the Generate New Key button, then the Name field appears empty. The full API key is displayed in the Key field at the bottom of the page if a new API key is generated.

IMPORTANT This key will not be displayed in its full state again and must be copied and stored for use.

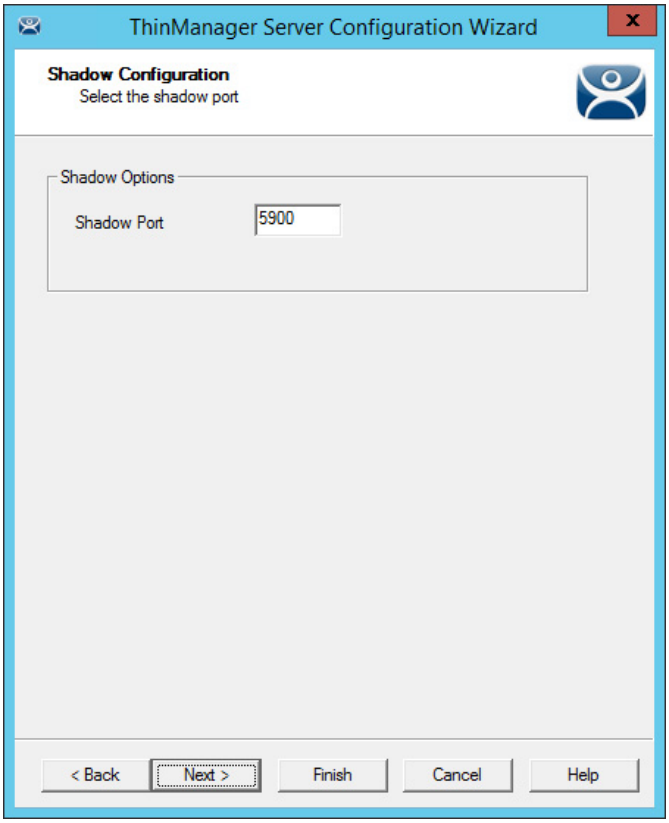
Fields	Description
Name	Enter the name of an application key here. If the page was accessed from the Edit button on the Manage API Keys page, this field is already populated and can be edited from this window.
Disable at	Set the date and time to disable the key, which prohibits the connection to any API endpoints that occur after the specified value.
Quota	(numeric input and rolling time duration) Set the limit for the number of times an API key can be used to authenticate a method within the specified rolling time frame. Each endpoint is authenticated every time a method is called from the API.
Available	This list box shows the ThinManager functions available via API endpoint when authenticating with the API key in the Name text field. Double-click the functions to add them to the Allowed list.
Allowed	This list box shows the ThinManager functions granted to the API key in the Name text field of the page. Double-click these functions to remove them from the list.
Key	Displays the API key required to establish communication with the API for any desired endpoint. When editing a key, only the key prefix is shown. The key prefix cannot be used to authenticate the API. Note: When creating a new application key, the key is only displayed in its full state one time. Therefore, the key must be copied and saved in a safe place for use.

Why Change from Default Settings?

API keys grant access to endpoint methods. Key creation and modification allow for granular permissions to be distributed to users and applications utilizing the ThinManager API. Quotas and disable dates, prevent unauthorized access, and provide a method to revoke access for applications or users who access ThinManager from the API.

Shadow Configuration Page

Figure 871 - Shadow Configuration Port



By default, the Shadow port in ThinManager is Port 5900. This can be changed under Shadow Options.

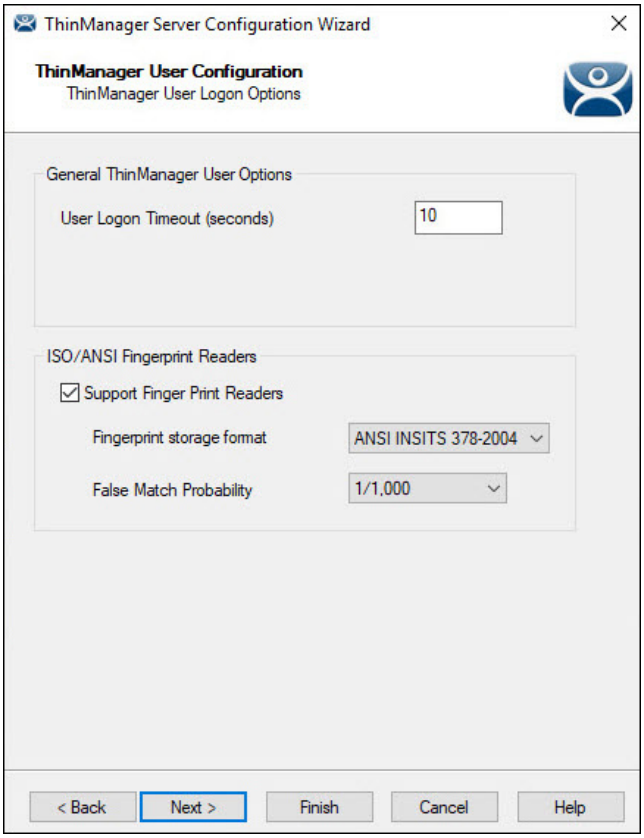
Setting	Description
Shadow Port	ThinManager uses port 5900 as the default shadow port. Enter a different port number into the Shadow Port field to change the port used if it is in conflict with another process's use of the port.

ThinManager uses the same port as VNC. If VNC is installed on a WinTMC PC, then there could be a conflict between shadow services. If this happens, the port can be changed in ThinManager.

1. Click Finish to accept changes or select Cancel to close without making changes.

ThinManager User Configuration Page

Figure 872 - ThinManager User Configuration



1. Navigate to the ThinManager User Configuration page and select the properties, as required, as described here.

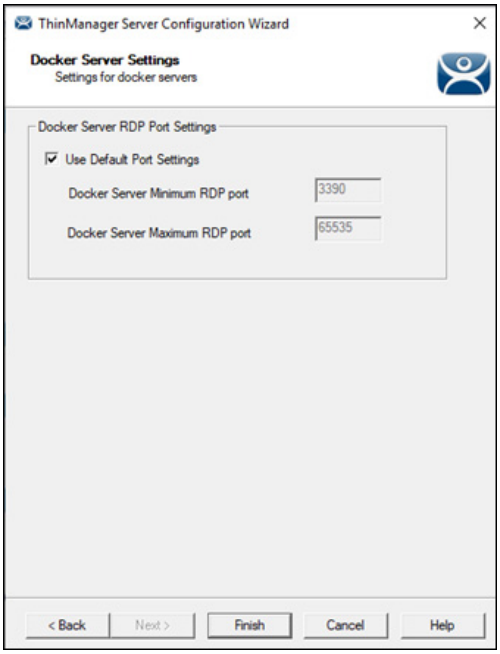
Settings	Description
General ThinManager User Options	
User Logon Timeout (seconds)	Specify the amount of time a terminal should wait for the ThinManager server to return a valid user configuration. If the terminal does not receive a reply in the amount of time specified, an error message is displayed on the terminal.
ISO/ANSI Fingerprint Readers	
Support Finger Print Readers	Allows ThinManager to use the Digital Persona fingerprint readers.
Fingerprint storage format	The pull-down menu allows for the specification of use of an ISO or ANSI format to store fingerprint data. There are two formats: ISO_19794_2_2005 and ANSI_378_2004.
False Match Probability	Sets the sensitivity of the scan. 1/100 is less sensitive than 1/1,000,000.

2. Click Finish to accept the changes.

Docker Server Settings Page

The Docker® Server Settings page of the wizard is where the user can set the range of ports used for containers. Each connection to a container uses its own unique RDP port.

Figure 873 - Docker Server Settings Page



If Use Default Port Settings is checked, containers use port 3390 and increment by one per connection. If the checkbox is cleared, the user can input custom port numbers.

Notes:

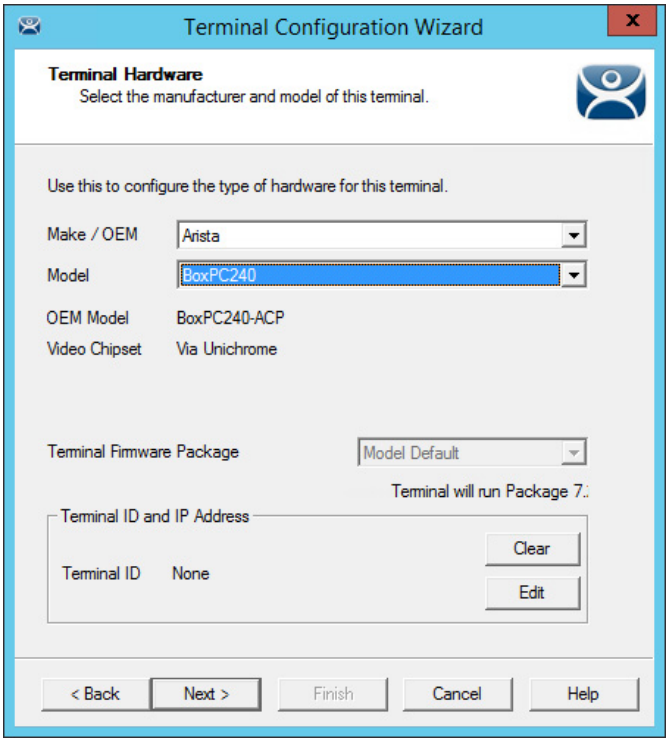
MultiMonitor

The MultiMonitor method uses specific ThinManager-ready thin clients that have multiple video ports built into the hardware. Beginning with ThinManager version 11.1, the number of monitors is dependent on available video ports on a thin client. 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.

WinTMC supports MultiMonitor sessions on PCs that run Windows on multiple desktops.

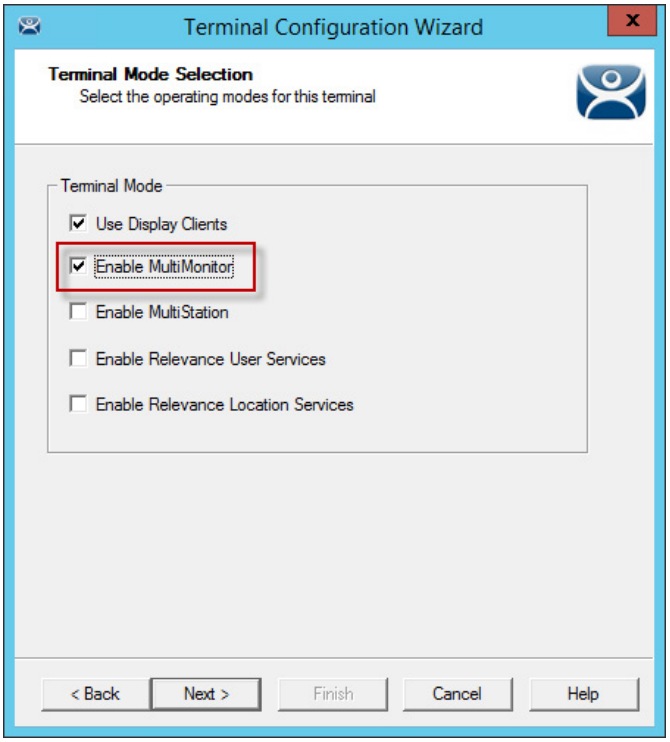
MultiMonitor is configured in the Terminal Configuration Wizard or the Group Configuration Wizard.

Figure 874 - Terminal Hardware



1. On the Terminal Hardware page of the Terminal Configuration Wizard, choose a MultiMonitor-capable thin client to initiate MultiMonitor configuration.

Figure 875 - MultiMonitor – Enable MultiMonitors



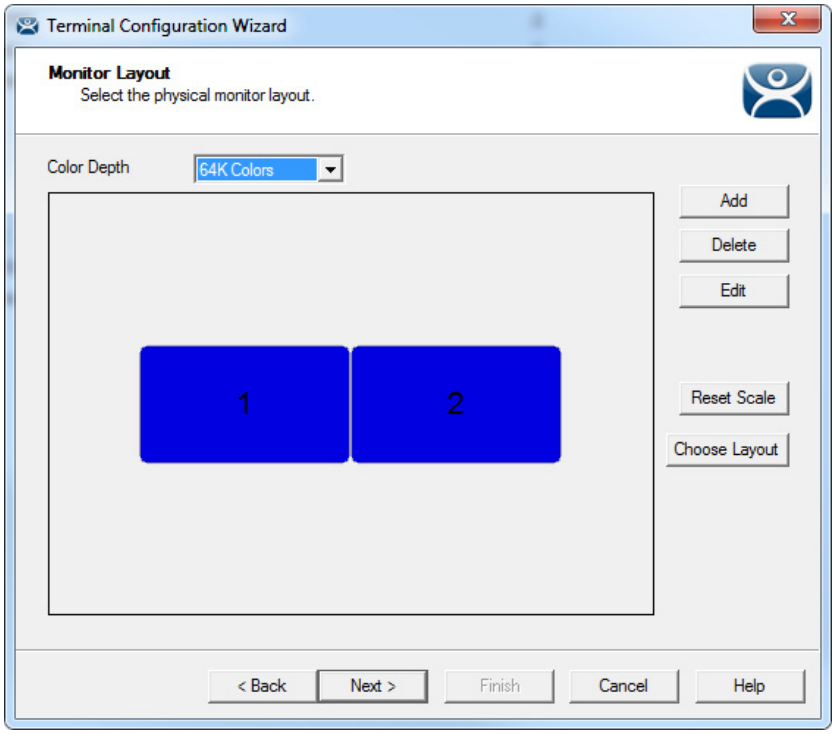
MultiMonitor requires the use of Display Clients.

2. On the Terminal Mode Selection page, check Use Display Clients to make the Enable MultiMonitor terminal mode available.
3. Click Next until the MultiMonitor Layout page appears.

MultiMonitor Layout Page

The MultiMonitor configuration process changed in ThinManager 11.1.

Figure 876 - Monitor Layout



The default setting shows two monitors. You can add more as needed.

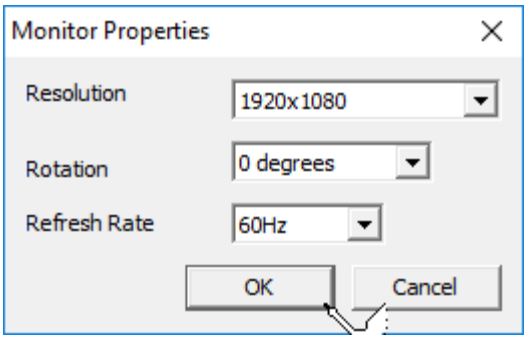
Setting	Description
Add	Launches the Monitor Properties dialog box and adds a new monitor.
Delete	Deletes a highlighted monitor.
Edit	Opens the Monitor Properties dialog box of a highlighted monitor, where the resolution can be changed.
Reset Scale	Centers the monitors in the configuration wizard. Also, you can use the scroll wheel of the mouse to zoom in and out.
Choose Layout	Allows you to select from layout templates. Otherwise, you can drag monitors to a location.

The monitor resolution is set in the Monitor Properties.

1. Click Add.

   The Monitor Properties dialog box appears, where the monitor resolution is set when you create another monitor.

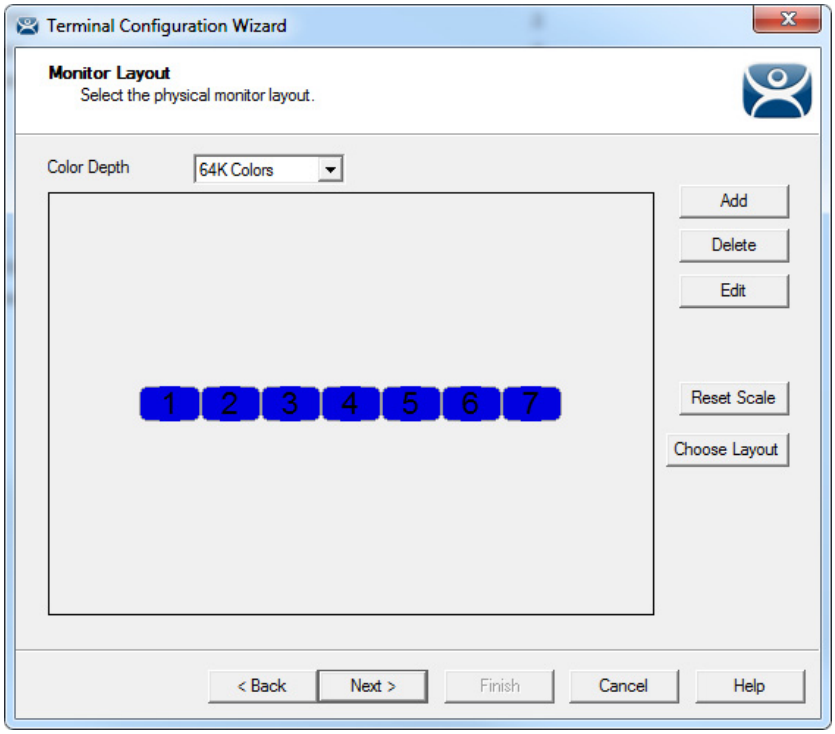
Figure 877 - Monitor Properties



Setting	Description
Resolution	Choose the desired video resolution for the monitor from the pull-down menu.
Rotation	Choose the clockwise rotation, in degrees, for a monitor from the pull-down menu. Use when the monitor is in vertical, portrait mode versus horizontal, landscape mode.
Refresh Rate	Choose the refresh rate for the monitor from the pull-down menu.

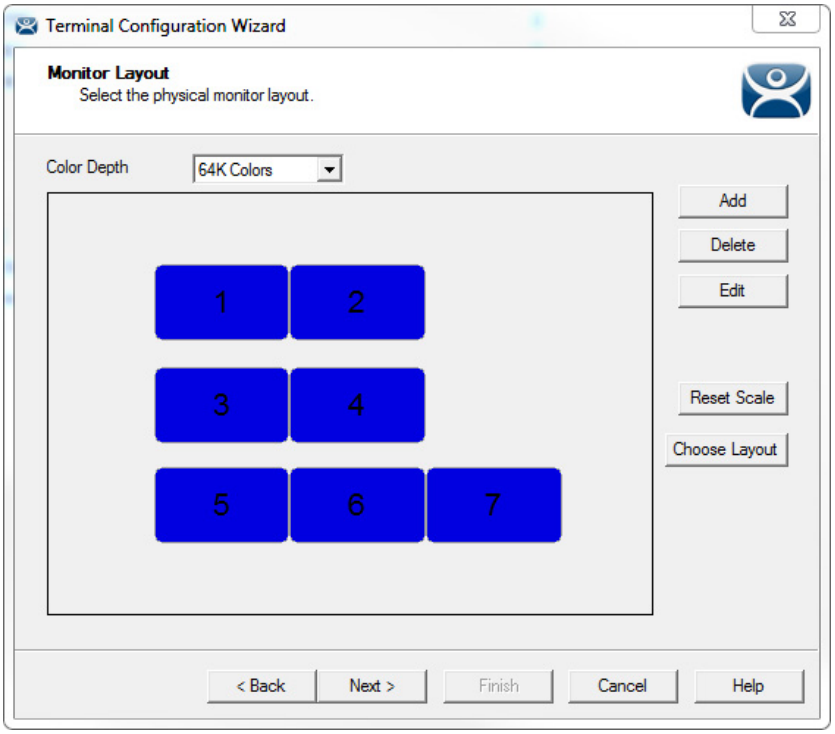
2. Click OK to return to the Monitor Layout page.

Figure 878 - Monitor Layout Page



Once the necessary monitors are added, drag them to move them.

Figure 879 - Monitor Layout - Rearranged

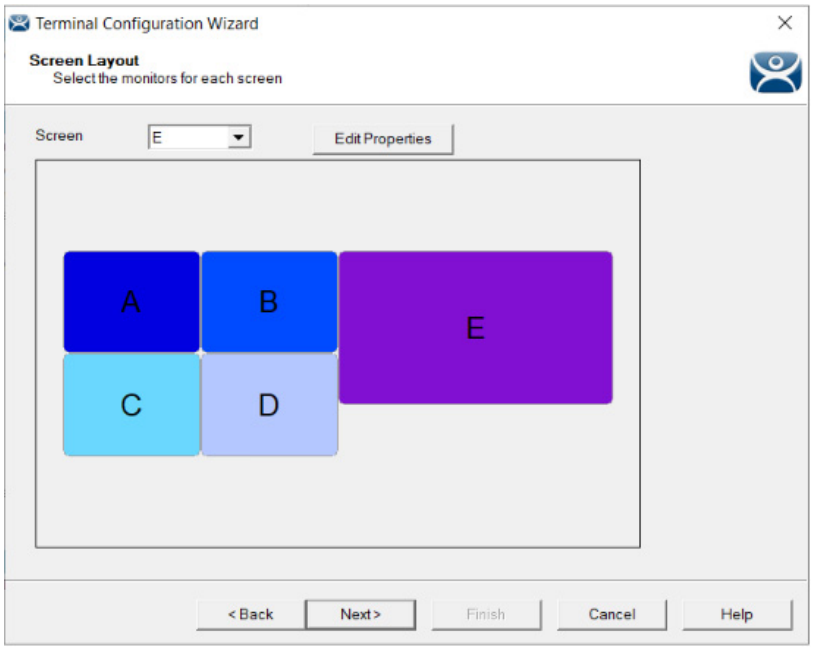


The Screen Layout page of the Terminal Configuration Wizard allows you to logically segment the monitors. Each letter represents a unique group of monitors. Sessions on monitors that share the same letter are called “Spanned” sessions and logically act like a single monitor. Sessions on monitors that have a unique letter are called “Screened” sessions, and the session appears on the specified monitor only.

Spanned monitors must form a rectangular shape and have the same resolution.

All monitors start as Screen A.

Figure 880 - Monitor Layout – Screen Letters Assigned



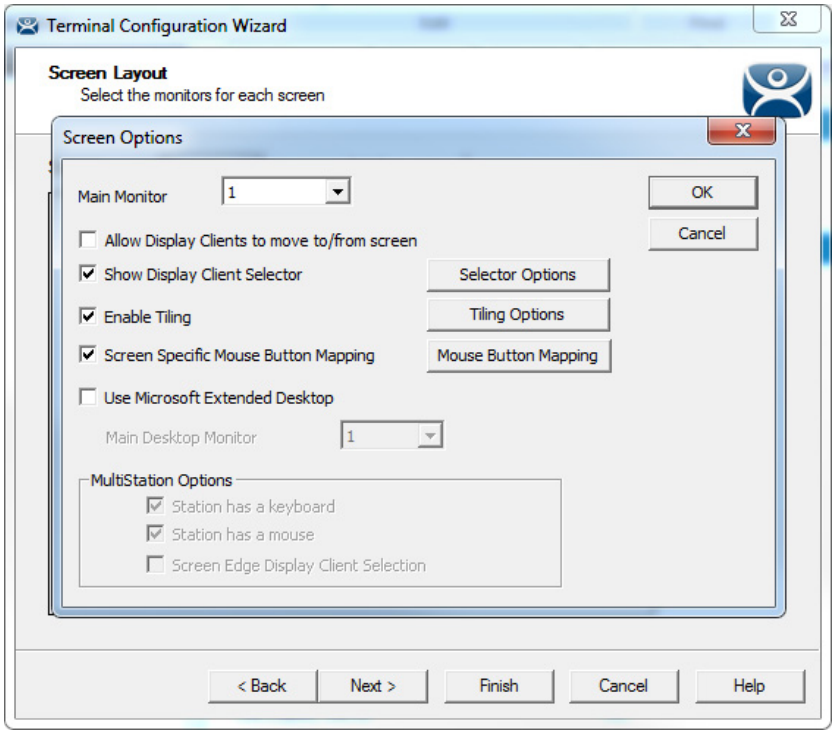
3. Choose the screen letter from the Screen pull-down menu to change a monitor letter designation, and then click a monitor icon, which applies the monitor letter to the screen.

Monitors can share a desktop if they have the same letter designation. They must be the same resolution and form a rectangle; they cannot be askew.

4. Click Edit Properties.

   The Screen Options dialog box appears, where you can configure monitor properties.

Figure 881 - Screen Options Dialog Box



The Reset Scale button on the Monitor Layout page makes monitor configuration easier to see once in order.

Setting	Description
Main Monitor	Sets which monitor has the mouse focus on boot and displays the Relevance Main Menu.
Allow Display Clients to move to/from screen	Allows you to move Display Clients from monitor to monitor because it lets you open the Display Client in a different monitor.
Show Display Client Selector	Makes the Group Selector pull-down menu available.
Selector Options	Makes the Display Client Selector Options dialog box appear.
Auto-hide Selector	Check to hide the Group Selector pull-down menu. Clear the checkbox to display the Group Selector.
Tile on Selector Activation	If selected, tiles the sessions when an auto-hide selector is activated.
Select Menu Size	Allows you to change the size of the Group Selector.
Enable Tiling	Shows all Display Clients assigned to a monitor in a tiled mode, if selected. Select one tile to display it on the full monitor.
Tiling Options	Opens the Tile Options dialog box that configures tile options.
Show Grid	Displays grid lines when it is tiled.
Tile Activity Time (secs)	Sets the time before the monitor reverts to tiled mode when a single screen is displayed.
Tile Display Clients at start up	Configures the monitor to show the display clients in tiled mode at startup.
Include Main Menu as tile	Adds a tile with the Main Menu in it, which is handy for terminals with touch screens.
Tile Interactive	Changes the behavior of the mouse. Instead of a switch from tiled mode to a single display client, it allows the user to click in the tiled session and use the session in the tiled mode.
Screen Specific Mouse Button Mapping	Allows you to assign actions to mouse buttons.

Setting	Description
Mouse Button Mapping	Opens the Mouse Button Mapping dialog box, where each mouse button can be configured with one of these actions.(1) • Calibrate Touch Screen • Tile • Swap • Full Screen • Go to next display client • Go to previous display client • Log on ThinManager user • Main Menu • Left Mouse Button • Right Mouse Button • Middle Mouse Button • Scroll Up • Scroll Down • Virtual Keyboard • Disable Button
Use Microsoft Extended Desktop	Apply the Microsoft Extended Desktop to a spanned set of monitors. With the Microsoft Extended Desktop, an expanded application stops at the monitor boundary as it does in Windows. Without the Microsoft Extended Desktop, an expanded application fills the entire desktop.
Main Desktop Monitor	Sets which monitor of a spanned set is the primary desktop.
MultiStation Options	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	Allows you to switch between display clients by moving the mouse to either edge of the monitor.

(1) Touch Screen Modules have a Hold Time that can convert a long touch to a right-click. Use the Mouse Button Mapping feature to apply any of these actions to the long hold.

The desktop of a spanned session is limited to 4096 x 2048 in Server 2008 R2 and earlier. The resolution of a Server 2012 is 8196 x 8196. The Use Session Size Limits pull-down menu on the MultiMonitor Video Setting page allows you to change to this higher resolution.

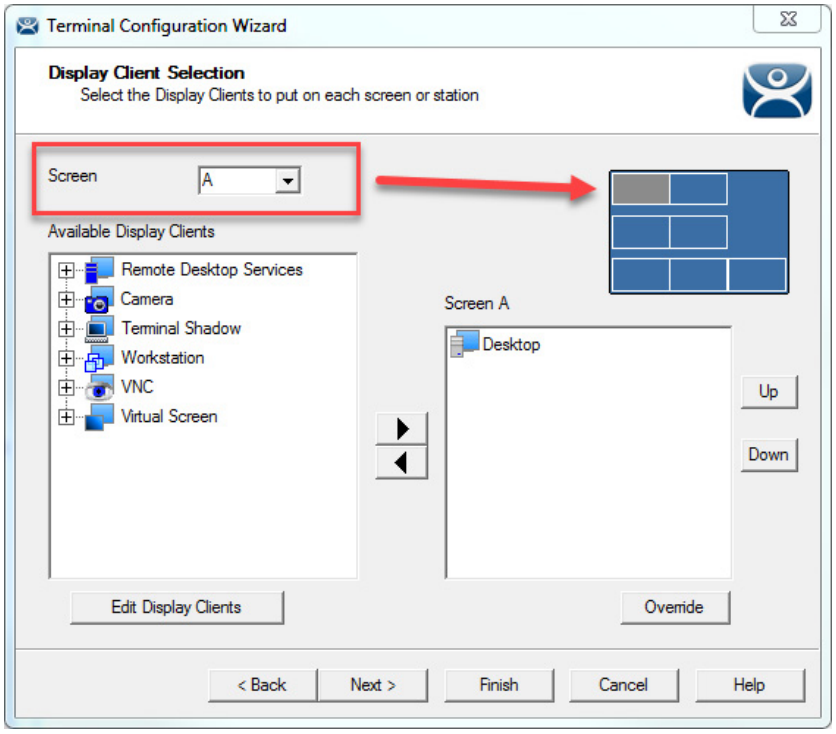
The selection of monitor resolution on the MultiMonitor Video Settings page can affect the number of monitors that you can add to a spanned session.

5. Click Next to continue.

The Display Client Selection page of the Terminal Configuration Wizard appears, where Display Clients are assigned to the screens.

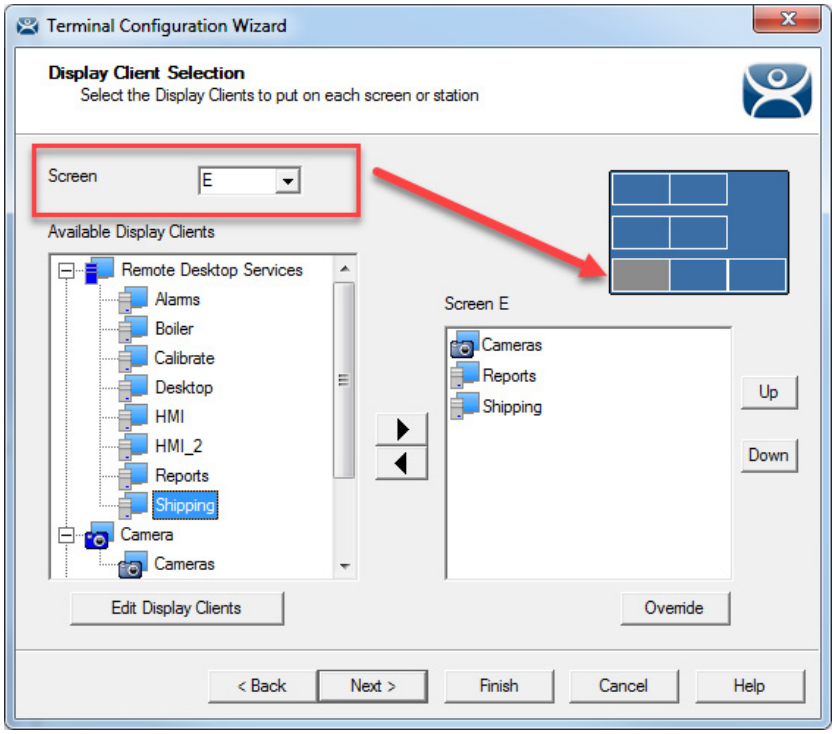
MultiMonitor Display Client Selection Page

Figure 882 - Display Client Selection



1. From the Screen pull-down menu, choose the screen.
2. Highlight a display client in Available Display Clients list and use the right-facing arrow to move it to the Screen list on the right side of the dialog box.

Figure 883 - Change Screen Letter



3. In the Screen pull-down menu, change the screen letter to choose a different screen to which to apply the display client. The icon of the screen changes color to show which screen is being edited.

Multiple display clients can be added to each screen.

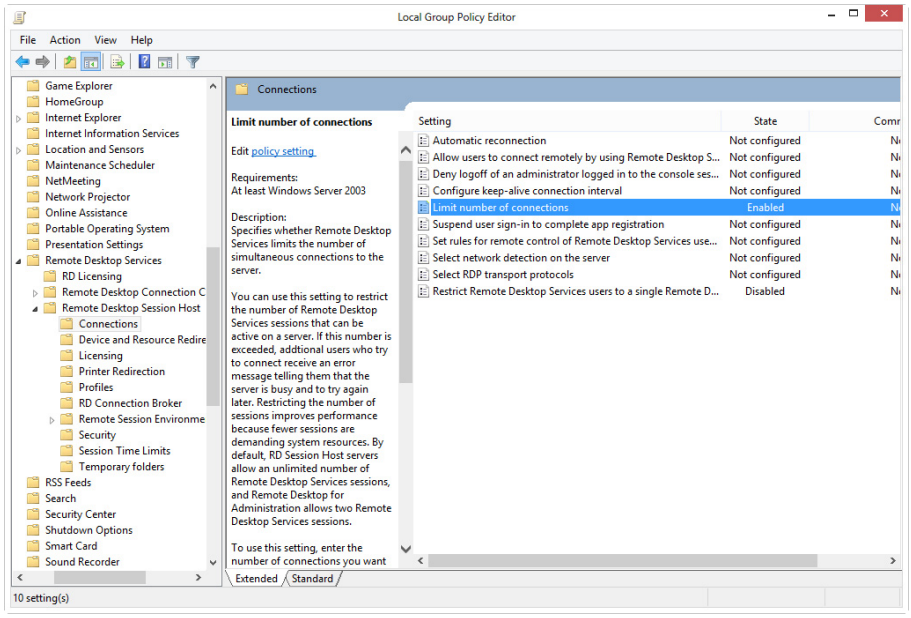
4. Click Override.

   The Override Settings dialog box appears, where you can apply customized settings to the display client.

Override Function

By default, Microsoft restricts each user to a single session on a serve. Keep this setting to prevent conflicts. If it is disabled, then a user creates multiple sessions, which consumes licenses and resources, which makes it more difficult to connect to the proper session.

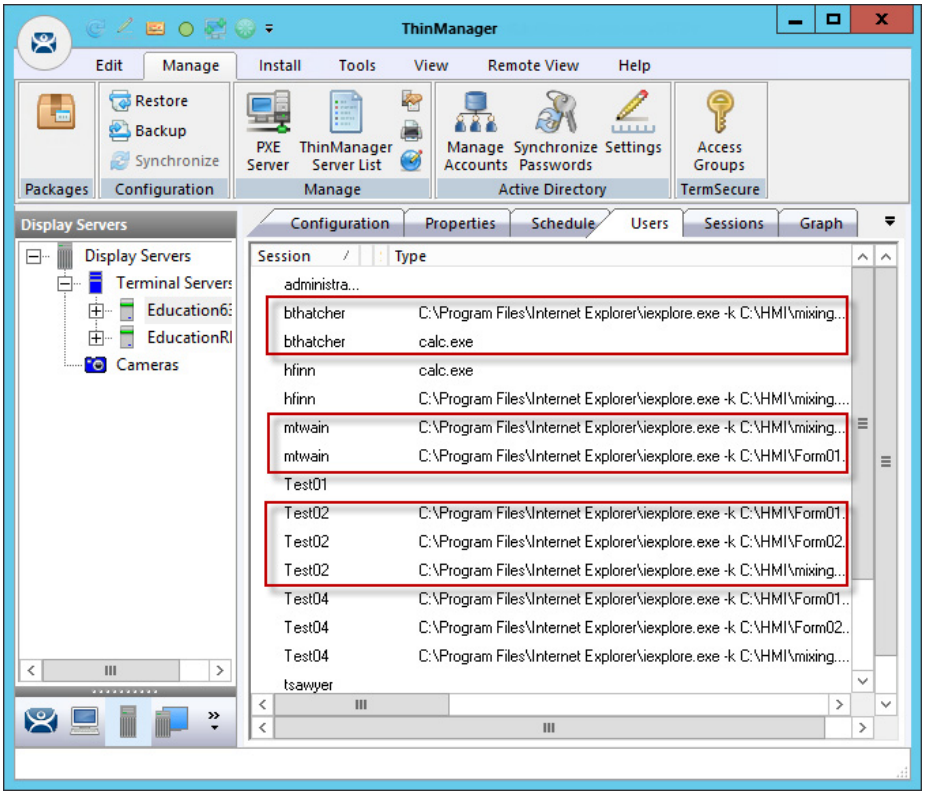
Figure 884 - Limit Number of Sessions



MultiMonitor has an Override function that allows Display Clients on a MultiMonitor thin client to log in with different user accounts or video resolutions. This prevents conflicts between monitors over a single session.

This could be necessary to run duplicate copies of a program on the same thin client.

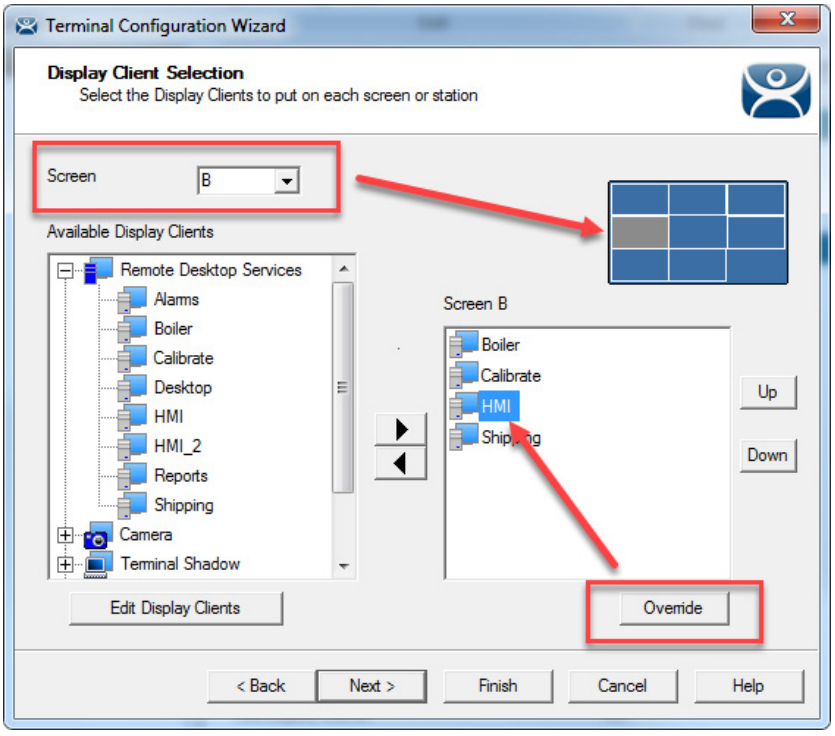
Figure 885 - Remote Desktop Server Users



In reality, a user can log in to a Remote Desktop Server multiple times as long as they are running different applications. Each Username/Application needs to be unique.

It is common to want to run the same application twice on MultiMonitor displays. Typically, that presents a problem. However, the Override function solves this issue.

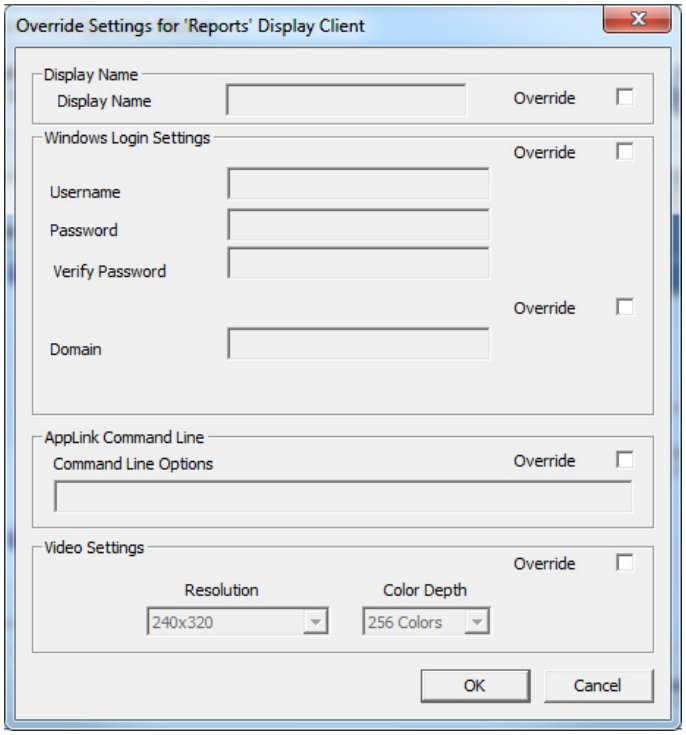
Figure 886 - Override Button



1. Highlight a Display Client assigned to the MultiMonitor thin client on the Display Client Selection page.
2. Click Override.

   The Override Settings dialog box appears.

Figure 887 - Override Settings



3. Click Override to activate the respective override setting and allow customization.

Setting	Description
Display Name	Allows the display client to show a different name than the one originally listed.
Windows Login Settings	Allows different credentials to be used for the display client.
AppLink Command Line	Allows different command line parameters to be applied to the program.
Video Settings	Allows the resolution of the display client to be changed from the monitor setting.

When multiple user accounts are used on a Terminal, it does not affect the "Per Device" TS/RDS CAL count, but it requires more "Per User" TS/RDS CALs.

Figure 888 - Display Client Selection

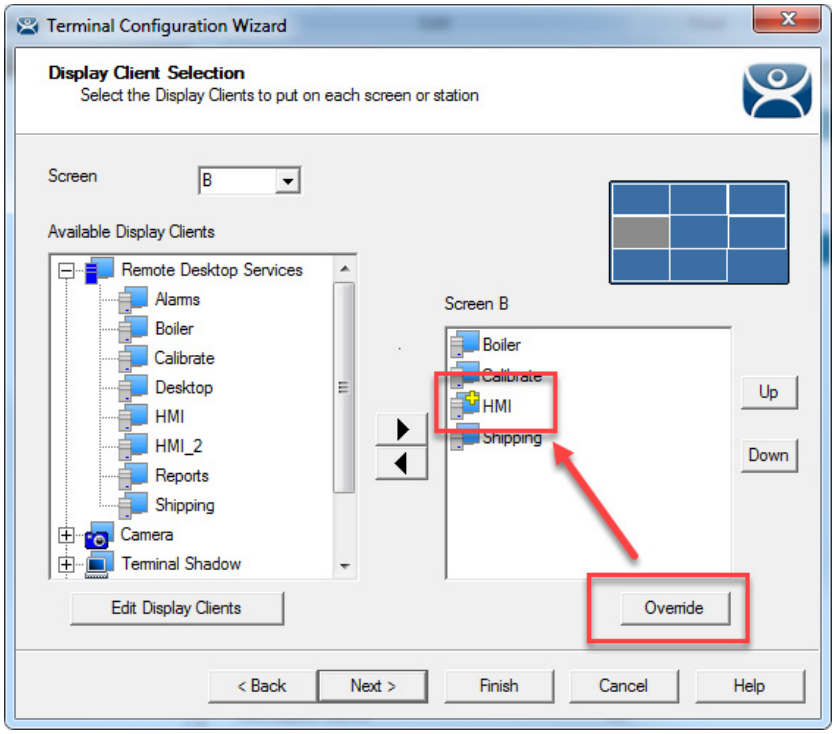


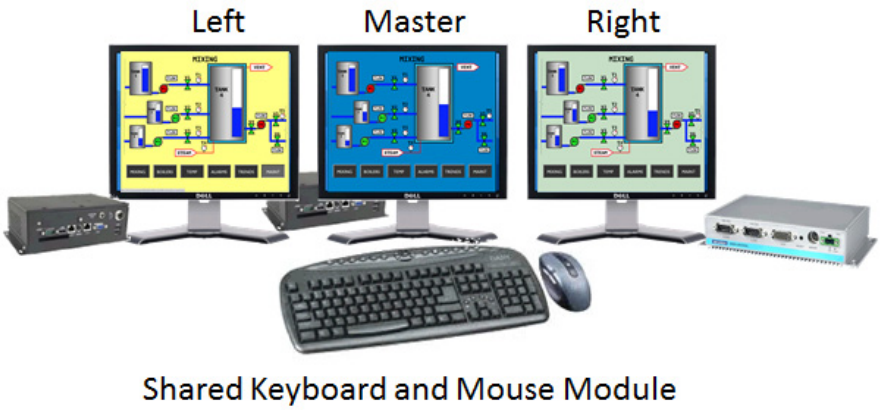
Figure 888 shows the Override button and the Plus icon for a Display Client with its properties overridden.

4. Repeat for any display client that requires a different user account.

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 (Keyboard/Video/Mouse) switch.

Figure 889 - Share Keyboard and Mouse Layout



The Share Keyboard and Mouse module 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 follower thin clients. The other Terminals receive the Share Keyboard and Mouse follower module.

Place three Terminals and their monitors side-by-side.

Master Thin Client Configuration

One thin client needs to be configured as the Master. It is the dominant Terminal whose keyboard and mouse are used to control the grouped Terminals.

1. Double-click the center Terminal in the ThinManager tree.

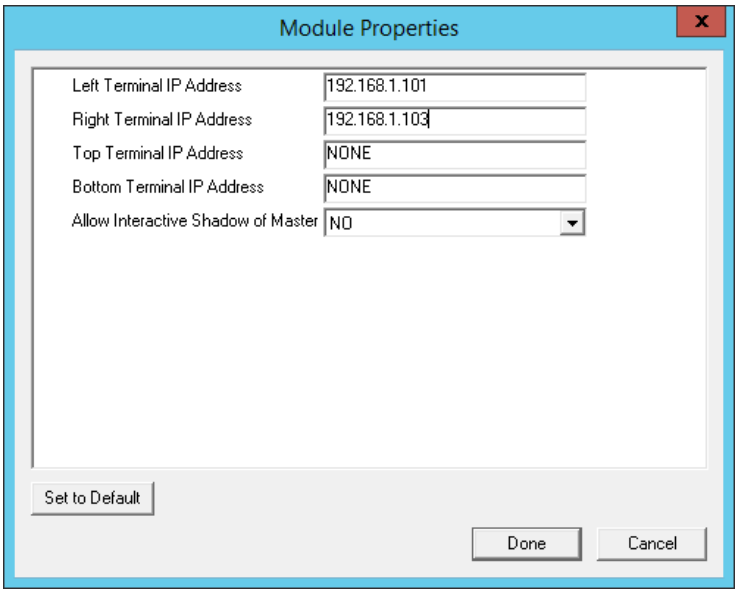
   The Terminal Configuration Wizard appears.
2. Click Next until the Module Selection page appears.
3. Click Add.

   The Attach Module to Terminal dialog box appears.
4. Highlight Share Keyboard and Mouse Master Module and click OK.

   The module appears in the Installed Modules list of the Module Selection page.
5. Highlight Share Keyboard and Mouse Master Module and click Configure.

   The Module Properties dialog box appears.

Figure 890 - Share Keyboard and Mouse Master Module



The Share Keyboard and Mouse Master module has a few settings.

Setting	Description
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	Controls whether the master Terminal is allowed to be controlled by a remote user.

6. Click Done.
7. Restart the ThinManager-ready thin client to apply the changes.

Replica Thin Client Configuration

The other Terminals in the group need the Replica module.

1. Double-click each Terminal in the ThinManager tree.

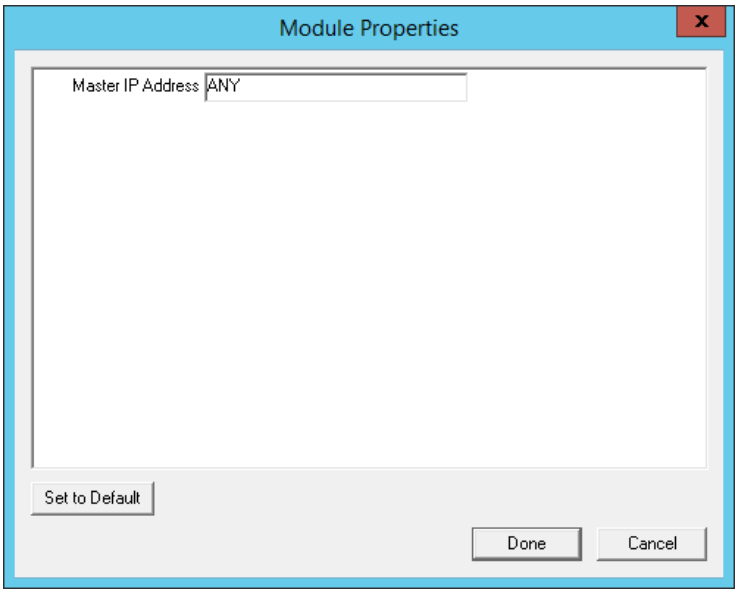
   The Terminal Configuration Wizard appears.
2. Click Next until the Module Selection page appears.
3. Click Add.

   The Attach Module to Terminal dialog box appears.
4. Highlight Share Keyboard and Mouse Follower Module and click OK.

   The module appears in the Installed Modules list of the Module Selection page.
5. Highlight Share Keyboard and Mouse Follower Module and click Configure.

   The Module Properties dialog box appears.

Figure 891 - Share Keyboard and Mouse Follower Module Properties



The Share Keyboard and Mouse Follower Module Properties dialog box has one parameter that allows the replicas to point to a master.

Setting	Description
Master IP Address	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.

6. Click Done.
7. 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 is active in the screen on which the mouse pointer is present.

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.

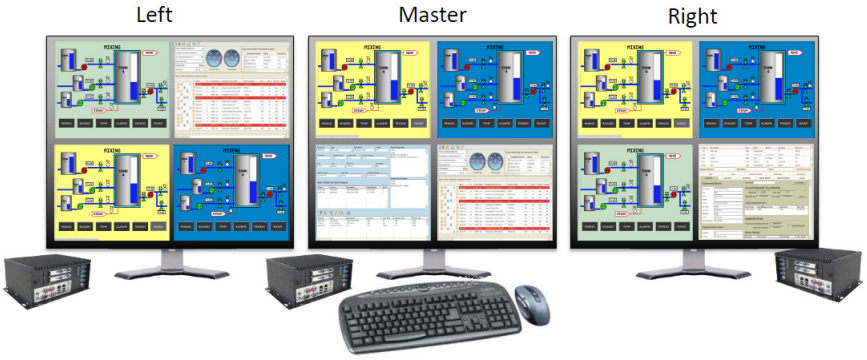
A Controller Share Keyboard and Mouse session cannot be interactively shadowed in ThinManager unless that parameter is activated.

The keyboards and mice for the follower thin clients can be left attached, but stowed away until a multi-user configuration is needed.

Share Keyboard and Mouse with MultiMonitor

The Share Keyboard and Mouse module became less popular as MultiMonitor hardware was introduced. It is easier to use a single MultiMonitor thin client to show multiple displays than to use several thin clients and the Share Keyboard and Mouse module. However, the module regained popularity when using it to tie multiple MultiMonitor thin clients to set up a control room environment.

Figure 892 - MultiMonitor with Share Keyboard and Mouse



MultiMonitor Shared Keyboard and Mouse Module

The configuration of the Controller and Follower Share Keyboard and Mouse modules are the same with MultiMonitor thin clients as they are with single monitor thin clients.

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 Report tab on the Details pane shows a report for a highlighted ThinManager Server, Terminal, Terminal group, Remote Desktop Server, TermSecure user, or ThinManager User group.

Reports can be scheduled to be run and saved as *.html or *.CSV files for storage or further analysis.

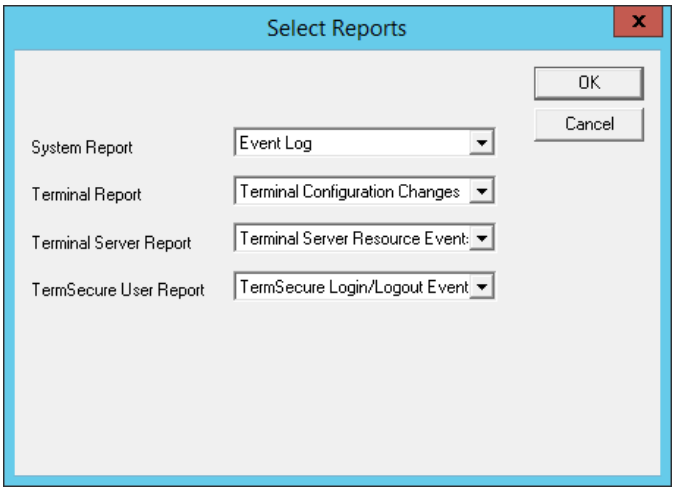
Select Reports

The reports are displayed on a Report tab in ThinManager.

1. Choose View>Select Reports from the ThinManager menu.

The Select Reports dialog box appears, which allows the selection of which report to display.

Figure 893 - Select Reports



The Select Reports dialog box has four fields that determine which report is displayed on the report tab.

Setting	Description
System Report	Choose the report to display on the Report tab when the ThinManager Server is highlighted.

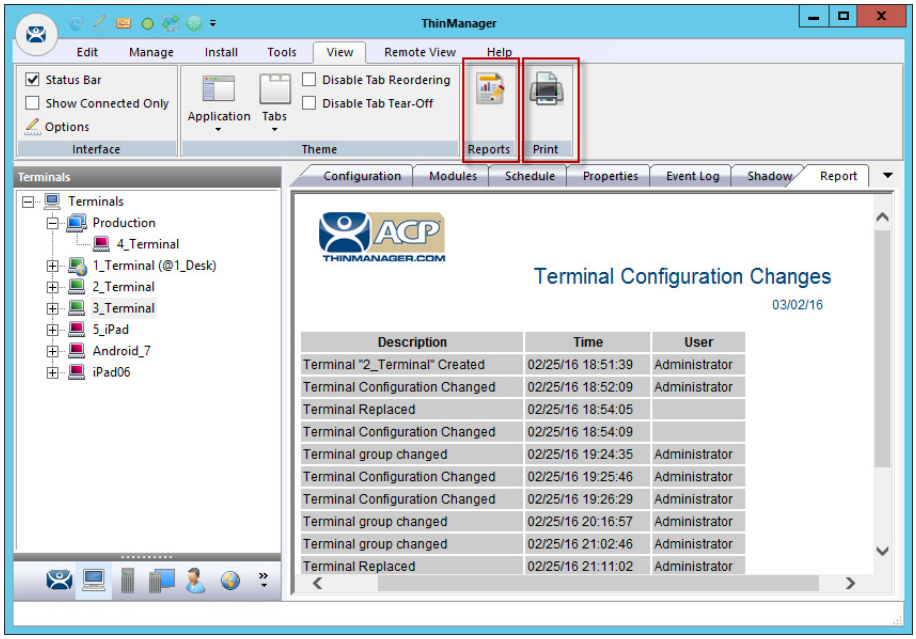
Setting	Description
Terminal Report	Choose the report to display on the Report tab when a Terminal or Terminal group is highlighted.
Remote Desktop Server Report	Choose the report to display on the Report tab when a Remote Desktop Server is highlighted.
ThinManager User Report	Choose the report to display on the Report tab when a ThinManager User or ThinManager User Group is highlighted.

2. Use the pull-down list to select the desired reports.

Report Tab

The reports chosen in the Select Reports dialog box are displayed on the Report tab in ThinManager.

Figure 894 - Report Tab



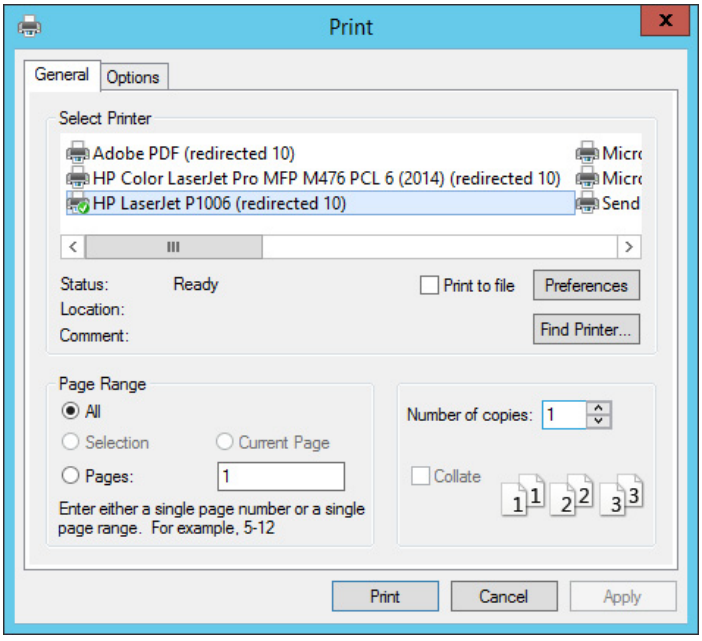
3. Highlight the desired ThinManager Server, Terminal, Terminal group, Remote Desktop Server, or ThinManager user, then click the Report tab to display the report.

Print Report

1. Choose one of the following methods to start the process to print a report.
   a. Click the Report tab and choose View>Print from the ThinManager menu.
   b. Right-click on the report inside of the Details pane.

   The Print dialog box appears with all the printers defined on the ThinManager Server.

Figure 895 - Print Dialog Box



2. Highlight the desired printer and click Print to print the report.

Report Template Installation

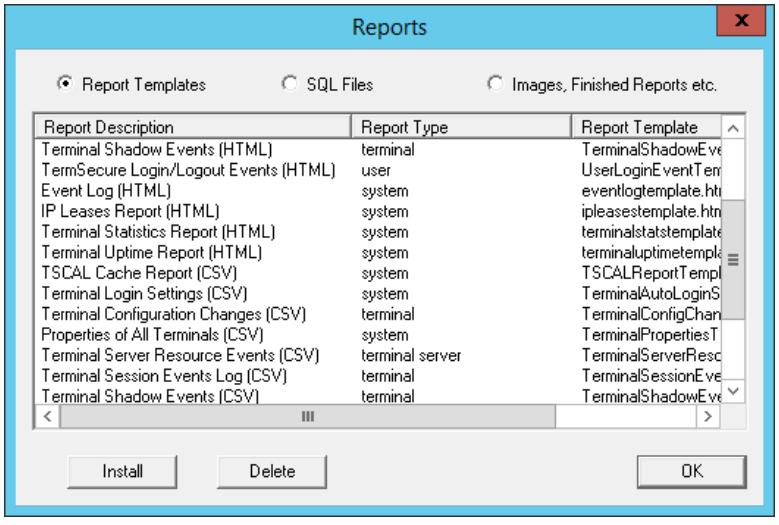
ThinManager installs a number of reports into the ThinManager folder at installation. The default location is C:\Program Files\Automation Control Products\ThinManager\ReportTemplates.

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.

1. Choose Install>Reports from the ThinManager menu to install new reports.

   The Reports dialog box appears.

Figure 896 - Reports

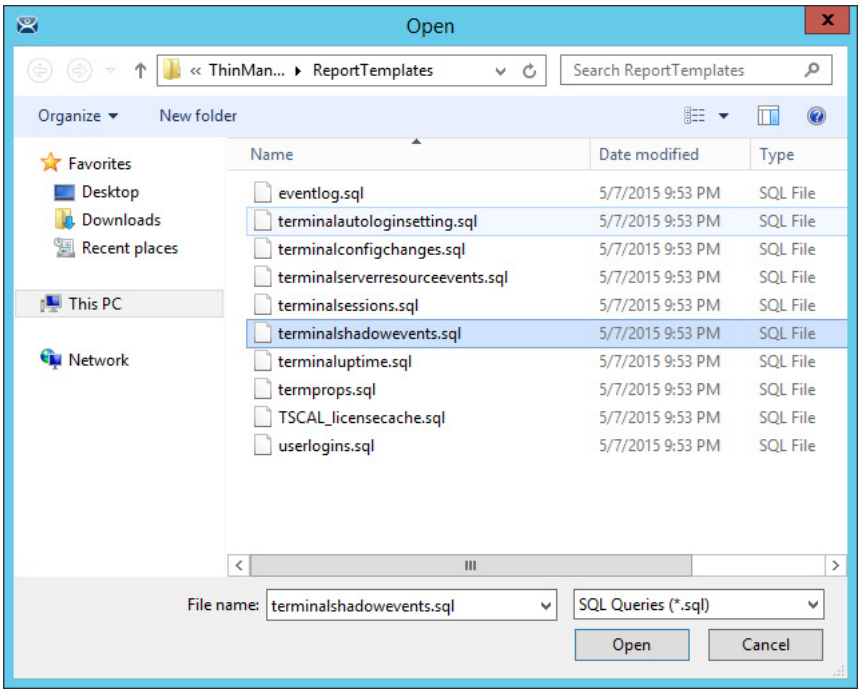


2. Click one of the following radio buttons.

Setting	Description
Report Templates	Click to browse for *.html files.
SQL Files	Click to browse for *.sql files.
Images, Finished Reports, etc.	Click to browse for assorted files.

3. Click Install.

Figure 897 - File Browser



Each report has an *.html or *.CSV component and an *.sql component.

4. Click the Report Templates radio button, browse to the new *.html file, and click Open to install.
5. Click the SQL Files radio button, browse to the new *.sql file, and click Open to install.

   Once these two components are added, the report is available.

Scheduling

Reports can be scheduled to run once at a specified time or regularly at a specific time. The reports are saved as *.html files for storage or further analysis.

Scheduling is available for more than to run reports. Schedules can be created for these items.

- 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 ThinManager User Configuration Wizard

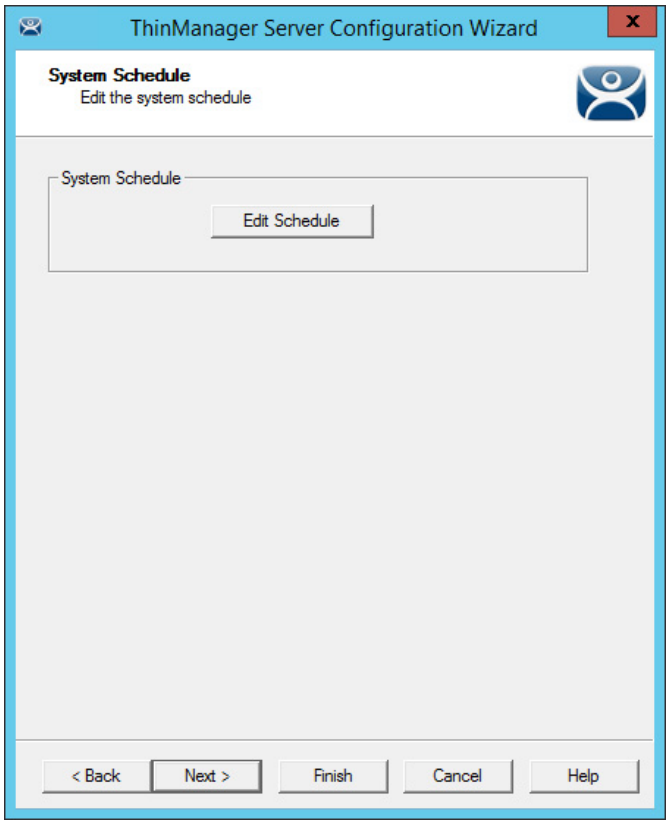
System Scheduling of Reports

Reports are scheduled on the ThinManager Server Configuration Wizard. Follow these steps to schedule report generation.

1. Right-click on the ThinManager Server icon and choose Modify.

   The ThinManager Server Configuration Wizard appears.

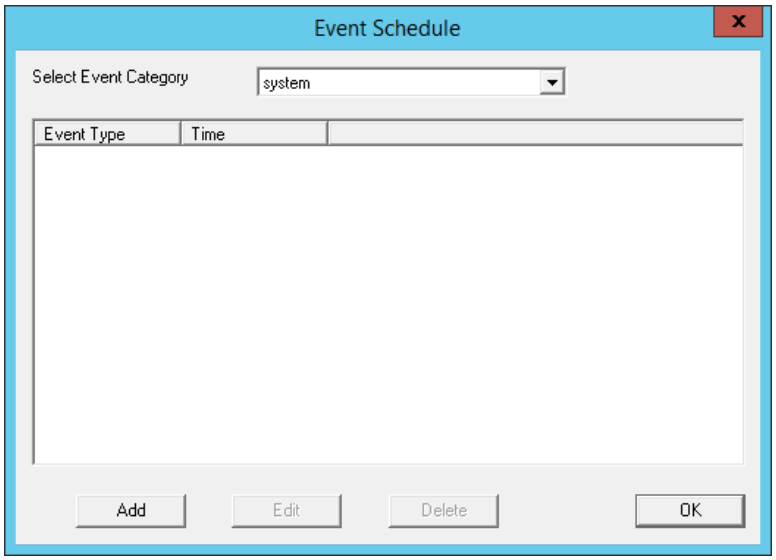
Figure 898 - ThinManager Server Configuration Wizard – System Schedule



2. Click Next until the System Schedule page appears.
3. Click Edit Schedule.

   The Event Schedule dialog box appears.

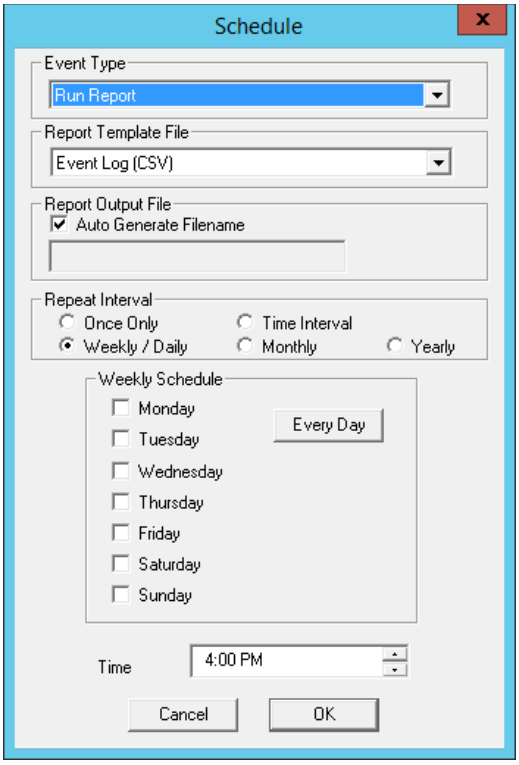
Figure 899 - Event Schedule



4. Click Add.

   The Schedule dialog box appears, which allows system events configuration.

Figure 900 - Schedule Window



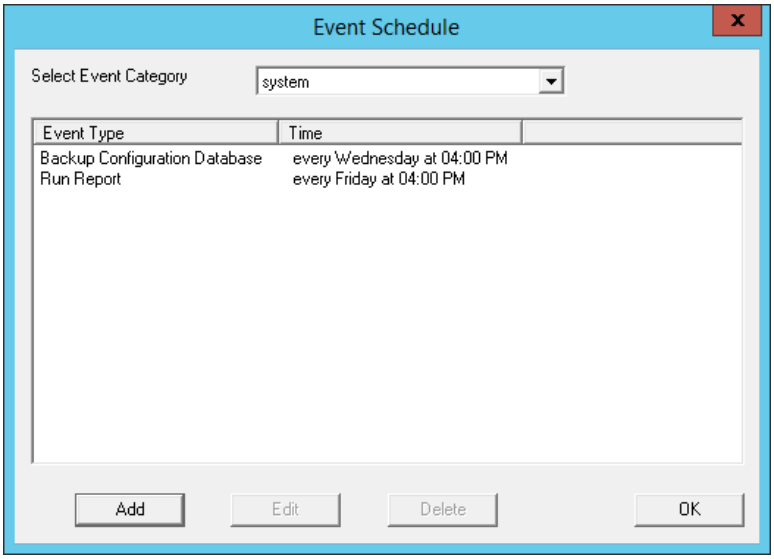
Setting	Description
Event Type	Choose the event.
Backup Biometric Database	Choose to schedule automatic backup of the biometric (fingerprint) data, which is kept in a separate database.
Backup Configuration Database	Allows an automatic schedule of the configuration database.
Run Report	Allows you to run a report and save it as an *.html file on a regular basis.
Report Template File	Allows you to select the type of report and whether to save it as *.html or *.CSV.
Report Output File	Applies the naming convention to the saved reports.
Auto Generate Filename	Check to save the file to the ThinManager folder with the report name and a time stamp as its title. Clear the checkbox to type a desired filename, which must end in .html or *.CSV, depending on the template.
Repeat Interval	Sets the frequency of report generation.
Time	Sets the time of report generation and changes based on the Report Interval. The Time field can allow dates, days, hours, or intervals to be set for the report.

There are a few changes that allow the filename to be modified with a timestamp for identification purposes. If you do not use a timestamp, the file is 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

5. Once the report is configured, click OK to accept the report schedule.

Figure 901 - Event Schedule

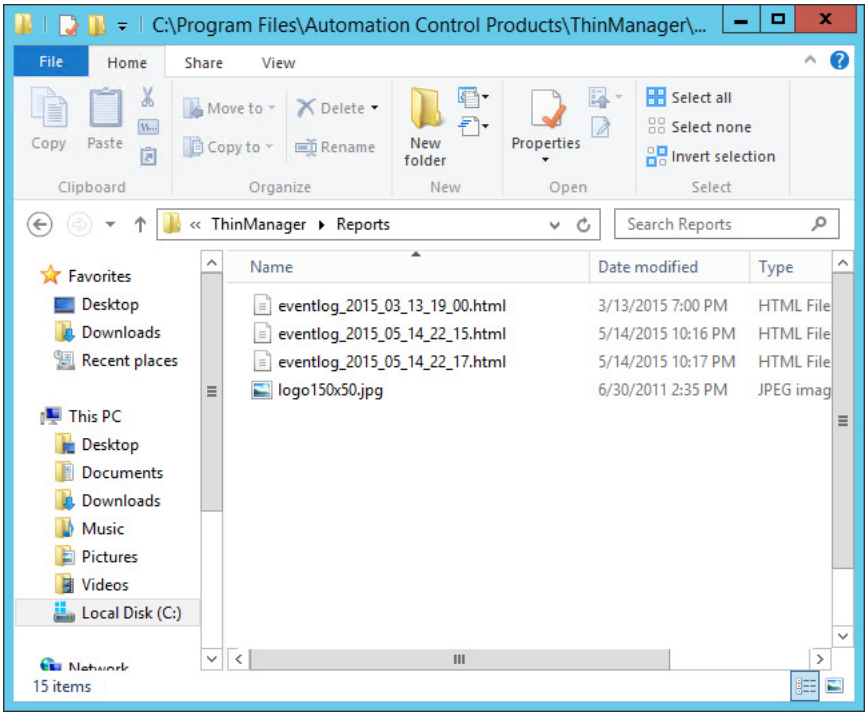


The scheduled report is displayed in the Event Schedule dialog box.

Setting	Description
Add	Adds another report schedule.
Edit	Edits the schedule of a highlighted report.
Delete	Deletes the schedule of a highlighted report.
OK	Accepts the schedules and closes the dialog box.

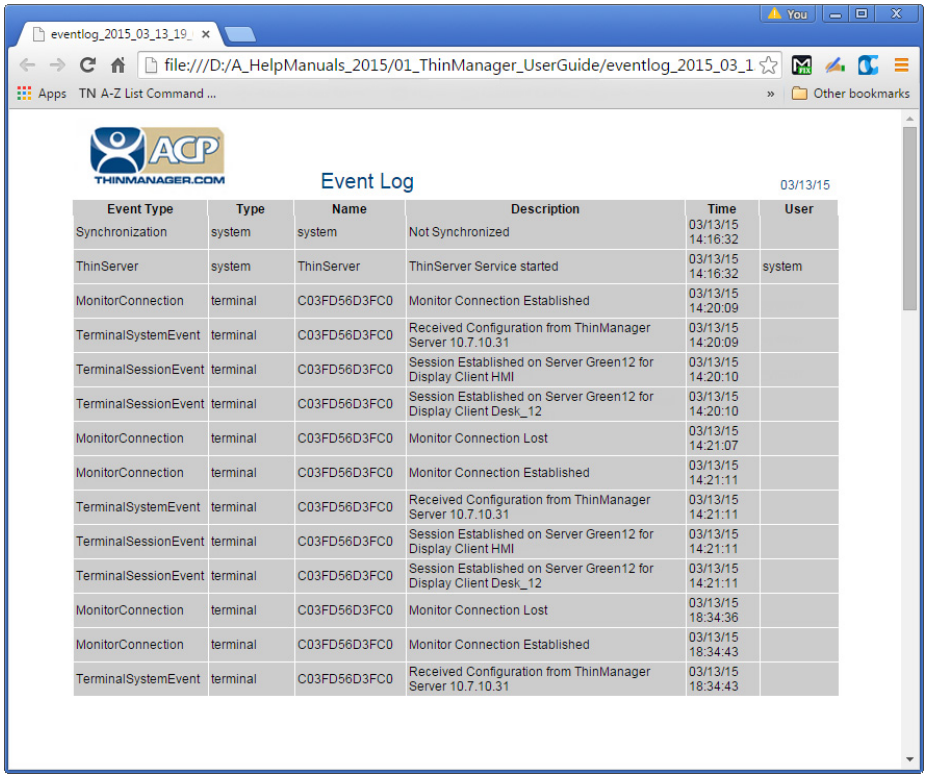
When a report is run, the files are saved to be viewed.

Figure 902 - Saved Reports



Once the report is run, it can be opened in a web browser if it is in *.HTML format or in a spreadsheet application if in*.CSV format.

Figure 903 - Report Shown in Browser



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	

Once the report is generated the data can be saved or reformatted, as desired, using standard HTML tools.

Schedule Configuration Backups

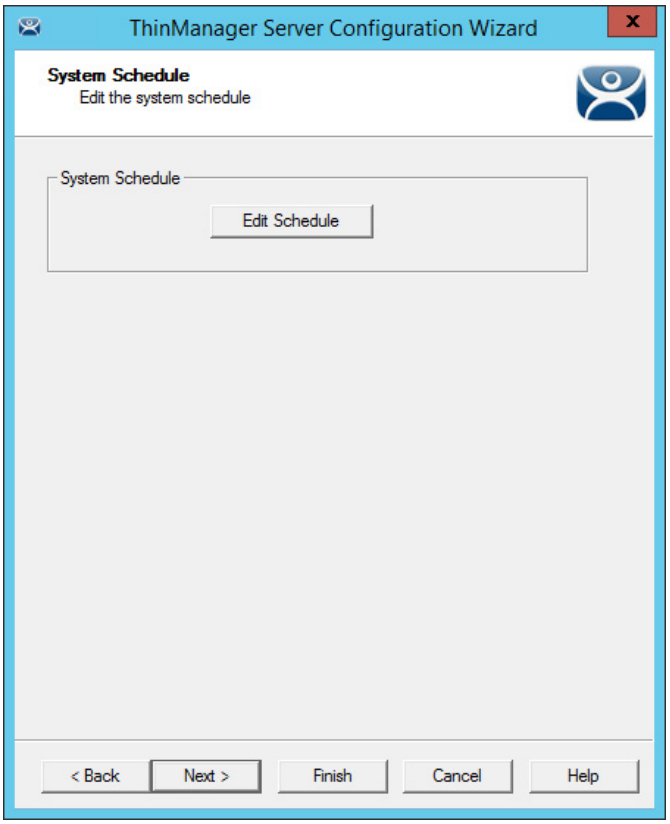
It is a good idea to back up your ThinManager configuration before you make any major changes. You can use the Scheduler to do this automatically.

To schedule report generation, follow these instructions.

1. Right-click the ThinManager Server and choose File>Modify.

   The ThinManager Server Configuration Wizard appears.
2. Click Next until the System Schedule page appears.

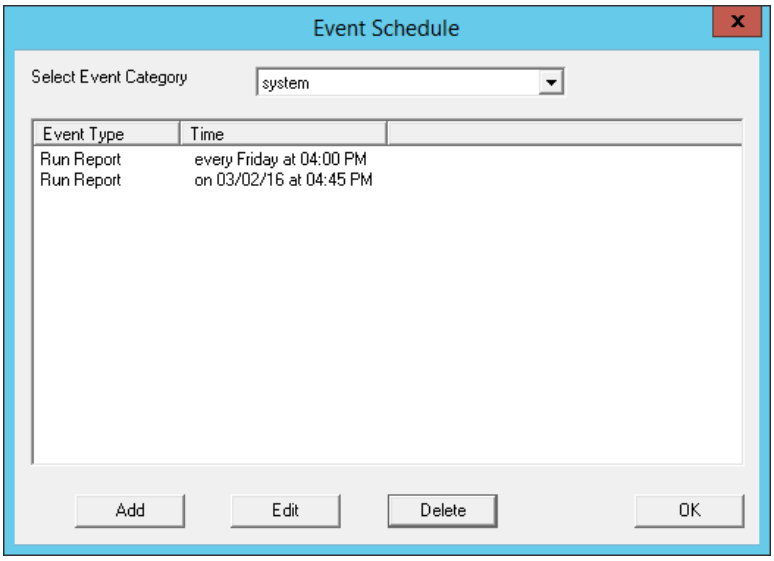
Figure 904 - System Schedule Page



3. Click Edit Schedule.

   The Event Schedule dialog box appears.

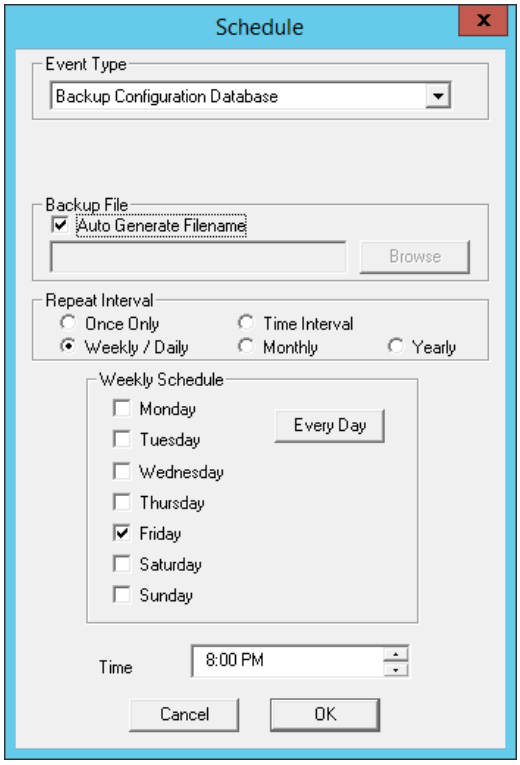
Figure 905 - Event Schedule



4. Click Add.

   The Schedule dialog box appears, which allows system events, like configuration backups, to be created.

Figure 906 - Schedule Dialog Box



Create a system event based on these settings.

Setting	Description
Event Type	Choose Backup Configuration Database from the pull-down menu.
Repeat Interval	Click Weekly/Daily.
Weekly Schedule	Check a day.
Time	Choose a time.

5. Click OK to accept the changes.

A weekly backup allows you to have a current configuration available in case you need one.

Notes:

TermMon ActiveX

ActiveX can be used to monitor and provide useful information about client hardware. TermMon (Terminal Monitoring) ActiveX can be embedded into an application that runs on the Remote Desktop Server. When a Terminal starts a session on the server and launches the application with TermMon ActiveX, ActiveX creates a socket connection to the Terminal and the session. ActiveX is able to pull data from the Terminal into the application using the events, methods, and properties that are provided by TermMon.

TermMon Active X is commonly used by customers that have Automation HMI products. 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 Location Services, the main use case is for Location. Once a mobile device resolves 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 HMIs and want to control access to pages, security, and other things based on the Location.

One other Location Services 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, the feature could be added to a button to run a pump. Prior to the command to run, an event can be triggered that prompts the Operator to scan a code. The operator then scans a QR Code, which returns a result to the HMI. Then, the code on the button determines if it can provide the command to run the pump based on whether it received the expected information from the Location via the ActiveX.

The ActiveX also contains properties that allow you to Logon or Logoff (Enter or Exit) of a Location via ActiveX. This tells the session which Location to log in to by passing a string to the appropriate ActiveX property. The Logoff item is the same as the Leave button that is part of the iTMC application.

Register the Control

The TermMon ActiveX Control can be found on the ThinManager CD as `termmon.ocx`. Also, it is 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>`.

Read-only Properties

The following properties are read-only strings. An event is generated any time one of these properties changes. The Enable method must be invoked prior to reading these properties.

Property	Description
TerminalName	Name of the Terminal.
TerminalModel	Terminal model number.
TerminalIP	Terminal IP address.
TerminalMAC	Terminal MAC address.
TerminalBootLoaderVersion	Terminal network boot loader version.
TerminalFirmwareVersion	Firmware version that the Terminal runs.
TerminalWindowsUsername	Windows Username that is specified in the Terminal's ThinManager configuration.
TermSecureUsername	TermSecure username of the TermSecure user currently logged on to the Terminal. If no TermSecure user is logged on, this value is blank.
TermSecureWindowsUsername	Windows Username associated with a TermSecure user and all TermSecure user sessions. If no TermSecure user is logged on, this value is blank.
TerminalServerGroupList	A comma-separated list of Display Clients currently run on the Terminal.
ConnectionState	The Control's connection state with the Terminal.
CurrentTerminalServerGroup	The Display Client that is currently displayed on the Terminal.
CurrentWindowsUsername	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	Name of the Remote Desktop Server where the Control runs. This property is not available when the RunInSession property is set to False.
UserID	Identifier associated with a TermSecure user; for example, the number of a security badge used by a TermSecure user when the badge is scanned. Use of this property may require the "Expose ID" setting to be enabled in the appropriate ThinManager module, such as RFIdeas pcProx USB Module.
RelevanceLocationName	The complete path and name of the current Location.
ScanResult	Contains the result of the Command Method Scan Code commands.
BiometricData	Contains the raw data returned from a biometric scan. The format of this data is determined by the Biometric module as configured on the Terminal.
BiometricLookupResult	Contains 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	Contains the TermSecure username when the result of the ScanBiometricAndQueryUser command is successful.

Read-Write Properties

These properties can be set by the application.

Property	Description
RunInSession	When the RunInSession property is set to True, the Control runs in the Terminal's Remote Desktop Services session. The Terminal IP Address is determined automatically by the control.
OverrideIP	If the RunInSession property is set to False, the OverrideIP property specifies the IP Address of the Terminal to which the Control connects.(1)
WatchdogTime	The number of seconds before the watchdog resets 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.(2)
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.

(1) 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.

(2) The Enable Method does not need to be called for watchdog operation. Watchdog operation is independent of the Enable and Disable Methods.

Events

When a property value changes, an event is 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

Methods

Method	Description
Enable	Invoke this method to enable the Control. The Control attempts to connect to the Terminal and generates events to update the Control Properties. The Control maintains a connection to the Terminal as long as it is enabled.
Disable	Invoke this method, which causes the Control to break the connection with the Terminal. Events are 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 (aside for noted exceptions). The supported commands follow.
Reboot	Initiates a Terminal reboot.
Restart	Initiates a Terminal restart.
Calibrate	Initiates a touch screen calibration.
GotoMainMenu	Causes the Main Menu to be displayed.
SwitchToNextGroup	Switches to the next Display Client.
SwitchToPrevGroup	Switches to the previous Display Client.
SwitchInstFailover	Switches the instant failover group.
ChangeTermSecureUser	Disconnectes any current TermSecure user sessions, and then displays the TermSecure Log On menu.
LogOffAndChangeTermSecureUser	Logs off any current TermSecure user sessions, and then displays the TermSecure Log On menu.
LogOffTermSecureUser	Logs off any current TermSecure user sessions and returns to a Display Client, which is assigned to the Terminal. If no Display Clients are configured on the Terminal, the TermSecure Log On menu is displayed.
DisconnectTermSecureUser	Disconnects any current TermSecure user sessions and returns to a Display Client, which is assigned to the Terminal. If no Display Clients are configured on the Terminal, the TermSecure Log On menu is displayed.
DisconnectSession	Disconnects the Remote Desktop Services Session on the Terminal. This command does not require that the Enable Method is invoked prior to execution.
LogOffSession	Logs off the Remote Desktop Services Session on the Terminal. This command does not require that the Enable Method is invoked prior to execution.
TileStart	Tiles the Display Clients on the current Screen.
TileEnd	Untiles the Display Clients on the current Screen.
ScanCodeReturnData	Prompts the user to scan a QR Code or Barcode. After the scan is complete, the scan data is returned in the ScanResult property.
ScanCodeAndQueryLocation	Prompts the user to scan a QR Code or Barcode. After the scan is complete, the location path and name is returned in the ScanResult property.
ScanBiometricAndQueryUser	Sends the next Biometric scan to ThinServer and returns the associated TermSecure Username. The result of the operation is returned in the BiometricLookupResult property. Upon a successful result, the TermSecure username is returned in the BiometricLookupUsername property.
SendGenericEvent	Sends an event expression as a string type parameter to ThinServer. Once received by ThinServer, a ThinManager Event with an expression matching the generic event executes the configured ThinManager Event Action.

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
- TermMonCommand.SendGenericEvent

Method	Description
ChangeTerminalServerGroup	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	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	User is not a member of the specified TermSecure Access Group.
TermMonConst.ValidMember	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	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	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	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	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	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	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	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.

Method	Description
CameraOverlaySwitchPrev	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	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	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	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	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	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	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	Used to log into a 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	Log the device out of the current location.
GetCustomVariable	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.

Control Constants

Constant values provided by the Control are as follows.

TermMonEvent

Constant	Value
TerminalName	1
TerminalModel	2
TerminalIP	3
TerminalMAC	4
TerminalBootLoaderVersion	5
TerminalFirmwareVersion	6
TermSecureWindowsUsername	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

Constant	Value
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

Constant	Value
Success	1
Fail	2
Disconnected	3
Connected	4
Timeout	5
Busy	6
Updating	7
RequestFailed	8
InvalidMember	9
ValidMember	10
UserNotFound	11
GroupNotFound	12
BadPassword	13
NoPermission	14
PasswordChangeReq	15
NoWindowsUsername	16
NoWindowsPassword	17

TermMonRelevance

Constant	Value
ActionNone	0
ActionTransfer	1
ActionClone	2
ActionShadow	3

The following terms and abbreviations are used throughout this manual. For definitions of terms not listed here, refer to the Allen-Bradley Industrial Automation Glossary, publication AG-7.1.

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

Basic Service Set Identifiers (BSSID) Describes sections of wireless local area network, or WLAN. Recognizes the access point or router because it has a unique address, which creates the wireless network.

Content The data, sessions, or information 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. Deployed as Display Clients.

Dynamic Host Configuration Protocol (DHCP) A network protocol that enables a server to automatically assign an IP address to a computer from a defined range of numbers.

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

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

Global Positioning System (GPS) A U.S.-owned utility that provides users with positioning, navigation, and timing (PNT) services.

Installation ID An identifier used in licensing, found near the bottom of the Licensing dialog box. Choose Install>Licenses to launch the Licensing dialog box.

Location A configured element that is used as an endpoint 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.

MAC Address Media Access Control address, a unique identifier assigned to a network interface controller for use as a network address in communications within a network segment.

Mobile Device Apple®, Android®, or Windows® device that has the appropriate ThinManager application installed and configured so that it can interact with the ThinManager Platform through Relevance.

Preboot Execution Environment (PXE) A standardized client-server interface that allows networked computers that are not yet loaded with an operating system to be configured and booted remotely by an administrator.

Relevance A function of ThinManager that controlled access to applications and assets through Location or User Permissions. Deprecated with version 13.

Relevance ID The unique ID and name assigned to a new resolver device when it was added to the system. Deprecated with version 13.

Remote Desktop Protocol (RDP) Microsoft's proprietary protocol that provides a user with a graphical interface to connect to another computer over a network connection.

Remote Desktop Server (RDS) A 2008 R2 or later terminal server.

Resolver A Bluetooth® beacon, GPS, iBeacon, QR code, or Wi-Fi access point that a mobile device uses to identify a particular area.

Resolver Actions The functions that are authorized on a mobile device by a resolver, which include Shadow, Transfer, Forced Transfer, and Clone.

SmartSession Provides load balancing between member remote desktop servers. This feature uses CPU availability, memory usage, and session count on the remote desktop servers to determine the load on the servers. ThinManager polls the server every eight seconds to maintain accurate status levels. Thin clients connect to the Remote Desktop Server with the most available resources. When SmartSession is not used, polling is turned off by default.

TermCap Terminal Capability, a software library and database that enables programs to use display terminals in a terminal-dependent manner; describes the capabilities of hundreds of different display terminals in great detail.

Terminal A client that connects to a server.

Terminal Server A computer that acts like a mainframe, allowing clients to log in, start sessions, and run apps on the server but display the results on a terminal.

TermSecure The former name for the security component of ThinManager that grants or denies access to content in Relevance, which was deprecated with version 13. Now, ThinManager User Services.

Thin client Also, Zero client. A terminal without a hard drive that connects to a server.

ThinManager The graphic user interface component of the ThinManager system used to control and configure the ThinServer database.

ThinManager Server A computer running the ThinManager interface and the ThinServer service.

ThinManager User Services See TermSecure.

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

Unified Extensible Firmware Interface (UEFI) New BIOS format for ThinManager Compatible PXE boot thin clients. It requires Port UDP-4011 open.

Uniform Resource Locator (URL) Web address of a resource on the Internet or a locally stored file. The resource can be any type of file stored on a server, such as a Web page, a text file, a graphics file, or an application program.

Zero client See Thin client.

Rockwell Automation Support

Use these resources to access support information.

Technical Support Center	Find help with how-to videos, FAQs, chat, user forums, and product notification updates.	rok.auto/support
Knowledgebase	Access Knowledgebase articles.	rok.auto/knowledgebase
Local Technical Support Phone Numbers	Locate the telephone number for your country.	rok.auto/phonesupport
Literature Library	Find installation instructions, manuals, brochures, and technical data publications.	rok.auto/literature
Product Compatibility and Download Center (PCDC)	Download firmware, associated files (such as AOP, EDS, and DTM), and access product release notes.	rok.auto/pcdc

ThinManager Website	Visit the ThinManager website to download resources for your ThinManager solution.	https://thinmanager.com/

Documentation Feedback

Your comments help us serve your documentation needs better. If you have any suggestions on how to improve our content, complete the form at rok.auto/docfeedback.

Waste Electrical and Electronic Equipment (WEEE)

At the end of life, this equipment should be collected separately from any unsorted municipal waste.

Rockwell Automation maintains current product environmental information on its website at rok.auto/pec.

Allen-Bradley, expanding human possibility, FactoryTalk, ThinManager, and Rockwell Automation are trademarks of Rockwell Automation, Inc.
Android and Google Play are trademarks of Google LLC.
Apple, App Store, iPad, and iTunes are trademarks of Apple Inc.
Bluetooth is a trademark of Bluetooth SIG, Inc.
Docker is a trademark of Docker, Inc.
Ethernet is a trademark of Fuji Xerox Co., Ltd.
EtherNet/IP is a trademark of ODVA, Inc.
iOS is a trademark of Cisco Systems, Inc.
VMware vCenter is a trademark of VMware, Inc.
Windows is a trademark of Microsoft Corporation.
Trademarks not belonging to Rockwell Automation are property of their respective companies.

Rockwell Otomasyon Ticaret A.Ş. Kar Plaza İş Merkezi E Blok Kat:6 34752, İçerenköy, İstanbul, Tel: +90 (216) 5698400 EEE YÖnetmeliğine Uygundur

Connect with us.

rockwellautomation.com — expanding **human possibility**™

AMERICAS: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel: (1) 414.382.2000, Fax: (1) 414.382.4444
EUROPE/MIDDLE EAST/AFRICA: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgium, Tel: (32) 2 663 0600, Fax: (32) 2 663 0640
ASIA PACIFIC: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel: (852) 2887 4788, Fax: (852) 2508 1846

Publication TM-UM001K-EN-P - May 2025
Supersedes Publication TM-UM001J-EN-P - June 2024

Copyright © 2025 Rockwell Automation, Inc. All rights reserved. Printed in the U.S.A.