



Rockwell Automation

ThinManager™ Basic – Cloud – 2019



Important User Information

This documentation, whether, illustrative, printed, “online” or electronic (hereinafter “Documentation”) is intended for use only as a learning aid when using Rockwell Automation approved demonstration hardware, software and firmware. The Documentation should only be used as a learning tool by qualified professionals.

The variety of uses for the hardware, software and firmware (hereinafter “Products”) described in this Documentation, mandates that those responsible for the application and use of those Products must satisfy themselves that all necessary steps have been taken to ensure that each application and actual use meets all performance and safety requirements, including any applicable laws, regulations, codes and standards in addition to any applicable technical documents.

In no event will Rockwell Automation, Inc., or any of its affiliate or subsidiary companies (hereinafter “Rockwell Automation”) be responsible or liable for any indirect or consequential damages resulting from the use or application of the Products described in this Documentation. Rockwell Automation does not assume responsibility or liability for damages of any kind based on the alleged use of, or reliance on, this Documentation.

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

Except as specifically agreed in writing as part of a maintenance or support contract, equipment users are responsible for:

- properly using, calibrating, operating, monitoring and maintaining all Products consistent with all Rockwell Automation or third-party provided instructions, warnings, recommendations and documentation;
- ensuring that only properly trained personnel use, operate and maintain the Products at all times;
- staying informed of all Product updates and alerts and implementing all updates and fixes; and
- all other factors affecting the Products that are outside of the direct control of Rockwell Automation.

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

Throughout this manual we use the following 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.

IMPORTANT

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

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
 - recognize the consequence
-

SHOCK HAZARD

Labels may be located on or inside the drive to alert people that dangerous voltage may be present.

BURN HAZARD

Labels may be located on or inside the drive to alert people that surfaces may be dangerous temperatures.

ThinManager All in One Lab

Contents

Before you begin	6
About this lab	7
Tools & prerequisites	9
Additional References	10
Section 1: Defining ThinManager Display Servers, Display Clients and Terminals	11
Overview	11
Create Display Servers	13
Create a Display Client	16
Create a Terminal Profile	19
Configure PXE Server	23
Assign the Terminal Profile to a Thin Client	26
Shadow Thin Client from ThinManager	29
Section 2: Configuring ThinManager Application Link and Failover for FactoryTalk View SE	30
Overview	30
Add Terminal Names to FactoryTalk Directory	31
Add Windows Linked User Group to FactoryTalk Directory	34
Create a RemoteApp for FactoryTalk View SE	37
Create a New ThinManager Display Client with Application Link	41
Apply New Display Client to Terminal	45
Add Automatic Remote Desktop Server Failover	51
Allow Remote Start of Unlisted Programs	55
Section 3: Terminal Replacement in under 2 Minutes	61
Overview	61
Power Down the Virtual Thin Client	62
Reassign the VersaView5200 Terminal Profile	63
Section 4: Deploying Additional Content Using MultiSession and Tiling	66
Overview	66

Create InstantFizz Remote Desktop Services Display Client	67
Create Excel Remote Desktop Services Display Client.....	71
Create SuperJuice VNC Display Client.....	74
Create Camera Display Client	79
Apply Display Clients to Terminal and Enable Tiling	86
FactoryTalk View SE Client Licensing Benefits	94
Remove Tiled Display Clients	96
Section 5: MultiMonitor, Virtual Screens and Session Scaling	97
Overview	97
Split Content across Multiple Monitors.....	98
Create Virtual Screen Display Client.....	108
Apply Virtual Screen to Terminal	116
Add Virtual Screen Swapping	118
Section 6: Relevance User Services - User Based Content Delivery.....	123
Overview	123
Create View Studio Display Client	124
Create an Engineer User Group	128
Create an Engineer User	133
Enable User Services for Terminal	137
Login as Engineer User	139
Add RF IDEas Badge Reader	142
Configure ThinManager to Cache Password	147
Add Multifactor Authentication with a PIN and Password Storage	149
Authentication Pass Through.....	153
Remove Tiled Display Clients	156
Section 7: Relevance Location Services – Location Based Content Delivery.....	157
Overview	157
Install iTMC on Your Mobile Device (iOS Users).....	160
Install aTMC on Your Mobile Device (Android Users)	165
Create Terminal Profile for Mobile Device	169
Assign Terminal Profile to Mobile Device	174
Create Public Display Server	177
Reassign Display Client to Public Display Server.....	179
Login as Engineer User	181
Create Logix Designer Display Client	183

Register QR Code Location Resolver from Mobile Device	186
Create Engineer Access Group	190
Create Relevance Location for Logix PLC.....	192
Resolve to Location from Mobile Device.....	196

Before you begin

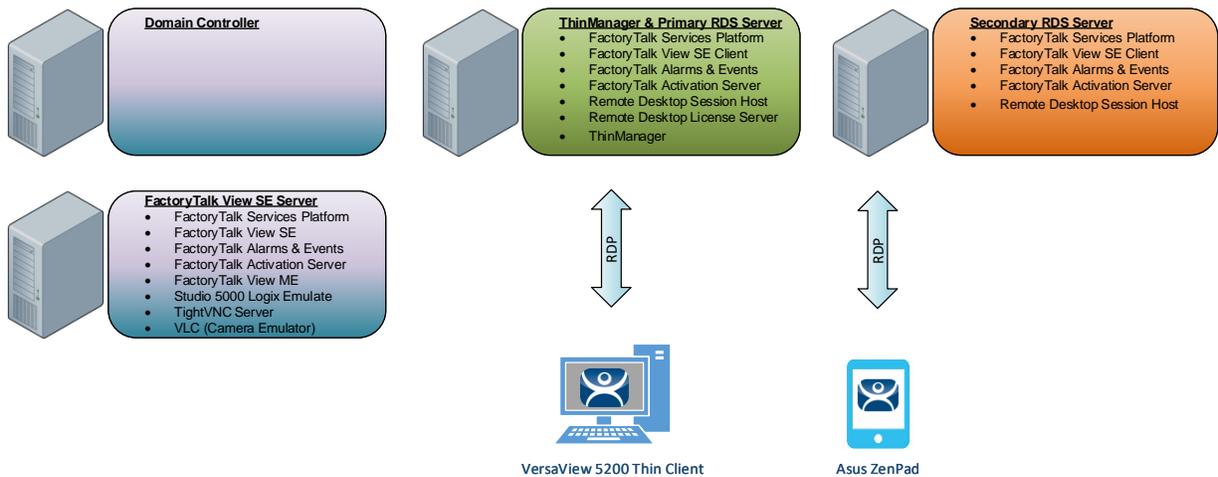
ThinManager is a centralized content delivery and device management platform designed for the plant floor. While the most common type of content delivered by ThinManager is Windows based applications via Microsoft's Remote Desktop Services (RDS), other content sources are supported as well including VNC Servers, IP Cameras and Terminal to Terminal Shadowing. Instead of maintaining multiple plant floor PCs, each with their own operating systems, applications and anti-virus requirements, migrating the plant floor applications to a Remote Desktop Server architecture can greatly simplify the deployment and maintenance of the system. In addition to content delivery, ThinManager enables central management of the devices to which the content will be delivered. In addition to thin/zero clients, ThinManager supports mobile devices like smartphones and tablets, as well as even PCs. All of these different device types can be managed under one umbrella, and managed in exactly the same way, regardless of the device type. If a virtualized desktop infrastructure (VDI) is preferred over Remote Desktop Services, ThinManager supports this architecture as well, or even a combination of both RDS and VDI. As this lab will demonstrate, ThinManager is a solution that IT departments can embrace, but does not require them to deploy or support, allowing Engineering and Maintenance to maintain the critical plant floor content.

In the event of being prompted for logins, please use the following:

- If the **Log On To Windows** dialog is active, use the username '**tmlab\labuser**' and '**rw**' for the password.
- Use the same login information if prompted to log on to FactoryTalk Directory.

About this lab

In this lab, you will complete an example deployment utilizing FactoryTalk View with ThinManager. Keep in mind that while this lab will focus on FactoryTalk content types, just about any Windows based application could be delivered using ThinManager. The thin clients and content delivered to them will be managed using ThinManager. Along the way, you will have an opportunity to work with some of the unique capabilities of ThinManager. The basic architecture being utilized is shown in the figure below:



This lab utilizes 6 different VMWare images running in the Amazon Elastic Cloud (EC2) and will require you to perform tasks on RDS1, RDS2, DC and the two Virtual Thin Clients. An Active Directory domain was created named TMLAB.LOC. Each of the Windows-based images have been pre-joined to the domain. The four images are:

1. Domain Controller – Windows Server 2012 R2 – fully qualified hostname = DC.TMLAB.LOC
2. HMI Server – Windows Server 2016 – fully qualified hostname = HMI.TMLAB.LOC
3. ThinManager/Primary RDS Server – Windows Server 2016 – fully qualified hostname = RDS1.TMLAB.LOC
4. Secondary RDS Server – Windows Server 2016 – fully qualified hostname = RDS2.TMLAB.LOC
5. Virtual Thin Client 1 (Thin01 running inside of RDS1)
6. Virtual Thin Client 2 (Thin02 running inside of RDS2)

The HMI server and applications for this lab are pre-built for your convenience and should not require any modifications. An ME Runtime exists on the HMI server as well, just to demonstrate VNC Server connectivity (basically emulating a PanelView Plus for the purposes of the lab).

The RDS1 image is a fresh Server 2016 build, with only a few items pre-installed. The lab will walk you through the installation of the Remote Desktop Services role, the FactoryTalk View SE Client and ThinManager.

RDS2 already has the Remote Desktop Services role, FactoryTalk View SE Client and ThinManager installed to save time. It will be used to demonstrate ThinManager Redundancy.

This lab will be performed by utilizing 2 virtualized thin clients and an Android Tablet. A virtual thin client can be created with VMWare Player or Workstation by just creating a new virtual machine without installing an Operating System (OS) on it, which is the essence of a zero client – no OS stored at the client, making it easier to manage. These virtual thin clients will then receive the ThinManager firmware utilizing PXE (Pre-Boot Execution Environment). While a virtual thin client may not be very useful in a production environment, it is ideal for demonstration and training purposes.

This lab is broken up into 7 separate sections. In this lab, you will specifically gain experience with the following topics:

- Section 1: Defining ThinManager Display Servers, Display Clients and Terminals
- Section 2: Configuring ThinManager Application Link and Failover for FactoryTalk View SE
- Section 3: Terminal Replacement in Under 2 Minutes
- Section 4: Deploying Additional Content Using MultiSession and Tiling
- Section 5: MultiMonitor, Virtual Screens and Session Scaling
- Section 6: Relevance User Services - User Based Content Delivery
- Section 7: Relevance Location Services - Location Based Content Delivery

Tools & prerequisites

A ControlLogix processor may be used in place of the Logix Emulate 5000 instance running on the HMI image, which is used to drive the FactoryTalk View SE and ME demo applications.

Software

- FactoryTalk Services Platform v6.11.00 (CPR 9 SR 11)
- FactoryTalk View Site Edition v11.00.00 (CPR 9 SR 11)
- FactoryTalk View ME Runtime v11.00.00 (CPR 9 SR 11)
- FactoryTalk Linx v6.11.00 (CPR 9 SR 11)
- FactoryTalk Alarms and Events v6.11.00 (CPR 9 SR 11)
- FactoryTalk Diagnostics v6.11.00 (CPR 9 SR 11)
- FactoryTalk Activation Manager v4.03.03
- RSLinx Classic v3.90.00 (CPR 9 SR 9)
- Studio 5000 Logix Designer v30.01.00 (CPR 9 SR 9)
- RSLogix Emulate 5000 v30.01.00 (CPR 9 SR 9)
- Internet Explorer 11
- Adobe Reader XI
- ThinManager v11 SP1
- TightVNC v2.8.5

Operating Systems

- Windows Server 2016
- Android 6.0 or Later

Additional References

For additional information on FactoryTalk View Site Edition and Remote Desktop Services, you can review the following Rockwell Automation Knowledge Base article:

[AID 554813 - Using FactoryTalk View SE with Remote Desktop Services - References TOC.](#)

For additional information on Remote Desktop Services and its various components, you can review the following:

[Microsoft TechNet Windows Server site for Remote Desktop Services](#)

[Remote Desktop Services Component Architecture Poster](#)

For a comprehensive directory of Rockwell Automation Knowledge Base articles subject to ThinManager, refer to the following:

[AID 1081869 - ThinManager TOC](#)

For the ThinManager and FactoryTalk View SE Deployment Guide:

[AID 1085134 - Deploying FactoryTalk View SE with ThinManager](#)

Section 1: Defining ThinManager Display Servers, Display Clients and Terminals

Overview

In this section, you will create the 3 primary building blocks of ThinManager:

1. Display Servers
2. Display Clients
3. Terminals

In ThinManager, **Display Servers** are the server sources of content that you want to deliver to your devices. A **Display Server** is typically a Remote Desktop Server, but can also be an IP/USB Camera or a VNC Server (like a PanelView Plus or a MacBook Pro).

Display Clients, not to be confused with the FactoryTalk View SE executable DisplayClient.exe, represent the actual content you will be delivering to your devices, which are referred to as **Terminals** in ThinManager. There are 6 types of **Display Clients** supported in ThinManager: (1) Remote Desktop Services, (2) Camera, (3) Terminal Shadow, (4) Workstation, (5) VNC and (6) Virtual Screen. Within this lab, you will have an opportunity to create several of these Display Client types.

You will use **Display Servers** and **Display Clients** to setup the content you want to deliver to the devices managed by ThinManager. This content can be assigned and delivered in 3 ways with ThinManager:

1. By Device
2. By User
3. By Location

While you will experience all 3 content type delivery methods in this lab, you will start with the first one, By Device, in this section. By Device allows you to assign content to the Terminal Profile, representing the default content that will be delivered to a device when it is powered on. Terminals are the thin or zero clients, mobile devices and/or PCs that you will be managing with ThinManager. Each device will have a unique Terminal Profile in ThinManager.

A zero client may look very similar to a thin client physically, but it does not have an operating system. A thin client, on the other hand, has an operating system - maybe a scaled down version of Linux capable of connecting to a Remote Desktop Server, or maybe even Windows Embedded. ThinManager treats each of these device types in much the same way in that the same ThinManager firmware is delivered to either device type. The ThinManager firmware should be viewed as the operating system for ThinManager thin or zero clients. So, if a device has no operating system like a zero client, or has an operating system like a thin client, it will receive the ThinManager firmware when it boots up and boot from it. We will refer to the virtual thin client(s) as a thin client often but it is actually a zero client, since it does not have local storage and therefore no Operating System.

ThinManager supports 2 types of thin or zero clients:

- ThinManager Ready
- ThinManager Compatible

ThinManager Ready terminals have the ThinManager BIOS extension image embedded in them by the manufacturer. When these terminals are powered on, they know how to find a ThinManager Server right out of the box. Once found, the ThinServer service delivers the terminal's firmware and configuration.

ThinManager Compatible terminals do not have the ThinManager BIOS extension image. However, the ThinManager firmware is hardware compatible with the majority of thin clients on the market. This is because the ThinManager firmware is compiled for the x86 platform, and the majority of thin clients are x86-based. In order to deliver the ThinManager firmware to these devices, PXE is utilized. **P**reboot **e**Xecution **E**nvironment (PXE) is an Intel standard whereby an operating system can be delivered over the network. The virtual thin clients used in this Cloud Lab are examples of ThinManager Compatible terminals.

Functionally, there is no real difference between a ThinManager Ready terminal and a ThinManager compatible terminal.

In this section, you will register your **RDS1** virtual machine as a Display Server within ThinManager. With this Display Server created, you will create a **Display Client** to deliver a Windows desktop session from **RDS1**. You will then create a **Terminal Profile** to which you will assign the newly created **Display Client**. Lastly, you will start the virtual thin client and assign the new terminal profile to it in order to see the results. To do this, you will be performing the following tasks:

1. Create Display Servers
2. Create a Display Client
3. Create a Terminal Profile
4. Configure PXE Server
5. Assign the Terminal Profile to a Thin Client
6. Shadow Terminal from ThinManager

ThinManager is primarily composed of 2 components – the ThinServer service and the ThinManager administrative console (admin console).

The ThinServer service is a Windows based service that is the engine of ThinManager. It delivers the terminal's firmware and configuration, and therefore is essential in order for a terminal to boot.

The ThinManager admin console, on the other hand, is not licensed, and is the interface from which you manage the entire ThinManager environment.

While these 2 components do not have to be co-located or installed on a Remote Desktop Server, they often are due to the benefits of the Remote Desktop Services architecture.

Create Display Servers

Register **RDS1** and **RDS2** as Display Servers in ThinManager.

1. Launch the ThinManager user interface from the desktop of **RDS1**.

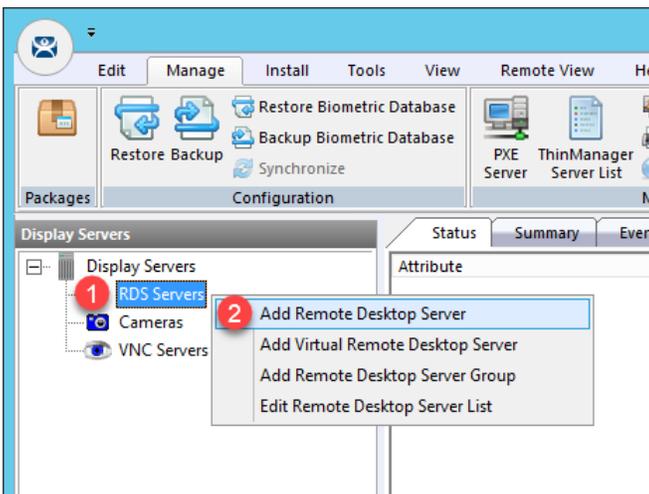


2. Click the **Display Servers** icon  in the ThinManager tree selector.

The tree selector can be expanded or collapsed using the bar above directly above it.



3. From the **Display Servers** tree, right click the **RDS Servers** branch and select **Add Remote Desktop Server**. This will launch the Remote Desktop Server Wizard.



4. From the **Introduction** page of the **Remote Desktop Server Wizard**, click the **Next** button.
5. From the **Remote Desktop Server Name** page of the wizard, type **RDS1** in the **Name** field.
6. Click the **Discover** button. If the name is successfully resolved, the IP address of **RDS1** should be filled in automatically.
7. Type **tmservice@tmlab.loc** in the **User Name** field.
8. Type **rw** in the **Password** field.
9. Click the **Verify** button which should confirm that the credentials entered are valid, followed by the **OK** button.

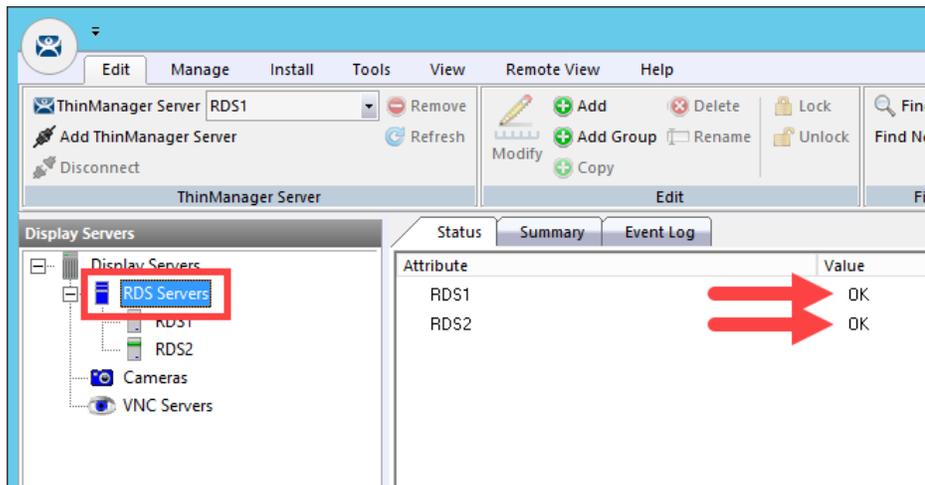
10. Click the **Finish** button.

The screenshot shows the 'Remote Desktop Server Wizard' window. The title bar reads 'Remote Desktop Server Wizard'. Below the title bar, the text 'Remote Desktop Server Name' is followed by the instruction 'Enter the Remote Desktop Server Name and Log In information.' A red callout bubble points to the 'Name' field with the text 'This will show your student number.' The 'Remote Desktop Server' section contains a 'Name' field with 'RDS1', an 'IP Address' field with '10 . 6 . 10 . 51', and a 'Discover' button. Below this is a 'Change Group' button. The 'Log In Information' section contains a 'User Name' field with 'lmservice@tmlab.loc', a 'Password' field with two asterisks, and a 'Domain' field. There are 'Search', 'Verify', and 'Password Options' buttons. At the bottom, there are navigation buttons: '< Back', 'Next >', 'Finish', 'Cancel', and 'Help'. A red circle with the number '5' is placed over the 'Finish' button.

11. **RDS1** should now be added to the Remote Desktop Servers group. You may have to click the Display Servers branch to refresh the Remote Desktop Servers group.
12. Repeat steps 3 through 11, but this time register **RDS2**.

The screenshot shows the 'Remote Desktop Server Wizard' window for the second server. The title bar reads 'Remote Desktop Server Wizard'. Below the title bar, the text 'Remote Desktop Server Name' is followed by the instruction 'Enter the Remote Desktop Server Name and Log In information.' A red callout bubble points to the 'Name' field with the text 'This will show your student number.' The 'Remote Desktop Server' section contains a 'Name' field with 'RDS2', an 'IP Address' field with '10 . 6 . 10 . 52', and a 'Discover' button. Below this is a 'Change Group' button. The 'Log In Information' section contains a 'User Name' field with 'lmservice@tmlab.loc', a 'Password' field with two asterisks, and a 'Domain' field. There are 'Search', 'Verify', and 'Password Options' buttons. At the bottom, there are navigation buttons: '< Back', 'Next >', 'Finish', 'Cancel', and 'Help'. A red circle with the number '5' is placed over the 'Finish' button.

- If not already selected, click the **RDS Servers** branch and note the status of **RDS1** and **RDS2** on the right-hand side. It should indicate a Value of **OK** for each (it may take RDS2 a few seconds to change to OK). This indicates that the IP address and credentials provided for the Remote Desktop Servers are in fact valid.



The credentials entered when configuring a Remote Desktop Server must have Administrative rights on the Remote Desktop Server. This is required for SmartSession and to populate the User, Sessions and Process tabs of the details pane, which are available when you click on the Remote Desktop Server of interest. SmartSession is ThinManager's load balancing solution. With SmartSession, Remote Desktop Server sessions will be started on the least loaded Remote Desktop Server based on CPU Utilization, RAM Utilization and Number of Sessions. Once a session is started on a Remote Desktop Server, the session will not be moved dynamically. You can learn more about SmartSession in [Section 15](#).

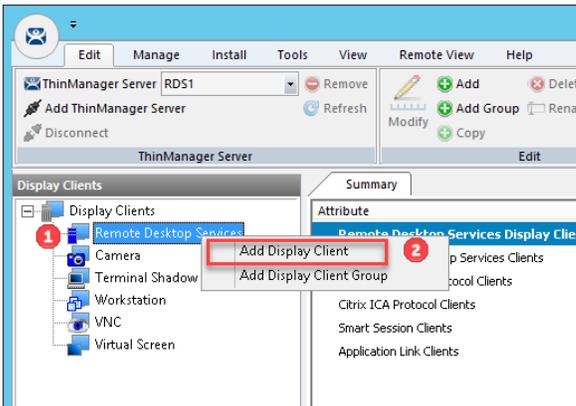
In order for ThinManager to connect to a Remote Desktop Server (like RDS1 in the example above), the provided Administrative credentials for that Remote Desktop Server in ThinManager should also be used as the ThinServer service credentials. The ThinServer service credentials on RDS1 are in fact configured as `tmservice@tmlab.loc` with password of `rw`, which are the same credentials entered for the RDS1 Remote Desktop Server. This domain user also has local Administrator permissions on RDS2.

Create a Display Client

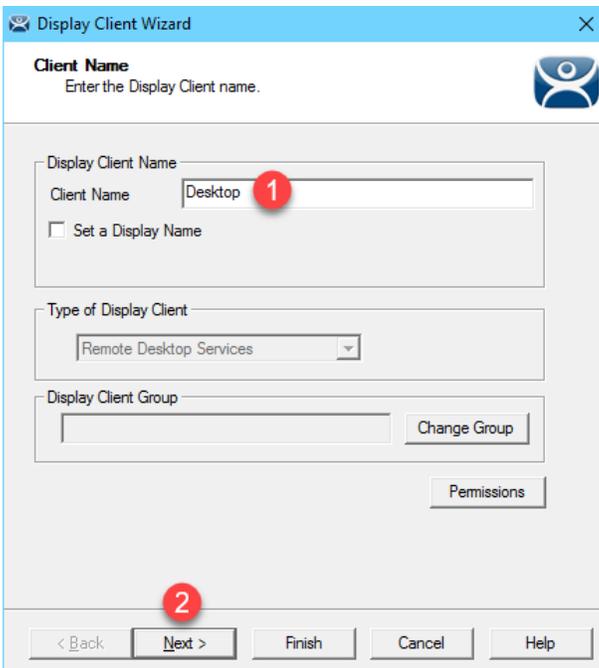
1. Click the **Display Clients** icon from the ThinManager tree selector.



2. From the **Display Clients** tree, right click the **Remote Desktop Services** branch and select **Add Display Client**. This will launch the **Display Client Wizard**.

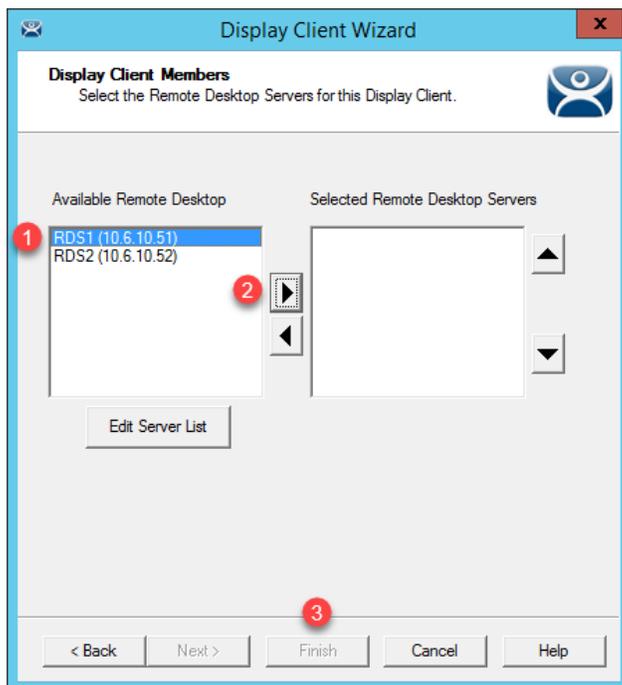


3. Type *Desktop* as the **Client Name** on the **Client Name** page of the wizard. Click the **Next** button.

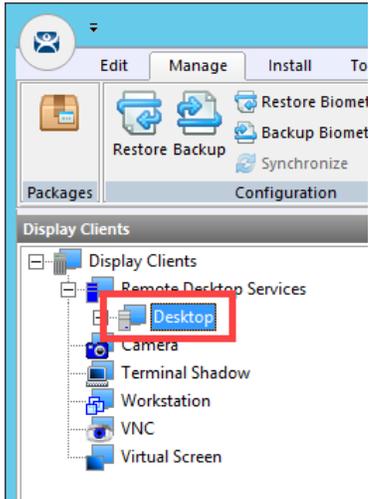


The **Set a Display Name** checkbox is new for ThinManager 11 and provides the ability to assign an Alias to a Display Client that will be shown at the Terminal in the Display Client Selector instead of the **Client Name** entered. This feature requires firmware package 8.2 or newer. Firmware packages will be explained in the Advanced Lab.

4. Click the **Next** button on the **Display Client Options** page of the wizard.
5. Click the **Next** button on the **Remote Desktop Services and Workstation Options** page of the wizard.
6. Click the **Next** button on the **Screen Resolution / Scaling Options** page of the wizard.
7. Select **RDS1** from the **Available Remote Desktop Servers** list and click the **Right Arrow** button to move it to the **Selected Remote Desktop Servers** list. This is the Remote Desktop Server on which this **Display Client** will run. Click the **Finish** button.



8. You should see the **Desktop** Display Client under the **Remote Desktop Services** branch. You may have to click the **Display Clients** node for the branch to refresh.

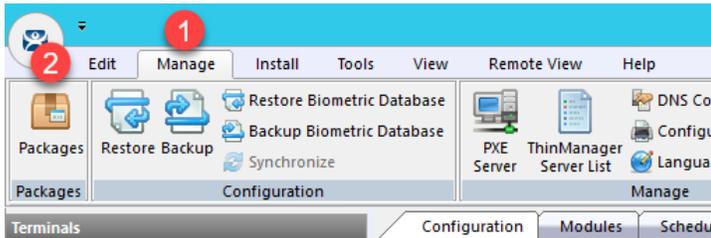


New in ThinManager 11, you can now create **Display Client Groups**. **Display Client Groups** provide the ability to better organize large quantities of content. You can create **Display Client Groups** much like folders in Windows Explorer, and then add **Display Clients** to the **Display Client Group**. Nested **Display Client Groups** are supported as well.

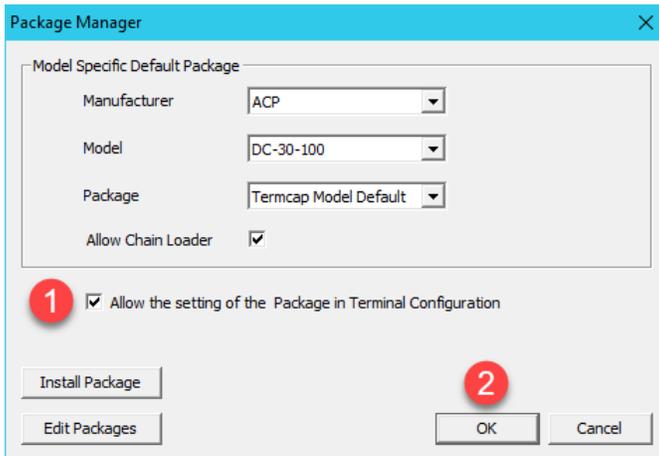
Create a Terminal Profile

As previously mentioned, each device that you will be managing (thin clients, zero clients, tablets, smart phones or PCs) will have a unique Terminal Profile created in ThinManager like the one you are about to create.

1. For this Cloud lab, we will be running **firmware package 8.1** for our virtual thin client(s). However, in ThinManager v11, the default firmware package for **PXE** clients is **8.2**. The next couple of steps will enable us to change the package on a terminal by terminal basis. Select the **Manage** ribbon followed by the **Packages** icon.



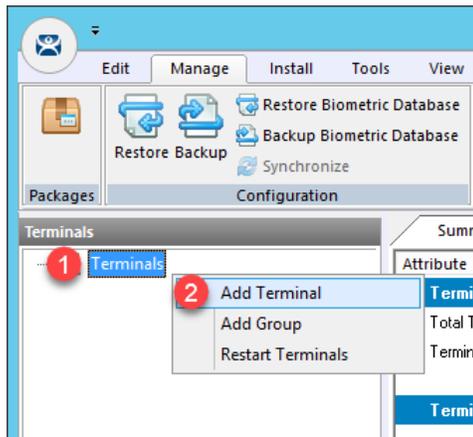
2. The **Package Manager** window enables firmware packages to be assigned in 2 different ways – by terminal model or on a terminal by terminal basis. We are going to utilize the latter. To enable this capability, check the **Allow the setting of the Package in Terminal Configuration** checkbox. Click the **OK** button.



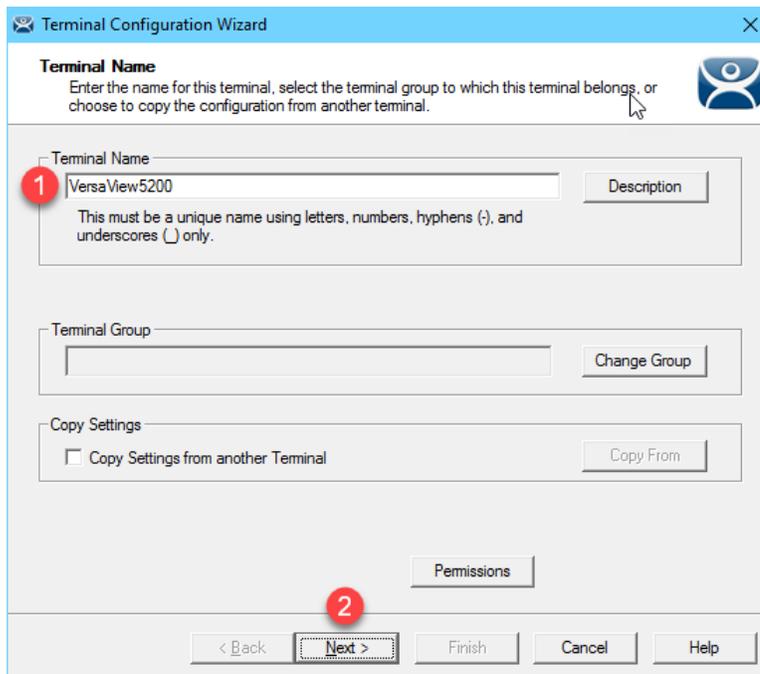
3. Click the **Terminals** icon  from the ThinManager tree selector.



- From the **Terminals** tree, right click the **Terminals** node and select **Add Terminal**. This will launch the **Terminal Configuration Wizard**.

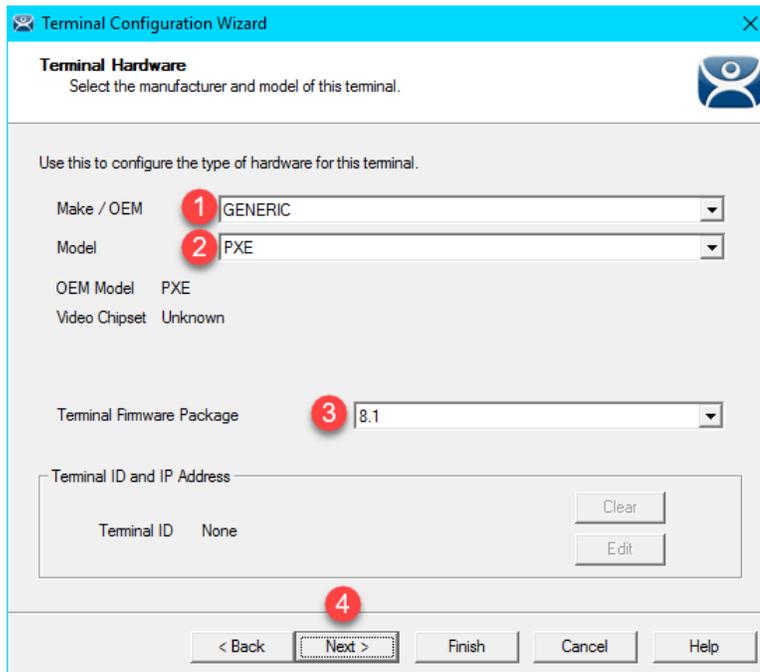


- Type *VersaView5200* as the **Terminal Name** on the **Terminal Name** page of the wizard. Click the **Next** button.

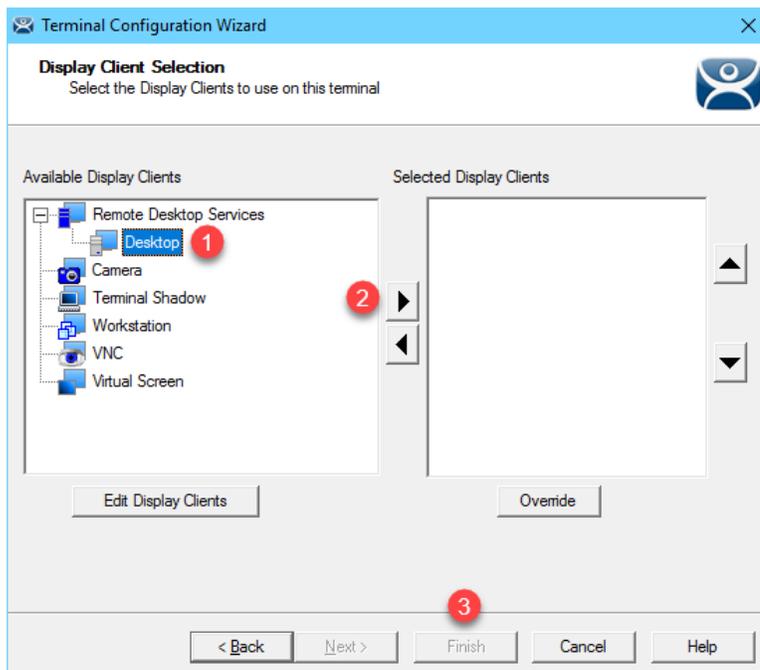


Clicking the **Description** button on the **Terminal Name** page of the wizard will not only allow you to enter a **Description** for the terminal, but also allow you to create **Custom Variables** for the terminal. **Custom Variables** were added in ThinManager 8.1. The **Custom Variable** can be used in the **Display Client** command line or by the **TermMon ActiveX**. This would allow you to create a single **Display Client** in ThinManager that utilizes a **Custom Variable** and it would direct that **Display Client** to different content based on the terminal to which it was assigned. For instance, if you have several FactoryTalk View SE Client configuration files (CLIs) that you need to deploy, you could create a **Custom Variable** on each terminal that would include the name of the CLI file to deliver to it. You would then create a single **Display Client** that references the path to the CLI files and appends the **Custom Variable** to it in the command line. In addition to **Terminals**, **Custom Variables** can also be created and assigned to **Relevance Users** and **Locations**.

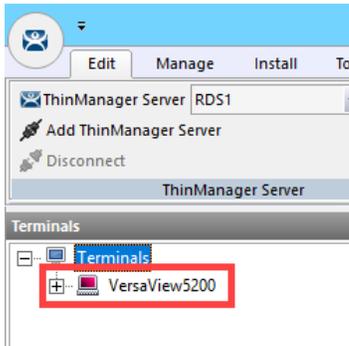
- Accept the defaults of **Generic / PXE** from the **Make / OEM** and **Model** drop down lists, respectively. Select **8.1** from the **Terminal Firmware Package** drop down list. Click the **Next** button.



- Click the **Next** button on the **Terminal Options** page of the wizard.
- Click the **Next** button on the **Terminal Mode Selection** page of the wizard.
- Select **Desktop** from the **Available Display Clients** list and click the **Right Arrow** button to move it to the **Selected Display Clients** list. This is the **Display Client** that will be delivered to this **Terminal**. Click the **Finish** button.



10. You should see the **VersaView5200** terminal under the **Terminals** node.



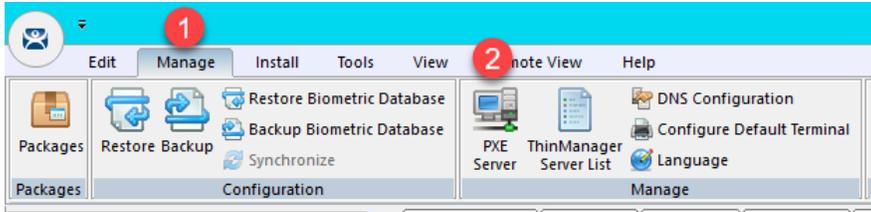
You can also create **Terminal Groups** in ThinManager. **Terminal Groups** provide 2 key capabilities: (1) terminal organization and (2) property inheritance. With terminal organization, you can create **Terminal Groups** much like folders in Windows Explorer, and then add **Terminals** to the **Terminal Group**. The other key benefit of **Terminal Groups** is that you can assign **Terminal** properties at the **Terminal Group** level and choose to make these settings a **Group Setting**. By doing so, each **Terminal** member of the **Terminal Group** would receive that setting as defined in the **Terminal Group**. In both cases, nested **Terminal Groups** are support as well. You will learn more about **Terminal Groups** in [Section 13](#).

Even though you will be using virtual thin clients for this Cloud based training, this hands on lab was based on the ThinManager MR Demo Kit which includes a VersaView 5200 Dual HD (Catalog #: 6200T-NA) industrial grade thin client. In addition to the 6200T-NA, the **VersaView 5200** family includes four additional models. The **VersaView5200 Single HD Display** (Catalog #: 6200T-BA) which has a smaller form factor and provides a single **HD Display** output. The **VersaView Dual 4K Display** (Catalog #: 6200T-KB) has the same form factor as the 6200T-NA but provides two 4K video outputs (one HDMI and one DisplayPort). For Control Room applications, the **VersaView 5200 Multi 4K Display** (Catalog #: 6200T-RC or 6200T-RE) is available. The 6200T-RC provides three **4K** outputs (all DisplayPort), while the 6200T-RE provides **seven 4K** outputs (3 DisplayPort and 4 mini-DisplayPort).

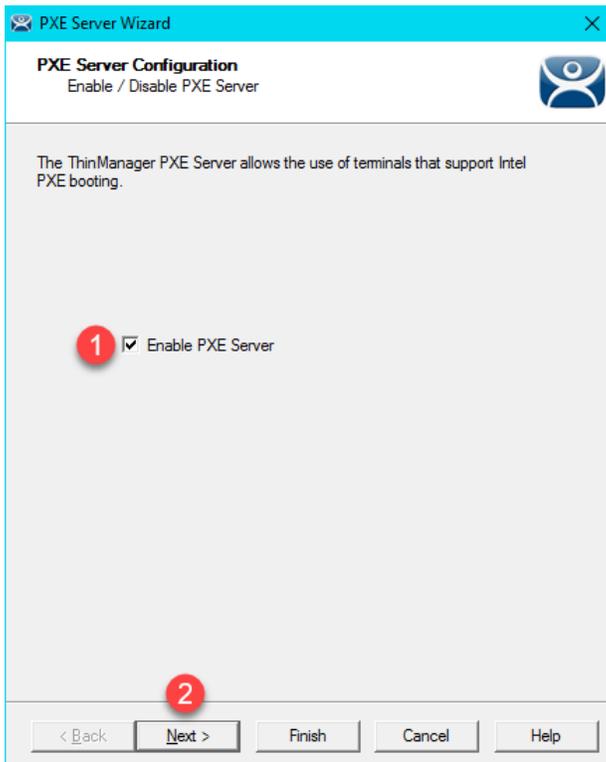
Configure PXE Server

Since this Cloud lab is utilizing virtual thin clients, we will need to boot them using PXE; therefore, the ThinManager PXE Server must be configured.

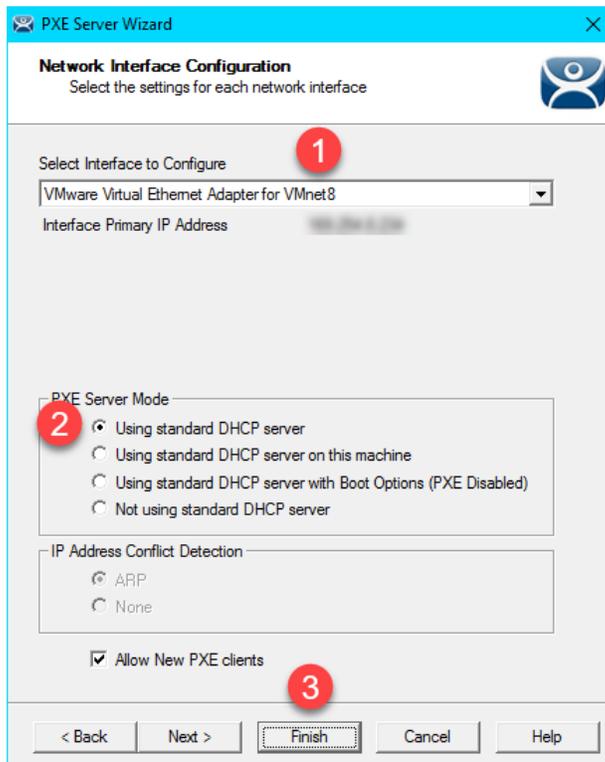
1. From the **ThinManager Admin Console**, select the **Manage** ribbon, followed by the **PXE Server** icon.



2. From the **PXE Server Configuration** page of the wizard, check the **Enable PXE Server** checkbox.



- From the **Network Interface Configuration** page of the wizard, make sure **VMWare Virtual Ethernet Adapter for VMNet8** is selected from the **Select Interface to Configure** drop down list, and **Using standard DHCP server** is selected from the **PXE Server Mode** list. Click the **Finish** button.



Some notes when configuring this page in your own deployments. Make sure you have selected the correct network interface in the **Select Interface to Configure** drop down list. In other words, on which network adapter should ThinManager listen for PXE requests. The **PXE Server Mode** selection is not as obvious. PXE, by definition, requires a DHCP Server. This setting basically tells ThinManager about the DHCP Server to be used for PXE requests. When a PXE client is booted, it not only needs an IP Address, but it also needs an IP address for its boot server, as well as a boot filename.

Here is a quick summary of the options:

- Using standard DHCP server** – choose this when you have an existing DHCP server that you want to use for PXE, but you want ThinManager to provide the additional boot details, like the IP addresses of the ThinManager Server(s) and the name of the boot file. This is the preferred choice if you are using an existing DHCP server.
- Using standard DHCP server on this machine** – similar to the first option, except the actual DHCP server is located on the same machine as ThinManager.
- Using standard DHCP server with Boot Options (PXE Disabled)** – choose this when you have an existing DHCP server that you want to use, but you do not want ThinManager to provide the additional boot details. Instead, you will need to specify Option 66 and Option 67 in your DHCP Server to specify these details.
- Not using standard DHCP server** – choose this when you want ThinManager to provide everything – the client IP address, the boot server IP address(es) and the boot filename. ThinManager will only respond to DHCP requests associated with PXE, not to standard DHCP requests.

If you will be using Legacy PXE clients and UEFI PXE clients with your ThinManager deployment, it is important to note that they require different boot files. This is automatically handled by ThinManager if you choose options 1, 2 or 4 above. However, if you choose option 3, you will need to apply Vendor Classes in your DHCP Server for Option 67 in order to deliver the correct boot filename based on the type of thin client requesting it. Legacy PXE clients use a boot filename of **acpboot.bin**, while UEFI PXE clients use **tmboot32.bin** for x86 UEFI and **tmboot64.bin** for x64 UEFI.

Through the majority of this Cloud lab, we will be using the **PXE Server Mode** configured above – namely, **Using standard DHCP server**. Again, this means we have an existing DHCP Server that will supply the IP address to our PXE client, and ThinManager will provide the additional details needed to boot it (i.e.: boot server IP address(es) and boot filename). In this configuration, we will depend on VMWare Player, which will host our virtual thin client(s) to provide a **NAT'd (Network Address Translation)** IP address. This mode proved to be the most reliable for the virtual thin client(s).

Assign the Terminal Profile to a Thin Client

1. Minimize the **ThinManager Admin Console**, and double click the **Thin01** virtual machine shortcut on the desktop. It may take a minute or so to initially launch since your Cloud lab image does not have full connectivity to the Internet.

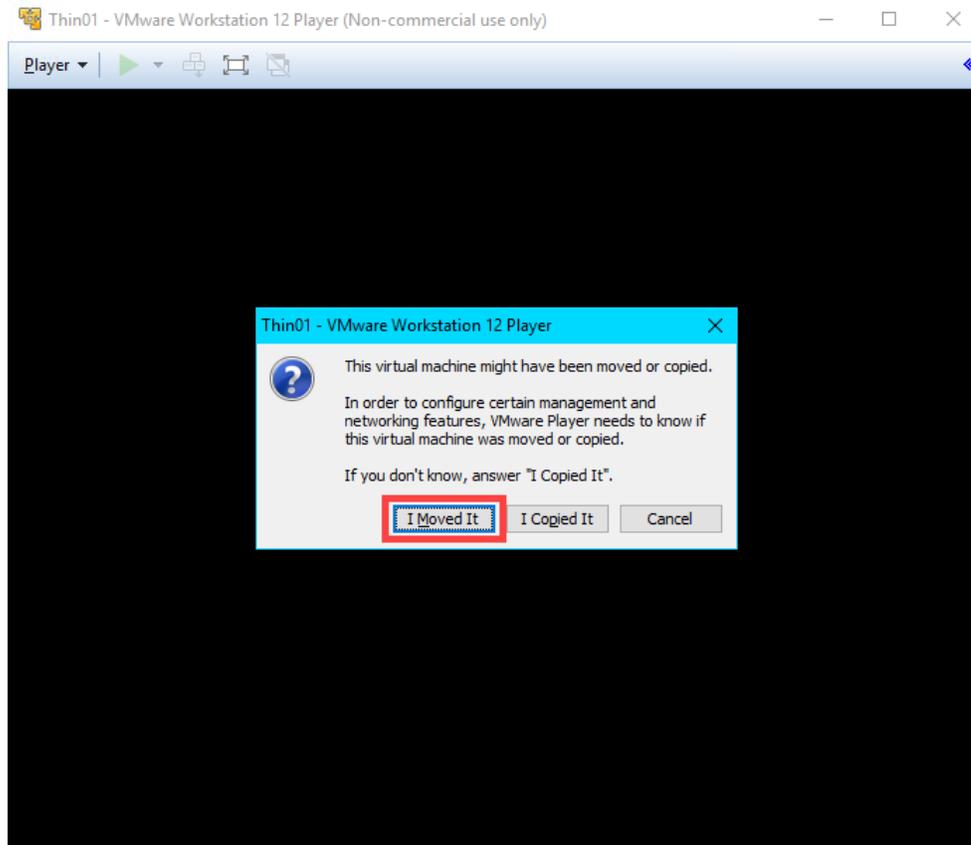


NOTE: Do not use the **VMWare Full Screen** option, as it has proven to be somewhat unstable in the cloud. It is ok to maximize the window.

Upon starting, the virtual thin client will recognize that it has no operating system installed and will therefore attempt to contact a **PXE Server**. The **ThinManager PXE Server** will respond to the **PXE** request and deliver the ThinManager firmware via **TFTP**.

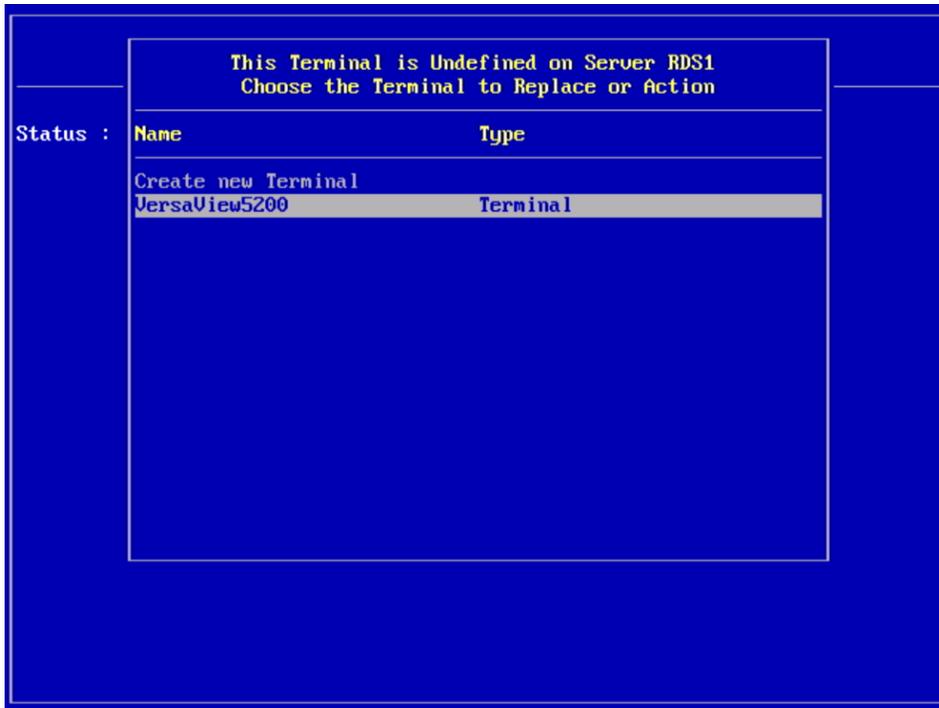
Since VMWare Tools cannot be installed within the virtual thin clients, the mouse pointer will get locked within each virtual machine when one of the virtual thin clients is active. To return the mouse pointer to the host, hit the CTRL+ALT key sequence.

2. If you receive a message box asking if you moved or copied the virtual machine, click the **I Moved It** button.



You may notice that the virtual thin client receives an IP address in the 192.168.x.y subnet. This is because we have it configured for NAT at this point in the lab.

- Once the **Thin01** has received the ThinManager firmware, it will communicate with the ThinManager Server, asking for a **Terminal Profile**. ThinManager identifies terminals by their **MAC address**. Since we have not previously assigned a **Terminal Profile** to the MAC address of this terminal, ThinManager will ask which profile to assign to it. Hit the **down arrow key** to select the **VersaView5200** profile we created previously and hit the **Enter** key.

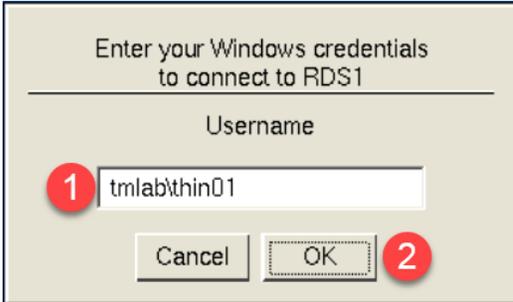


If the **Create new Terminal** option was selected above, the **Terminal Configuration Wizard** would be launched within ThinManager that would facilitate the creation of a new Terminal Profile that would then be assigned to the terminal being booted.

Additionally, you can control whether a Terminal Profile becomes available in this selection list. By default, a Terminal Profile becomes available for assignment when its associated terminal is offline. The **Allow replacement at terminal if off line** setting can be found on the **Terminal Options** page of the **Terminal Configuration Wizard**.

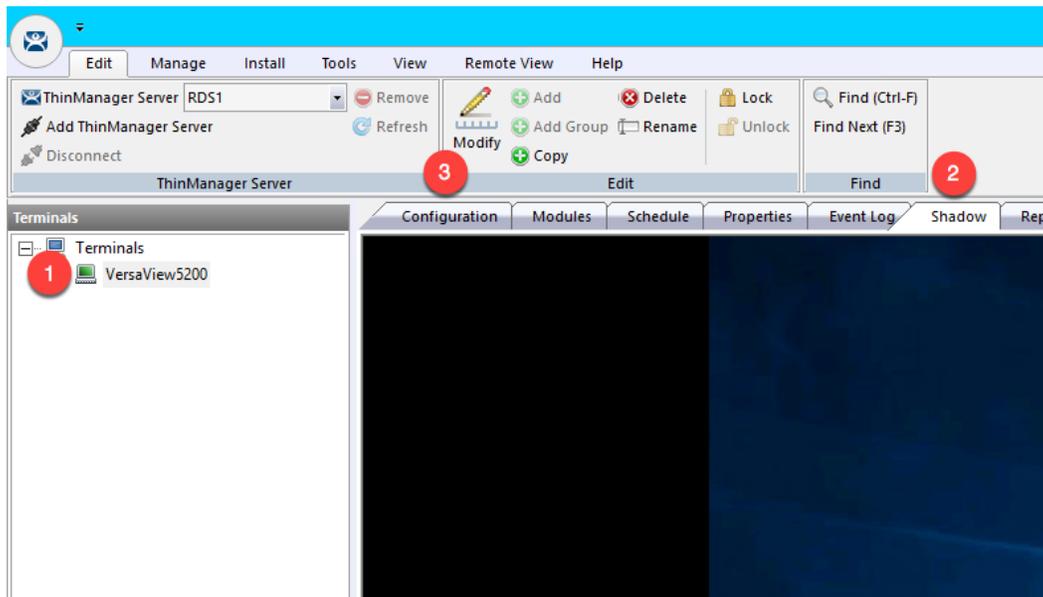
If your mouse gets locked inside the virtual machine, you can hit the **CTRL-ALT** keys on your keyboard to release it. This is happening because we have not (and cannot) installed VMWare Tools inside our virtual machine.

- The **VersaView5200 Terminal Profile** will now be delivered to the **Thin01**, and any default content (**Display Clients**) assigned to the **VersaView5200 Terminal Profile** will be delivered. Since we are starting with a Desktop session and we have not configured **Auto Login**, you will be prompted with a login dialog box to start the Windows Remote Desktop session on **RDS1**. Enter *tmlab\thin01* as the username and *rw* as the password. Once authenticated, you should be presented with a Windows Desktop Session on **RDS1**.



Shadow Thin Client from ThinManager

1. Return to the **RDS1** lab image, and click the **Terminals** icon  from the ThinManager tree selector.
2. Expand the **Terminals** node in the **Terminals** tree and select the **VersaView5200** terminal.
3. Select the **Shadow** tab from the Details Pane. You should see a shadow of the terminal from within ThinManager. Notice that the shadow is fully interactive. Also notice that the **VersaView5200** terminal icon is green indicating that it is powered up and **ThinManager** has connectivity to it. Click the **Configuration** tab when finished shadowing.



Each ThinManager terminal has a shadowing setting that determines if the terminal can be shadowed or not. This setting is available by double clicking the terminal to open the **Terminal Configuration Wizard** and navigating to the **Terminal Options** page of the wizard. The available shadowing options are Yes, No, Ask, Warn, and a checkbox for enabling Interactive Shadow or not. If you choose to experiment with these settings, remember that a terminal must be restarted for configuration changes to be applied to it. To perform a terminal restart, right click the terminal and select **Restart Terminal**.

This completes the section **Defining ThinManager Display Servers, Display Clients and Terminals** of the lab. Continue on to deliver a FactoryTalk View SE application without a Windows desktop and implement automatic Remote Desktop Server failover.

Section 2: Configuring ThinManager Application Link and Failover for FactoryTalk View SE

Overview

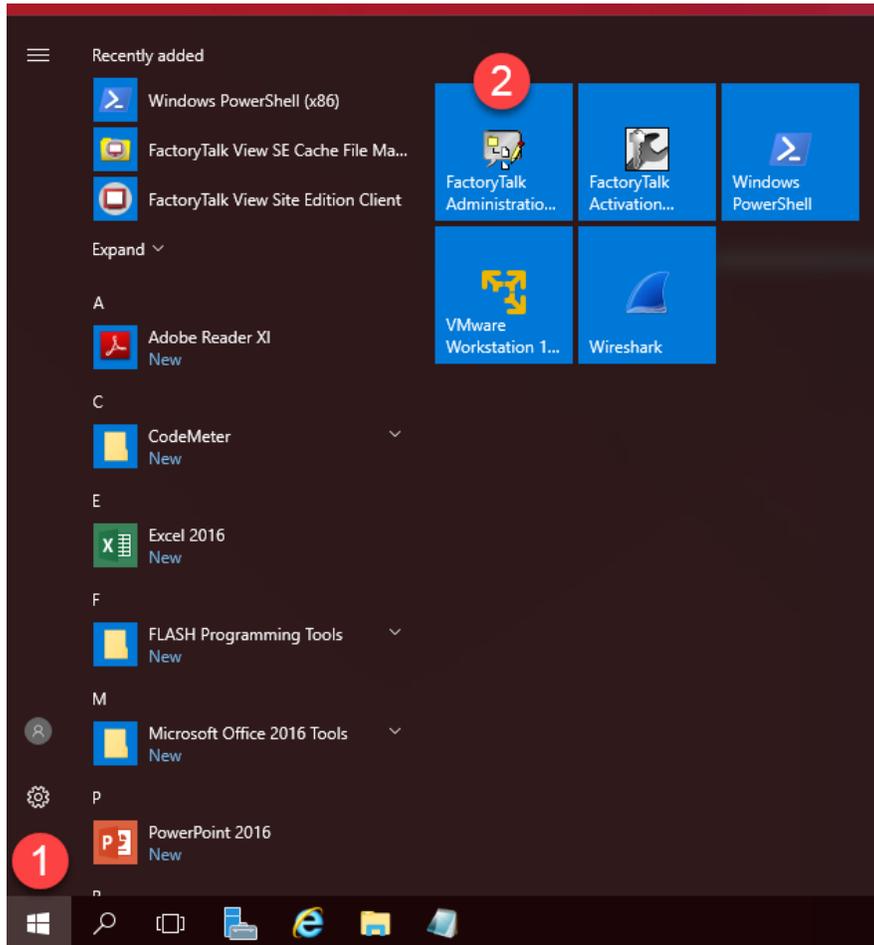
In the last lab section, you successfully delivered a Windows Desktop to the a virtual thin client using ThinManager. Typically, we go through great lengths to actually prevent access to the Windows Desktop on the plant floor, which is one reason why VDI is not always the best option for plant floor deployments – since delivering desktops is one of the strengths of VDI. This section will use ThinManager Application Link to deliver the FactoryTalk View SE Cookie Factory demo to the virtual thin client **without** a desktop. In addition, this section will demonstrate how easy it is to configure automatic Remote Desktop Server failover for your ThinManager terminals. To do this, you will be performing the following tasks:

1. Add Terminal Names to FactoryTalk Directory
2. Add Windows Linked User Group to FactoryTalk Directory
3. Create a RemoteApp for FactoryTalk View SE
4. Create a New ThinManager Display Client with Application Link
5. Apply New Display Client to Terminal
6. Add Automatic Remote Desktop Server Failover
7. Allow Remote Start of Unlisted Programs

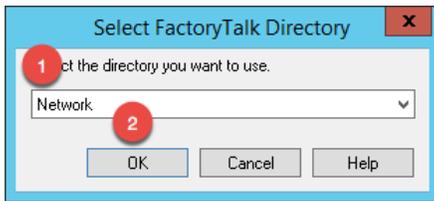
Add Terminal Names to FactoryTalk Directory

By default, every Computer connecting to the FactoryTalk Directory must be added as a Computer Account – ThinManager terminals are no different. This section will add the ThinManager terminal names to the FactoryTalk Directory as Computer Accounts.

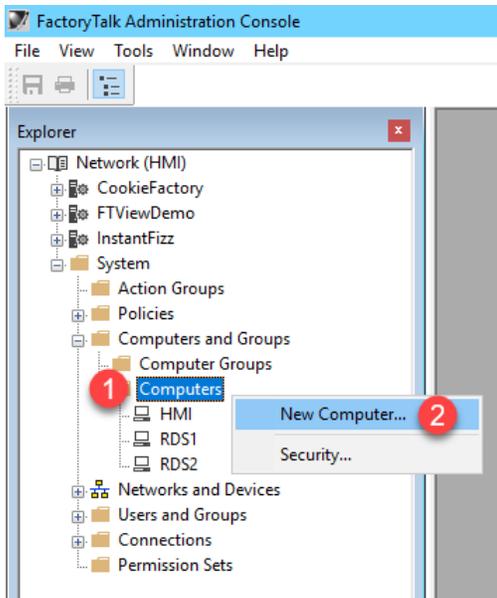
1. Click the **Windows Start** button from the **RDS1** host image – **NOT** the shadowed Desktop delivered to the thin client or the thin client itself.



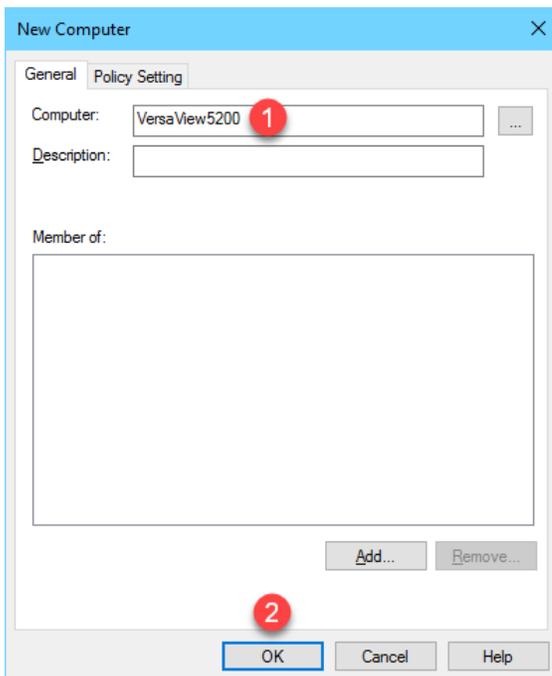
2. On the **Select FactoryTalk Directory** dialog, make sure **Network** is selected and click the **OK** button.



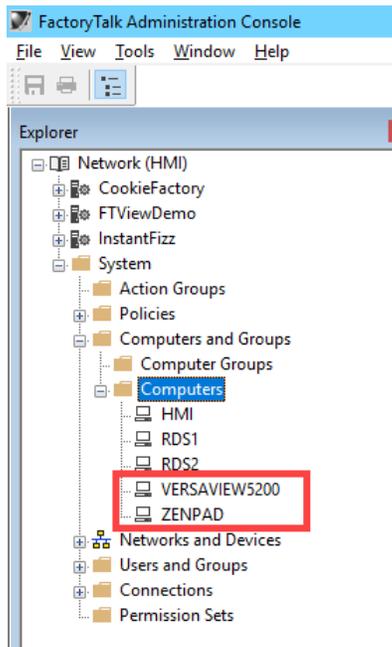
3. In the **Explorer** view, browse to **Network (THIS COMPUTER) → System → Computers and Groups → Computers**, right click **Computers** and select **New Computer...** from the menu.



4. In the **Computer** textbox, enter *VersaView5200* and click the **OK** button.



- Repeat the previous 2 steps but this time add *ZENPAD*. When finished, you should have **ZENPAD** and **VersaView5200** added to the **Computers** folder.

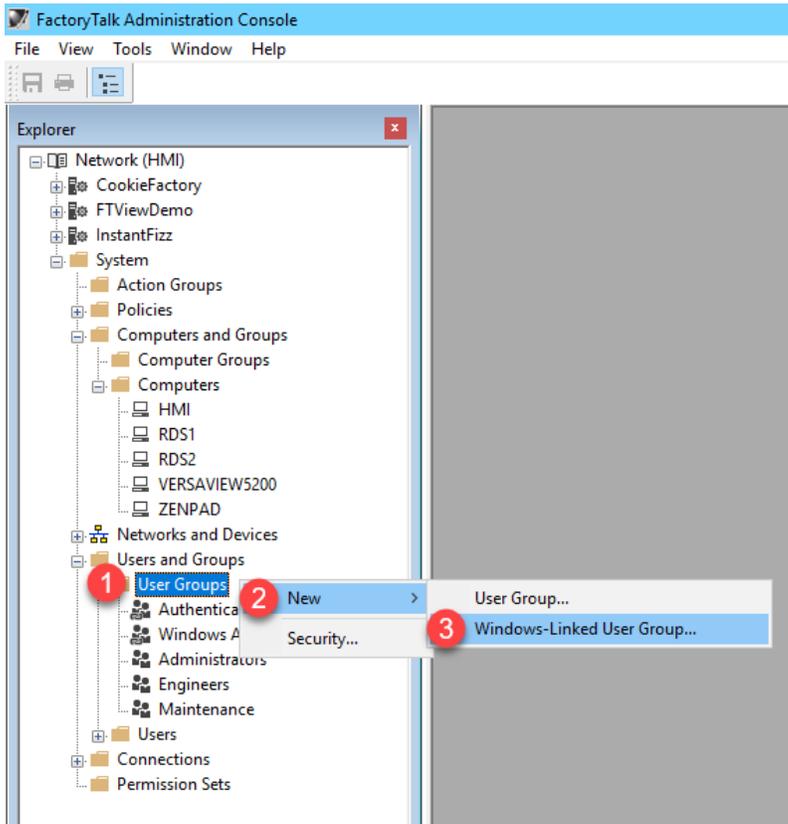


- Keep the **FactoryTalk Administration Console** open for the next section.

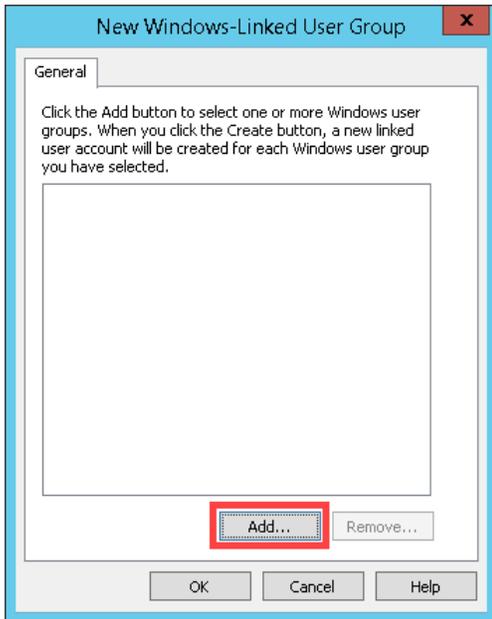
Add Windows Linked User Group to FactoryTalk Directory

In addition to adding the terminal name as a Computer Account to the FactoryTalk Directory, you will typically have to add the Windows user account that is assigned to the terminal, and therefore launching the session, to the FactoryTalk Directory as well. In this section, you will add a Windows Linked Group to the TMLAB\Domain Users group.

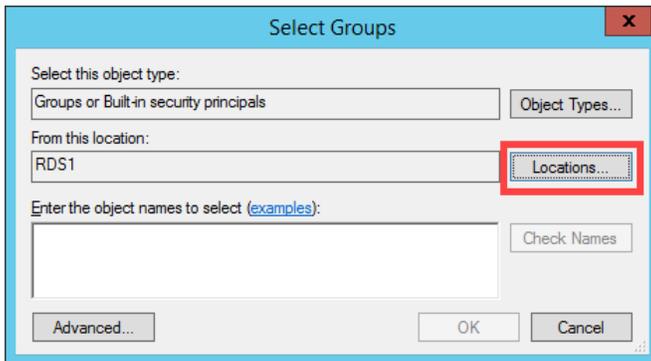
1. In the **Explorer** view, browse to **Network (THIS COMPUTER) → System → Users and Groups → User Groups**, right click **User Groups** and select **New | Windows-Linked User Group...** from the menu.



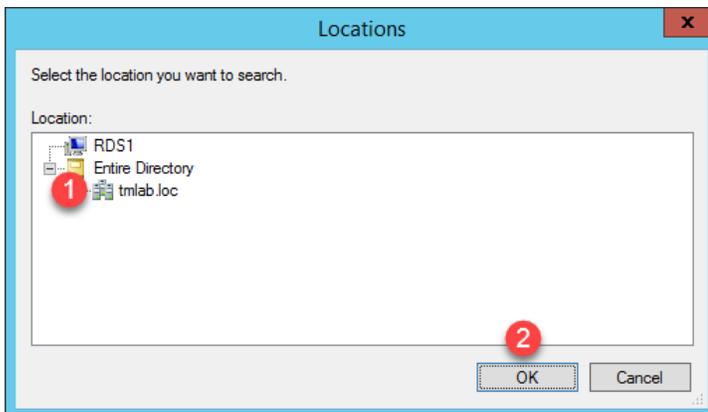
- From the **New Windows-Linked User Group** popup, click the **Add** button.



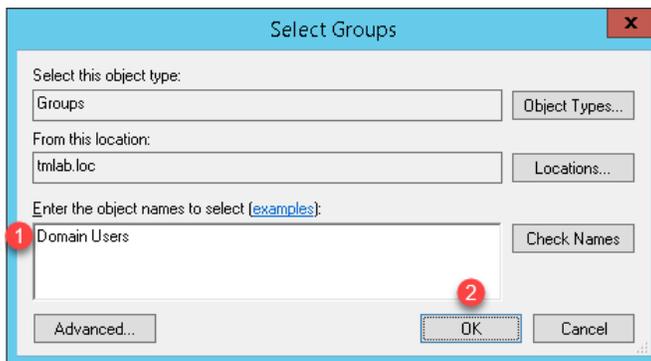
- By default, this dialog box will show the local computer's user and groups, but we want to browse the **TMLAB** domain. From the **Select Groups** window, click the **Locations...** button.



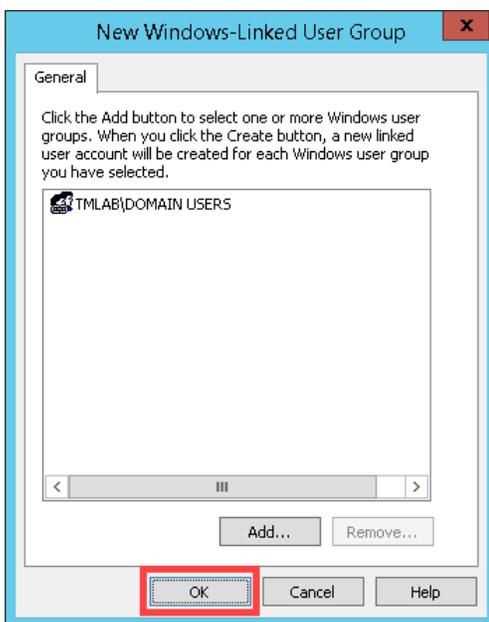
- From the **Locations** selection box, expand the **Entire Directory** item and select the **tmlab.loc** item. Click the **OK** button.



5. Back at the **Select Groups** window, enter *Domain Users* in the text box and click the **OK** button.



6. From the **New Windows-Linked User Group** window, you should now have **TMLAB\DOMAIN USERS** listed. Click the **OK** button.



7. Close the **FactoryTalk Administration Console**.

In your deployments, you will most likely want to be more selective with which Windows user groups to link and to which FactoryTalk group to assign them. This section utilized the entire Domain Users group to simplify the lab going forward.

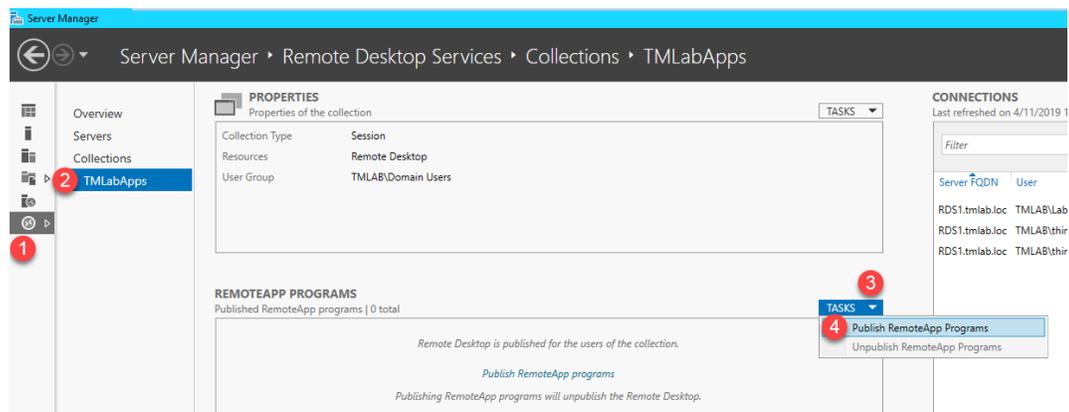
Create a RemoteApp for FactoryTalk View SE

Remote Desktop Services considers any program configured to run initially - like the one you are about to configure with ThinManager ApplicationLink in this section - an "Initial Program." By default, Windows Server 2008R2 and later Remote Desktop Services requires that each Initial Program be added to the published RemoteApp list, or you will receive an Access Denied message when the Display Client attempts to launch.

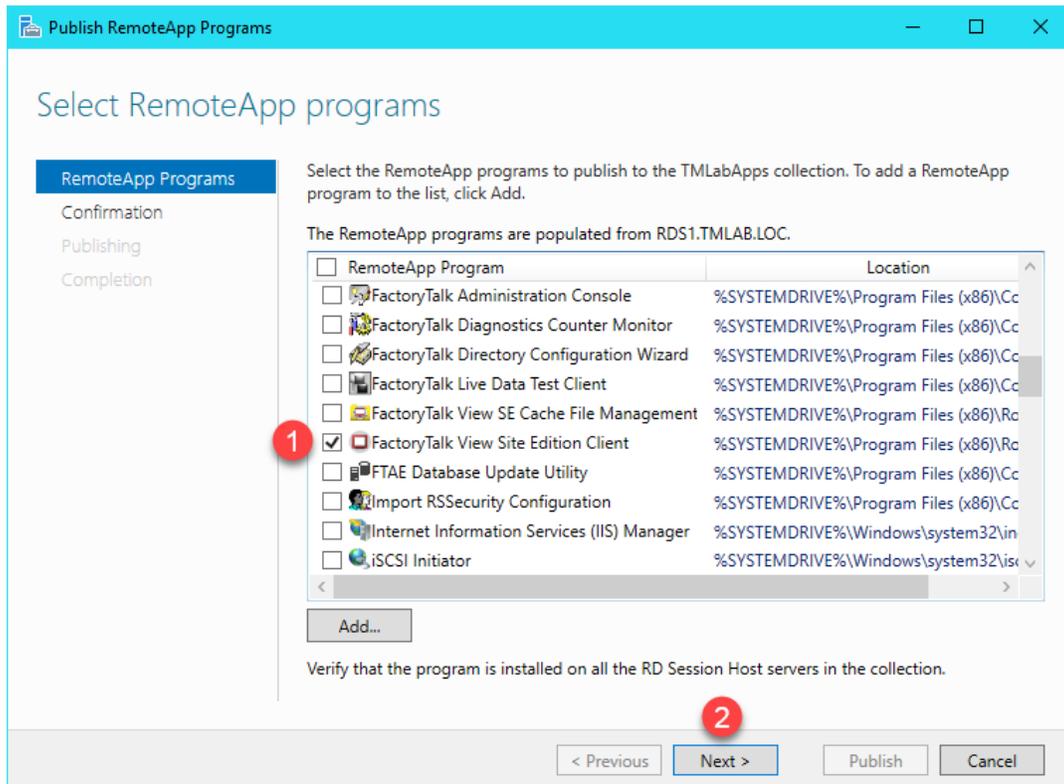
While it is recommended that this default security measure be maintained, it can also be disabled through Local or Group Policy (from the Group Policy Editor: Default Domain Policy | Computer Configuration | Policies | Administrative Templates | Windows Components | Remote Desktop Services | Remote Desktop Session Host | Connections | Allow remote start of unlisted programs).

With Windows Server 2012 or newer, the RemoteApp list is managed through Session Collections for domain deployments. In this lab we will maintain the default security behavior and maintain the RemoteApp list. A number of RemoteApps have already been added. In this section, you will add a new one for the FactoryTalk View SE Client application.

1. From the RDS1 image, launch **Server Manager** by clicking the **Server Manager** icon  from the **Windows** taskbar. **MAKE SURE YOU CLICK THE SERVER MANAGER ICON ON THE RDS1 IMAGE AND NOT THE SHADOW OF THE THIN CLIENT.**
2. From **Server Manager**, select the **Remote Desktop Services** panel item, followed by the **TMLabApps** panel item (under **Collections**).
3. Click the **Tasks** dropdown list in the **RemoteApp Programs** frame, followed by the **Publish RemoteApp Programs** item.



- From the **Publish RemoteApp Programs** dialog, scroll down and check the **FactoryTalk View Site Edition Client** list item, followed by **Next>**.



- Click the **Publish** button on the **Confirmation** page.
- Once **Status** changes to **Published**, click the **Close** button.

7. Right click the newly listed **RemoteApp** and select **Edit Properties**.

The screenshot shows the Server Manager interface. The breadcrumb path is "Server Manager > Remote Desktop Services > Collections > TMLabA". The left-hand navigation pane has "Collections" selected, with "TMLabApps" highlighted. The main area is divided into two sections: "PROPERTIES" and "REMOTEAPP PROGRAMS".

PROPERTIES
Properties of the collection

Collection Type	Session
Resources	RemoteApp Programs
User Group	TMLAB\Domain Users

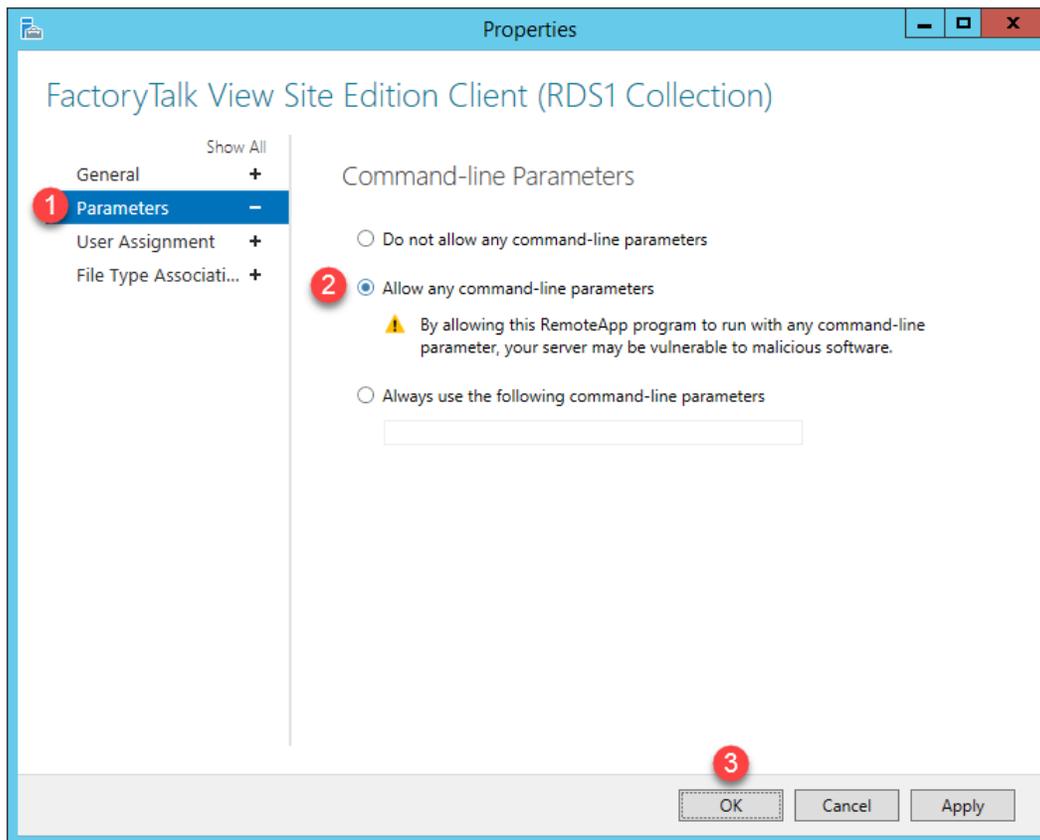
REMOTEAPP PROGRAMS
Last refreshed on 4/11/2019 11:43:12 AM | Published RemoteApp programs | 1 total

Filter [] [] []

RemoteApp Program Name	Alias	Visible in RD Web Access
FactoryTalk View Site Edition Client	DisplayClient	Yes

A red circle with the number "1" is positioned over the first row of the table. A red circle with the number "2" is positioned over the "Edit Properties" button in the right-hand corner of the table row.

8. Select the **Parameters** panel item and then select the **Allow any command-line parameters** option. Click the **OK** button and the close **Server Manager**.



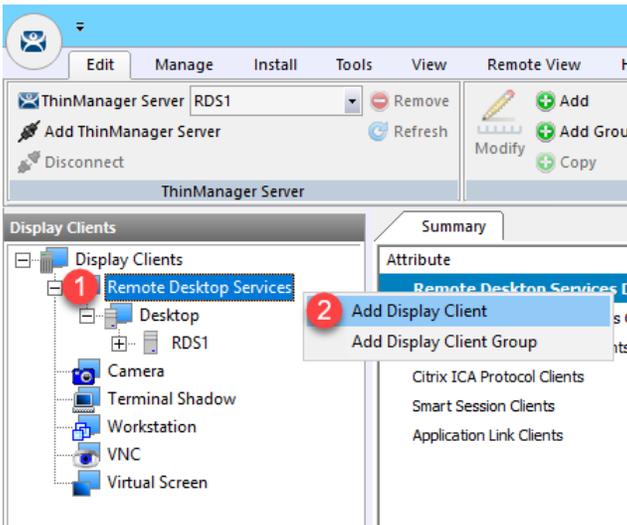
If your RemoteApp requires command line parameters, then selecting Allow any command-line parameters is less than secure than selecting Always use the following command-line parameters. We have chosen the less secure option for this lab as you will be creating several ThinManager Display Clients, each of which will launch a separate FactoryTalk View SE Client configuration file, and therefore require a different command-line. This option was chosen simply to save time in the lab.

Create a New ThinManager Display Client with Application Link

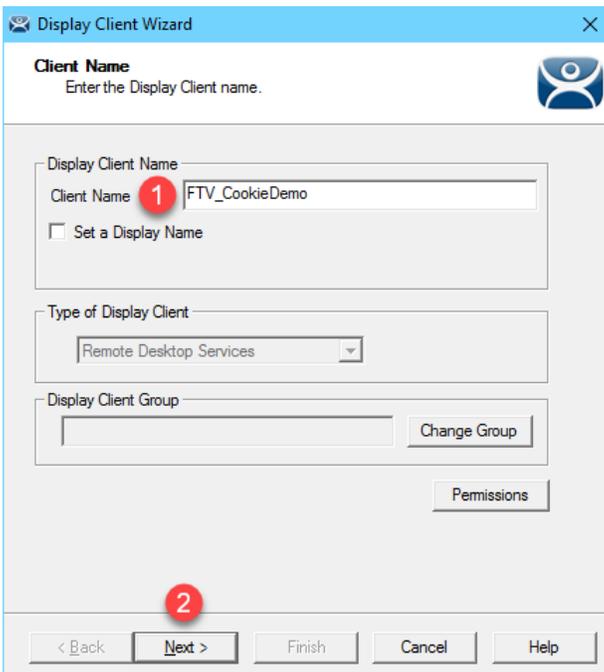
1. Return to ThinManager and click the **Display Clients** icon  from the ThinManager tree selector.



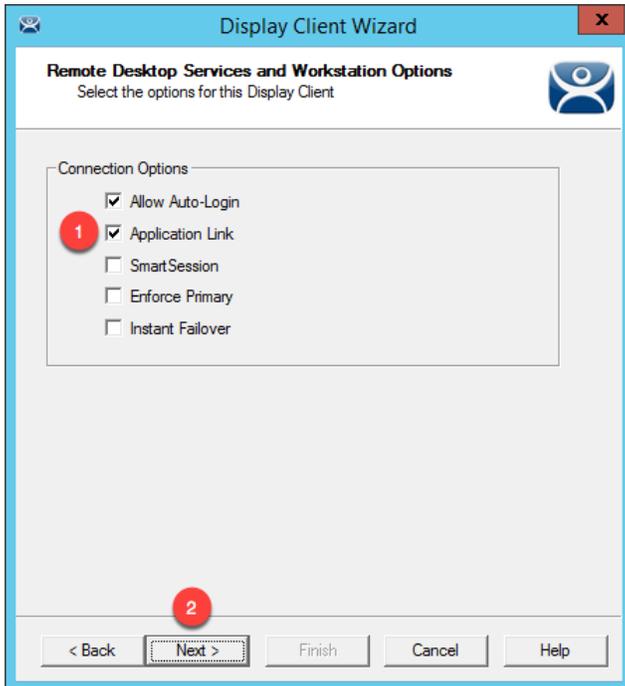
2. From the **Display Clients** tree, right click the **Remote Desktop Services** branch and select **Add Display Client**. This will launch the **Display Client Wizard**.



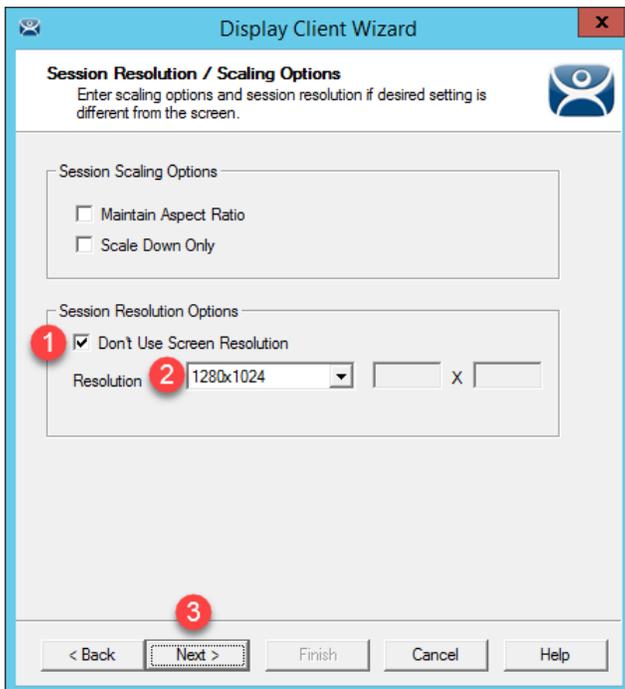
3. Type *FTV_CookieDemo* as the **Client Name** on the **Client Name** page of the wizard. Click the **Next** button.



- Click the **Next** button on the **Display Client Options** page of the wizard.
- Check the **Application Link** checkbox on the **Remote Desktop Services and Workstation Options** page of the wizard. Click the **Next** button.

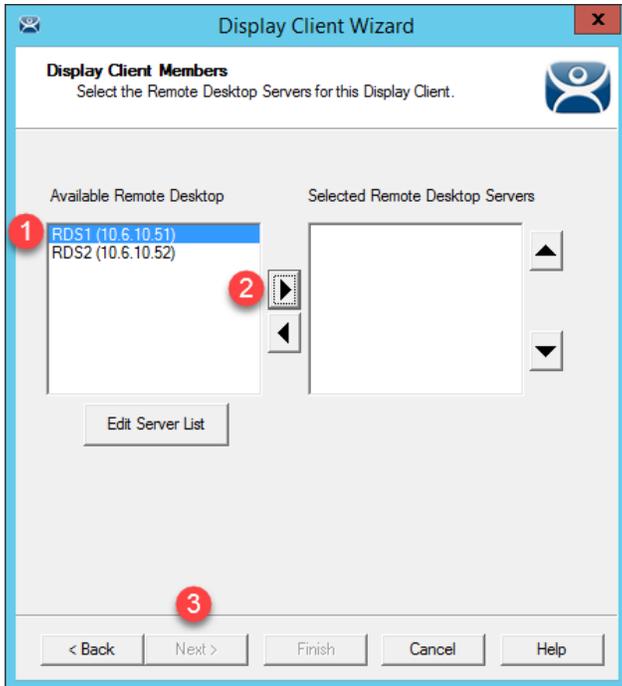


- From the **Screen Resolution / Scaling Options** page of the wizard, check the box for **Don't Use Screen Resolution**, and select **1280x1024** from the **Resolution** drop down list. Click the **Next** button.



By default, Remote Desktop Services sessions are started using the screen resolution of the Terminal Profile where the Display Client is assigned. This setting overrides that behavior for this Display Client. So even if the screen resolution of the terminal is different, this Display Client will start with a resolution of 1280x1024, and ThinManager will automatically scale it to fit the screen resolution of the physical display where it is delivered.

7. Select **RDS1** from the **Available Remote Desktop Servers** list and click the **Right Arrow** button to move it to the **Selected Remote Desktop Servers** list. This is the Remote Desktop Server on which this **Display Client** will run. Click the **Next** button.



8. From the **AppLink** page of the wizard, enter the following path for the **Program Path and Filename** field and **Command Line Options** field (you can also copy and paste these paths from the **LabPaths.txt** file by right clicking the **Notepad** icon pinned to the start bar and selecting **LabPaths.txt**):

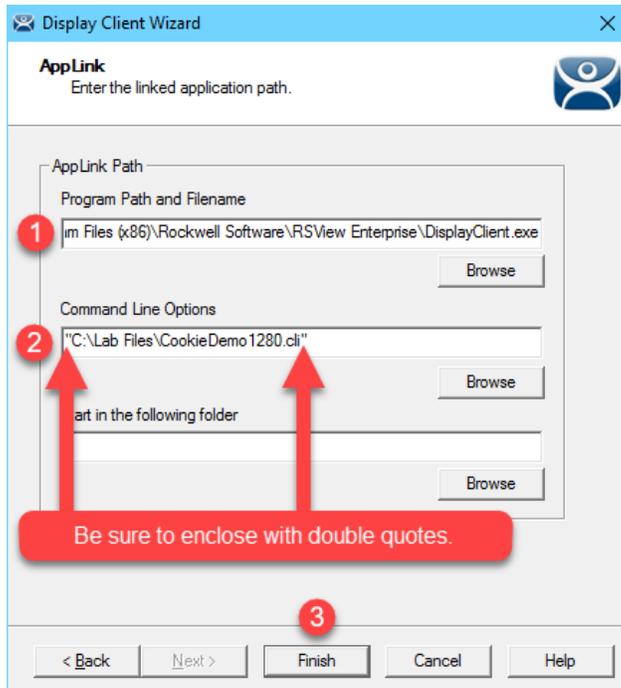
Program Path and Filename:

```
C:\Program Files (x86)\Rockwell Software\RSView  
Enterprise\DisplayClient.exe
```

Command Line Options:

```
"C:\Lab Files\CookieDemo1280.cli"
```

9. Make sure to enclose the **Command Line Options** path in double quotes. Click the **Finish** button.

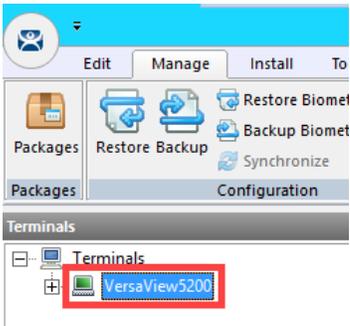


Apply New Display Client to Terminal

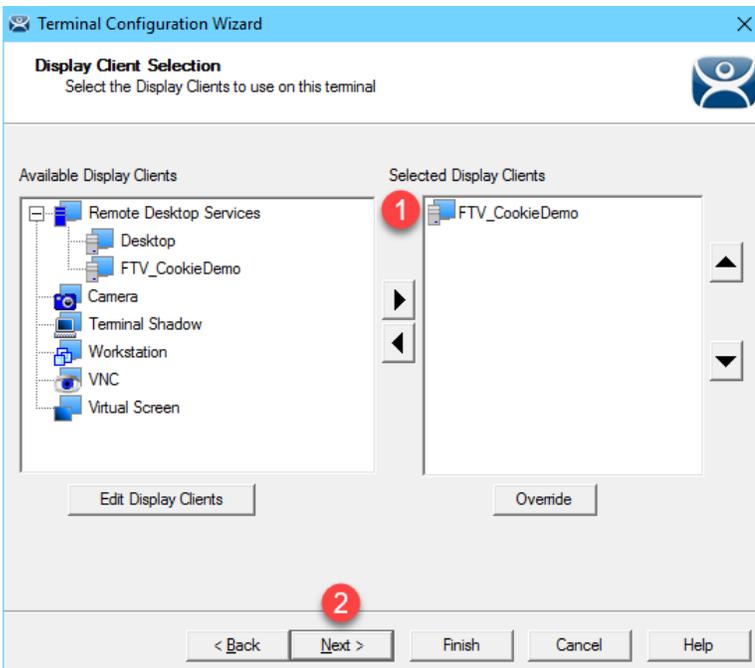
1. Click the **Terminals** icon  from the ThinManager tree selector.



2. From the **Terminals** tree, double click the **VersaView5200** terminal to launch the **Terminal Configuration Wizard**.



3. Click the **Next** button on the **Terminal Name** page of the wizard.
4. Click the **Next** button on the **Terminal Hardware** page of the wizard.
5. Click the **Next** button on the **Terminal Options** page of the wizard.
6. Click the **Next** button on the **Terminal Mode Selection** page of the wizard.
7. Select **FTV_CookieDemo** from the **Available Display Clients** list and click the **Right Arrow** button to move it to the **Selected Display Clients** list. Select **Desktop** from the **Selected Display Clients** list and click the **Left Arrow** button to move it to the **Available Display Clients** list. Click the **Next** button.



8. Click the **Next** button on the **Terminal Interface Options** page of the wizard.
9. Click the **Next** button on the **Hotkey Configuration** page of the wizard.
10. On the **Log In Information** page of the wizard, enter *thin01@tmlab.loc* as the **Username** and *rw* as the **Password**. The terminal will use these credentials to login to the Remote Desktop Server for those Display Clients applied to it that have the **Allow Auto Login** property enabled. Click the **Verify** button which should confirm that the credentials entered are valid. Click the **Next** button.

Terminal Configuration Wizard

Log In Information
Enter the log in information to log in automatically. Leave the log in information blank or fill only some of the fields to force manual log in.

Windows Log In Information

Username **1** thin01@tmlab.loc Search

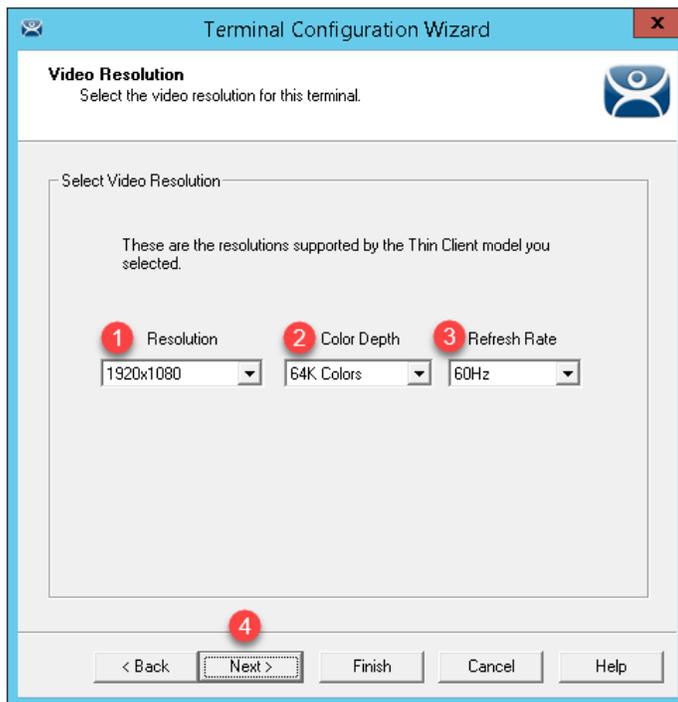
Password **2** Password Options

Domain **3** Verify

4

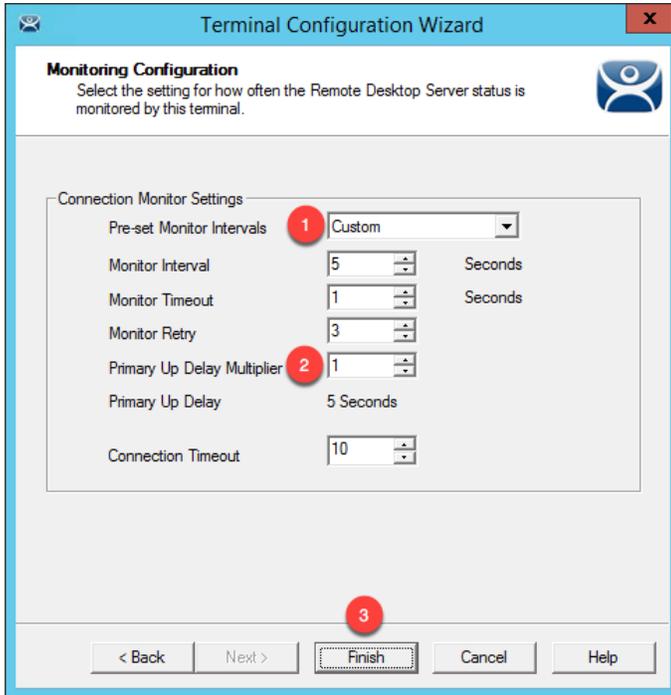
< Back Next > Finish Cancel Help

11. From the **Video Resolution** screen of the wizard, select **1920x1080** as the **Screen Resolution**, **64K Colors** as the **Color Depth** and **60Hz** as the **Refresh Rate**. Click the **Next** button.

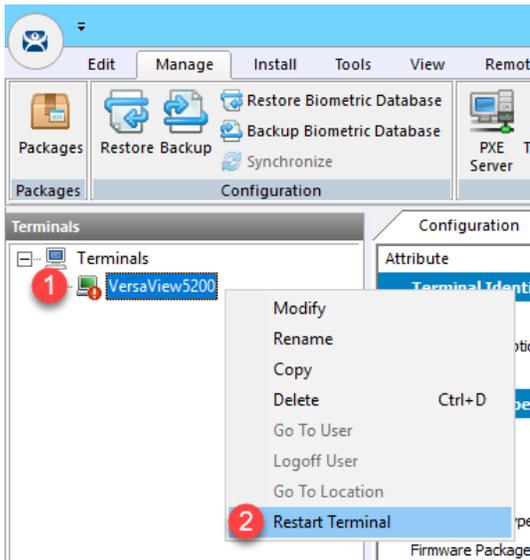


12. Click the **Next** button on the **Module Selection** page of the **Terminal Configuration Wizard**.
13. Click the **Next** button on the **ThinManager Server Monitor List** page of the **Terminal Configuration Wizard**.

14. From the **Monitoring Configuration** page of the wizard, select the **Custom** radio button within the **Monitor Interval**. Keep the defaults for **Monitor Interval**, **Monitor Timeout** and **Monitor Retry**. Enter a value of **1** for the **Primary Up Delay Multiplier**. This will speed up the Remote Desktop Server failover time in a later section. Click the **Finish** button.



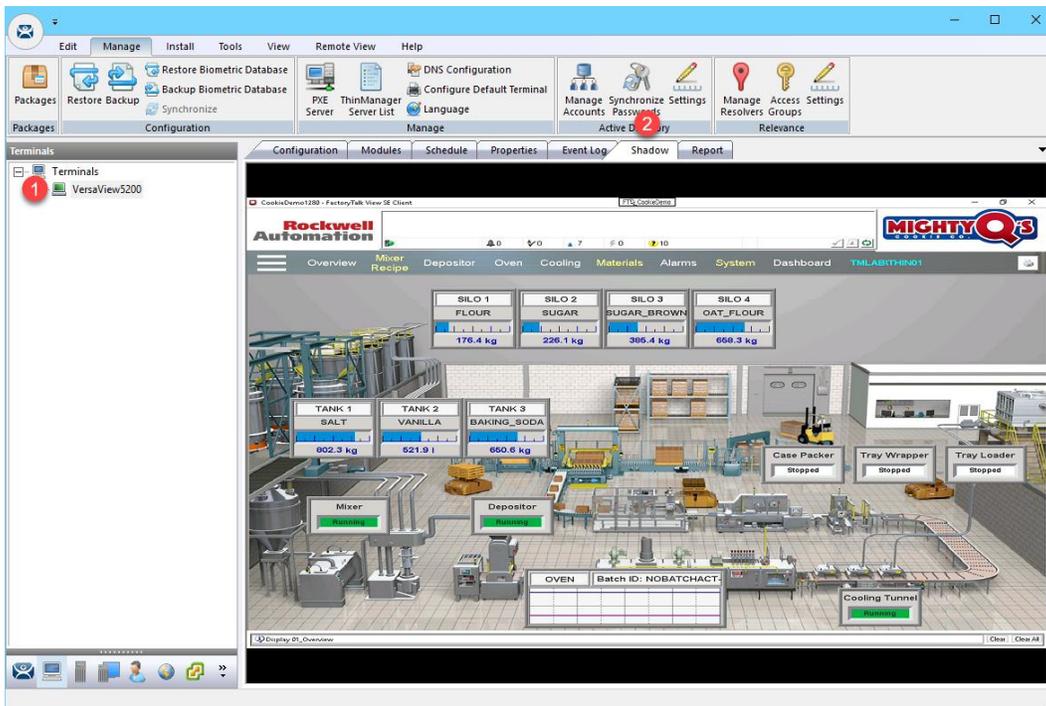
15. Right click the **VersaView5200** terminal from the **Terminals** tree and select **Restart Terminal** to apply the changes. Click **Yes** to restart the terminal.



You may notice a small red exclamation icon appear in the bottom of the terminal icon. This indicates that a change has been made to the terminal's configuration that has not been published to the terminal yet. Restarting the terminal will republish the terminal's configuration, including any recent changes.

If you need to apply a change to a terminal's configuration, simply right click the terminal of interest from the Terminals tree and select **Restart Terminal**. Restarting a terminal simply reapplies the terminal's configuration – unless ThinManager automatically detects a configuration change that requires a terminal reboot, in which case a reboot is performed. **Reboot Terminal**, available from the **Tools** ribbon bar, is equivalent to cycling power to the terminal, and therefore resends the firmware as well as the configuration. It is important to note that in both of these cases the sessions running on the Remote Desktop Servers are not restarted by default. You need to perform a **Reset Session** in this case. To reset a session, return to the **Display Servers** tree segment, and select the Remote Desktop Server on which the session of interest is running. Select the **Sessions** tab from the **Details Pane**. A list of all of the sessions running on the selected Remote Desktop Server will be displayed. Right click the session desired and select **Reset Session**.

- With the **VersaView5200** terminal still selected, click on the **Shadow** tab in the Details Pane of **ThinManager**. If the **Shadow** does not start, click the **Configuration** tab, then the **Shadow** tab to reactivate the shadow. The **CookieDemo** application utilized was developed as a 1280x1024 application, yet we are delivering it to a 1920x1080 display. While it appears to be stretched, this is due to the fact that we are going from a 4x3 aspect ratio to a 16x9 ratio, but ThinManager's new session scaling delivers the 1280x1024 session without bars to a 1920x1080 display.



17. If you click the red “X” in the top right corner of FactoryTalk View SE application (either from the Shadow or at the virtual thin client), it will close, leaving an empty black screen **without** a desktop.

Once the application closes, you will see the desktop background with no Start menu bar for about 30 seconds before you are automatically logged out. When using AppLink, the user does not have access to any other programs or the desktop when connecting and once that application terminates, the user is automatically logged off. The logoff delay is due to the FactoryTalk View Site Edition client continuing to shut down in the background after the display is closed.

If you hit the CTRL+ALT+DEL keyboard sequence from the virtual thin client (by clicking the icon in the taskbar of VMWare Player) while the empty black screen is active, you will be presented with the Task Manager, from which Windows File Explorer could certainly be launched. With ThinManager, this is easily rectified by adding the Key Block Module to your terminal(s), which is a simple way to block common keyboard sequences like CTRL+ALT+DEL, CTRL+ESC, etc. You will use the Key Block Module in [Section 12](#).

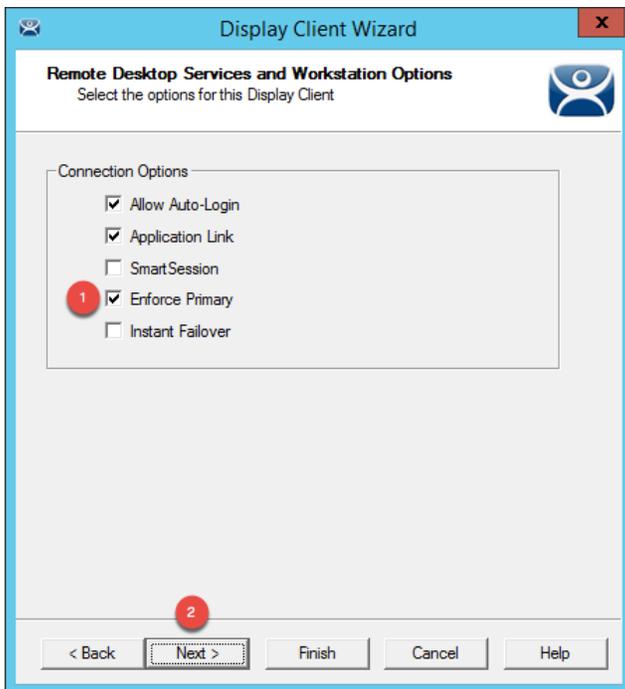
A module is a small driver that can be applied to a terminal to provide additional capabilities. For example, ThinManager includes 15 unique Touch Screen Modules, a Redundant Ethernet Module for thin clients with dual Ethernet ports (provides automatic failover of network interfaces connected to the thin client) as well as a MultiSession Screen Saver Module (each Display Client applied to a thin client is automatically cycled on a configurable time basis as a screen saver) – just to name a few. Modules are added to a terminal using the Terminal Configuration Wizard and will be explored in more detail, as mentioned above, in [Section 12](#).

Add Automatic Remote Desktop Server Failover

1. From the RDS1 image, select the **Terminals** tree, expand the **VersaView5200** terminal. Double click the **FTV_CookieDemo** Display Client under the **VersaView5200** terminal to launch the **Display Client Wizard**.

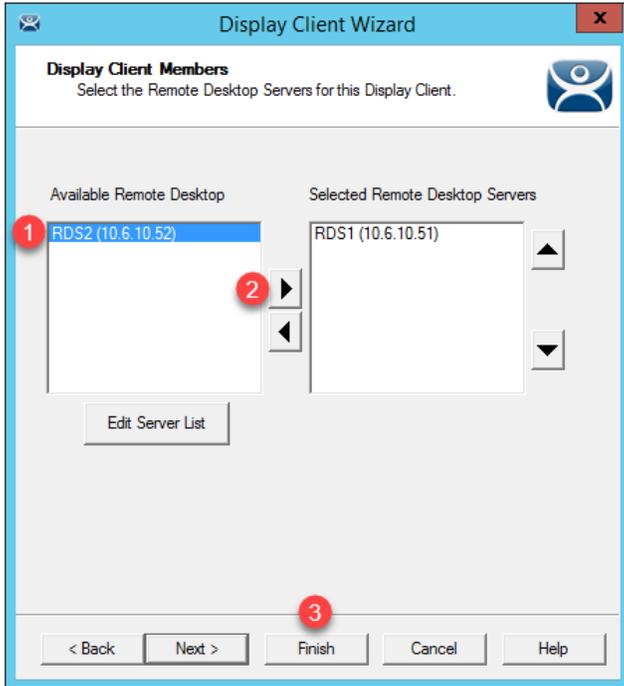


2. Click the **Next** button on the **Client Name** page of the wizard.
3. Click the **Next** button on the **Display Client Options** page of the wizard.
4. Check the **Enforce Primary** checkbox on the **Remote Desktop Services and Workstation Options** page of the wizard. Click the **Next** button.



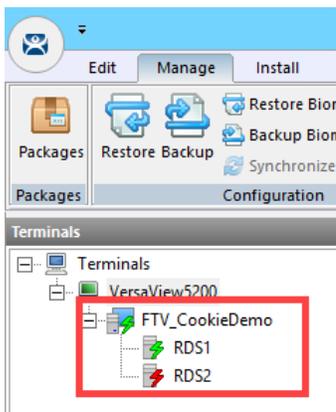
5. Click the **Next** button on the **Screen Resolution / Scaling Options** page of the wizard.

6. Select **RDS2** from the **Available Remote Desktop Servers** list and click the **Right Arrow** button to move it to the **Selected Remote Desktop Servers** list. Click the **Finish** button.

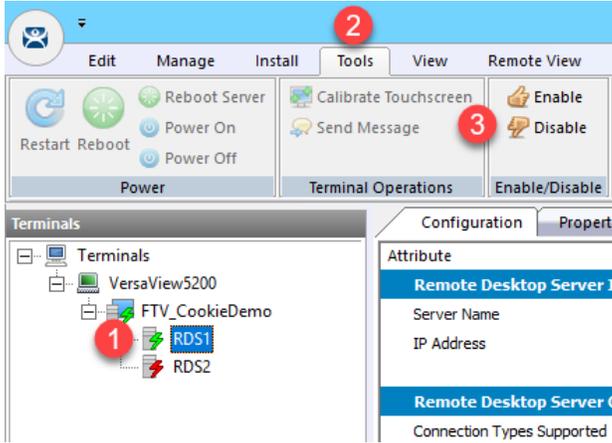


By adding more than 1 Remote Desktop Server to the **Selected Remote Desktop Servers** list, you have added automatic Remote Desktop Server failover for this Display Client. The order of the servers listed determines the order of failover. In this case, **RDS1** would be the primary and **RDS2** would be the secondary. There is no limit to how many Remote Desktop Servers you can add, the terminal will just keep failing to the next available server in the list.

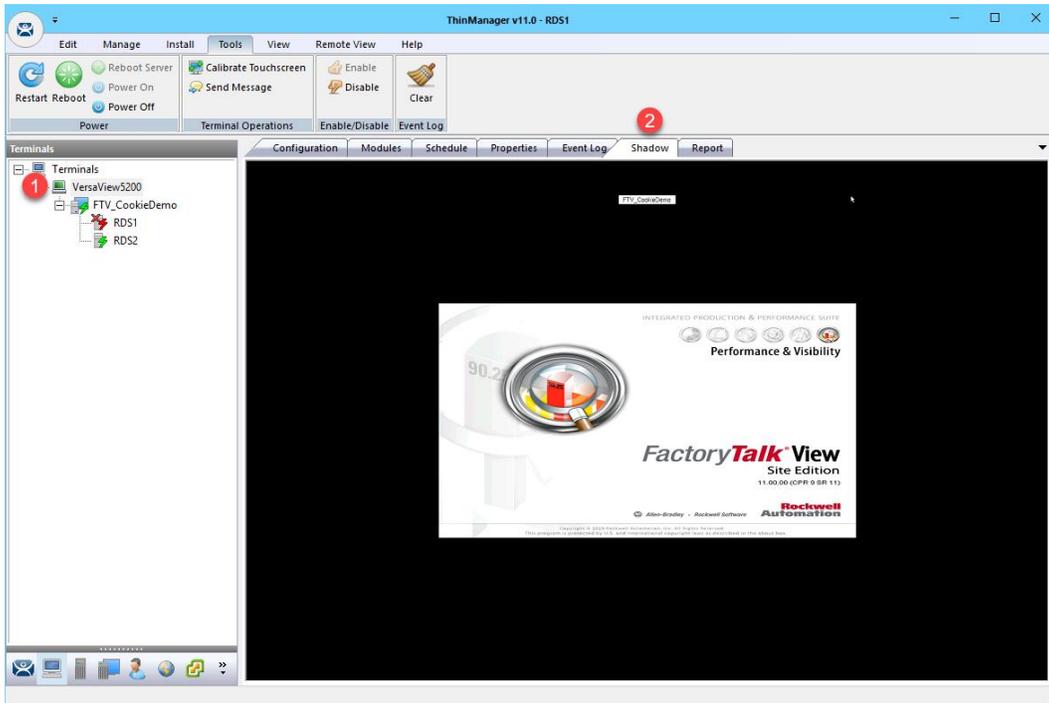
7. Right click the **VersaView5200** terminal and select **Restart Terminal** to apply the changes. Click **Yes** on the confirmation dialog box. If you expand the **VersaView5200** terminal, and then expand the **FTV_CookieDemo** Display Client, you will now see both **RDS1** and **RDS2** are listed. The green lightning bolt next to **RDS1** indicates that the session being delivered to the terminal is running on **RDS1**. Notice that **RDS2** has a red lightning bolt next to it.



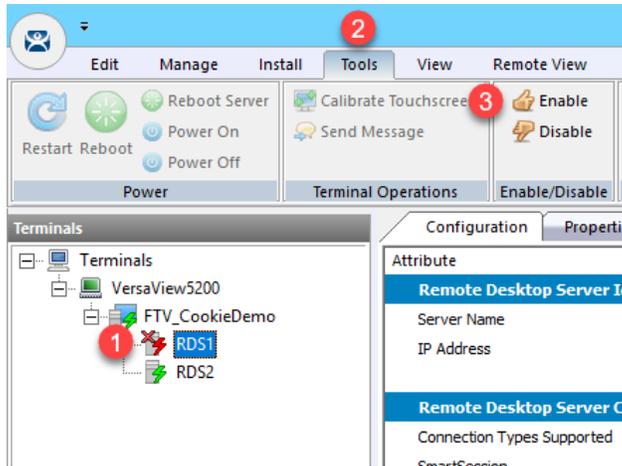
- To force a failover to occur, we can manually disable the **RDS1** Remote Desktop Server from **ThinManager**. This will disconnect all Remote Desktop Server sessions connected to **RDS1**. From the **Terminals** tree, expand the **VersaView5200** terminal, and then expand the **FTV_CookieDemo** Display Client. Select the **RDS1** Remote Desktop Server under the **FTV_CookieDemo** Display Client. With **RDS1** selected, click the **Tools** ribbon, followed by the **Disable** icon.



- If you quickly shadow **VersaView5200** (or look at your demo kit) you will see the new FactoryTalk View SE session launching on **RDS2**. To shadow, simply select **VersaView5200** from the **Terminals** tree and then click the **Shadow** tab from the Details Pane. With the **RDS1** Remote Desktop Server disabled, its icon has changed from a green lightning bolt to a red lightning bolt with an X, while the **RDS2** Remote Desktop Server has changed from a red lightning bolt to green.



10. To re-enable **RDS1**, select **RDS1** from the **Terminals** tree and then click the **Enable** button in the **Tools** ribbon. Notice that the green lightning bolt returns to **RDS1**, while **RDS2** returns to red. The active session on the terminal has returned to the primary, **RDS1**. This is because we checked the **Enforce Primary** option of the **Display Client Wizard** in a previous step.



There are actually 2 types of automatic Remote Desktop Server failover supported by ThinManager. The one demonstrated above is called **Standard Failover**. With **Standard Failover**, the failover session is started on-demand. The other type is called **Instant Failover**, which differs by keeping sessions running on each Remote Desktop Server – the active one, and a hot standby one. **Instant Failover** is a great option for deployments that cannot be without visualization for any length of time. Otherwise, **Standard Failover** is perfectly suitable. To enable **Instant Failover** in our example above, we would have additionally checked the **Instant Failover** checkbox in Step 4 above.

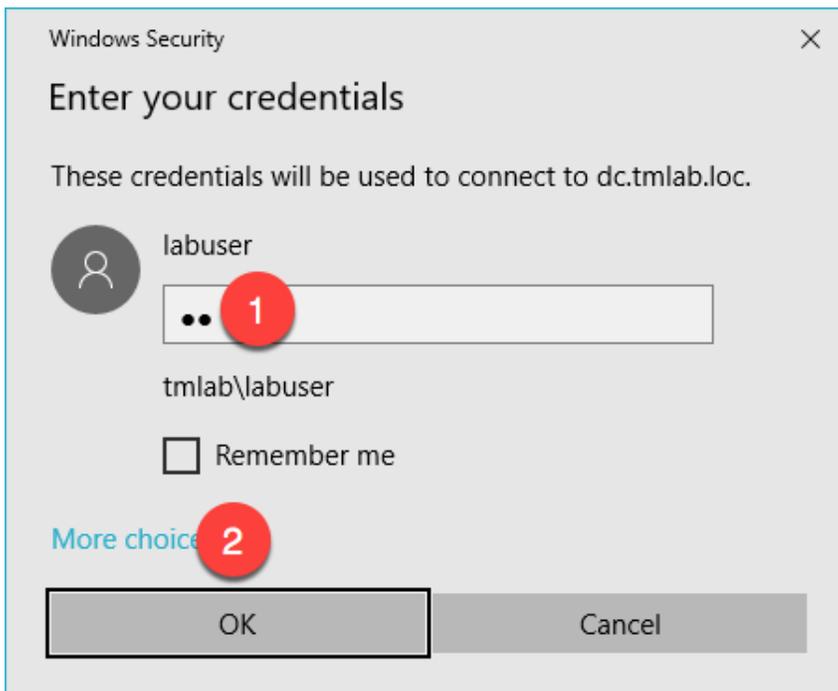
Allow Remote Start of Unlisted Programs

As described previously, Remote Desktop Services considers any program configured to run initially - like the ones used with ThinManager **ApplicationLink** - an "Initial Program." By default, Windows Server 2008R2 and later Remote Desktop Services requires that each Initial Program be added to the published **RemoteApp** list, or you will receive an Access Denied message when the **Display Client** attempts to launch. Previously in this section, the **FactoryTalk View SE Client** was added to the **RemoteApp** list. In this lab, we are going to disable this default behavior via **Group Policy**, resulting in the ability to launch any initial program through Remote Desktop Services without having to maintain the **RemoteApp** list. Through **Group Policy**, we can make this change on the **Domain Controller** and update both **RDS1** and **RDS2** to receive the policy change.

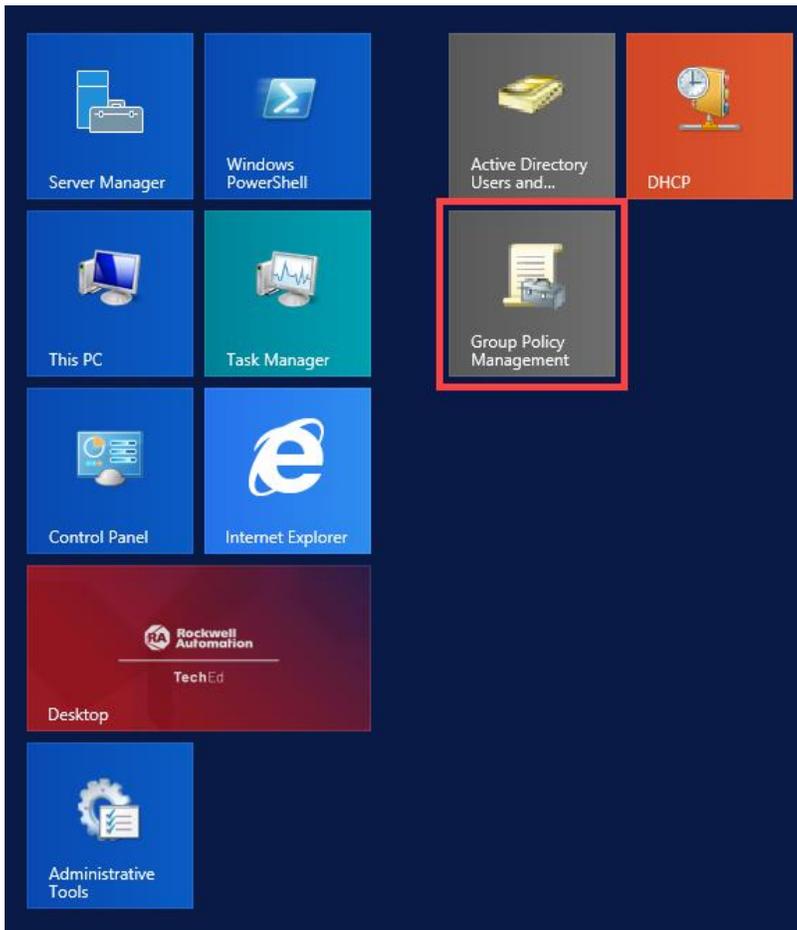
1. Minimize the **ThinManager Admin Console** if it is maximized and double click the **dc.tmlab.loc** shortcut on the desktop to launch a remote desktop session on the **DC** virtual image.



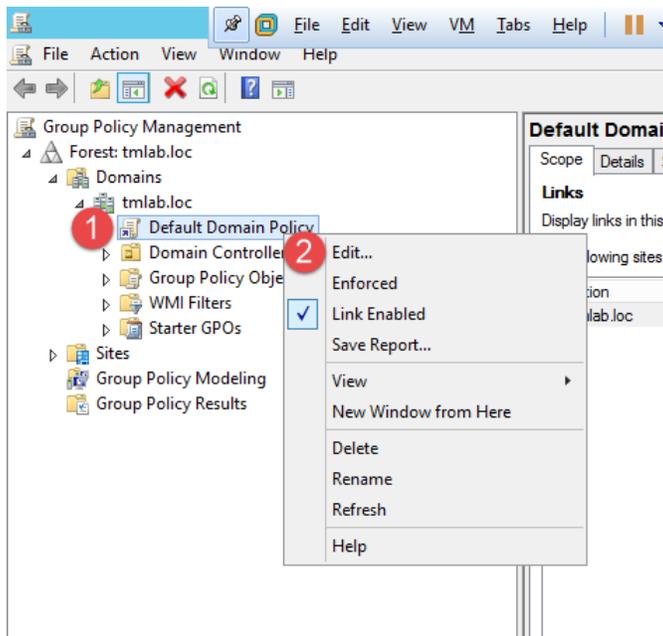
2. If you are prompted to enter login credentials, make sure the username is *tmlab\labuser* and enter a password of *nw*.



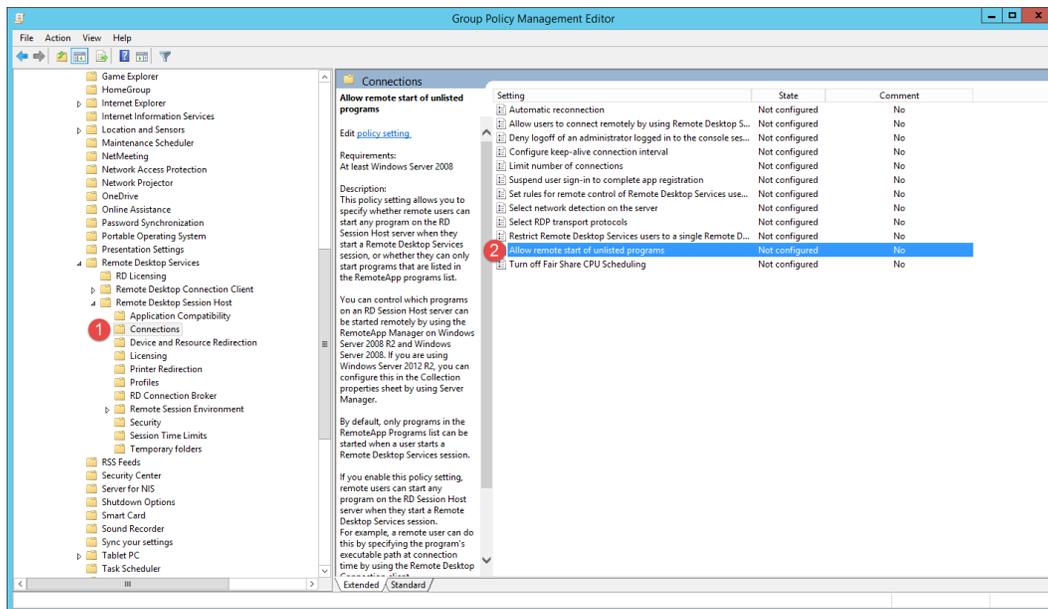
3. Click the **Windows Start** button.
4. From the **Windows Start Menu**, click the **Group Policy Management** icon.



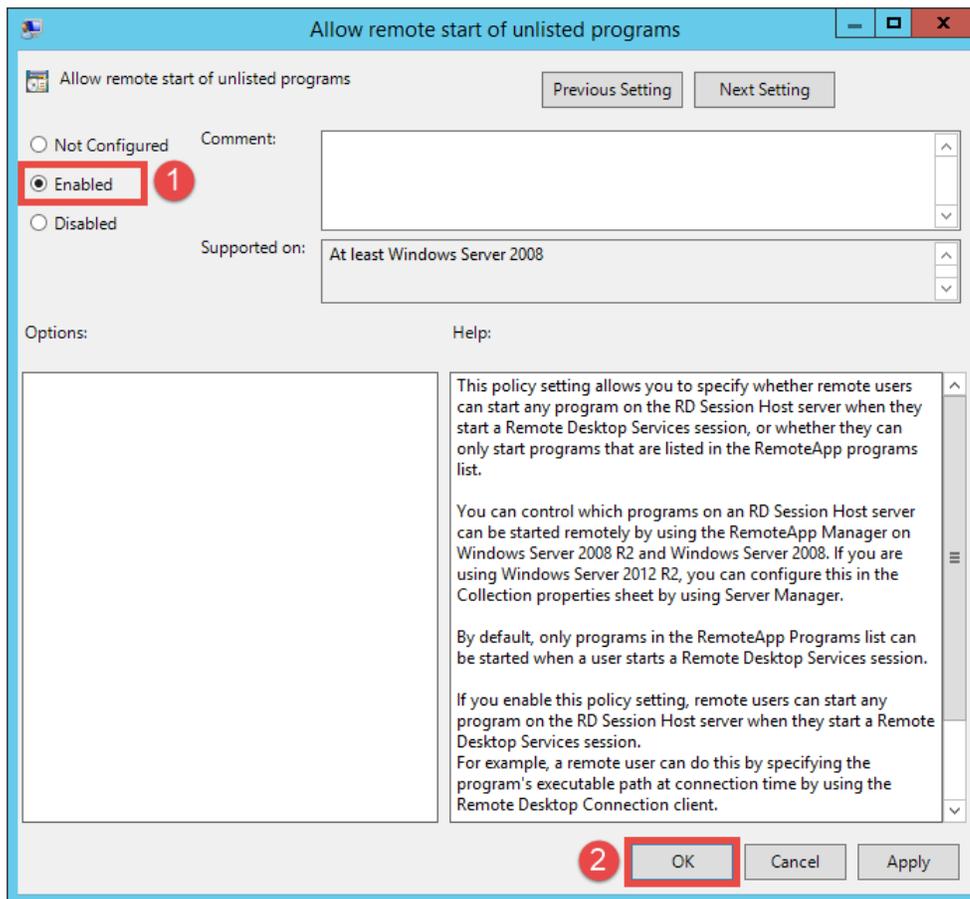
- From the **Group Policy Editor**, right click the **Default Domain Policy** item and click **Edit...**



- From the **Group Policy Management Editor**, navigate to **Default Domain Policy [DC.TMLAB.LOC] Policy → Computer Configuration → Policies → Administrative Templates → Windows Components → Remote Desktop Services → Remote Desktop Session Host → Connections**. Double click the **Allow remote start of unlisted programs** setting on the right-hand side.



7. From the ensuing policy setting dialog box, click the **Enabled** option button followed by the **OK** button. Close the **Group Policy Management Editor** and the **Group Policy Management** window.



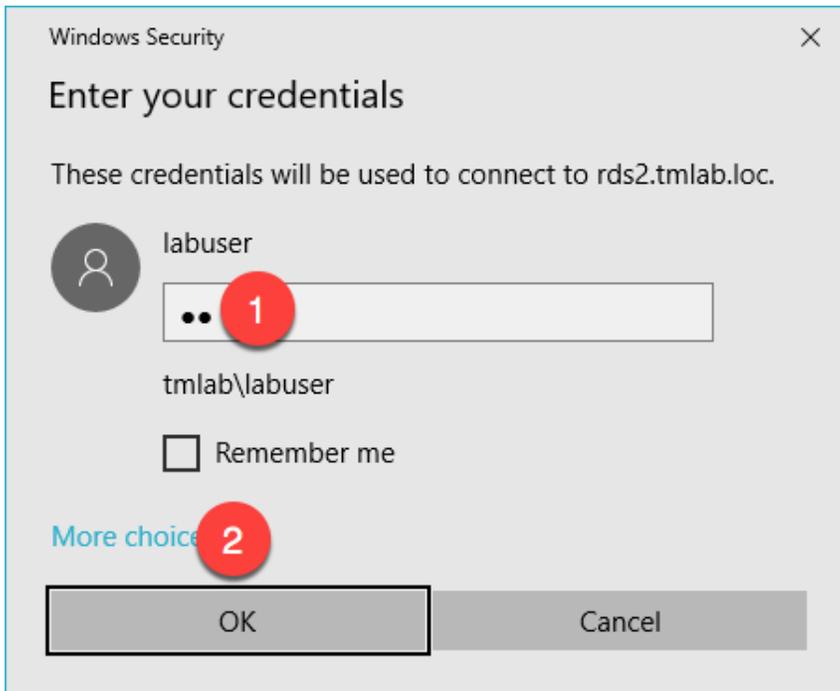
8. Close the remote desktop session on **dc.tmlab.loc**. Click **OK** to the confirmation dialog box.



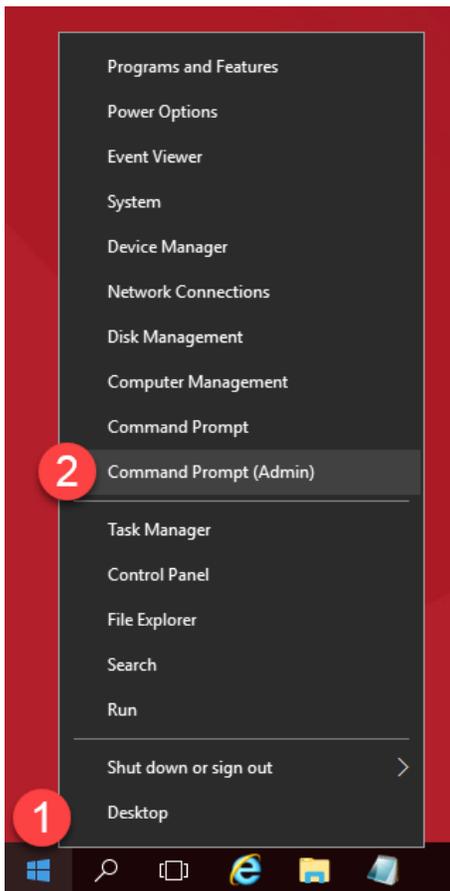
9. The **Group Policy** does not take effect immediately on the member **Remote Desktop Servers**. The final steps of this section will force the update to occur. To apply the change to **RDS2**, double click the **rds2.tmlab.loc** shortcut on the **RDS1** desktop.



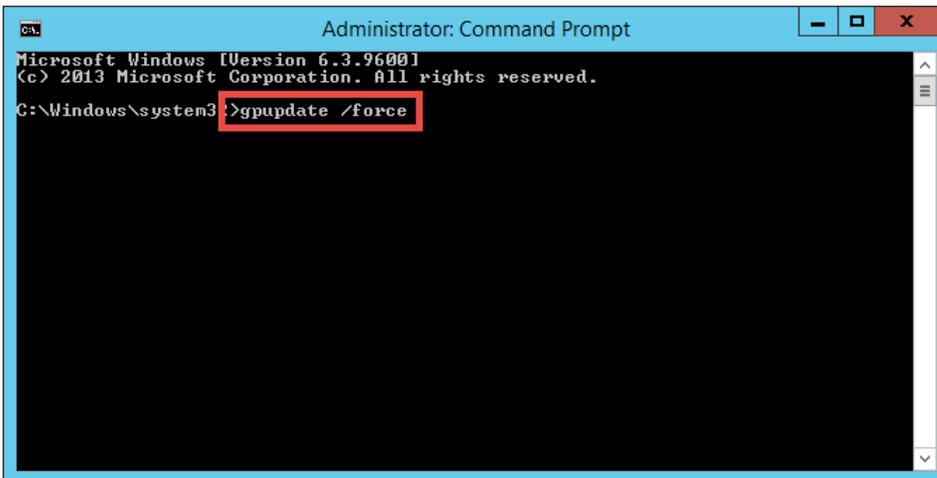
10. If you are presented with a login dialog box, make sure the username is *tmlab\labuser* and enter a password of *rw*.



11. From RDS2, right click the **Windows Start Button** and click **Command Prompt (Admin)**.

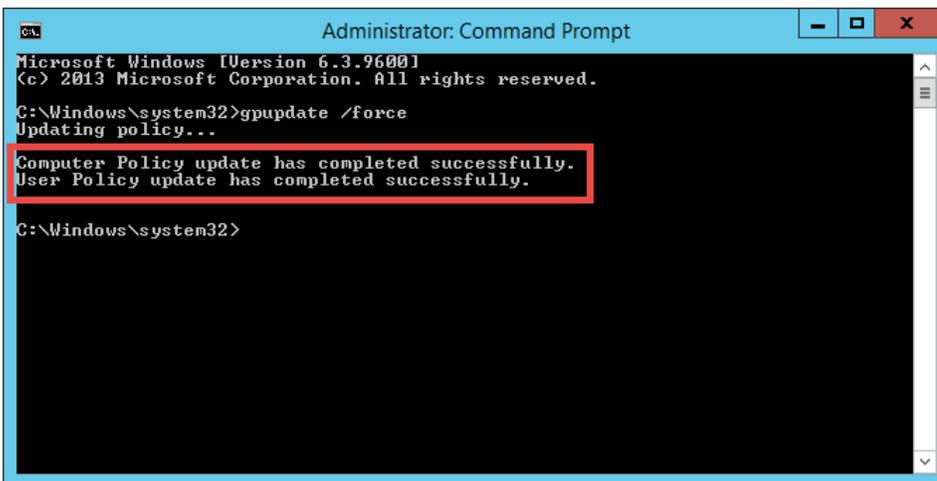


12. From the **Administrator: Command Prompt** window, enter `gpupdate /force` followed by the **ENTER** key.



```
Administrator: Command Prompt
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.
C:\Windows\system32>gpupdate /force
```

13. Once the updated policy has been applied, close the **Administrator: Command Prompt** window.



```
Administrator: Command Prompt
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.
C:\Windows\system32>gpupdate /force
Updating policy...
Computer Policy update has completed successfully.
User Policy update has completed successfully.
C:\Windows\system32>
```

11. Close the remote desktop session on **rds2.tmlab.loc**. Click the **OK** button if you receive a confirmation dialog box.



12. Repeat steps 7 – 11 from above on **RDS1**.

This completes the section **Configuring ThinManager Application Link and Failover for FactoryTalk View SE** of the lab. Continue on to see how easy it is to replace a failed terminal with ThinManager.

Section 3: Terminal Replacement in under 2 Minutes

Overview

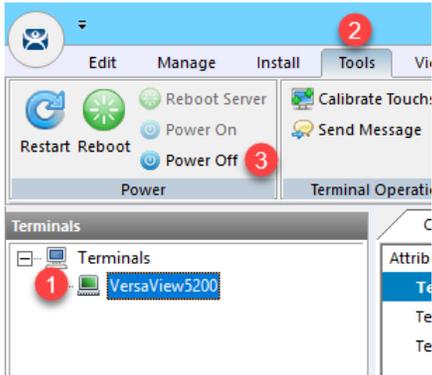
While industrial grade terminals like the **VersaView 5200** do not fail often (since it has no moving parts), it can be replaced in under 2 minutes when it does. Replacement starts by disconnecting the failed terminal and connecting the new terminal in its place. When the new terminal is powered up for the 1st time, ThinManager will recognize that it has not been associated with a ThinManager **Terminal Profile** previously and prompt you to assign one to it. One of the available terminal configurations will be the configuration for the failed terminal, since it is no longer in service. Once that terminal configuration is selected, ThinManager will create an association between the **Terminal** and **Terminal Profile** based on the **MAC address** of the terminal, and will therefore not prompt for this assignment on subsequent reboots of the terminal. Once assigned, the new terminal will essentially assume the identity of the failed terminal and even reconnect to the failed terminal's sessions (Remote Desktop Server, VDI, etc.), which typically are configured to run uninterrupted on the server during this process.

This lab section is composed of the following tasks:

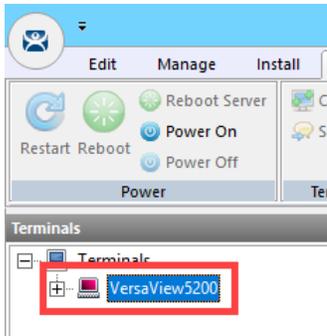
1. Power Down the Virtual Thin Client
2. Reassign the VersaView5200 Terminal Profile

Power Down the Virtual Thin Client

1. Click the **Terminals** icon  from the ThinManager tree selector.
2. Under the **Terminals** node, select the **VersaView5200** terminal.
3. Select the **Tools** ribbon, and then click the **Power Off** icon. Click the **Yes** button on the confirmation dialog box. This will remotely power down the virtual thin client.



4. To confirm, the **VersaView5200** terminal icon in the **Terminals** tree should be **Red** before continuing. The **Thin01** virtual thin client will automatically close upon powering off.

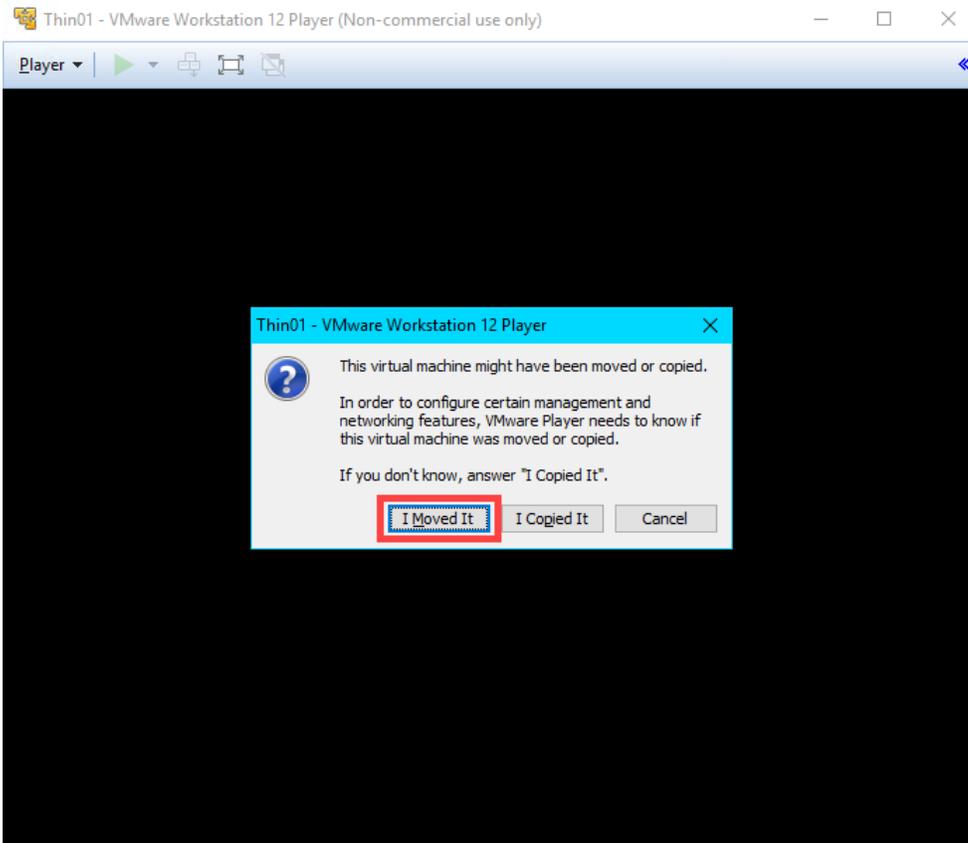


Reassign the VersaView5200 Terminal Profile

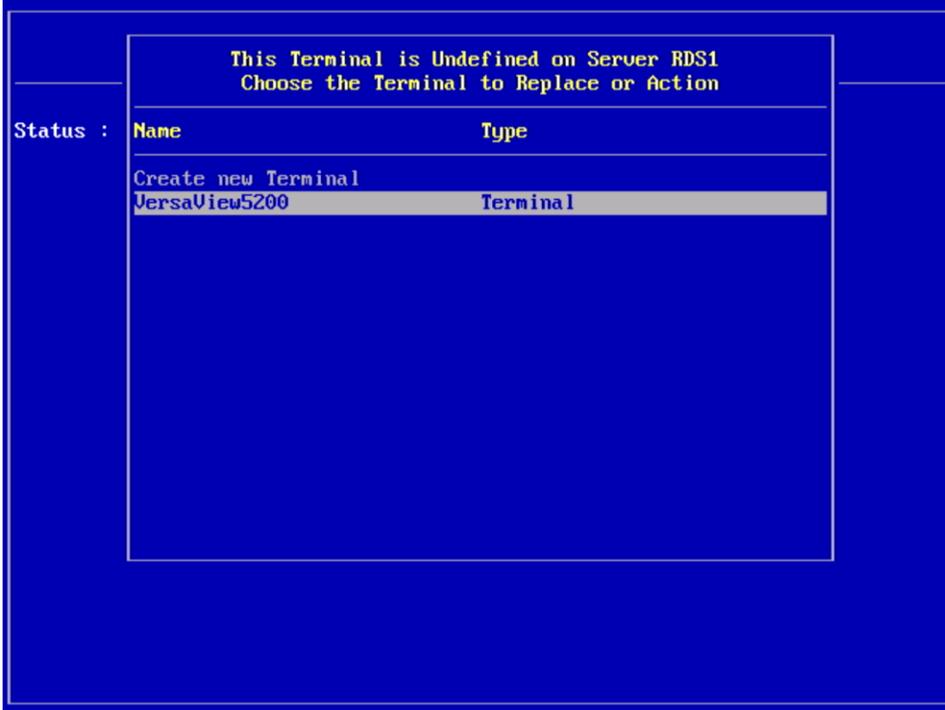
1. Double click the **Thin02** shortcut from the **RDS1** desktop. Since we are using virtual thin clients, you should think of this step as removing a failed physical thin client with a replacement thin client – as the



2. If you receive a message box asking if you moved or copied the virtual machine, click the **I Moved It** button.



3. Upon powering up, the ThinManager firmware should get delivered to the replacement terminal. Because ThinManager does not have an existing terminal configuration that matches the **MAC address** of the replacement unit, you will be prompted to either **Create new Terminal** or select an existing terminal configuration that is currently not active, **VersaView5200**. Select **VersaView5200** from the list using the **Down Arrow** of your keyboard and hit **Enter**.



If this was an actual **ThinManager Ready** terminal, like the **VersaView 5200**, you would have the option of assigning a static IP address to the terminal (or using **DHCP**). **ThinManager Compatible** terminals use **PXE** which is inherently dependent on **DHCP**.

Section 4: Deploying Additional Content Using MultiSession and Tiling

Overview

To this point, we have only delivered a single ThinManager Display Client to **VersaView5200**. First, the **Desktop** Display Client, then the **FTV_CookieDemo** Display Client. This lab will focus on applying multiple Display Clients as well as the options to visualize and switch between them from a ThinManager-managed Terminal. When more than one Display Client is applied to a terminal, it is referred to as **MultiSession**. The Display Clients applied to a terminal can be run from the same Remote Desktop Server, or from multiple Remote Desktop Servers – even on different networks. In addition to Remote Desktop Services Display Clients, IP Cameras, VNC and Terminal Shadow Display Clients can be delivered with **MultiSession**. This makes it possible to deliver a very diverse set of content to a single terminal, creating composite applications. The Display Clients can be visualized as tiles on a display so that multiple Display Clients can be monitored at the same time and/or spread out across multiple monitors – or a combination. This lab section is composed of the following tasks:

1. Create InstantFizz Remote Desktop Services Display Client
2. Create Excel Remote Desktop Services Display Client
3. Create SuperJuice VNC Display Client
4. Create Camera Display Client
5. Apply Display Clients to Terminal and Enable Tiling
6. FactoryTalk View SE Client Licensing Benefits
7. Remove Tiled Display Clients

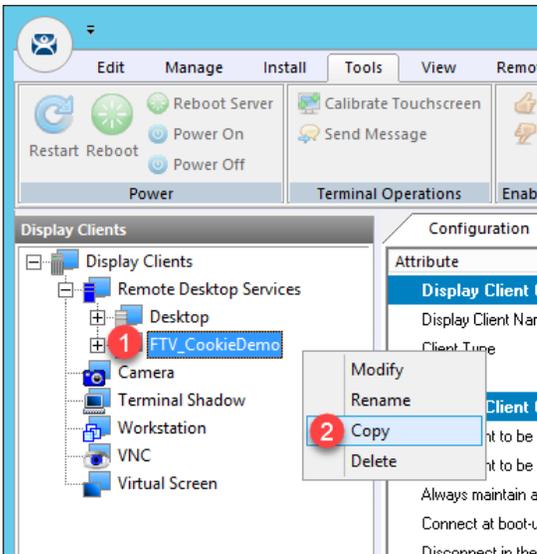
Create InstantFizz Remote Desktop Services Display Client

We are going to copy the **FTV_CookieDemo** Display Client to create another View SE Display Client, but this time to launch a different View SE application. We won't need Automatic Remote Desktop Failover, so we will disable this from the copied terminal profile.

1. From ThinManager, click the **Display Clients** icon  from the ThinManager tree selector.



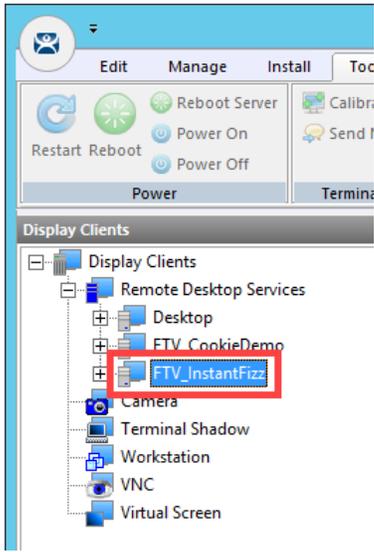
2. From the **Display Clients** tree, expand the **Remote Desktop Services** branch and right click the **FTV_CookieDemo** item and select **Copy**.



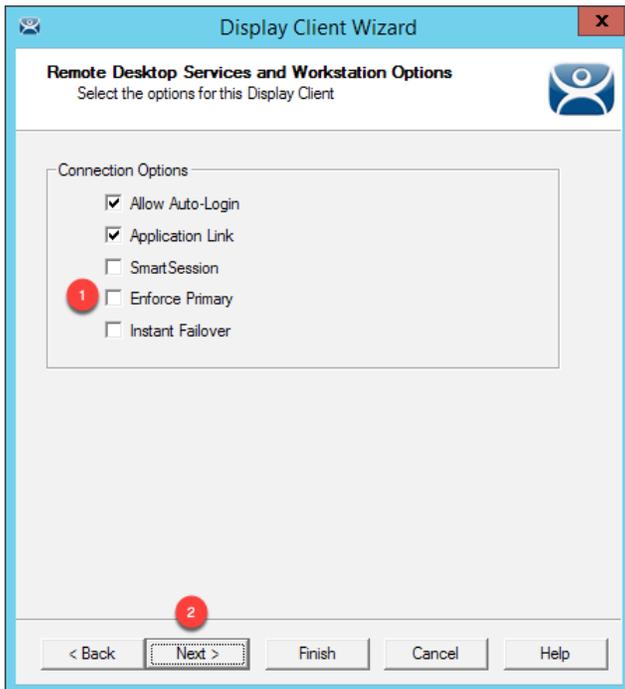
3. Type **FTV_InstantFizz** in the **Enter new Display Client Name** text box and click the **OK** button.



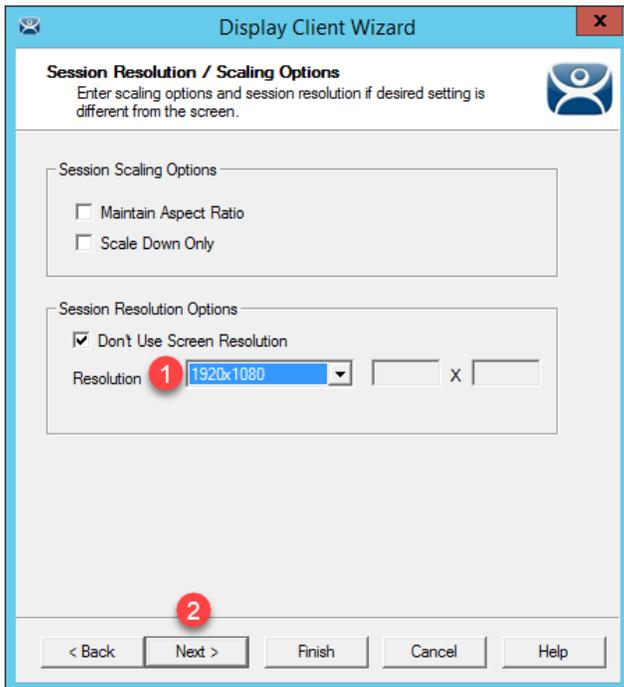
4. Double click the **FTV_InstantFizz** Display Client item.



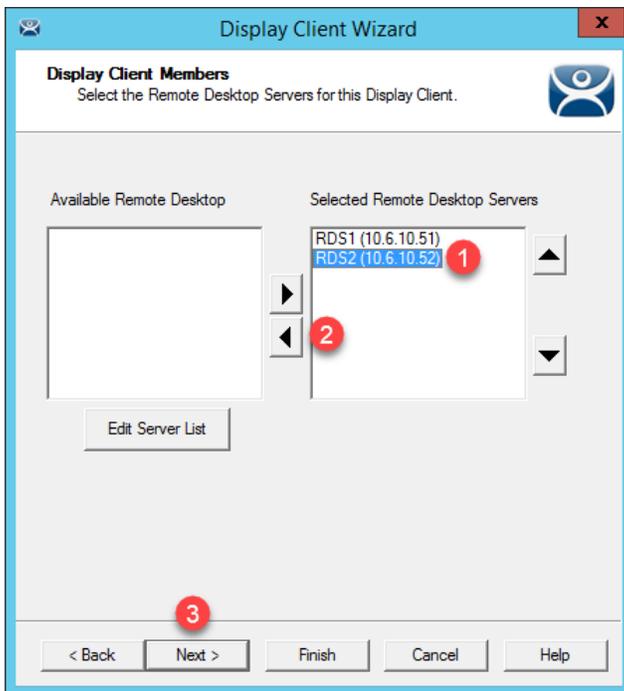
5. From the **Client Name** page of the wizard, click the **Next** button.
6. From the **Display Client Options** page of the wizard, click the **Next** button.
7. From the **Remote Desktop Services and Workstation Options** page of the wizard, uncheck the **Enforce Primary** checkbox and click the **Next** button.



- From the **Screen Resolution / Scaling Options** page of the wizard, change the **Resolution** to **1920x1080** and click the **Next** button.

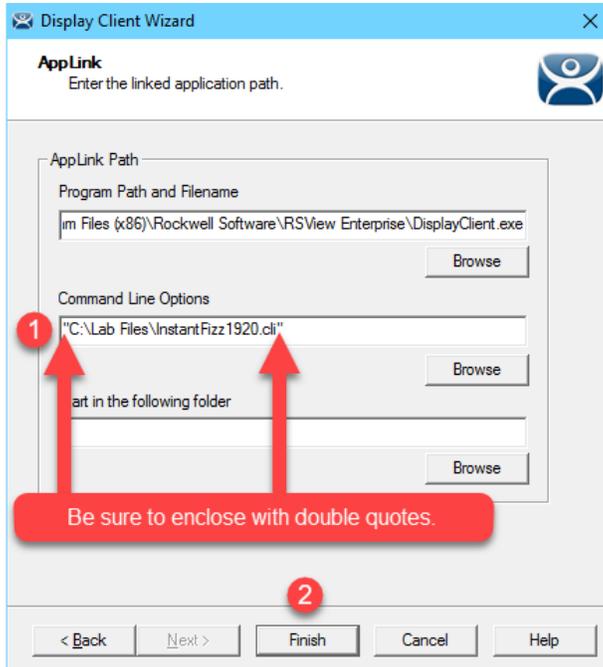


- From the **Display Client Members** page of the wizard, select **RDS2** from the **Selected** list and click the **Left** arrow button to remove it. Click the **Next** button.



- From the **AppLink** page of the wizard, replace **CookieDemo1280** in the **Command Line Options** path with *InstantFizz1920* like below (you can also copy and paste this path from the **LabPaths.txt** file by right clicking the **Notepad** icon pinned to the start bar and selecting **LabPaths.txt**):

"C:\Lab Files\InstantFizz1920.cli"



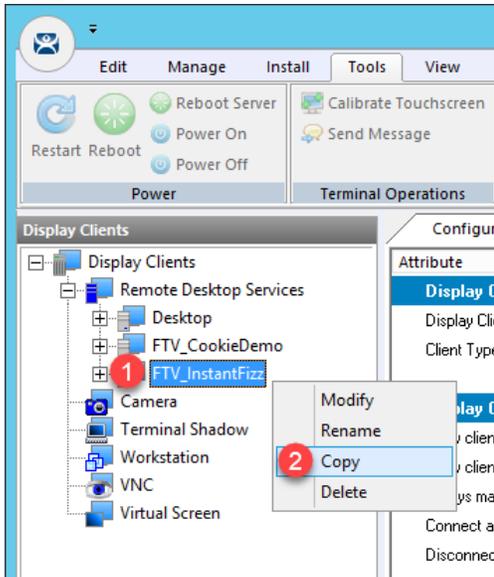
- Click the **Finish** button.

Notice that we did not have to publish another Remote Desktop Services RemoteApp for this Display Client since we selected the option for allowing any command line parameters when we published the FactoryTalk View SE RemoteApp in [Section 5](#).

Create Excel Remote Desktop Services Display Client

We are going to copy the **FTV_InstantFizz** Display Client to create another Remote Desktop Services Display Client.

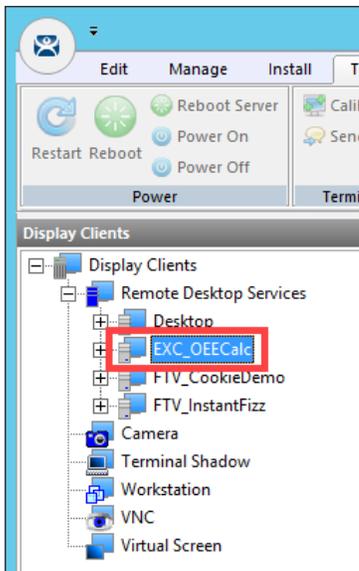
1. From the **Display Clients** tree, expand the **Remote Desktop Services** branch and right click the **FTV_InstantFizz** item and select **Copy**.



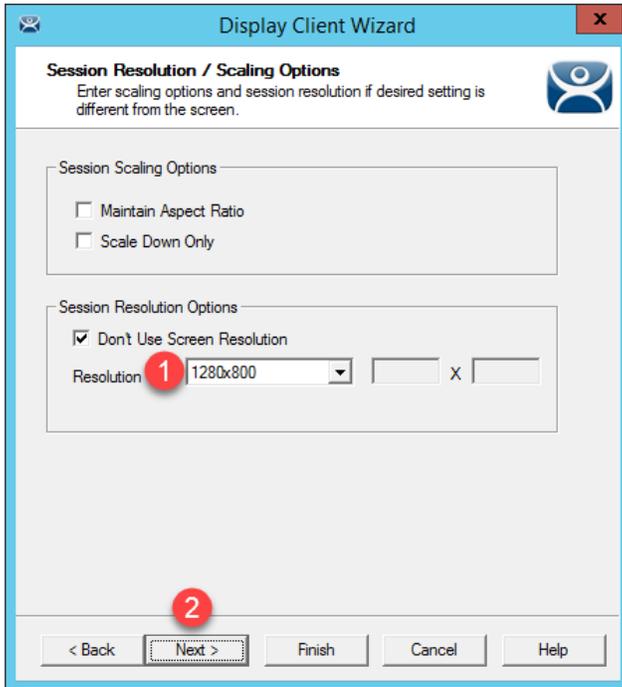
2. Type **EXC_OEECalc** in the **Enter new Display Client Name** text box and click the **OK** button.



3. Double click the **EXC_OEECalc** Display Client item.



4. From the **Client Name** page of the wizard, click the **Next** button.
5. From the **Display Client Options** page of the wizard, click the **Next** button.
6. From the **Remote Desktop Services and Workstation Options** page of the wizard, click the **Next** button.
7. From the **Screen Resolution / Scaling Options** page of the wizard, change the **Resolution** from 1920x1080 to **1280x800** and click the **Next** button.



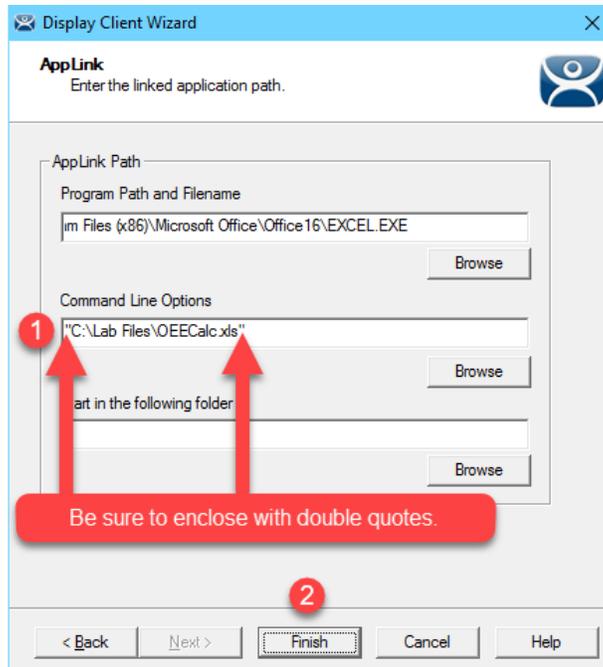
- From the **Display Client Members** page of the wizard, click the **Next** button.
- From the **AppLink** page of the wizard, replace the **Program Path and Filename** and the **Command Line Options** paths with the ones below (you can also copy and paste this path from the **LabPaths.txt** file by right clicking the **Notepad** icon pinned to the start bar and selecting **LabPaths.txt**):

Program Path and Filename:

C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

Command Line Options:

"C:\Lab Files\OEECalc.xls"



- Click the **Finish** button.

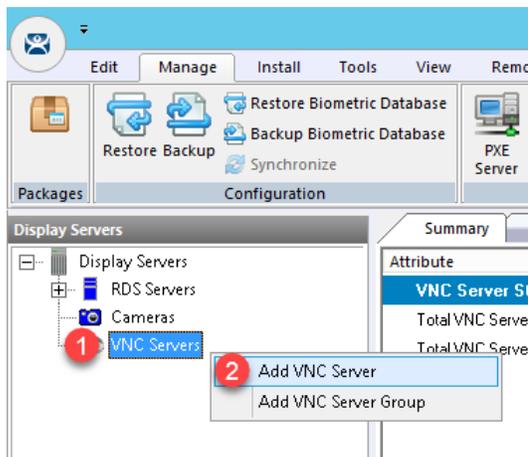
Create SuperJuice VNC Display Client

An instance of the FactoryTalk View ME Runtime is running on the HMI image. In addition, a VNC Server was installed and running. Together, they will simulate a PanelView Plus for the purposes of this lab. As a sidebar, only one instance of the ME Runtime can be hosted on a single machine, even if it is a Remote Desktop Server.

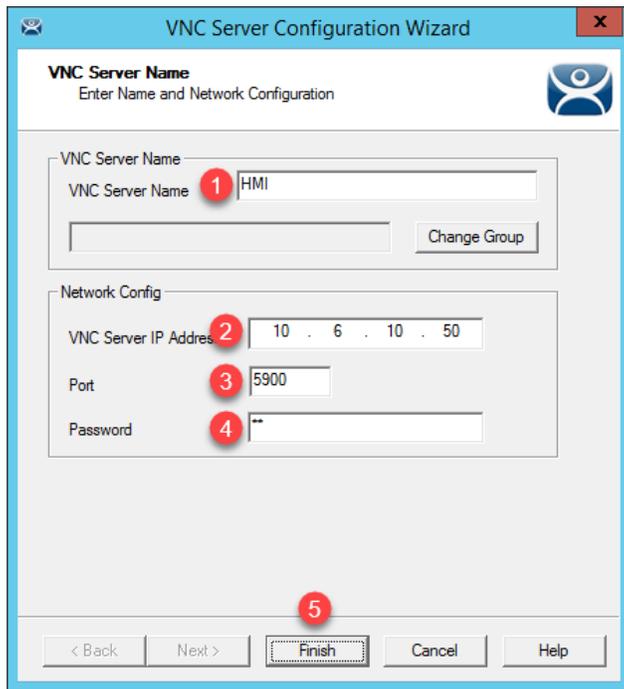
1. Click the **Display Servers** icon  in the ThinManager tree selector.



2. From the **Display Servers** tree, right click the **VNC Servers** branch and select **Add VNC Server**. This will launch the **VNC Server Configuration Wizard**.



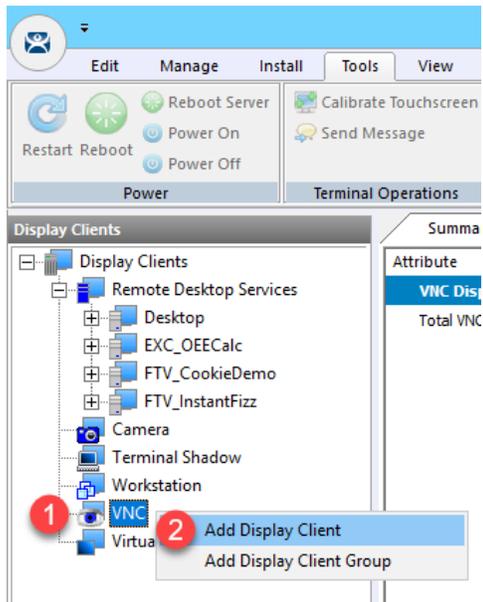
- From the **VNC Server Name** page of the wizard, enter *HMI* in the **VNC Server Name** text box. Enter *10.6.10.50* in the **VNC Server IP Address** text box. Keep **5900** as the **Port**, and enter *rw* in the **Password** field. Click the **Finish** button.



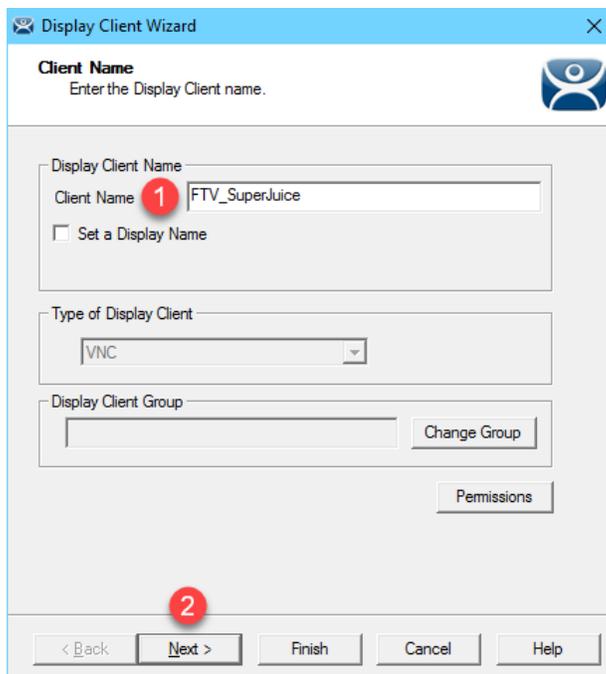
- Click the **Display Clients** icon from the ThinManager tree selector.



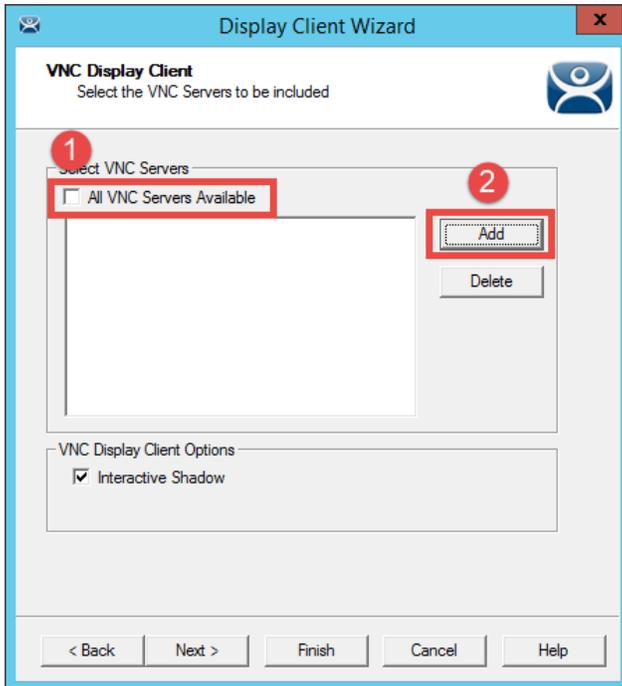
5. Expand the **Display Clients** tree, right click the **VNC** branch and select **Add Display Client**.



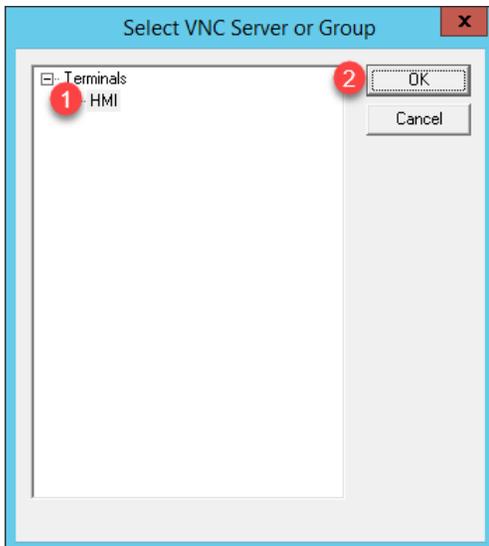
6. From the **Client Name** page of the wizard, enter *FTV_SuperJuice* as the **Client Name**. Click the **Next** button.



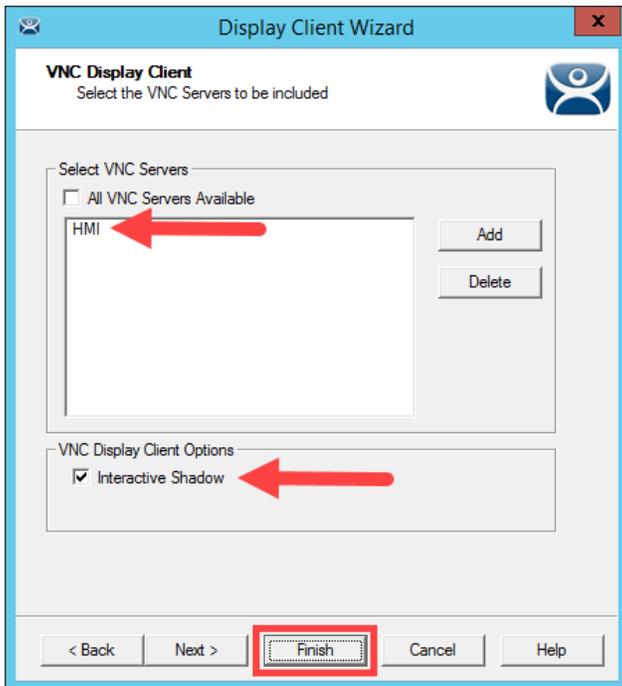
- From the **Display Client Options** page of the wizard, click the **Next** button.
- From the **VNC Display Client** page of the wizard, uncheck the **All VNC Servers Available** checkbox and then click **Add** button.



- Select **HMI** from the **Terminals** tree and click the **OK** button.



10. Back on the **VNC Display Client** page, keep the check for **Interactive Shadow** and click the **Finish** button.



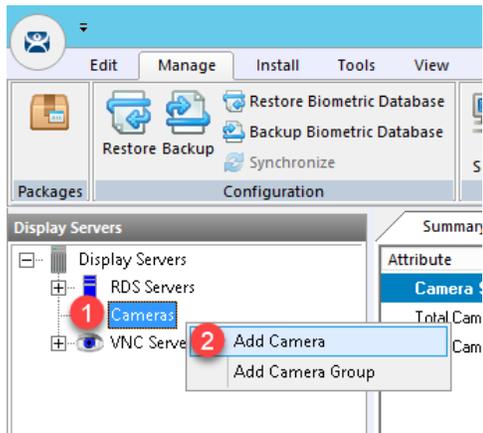
Create Camera Display Client

We will now configure a Display Client to access the IP Camera's video stream located at your lab station using Real Time Steaming Protocol (RTSP).

1. Click the **Display Servers** icon  in the ThinManager tree selector.



2. From the **Display Servers** tree, right click the **Cameras** branch and select **Add Camera**. This will launch the **Camera Configuration Wizard**.



3. From the **Camera Name** page of the wizard, enter/select the following and then click the **Next** button.

- **Camera Name** = *Axis*
- **IP Address** = *131.173.8.23*
- **Port** = *80*
- **Streaming Protocol** = Legacy Motion JPEG
- **Make** = Generic
- **Model** = Default

Camera Configuration Wizard

Camera Name
Enter the camera name and network location

Camera Name
Camera Name **1** Axis
Change Group

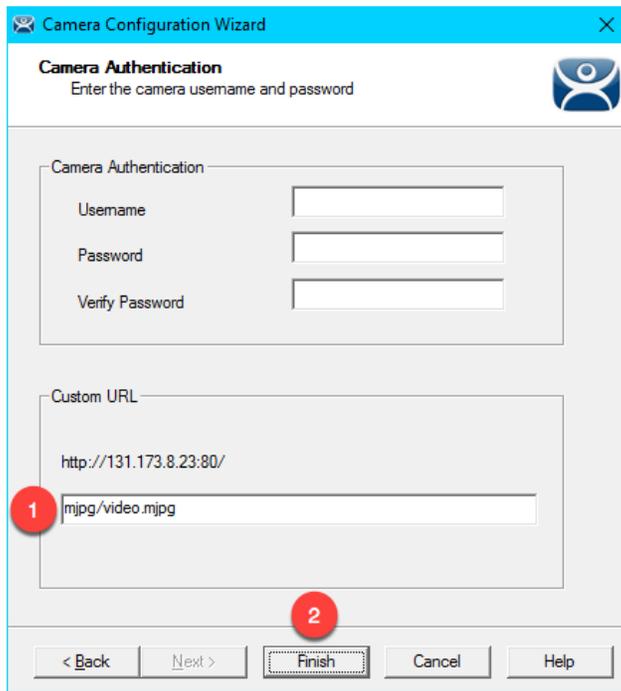
Camera Network Setup
Type IP Camera
IP Address **2** 131 . 173 . 8 . 23
Port **3** 80

Camera Connection
Streaming Protocol **4** Legacy Motion JPEG
Make **5** Generic
Model **6** Default

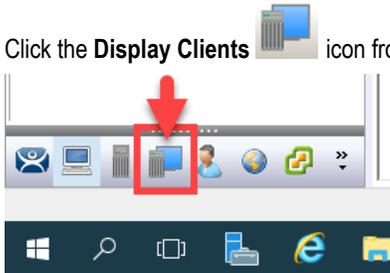
7
< Back Next > Finish Cancel Help

This is a public facing IP camera located at Osnabrück University in Lower Saxony, Germany. The camera is focused on a Foucault pendulum, a device named after the French physicist Léon Foucault. It was created to demonstrate the Earth's rotation. While the camera performs reasonably well over the Internet, it will be a bit sluggish in our virtual thin client, but still effectively shows the concept.

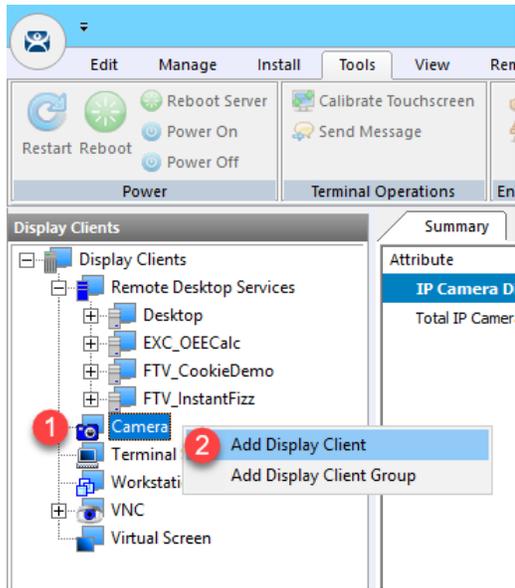
- From the **Camera Authentication** page of the wizard, leave the **Camera Authentication** frame blank and enter *mjpg/video.mjpg* in the **Custom URL** field (or copy and paste from the **LabPaths** shortcut on your Desktop) and click the **Finish** button.



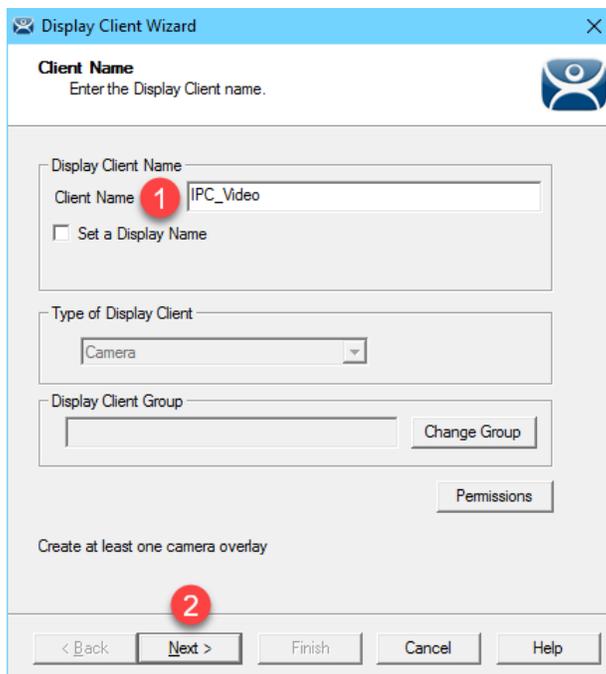
- Click the **Display Clients** icon from the ThinManager tree selector.



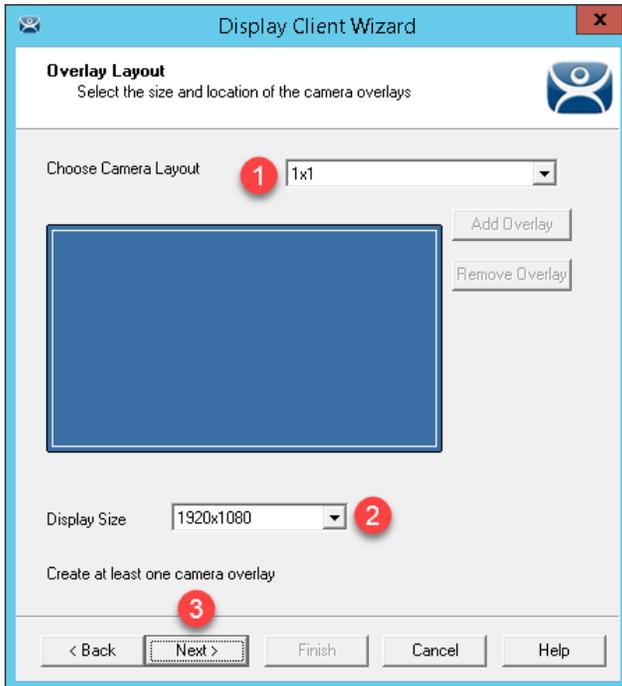
- Expand the **Display Clients** tree, right click the **Camera** branch and select **Add Display Client**.



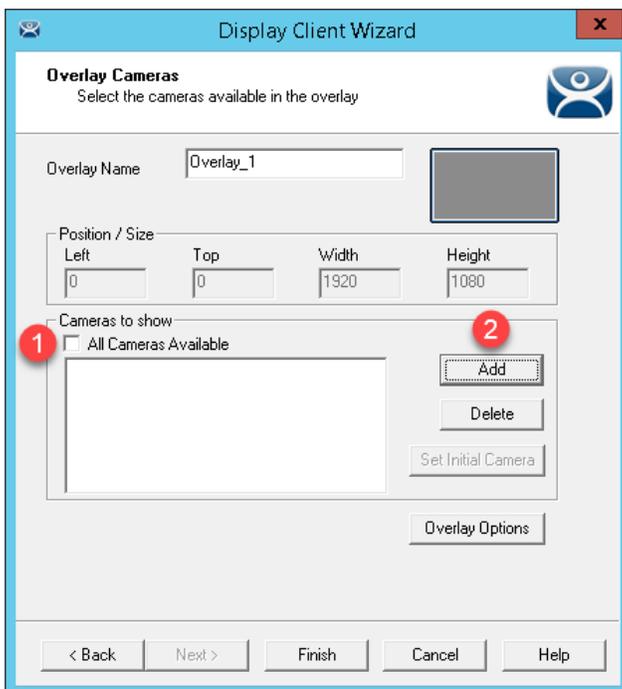
- From the **Client Name** page of the wizard, enter *IPC_Video* as the **Client Name**. Click the **Next** button.



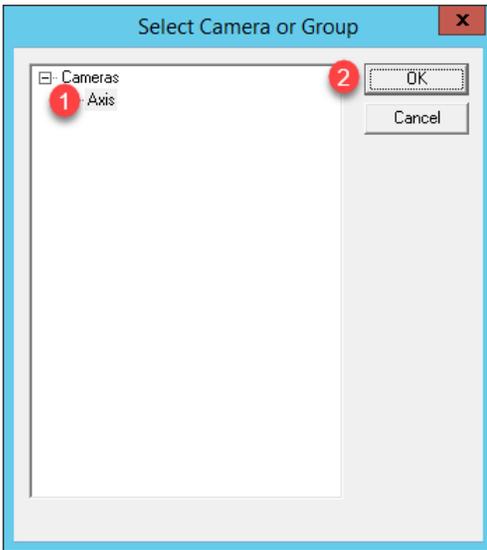
- From the **Display Client Options** page of the wizard, click the **Next** button.
- From the **Overlay Layout** page of the wizard, select **1x1** from the **Choose Camera Layout** drop down list and select **1920x1080** from the **Display Size** drop down list. Click the **Next** button.



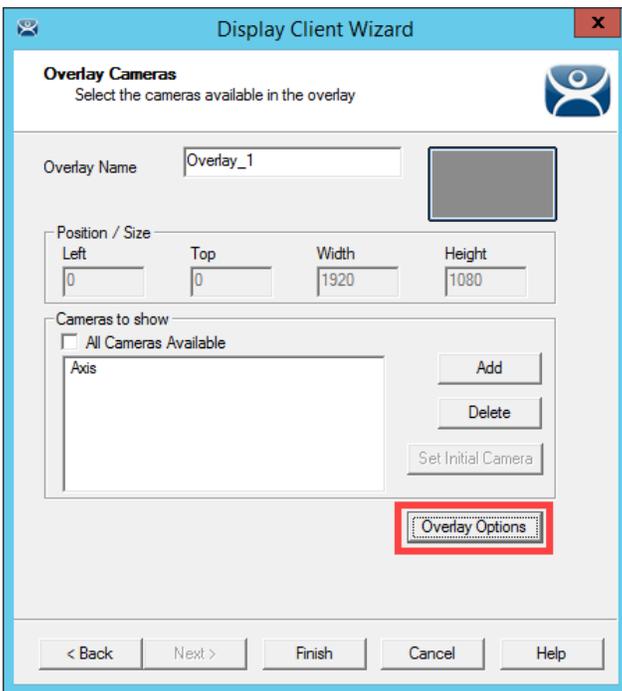
- From the **Overlay Cameras** page of the wizard, un-check the **All Cameras Available** checkbox and click the **Add** button.



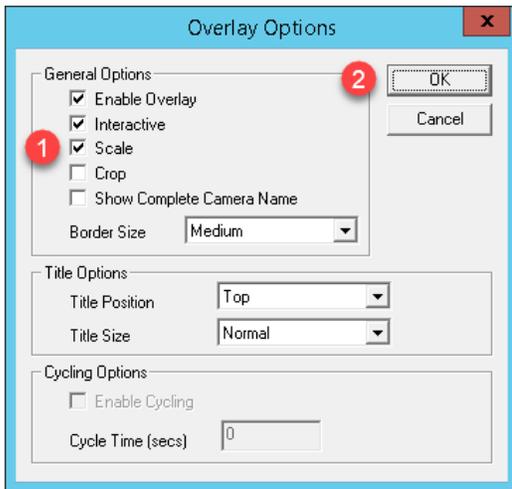
11. From the **Select Camera or Group** window, select the **Axis** item and click the **OK** button.



12. Back at the **Overlay Cameras** page of the wizard, click the **Overlay Options** button.



13. From the **Overlay Options** window, check the **Scale** checkbox and click the **OK** button followed by the **Finish** button.



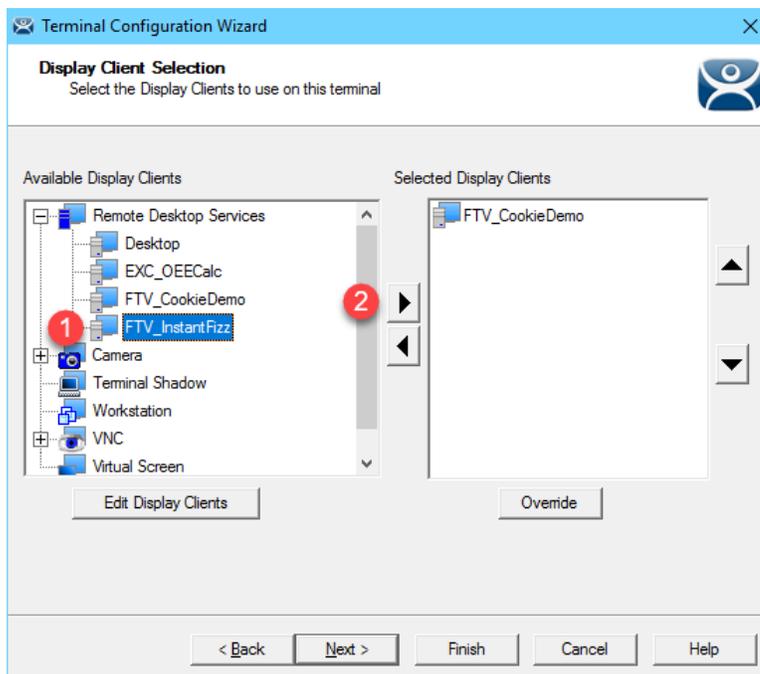
ThinManager also supports USB Cameras as sources of content. A camera's video stream can be delivered as its own Display Client, or as an overlay to an existing Display Client. ThinManager supports real time streaming protocols (RTSP) like H.264. RTSP can be decoded by the terminal's CPU or for certain Intel graphics chipsets, by the on-board graphics, reducing the load on the terminal's CPU. The **VersaView 5200** supports RTSP decoding by the on-board graphics chipset.

Apply Display Clients to Terminal and Enable Tiling

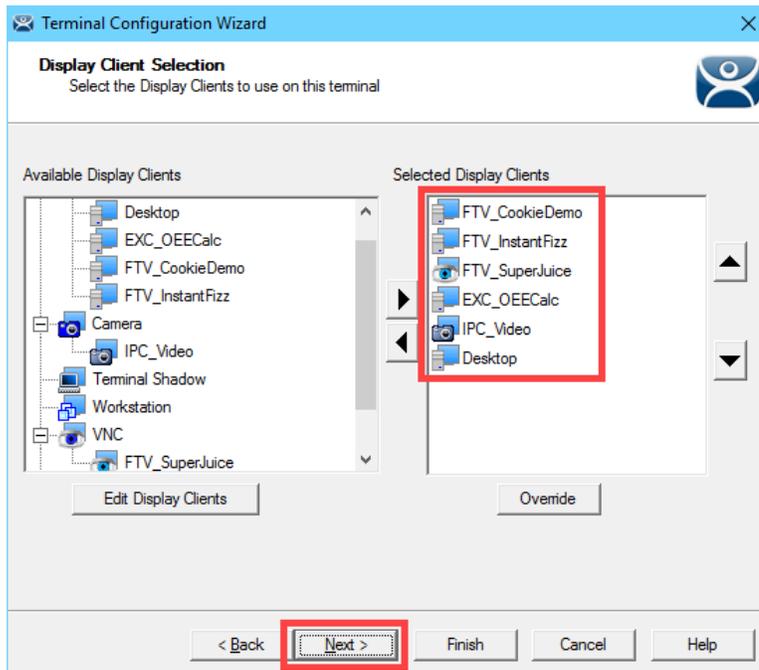
1. Click the **Terminals** icon  from the ThinManager tree selector.



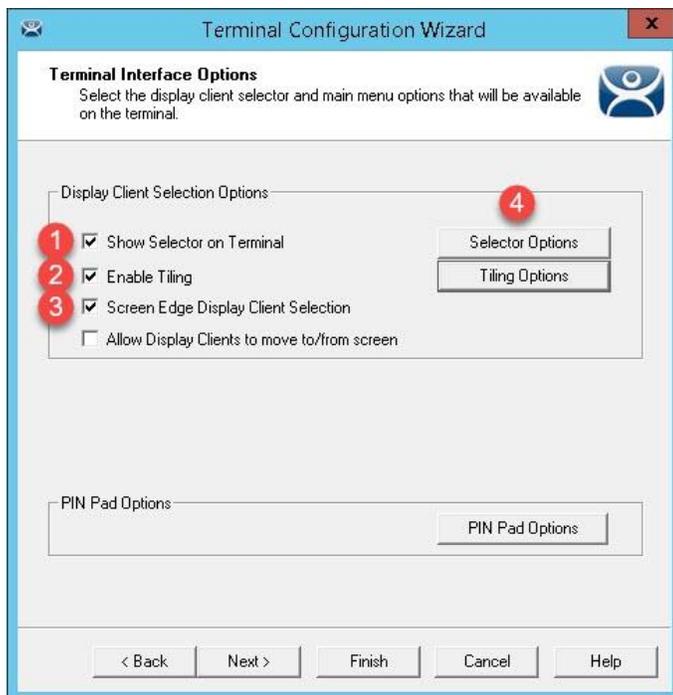
2. From the **Terminals** tree, double click the **VersaView5200** terminal to launch the **Terminal Configuration Wizard**.
3. Click the **Next** button on the **Terminal Name** page of the wizard.
4. Click the **Next** button on the **Terminal Hardware** page of the wizard.
5. Click the **Next** button on the **Terminal Options** page of the wizard.
6. Click the **Next** button on the **Terminal Mode Selection** page of the wizard.
7. Select **FTV_InstantFizz** from the **Available Display Clients** list and click the **Right Arrow** button to move it to the **Selected Display Clients** list.



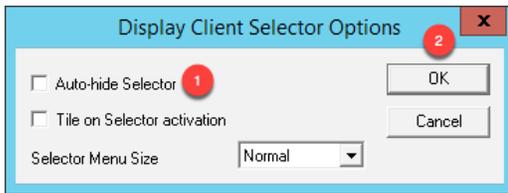
8. Repeat the previous step for the **FTV_SuperJuice**, **EXC_OEECalc**, **IPC_Video** and **Desktop Display Clients**. Click the **Next** button.



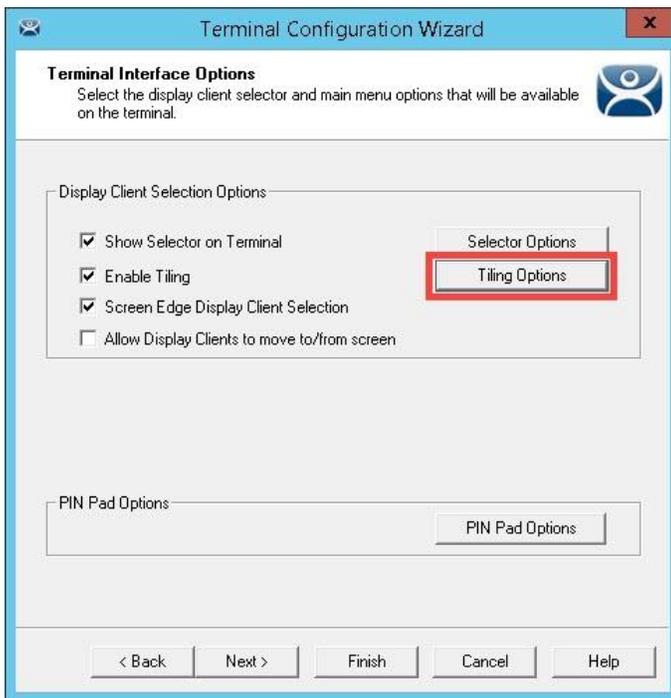
9. On the **Terminal Interface Options** page of the wizard, make sure **Show Selector on Terminal**, **Enable Tiling** and **Screen Edge Display Client Selection** are checked. Click the **Selector Options** button.



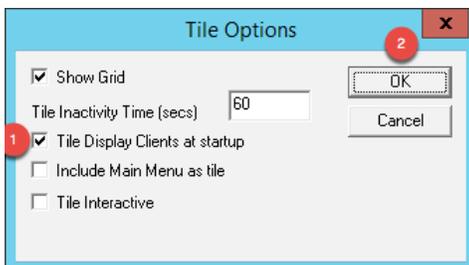
10. Click on the **Selector Options** button. Uncheck Auto-hide Selector and click the **OK** button.



11. Back on the **Terminal Interface Options** page of the wizard, click the **Tiling Options** button.

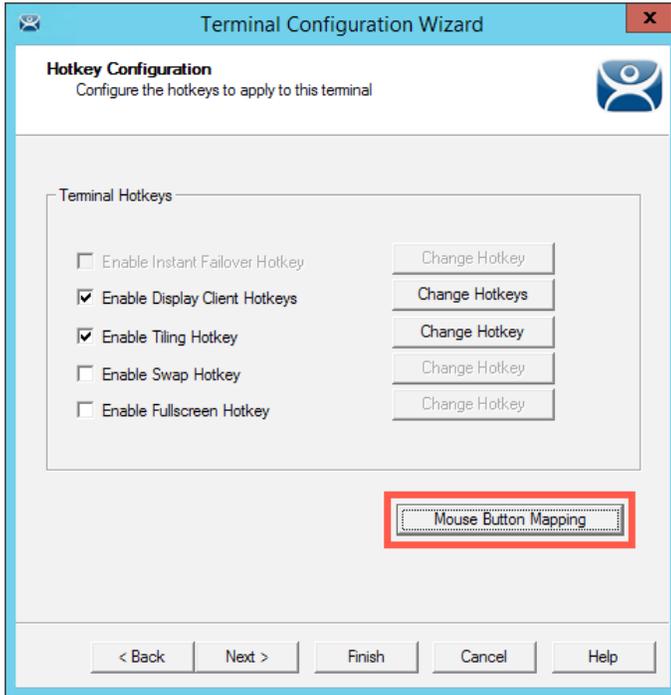


12. Make sure **Show Grid** is checked, and also check **Tile Display Clients at startup**. Click the **OK** button.

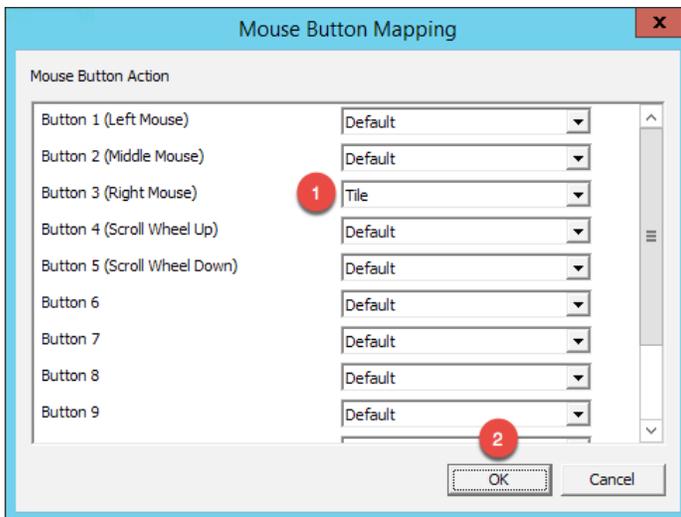


13. Click the **Next** button when you return to the **Terminal Interface Options** page of the wizard.

14. From the **Hotkey Configuration** page of the wizard, make sure **Enable Display Client Hotkeys** and **Enable Tiling Hotkey** are both checked. Click the **Mouse Button Mapping** button.

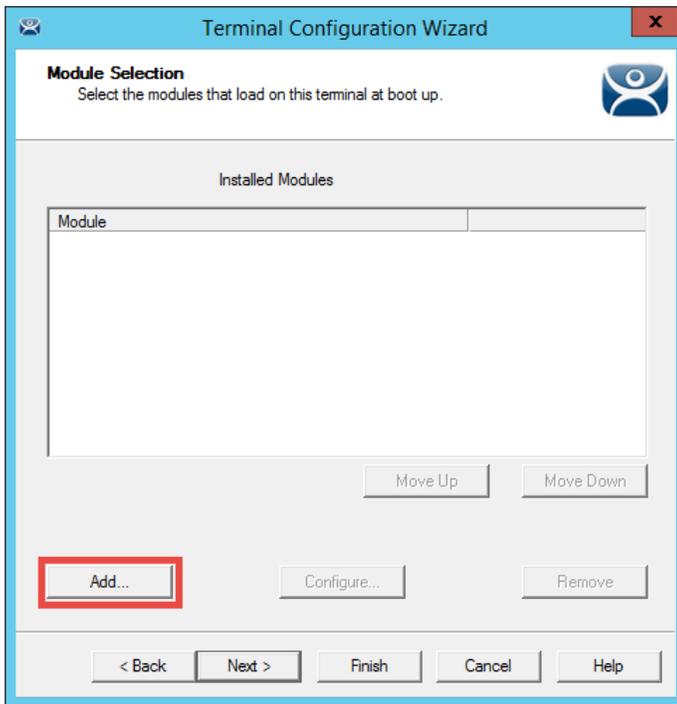


15. From the **Mouse Button Mapping** dialog box, select **Tile** from the **Button 3 (Right Mouse)** drop down list. Click the **OK** button followed by the **Next** button.

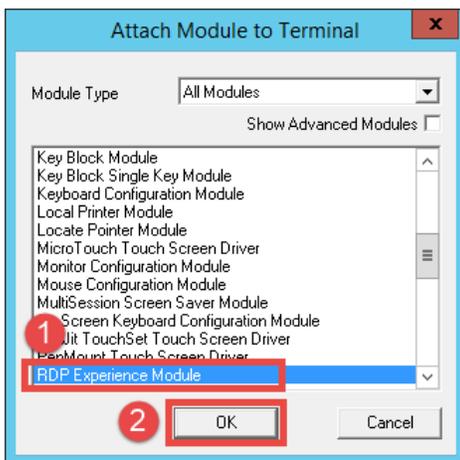


ThinManager 9 introduced more mouse button mapping options, including all mouse button types to a number of new mouse button actions like Swap and Full Screen, both of which are applicable to Virtual Screens, which will be introduced in the next section.

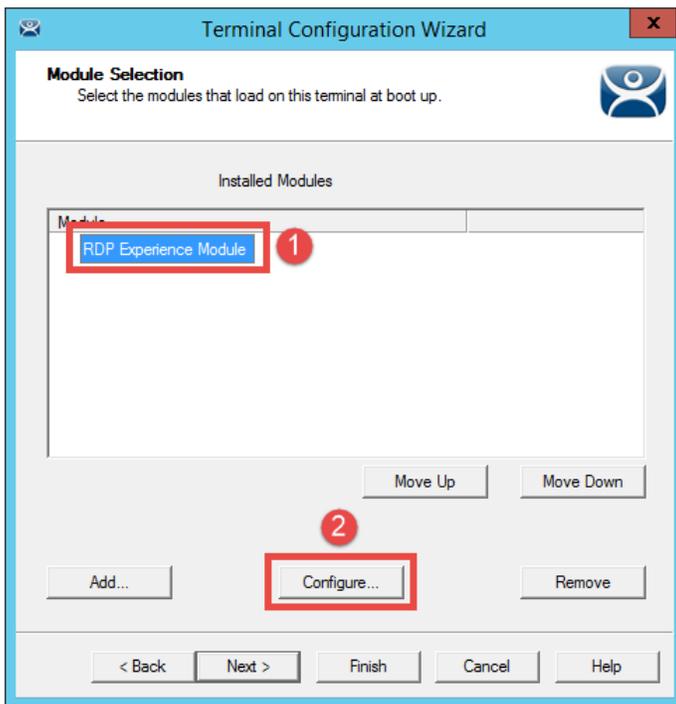
16. From the **Log In Information** page of the wizard, click the **Next** button.
17. From the **Video Resolution** page of the wizard, click the **Next** button.
18. From the **Module Selection** page of the wizard, click the **Add...** button.



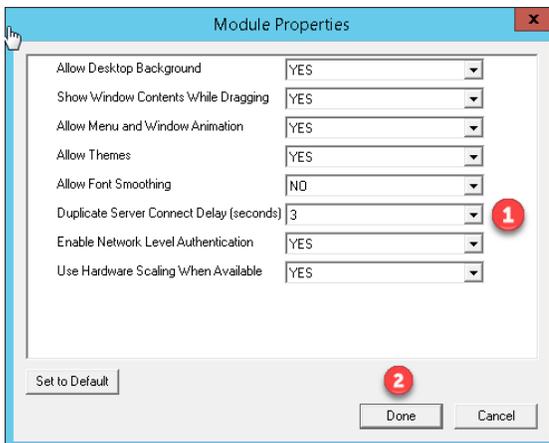
19. From the **Attach Module to Terminal** dialog box, scroll down and select the **RDP Experience Module** and click the **OK** button.



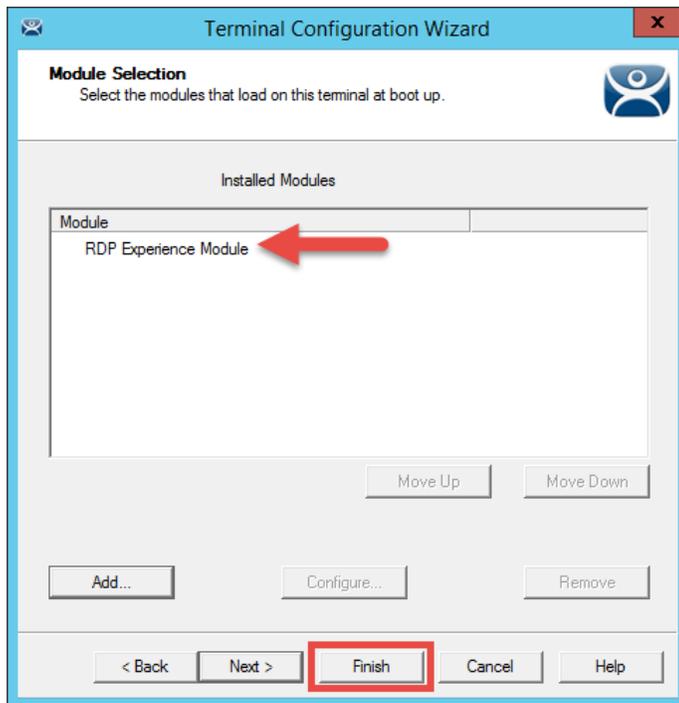
20. Back on the **Module Selection** page of the wizard, select the **RDP Experience Module** and click the **Configure** button.



21. From the **Module Properties** dialog box, select **3** from the **Duplicate Server Connect Delay (seconds)**. Click the **Done** button.



22. Back on the **Module Selection** page of the wizard, click the **Finish** button.



The RDP Experience Module enables configuration of how the RDP session is rendered at the terminal, including if the Desktop Background or Themes are delivered, if Network Level Authentication (NLA) is enabled, etc. It is typically used with MultiSession because it also staggers the starting of the sessions on the Remote Desktop Server. Without staggering the starting of the sessions, the Remote Desktop Server can respond with a warning message that it is busy.

23. Right click the **VersaView5200** terminal from the **Terminals** tree and select **Restart Terminal** to apply the changes. Click **Yes** to the confirmation dialog.
24. Shadowing the **VersaView5200** should show the 6 **Display Clients** in a 2x3 grid referred to as **Tile Mode**. **If you see an Activation window in Microsoft Excel, just ignore it.**



In addition to using **Tile Mode** to switch between the **Display Clients**, the **Display Client Selector** at the top of the terminal can be used. To use the **Display Client Selector**, click and hold the selector to expand the menu. While still holding the mouse button, point to the desired **Display Client** and release the mouse button to select it. You can also return to **Tile Mode** from the **Display Client Selector**.

You may also notice when dragging your mouse back to the lab manual that the **Display Client** will change. This is due to the **Screen Edge Selection** feature that we enabled. Dragging the mouse to either edge of the screen will select the next **Display Client** automatically.

25. By default, the hotkeys **CTRL-PAGE UP** and **CTRL-PAGE DOWN** will also cycle through the **Display Clients**. We also enabled the **Screen Edge Selector** which allows you to move the pointer to the edge of the screen and shift the next **Display Client** into view. Experiment with each of these. Similarly, the hotkey **CTRL-t** will return to **Tile Mode**.

You can deploy up to 25 (a 5x5 Grid) **Display Clients** using **Tiling Mode** to a single monitor. If you are not using **Tiling Mode**, there is no limit to the number of **Display Clients** that can be applied to a single monitor. All of the processing required for this content is not occurring at the terminal, but at the server.

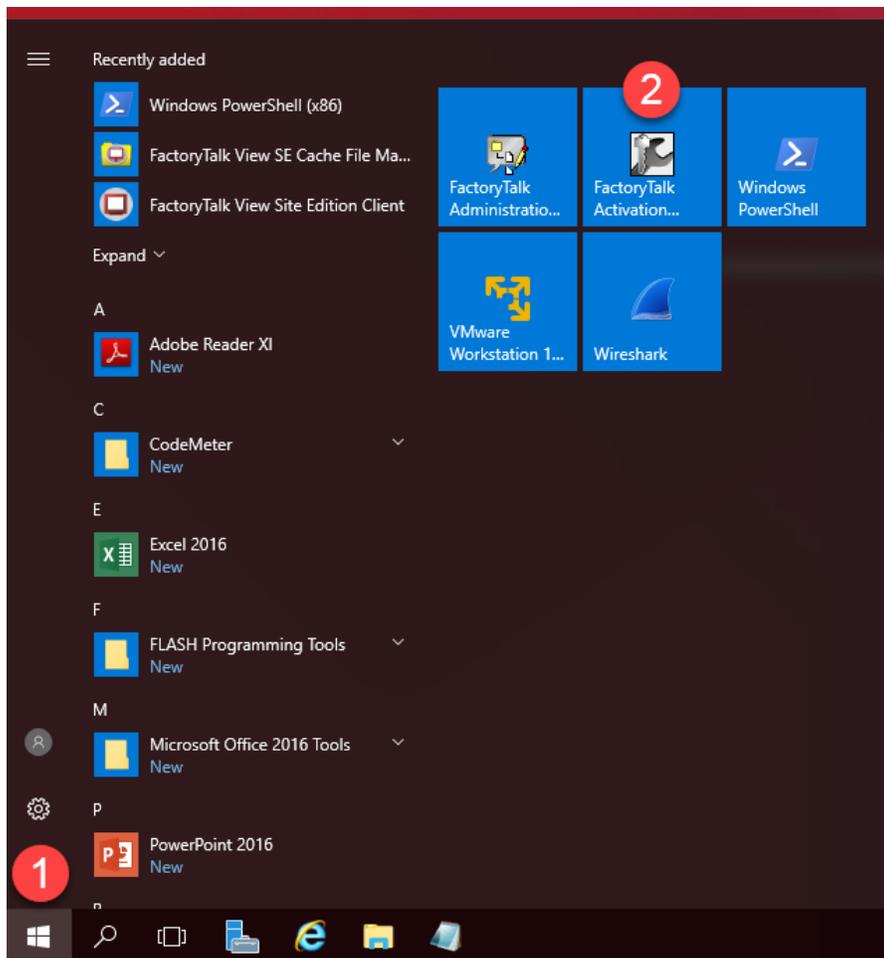
FactoryTalk View SE Client Licensing Benefits

The FactoryTalk View Site Edition Client consumes one SE Client license for each unique session running on a Remote Desktop Server that launches **DisplayClient.exe** in a distributed architecture. With the release of ThinManager 11.0 and FactoryTalk View SE 11.0, a single FactoryTalk View SE Client license is all that is required per ThinManager-managed Terminal. This enables you to deliver an unlimited number of sessions (either for ThinManager MultiSession and/or Failover) and consume only 1 SE Client license. The required versions of software for this to work are FactoryTalk View SE Client 11.00.00 or higher and ThinManager 11.0 or higher. This functionally also requires ThinManager to be at Firmware Package 8.1.11 or higher.

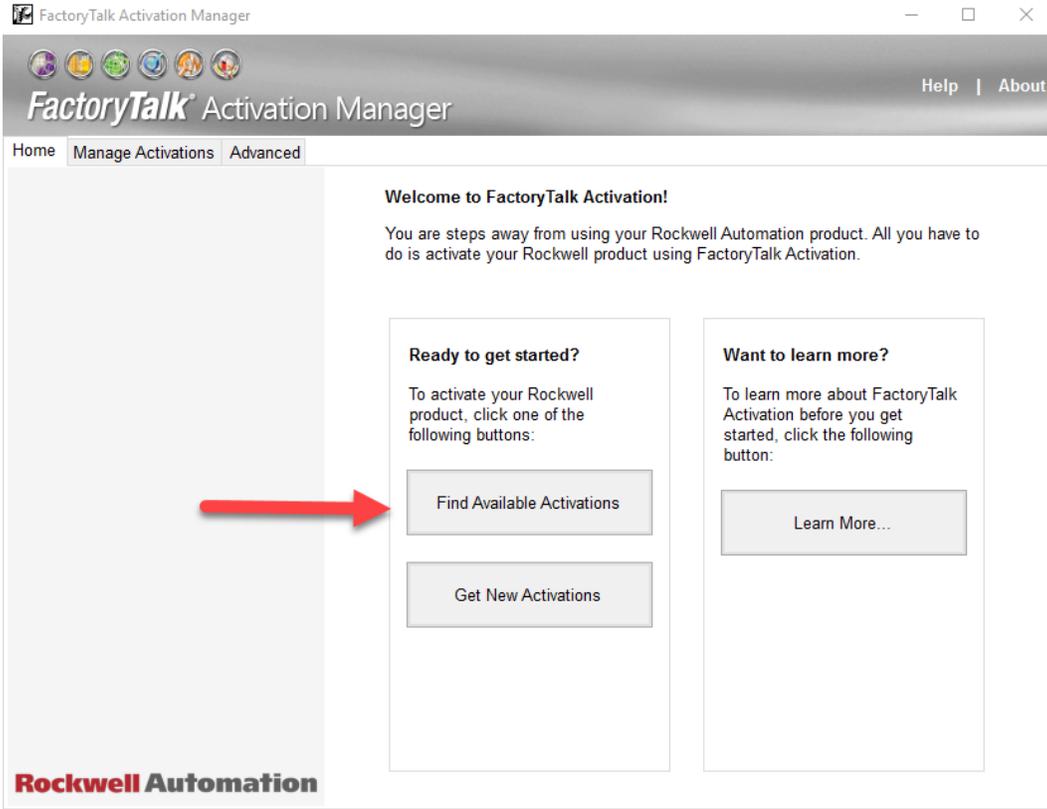
The **VersaView5200** terminal is currently hosting (6) different pieces of content, utilizing the Tiling and MultiSession features. Two of the sessions are unique FactoryTalk View SE Client sessions – FTV_CookieDemo and FTV_InstantFizz.

FTV_CookieDemo is configured for Failover, so at most, we could launch up to 3 FactoryTalk View SE client sessions for this one terminal. We will open the FactoryTalk Activation Manager to review how the terminal only requires (1) FT View SE Client license for the (2) FT View SE Client sessions.

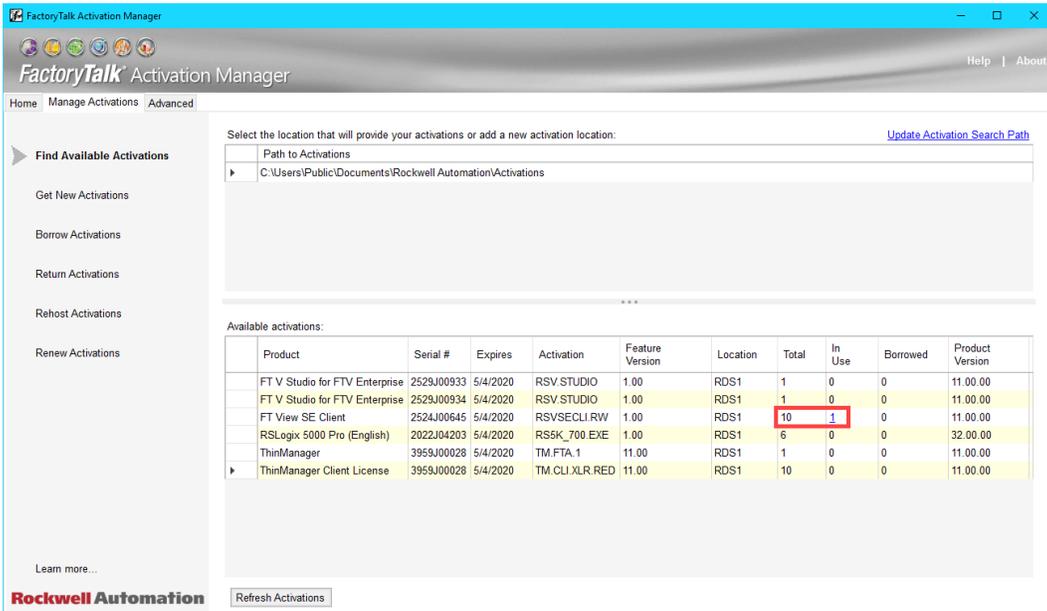
1. From the **Start Menu** click the **FactoryTalk Activation Manager** icon.



- Once it launches, click the **Find Available Activations** button.



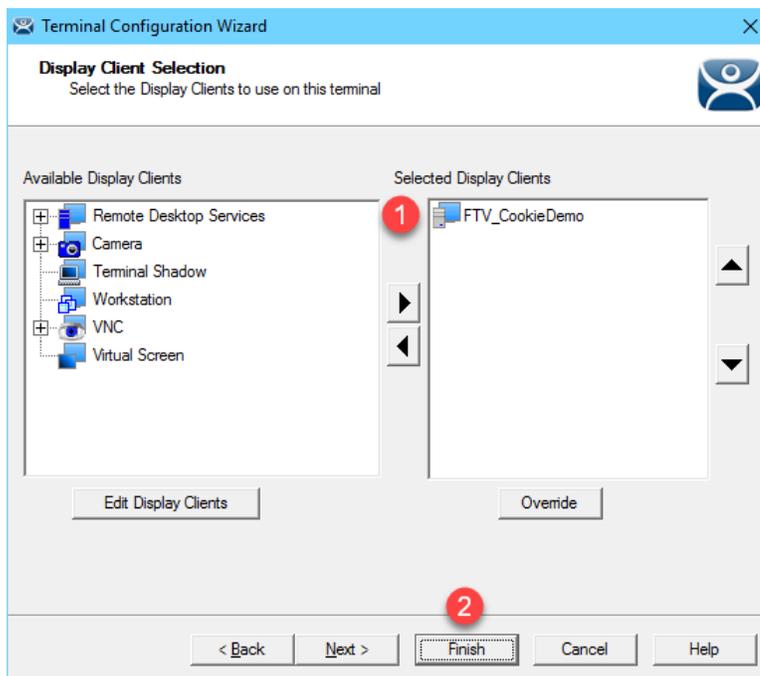
- Here you will see all the FactoryTalk Activations for the local server. Find the **FactoryTalk View SE Client** item in the list and notice that only 1 of the 10 SE Client licenses is currently in use despite running 2 separate sessions of the **FactoryTalk View SE Client** on the virtual thin client.



- Close out of the **FactoryTalk Activation Manager**.

Remove Tiled Display Clients

1. Click the **Terminals** icon  from the ThinManager tree selector.
2. From the **Terminals** tree, double click the **VersaView5200** terminal to launch the **Terminal Configuration Wizard**.
3. Click the **Next** button on the **Terminal Name** page of the wizard.
4. Click the **Next** button on the **Terminal Hardware** page of the wizard.
5. Click the **Next** button on the **Terminal Options** page of the wizard.
6. Click the **Next** button on the **Terminal Mode Selection** page of the wizard.
7. Remove the **FTV_InstantFizz**, **FTV_SuperJuice**, **EXC_OEECalc**, **IPC_Video** and **Desktop Display Clients** from the **Selected Display Clients** list. The **FTV_CookieDemo** should be the only **Selected Display Client**. Click the **Finish** button.



8. Right click the **VersaView5200** terminal from the **Terminals** tree and select **Restart Terminal** to apply the changes. Click **Yes** to the confirmation dialog.

This completes the section **Deploying Additional Content Using MultiSession and Tiling** of the lab. Continue on to explore MultiMonitor and its evolution, Virtual Screening.

Section 5: MultiMonitor, Virtual Screens and Session Scaling

Overview

ThinManager v11 supports up to 7 physical displays connected to a single ThinManager-managed thin client. In addition, ThinManager v9 introduced the concept of a **Virtual Screen Display Client**. The **Virtual Screen Display Client** is similar to the **Tiling** concept but enables you to determine the layout of the content in completely configurable areas, to which you can assign **Display Clients**. You can also overlay **Virtual Screens** to create a picture-in-picture effect with the ability to swap content in/out. Prior to ThinManager 9, the concept of overlays was supported, but only for IP cameras. Now, any type of **Display Client** can be applied to a **Virtual Screen**, and it can be automatically scaled to the size of the **Virtual Screen**. This section will introduce you to **MultiMonitor** and **Virtual Screens** and will be composed of the following tasks:

1. Split Content across Multiple Monitors
2. Create Virtual Screen Display Client
3. Apply Virtual Screen to Terminal
4. Add Virtual Screen Swapping

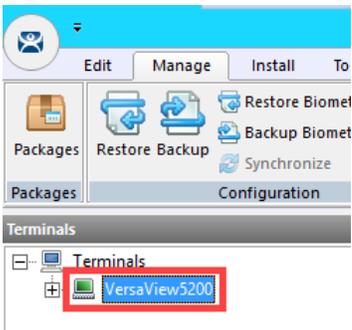
Split Content across Multiple Monitors

Instead of applying multiple **Display Clients** to a single monitor, we will split the content across 2 monitors using **ThinManager's MultiMonitor**.

1. If not already there, return to **ThinManager** on **RDS1**.
2. Click the **Terminals** tree selector icon.

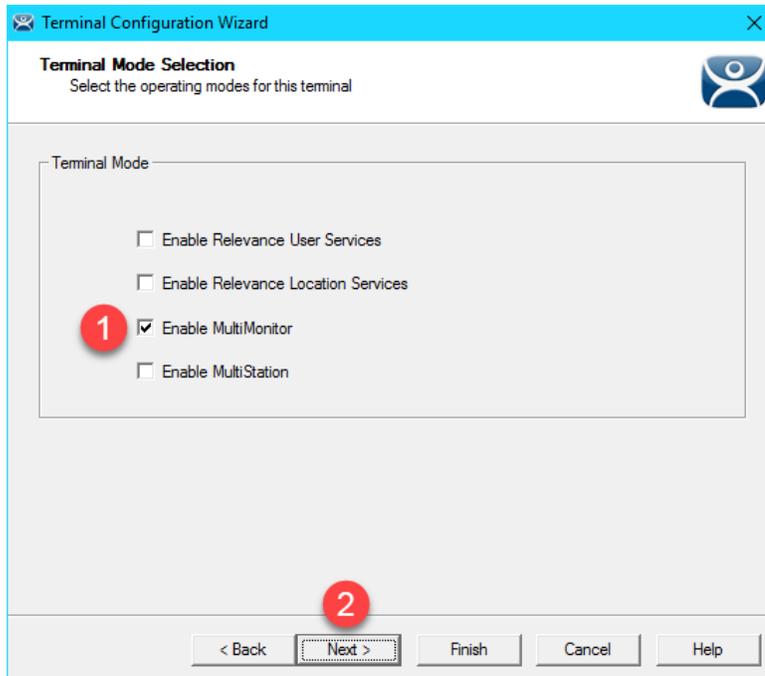


3. From the **Terminals** tree, double click the **VersaView5200** terminal to launch the **Terminal Configuration Wizard**.

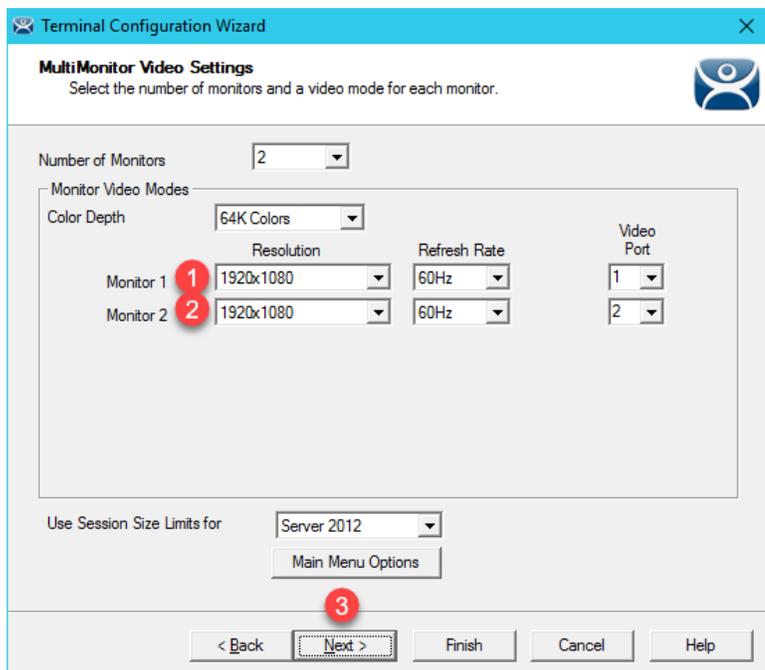


4. Click the **Next** button on the **Terminal Name** page of the wizard.
5. Click the **Next** button on the **Terminal Hardware** page of the wizard.
6. Click the **Next** button on the **Terminal Options** page of the wizard.

7. From the **Terminal Mode Selection** page of the wizard, check **Enable MultiMonitor**. Click the **Next** button.



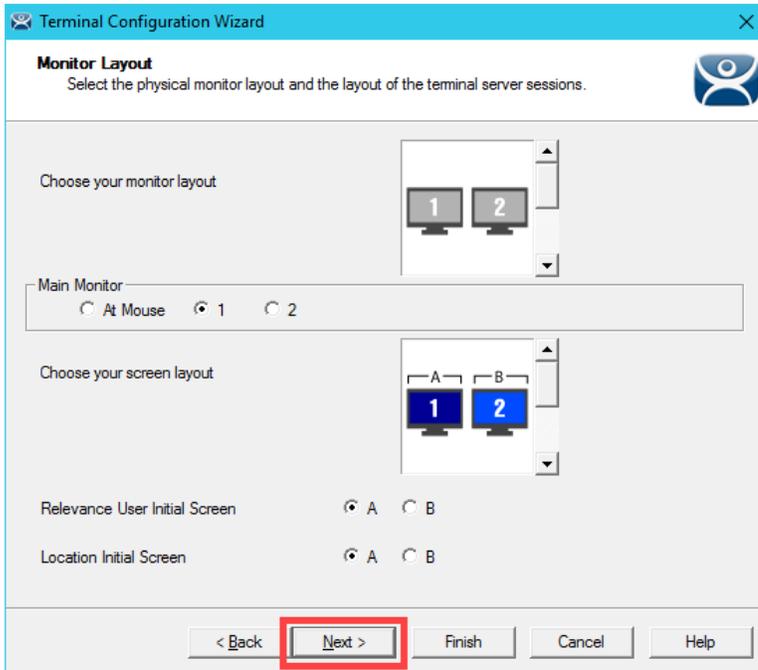
8. From the **MultiMonitor Video Settings** page of the wizard, make sure the following is selected: **2 Monitors** radio button, **64K Colors Color Depth**, **1920x1080 Resolution** for each monitor, **60Hz Refresh Rate** for each monitor, **Video Port 1** for **Monitor 1**, and **Video Port 2** for **Monitor 2**. Click the **Next** button.



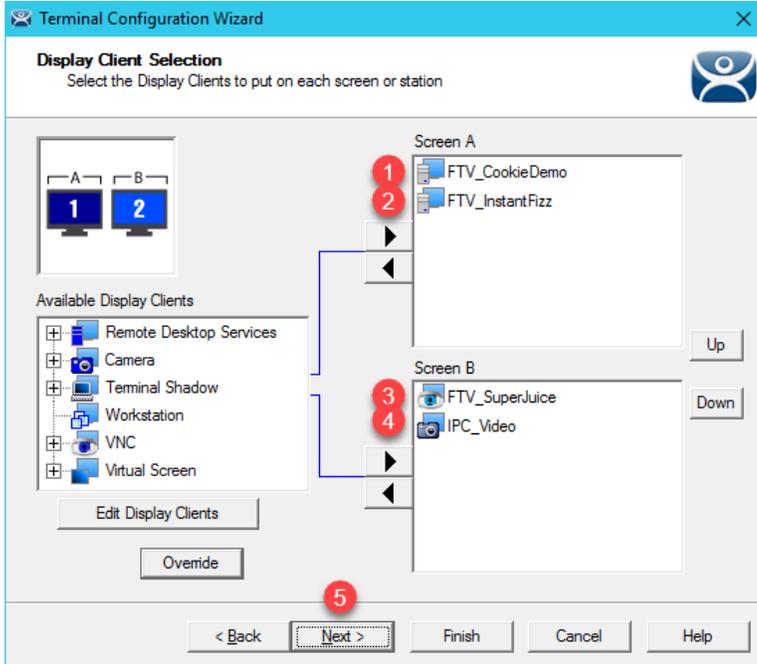
The **Use Session Size Limits** for drop down list allows you to specify either **Server 2012** or **Server 2008 R2** session size limits. Prior to Windows Server 2012, the maximum screen resolution for an RDP session was 4096 x 2048. Windows Server 2012 has increased this maximum to 8192 x 8192.

- From the **Monitor Layout** wizard, accept the defaults. This is where you tell ThinManager how your monitors are physically oriented via the **Monitor Layout** section, as well as how to treat each individual monitor via the **Screen Layout** section. Click the **Next** button.

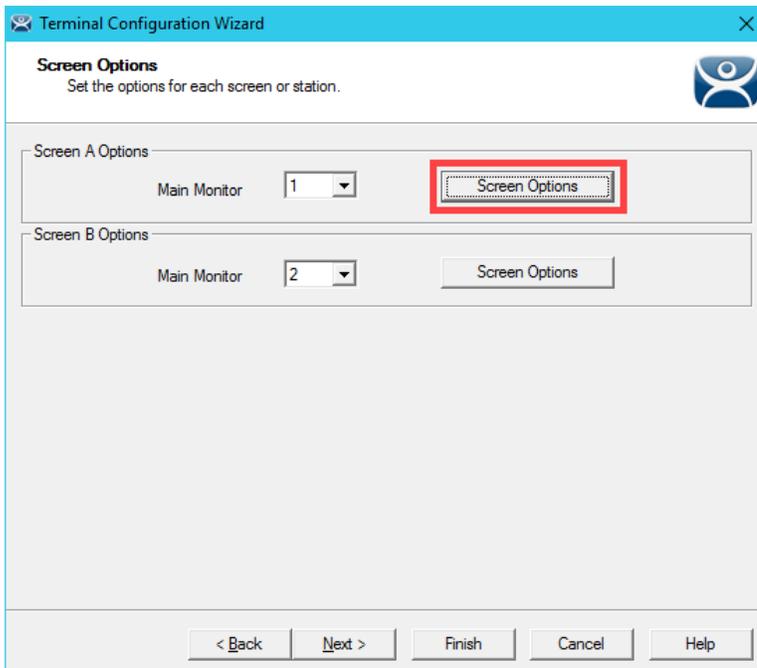
Screens are treated individually by default, which is referred to as **Screening**. Or the screens can be combined logically, which is referred to as **Spanning**.



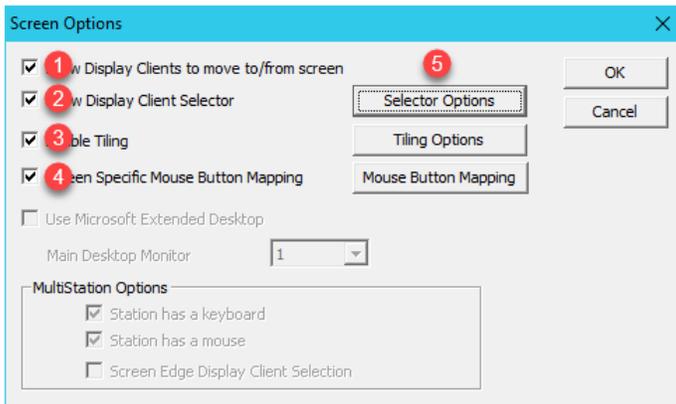
10. Select **FTV_CookieDemo** from the **Available Display Clients** list and click the **Right Arrow** button for **Screen A** to move it to the **Selected Display Clients** list. Repeat this step to move the **FTV_InstantFizz** Display Client to **Screen A** as well. Select **FTV_SuperJuice** from the **Available Display Clients** list and click the **Right Arrow** button for **Screen B** to move it to the **Selected Display Clients** list. Repeat this step to move the **IPC_Video** Display Client to **Screen B** as well. Click the **Next** button.



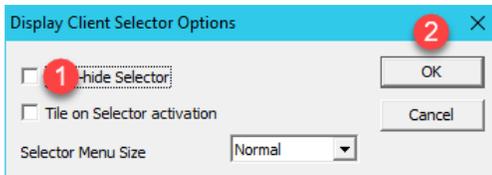
11. On the **Screen Options** page of the wizard, click the **Screen Options** button for **Screen A**.



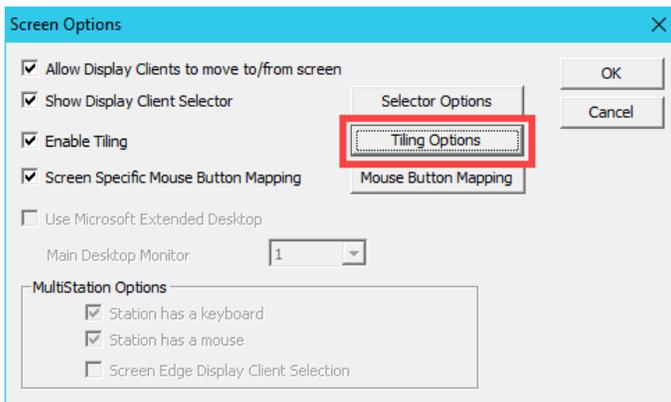
12. Make sure **Show Display Client Selector**, **Enable Tiling**, **Allow Display Clients to move to/from screen** and **Screen Specific Mouse Button Mapping** checkboxes are checked. Click the **Selector Options** button.



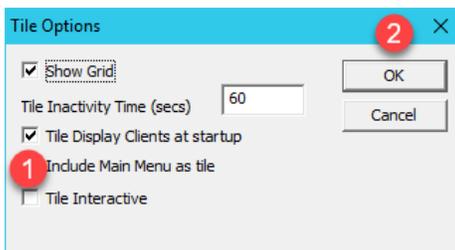
13. From the **Display Client Selector Options** popup, uncheck **Auto-hide Selector** and click the **OK** button.



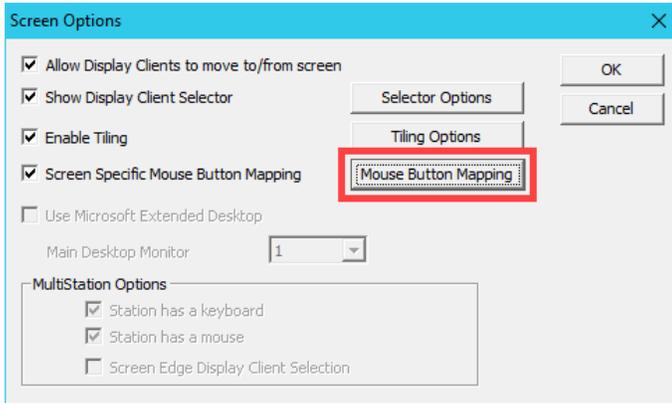
14. Back on the **Screen Options** popup, now click the **Tiling Options** button.



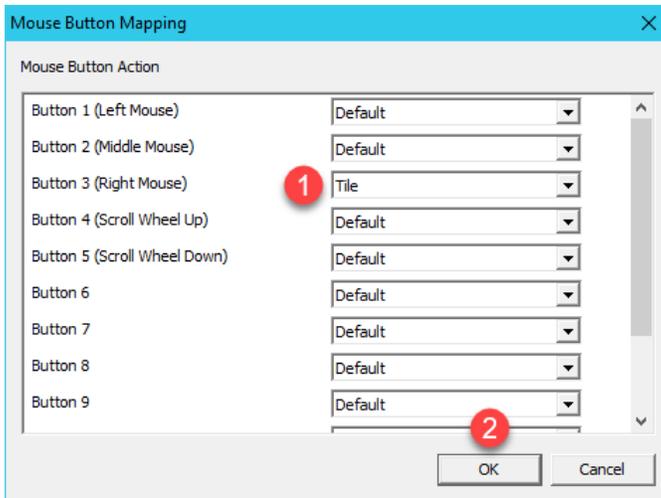
15. From the **Tile Options** popup, check the **Tile Display Clients and startup** check box. Click the **OK** button on the **Tile Options** popup.



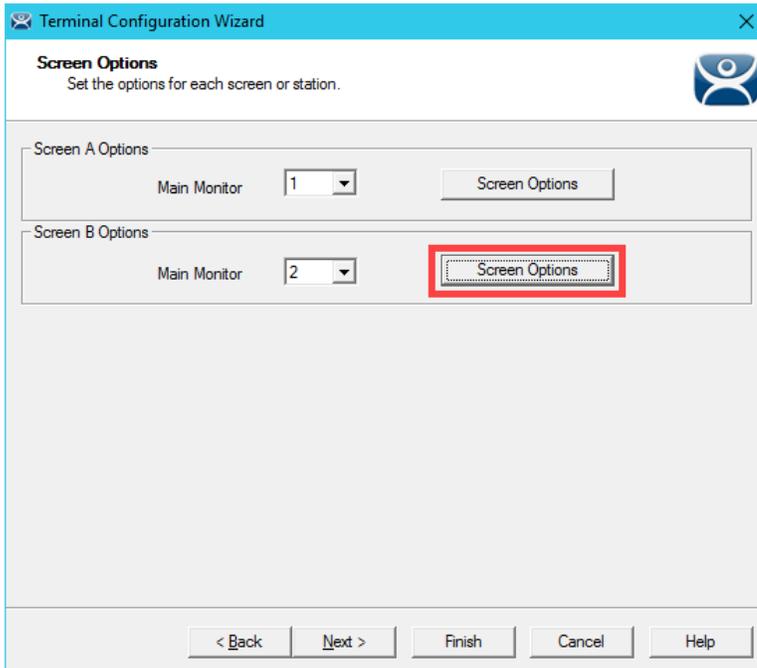
16. Click the **Mouse Button Mapping** button on the **Screen Options** popup.



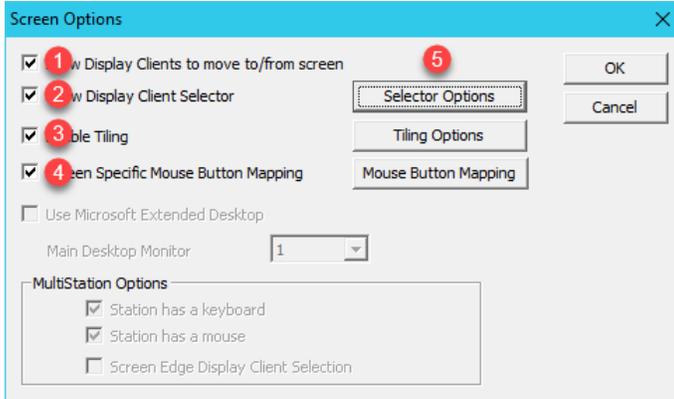
17. From the **Mouse Button Mapping** dialog box, select **Tile** from the **Button 3 (Right Mouse)** drop down list. Click the **OK** button.



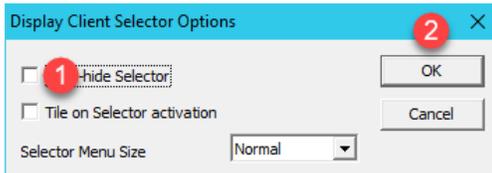
18. Click the **OK** button on the **Screen Options** popup.
19. Back on the **Screen Options** page of the wizard, click the **Screen Options** button for **Screen B**.



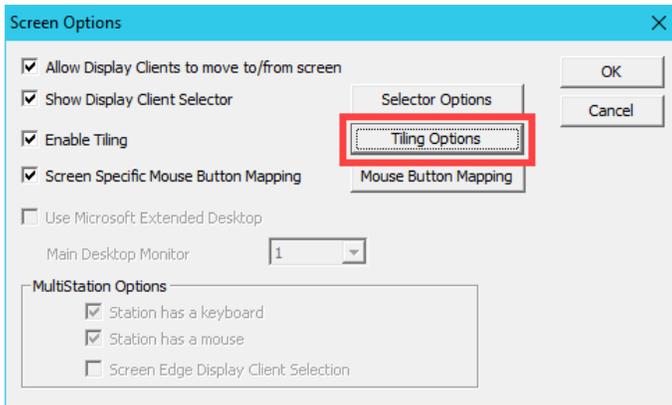
20. Make sure **Show Screen Specific Mouse Button Mapping** checkboxes are checked. Click the **Selector Options** button.



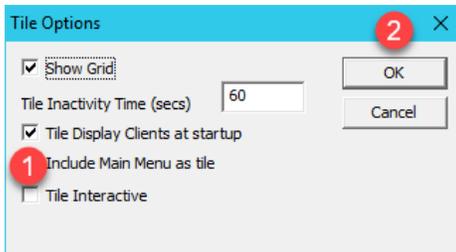
21. From the **Display Client Selector Options** popup, uncheck **Auto-hide Selector** and click the **OK** button.



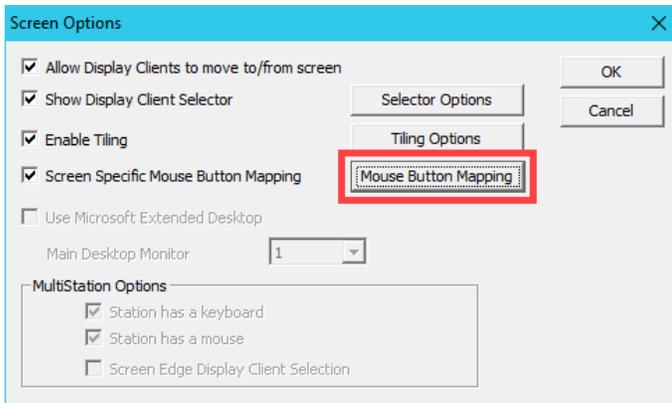
22. Back on the **Screen Options** popup, now click the **Tiling Options** button.



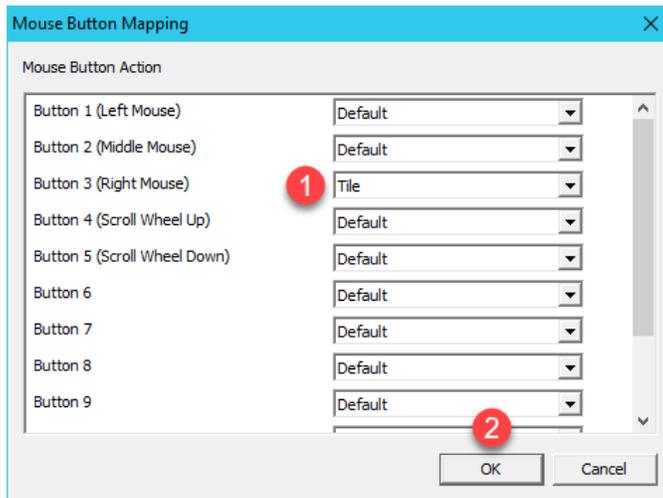
23. From the **Tile Options** popup, check the **Tile Display Clients and startup** check box. Click the **OK** button on the **Tile Options** popup.



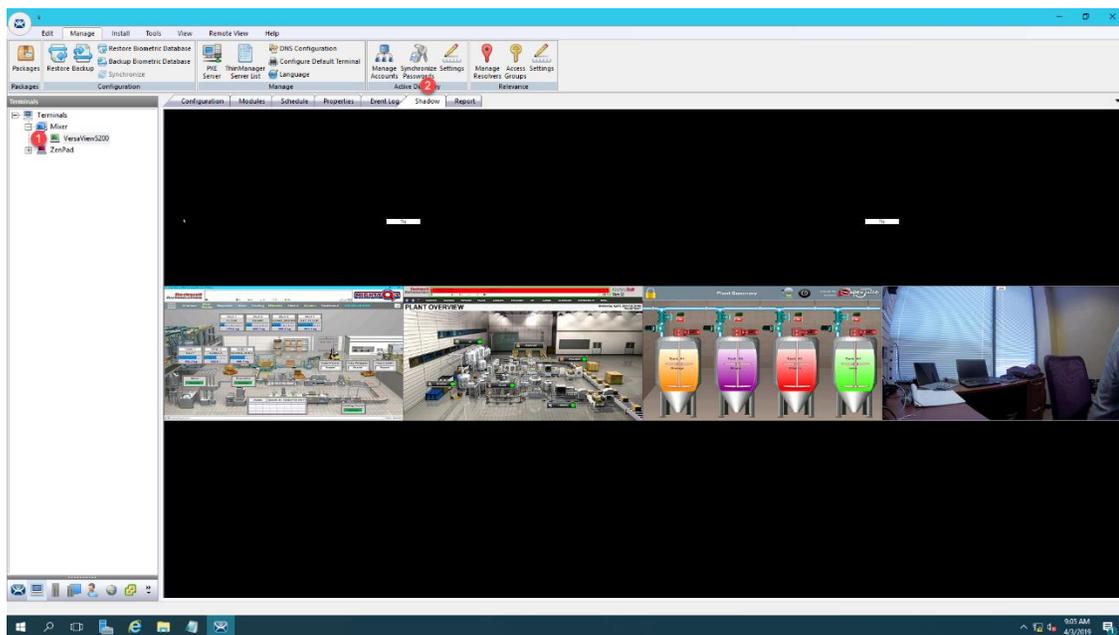
24. Click the **Mouse Button Mapping** button on the **Screen Options** popup.



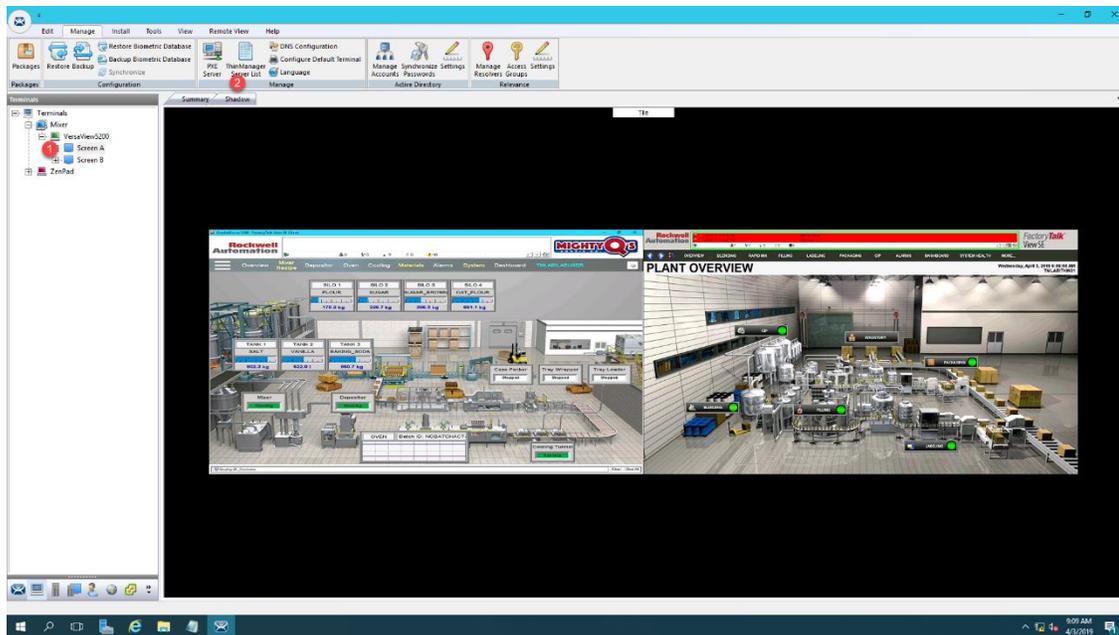
25. From the **Mouse Button Mapping** dialog box, select **Tile** from the **Button 3 (Right Mouse)** drop down list. Click the **OK** button.



26. Click the **OK** button on the **Screen Options** popup.
27. Click the **Finish** button.
28. Right click the **VersaView5200** terminal from the **Terminals** tree and select **Restart Terminal** to apply the changes. Click **Yes** to the confirmation dialog.
29. To see the results, select the **VersaView5200** terminal and then click the **Shadow** tab in the Details Pane.



30. Experiment with the **Display Client Selector** of each monitor while **Shadowing**. You can move **Display Clients** from one monitor to the other and back again. This behavior is fully configurable.
31. You can also shadow an individual monitor, as opposed to both at the same time. Expand the **VersaViewV5200** terminal and select **Screen A**. Now click the **Shadow** tab in the Details Pane to shadow just **Screen A**.



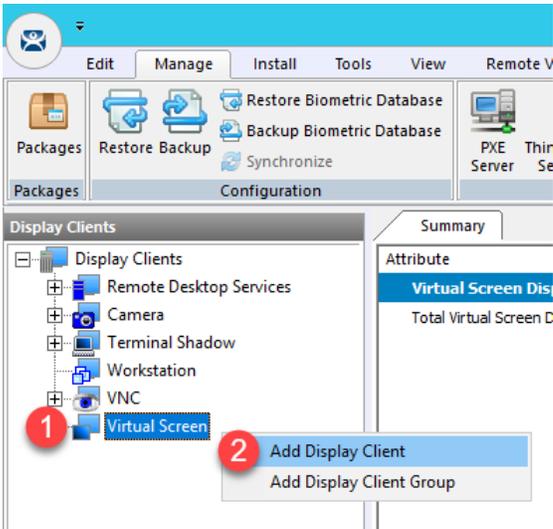
MultiMonitor combined with **Tiling** and/or **Virtual Screens** are extremely powerful tools that really elevate the user experience at the terminal. They are especially valuable in **Control Room** settings, or anywhere centralized monitoring is desired. As previously mentioned, some thin clients can support up to 7 monitors. **ThinManager** also includes a **Shared Keyboard** and **Mouse Module** that can be applied to a group of thin clients. The **Shared Keyboard and Mouse Module** allows you to control several thin clients using a single keyboard and mouse. As an example, you could have three 7 monitor thin clients in your **Control Room** driving a total of 21 displays all being controlled by a single keyboard and mouse. The **Virtual Screen** section will show you an evolution of this **MultiMonitor** concept and really take content visualization to the next level.

Create Virtual Screen Display Client

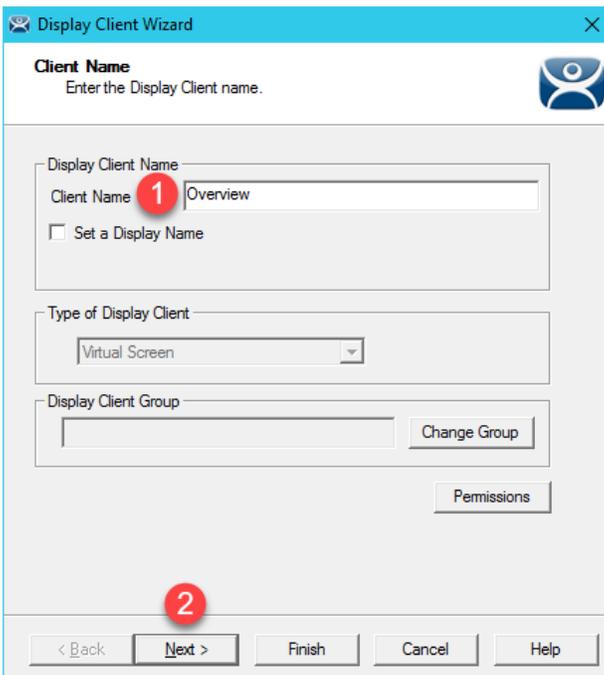
1. Click the **Display Clients**  icon from the ThinManager tree selector.



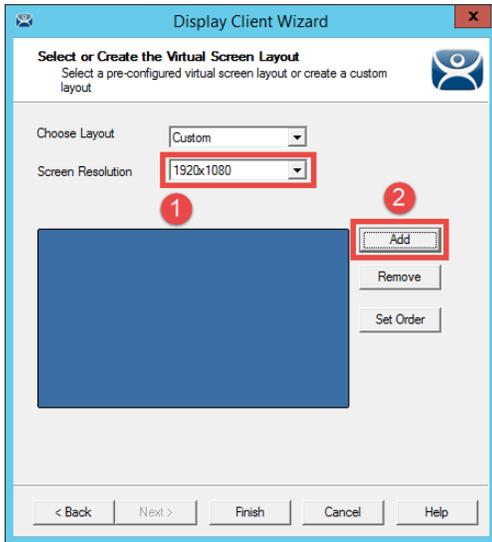
2. Right click the **Virtual Screen** branch and select the **Add Display Client** item.



3. From the **Client Name** page of the wizard, enter *Overview* as the **Client Name**. Click the **Next** button.



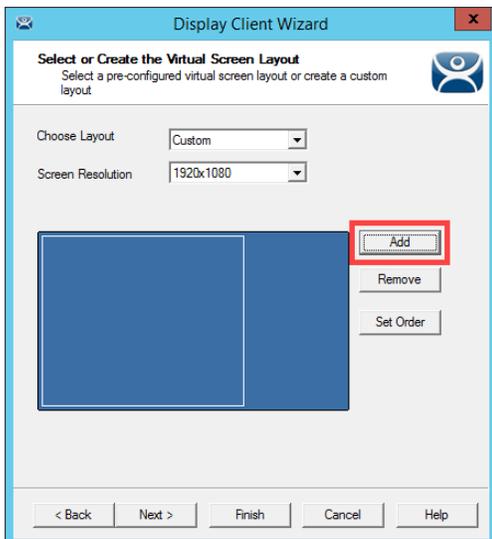
- From the **Display Client Options** page of the wizard, click the **Next** button.
- From the **Select or Create the Virtual Screen Layout** page of the wizard, select **1920x1080** from the **Screen Resolution** drop down list and then click the **Add** button.



- From the **Custom Overlay** dialog box, enter *Main* as the **Overlay Name**, keep *0* in the **Left** field, keep *0* in the **Top** field, *1280* in the **Width** field and *1080* in the **Height** field. Click the **OK** button.



- Back at the **Select or Create the Virtual Screen Layout** page of the wizard, click the **Add** button again to add another overlay.



8. From the **Custom Overlay** dialog box, enter *Side1* as the **Overlay Name**, *1280* in the **Left** field, *0* in the **Top** field, *640* in the **Width** field and *360* in the **Height** field. Click the **OK** button.

Custom Overlay

Overlay Name **1** Side1 **5** OK Cancel

Position / Size **2**

Left	Top	Width	Height
1280	0	640 3	360 4

9. Back at the **Select or Create the Virtual Screen Layout** page of the wizard, click the **Add** button again to add another overlay.

Display Client Wizard

Select or Create the Virtual Screen Layout
Select a pre-configured virtual screen layout or create a custom layout

Choose Layout Custom

Screen Resolution 1920x1080

Add Remove Set Order

< Back Next > Finish Cancel Help

10. From the **Custom Overlay** dialog box, enter *Side2* as the **Overlay Name**, *1280* in the **Left** field, *360* in the **Top** field, *640* in the **Width** field and *360* in the **Height** field. Click the **OK** button.

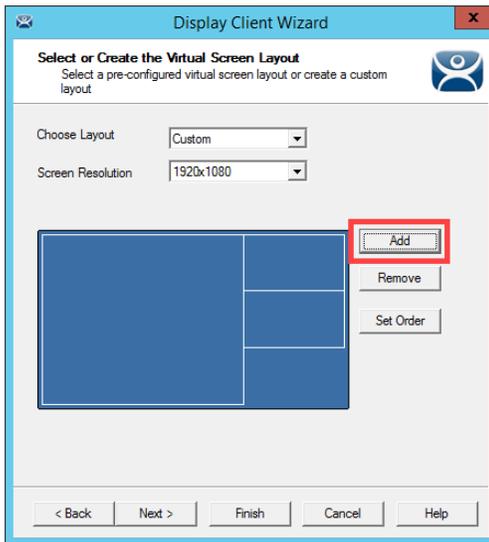
Custom Overlay

Overlay Name **1** Side2 **6** OK Cancel

Position / Size **2**

Left	Top	Width	Height
1280	360 3	640 4	360 5

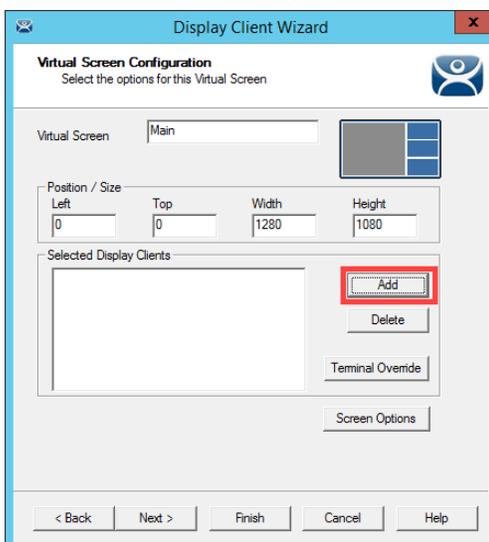
11. Back at the **Select or Create the Virtual Screen Layout** page of the wizard, click the **Add** button again to add another overlay.



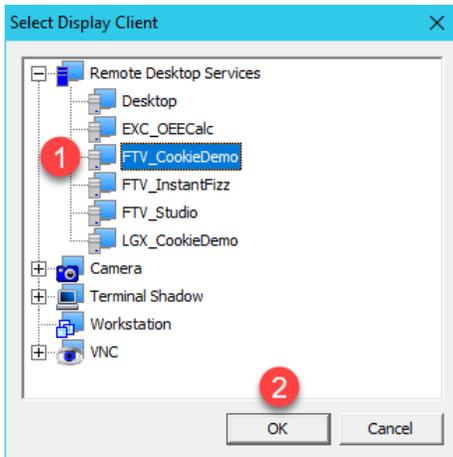
12. From the **Custom Overlay** dialog box, enter *Side3* as the **Overlay Name**, *1280* in the **Left** field, *720* in the **Top** field, *640* in the **Width** field and *360* in the **Height** field. Click the **OK** button, followed by the **Next** button.



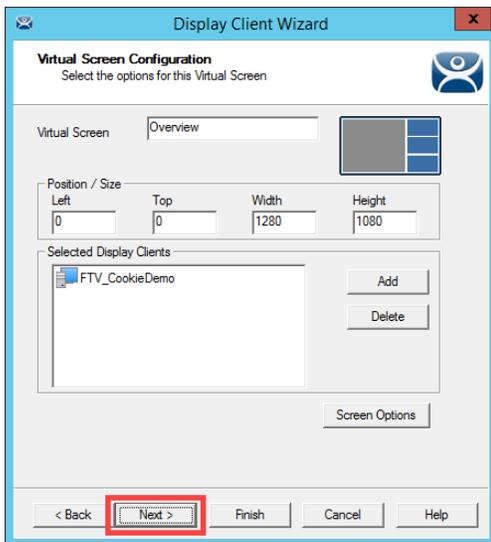
13. We will now assign content to each of the Virtual Screens created, starting with the **Main** Virtual Screen. Click the **Add** button in the **Selected Display Clients** frame.



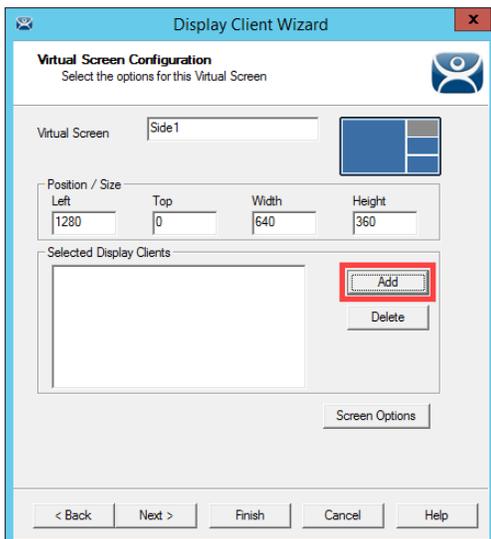
14. Select the **FTV_CookieDemo** item from the list and click the **OK** button.



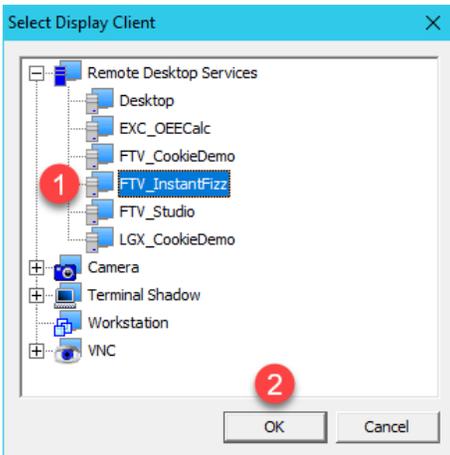
15. Back at the **Virtual Screen Configuration** page of the wizard, click the **Next** button.



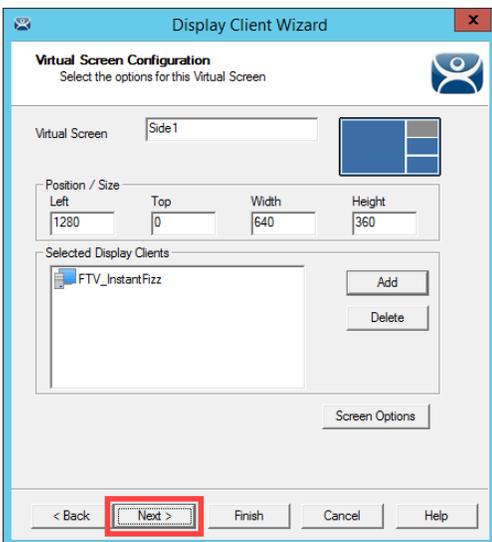
16. Now for the **Side1** Virtual Screen, click the **Add** button.



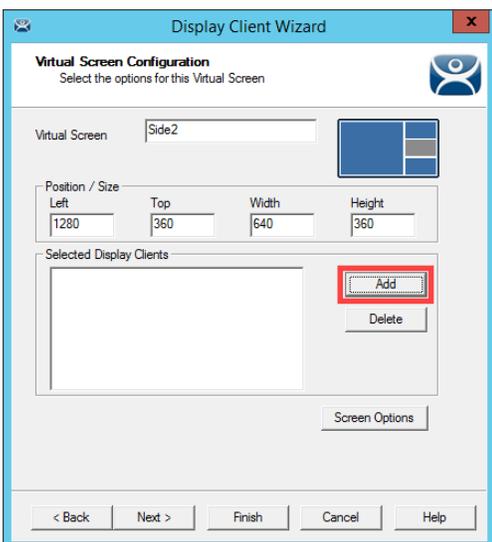
17. Select the **FTV_InstanFizz** item from the list and click the **OK** button.



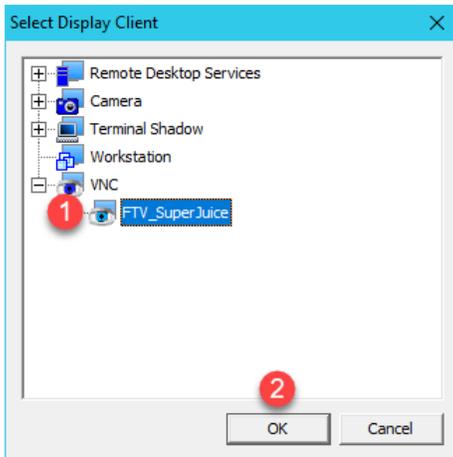
18. Back at the **Virtual Screen Configuration** page of the wizard, click the **Next** button.



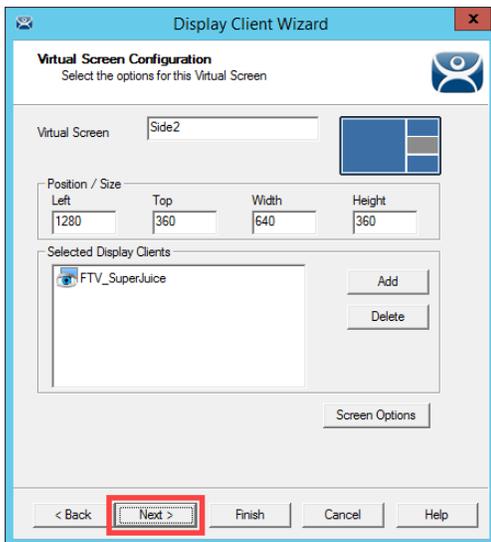
19. Now for the **Side2** Virtual Screen, click the **Add** button.



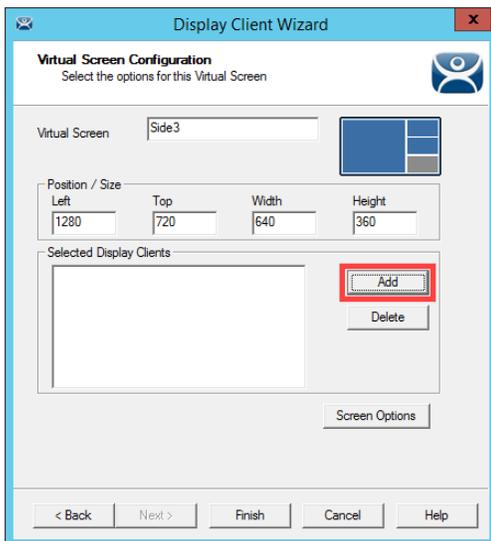
20. Select the **FTV_SuperJuice** item from the list and click the **OK** button.



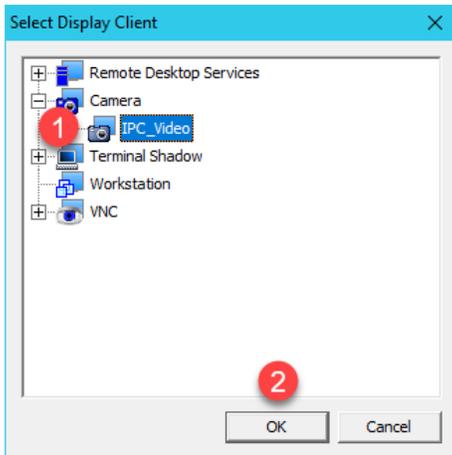
21. Back at the **Virtual Screen Configuration** page of the wizard, click the **Next** button.



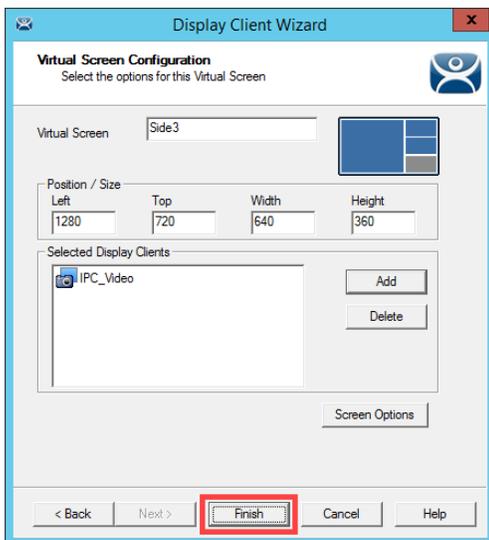
22. Now for the **Side3** Virtual Screen, click the **Add** button.



23. Select the **IPC_Video** item from the list and click the **OK** button.



24. Back at the **Virtual Screen Configuration** page of the wizard, click the **Finish** button.

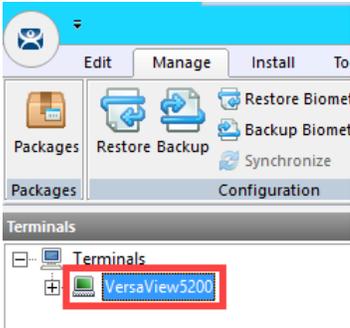


Apply Virtual Screen to Terminal

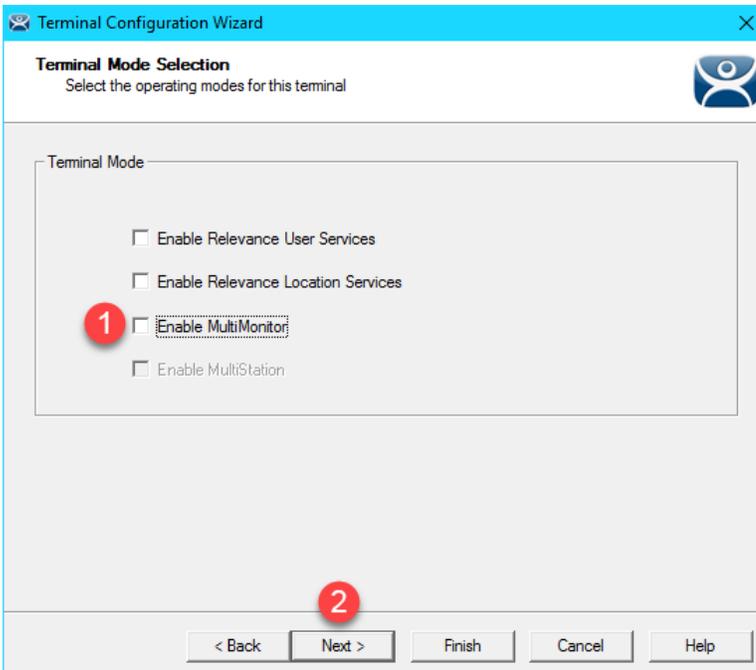
1. Click the **Terminals** tree selector icon.



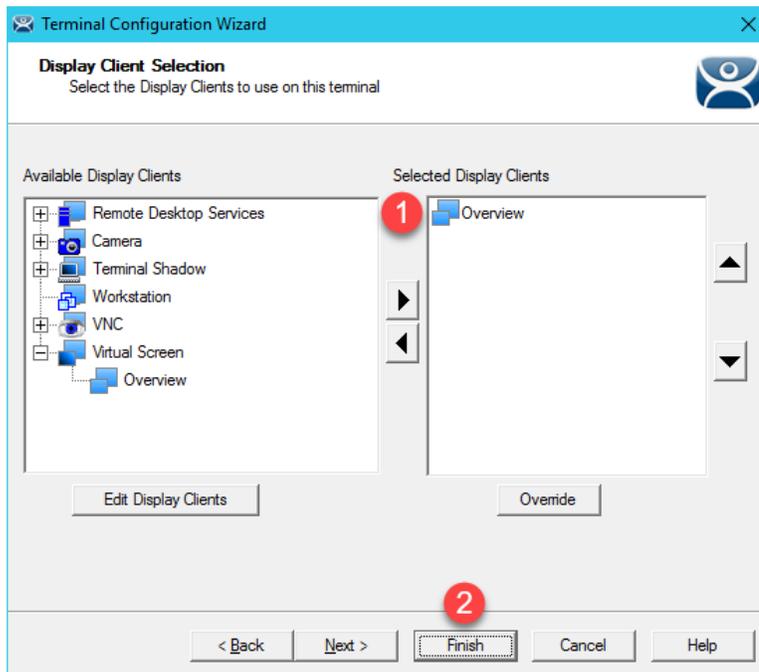
2. Double click the **VersaView5200** terminal.



3. Click the **Next** button on the **Terminal Name** page of the wizard.
4. Click the **Next** button on the **Terminal Hardware** page of the wizard.
5. Click the **Next** button on the **Terminal Options** page of the wizard.
6. From the **Terminal Mode Selection** page of the wizard, un-check **Enable MultiMonitor**.



- From the **Display Client Selection** page of wizard, remove all of the **Display Clients** from the **Selected Display Clients** list. Select the **Overview Display Client** from the **Available Display Clients** list and click the **Right Arrow** button to move it to the **Selected Display Clients** list. Click the **Finish** button.



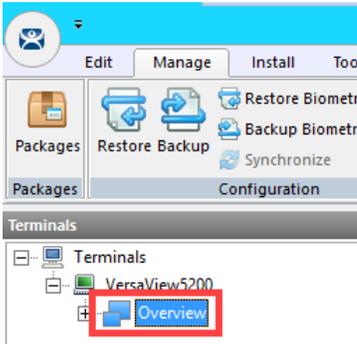
- Right click the **VersaView5200** terminal and select the **Restart Terminal** item. Click the **Yes** button to confirm.

Like **MultiMonitor Display Clients**, **Virtual Screen Display Clients** can be configured to be moveable from one **Virtual Screen** to another. You can also enable **Tiling** within a **Virtual Screen**. In addition, you can select any of the **Virtual Screens** to go **Full Screen** from their respective **Display Client Selector**, and then return to **Virtual Screen** mode. **Virtual Screening** allows you to take the concept of digital signage to the plant floor and deliver a wide range of content in virtually an unlimited number of ways.

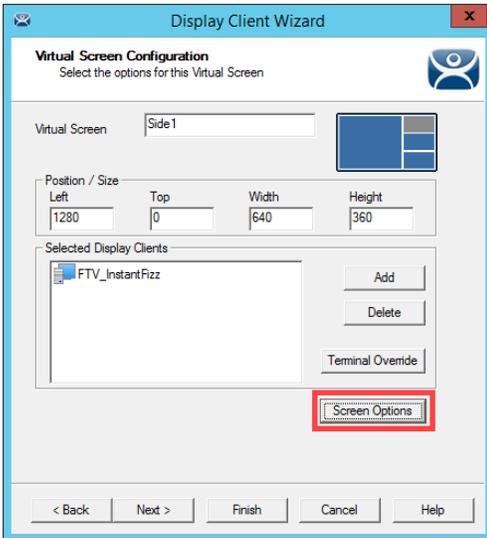
ThinManager 8.1 added support for 4K monitors. For thin clients with the graphics horsepower to drive a 4K display (3840x2160), you can, for example, carve up the 4K display into 4 separate 1920x1080 quadrants and treat them as individual displays within **ThinManager using Virtual Screening**.

Add Virtual Screen Swapping

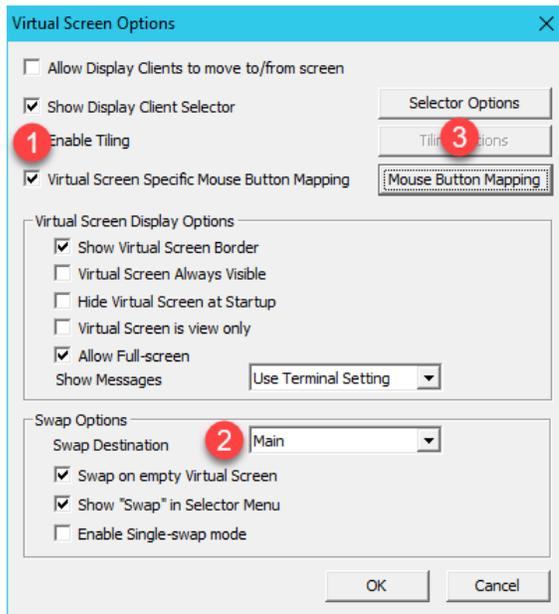
1. From the **Terminals** tree, expand the **VersaView5200** terminal and then double click the **Overview Virtual Screen Display Client** to launch the **Display Client Wizard**.



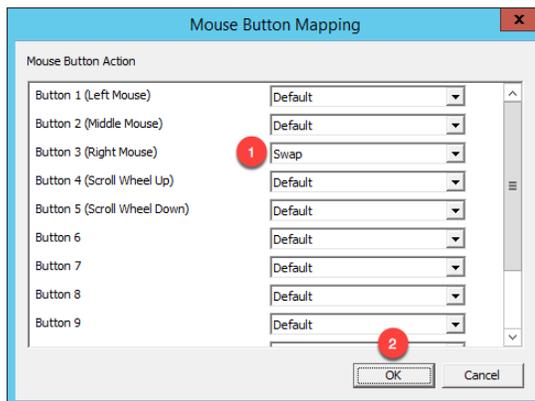
2. From the **Client Name** page of the wizard, click the **Next** button.
3. From the **Display Client Options** page of the wizard, click the **Next** button.
4. From the **Select or Create the Virtual Screen Layout** page of the wizard, click the **Next** button.
5. From the **Main Virtual Screen Configuration** page of the wizard, click the **Next** button.
6. From the **Side1 Virtual Screen Configuration** page of the wizard, click the **Screen Options** button.



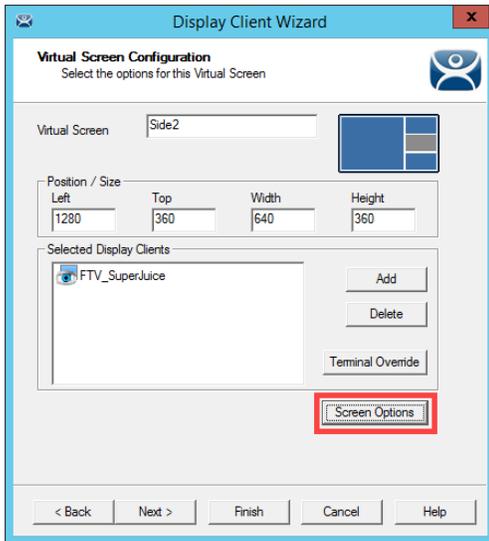
7. From the **Virtual Screen Options** dialog, check the **Virtual Screen Specific Mouse Button Mapping** checkbox, and select **Main** from the **Swap Destination** drop down list. Click the **Mouse Button Mapping** button.



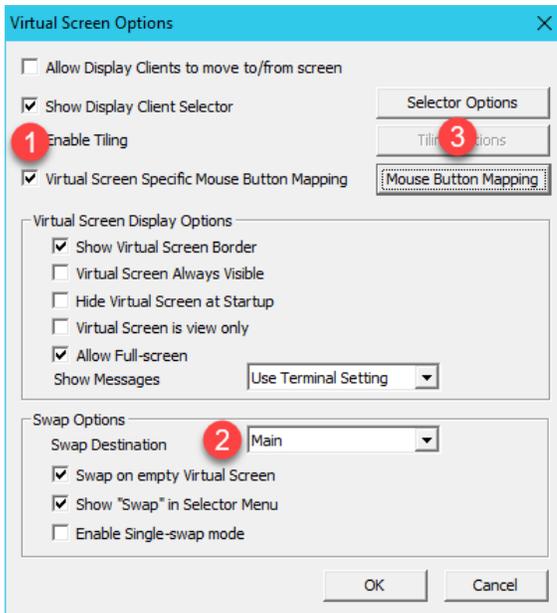
8. From the **Mouse Button Mapping** dialog, select **Swap** from the **Button 3 (Right Mouse)** drop down list. Click the **OK** button twice, followed by the **Next** button.



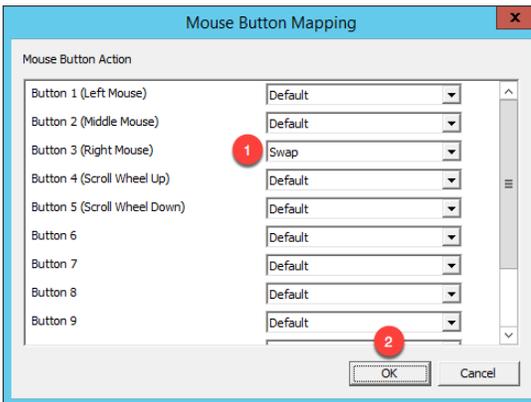
9. Back at the **Side 2 Virtual Screen Configuration** page of the wizard, click the **Screen Options** button.



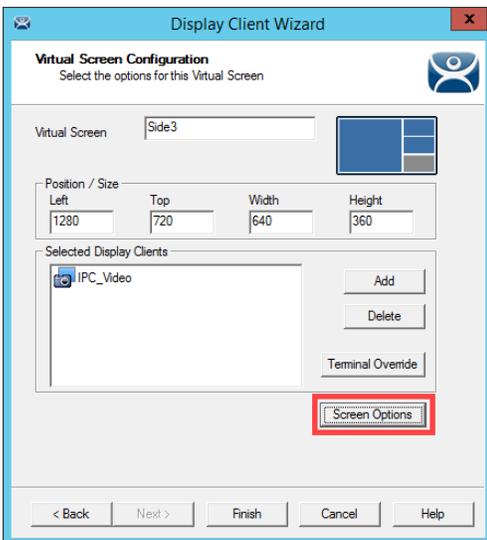
10. From the **Virtual Screen Options** dialog, check the **Virtual Screen Specific Mouse Button Mapping** checkbox, and select **Main** from the **Swap Destination** drop down list. Click the **Mouse Button Mapping** button.



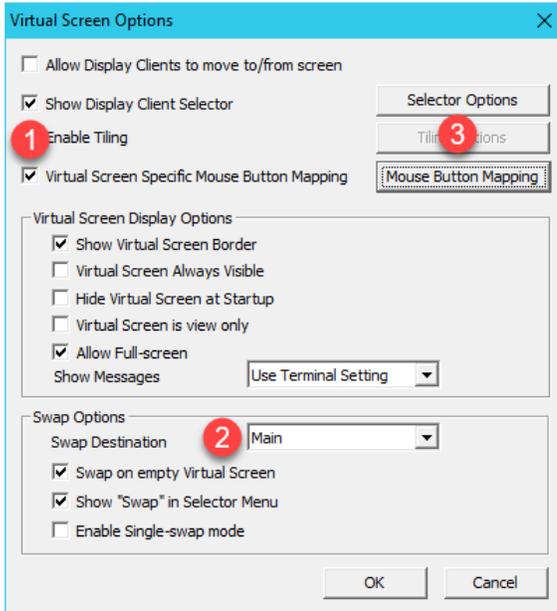
11. From the **Mouse Button Mapping** dialog, select **Swap** from the **Button 3 (Right Mouse)** drop down list. Click the **OK** button twice, followed by the **Next** button.



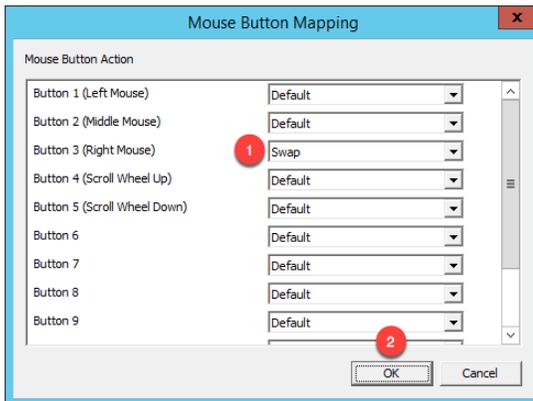
12. Back at the **Side 3 Virtual Screen Configuration** page of the wizard, click the **Screen Options** button.



- From the **Virtual Screen Options** dialog, check the **Virtual Screen Specific Mouse Button Mapping** checkbox, and select **Main** from the **Swap Destination** drop down list. Click the **Mouse Button Mapping** button.



- From the **Mouse Button Mapping** dialog, select **Swap** from the **Button 3 (Right Mouse)** drop down list. Click the **OK** button twice, followed by the **Finish** button.



- Right click the **VersaView5200** terminal from the **Terminals** tree and select **Restart Terminal** to apply the changes. Click **Yes** to the confirmation dialog.
- Select the **Shadow** tab to see the results. **Right click** on any of the 3 side virtual screens to test the swapping capability.

This completes the section **Virtual Screens and Session Scaling** of the lab. Please continue on to **Relevance User Services** to explore user based content delivery.

Section 6: Relevance User Services - User Based Content Delivery

Overview

Up to this point in the lab, you have assigned default content to the **Terminal's Profile**. In other words, the content is owned by the terminal and is the same regardless of who is physically at the terminal. You can control a user's access within each application at the terminal by requiring them to login **within** the application and then customizing their experience there – but this is completely separate from ThinManager. This lab section will demonstrate how you can customize the actual content that a user receives at a **Terminal in addition** to the default content that is assigned to the **Terminal Profile**. For instance, you may want to deliver additional content to a Maintenance user that logs into the terminal using ThinManager security, such as the Maintenance Work Order System, or possibly Logix Designer.

This lab section is composed of the following tasks:

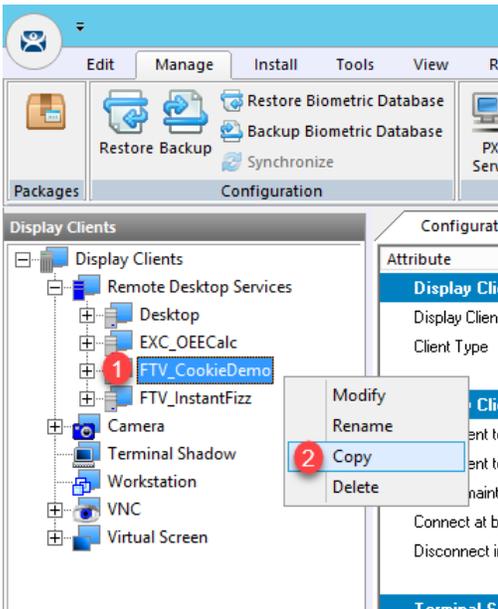
1. Create a View Studio Display Client
2. Create an Engineer User Group
3. Create an Engineer User
4. Enable User Services for Terminal
5. Login as Engineer User
6. Add RF IDEas Badge Reader
7. Configure ThinManager to Cache Password
8. Add Multifactor Authentication with a PIN and Password Storage
9. Authentication Pass Through
10. Remove Tiled Display Clients

Create View Studio Display Client

1. From ThinManager, click the **Display Clients** icon  from the ThinManager tree selector.

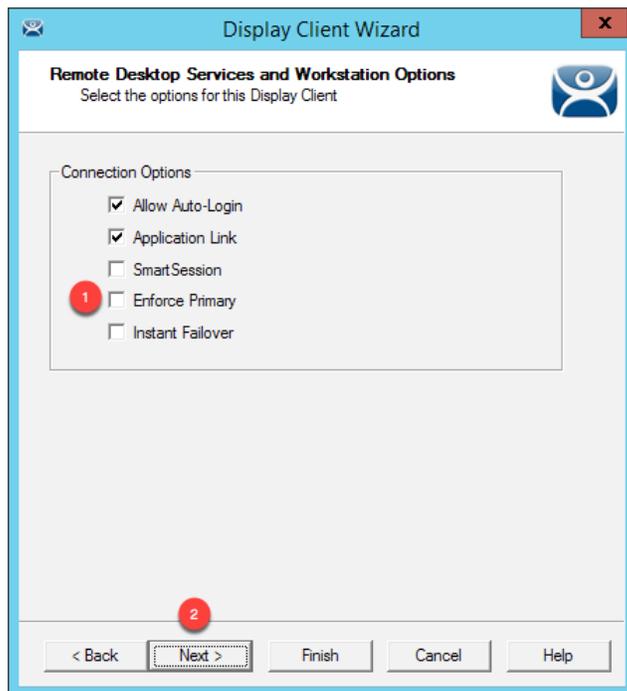


2. From the **Display Clients** tree, expand the **Remote Desktop Services** branch and right click the **FTV_CookieDemo** item and select **Copy**.

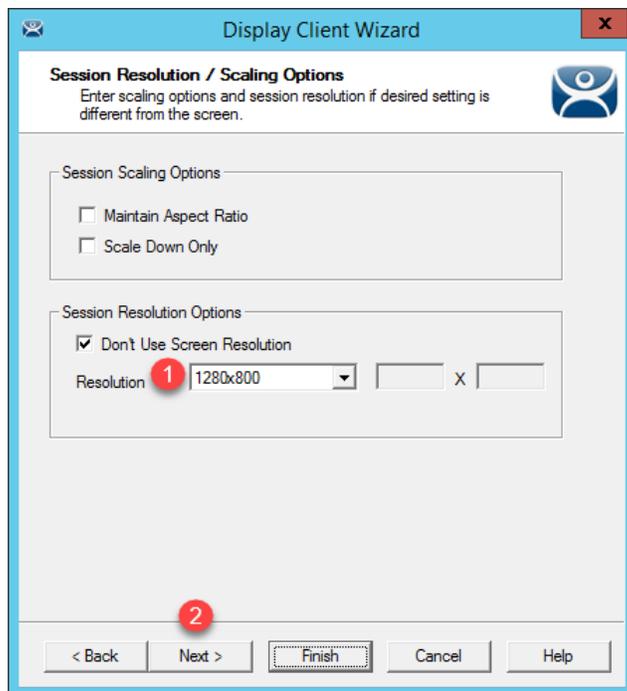


3. Type *FTV_Studio* in the **Enter new Display Client Name** text box and click the **OK** button.
4. Double click the new **FTV_Studio** Display Client item.
5. Click the **Next** button on the **Client Name** page of the wizard.
6. Click the **Next** button on the **Display Client Options** page of the wizard.

- From the **Remote Desktop Services and Workstation Options** page of the wizard, uncheck the **Enforce Primary** checkbox and click the **Next** button.

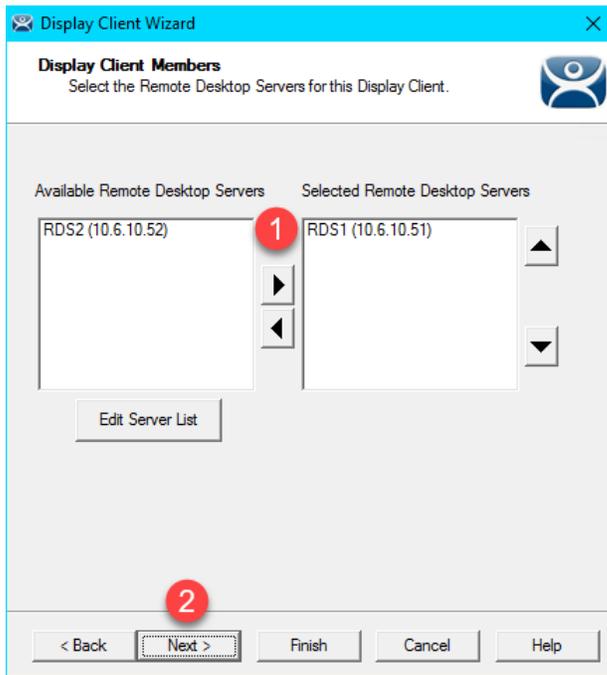


- From the **Screen Resolution / Scaling Options** page of the wizard, change the **Resolution** to **1280x800**. Click the **Next** button.



We are assigning the 1280x800 resolution here so that the Display Client will scale nicely on the Asus ZenPad in the next section.

- From the **Display Client Members** page of the wizard, remove **RDS2** from the **Selected Remote Desktop Servers** list, leaving just **RDS1**, click **Next**.



- From the **AppLink** page of the wizard, replace the **Program Path and Filename** and **Command Line Options** with the ones below (you can also copy and paste this path from the **LabPaths.txt** file by right clicking the **Notepad** icon pinned to the start bar and selecting **LabPaths.txt**):

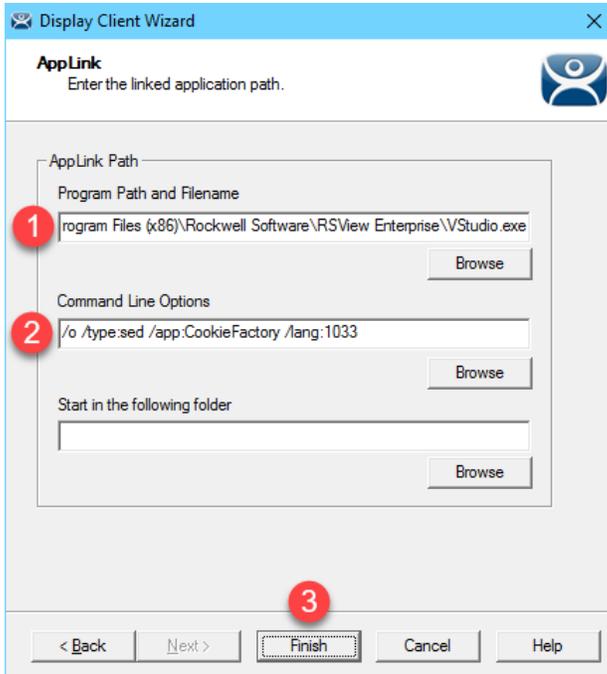
Program Path and Filename:

C:\Program Files (x86)\Rockwell Software\RSView Enterprise\VStudio.exe

Command Line Options:

/o /type:sed /app:CookieFactory /lang:1033

Click the **Finish** button.

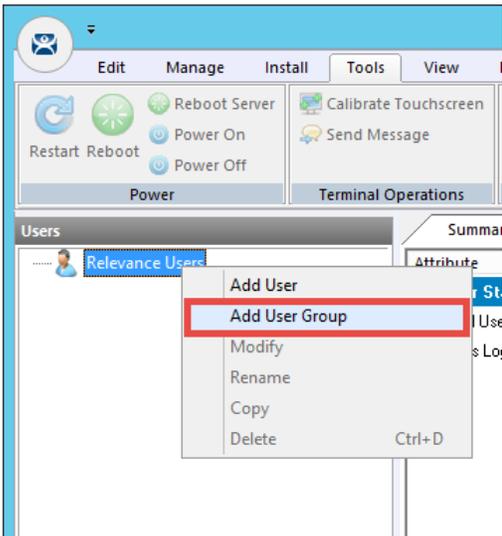


Create an Engineer User Group

1. Click the **Users** icon  in the ThinManager tree selector.



2. From the **Relevance Users** tree, right click the **Relevance Users** node and select **Add User Group**. This will launch the **Relevance User Configuration Wizard**.

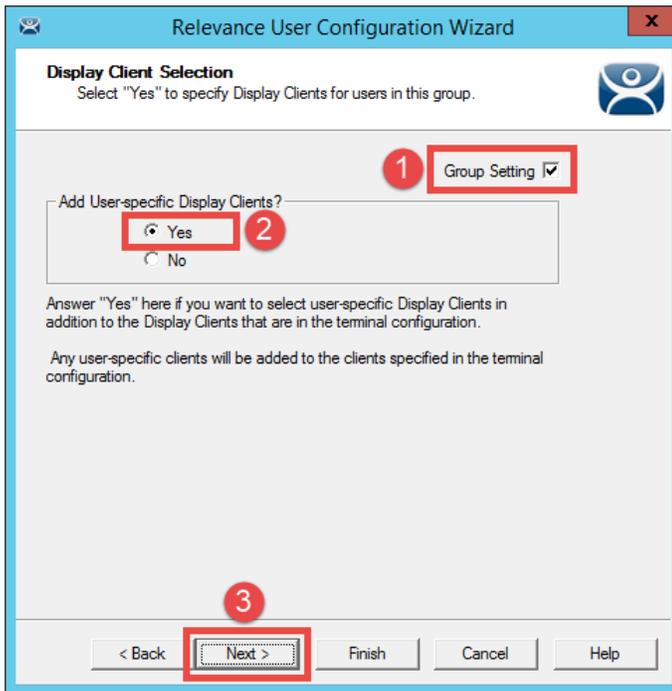


- From the **Relevance User Group Information** page of the wizard, enter *Engineer* as the **User Name** in the **Group Name** frame. Click the **Next** button.

The screenshot shows the 'Relevance User Configuration Wizard' window. The title bar reads 'Relevance User Configuration Wizard'. The main window title is 'Relevance User Group Information' with the instruction 'Enter the Relevance User Group name.' Below this, there is a checkbox for 'AD Synchronization Group'. Underneath, the 'Group Name' section contains a 'User Name' field with the text 'Engineer' and a red circle with the number '1' next to it. There are also 'Password' and 'Verify Password' fields. Below these are buttons for 'Customize', 'Password Options', and a 'Group Setting' checkbox. A 'Group' field is also present with a 'Change Group' button. At the bottom, there is a 'Permissions' button and a navigation bar with buttons for '< Back', 'Next >', 'Finish', 'Cancel', and 'Help'. A red circle with the number '2' is placed over the 'Next >' button.

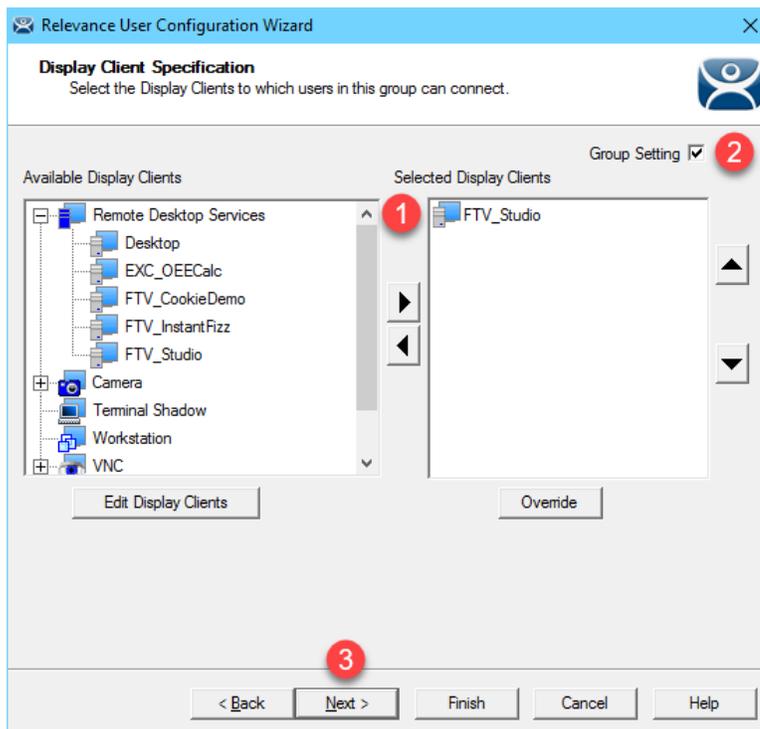
ThinManager 8 included much tighter integration with Active Directory. For example, a Relevance User Group can be automatically synchronized with an Active Directory group. In doing so, ThinManager would automatically create Relevance Users for each member of the synchronized Active Directory group. It should be noted that only 1 AD Security Group can be used to synchronize with Active Directory in ThinManager. This limitation is because an Active Directory user can be a member of multiple Active Directory groups, but ThinManager does not support this membership model (i.e.: a Relevance User can only belong to one Relevance User Group). ThinManager can also synchronize with an Organizational Unit and automatically create the associated Relevance users.

- From the **Display Client Selection** page of the wizard, check the **Group Setting** checkbox. Select **Yes** from the **Add User-specific Display Clients** radio button group. Click the **Next** button.



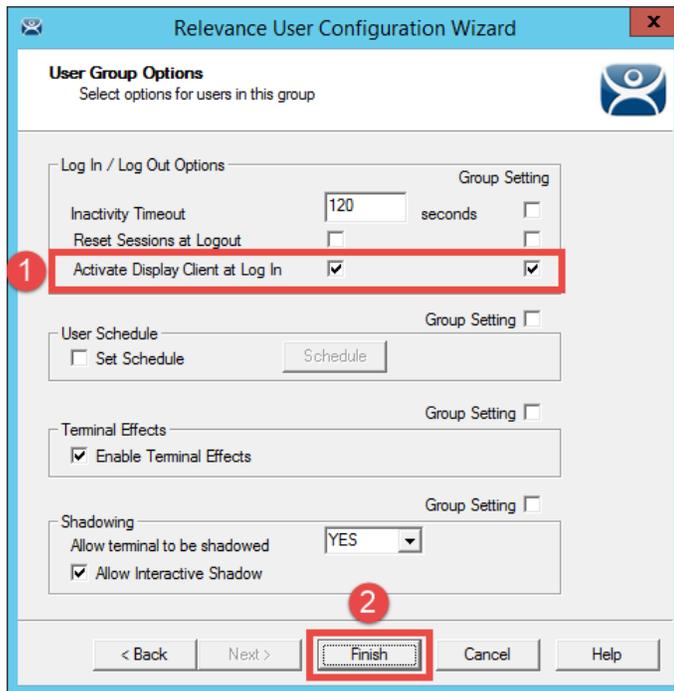
Clicking the Group Setting checkbox will pass the setting onto members of the group.

5. Select **FTV_Studio** from the **Available Display Clients** list and click the **Right Arrow** button to move it to the **Selected Display Clients** list. Click the **Group Setting** checkbox and then click the **Next** button.



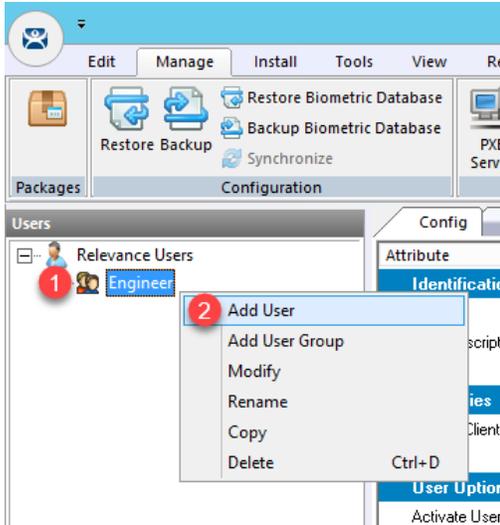
6. From the **Windows Log In Information** page of the wizard, click the **Next** button.
7. From the **Terminal Interface Options** page of the wizard, note that you can override the default **Terminal** settings by making changes here. Leave the default settings in place. Click the **Next** button.
8. From the **Terminal Hotkey Options** page of the wizard, click the **Next** button.

- From the **User Group Options** page of the wizard, click the **Activate Display Client at Log In** checkbox, as well as its **Group Setting** checkbox. This setting will pull the user's configured **Display Clients** to the foreground at the **Terminal** when they login. Click the **Finish** button.

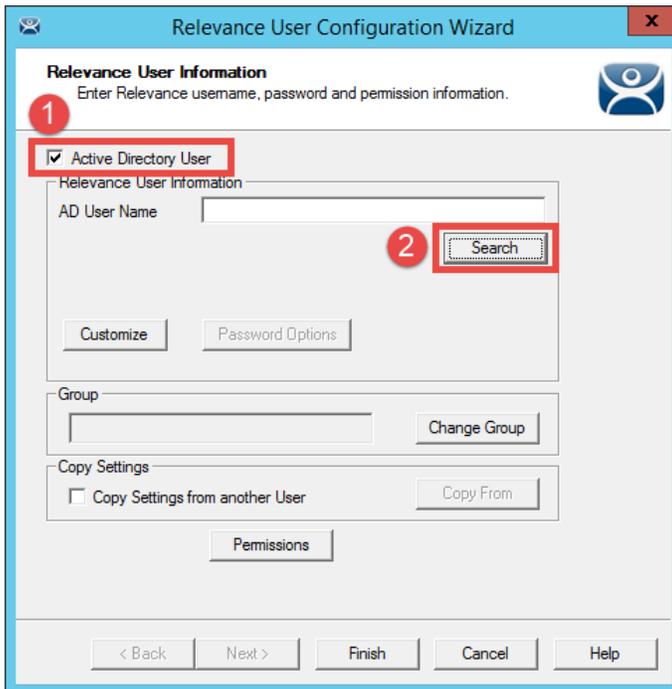


Create an Engineer User

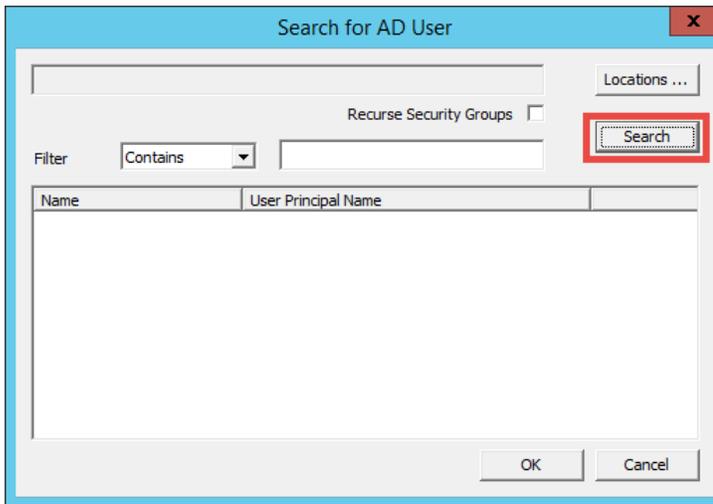
1. Expand the **Relevance Users** node.
2. Right click the newly created **Engineer User Group** and select **Add User**. This will launch the **Relevance User Configuration** wizard.



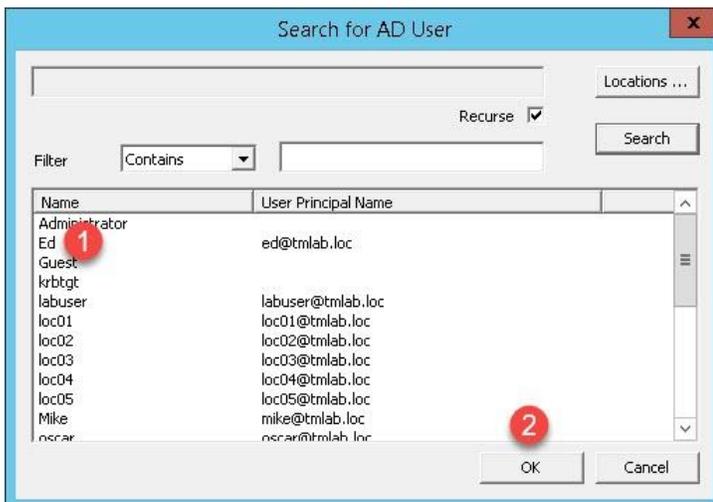
3. From the **Relevance User Information** page of the wizard, check the **Active Directory User** checkbox if it is not already checked. Click the **Search** button.



- From the **Search for AD User** dialog box, click the **Search** button.



- Select **Ed** from the user list and then click the **OK** button.



By linking to an Active Directory User, this Relevance user's credentials will reside in Active Directory, not within ThinManager. You can also create non-linked Active Directory users in ThinManager, in which case their credentials would reside in ThinManager.

6. Back at the **Relevance User Information** page of the wizard, click the **Next** button.

Relevance User Configuration Wizard

Relevance User Information
Enter Relevance username, password and permission information.

Active Directory User

Relevance User Information

AD User Name: Ed [Search]

[Customize] [Password Options]

Group: [Change Group]

Copy Settings

Copy Settings from another User [Copy From]

[Permissions]

< Back [Next >] Finish Cancel Help

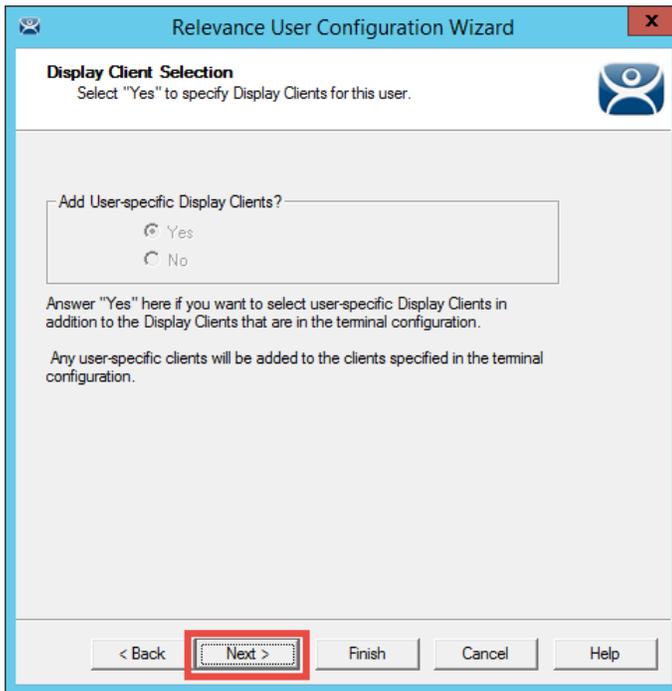
7. From the **Active Directory Password** page of the wizard click the **Next** button.

Note that you can choose to store the Active Directory password for this user within ThinManager. This is sometimes done when using badge readers or fingerprint scanners so the user can either scan his/her badge or scan his/her fingerprint only to login (i.e.: no password entry is required). If the Active Directory password were to change outside of ThinManager, the user would be prompted to enter the new password upon their next login attempt, which would then result in ThinManager storing the updated password.

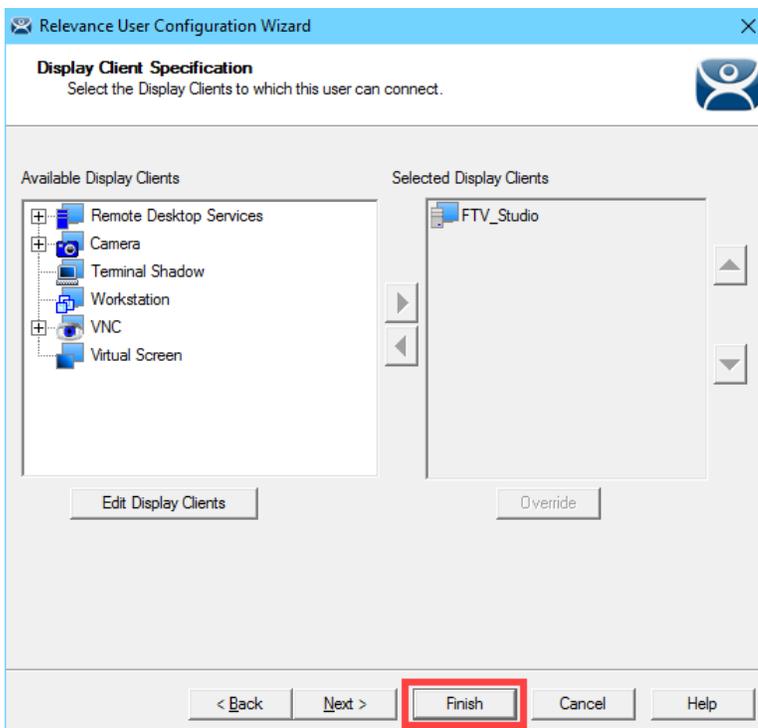
You can also allow ThinManager to automatically rotate the user's Active Directory password based on pre-defined criteria, in which case, only ThinManager would know the active password. Many times end users choose to have their terminals automatically login to the Remote Desktop Servers with a service account, and then security is managed within the application delivered. Prior to ThinManager 8, a service account with a non-expiring password would have to be created in this scenario.

8. From the **Card / Badge Information** page of the wizard, click the **Next** button. We will incorporate an RF IDEas badge reader shortly.
9. From the **Relevance Resolver Selection** page of the wizard, click the **Next** button.

10. From the **Display Client Selection** page of the wizard, notice that the selection is disabled. This is because we chose **Group Setting** for this setting on the **User Group**. Click the **Next** button.



11. From the **Display Client Specification** page of the wizard, notice that the selection is disabled here as well. Click the **Finish** button.

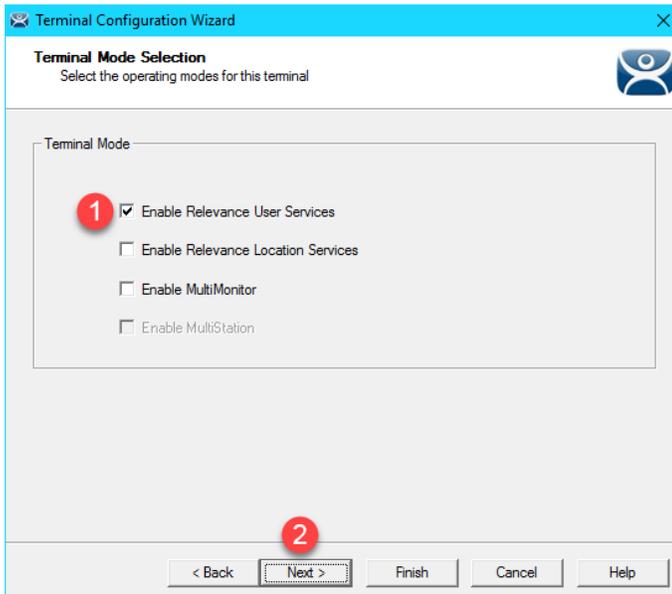


Enable User Services for Terminal

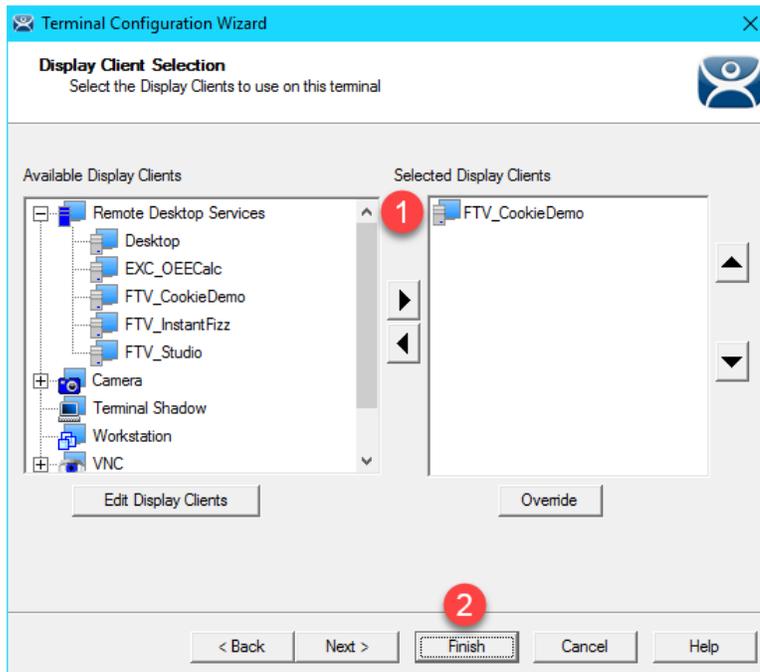
1. Click the **Terminals** icon  from the ThinManager tree selector.



2. Under the **Terminals** node, double click the **VersaView5200** terminal to launch the **Terminal Configuration Wizard**.
3. Click the **Next** button on the **Terminal Name** page of the wizard.
4. Click the **Next** button on the **Terminal Hardware** page of the wizard.
5. Click the **Next** button on the **Terminal Options** page of the wizard.
6. From the **Terminal Mode Selection** page of the wizard, check **Enable Relevance User Services**. Click the **Next** button.



- From the **Display Client Selection** page of the wizard, remove the **Overview Display Client** from the **Select Display Clients** listbox and add the **FTV_CookieDemo Display Client**.

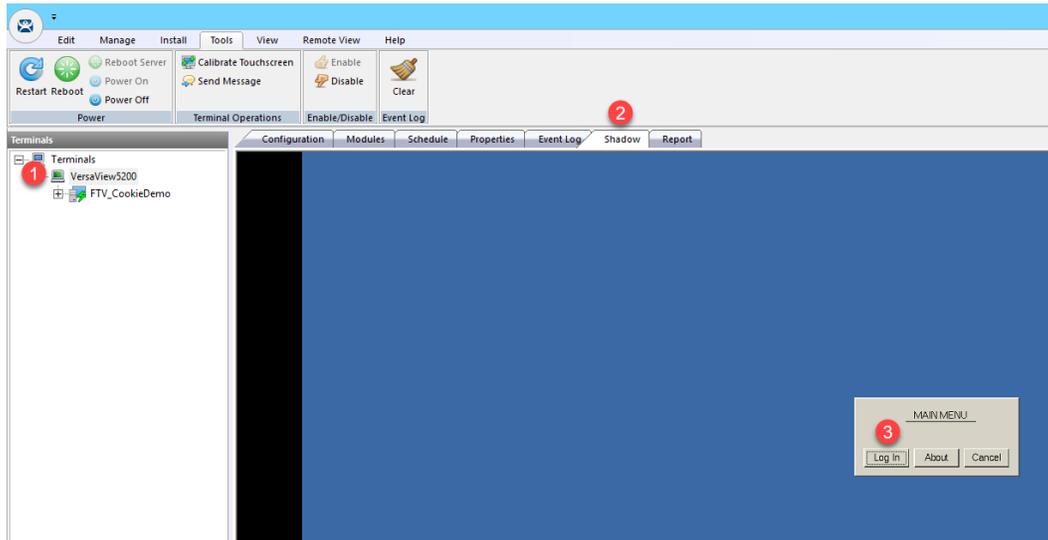


- Right click **VersaView5200** and select **Restart Terminal** to apply the change.

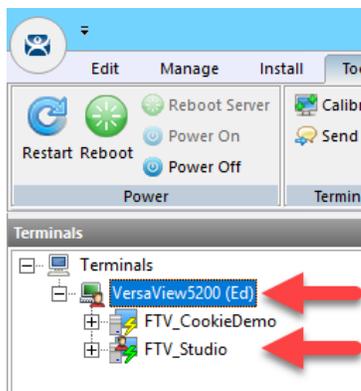
When deploying **Relevance Users** for the first time, Enabling **Relevance User Services** at the **Terminal** is a commonly missed step. Without Enabling **Relevance User Services** at the terminals where you want to enable Relevance User logins, the Login option will not be available from the **Main Menu**. If you would like to Enable **Relevance User Services** for all of your terminals, you can create a **Terminal Group**, enable it there, and check the **Group Setting** checkbox. Each Terminal member of the Terminal Group would then have it enabled. Again, **Terminal Groups** will be explored in [Section 13](#).

Login as Engineer User

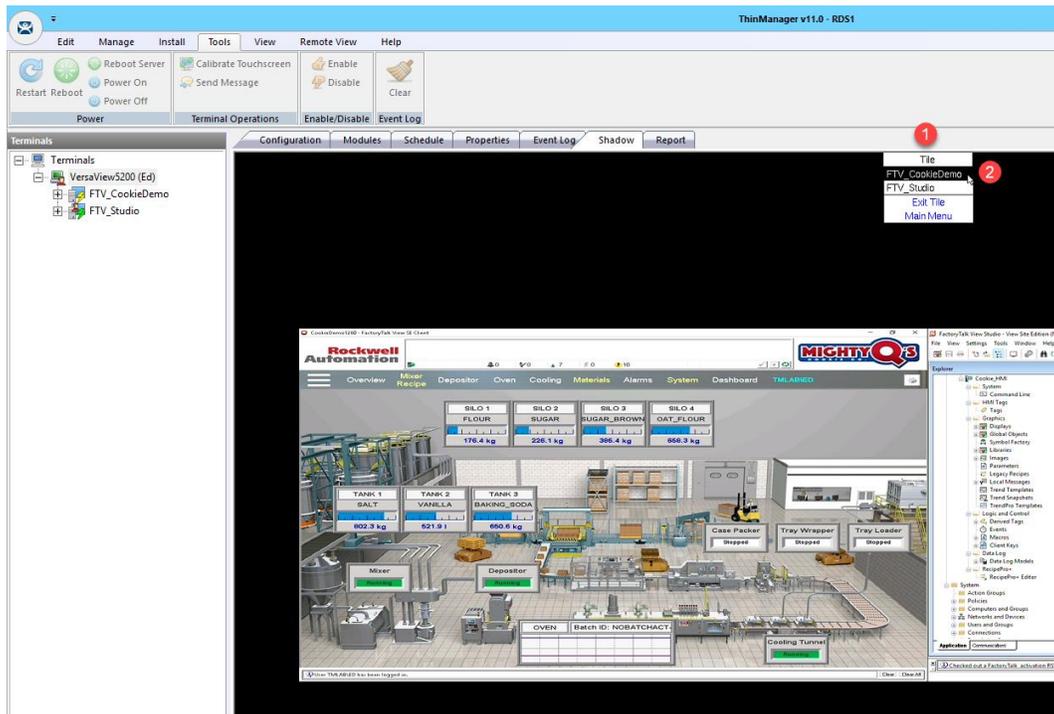
1. From the **Terminals** icon  in the ThinManager tree selector, select **VersaView5200**.
2. Click the **Shadow** tab from the Details Pane.
3. Hit CTRL-m to access the **Main Menu**.
4. From the **Main Menu**, click the **Log In** button.



5. From the **Log In** popup, enter *Ed* as the **User Name**.
6. From the **Password** popup, enter *rw* as the **Password**.
7. Once logged in, the **View Studio Display Client** should be launched. Notice that there are now 2 **Display Clients** listed under the **VersaView5200 Terminal** in the **Terminals** tree. Also notice that the **VersaView5200 Terminal** label now indicates that (**Ed**) is logged in there.



- Click and hold the **Display Client Selector** within the **Shadow** and hover over the **FTV_CookieDemo Display Client** to activate it.



- Click and hold the **Display Client Selector** again and hover over the **FTV_Studio Display Client** to activate it. **Tiling** is also available. This can be controlled within the **VersaView5200 Terminal Profile** or overridden through the **User Configuration Wizard**.
- Click the **Display Client Selector** once more and this time select **Main Menu**.
- From the **Main Menu**, click the **Log Off** button. **Ed** will be logged off, and the **FTV_Studio Display Client** will be removed.

There is an Inactivity Timeout setting available either at the User Group level or at the User object itself that will automatically logoff the Relevance User after a period of inactivity. The default is 120 seconds. It can be found on the last page of the User Configuration Wizard.

If Ed were to leave VersaView5200 and log into another Terminal (either thin client, PC or mobile device), his content would follow him. You can control what happens to a Disconnected session with the Session Collection in Windows Server 2012 or newer.

If you would prefer Ed to only receive content at a specific Terminal, you can use ThinManager Access Groups (introduced in [Section 10](#)) to apply permissions to specific Display Clients. Access Groups can be configured from the Manage ribbon. Once an Access Group is created, it can then be associated with a Relevance User Group. The same Access Group can then be applied as a Permission on the Display Client(s) that you want to restrict or provide access to. When you apply these restricted Display Clients to a Terminal, they will only become visible when a user assigned to that Access Group logs into the Terminal.

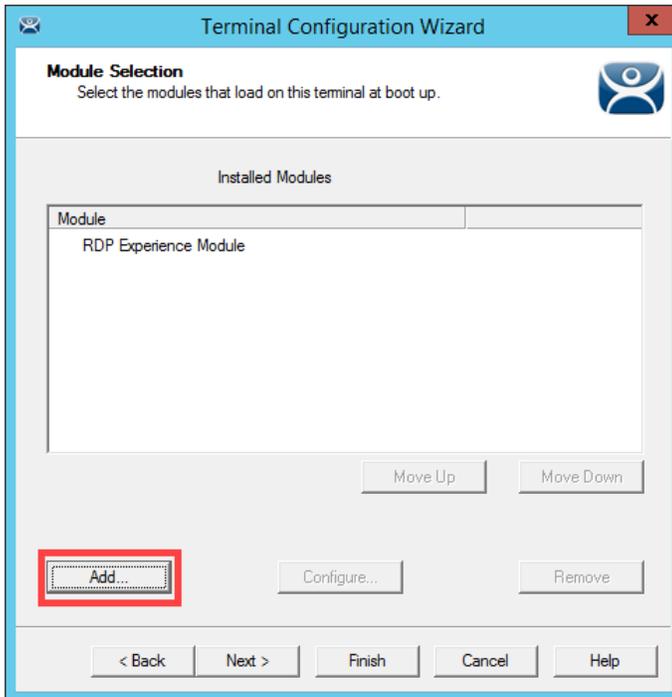
ThinManager ships with the TermMon ActiveX control that can be utilized by any ActiveX container, like FactoryTalk View SE. The ActiveX extends most of the ThinManager feature set to the ActiveX container, so you can then programmatically control many elements of ThinManager right from FactoryTalk View SE. As an example, you can trigger a Touchscreen Calibration to launch from a button within FactoryTalk View SE using the ActiveX control. You can also respond to ThinManager events from within FactoryTalk View SE. You can experience the TermMon ActiveX control in [Section 18](#). More details on the ActiveX control can be found at: http://www.thinmanager.com/kb/index.php/TermMon_ActiveX_Control

Add RF IDEas Badge Reader

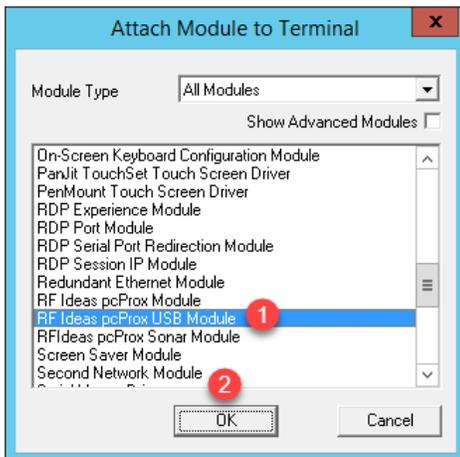
An RF IDEas Badge Reader could be connected to a physical thin client via USB. Since we are using a virtual thin client, we will be unable to test the results of this section, but will still go through the steps to add the module.

1. From the **Terminals** icon  in the ThinManager tree selector, double click the **VersaView5200** terminal profile.
2. Click the **Next** button on the **Terminal Name** page of the wizard.
3. Click the **Next** button on the **Terminal Hardware** page of the wizard.
4. Click the **Next** button on the **Terminal Options** page of the wizard.
5. Click the **Next** button on the **Terminal Mode Selection** page of the wizard.
6. Click the **Next** button on the **Display Client Selection** page of the wizard.
7. Click the **Next** button on the **Terminal Interface Options** page of the wizard.
8. Click the **Next** button on the **Hotkey Configuration** page of the wizard.
9. Click the **Next** button from the **Log In Information** page of the wizard.
10. Click the **Next** button from the **Video Resolution** page of the wizard.

11. From the **Module Selection** page of the wizard, click the **Add...** button.

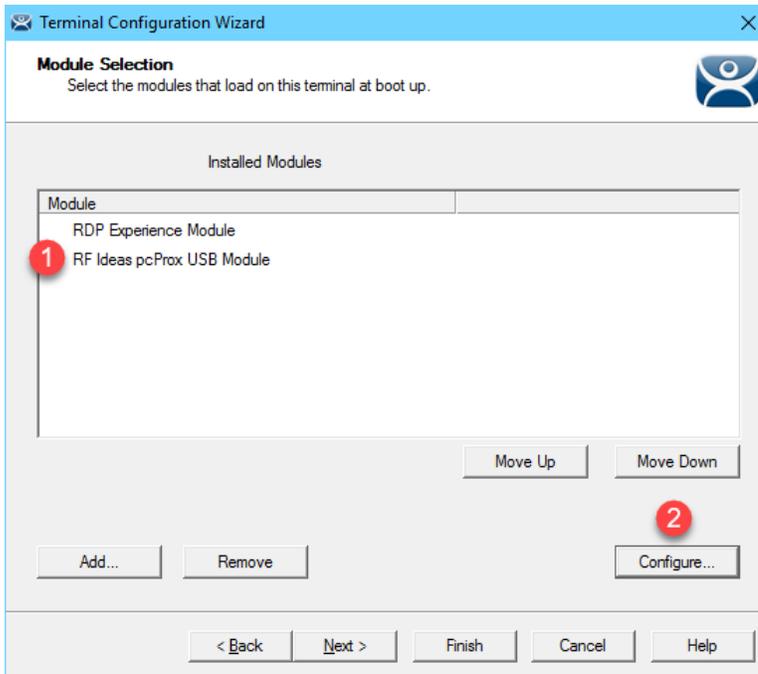


12. From **Attach Module to Terminal** dialog box, select the **RF Ideas pcProx USB Module** and click the **OK** button.

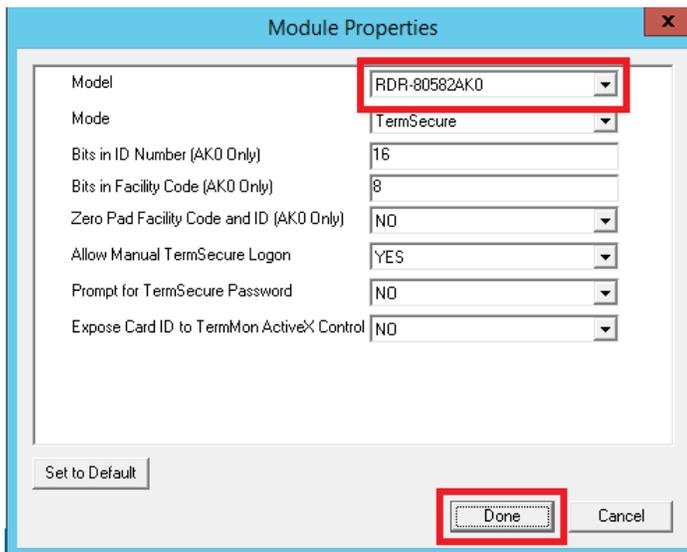


The release of ThinManager 11 includes the new USB ID Reader Module, which enables ThinManager to support generic Badge Reader modules that act as a keyboard emulator.

13. Select the **RF Ideas pcProx USB Module** from the Installed Modules list and click the **Configure** button.



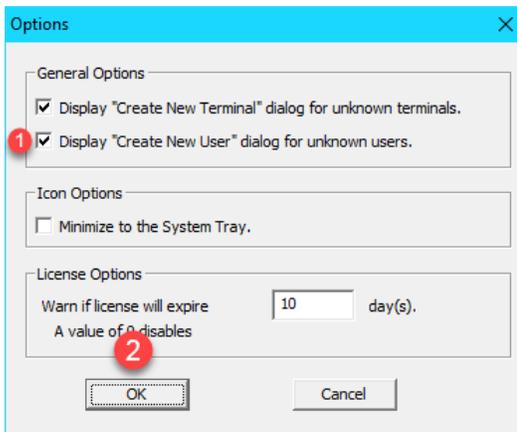
14. From the **Module Properties** dialog box, select **RDR-80582AK0** from the **Model** drop down list and click the **Done** button.



15. Back at the **Module Selection** page of the wizard, click the **Finish** button.
16. Right click **VersaView5200** and select **Restart Terminal** to apply the change.
17. We want ThinManager to prompt us to assign new badges to users. To enable this option, click the **View** ribbon, followed by the **Options** icon.

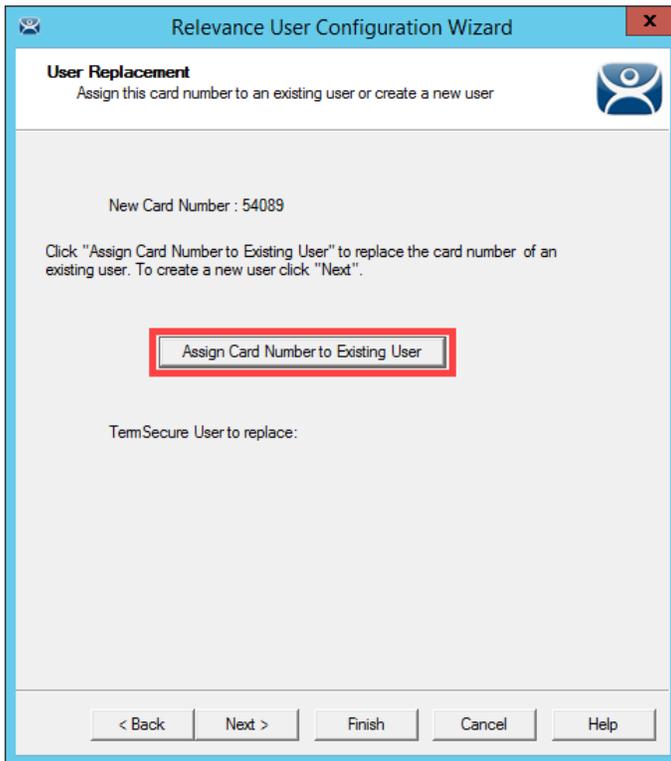


18. From the **Options** window, check the **Display "Create New User" dialog for unknown users** and click the **OK** button.



19. At this point, if you had a badge reader, you would take the **badge** and tap it on the RF IDEas badge reader.

20. If this was a new badge to ThinManager, you would be presented with the option to assign it to a user. **NOTE:** Since you do not have a badge reader in the Cloud lab, you will not see this window appear.



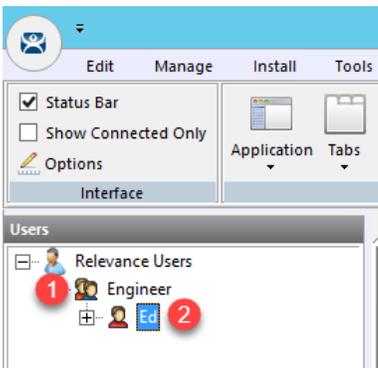
Configure ThinManager to Cache Password

In the next steps you will configure ThinManager to cache Ed's password, so he does not have to enter it for a configurable amount of time after initial login.

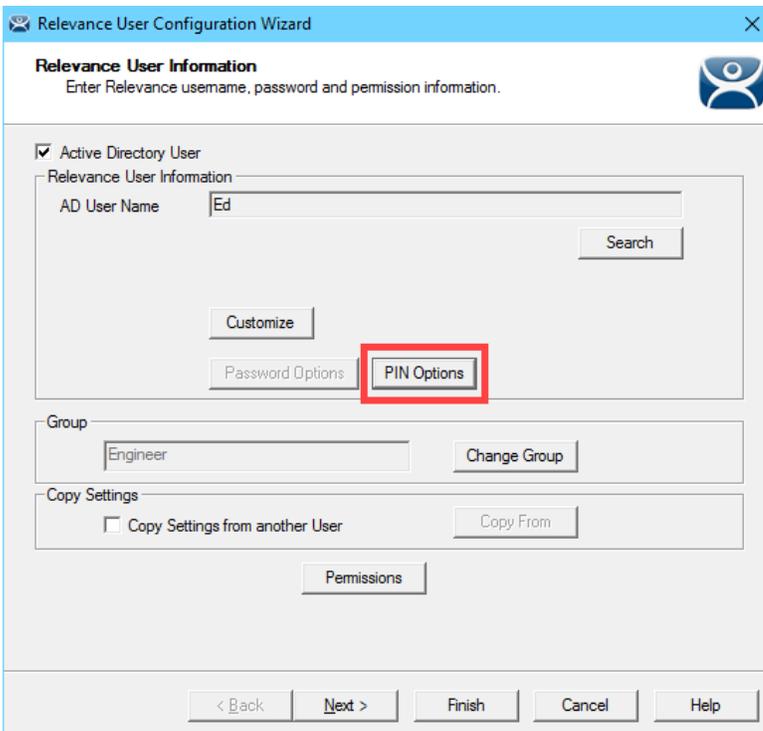
1. Click the **Users** icon  in the ThinManager tree selector.



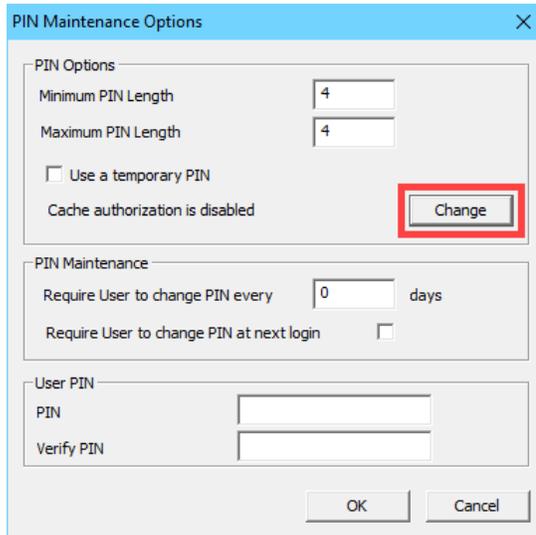
2. Expand the **Engineer** group and double click the icon for **Ed**.



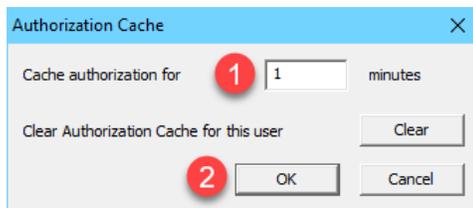
3. Click the **PIN Options** button on the **Relevance User Information** page of the wizard.



- From the **PIN Maintenance Options** popup, click the **Change** button next to **Cache authorization is disabled**.



- Enable password caching for 1 minute by entering a **1** in the input field next to the **Cache authorization for** item. Click **OK**.



- Click **OK** on the **PIN Maintenance Options** popup, followed by the **Finish** button.

As previously mentioned, you could also configure ThinManager to permanently store a user's password, so that they only provide a single factor (i.e.: badge, fingerprint scan) to authenticate. Furthermore, ThinManager can be configured to automatically rotate the password at a configurable interval to comply with password change policy.

- Return to the shadow of the **VersaView5200** terminal, hit CTRL-m on the keyboard to open the **Main Menu**.
- Click the **Log In** button.
- Enter **ed** as the **User Name** with a **Password** of **rw** as before to login as Ed.
- Hit CTRL-m on the keyboard to open the **Main Menu** again, and click the **Log Off** button.
- Once Ed has been logged off, hit CTRL-m on the keyboard one more time to return to the **Main Menu** and click the **Log In** button.
- This time you will notice that you only have to enter **ed** as the username since the password has been cached by ThinManager for 1 minute. Password caching is generally used with badging and/or fingerprint scanning. **Log Off** Ed.

Add Multifactor Authentication with a PIN and Password Storage

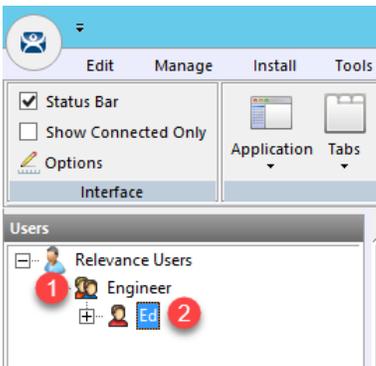
As part of ThinManager 10, a permanent or temporary PIN can be assigned to Relevance Users as an additional option for authenticating.

In the next steps you will configure ThinManager to store the Active Directory password for Ed so that a password will not be required, and instead you will assign a PIN to Ed's user account and require the PIN to authenticate.

1. Click the **Users** icon  in the ThinManager tree selector.



2. Expand the **Engineer** group and double click the icon for **Ed**.



- Click the **PIN Options** button on the **Relevance User Information** page of the wizard.

Relevance User Configuration Wizard

Relevance User Information
Enter Relevance username, password and permission information.

Active Directory User

Relevance User Information

AD User Name: Ed

Search

Customize

Password Options

PIN Options 1

Group: Engineer

Change Group

Copy Settings

Copy Settings from another User

Copy From

Permissions

< Back Next > Finish Cancel Help

- Click the **Change** button within the **PIN Options** frame.

PIN Maintenance Options

PIN Options

Minimum PIN Length: 4

Maximum PIN Length: 4

Use a temporary PIN

Cache authorization for 1 minute

Change

PIN Maintenance

Require User to change PIN every: 0 days

Require User to change PIN at next login:

User PIN

PIN: []

Verify PIN: []

OK Cancel

- Enter a **0** for the **Cache authorization for** textbox and click the **Clear** button next to the **Clear Authorization Cache for this user** to reset the cache. Confirm the **Clear User Authorization Cache** prompt and click **OK**.

Authorization Cache

Cache authorization for: 0 minutes

Clear Authorization Cache for this user:

Clear

OK Cancel

6. Enter 1234 in the **PIN** field within the **User PIN** frame and re-enter in the **Verify PIN** field. Click the **OK** button, followed by the **Next** button.

PIN Maintenance Options

PIN Options

Minimum PIN Length: 4

Maximum PIN Length: 4

Use a temporary PIN

Cache authorization is disabled Change

PIN Maintenance

Require User to change PIN every: 0 days

Require User to change PIN at next login:

User PIN

PIN: ****

Verify PIN: ****

OK Cancel

7. From the **Active Directory Password** page of the wizard, check the **Allow ThinManager to store password** checkbox, and enter *rw* as the password. Click the **Verify** button which should confirm that the credentials entered are valid. Click **Next**.

Relevance User Configuration Wizard

Active Directory Password
Password Maintenance Options

Active Directory Password

Allow ThinManager to store password

Password: rw Verify

Re-Sync Account

Password Maintenance

Allow ThinManager to rotate password

Use System Defaults

Minimum Password Length: 20

Maximum Password Length: 60

Rotate Password every: 0 days

Authorization Caching

Cache authorization is disabled Change

< Back **Next >** Finish Cancel Help

- On the **Card/Badge Information** page of the wizard, uncheck the **Prompt for Password** checkbox under the **Manual Login** frame, and check the **Prompt for PIN** checkbox. Click the **Finish** button.

Relevance User Configuration Wizard

Card / Badge Information
Enter card/badge information if user has one.

Card / Badge Login

This user will use a card or badge to log in

Enter Card/Badge ID number

Prompt for Password

Prompt for PIN

Biometric Login



Prompt for Password

Prompt for PIN

Manual Login

Prompt for Password

Prompt for PIN

- Return to the shadow of **VersaView5200** and hit CTRL-m again to open the **Main Menu**.
- Click the **Log In** button.
- Enter **ed** as the **User Name**.
- Using the keyboard, enter Ed's **PIN – 1234**, to complete the login process. As before, the **FTV_Studio Display Client** should be delivered.
- Once finished experimenting **Log Off** so that **Ed** is no longer logged in.

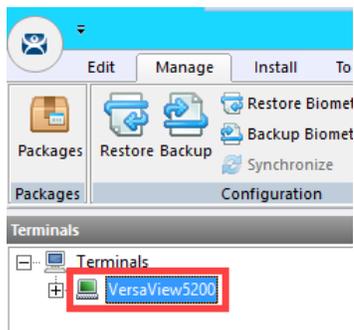
In the example above, we set a permanent PIN for Ed. We could have just as easily required a temporary PIN that Ed would create for himself at the terminal. We could also require him to change this PIN on a scheduled interval.

Authentication Pass Through

With ThinManager 10 and FactoryTalk View 10 or higher, a **Relevance User** login can be automatically passed into running sessions of FactoryTalk View SE. This is accomplished by seamlessly and securely passing a security token from ThinManager to those instances of FactoryTalk View SE being delivered to the ThinManager-managed terminal where the login occurred. There is no longer a need to hard-code passwords and/or write VBA code to pass login credentials from ThinManager to FactoryTalk View SE.

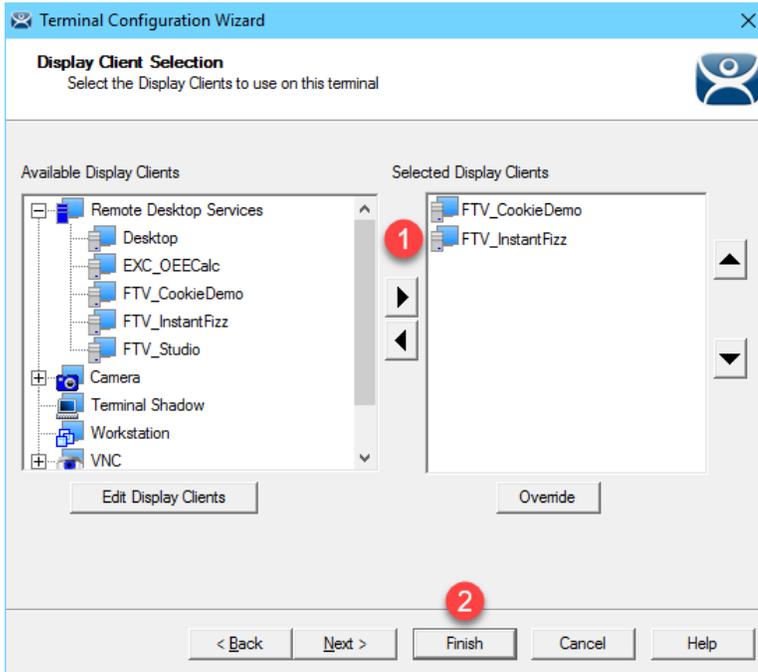
In the next steps you will configure ThinManager to deliver (2) separate FactoryTalk View SE Display Clients to the virtual thin client in tile mode. The **tmlab\thin01** user will automatically establish the two sessions, as this is the domain user that is assigned to the **VersaView5200** terminal profile. Next you will badge in with Ed's badge and see the results of the built-in Authentication Pass Through feature.

1. From the **Terminals** icon  in the ThinManager tree selector, double click the **VersaView5200** terminal profile.



2. Click the **Next** button on the **Terminal Name** page of the wizard.
3. Click the **Next** button on the **Terminal Hardware** page of the wizard.
4. Click the **Next** button on the **Terminal Options** page of the wizard.
5. Click the **Next** button on the **Terminal Mode Selection** page of the wizard.

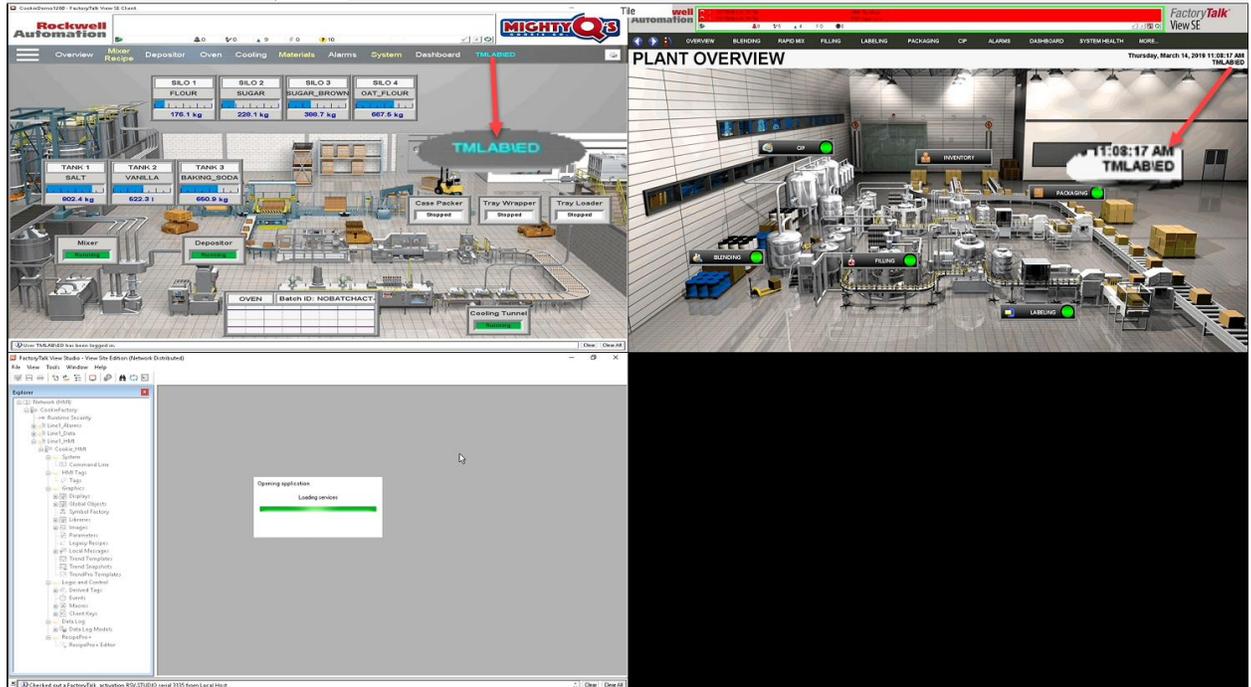
- From the **Display Client Selection** page of the wizard, select **FTV_InstanFizz** from the **Available Display Clients** list and click the **Right Arrow** button to move it to the **Selected Display Clients** list, click the **Finish** button.



- Right click the **VersaView5200** terminal from the **Terminals** tree and select **Restart Terminal** to apply the changes. Click **Yes** to the confirmation dialog.
- Shadow the **VersaView5200** terminal and confirm that user **tmlabthino1** is signed-in to both FactoryTalk View SE client sessions.



9. From the shadow, hit CTRL-m on the keyboard to open the **Main Menu**.
10. Click the **Log In** button.
11. Enter **ed** as the **User Name** and **1234** as the **PIN**. Verify that **tml1abled** user automatically logged into both **FactoryTalk View SE** display clients, and that the **FTV_Studio** client is delivered in tile mode.



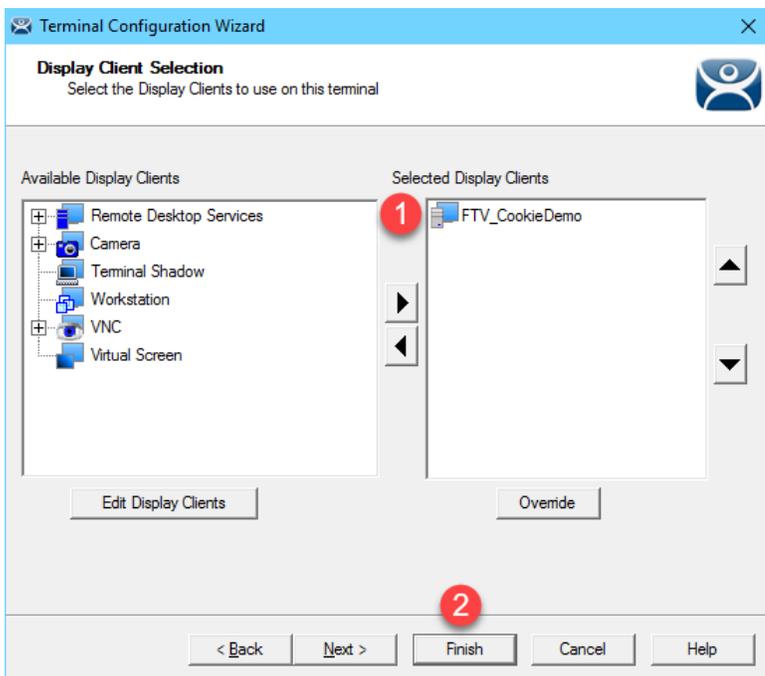
12. Hit CTRL-m on the keyboard again to open the **Main Menu**.
13. Click the **Log Off** button.
14. Verify that the **tmlab\thin01** user is logged back into the tiled FactoryTalk View SE display clients.

Remove Tiled Display Clients

1. Click the **Terminals** icon  from the ThinManager tree selector.



2. From the **Terminals** tree, double click the **VersaView5200** terminal to launch the **Terminal Configuration Wizard**.
3. Click the **Next** button on the **Terminal Name** page of the wizard.
4. Click the **Next** button on the **Terminal Hardware** page of the wizard.
5. Click the **Next** button on the **Terminal Options** page of the wizard.
6. Click the **Next** button on the **Terminal Mode Selection** page of the wizard.
7. Remove the **FTV_InstanFizz** Display Client from the **Selected Display Clients** list. The **FTV_CookieDemo** should be the only **Selected Display Client**. Click the **Finish** button.



8. Right click the **VersaView5200** terminal from the **Terminals** tree and select **Restart Terminal** to apply the changes. Click **Yes** to the confirmation dialog.

This completes the **User Based Content Delivery** section of the lab. Continue on to deliver location based content with Relevance Location Services.

Section 7: Relevance Location Services – Location Based Content Delivery

Overview

So far we have assigned and delivered content to a terminal, as well as content to a user. The next level of the content delivery model is **Location**. When talking about mobility on the plant floor, providing access anywhere to applications that control moving processes may cause more problems than solve. ThinManager **Relevance** provides the tools to safely provide access to these applications because you can define a **Location** and associate **Display Client(s)** with that **Location**. When a mobile device leaves a specified **Location**, the content associated with that **Location** will be no longer delivered to the mobile device. Different users may receive different content from the same **Location** based on their **Access Groups** in ThinManager.

So how does ThinManager determine a mobile device's location? By using **Location Resolver** technologies like:

1. Quick Response Codes (QR Codes)
2. Bluetooth Beacons
3. Wireless Access Points
4. Global Positioning Systems (GPS)

Relevance supports iOS, Android and Windows mobile devices. For iOS devices, ThinManager offers the iTMC application which is available through the App Store. For Android devices, ThinManager offers the aTMC application which is available through the Google Play Store. And for Windows tablets, ThinManager offers WinTMC, which is a Windows based application that essentially emulates a ThinManager terminal. In order to leverage all of the available Location Resolver technologies on a Windows Tablet, it is recommended that Windows 10 be utilized.

Location Resolvers can be easily registered through iTMC, aTMC or WinTMC. In this section you will register a QR Code to represent a location of a Logix PLC.

Once you have registered your **Location Resolvers**, you can then assign them to **Locations** created within ThinManager, and in turn, specific **Display Clients** can be associated with that **Location**.

As an example, let's say we would like to apply laminated QR Codes to all of our process automation assets, so that our Maintenance staff could walk up to an instrument with their mobile device, scan a QR Code, and instantly receive a series of documents and/or applications that are assigned to that instrument. To do so, we would first need to register each QR Code from the mobile device (using a ThinManager client application). Within ThinManager, we would create the **Display Clients** necessary for the desired documentation. This might include a series of **Display Clients** for Adobe Reader that open specific user manuals and/or standard operating procedures located on a file share. With the **Display Clients** created, we would then create a new **Location** in ThinManager, assign the **Display Clients** to it, and then associate the new QR Code **Resolver** to the **Location**.

We can also assign a default **Location** to a **Terminal**, which would enable a mobile device to interact with that **Terminal** in some very unique ways. Instead of applying **Display Clients** to a **Terminal** like we have throughout the lab so far, we would assign the **Display Client(s)** to the **Location** and then assign the **Location** to the **Terminal**. This extra level of indirection creates some very interesting possibilities. For instance, we could allow a user to scan a QR Code at the terminal that would actually **Transfer**, or redirect, the content from the terminal to the mobile device. We could also confine access to this content by applying a Bluetooth Beacon to “geo-fence” the user. When the user walks outside of the range established for the Bluetooth Beacon, the content would automatically be removed from the device, as it would be returned to the terminal. In this example, the **Transfer** is considered a **Resolver Action**. ThinManager **Relevance** supports 5 **Resolver Actions**:

1. Forced Transfer
2. Manual Transfer
3. Clone
4. View Only Shadow
5. Shadow

The **Forced Transfer** re-directs **Display Client(s)** from a terminal to a mobile device without requiring approval at the terminal. **Manual Transfer**, on the other hand, would require a user’s acknowledgement at the terminal to approve the **Transfer** request. **Clone** would spin up new, independent sessions of the **Display Clients** assigned to the terminal, while **View Only Shadow** and **Shadow** would do just what you would expect.

This lab section is composed of the following tasks:

1. Install iTMC on Your Mobile Device (iOS Users)
2. Install aTMC on Your Mobile Device (Android Users)
3. Create Terminal Shadow Display Client
4. Create Terminal Profile for Mobile Device
5. Assign Terminal Profile to Mobile Device
6. Create Public Display Server
7. Reassign Display Client to Public Display Server
8. Login as Engineer User
9. Create Logix Designer Display Client
10. Register QR Code Location Resolver from Mobile Device
11. Create Engineer Access Group
12. Create Relevance Location for Logix PLC
13. Resolve to Location from Mobile Device

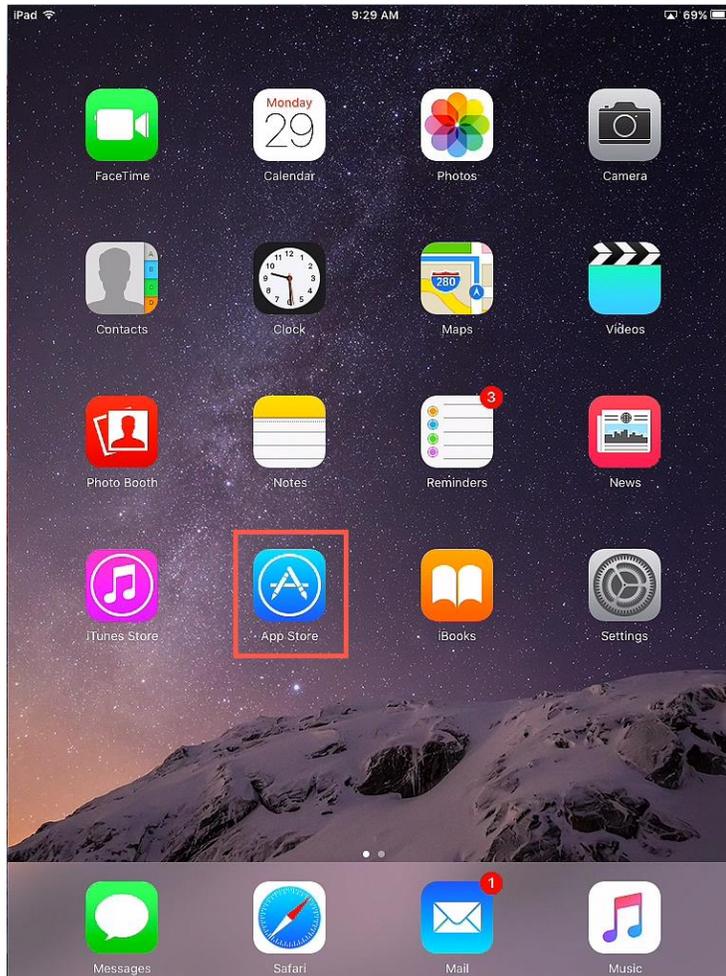
QR Codes are essentially more robust alphanumeric versions of barcodes. QR Codes can be generated and printed from several websites. Bluetooth Beacons are essentially proximity sensors for mobile devices. They offer a tunable signal strength, and hence range, from 0 to approximately 50 meters. ThinManager 8 introduced support for the iBeacon, which utilizes Apple's Bluetooth beacon protocol. There are numerous iBeacons available in various forms. Wireless Access Points expose a unique identifier called a BSSID which ThinManager can use to determine on which Access Point a mobile device is connected. GPS offers accurate location resolution down to 5 feet, but is only for outdoor applications.

Fencing (or geo-fencing) is defined as combining resolvers to limit access to specific Display Clients based on Location. For instance, a Bluetooth Beacon can be used to geo-fence in a QR Code so that a mobile device must be within range of the Bluetooth Beacon when they scan the QR Code to actually resolve to the associated Location and receive its content. Once the mobile device is outside the range of the Bluetooth Beacon, the Display Clients associated with the Location would not be delivered to the mobile device.

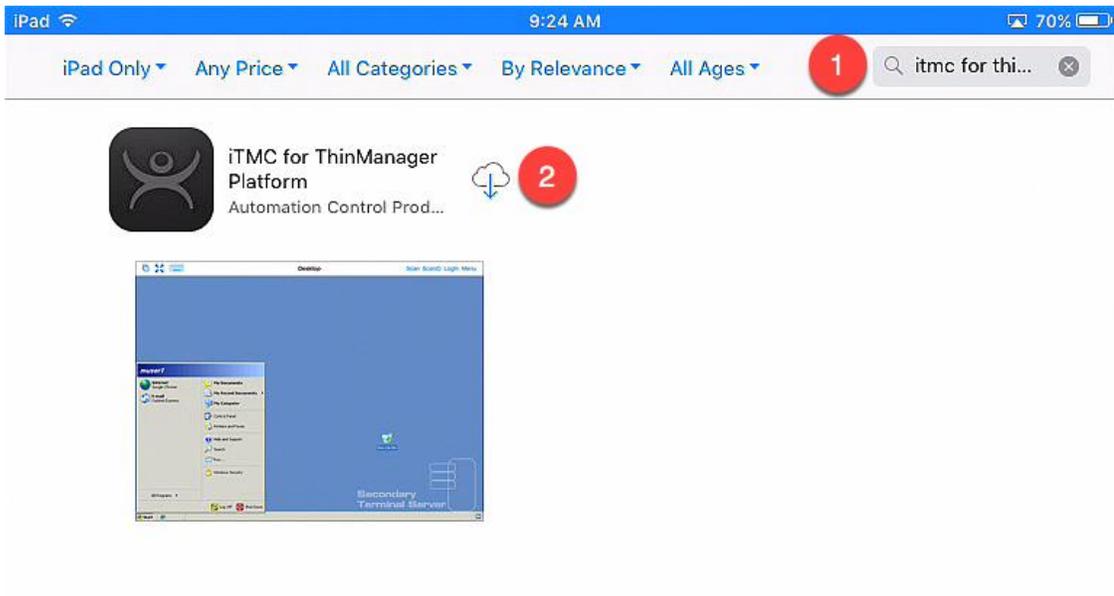
Install iTMC on Your Mobile Device (iOS Users)

If you will be using an iOS mobile device, you will need to install iTMC in order to complete the mobility portions of this lab. If you have an Android mobile device, you may skip onto the next section.

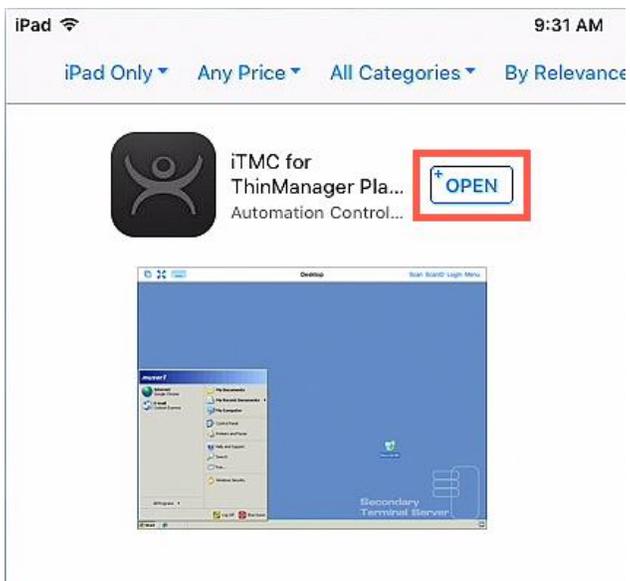
1. Launch the App Store from your iOS device.



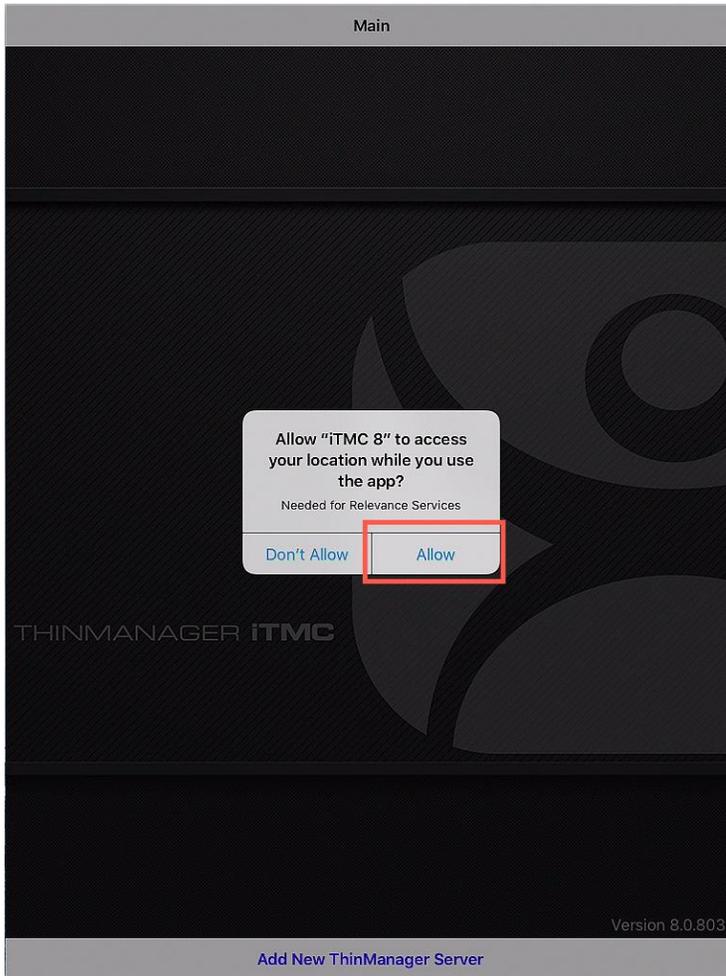
2. In the **Search** field, enter *iTMC for ThinManager Platform*. Touch the **Download** icon.



3. Once the download is complete, touch the **OPEN** button.

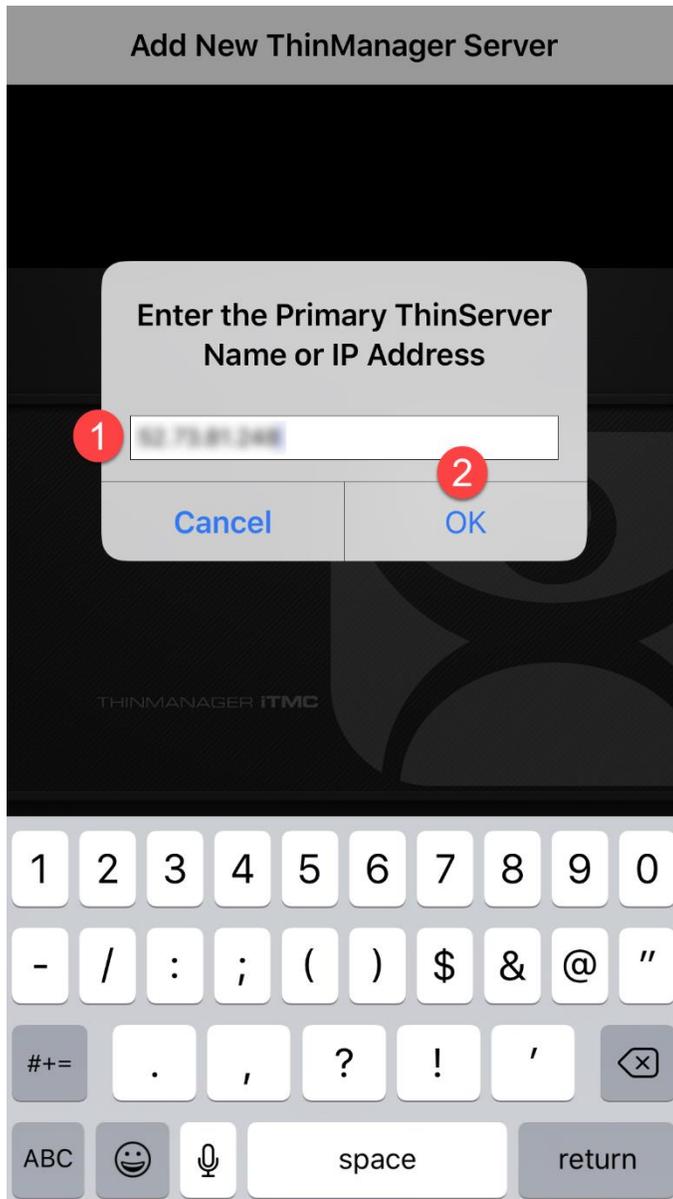


4. Launch iTMC. If it requests to access to your location while using the app, touch the **Allow** button.



iOS treats Bluetooth beacons as Location Services devices, so if you intend to use beacons with an iOS device, you will need to enable Location Services for iTMC.

5. Enter the **public IP address** of your **RDS1** server and touch the **OK** button.



6. Enter a **Description** for this connection and touch the **Save** button.

[Cancel](#) **Add ThinManager Server** [Save](#)

DESCRIPTION 2

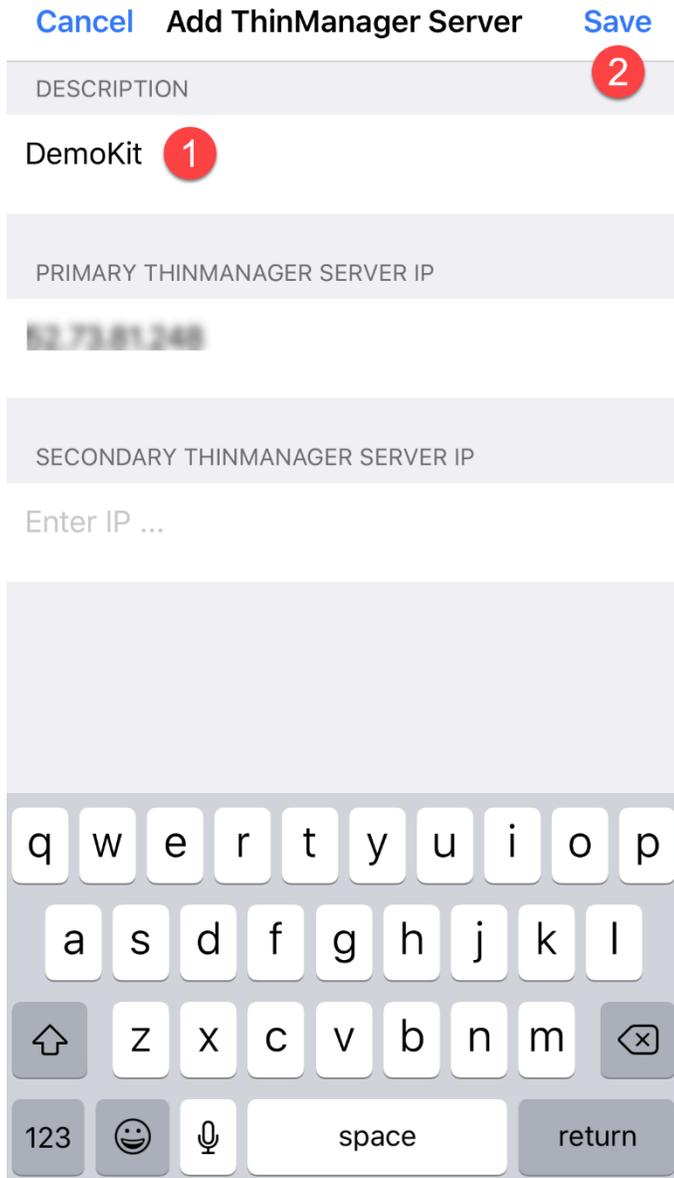
DemoKit 1

PRIMARY THINMANAGER SERVER IP

12.73.81.248

SECONDARY THINMANAGER SERVER IP

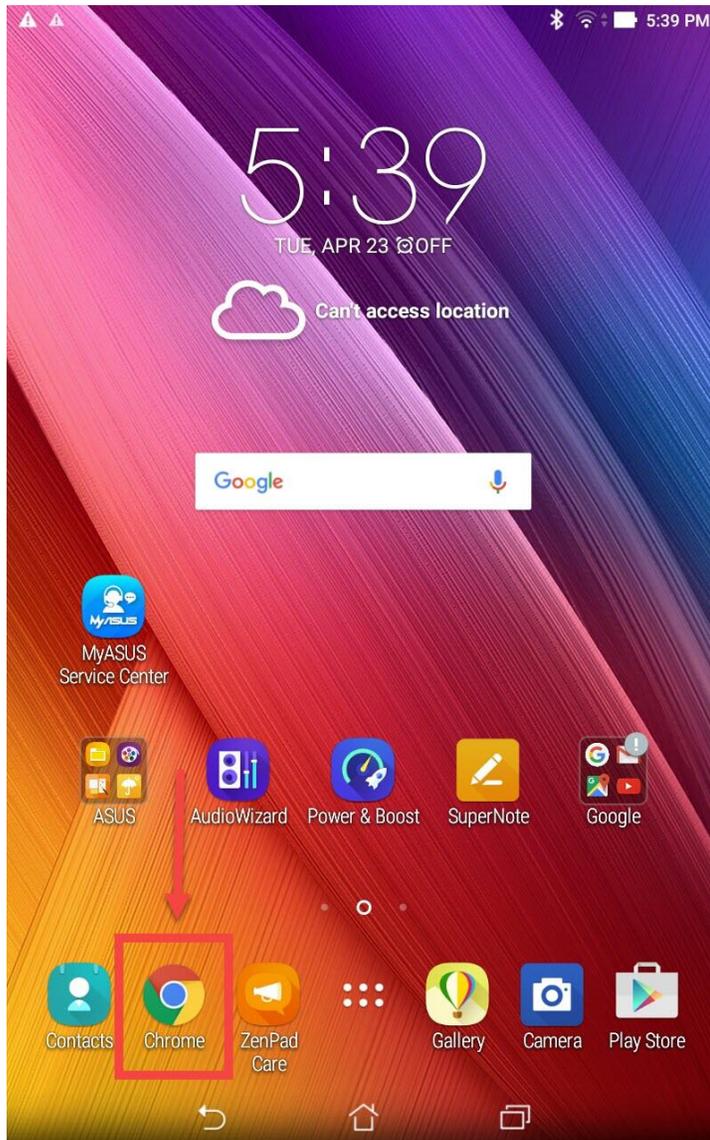
Enter IP ...



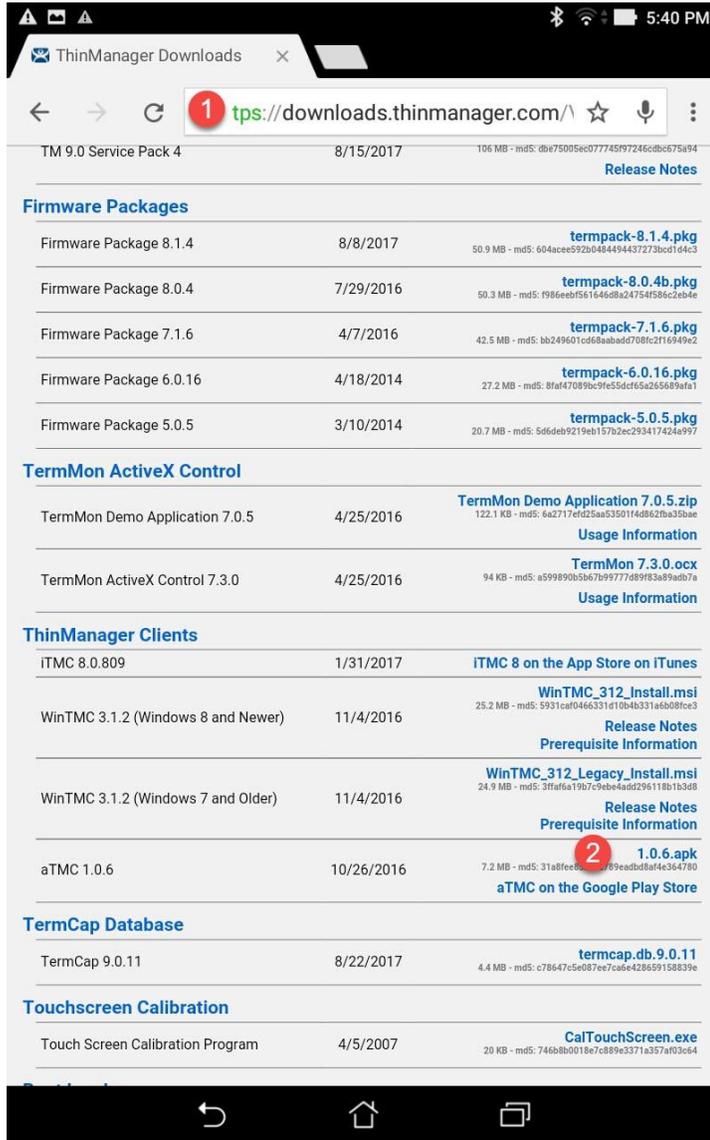
Install aTMC on Your Mobile Device (Android Users)

If you will be using an Android mobile device, you will need to install aTMC in order to complete the mobility portions of this lab.

1. Ensure your mobile device has an Internet connection and open Chrome.

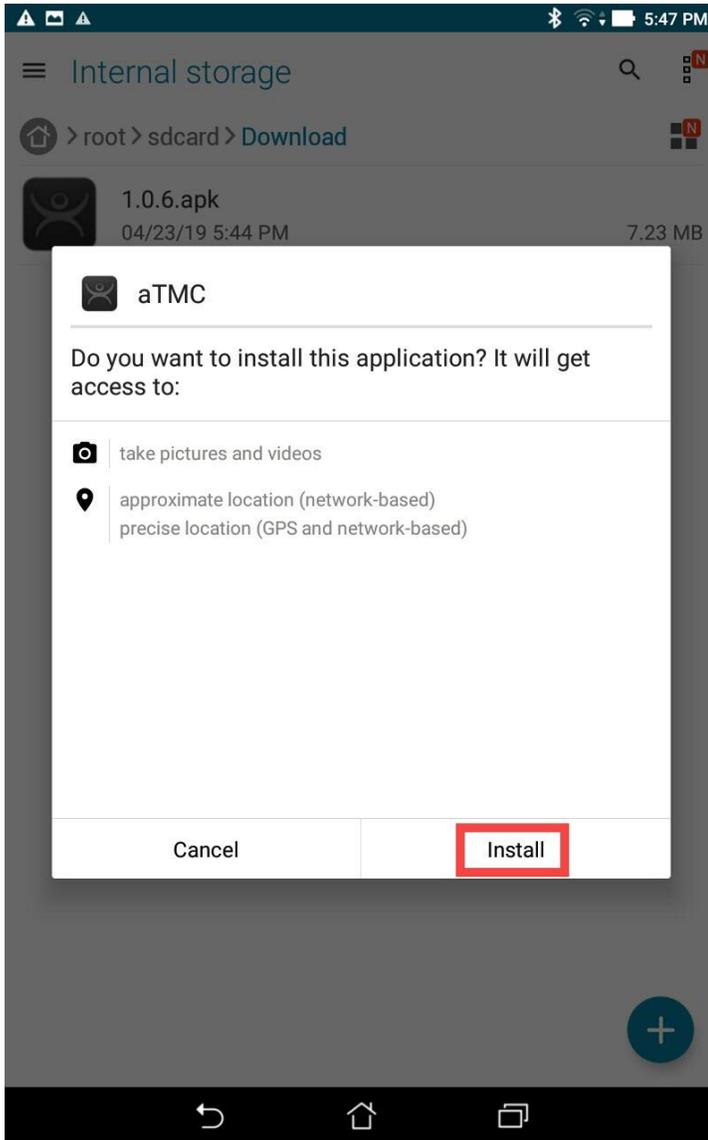


- From **Chrome**, enter the following **URL**: *downloads.thinmanager.com*. Touch on the **aTMC** download link (1.0.6.apk in the screen shot below, but you may see a newer version which is ok).

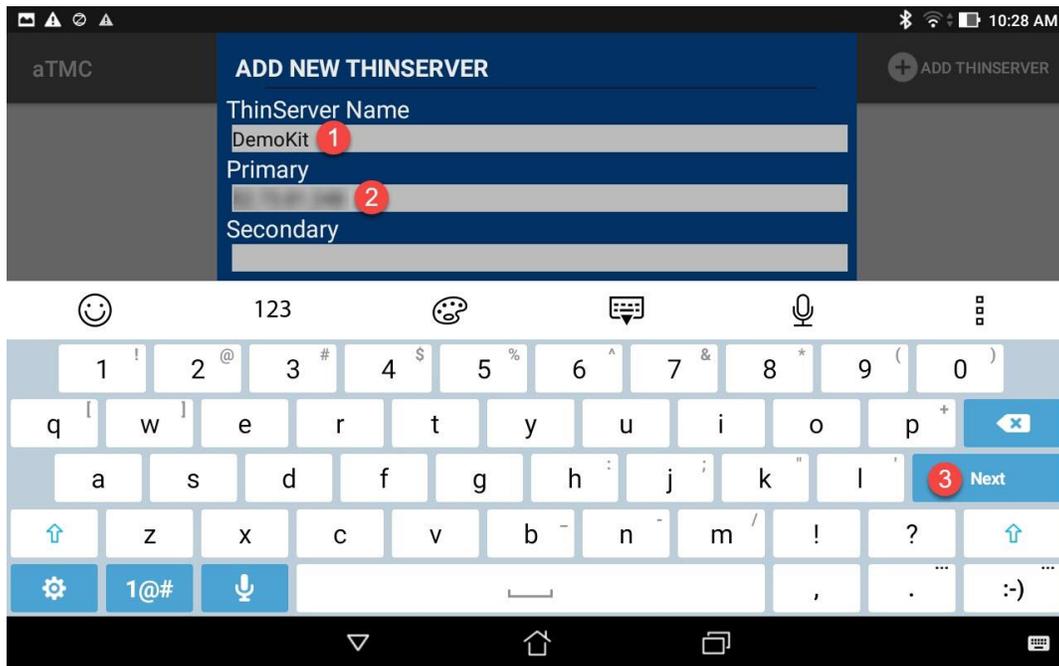


aTMC can also be downloaded from the Google Play Store.

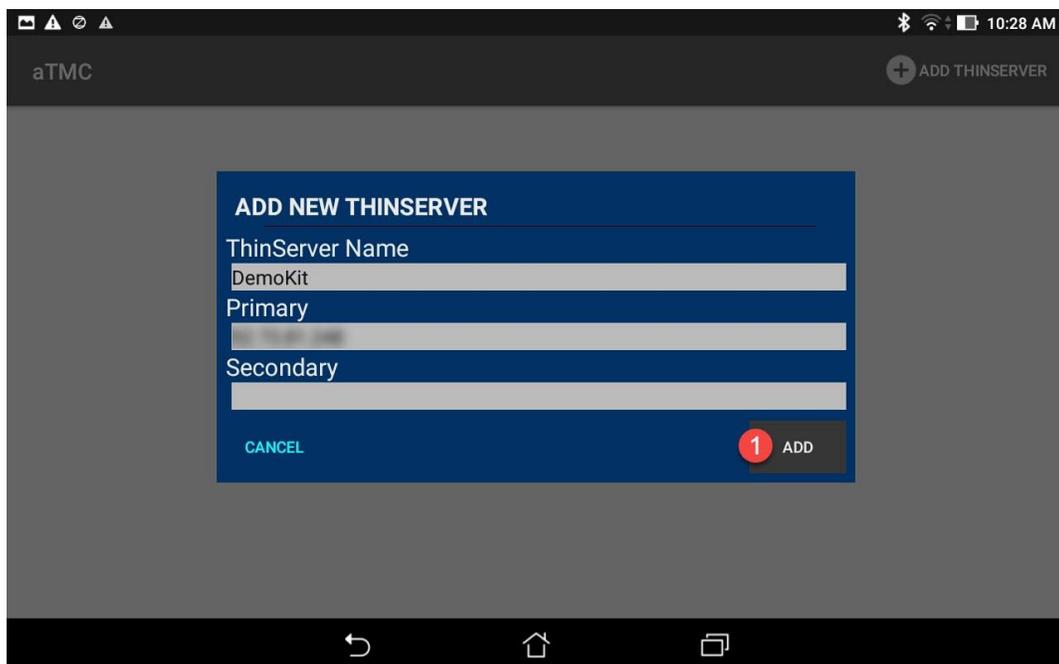
3. Once **aTMC** is downloaded, install it.



- Once **aTMC** is installed, launch it. Give this connection a **ThinServer Name** (DemoKit in the screen shot below), and then enter the **public IP address** of your assigned **Cloud** server. You can find the **Public IP Address** of your **RDS1** server on the **Desktop Wallpaper of RDS1** in the top right corner. Touch the **Next** button.

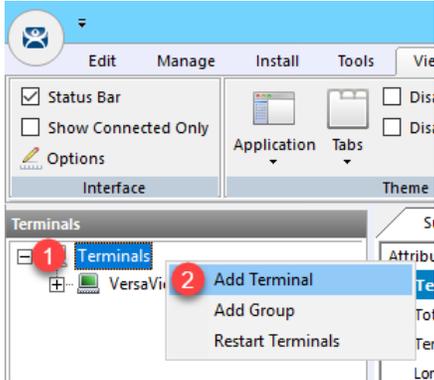


- Click the **Add** button.

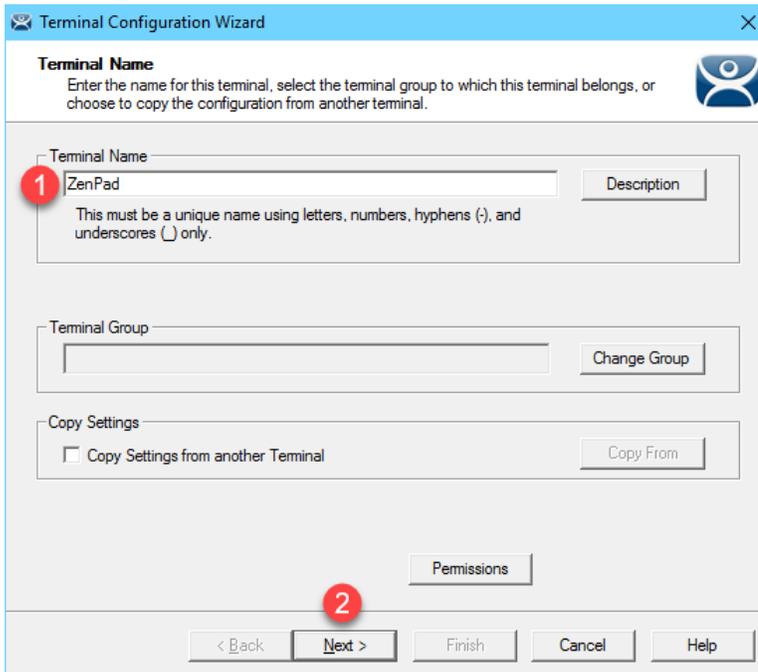


Create Terminal Profile for Mobile Device

1. Click the **Terminals** icon  from the ThinManager tree selector.
2. From the **Terminals** tree, right click the **Terminals** node and select **Add Terminal**. This will launch the **Terminal Configuration Wizard**.



3. Type *ZenPad* as the **Terminal Name** on the **Terminal Name** page of the wizard. Click the **Next** button.



4. Select **Generic** from the **Make/OEM** drop down list and **Android Device** from the **Model** drop down list. Click the **Next** button.

Terminal Configuration Wizard

Terminal Hardware
Select the manufacturer and model of this terminal.

Use this to configure the type of hardware for this terminal.

Make / OEM 1 GENERIC

Model 2 Android Device

OEM Model Android

Video Chipset UNKNOWN

Terminal Firmware Package Model Default

Terminal will run Package 8.2

Terminal ID and IP Address

Terminal ID None

Clear

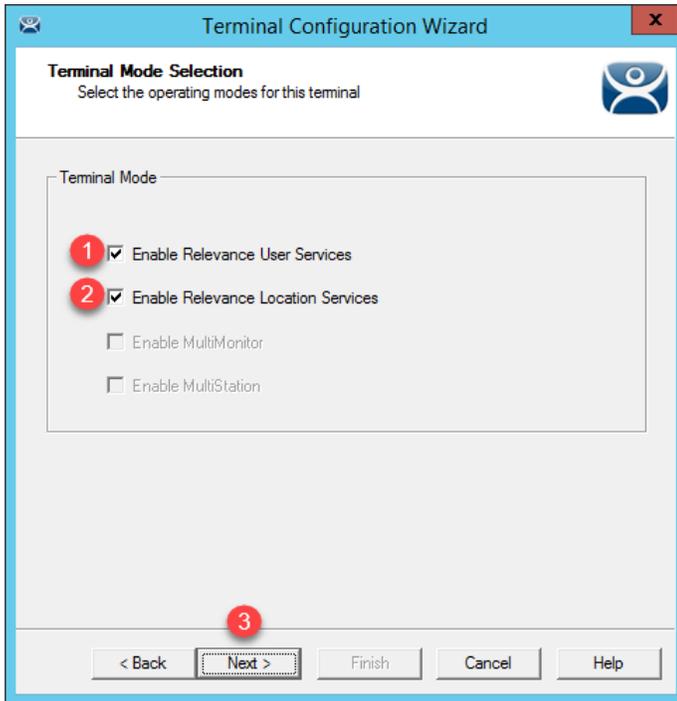
Edit

3

< Back Next > Finish Cancel Help

If you are using an iOS device in the lab, you would select **Apple** as the **Make / OEM** and **iOS Device** as the **Model**.

5. Click the **Next** button on the **Terminal Options** page of the wizard.
6. Check the **Use Display Clients**, **Enable Relevance User Services**, and **Enable Relevance Location Services** checkboxes on the **Terminal Mode Selection** page of the wizard. Click the **Next** button.



7. Click the **Next** button from the **Display Client Selection** page of the wizard.
8. Click the **Next** button on the **Terminal Interface Options** page of the wizard.
9. Check the **Enable QR Code Location Ids** and **Enable Bluetooth Locations** checkboxes from the **Relevance Options** page of the wizard. Click the **Next** button.

Terminal Configuration Wizard

Relevance Options
Select the types of Relevance Resolvers to use on this client. Optionally choose an assigned location for this client

Assigned Location

Options

Enabled Resolver Types

- Enable QR Code Location Ids
- Enable Bluetooth Locations
- Enable GPS Locations
- Enable Wi-Fi Locations

Use Force Transfer to restore Assigned Location

Allow selection of Location manually

Enforce fencing on manual Location selection

Confirm before entering a location

Resolver Update Interval ms

< Back Finish Cancel Help

10. From the **Log In Information** page of the wizard, enter *tab01@tmlab.loc* as the **Username** and *rw* as the **Password**. Click the **Verify** button to validate these credentials, and then click the **Next** button.

The screenshot shows the 'Terminal Configuration Wizard' window with the 'Log In Information' tab selected. The window title is 'Terminal Configuration Wizard'. Below the title bar, there is a sub-header 'Log In Information' and a brief instruction: 'Enter the log in information to log in automatically. Leave the log in information blank or fill only some of the fields to force manual log in.' The main area contains a 'Windows Log In Information' section with three input fields: 'Username' (containing 'tab01@tmlab.loc'), 'Password' (containing 'rw'), and 'Domain' (empty). There are 'Search', 'Password Options', and 'Verify' buttons. At the bottom, there are navigation buttons: '< Back', 'Next >', 'Finish', 'Cancel', and 'Help'. Red circles with numbers 1, 2, 3, and 4 highlight the Username field, Password field, Verify button, and Next button respectively.

11. From the **Video Resolution** screen of the wizard, select **1280x800** as the **Resolution**, and keep other default settings. Click the **Finish** button.

The screenshot shows the 'Terminal Configuration Wizard' window with the 'Video Resolution' tab selected. The window title is 'Terminal Configuration Wizard'. Below the title bar, there is a sub-header 'Video Resolution' and an instruction: 'Select the video resolution for this terminal.' The main area contains a 'Select Video Resolution' section with a message: 'These are the resolutions supported by the Thin Client model you selected.' Below this, there are three dropdown menus: 'Resolution' (set to '1280x800'), 'Color Depth' (set to '64K Colors'), and 'Refresh Rate' (set to '0Hz'). At the bottom, there are navigation buttons: '< Back', 'Next >', 'Finish', 'Cancel', and 'Help'. Red circles with numbers 1 and 2 highlight the Resolution dropdown and the Finish button respectively.

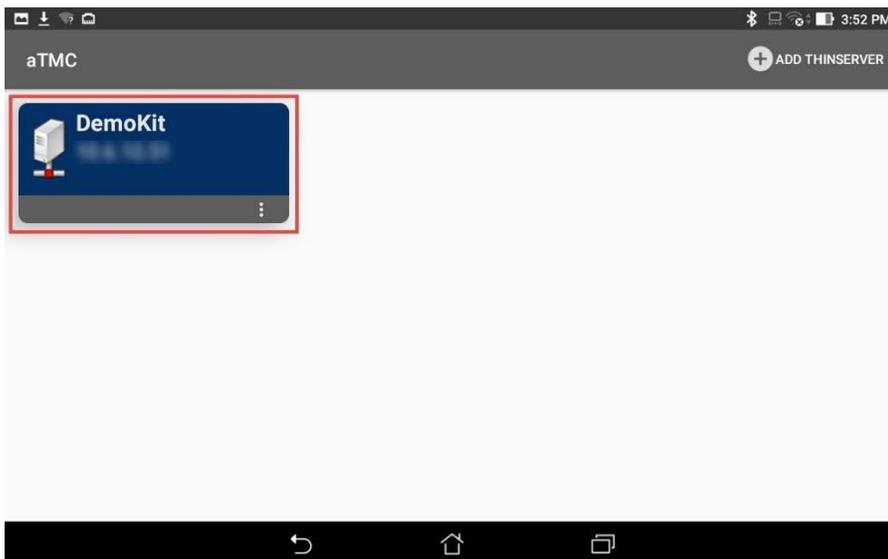
Assign Terminal Profile to Mobile Device

Unlike a thin client like the **VersaView 5200**, we are not going to deliver ThinManager firmware to a tablet, which already has its own OS. Instead, we will use the **aTMC** app to essentially emulate a ThinManager thin client.

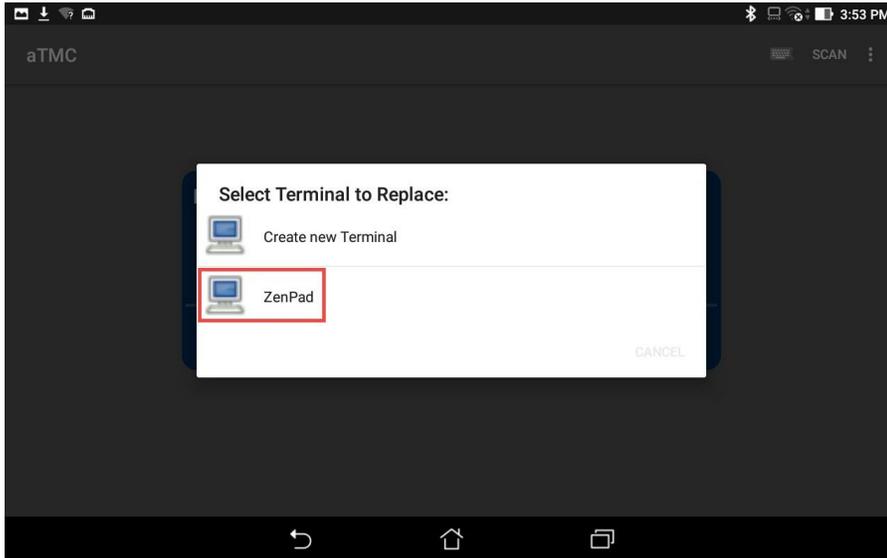
1. Launch **aTMC** from your mobile device.



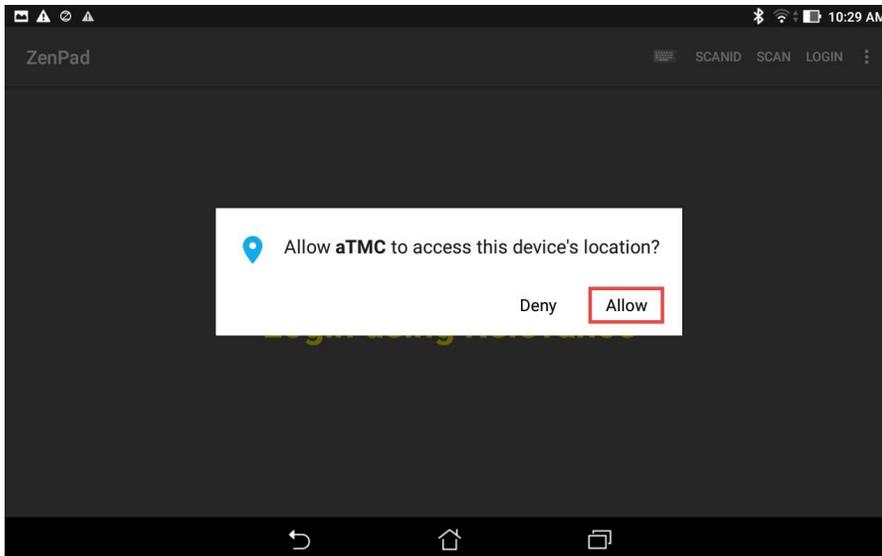
2. Touch the **DemoKit ThinServer** to connect to it.



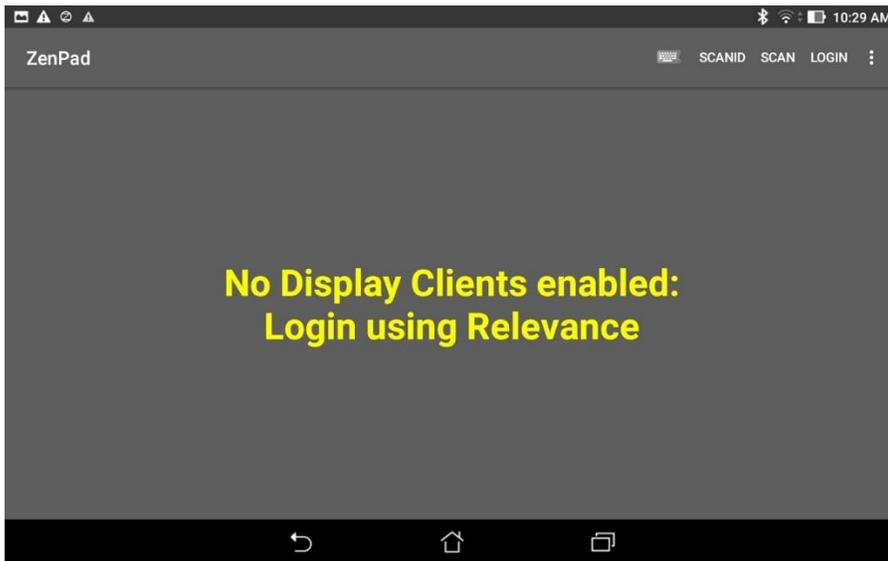
3. Since we have not assigned a **Terminal Profile** to the **ZenPad** yet, **aTMC** will prompt us to assign one of the available profiles to it. Touch the **ZenPad** profile that we created in the previous steps.



4. If you receive a prompt to allow **aTMC** access to the device's location, touch the **Allow** button.



5. The **ZenPad Terminal Profile** will be delivered to the tablet. Since we did not assign any **Display Clients** to the terminal profile, we will receive a blank screen.



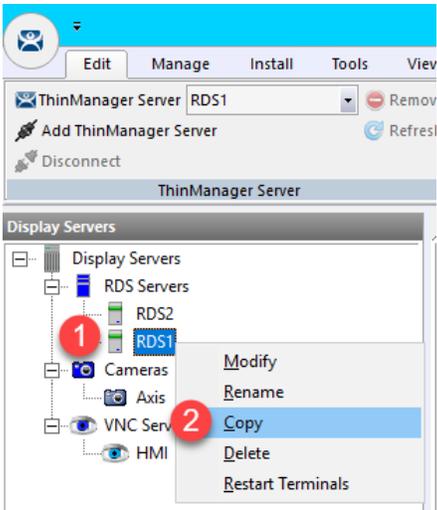
Create Public Display Server

The Display Servers we created earlier in the lab utilized private IP addresses (10.6.10.51 for RDS1 and 10.6.10.52 for RDS2), which will not be reachable from your remote tablet. Therefore, we will create an additional Display Server that utilizes the public IP address of RDS1 so your tablet can connect to it. This method is fine for testing and lab purposes, but if you need remote access to your Remote Desktop Servers, a Virtual Private Network (VPN) or Remote Desktop Gateway is recommended.

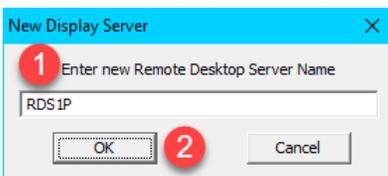
1. Click the **Display Servers** icon  in the ThinManager tree selector.
The tree selector can be expanded or collapsed using the bar above directly above it.



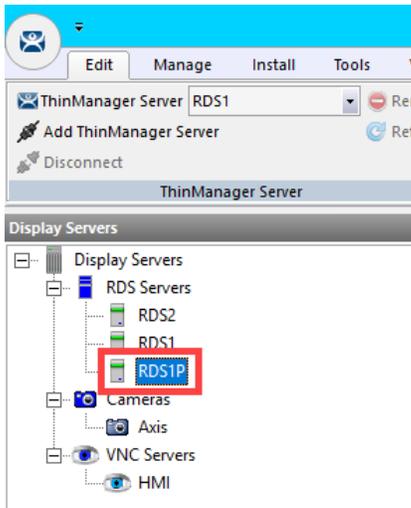
2. From the **Display Servers** tree, expand the **RDS Servers** branch, right click **RDS1** and click **Copy**.



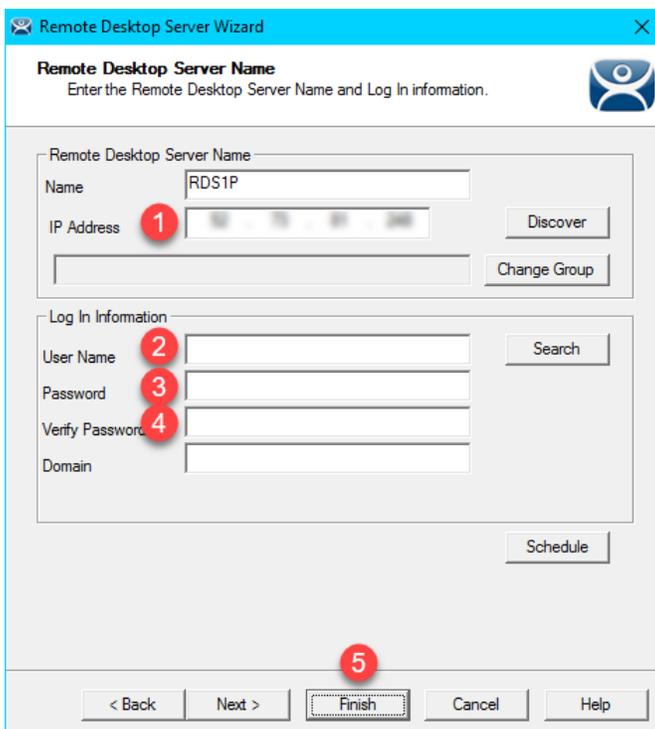
3. From the **New Display Server** input box, enter *RDS1P* and click the **OK** button.



4. Double click the newly created **Display Server RDS1P**.



5. From the **Introduction** page of the wizard, click the **Next** button.
6. From the **Remote Desktop Server Name** page of the wizard, change the IP address from 10.6.10.51 to the **public IP** address of your **RDS1** image. In addition, delete the **User Name**, **Password** and **Verify Password** entries. Click the **Finish** button.



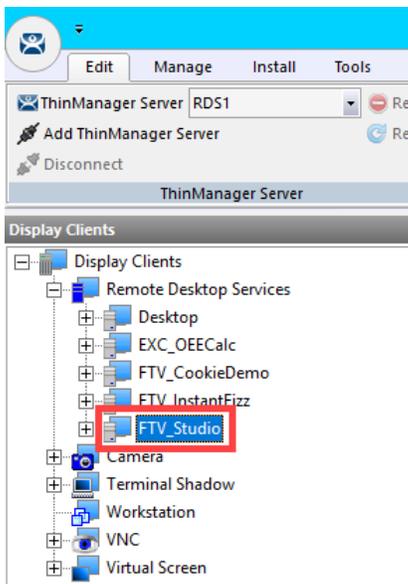
Reassign Display Client to Public Display Server

When we created the **FTV_Studio Display Client** in the previous section, we assigned the **RDS1 Display Server** to it, which has a private IP address of 10.6.10.51. This IP address will not be reachable by your remote tablet, so we will temporarily reassign it to **RDS1P**.

1. From ThinManager, click the **Display Clients** icon  from the ThinManager tree selector.

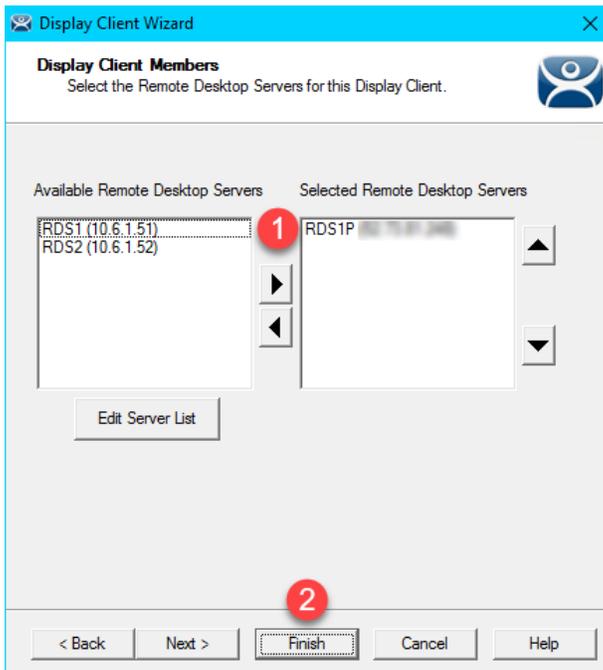


2. From the **Display Clients** tree, expand the **Remote Desktop Services** branch and double click the **FTV_Studio Display Client**.



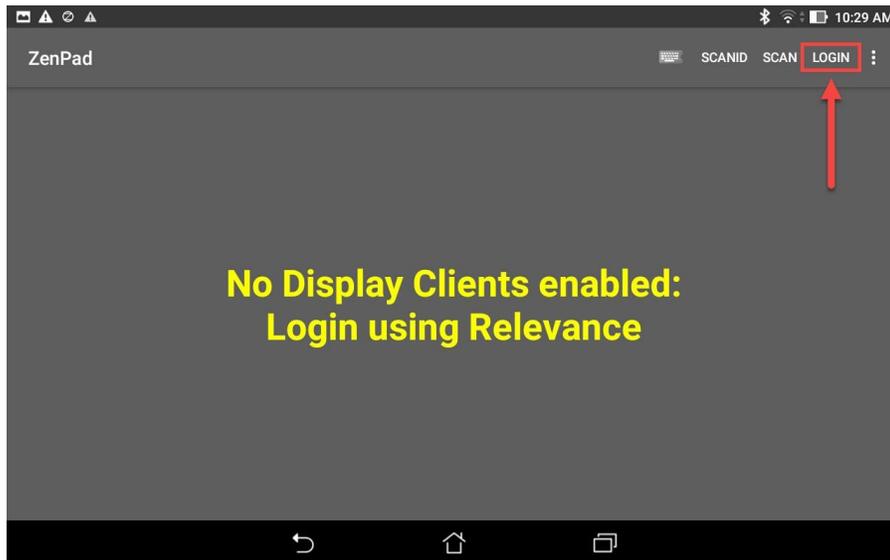
3. Click the **Next** button from the **Client Name** page of the wizard.
4. Click the **Next** button from the **Display Client Options** page of the wizard.
5. Click the **Next** button from the **Remote Desktop Services and Workstation Options** page of the wizard.
6. Click the **Next** button from the **Session Resolution / Scaling Options** page of the wizard.

- From the **Display Client Members** page of the wizard, remove **RDS2** from the **Selected Remote Desktop Servers** list box and add **RDS1P** instead. Click the **Finish** button.

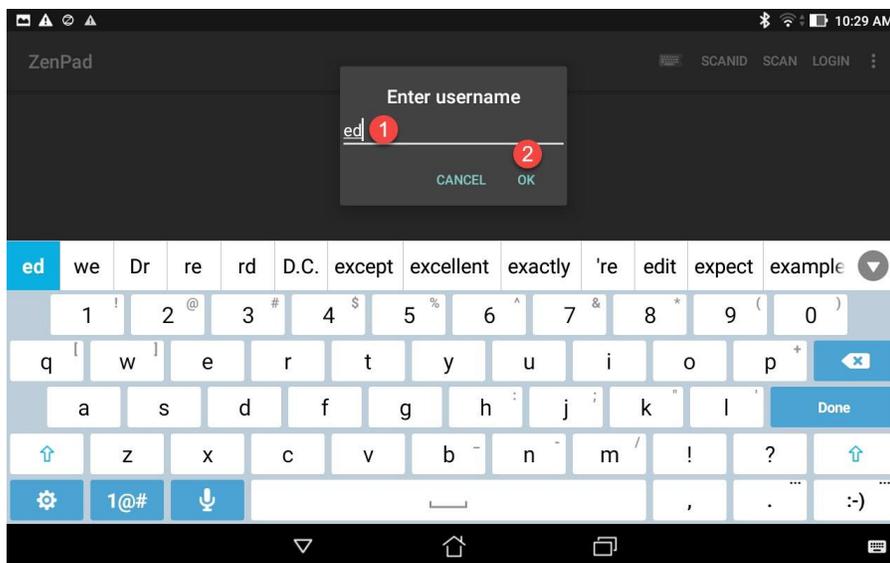


Login as Engineer User

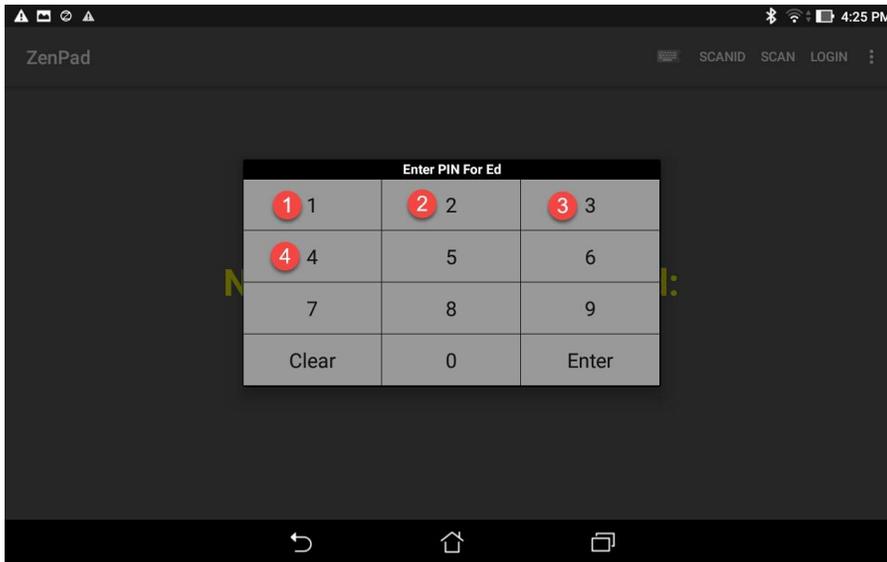
1. From the aTMC application, touch the **LOGIN** button in the top right corner.



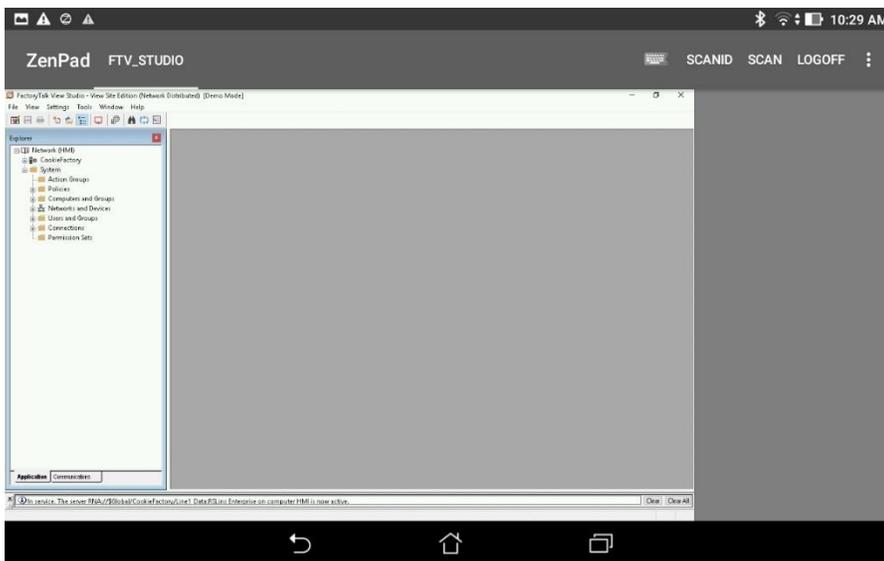
2. Enter **ed** as the **username** and touch the **Ok** button.



3. Enter 1234 as the PIN.



4. Upon successful authentication, you should receive the **FTV_Studio Display Client**. This is the same session that was delivered to the virtual thin client in the previous section. In fact, it is configured to just pick up right where Ed left off.



5. If you perform a 3 finger hold down, **aTMC** will go **Full Screen**, and the **FTV_Studio** session should scale perfectly to the ZenPad display.

Other tablet gestures are supported as well. Pinch and zoom works as expected. Once zoomed in, you can pan around the screen using two fingers on the tablet. You can also perform a 2 finger hold down, which will toggle the on screen keyboard.

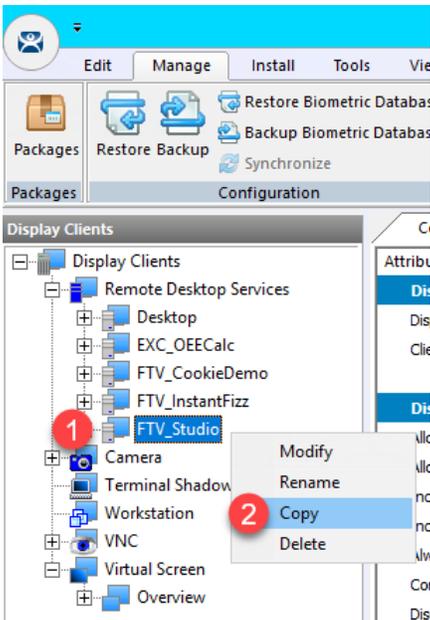
Create Logix Designer Display Client

In these last sections of the lab, we are going to set ThinManager up to deliver **Logix Designer** to the **ZenPad** just by simply scanning a QR Code. The first step is to create the **Display Client** for **Logix Designer**.

1. From ThinManager, click the **Display Clients** icon  from the ThinManager tree selector.



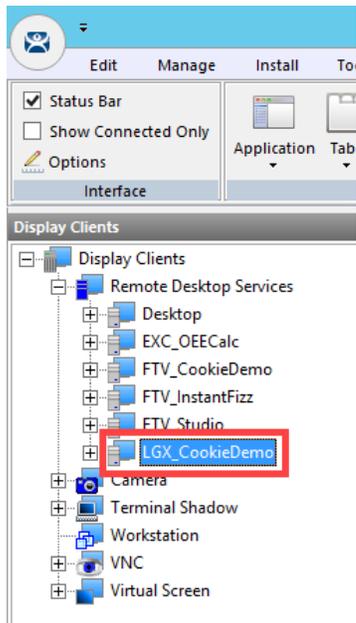
2. From the **Display Clients** tree, expand the **Remote Desktop Services** branch and right click the **FTV_Studio** item and select **Copy**.



3. Type **LGX_CookieDemo** in the **Enter new Display Client Name** text box and click the **OK** button.



4. Double click the new **LGX_CookieDemo** Display Client item.



5. From the **Client Name** page of the wizard, click the **Next** button.
6. From the **Display Client Options** page of the wizard, click the **Next** button.
7. From the **Remote Desktop Services and Workstation Options** page of the wizard, click the **Next** button.
8. From the **Screen Resolution / Scaling Options** page of the wizard, click the **Next** button.
9. From the **Display Client Members** page of the wizard, click the **Next** button.

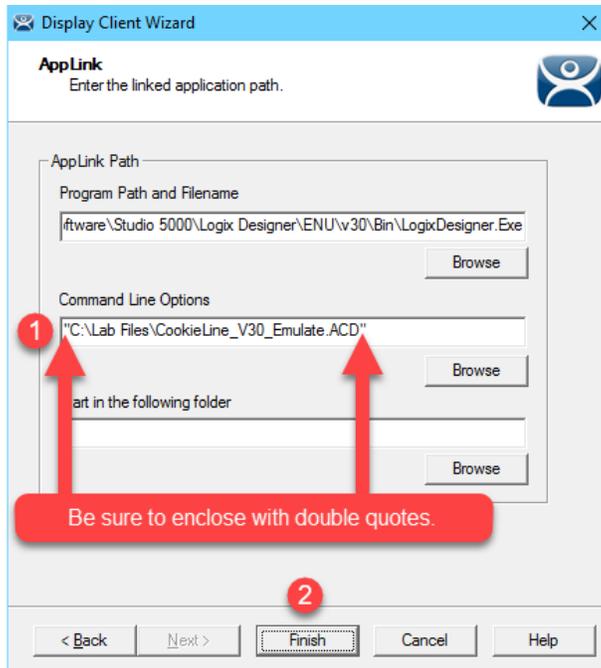
- From the **AppLink** page of the wizard, replace the **Program Path and Filename** and the **Command Line Options** paths with the ones below (you can also copy and paste this path from the **LabPaths.txt** file by right clicking the **Notepad** icon pinned to the start bar and selecting **LabPaths.txt**):

Program Path and Filename:

C:\Program Files (x86)\Rockwell Software\Studio 5000\Logix Designer\ENU\v30\Bin\LogixDesigner.Exe

Command Line Options:

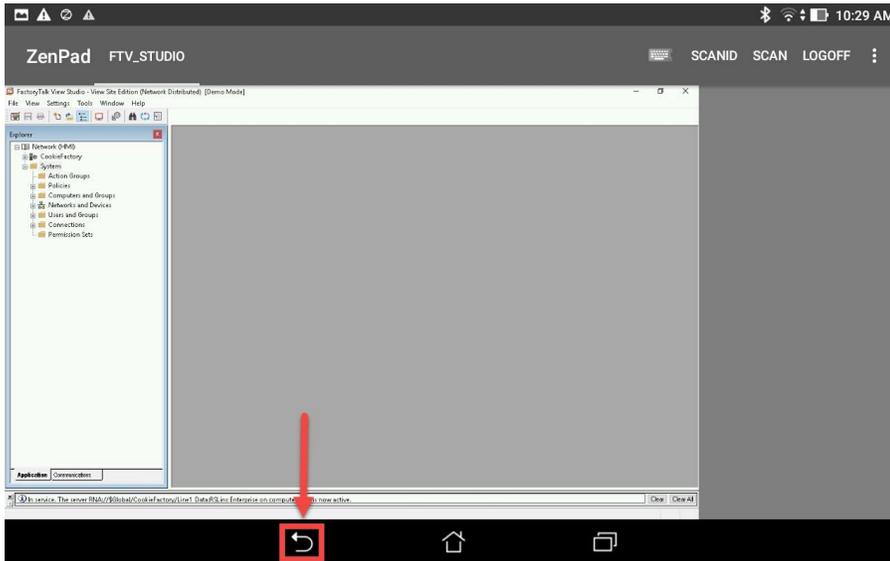
"C:\Lab Files\CookieLine_V30_Emulate.ACD"



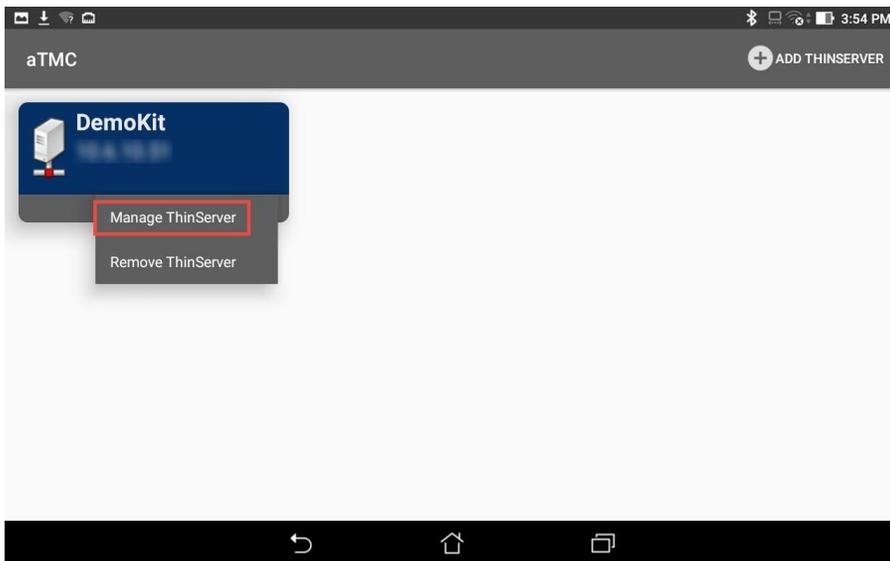
- Click the **Finish** button.

Register QR Code Location Resolver from Mobile Device

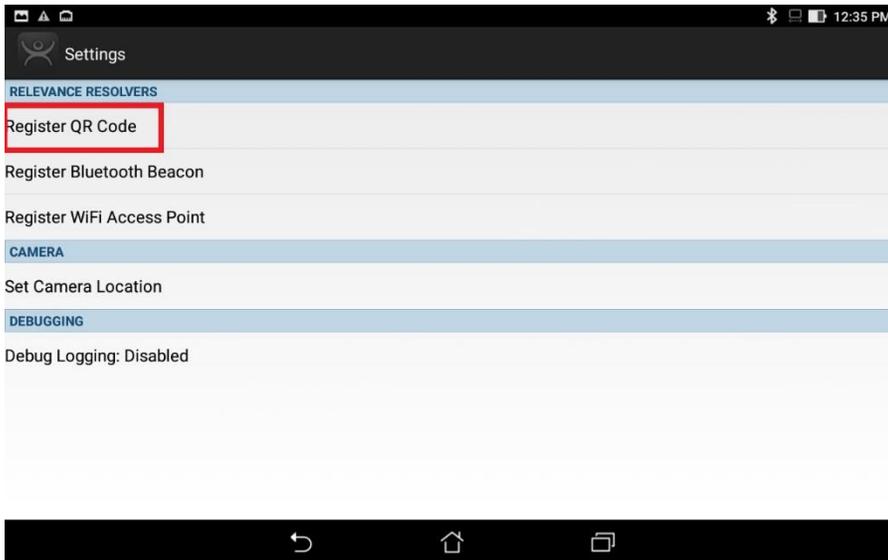
1. From aTMC, touch the **Back** button to return to the aTMC **Main Menu**. Touch **Yes** on the confirmation dialog.



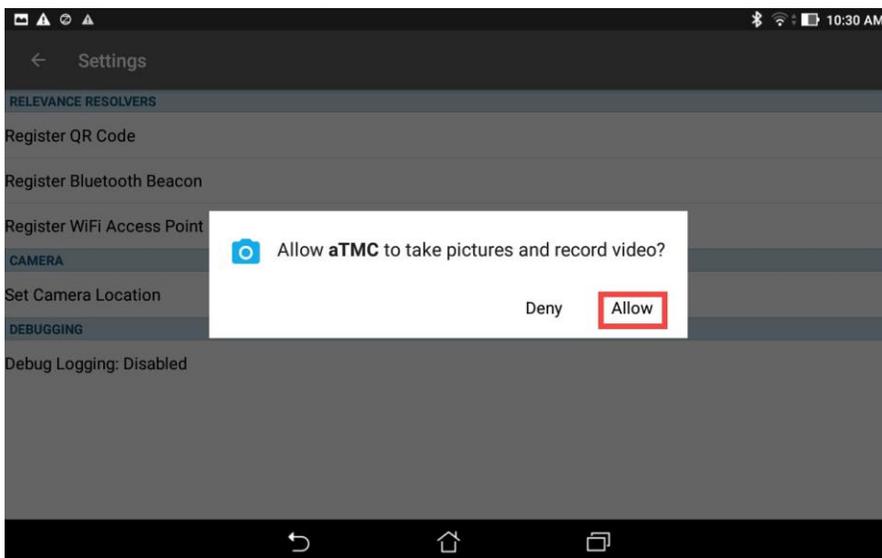
2. From the aTMC **Main Menu**, touch the **Settings** button (3 vertical dots below the **DemoKit** button), followed by the **Manage ThinServer** button.



3. From the aTMC **Settings** window, touch the **Register QR Code** button.



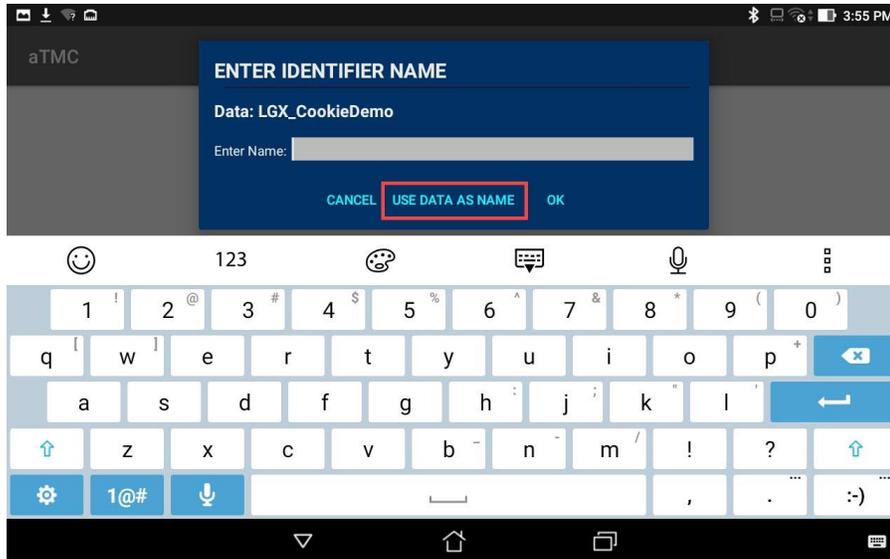
4. If you receive a prompt requesting permission for aTMC to take pictures and record video, touch the **Allow** button.



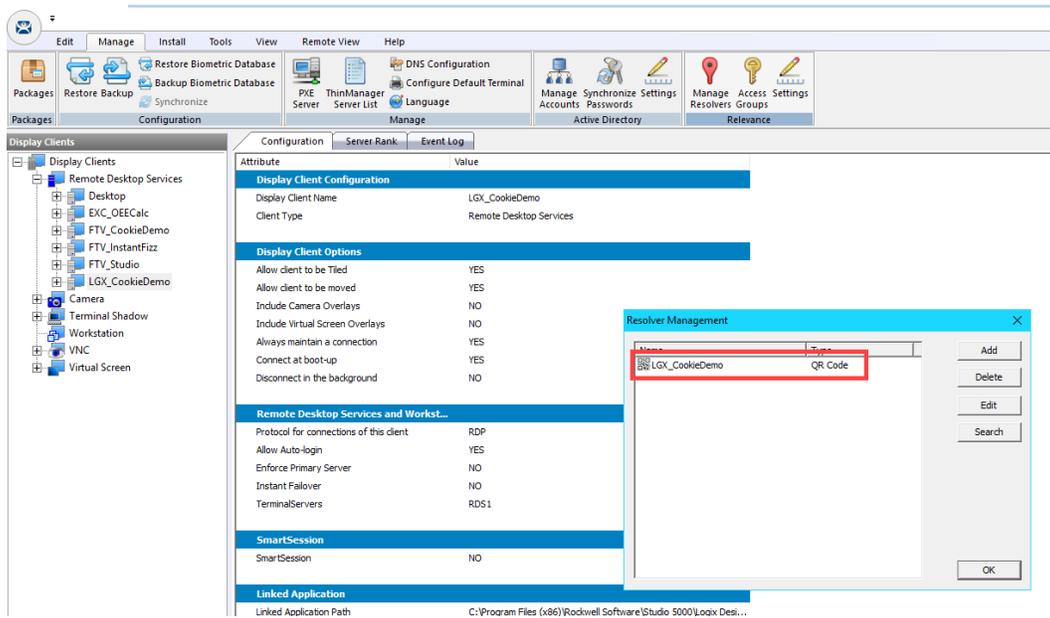
5. A camera window will appear. Point the Tablet camera at the **QR Code** below.



6. Once the **QR Code** is scanned by aTMC, you must give it a name. Touch the **USE DATA AS NAME** button which will use the data embedded in the **QR Code** as the name of the new **Location Resolver (LGX_CookieDemo)**.



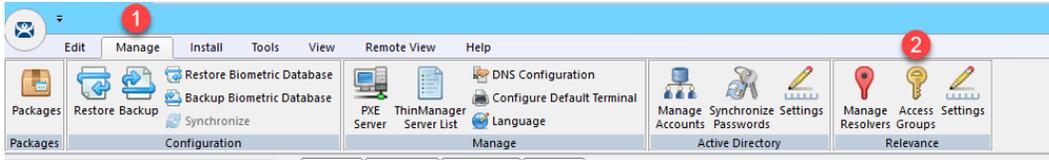
7. You should receive a successful confirmation dialog. Touch the **OK** button, followed by the **Back** button to return to the **Main Menu**.
8. To confirm the creation of the **Location Resolver**, return to **ThinManager** on **RDS1**, click the **Manage** ribbon, followed by the **Manage Resolvers** icon. You should see a new **QR Code** resolver named **LGX_CookieDemo** in the **Resolver Management** window. Click the **OK** button.



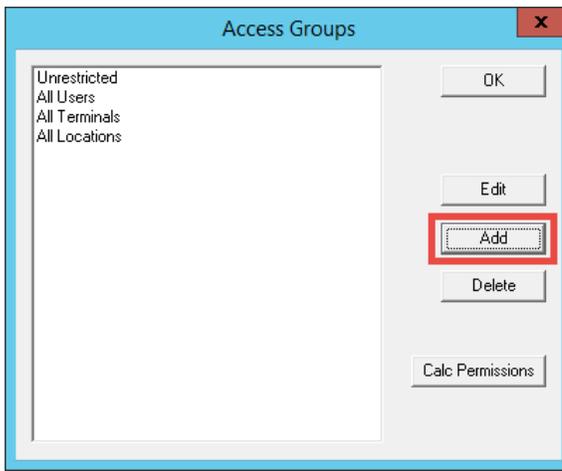
Create Engineer Access Group

We would like to restrict access to the new Location Resolver just created and its associated content. To do so, we will create a new Access Group and assign it to a Location in the following steps.

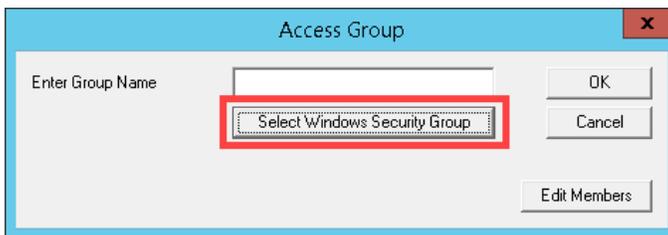
1. Click the **Manage** ribbon, followed by the **Access Groups** icon.



2. From the **Access Groups** popup, click the **Add** button.

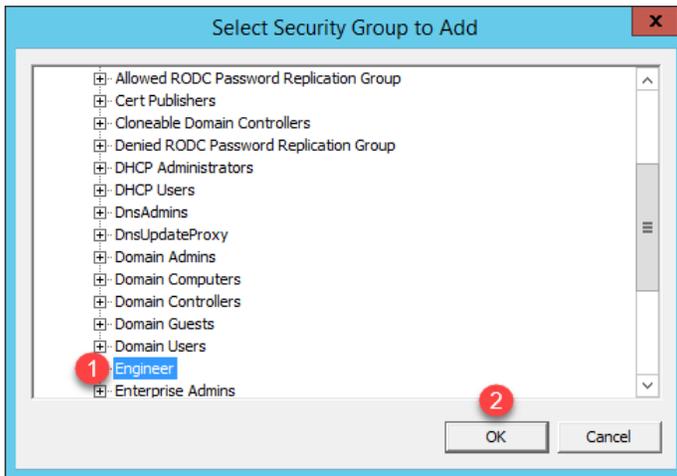


3. Click the **Select Windows Security Group** button.



The Select Windows Security Group provides the ability to link an Access Group to a Windows Security Group. Therefore, you could manage access to ThinManager resources (Terminals, Display Clients, etc.) through Windows Security Groups as well. You could also use the TermMon ActiveX within an ActiveX container, like View SE, to detect when a ThinManager logon event occurs and then to determine that user's Windows Security Group membership to determine their appropriate access within the application. You can learn more about the **TermMon ActiveX** in [Section 18](#).

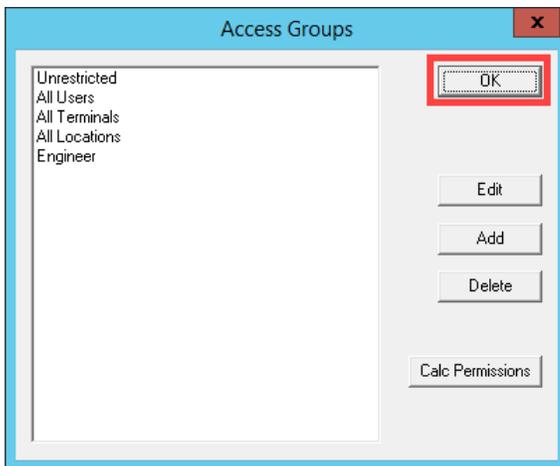
4. From the **Select Security Group to Add** window, expand the **Users** item and select the **Engineer** group.



5. From the **Access Group** window, click the **OK** button.



6. From the **Access Groups** window, click the **OK** button.

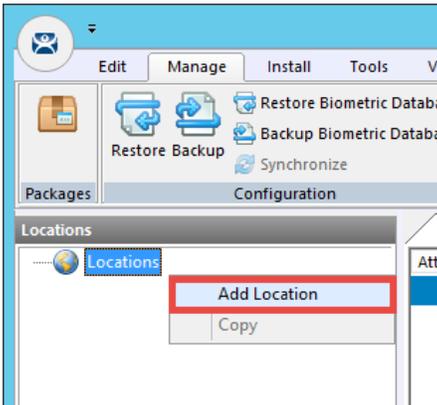


Create Relevance Location for Logix PLC

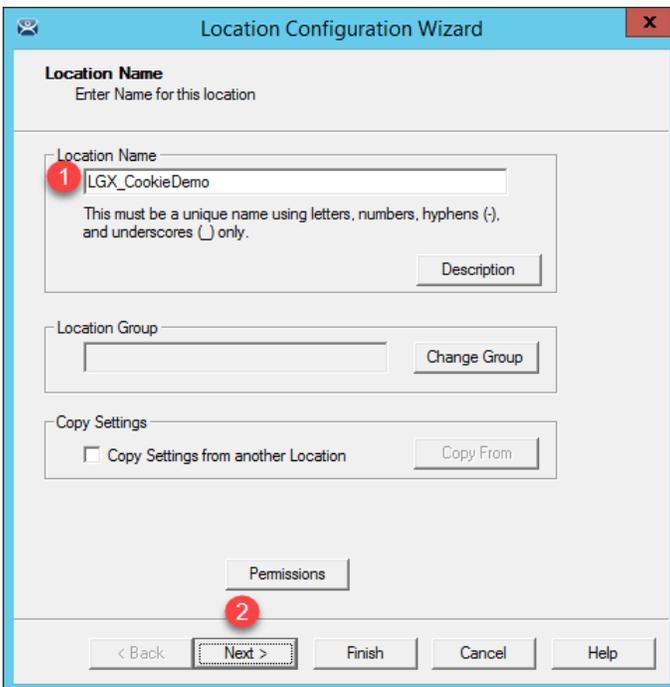
1. Click the **Locations** icon  in the tree selector.



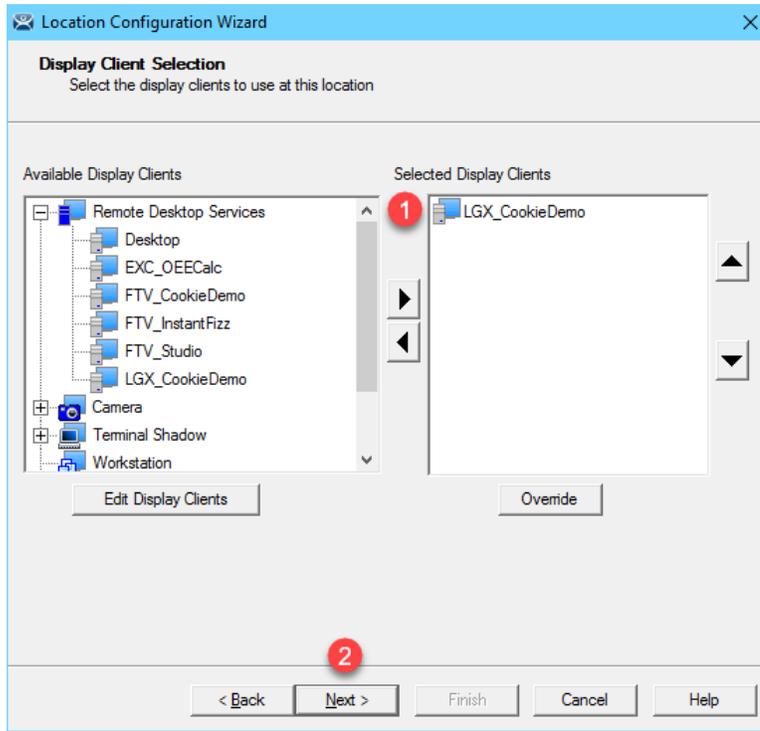
2. From the ensuing **Locations** tree, right click the **Locations** tree node and select **Add Location**.



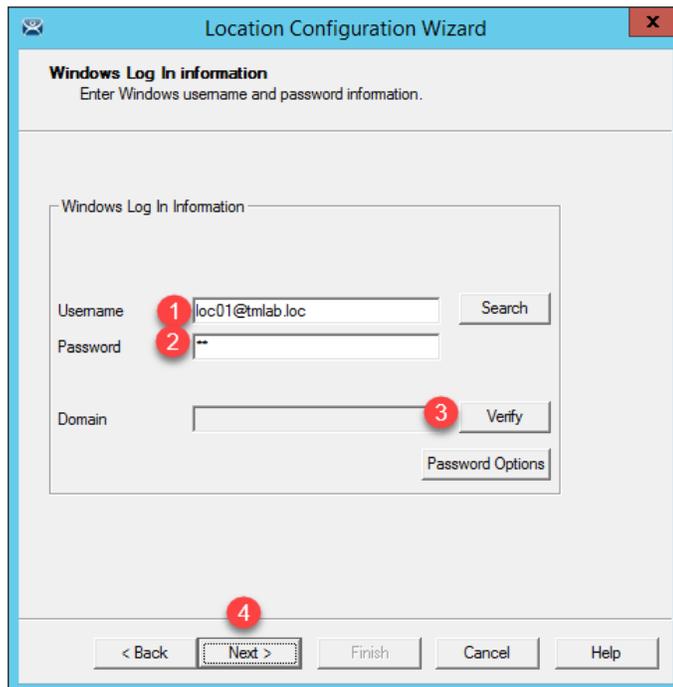
3. From the **Location Name** page of the **Location Configuration Wizard**, enter *LGX_CookieDemo* as the **Location Name**. Click the **Next** button.



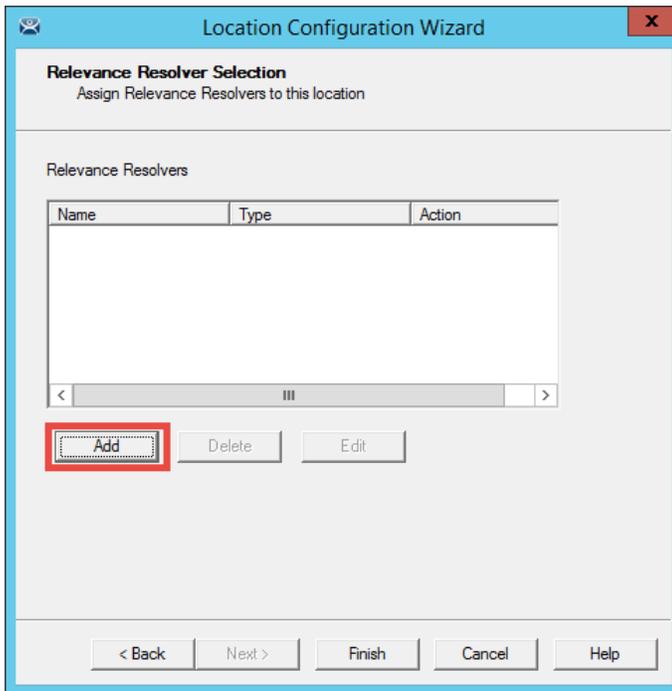
- From the **Location Options** page of the wizard, click the **Next** button.
- From the **Display Client Selection** page of the wizard, select the **LGX_CookieDemo Display Client** and click the **Right** arrow button to move it to the **Selected Display Clients** list, click **Next**.



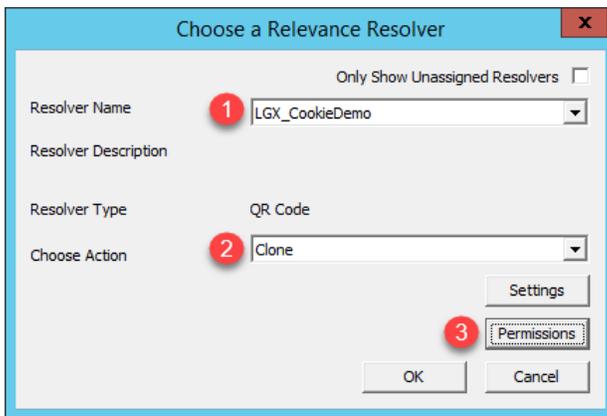
- From the **Windows Log In information**, enter *loc01@tmlab.loc* as the **Username** and *rw* as the **Password**. Click the **Verify** button to confirm the credentials are valid. Click the **Next** button.



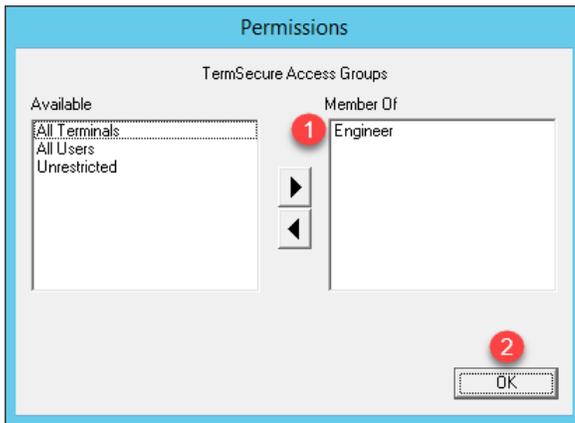
7. From the **Relevance Resolver Location** page of the wizard, click the **Add** button.



8. From the **Choose a Relevance Resolver** popup, select **LGX_CookieDemo** from the **Resolver Name** dropdown list, and **Clone** from the **Choose Action** dropdown list. Click the **Permissions** button.

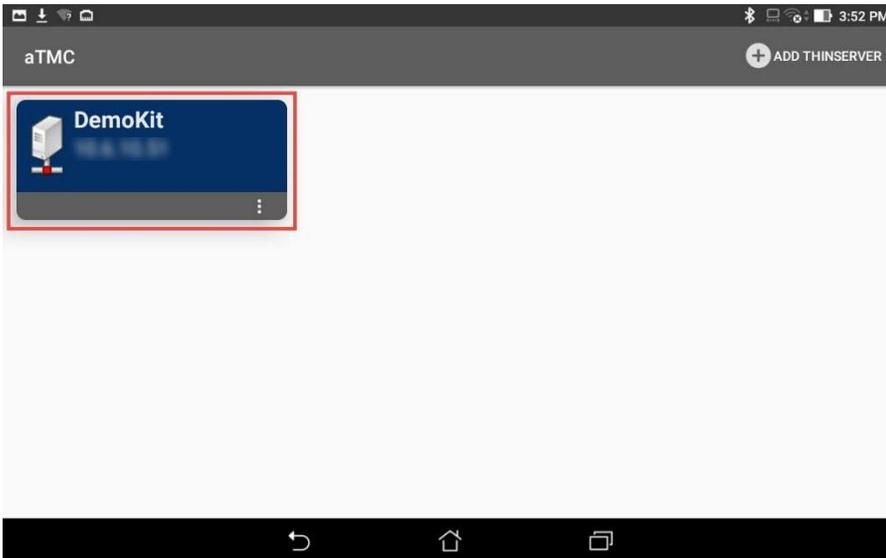


9. From the **Permissions** window, remove **Unrestricted** from the **Member Of** list, and move **Engineer** to the **Member Of** list. Click the **OK** button **twice**, followed by the **Finish** button.

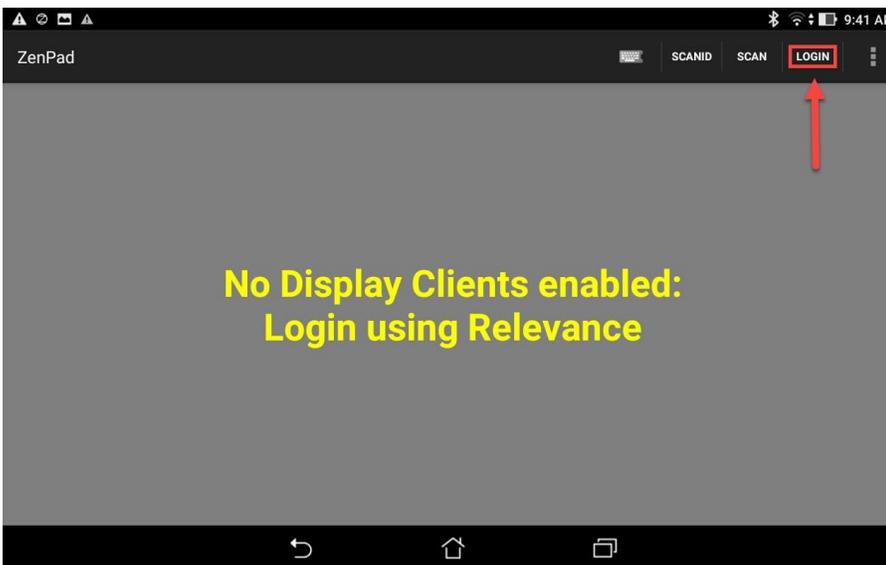


Resolve to Location from Mobile Device

1. Return to **aTMC**. You may have to power the ZenPad back on. If so, you may also have to reconnect **aTMC** to the **DemoKit** server listed.

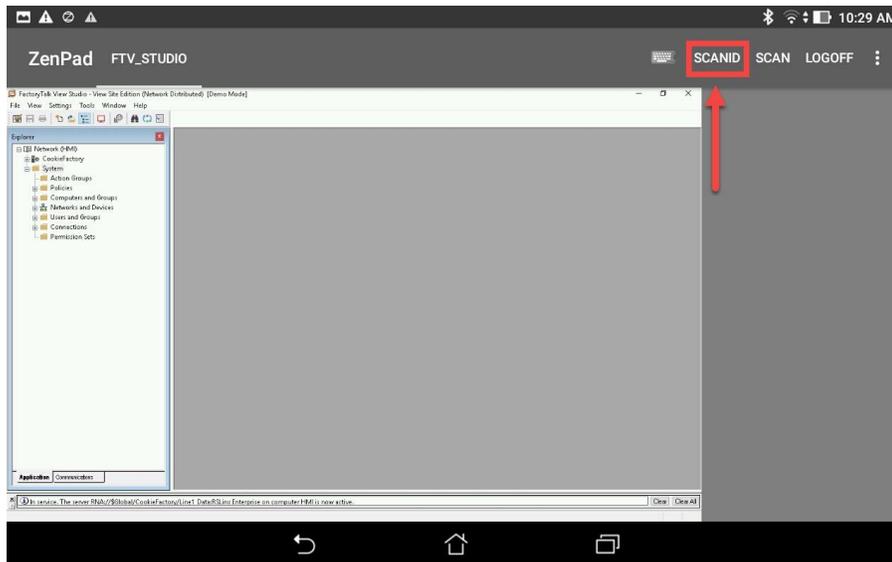


2. If not already logged in as **Ed**, touch the **LOGIN** button and enter a **username** of *ed* and a **PIN** of 1234.



If **aTMC** does not show a **LOGIN** button, please restart the **aTMC** app.

- Once logged in as Ed, touch the **SCANID** button in the top right corner.

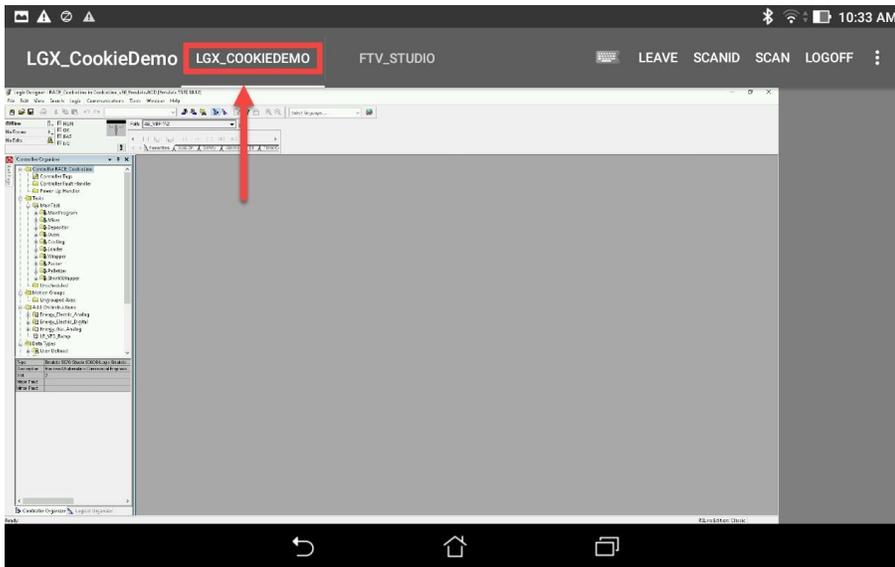


There is also a SCAN button available to the right of SCANID that enables the scanning of barcodes within the delivered applications.

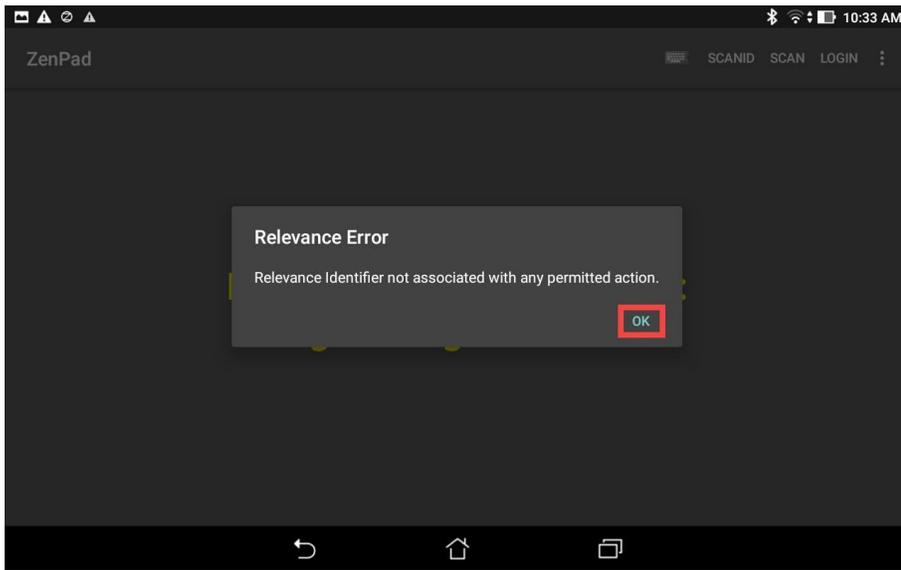
- The camera window will open within aTMC. Scan the QR Code below (this is the same QR Code we registered earlier).



- Since Ed is a member of the **Engineer Security Group**, he is permitted to resolve to the location represented by the **QR Code** above (which could be laminated and placed on the actual PLC panel). As a result, the **Logix Designer Display Client** should be delivered with the associated ACD file automatically opened. If not automatically activated, touch the **LGX_CookieDemo** tab at the top of **aTMC**.



- To verify the permissions required, touch the **LEAVE** button followed by the **LOGOFF** button and then attempt to re-scan the QR Code above. You should receive the following error message.



This completes the **Location Based Content Delivery** section of the lab. Please continue on to learn about **ThinManager Redundancy**