THE WORLD'S MOST POWERFUL THIN CLIENT MANAGEMENT PLATFORM

Relevance Deployment Guide

ThinManager 8

Revision 1 — January 15, 2015

David Gardner & Paul Burns

Table of Contents

1. Purpose of Relevance

Download the latest revision from http://www.thinmanager.com/support/manuals/

Traditional computing is device-based. Content is generated and processed on a specific device. With PCs the content is generated at each PC. With terminal services the content is generated on central servers and deployed to client devices.

Relevance introduces location-based computing. All of the content and applications are generated and deployed to a location. This location can have a specific assigned device at that location or have the content accessed by a mobile device.

There are two types of locations in Relevance, **Assigned** and **Unassigned**.

Assigned locations are locations that have a terminal and monitor at the given location, much like traditional computing. Relevance adds additional functions to the location that allows mobile devices to interact with the location and **Shadow**, **Clone**, or **Transfer** the control of location based content to the mobile device.

Unassigned locations are locations that lack a permanent terminal and monitor and all of the content is delivered to the mobile device.

Relevance is an extension of ThinManager and adds a new feature set to ThinManager when a Relevance license is added to a ThinManager 7.0 XLi license. It is helpful to know and understand ThinManager before deploying or converting to a Relevance system. Please see the ThinManager documentation for details on ThinManager at http://www.thinmanager.com/support/manuals/.

1.1. Purpose of this Document

The purpose of this document is to help system integrators and end users understand the architecture and design elements needed for a Relevance system. It will help guide the choices in the setup of locations, resolvers, and application access.

1.2. Glossary of Terms

These definitions will help explain the components of Relevance. More details and descriptions will be provided throughout the guide.

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

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

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

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

Mobile Device - Mobile devices are Apple or Android devices have the appropriate ACP ThinManager application installed and configured.

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

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

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

ThinManager - ThinManager is the graphic user interface component of the ThinManager system.

TermSecure - TermSecure is a security component of ThinManager whose functionality has been expanded in Relevance. It grants or denies access to content. When a Relevance license is applied to ThinManager the TermSecure elements, like TermSecure Users, become Relevance elements.

ThinServer - ThinServer is the Windows service of the ThinManager system. It runs as a Windows Service and is responsible for the main functions of the ThinManager System. ThinManager hardware will communicate with this service in order to receive their firmware, configuration, and to get information related to their Relevance setup.
The ThinManager interface connects to this service to view and edit the configuration.

2. Pre-Deployment Decisions

Before deploying Relevance you need to plan what the goals and outcome should be.

- What content do you want to deliver?

  This is normally an application from a terminal server but can be camera output, shadows of other terminal, or workstation desktops.

- Where should this content be delivered, a dedicated terminal, a mobile device, or both?

  Relevance can deliver information to a location that is assigned to a dedicated terminal or it can deliver content to an unassigned location that requires a mobile device for viewing.

- Who should be able to view the content? Should group restrictions be applied?

  The content can be made available to all operators and users or it can be restricted with access groups to be shown only to group members with valid permissions.

- How do you resolve the location? Do you use passive resolvers like Bluetooth or GPS or will you use an active scan of QR codes?

  Bluetooth, Wi-fi access points, and GPS can be set up as location resolvers so when a mobile device enters the range it notifies the system of the new location.

  QR codes can be created that resolve the location when the user scans the QR code with their mobile device.

- Has wireless access be deployed to the areas that you need?

  You don't need wall-to-wall WiFi coverage, just coverage for the positions you want to run your mobile devices.

3. Deployment Summary

- ❑ Install and license the ThinManager Platform with ThinManager XLi licenses and Relevance licenses.
- ❑ Configure the terminal servers and cameras to deploy the content.
- ❑ Define the Display Clients to deliver content and applications.
- ❑ Configure and connect a mobile device to add location resolvers.
- ❑ Create and define the Resolvers.
- ❑ Define your Locations in ThinManager.
- ❑ Add Resolvers to the Locations using the configuration wizards.
- ❑ Configure locations to include assigned terminals and associate the hardware to the Location.
- ❑ Configure the unassigned Locations.
- ❑ Create Access Groups. Create Users and apply permissions using access groups.
- ❑ Add your wireless infrastructure where you want to use the mobile devices.

4. ThinManager Installation and Licensing

This follows the methods from ThinManager.

- ❑ Install or upgrade to ThinManager 7.0 or later.
- ❑ Create a Master License on the ThinManager License Activation web site at http://www.thinmanager.com/licensing/ .
- ❑ Add enough XLi licenses for each terminal and mobile device.
- ❑ Add a Relevance license to the Master license.
- ❑ Activate the Master License with the Installation ID. The Installation ID is found on the Licensing window that is opened by selecting ***Install>Licenses*** on the ThinManager menu bar.
- ❑ Download the master license file and install it in ThinManager using the ***Install License*** button on the Licensing window.

5. Define Sources

This follows the methods from ThinManager.

- ❑ Build your Windows servers, using either 2008, 2008 R2, or 2012.
- ❑ Add the terminal services or remote desktop roles from the Windows Server Manager.
- ❑ Create a unique Windows user account for each location and mobile device. Add them to the Remote Desktop Services group.
- ❑ Define your terminal servers as Display Servers in ThinManager. Open the Display Server branch, right click on the Terminal Servers branch, and select ***Add Terminal Server***.

- ❑ Add an administrative account in the User name and Password fields of the **Terminal Server Name** page of the **Terminal Server Wizard**. This allows ThinManager to access data from the terminal server.

6. Define Content

This follows the methods used in ThinManager.

- ❑ Install your applications on your Windows Terminal Servers using the Install Mode. This can be entered by:
    - Selecting the ***Install Application on Terminal Server*** icon from the **Control Panel** on Server 2008
    - Selecting the ***Install Application in RDS*** icon from the **Control Panel** on Server 2012
    - Typing **`change user /install`** at a command prompt. You can then run the setup.exe to install your application. Type **`change user /execute`** when finished installing to leave the Install Mode.
- ❑ Define your applications as Display Clients in ThinManager. Open the Display Client branch, right click on the Terminal Services branch, and select ***Add Display Client*** to launch the wizard.
- ❑ The **Terminal Services and Workstation Options** page allows you to configure the application deployment.
    - ***Allow Auto-Login*** lets the application start automatically using the location or terminal user account. Un-select this if you want a manual login to the session.
    - ***Application Link*** allows you to specify a single application for the session. Un-selecting this will start a desktop.
    - ***SmartSession*** activates ThinManager load balancing.
      You need to have the ***Available for Display Clients using SmartSession*** checkbox on the **Terminal Server Capabilities** page of the **Terminal Server Configuration** wizard selected if you want a server to be used in SmartSession load balancing
    - ***Enforce Primary*** will designate the top terminal server in your list of terminal servers as the primary server and will try to connect to its original terminal server if that terminal server has failed and recovered. This is not available if SmartSession is selected.
- ❑ The **Display Client Members** page allows you to select what terminal servers you want to use as the source for the content.
- ❑ The **AppLink** page allows you to specify a single application to run in the session. This allows you to control what content is sent to the user.

7. Mobile Devices

Mobile devices are configured as terminals using the methods used in ThinManager.

7.1. Configuration in ThinManager

Relevance requires a mobile device like an Apple iPad or Android device.

- ❑ Configure an iPad as a terminal in ThinManager with ***Apple/iPad*** as the **Make/Model** or an Android device as ***GENERIC/Android*** on the **Terminal Hardware** page of the **Terminal Configuration Wizard**.
- ❑ Check the ***Use Display Clients***, ***Enable Relevance User Services***, and ***Enable Relevance Location Services*** on the **Terminal Mode Selection** page.
- ❑ Entering a default display client on the **Display Client Selection** page is optional. It can receive its display clients when it enters a location.
- ❑ Check which resolver types you want to use on the **Relevance Options** page.
  A mobile device does not need to have a location assigned but can assume a location through resolvers.
- ❑ Add a unique Windows user account on the **Log In Information** page.

7.2. Configuration on Mobile Device

- ❑ Install the ThinManager iTMC app on the iPad from the Apple App Store. You can search for iTMC or ThinManager and choose the iTMC program from Automation Control Products.
- ❑ Install the AndroidTMC app from the ThinManager web site or the Google Android store.
- ❑ Launch the app and select the ***Setting*** button to open the **Setting** page.
- ❑ Define your ThinManager Server by selecting ***Add ThinManager Server*** and entering the ***Name*** and ***IP address***, and selecting the ***Save*** button.
- ❑ Associate the mobile device with the configuration you created by selecting the defined ThinManager Server from the main menu, connecting to the ThinManager Server, and selecting the name of the configuration you created.

The mobile device is ready to register resolvers.

8. Register Resolvers

There are several Resolvers in Relevance.

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

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

8.1. QR Codes

- ❑ Open the iTMC app and select the ***Settings*** button at the bottom of the screen.
- ❑ Select the ***Register QR Code*** command in the **Relevance Resolver** section.
    - If you have a single ThinManager Server it will open a camera window.
    - If you have two or more ThinManager Servers defined you will be asked which ThinManager Server you want the resolver registered on. Select the correct ThinManager Server and a camera window will open.
- ❑ Point the camera window at the QR Code. After a successful scan it will ask for a name for the resolver. Enter a name and select ***Register***.
- ❑ A dialog box will confirm a successful QR code registration.
- ❑ Repeat as needed.

8.2. Bluetooth Beacons

- ❑ Open the iTMC app and select the ***Settings*** button at the bottom of the screen.
- ❑ Select the ***Register Bluetooth Beacon*** command in the Relevance Resolver section.
    - If you have a single ThinManager Server it will open a **Register Bluetooth** window.
    - If you have two or more ThinManager Servers defined you will be asked which ThinManager Server you want the resolver registered on. Select the correct ThinManager Server and a **Register Bluetooth** window will open.
- ❑ Bluetooth beacons in range will show a **Received Signal Strength Indication (RSSI)** number.
    - Because of the low strength of the signals the reading is shown as a negative number with the higher number (lower integer) as the nearer unit.
      For example, -42 would be closer than -65 which is closer than -92.
    - ACP programmed beacons will contain an ACP prefix.
- ❑ A dialog box will ask for you to stand at the entrance to the zone (***Stand at Zone Entrance***) to establish the base level of the entrance signal. Enter a Location description for the Bluetooth Beacon in the dialog box and click ***OK***. A success message will be displayed if accepted.
- ❑ The exit strength is set automatically with a 10 dBm offset. This can be changed in ThinManager in the ***Resolver Settings*** on the **Relevance Resolver** page of the **Location Configuration** wizard.
- ❑ Repeat as needed.

8.3. GPS

- ❑ Open the iTMC app and select the ***Settings*** button at the bottom of the screen.
- ❑ Select the ***Register GPS Location*** command in the Relevance Resolver section.
    - If you have a single ThinManager Server it will open a **Register Location** window.
    - If you have two or more ThinManager Servers defined you will be asked which ThinManager Server you want the resolver registered on. Select the correct ThinManager Server and a **Register Location** window will open.
- ❑ The **Register Location** screen will list the ***Latitude***, ***Longitude***, and ***Altitude*** of the device.
- ❑ Select the ***Tap Here to Register Location*** command to register the location.
- ❑ Enter a description in the dialog box and select ***OK*** to complete the registration. A success message will be displayed if accepted.
- ❑ The location radius is set automatically to 65 meters. This can be changed in ThinManager in the ***Resolver Settings*** on the **Relevance Resolver** page of the **Location Configuration** wizard.
- ❑ Repeat as needed.

8.4. Wi-Fi Access Points

- ❑ Open the iTMC app and select the ***Settings*** button at the bottom of the screen.
- ❑ Select the ***Register WiFi Access Point*** command in the Relevance Resolver section.
    - If you have a single ThinManager Server it will open a **Register Access Point** window.
    - If you have two or more ThinManager Servers defined you will be asked which ThinManager Server you want the resolver registered on. Select the correct ThinManager Server and a **Register Access Point** window will open.
- ❑ Wi-Fi access points in range will show a Basic service set identification (BSSID). This is the unique identifier for the access point.
- ❑ Select the ***Tap Here to Register*** command to register the access point.
- ❑ Enter a description in the dialog box and select ***OK*** to complete the registration. A success message will be displayed if accepted.
- ❑ Repeat as needed.

9. Create Locations

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

- ❑ Open the **Locations** branch by selecting the **Globe *Location*** icon in the **Tree Selector** at the bottom of the tree.
- ❑ Right click on the globe ***Locations*** icon in the tree and select ***Add Location*** to open the **Location Configuration Wizard.**

- ❑ Name the location on the **Location Name** page.
- ❑ Select options on the Location Options page including manually selected functions allowed.
    - ***Inactivity Timeout –*** A Relevance user will be logged off after this interval if inactive.
    - ***Relevance ID Signal Loss Timeout –*** This is the interval before a Relevance user is logged off due to lack of a signal.
    - ***Activate Display Client at Log In –*** This brings the display client to the forefront when the Relevance user logs in.
    - ***Enforce Location Fencing –*** This controls access in an area with nested locations. If local fencing is enforced the user has to be within the fence to access the sub-locations.
    - ***Inherit from parent Locations –*** This allows nested sub-locations to inherit the parent display clients.
    - ***Allow Local Access –*** This allows a Relevance user to access the location from that location. Unchecking this will only allow remote access.
    - ***Allow Remote Access -*** This allows a Relevance user to access the location from a remote site. Unchecking this will only allow access at the location.
    - ***Reset Cloned Sessions on Logout –*** This will reset any cloned sessions once they are disconnected.
    - ***Allow Location to be selected manually –*** This allows a location to be manually selected. Unchecking this will require the Relevance user to use a Resolver like QR Codes, Wi-Fi, or Bluetooth to initiate the location access. If this is selected checkboxes appear to allow selection of the three basic interactions – ***Shadowing***, ***Transferring***, and ***Cloning***.
- ❑ Add the display clients you want to use at the location on the **Display Client Selection** page.
- ❑ Each location needs a unique Windows user account added on the **Windows Log In Information** page. Enter a username and password in the *User Name* and *Password* fields. You can select an existing user from Active Directory by checking the *Active Directory User* checkbox and selecting the *Search* button. This will allow you to use a Windows domain account for the Location.
- ❑ Resolvers are added on the **Relevance Resolver Selection** page. This provides a way for the mobile device to authenticate to a location.
  See **Associating Resolvers to Locations and Actions** at Section 12.
- ❑ Create a terminal using the Terminal Configuration Wizard for each location that will have an assigned terminal. Add the location to the terminal to utilize the display client and user account instead of assigning them to the terminal itself.

  See **Adding a Terminal to a Location – Upgraded System** at Section 10 or see **Adding a Terminal to a Location – New System** at Section 11.

10. Adding a Terminal to a Location – Upgraded System

Relevance delivers content to a location.

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

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

- ❑ Highlight the **Terminal** icon in the ThinManager tree to open the **Terminal** branch.
- ❑ Double click on the terminal that you want to convert to using a location to open the **Terminal Configuration Wiz**ard.
- ❑ Navigate to the **Terminal Mode Selection** page. Select ***Enable Relevance Location Services*** to use locations.
  The optional ***Enable Relevance User Services*** will allow you to use access groups to control application deployment.
- ❑ Remove Display Clients from the ***Selected Display Client*** list on the **Display Client Selection** page. The display clients will be deployed via the location and not the terminal.
- ❑ Assign the location to the terminal by selecting the ***Change*** button on the **Relevance Options** page and selecting a created location from the **Select Location** popup window.
- ❑ Remove Windows user account from the ***Windows Log In Information*** fields on the **Log In Information** page. The user account will be deployed via the location and not the terminal.
- ❑ Select the ***Finish*** button to accept the changes.

11. Adding a Terminal to a Location – New System

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

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

- ❑ Do not enter a Windows user account in the ***Windows Log In Information*** fields on the **Log In Information** page. The user account will be deployed via the location and not the terminal.
- ❑ Select the video resolution on the **Video Resolution** page and select the ***Next*** button to continue.
- ❑ Add any needed modules on the **Module Selection** page and select the ***Next*** button to continue.
- ❑ Set the ***Monitoring Configuration*** speed on the **Monitoring Configuration** page and select the ***Finish*** button to accept the changes.

12. Associating Resolvers to Locations and Actions

- ❑ Register your resolvers as described in **Register Resolvers** at section 8.
- ❑ Create your locations as described in **Create Locations** at section 9.
- ❑ Open the **Locations** branch by selecting the globe ***Location*** icon in the **Tree Selector** at the bottom of the tree.
- ❑ Right click on a location to open the **Location Configuration Wizard.**
- ❑ Use the ***Next*** button to navigate to the **Relevance Resolver Selection** page of the Location Configuration Wizard.
- ❑ Select the ***Add*** button to launch the **Choose a Relevance Resolver Selection window.**
- ❑ Select the registered resolver from the ***Resolver Name*** drop-down.
- ❑ Select the action you want the resolver to trigger from the ***Choose Action*** drop-down.

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

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

- ❑ Select ***OK*** to add the action to the resolver at that location.
- ❑ Repeat as necessary to have different resolvers for different actions.
  See **Use Permissions to Control** at section 14.4 to see how to use Access Groups to have the same resolver grant different actions based on group membership.

13. Unassigned Locations

Unassigned Locations are locations that use a resolver to deploy content but the location does not have an assigned terminal. The content is accessed through a mobile device.

Create a Location as show in **Create Locations** at section 9. .

- ❑ Open the **Locations** branch by selecting the globe ***Location*** icon in the **Tree Selector** at the bottom of the tree.
- ❑ Right click on the globe ***Locations*** icon in the tree and select ***Add Location*** to open the **Location Configuration Wizard.**
- ❑ Name the location on the **Location Name** page.
- ❑ Select options on the Location Options page including manually selected functions allowed.
    - ***Inactivity Timeout –*** A Relevance user will be logged off after this interval if inactive.
    - ***Relevance ID Signal Loss Timeout –*** This is the interval before a Relevance user is logged off due to lack of a signal.
    - ***Activate Display Client at Log In –*** This brings the display client to the forefront when the Relevance user logs in.
    - ***Enforce Location Fencing –*** This controls access in an area with nested locations. If local fencing is enforced the user has to be within the fence to access the sub-locations.
    - ***Inherit from parent Locations –*** This allows nested sub-locations to inherit the parent display clients.
    - ***Allow Local Access –*** This allows a Relevance user to access the location from that location. Unchecking this will only allow remote access.
    - ***Allow Remote Access -*** This allows a Relevance user to access the location from a remote site. Unchecking this will only allow access at the location.
    - ***Reset Cloned Sessions on Logout –*** This will close any cloned sessions once they are disconnected.
    - ***Allow Location to be selected manually –*** This allows a location to be manually selected. Unchecking this will require the Relevance user to use a Resolver like QR Codes, Wi-Fi, or Bluetooth to initiate the location access. If this is selected checkboxes appear to allow selection of the three basic interactions – ***Shadowing***, ***Transferring***, and ***Cloning***.
- ❑ Add the display clients you want to use at the location on the **Display Client Selection** page.
- ❑ Each location needs a unique Windows user account added on the **Windows Log In Information** page.
- ❑ Resolvers are added on the Relevance Resolver Selection page. This provides a way for the mobile device to authenticate to a location.

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

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

These are not applicable to an unassigned location:

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

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

14. Access Groups and Users

Resolvers, actions, and applications can be limited to members of an access group. This allows you to control who has access to content.

14.1. Create Access Groups

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

14.2. Create Users

- ❑ Select the **User** icon at the bottom of the ThinManager tree to open the **Relevance Users** branch of the tree.
- ❑ Right click on the ***Relevance Users*** branch and select ***Add User*** to open the **Relevance User Information** wizard.
- ❑ Enter a user name and password in the ***User Name*** and ***Password*** fields. This does not need to match a Windows account. It can be a Relevance/ThinManager only account. You can select an existing user from Active Directory by checking the *Active Directory User* checkbox and selecting the *Search* button. This will allow you to use a Windows domain account for the Relevance user.
- ❑ Apply group membership by selecting the ***Permissions*** button and launching the **Relevance Access Groups** window.
- ❑ Move the access group you want the user to join into the ***Member of*** list and select the ***OK*** button.
- ❑ If you are using the account to access the applications on the locations and not assigning specific display clients to the user you can select the ***Finish*** button and save the user.
- ❑ If you want to assign a specific display client to the user select the ***Next*** button and navigate to the **Display Client Selection** page. Select the ***Yes*** radio button in the ***Add User-specific Display Clients*** frame. Select ***Next*** to continue.
- ❑ Move the desired user-specific display client to the ***Selected Display Client*** list.
- ❑ There are three login strategies for logging into a Windows session with user-specific display clients:
    - ***Use Terminal Configuration Login Information*** This setting will use the terminal Windows credentials to automatically login. This doesn't give the user a unique session, they access the session with each terminal's credentials.
    - ***Same as Relevance User username/password*** – Use this if the user account you create matches the user's actual windows account. This lets them access the application with their own credentials.

If a password is entered on the first page of the wizard then the password will need to be maintained in both Windows and ThinManager. Leave the ***Password*** blank on the first page to keep from having the passwords managed in both Windows in ThinManager.
This adds security as the user has to enter their Windows password to access their content.

- Entering a valid Windows user name and password in the ***Username*** and ***Password*** fields will provide an alias to the Relevance user. As the log in with their Relevance user account will receive the credentials of the hidden Windows account.

- ❑ Select the login strategy and select ***Next*** to continue.
- ❑ The **Terminal Interface Options** and **Terminal Hotkey Options** pages allow the user to have selector options and hot keys that are tied to the user account. The **User Options** page has additional settings as needed.
- ❑ Select ***Finish*** to close the wizard, accept the configuration, and create the account.
- ❑ Repeat as needed.

14.3. Apply Permissions to Content

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

14.4. Use Permissions to Control Display Client Access

- ❑ Select the **Location** icon in the ThinManager tree to open the **Location** branch.
- ❑ Double click on the location you want to control with permissions to open the **Location Configuration Wizard**.
- ❑ Navigate to the **Display Client Selection** page. Add the display clients that have permissions added to the ***Selected Display Client*** list.
- ❑ Select ***Finish*** to accept the changes.
- ❑ Select the **Terminal** icon in the ThinManager tree to open the **Terminals** branch.
- ❑ Double click on the terminal that has that location you want to control with permissions to open the **Terminal Configuration Wizard**

- ❑ Navigate to the **Terminal Mode Selection** page. Check the ***Enable Relevance User Services*** checkbox. The ***Enable Relevance Location Services*** should have been checked when the location was assigned.
- ❑ The Relevance user menu can be configured by selecting the ***Main Menu Options*** button on the **Terminal Interface Options** page. A Main Menu hotkey can be configured on the **Hotkey Configuration** page.
- ❑ Restart the terminal that is assigned to the location to apply the changes.

14.4.1. Testing the Log In to Access Content

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

15. Use Permissions to Control Resolver Actions

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

- ❑ Select the **Location** icon in the ThinManager tree to open the **Location** branch.
- ❑ Double click on the location you want to control with permissions to open the **Location Configuration Wizard**.
- ❑ Navigate to the **Relevance Resolver Selection** page.
- ❑ Select the ***Add*** button to add a resolver and select and action in the ***Choose Action*** drop-down on the Choose a Relevance Resolver window.
- ❑ Select the ***Permissions*** button to launch the **Permissions** window. Remove the ***Unrestricted*** group from the ***Member of*** list and add the access group you want to be able to perform the action. Select the ***OK*** button twice to close the **Permissions** window and **Choose a Resolver** window.
- ❑ To have the same resolver perform different functions for different permission groups add the resolver additional times, select a different action and add a different permission group each time.
- ❑ Select the ***Finish*** button to close the Relevance Resolver Selection wizard.

15.1.1. Testing the Resolver to Access Relevance Action

- ❑ Use a mobile device that is configured in ThinManager to use Relevance. See Mobile Devices at section 7 for details.
- ❑ Launch the iTMC app and connect to your ThinManager Server.
- ❑ Select ***ScanID*** from the iTMC menu bar and scan the resolver when you are not logged in with a Relevance user account or when you are logged in with an account that isn't granted

the proper permission set for the resolver.
You should receive a ***Relevance Error – Relevance Identifier not associated with any permitted action*** message.

- ❑ Log in as a user that is a member of the allowed access group. Select ***ScanID*** from the iTMC menu bar and scan the resolver.
  You should be granted the Relevance function that was configured for the resolver on the **Relevance Resolver Selection** page.

Access to restricted applications, functions, and locations are only granted to users logging in with matching membership.

16. Active Directory Integration

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

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

16.1. Using Active Directory for User Accounts

Each *Username* field has a *Search* button that allows you to access Active Directory Users. This applies to Locations, Terminals, and Relevance Users.

- ❑ Select the *Search* button at a *Username* field to launch the Search for AD User window.
- ❑ Select the *Locations* button to pick the AD location to search.
- ❑ Select the *Search* button to load the available accounts. Select an account and select OK. The user will be entered in the Username field.
- ❑ Enter the password for the account. You can set the password requirement by selecting the *Password Options* button. The *Resync Account* button on the Password Maintenance Options window will allow you to send the password entered in ThinManager to the Active Directory. It will prompt you to enter Domain Administrator credentials for the password update.
- ❑ Selecting the *Verify* button will check that the username and password are valid.

16.1.1. Manage Active Directory Accounts

ThinManager provides tools for managing Active Directory accounts.

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

16.2. Using Active Directory with Access Groups

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

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

16.3. Password Management with Active Directory

ThinManager can help manage Active Directory password rules.

16.3.1. Password Settings

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

16.3.2. Synchronize Passwords

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

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

17. Wireless Infrastructure

The wireless devices used for Relevance need a wireless network to communicate with ThinManager. This network doesn't have to provide coverage to your entire facility but needs to be accessible in the locations where the information is needed. When a user walks into a dead zone their applications will remain on the servers to be delivered once they re-enter a valid zone.

18. Use Case Examples

This section covers some examples of how Relevance is used to provide customers with location awareness, and improved mobility solutions.

18.1. Case Study One - Mobile HMI Control

18.1.1. Introduction

A customer has a new, large multi-acre, food manufacturing facility. This facility has multi-level equipment in several large rooms separated by concrete walls. There is an office area, maintenance area, locker rooms, and cafeteria. Hallways separate these spaces.

This new facility was built with excellent Wi-Fi coverage. Each room has one or two access points (AP) to provide coverage to every corner. There are also APs in the office, maintenance, locker room, and cafeteria areas.

The existing control and visualization system has thin clients throughout the plant. There are operator station enclosures with touch screens that allow wash-down for cleanliness.

They have embedded the TermMon ActiveX object into Rockwell's Factory Talk HMI product. This allows them to use the TermSecure User account to control features and functions within the application. Specifically, they enable or disable the ability to make writes to PLC's and controllers based on the login.

18.1.1. Goals

- Deploy the HMI application to a mobile device.
- Allow writing to the PLC while the user is on the floor but prevent writing to the PLC if mobile device is not on the plant floor.
- Allow operators to view and navigate the HMI application from anywhere in the facility

18.1.2. Plan

The original plan was to use Bluetooth beacons to identify locations. It was found that an operator could be 200+ feet away from the terminals, but still have a good visual on the operating equipment. This would mean that hundreds of Bluetooth devices would need to be in place in order to determine their location. A more manageable solution was sought.

It was decided that the plant could be segmented into a plant location and non-plant locations using the Wi-Fi access points as resolvers. Users in the plant location could be granted permission to view the HMI and write to the PLC while users outside the plant location could view the HMI but be denied the ability to write to the PLC.

18.1.1. Deployment

An iPad was used to create the Wi-Fi resolvers for the Plant, Office, and Cafeteria. The Plant location was assigned Wi-Fi resolvers with the No Action function. The HMI ActiveX integration was

modified to require that the user be within the Plant location to write to the PLC. If a user was outside the Plant location, like in the Office or Cafeteria they would be denied that ability.

The mobile devices were assigned the HMI display client and a Windows user account to allow them to run the application anywhere.

The Plant location does not have an assigned Display Client or User. The location is used just to pass the Location name into the HMI through the TermMon ActiveX to grant permission to write to the PLC..

An operator can carry an iPad and get the HMI but the location controls access to the PLC.

18.1.2. Results

- Wi-Fi access points were used as the resolvers due to the large area.
- Locations were configured without Display Clients or Windows users. The display client and Windows user accounts were applied to the mobile devices.
- The TermMon ActiveX was integrated with HMI to use the Location name to grant PLC access.
- A user can run the HMI and any location but will be limited to write to the PLC by location.
- Wi-Fi access points provided reliable boundaries due to the separation of the devices and the existence of physical barriers like walls and doors.

18.2. Case Study Two - Data Entry for Calibration

18.2.1. Introduction

A multi-acre chemical plant has a requirement to check calibration and instrumentation on an hourly basis.

The original system used un-managed hand-held devices for data input. The operator scanned an RFID tag to enter calibration and instrumentation data for a specific location. There are 15 different data locations, and a total number of 270 different data values that are manually collected.

These devices were un-managed, difficult to replace, expensive, and saved the data to a separate database from the HMI.

ThinManager was being used to deploy Wonderware InTouch HMI to industrial thin clients to control the process. They want to integrate both systems into a managed system with a common database.

18.2.2. Goals

- Replace current system for logging manual data.
- Replace the devices with equipment that is easier to manage and replace.
- Integrate the calibration data into the InTouch Historian database so that it will be easier to visualize and review.
- Create and launch a separate window for each of the 15 locations.
- Require Operator to scan a code at each location to verify the location.

18.2.3. Deployment

Since a single operator was gathering the calibration and instrumentation data a single HMI application could be run. They would use the location to control what data entry screen was available.

A new Wonderware InTouch application was created with a separate data collection window for each location. The TermMon ActiveX was integrated into the HMI application so that the location would launch the appropriate window. The operator could navigate to the proper window only by scanning the appropriate QR code.

A Parent Location was created and assigned the InTouch Display Client and a Windows user account. There were no Resolvers or actions on this location.

A Child Location was created for each of the 15 Data Locations. Each Child Location was set to inherit from parent location so that they received the Display Client and Windows user from the parent.

A QR Code was created and assigned to each of the 15 data collection locations with the Transfer function.

Scanning a QR code at any one of the 15 data collection areas transfers the HMI to the iPad and launches the appropriate window for that location. This allows a single HMI and license to be used at all 15 locations.

18.2.4. Results

- Older, unmanaged, proprietary hand-held devices are replaced with commonly available iPads that get managed through ThinManager.
- The new Wonderware InTouch application allows the data to be directly entered into the InTouch Historian database.
- Using Nested Locations in Relevance allows one HMI session to be used at all 15 data collection locations.
- QR Codes are used for Child Location identification.
- Scanning a QR Code to resolve to a location launches the correct window because of TermMon ActiveX integration.
- Terminals aren't needed at the data collection sites, the iPad serves that function.

18.3. Case Study Three - Reference Material Deployment

18.3.1. Introduction

A Food and Beverage company has a manufacturing facility with equipment for producing bottled food products. The process consists of mixing, cooking, filling, capping, pasteurizing, labeling, box packing, and palletizing.

They use SharePoint to organize the documentation of all of their diverse systems. A site was created to index all of the documentation, either by drilling down through layers or be direct links to documents.

They want to access the appropriate documentation at each equipment, device, or system without adding any operator stations.

18.3.1. Goals

- Enable mobile access to reference material
- Provide ability to auto-navigate to data for a specific line or piece of equipment
- Provide for security such that only maintenance users can access the data

18.3.2. Deploy

First, a Relevance Access Group was created for the maintenance workers. A Relevance Users account was created for each Maintenance worker. These Relevance Users were tied to the individual Windows user accounts of the maintenance workers.

Second, mobile device terminals are created and configured to use a unique Windows user account.

Third, a Display Client was created that launched reference material.

Fourth, locations were created for the system. Individual locations were created to represent each line, equipment, or system where data was needed to be accessed.

Fifth, QR Codes were created for the system. Individual QR Codes were created for each location.

Sixth, the Locations are configured with the Internet Explorer Display Client, a unique Windows user account, and the specific QR Code created for this location. The QR code resolver is set to grant the Clone action. The QR code has the Maintenance permission applied to the resolver so that a user has to be a member of the maintenance group to access the data.

Additionally, the Display Client Override was set with a command line override that listed the URL to open the specific page containing the links to the information that are needed for this location.

The Resolver Action is Clone, so that multiple users can access the same data if needed.

18.3.1. Use

The maintenance user connects the iPad to the ThinManager system. They login with their Relevance User account information, and then scan the desired QR Code.

The iPad connects to the Terminal Server, launches Internet Explorer. The QR code passes the URL to the session and opens the proper document.

Each user gets the data in with their own credentials because of the Clone function.

Data is restricted to authorized maintenance users because of the permissions fron the Relevance access group.

18.3.2. Results

- QR Codes provide navigation to equipment specific reference material information.
- Relevance permissions limit access to authorized users.
- The Display Client Override allows one display client to point to a wide variety of different documents without creating a display client for each document.

18.4. Case Study Four – Oil Field Security

18.4.1. Introduction

Customer has an oil field facility with equipment for pumping oil from the ground to a temporary storage, then to a refinery. The field contains a few fixed thin client stations. Maintenance personnel travel around the field performing inspections and maintenance of the equipment.

The customer would like be able to provide a mobile device to maintenance employees that allowed them access into the Computerized Maintenance Management System (CMMS), as well as to access the HMI as needed, throughout the field.

18.4.2. Goals

- Enable mobile access to the CMMS and HMI.
- Control access to the HMI so that it is only visible in the field.
- Provide for security so that only authorized users can access the CMMS or HMI.

18.4.3. Deploy

First, a Relevance Access Group was created for the maintenance workers. A Relevance Users account was created for each maintenance worker. These Relevance Users were tied to the individual Windows user accounts of the maintenance workers. This will be used to access the CMMS and HMI.

Secondly, mobile devices are configured for the maintenance users. They are configured without a display client or user account. They can only access an application if a user logs in with an authorized Relevance user account.

Third, a Parent Location is configured using a GPS Resolver that it covers the oil field. Fencing is enabled at this level. A display client is created to launch the CMMS application and applied to the parent location, with the action of Clone. A unique Windows user account is assigned to the location.

Fourth, the local fixed terminal stations in the field are converted to use Relevance. The HMI display clients and user accounts are moved from the terminal to the location. The location is assigned to the terminal station.

Each fixed terminal station is designated to cover a particular area of equipment. These new Locations for the fixed terminal stations are set as Child Locations under the field GPS parent location.

Fifth, QR codes are configured for each of these fixed terminal child locations, and affixed to the terminals and associated field equipment. The QR Code resolvers are setup with a Transfer Action so that the sessions are able to move to the mobile device.

18.4.4. Usage

A user can drive into the oil field. The GPS will resolve the location and verify that the mobile device is at the parent location.

The CMMS application belonging to the parent location is hidden by permission. A mobile user is prompted to enter their unique Relevance user information to run the session. If the operator logs into their mobile device with a valid Relevance user account that has the Maintenance permission then the CMMS application will launch. This provides the ability for a maintenance worker to use any of the configured Mobile Devices, and still get a unique individual connection to the CMMS.

Since the location has an action of Clone, a user connecting to the location will run the CMMS application with their credentials from the mobile device.

If the operator scans a QR code the HMI application will transfer from the thin client terminal station to the mobile device. If another Maintenance or Operations person is using the terminal HMI at the time, they can deny the Transfer.

In addition, since the Fence is enabled at the Parent level using GPS, the Mobile Device will not be able to access the HMI if they are away from the Field.

18.4.5. Results

- Parent Location fencing provides access only if a user is in the Field.
- A login with an account that has the Maintenance permissions is required for terminal use.
- Maintenance users are not restricted to a specific device but can use a pool of devices.
- The Relevance permission controls the access to the CMMS. Each user to get their unique CMMS data because of the clone function.
- QR Codes provide HMI access to correct HMI for their area.
- Operators can transfer the HMI from the stationary terminal to their mobile device.