Rockwell Automation

ThinManager™ All in One Lab - Cloud

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.

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.

Contents

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.

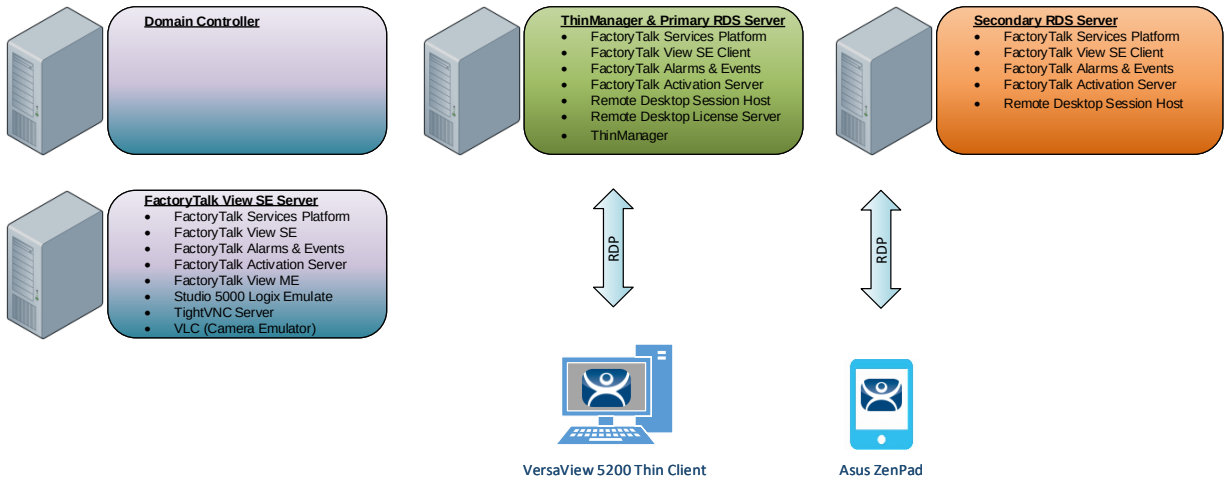
his lab is broken up into smaller segments and should be performed sequentially to start. Start by completing Sections 1 – 14 **in order**. Once Section 14 is completed you may proceed to complete **any** subsequent Section (15 – 18) in **any** order. To set expectations properly, it will most likely not be possible to complete all sections, as there is more content than allotted time. The lab manual will be available for future reference.

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 (**P**re-Boot E**x**ecution **E**nvironment). 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: Installation and Configuration of Remote Desktop Services

Overview

In this section, you will install and configure Remote Desktop Services on **RDS1**. To do this, you will be performing the following tasks:

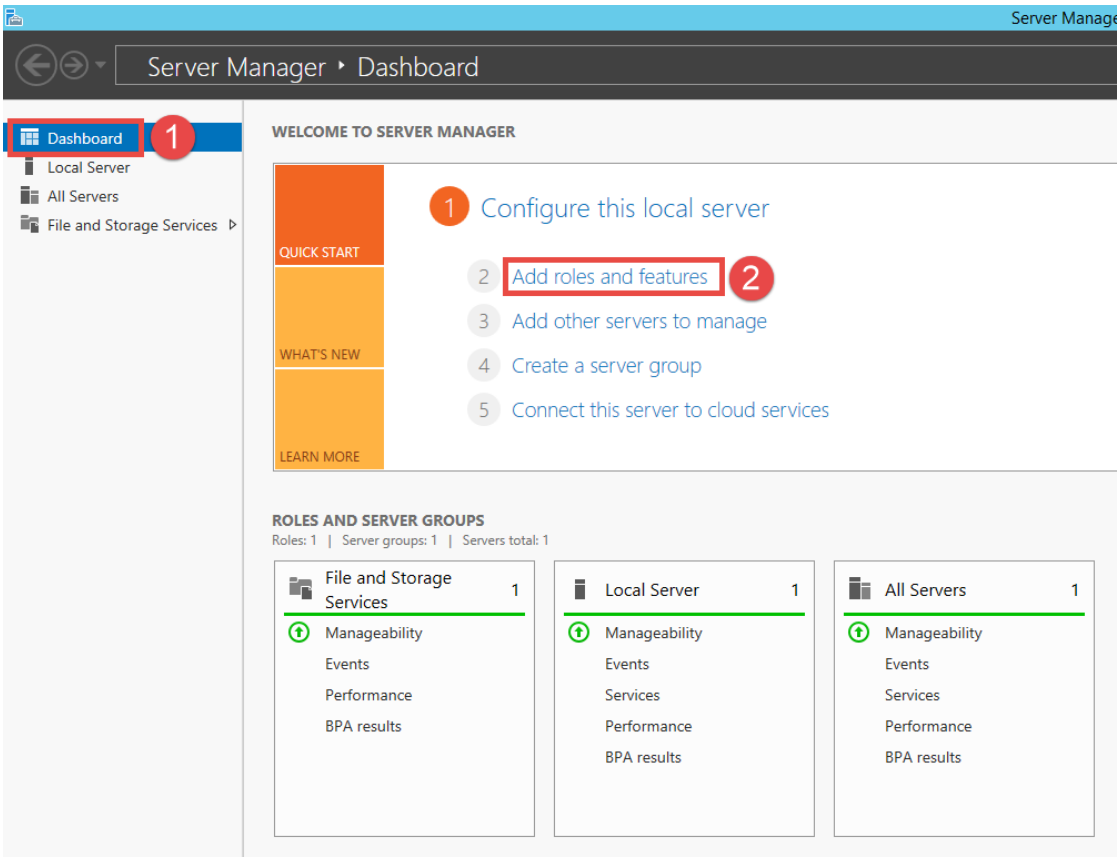
1. Install the Remote Desktop Services Role
2. Install the Remote Desktop Services Licensing Role
3. Create a Session Collection

> Windows Server 2016 is designed such that RDS servers should be joined to a domain using at least one Remote Desktop Services Connection Broker. All Remote Desktop Servers would then be managed as a Collection using Server Manager and/or PowerShell. However, Microsoft's Article ID 2833839, entitled "Guidelines for installing Remote Desktop Session Host role service on a computer running Windows Server 2016 without the Remote Desktop Connection Broker role service," describes that, although not ideal, the Remote Desktop Services role can be installed on a server joined to a workgroup as opposed to a domain. The major drawback to this architecture is that most of the User Interface tools provided to manage and configure Remote Desktop Services are not available to non-domain member servers. The configuration must take place using local group policy edits and/or PowerShell scripts.

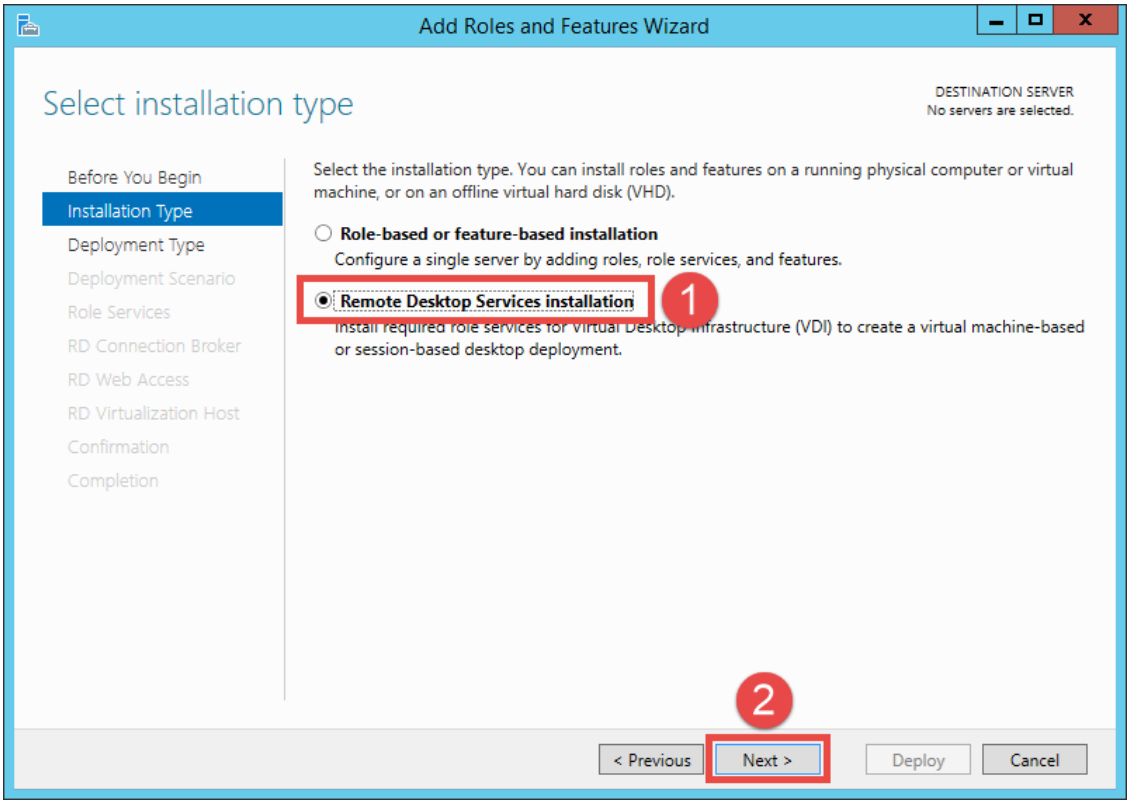
Install the Remote Desktop Services Role

Roles and Role Services are configured through the Server Manager after the operating system is installed. For Remote Desktop Servers, it is recommended that the Remote Desktop Services role be installed prior to any client applications.

1. Launch **Server Manager** by clicking the **Server Manager** icon from the **Windows** taskbar.
2. Once the Dashboard has refreshed (notice the streaming blue bar at the top while refreshing), click the **Add roles and features** link from the **Server Manager Dashboard**.

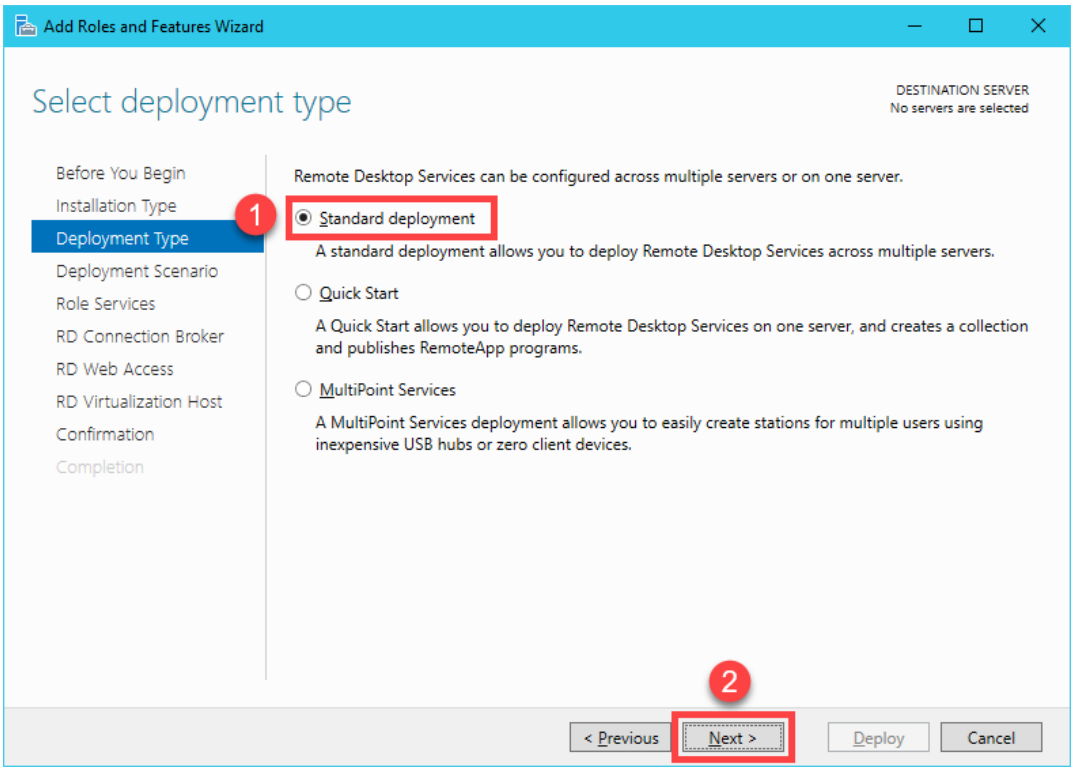


3. On the **Before You Begin** page of the **Add Roles and Features Wizard**, click **Next>**.
4. On the **Installation Type** page of the **Add Roles and Features Wizard**, select **Remote Desktop Services** installation and click **Next>**.



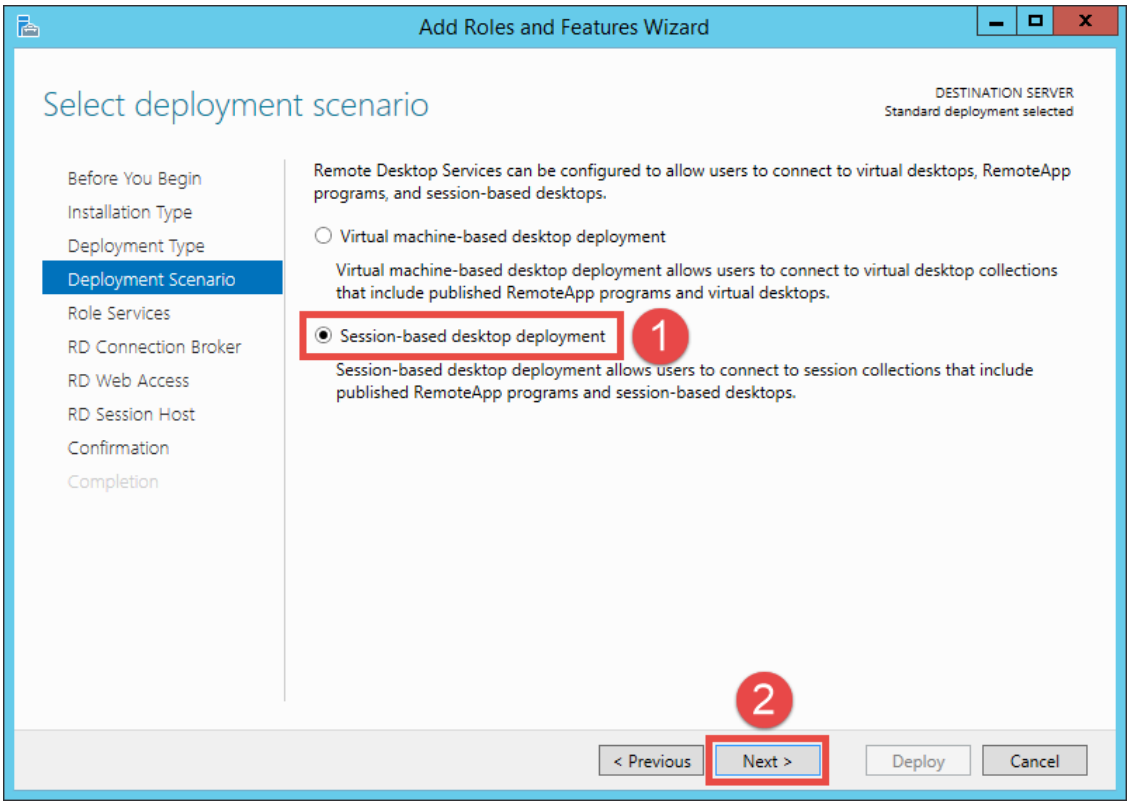
The Remote Desktop Services installation option is only available for Domain deployments. In addition, you can only perform a Domain Deployment if you are a Domain Administrator. If working in a Workgroup environment, the Role-based or feature-based installation must be selected.

5. On the **Deployment Type** page of the **Add Roles and Features Wizard**, select the **Standard deployment** option and click **Next>**.



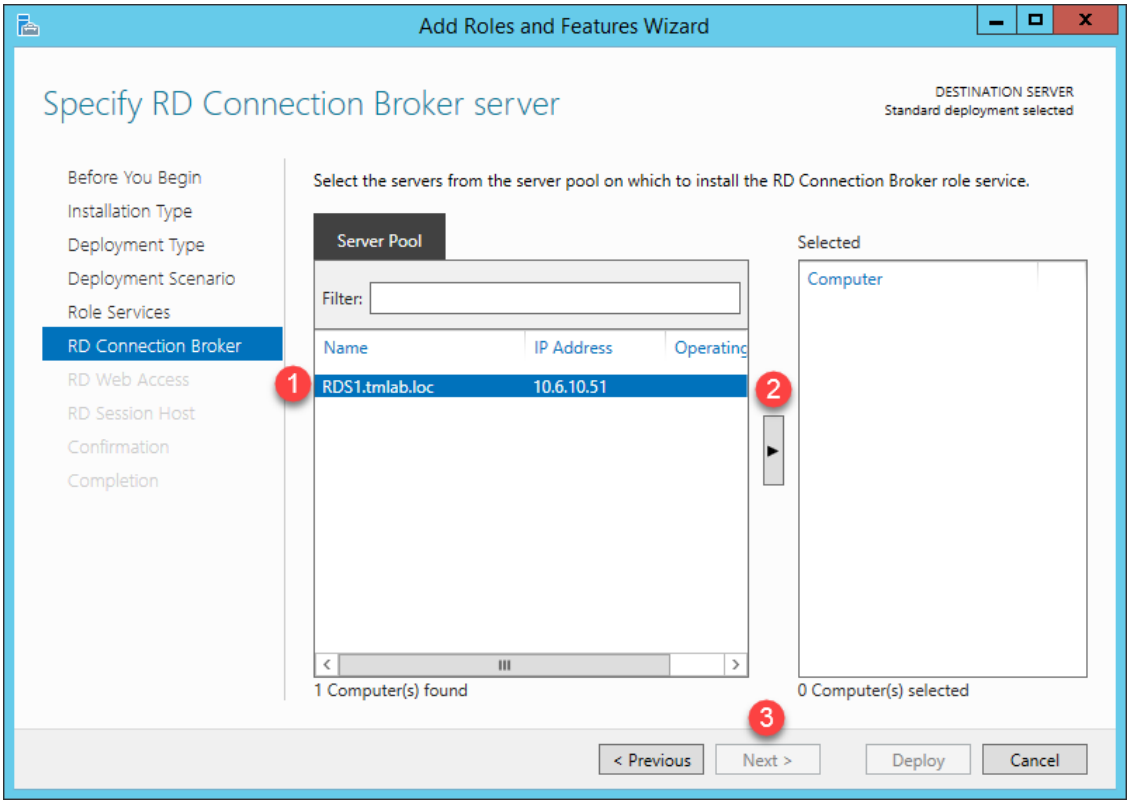
> The Quick Start option is only suitable when deploying a single Remote Desktop Server. Since this lab is only using a single Remote Desktop Server, this option could have been used as well.
>
> For deployments with more than one Remote Desktop Server, it is best to create a Server Group within Server Manager and add the Remote Desktop Servers to that group. Server groups allow you to view and manage a smaller subset of your server pool as a logical unit. To create a Server Group, click the Manage menu button within Server Manager, followed by the Create Server Group item. You can then add the desired servers to the new group.
>
> It is also a recommendation to create a separate Organizational Unit (OU) within the Active Directory domain for the Remote Desktop Servers. You will then be able to manage the Group Policies for all of your Remote Desktop Servers through a single OU.

6. On the **Deployment Scenario** page of the **Add Roles and Features Wizard**, select **Session-based desktop deployment** and click **Next>**.



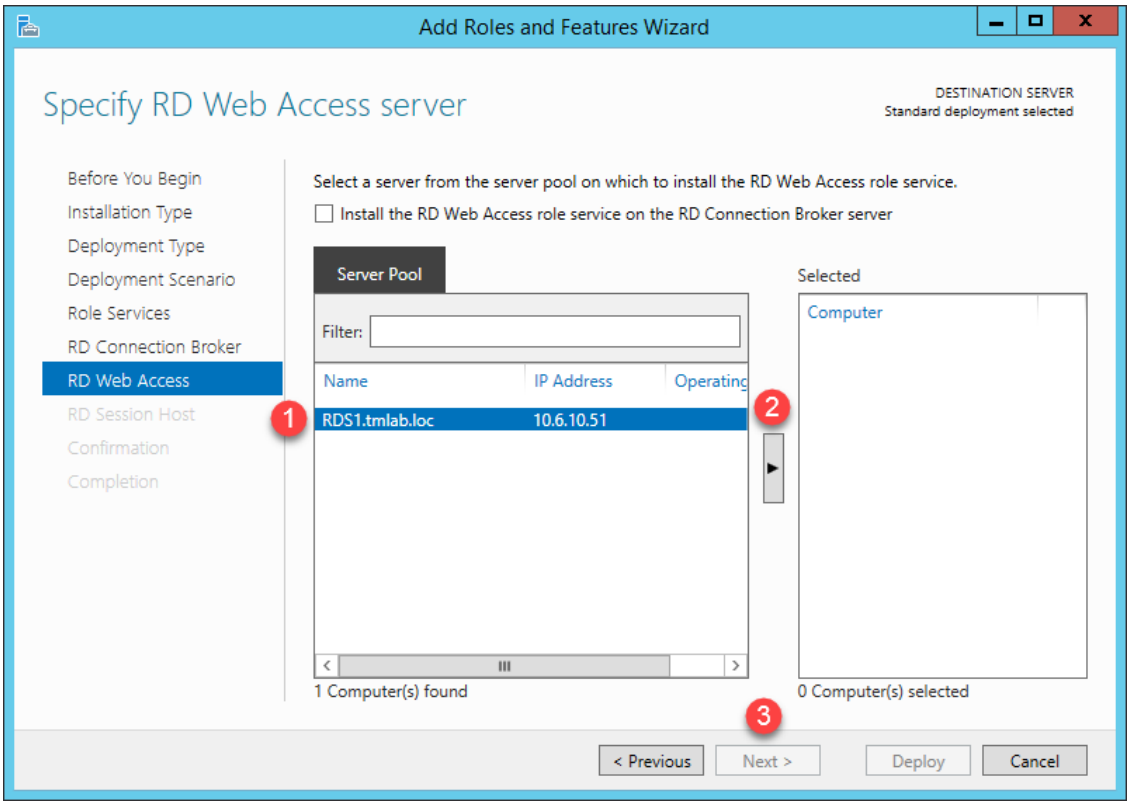
The Remote Desktop Virtualization Host role service provides virtual machine access on Hyper-V over Remote Desktop connections. We will not be using this component in the lab.

7. Click the **Next>** button on the **Role Services** page of the **Add Roles and Features Wizard**.
8. From the **RD Connection Broker** page of the **Add Roles and Features Wizard**, click the **Right Arrow** button to add the **RDS1.lab.loc** server to the **Selected** list, followed by **Next>**.



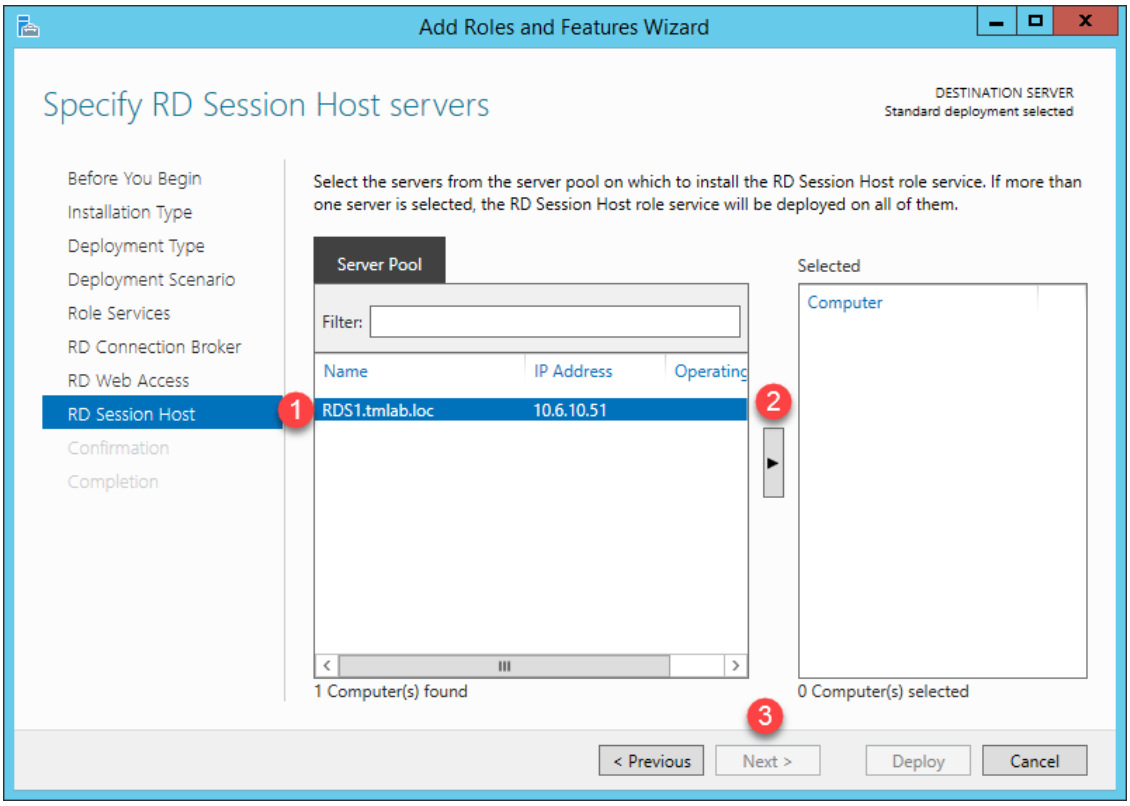
The Remote Desktop Connection Broker role service is used for creating server farms to handle load balancing and application aggregation.

9. On the **RD Web Access** page of the **Add Roles and Features Wizard**, click the **Right Arrow** button to add the **RDS1.lab.loc** server to the **Selected** list, then click **Next>**.

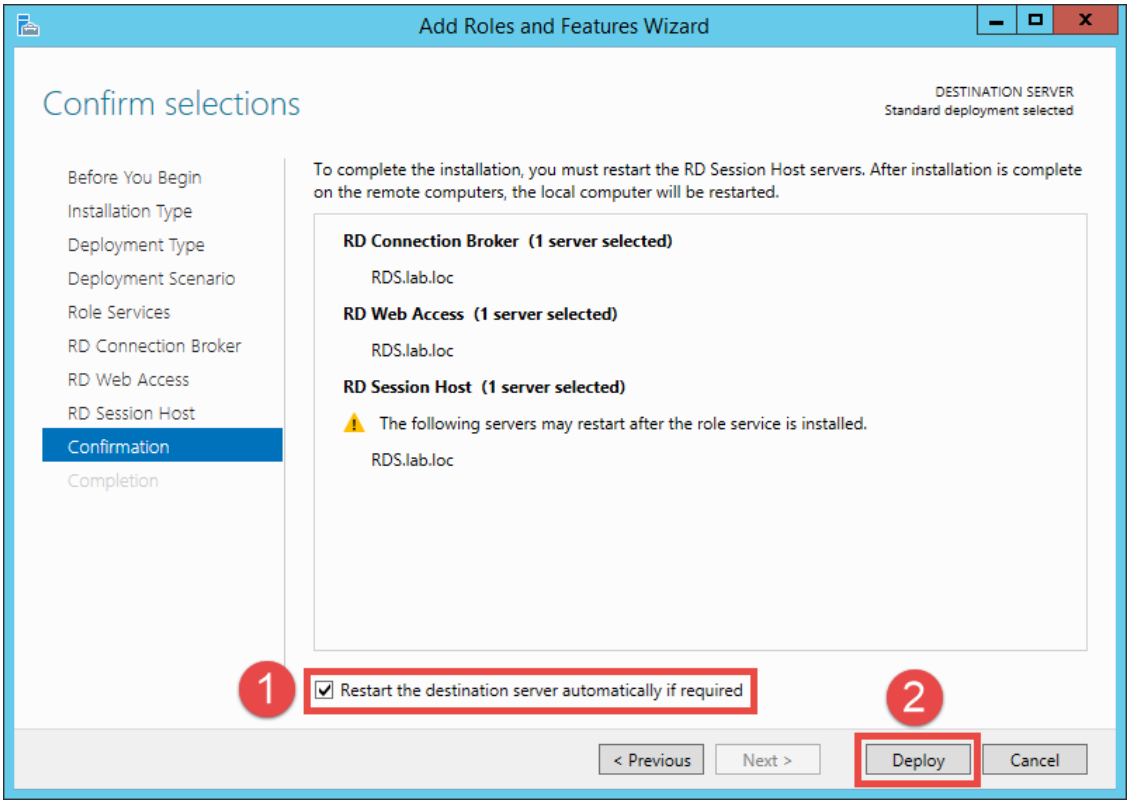


The RD Web Access role service is used to enable users to access Remote Desktop connections via a web browser.

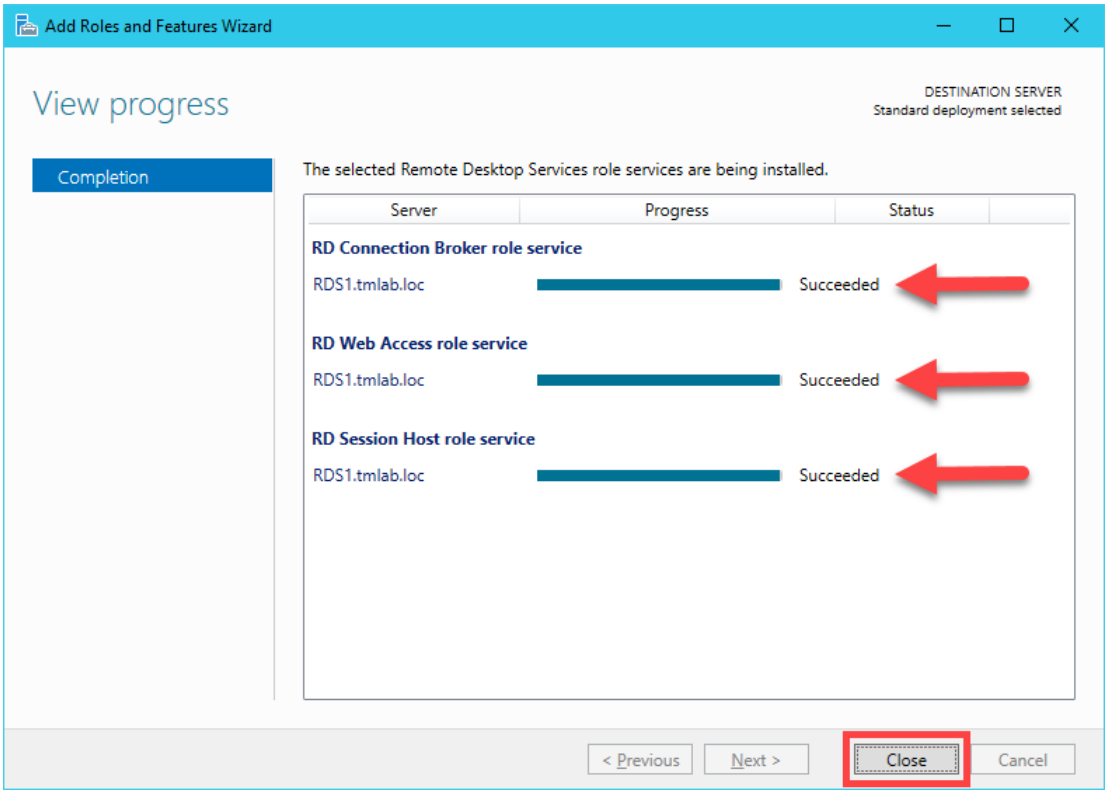
10. On the **RD Session Host** page of the **Add Roles and Features Wizard**, click the **Right Arrow** button to add the **RDS1.lab.loc** server to the **Selected** list, then click **Next>**.



11. On the **Confirmation** page of the **Add Roles and Features Wizard**, check the **Restart the destination server automatically if required** checkbox followed by clicking the **Deploy** button. The installation process will start and continue for a few minutes. Once finished, **RDS1** will automatically reboot. **<u>This process will take a few minutes to complete.</u>**



12. Once **RDS1** begins to restart, it will take approximately 2 minutes before you can reconnect to your Cloud image via **RDP**. Once you have reconnected to **RDS1**, click the **Server Manager** icon next to the **Windows Start** button. The **Add Roles and Features Wizard** will reappear and provide status on the installation progress. Once the Status indicates **Succeeded** for each of the 3 role services, click the **Close** button.



Note: This will disconnect you from RDS1. Reconnect to your lab station from Thinfinity after 2-5 minutes (just as you had done at the beginning of this lab).

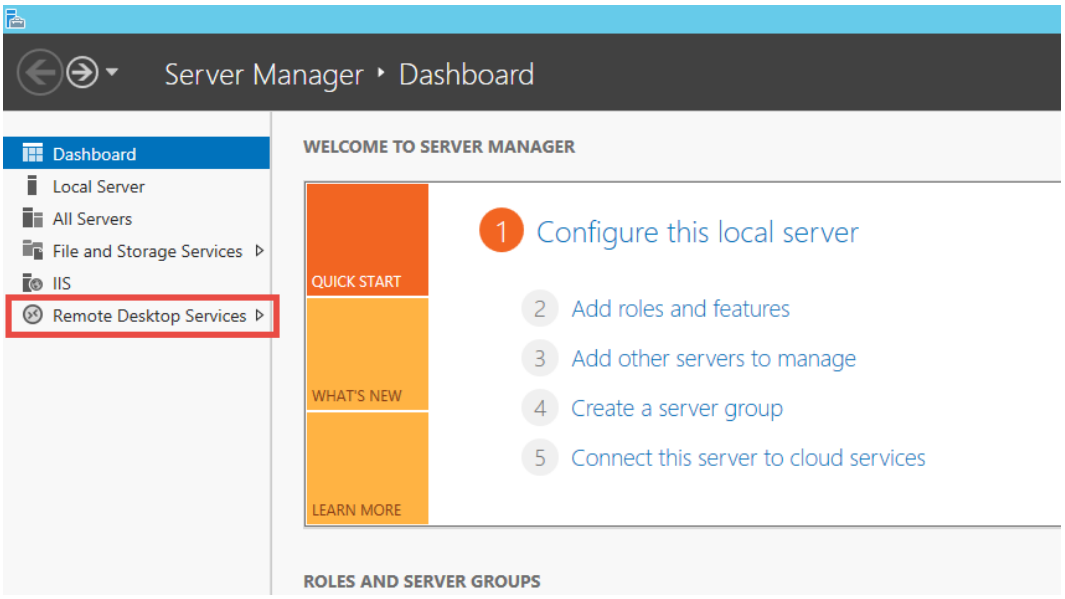
Install the Remote Desktop Services Licensing Role

When deploying Remote Desktop Services, consideration for Remote Desktop Services Client Access Licenses (RDSCALs) must be made. RDSCALs can be purchased from Microsoft in either Per User or Per Device. Use Per User licensing when individual users will be connecting from various devices and the number of users is generally smaller than the number of devices available to them for accessing the server.

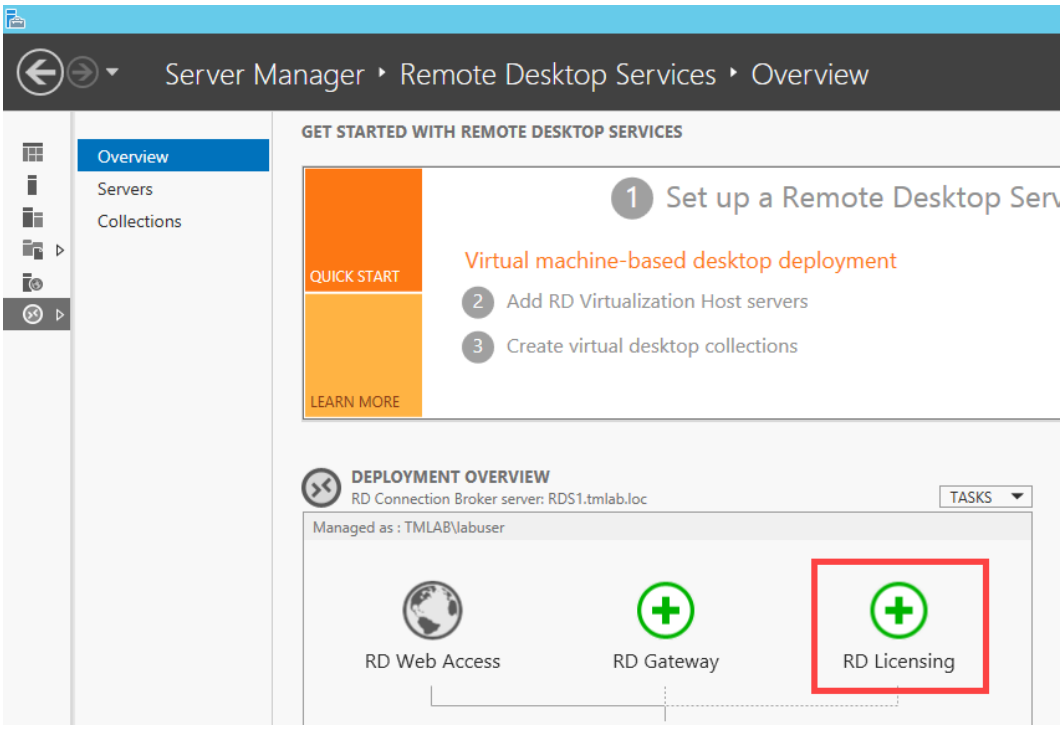
Use Per Device licensing when many users will be connecting from a fixed number of devices and the number of devices is generally smaller than the number of users using those devices. Per Device is generally best suited for ThinManager deployments.

> By default, 2 administrative connections are allowed to the server. These connections do not require licenses from the license pool to be available. To start an administrative session, you must use the latest version of the Microsoft Remote Desktop Connection client and specify *<servername> /admin* as the address of the remote computer. Older versions of the Remote Desktop Connection tool did this via command line parameters to mstsc.exe.

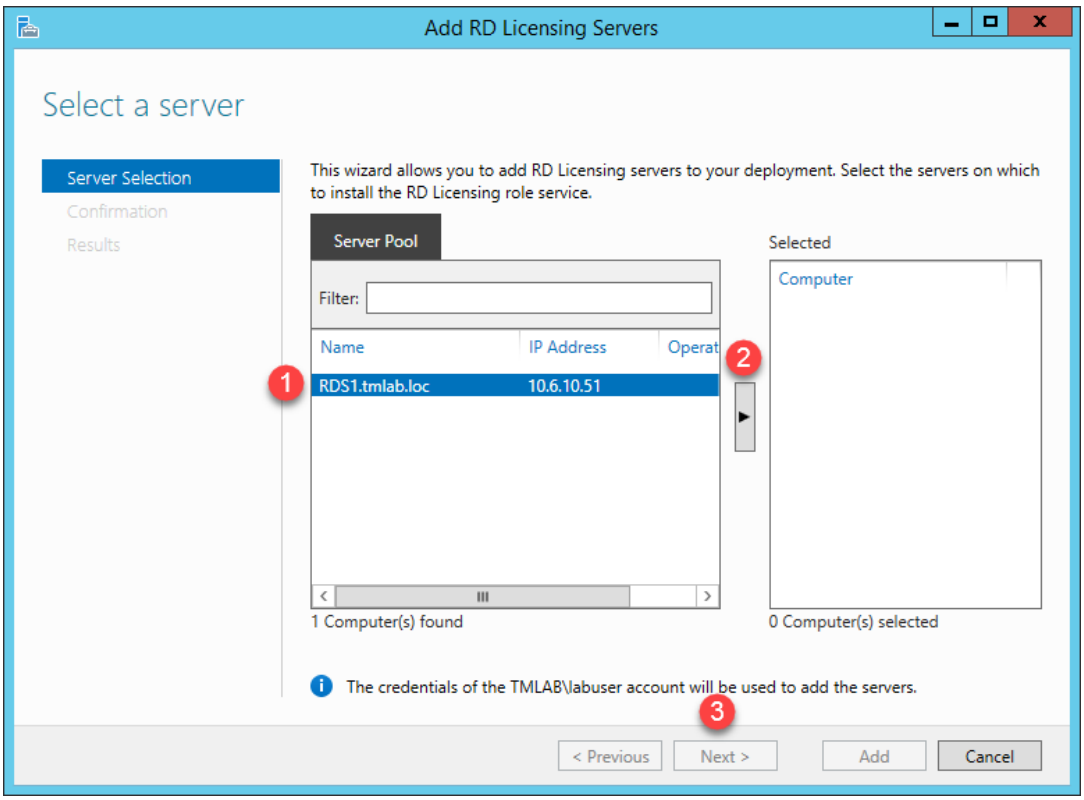
1. From **Server Manager**, click the **Remote Desktop Services** panel item.



2. From the **Overview** page of the **Remote Desktop Services** panel, click the **Green Plus** above **RD Licensing** to install the **Remote Desktop Licensing Service**.

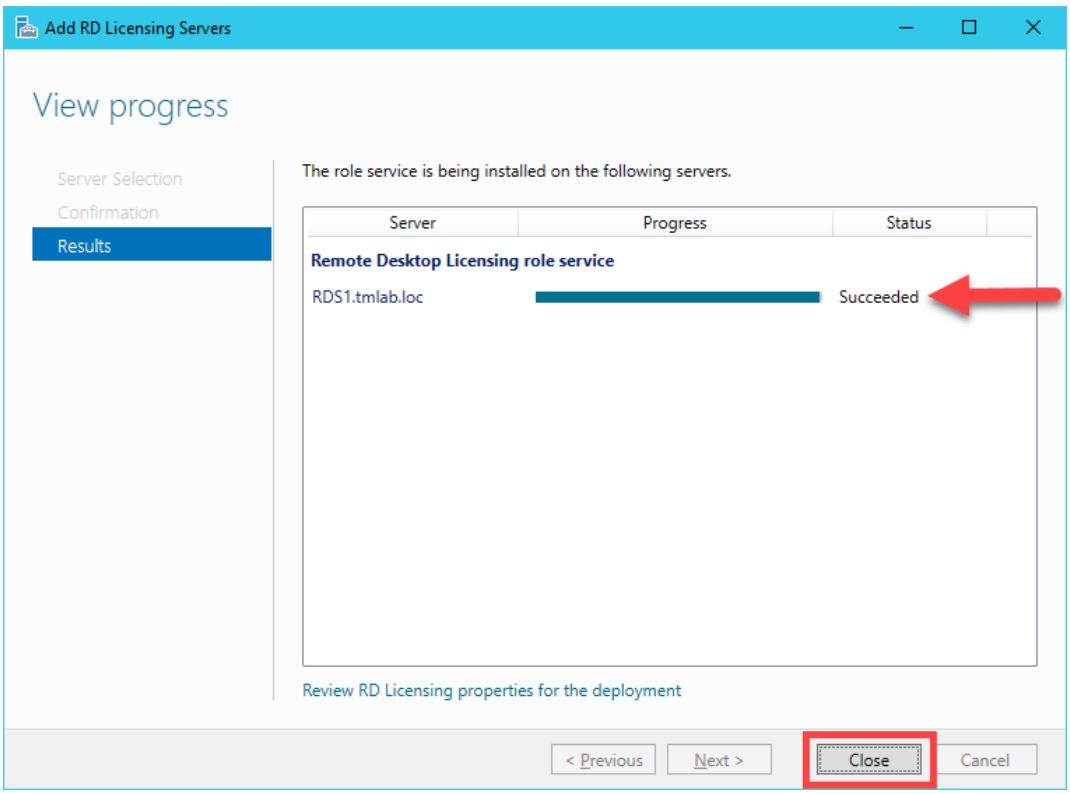


3. From the **Server Selection** page of the **Add RD Licensing Servers** wizard, click the **Right Arrow** button to add **RDS1.lab.loc** to the **Selected** list. Click **Next>**.

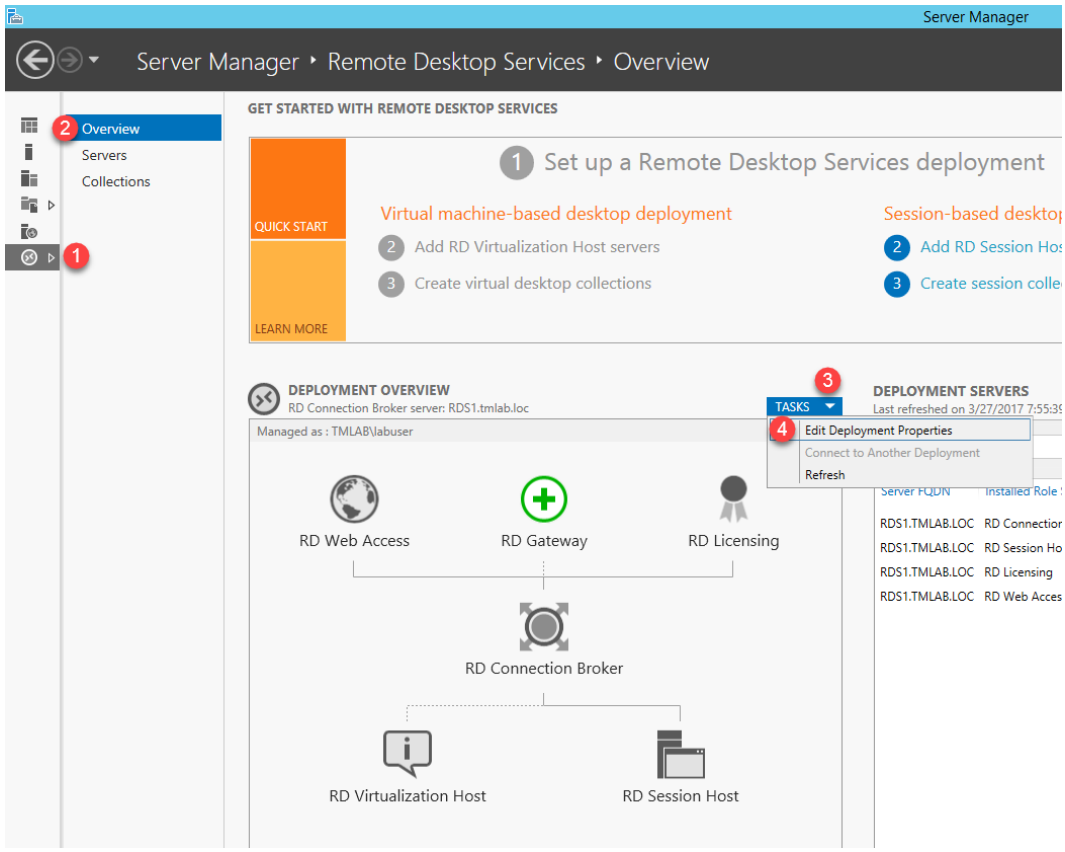


4. From the **Confirmation** page of the **Add RD Licensing Servers** wizard, click the **Add** button.

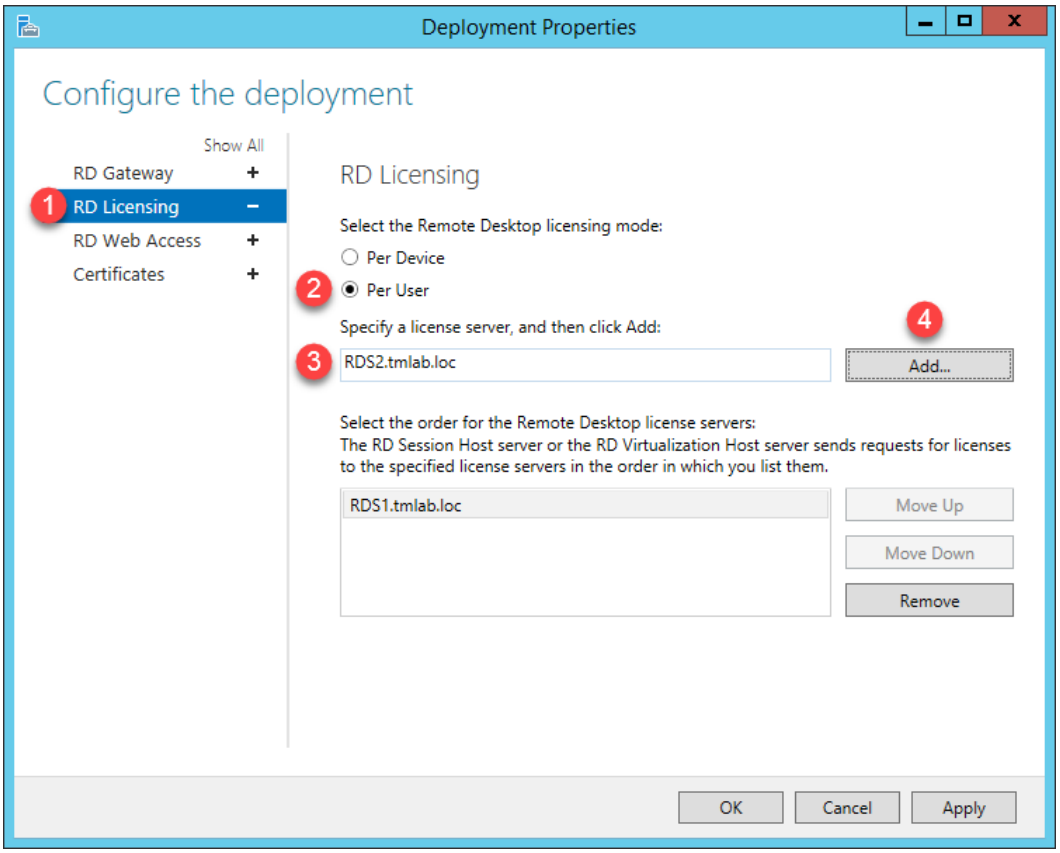
5. When the installation is complete, the **Status** will change to **Succeeded**. Click the **Close** button.



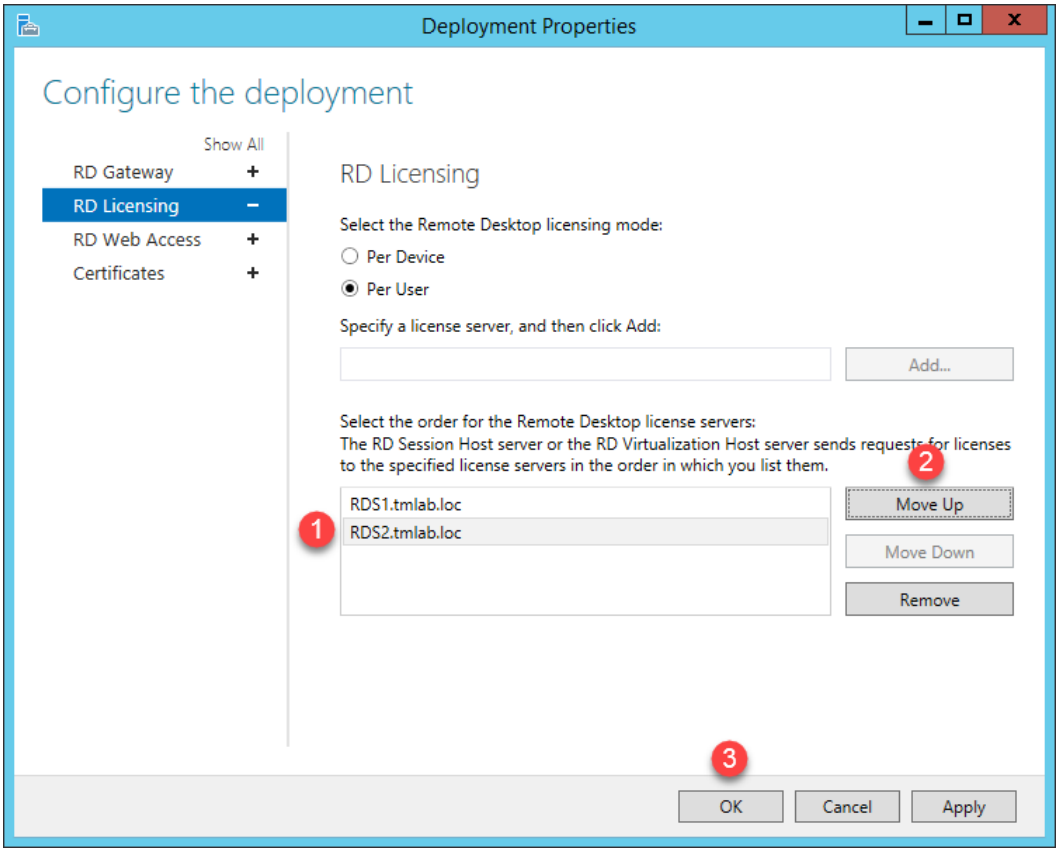
6. From the **Overview** panel of **Remote Desktop Services**, click the **Tasks** drop down list in the **Deployment Overview** frame and select the **Edit Deployment Properties** item.



7. From the **Deployment Properties** screen, select the **RD Licensing** panel, then click the **Per User** radio button. In addition, enter *RDS2.tmlab.loc* in the license server field and click the **Add…** button.



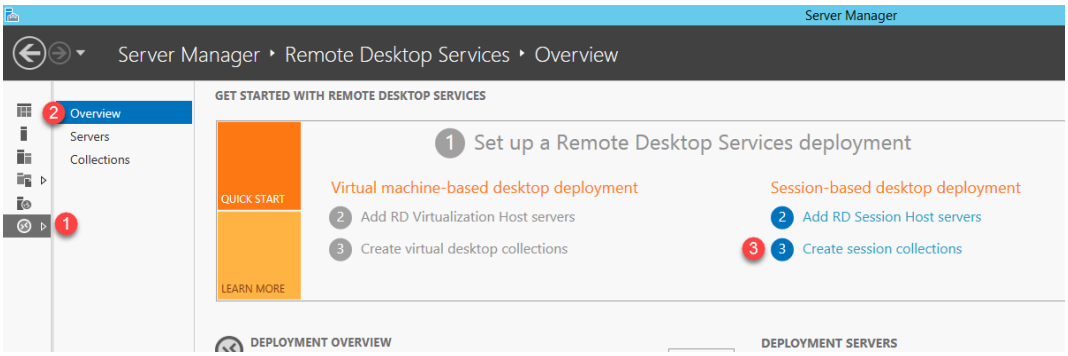
8. For the purposes of this lab, we will move the licensing server from **RDS2** to the top of the list (since it has been Activated an RD Licensing Server for you), so select **RDS2.tmlab.loc** from the license server list and click the **Move Up** button, followed by the **OK** button. This should stop that warning message you have probably seeing at the bottom right of the RDS1 screen regarding Licensing Servers.



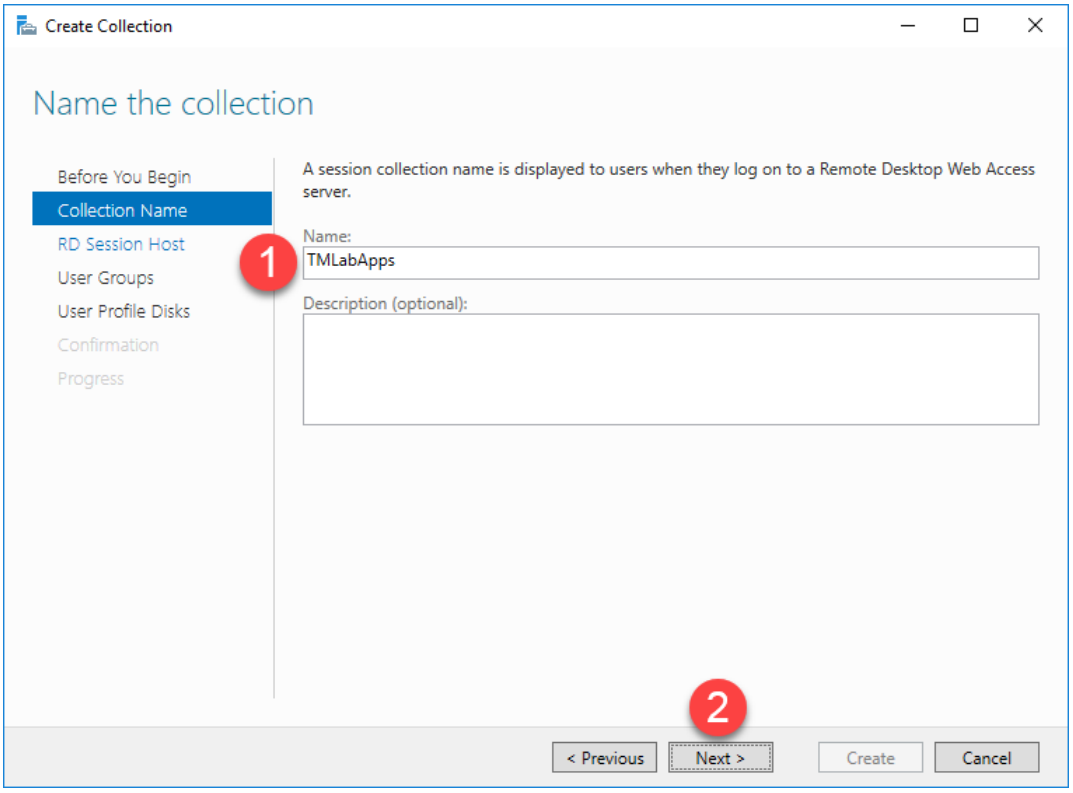
Create a Session Collection

Session Collections are only available for domain deployments. Collections allow you to group RD Session Host servers and manage their associated properties and published RemoteApps from a single location. A majority of the session based properties found in Server 2008 R2 and earlier can now be found at the Collection level.

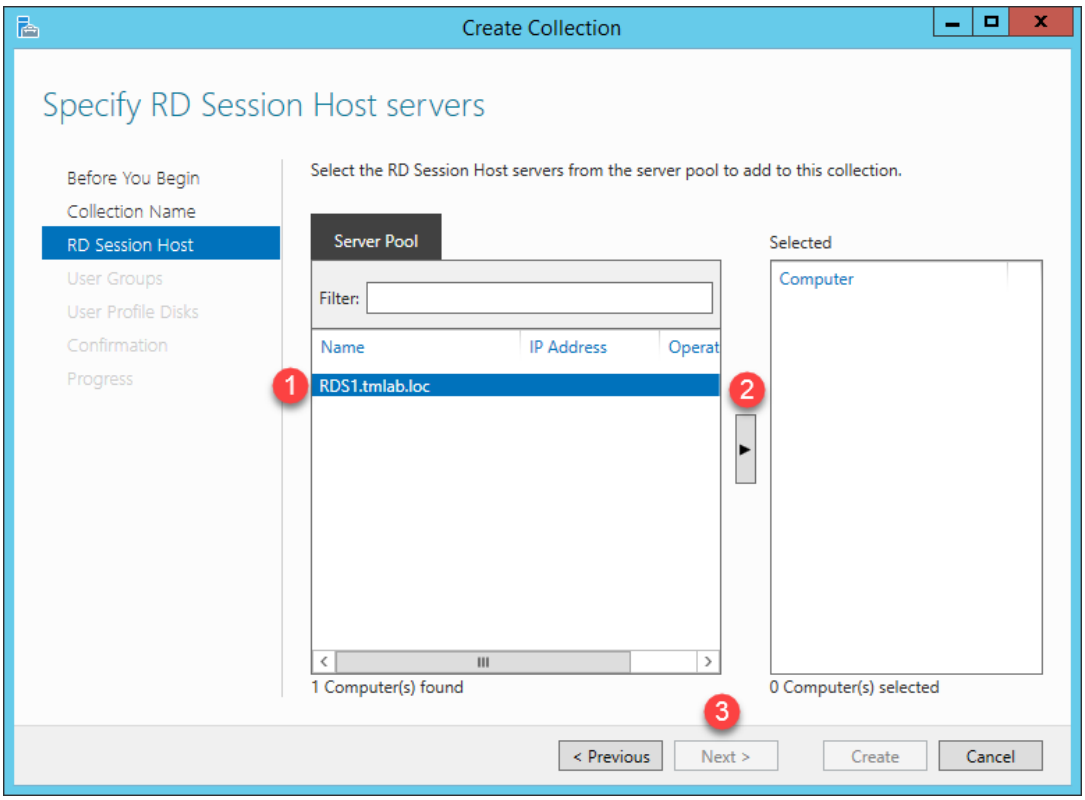
1. To create a new **Session Collection**, click the **Create session collections** link from the **Overview** page of the **Remote Desktop Services** panel.



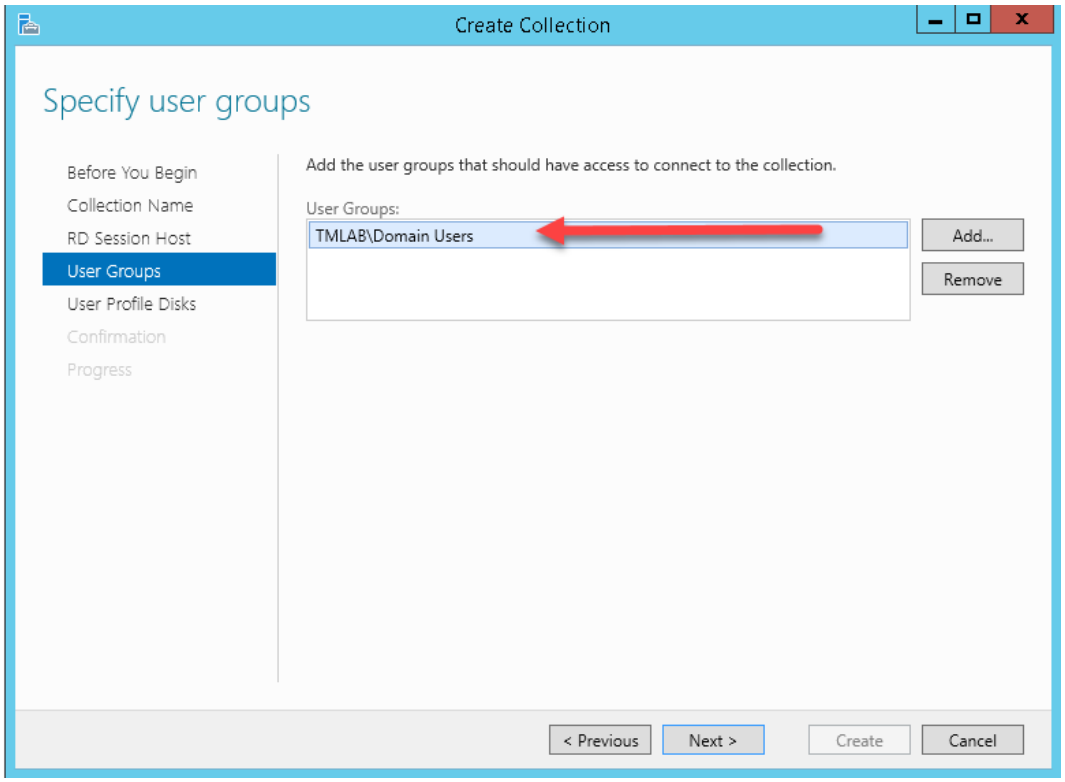
2. From the **Before You Begin** page of the **Create Collection** wizard, click **Next>**.
3. From the **Collection Name** page of the **Create Collection** wizard, enter ***TMLabApps***, then click **Next>**.



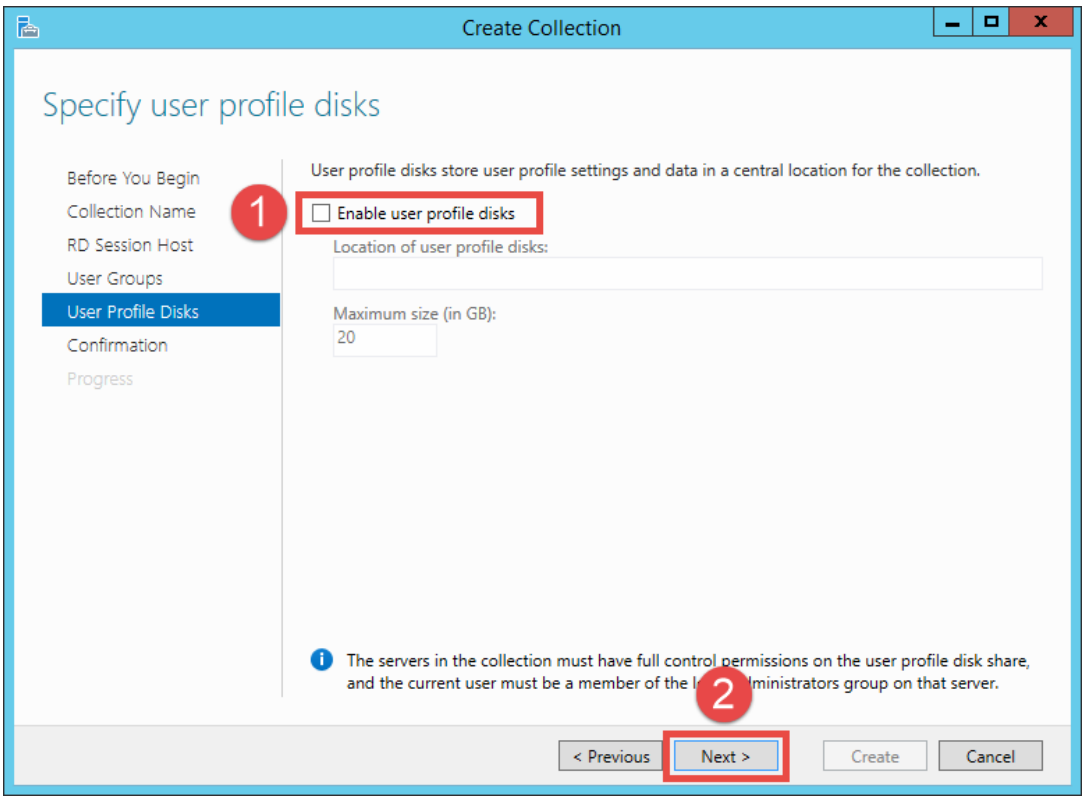
4. From the **RD Session Host** page of the **Create Collection** wizard, click the **Right Arrow** button to add **RDS1.lab.loc** to the **Selected** list and click **Next>**.



5. From the **User Groups** page of the **Create Collection** wizard, keep the default selection of **TMLAB\Domain Users**, which means that all users in the **TMLAB** domain will have access to this **Session Collection**. Click **Next>**.

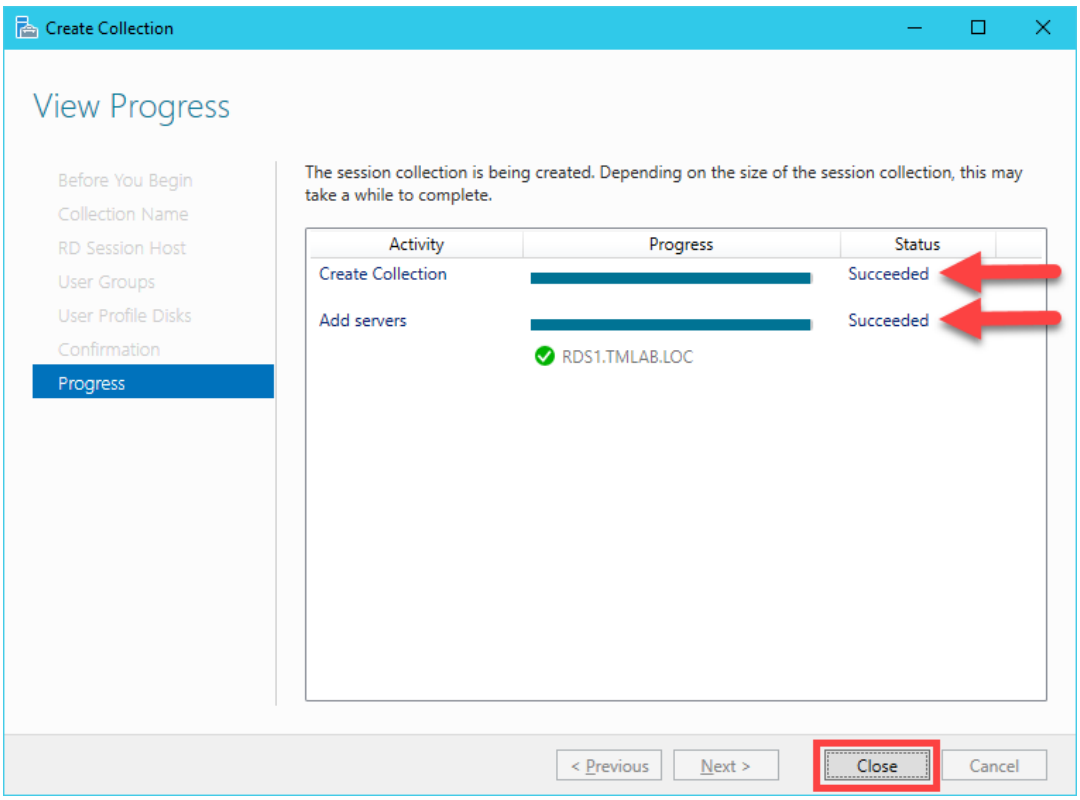


6. From the **User Profile Disks** page of the **Create Collection** wizard, uncheck the **Enable user profile disks** checkbox and click **Next>**.



7. Click the **Create** button from the **Confirmation** page of the **Create Collection** wizard.

8. Once complete, the **Status** indication should change to **Succeeded**. Click the **Close** button. Close **Server Manager** as well.



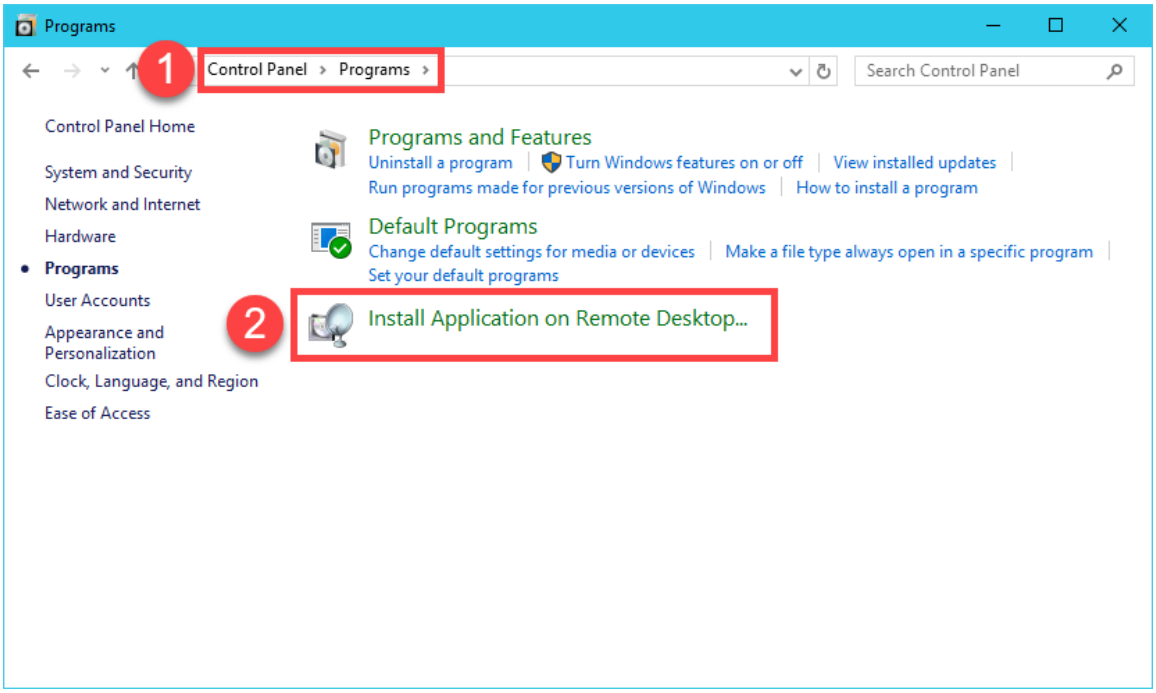
> As mentioned previously, many of the properties found in the **Remote Desktop Session Host Configuration** in Windows Server 2008 R2 are now found at the **Session Collection** level.

> With Windows Server 2012 or newer, the Remote Control Settings are now found in Group Policy, either Local or Domain, at Computer Configuration→Policies→Administrative Templates→Windows Components→Remote Desktop Services→Remote Desktop Session Host→Connections→Set rules for remote control of Remote Desktop user sessions. In addition, each domain user account has Remote Control settings as well which determine whether their remote sessions are enabled for remote control. If so, you can also control whether the user requires permission to be remotely controlled and whether the remote control session provides interactivity or not. These settings can be found on the Remote control tab of the user properties dialog box within the Active Directory Users and Computers application on the domain controller.

This completes the section **Installation and Configuration of Remote Desktop Services**. Continue on to the next section to learn about installing and configuring a **FactoryTalk View Site Edition Client** on a **Remote Desktop Server**.

Section 2: Installation and Configuration of FactoryTalk View Site Edition Client

To prevent idle time, the FactoryTalk View SE Client has been pre-installed on RDS1. Below, under the Overview section, there are links to the Lab Appendix where steps to complete the FactoryTalk View SE Client install and Network Directory configuration are located for your reference. Installing the Remote Desktop Service Role before installing client applications and performing client application(s) installation in RD-Install mode are best practices when deploying Remote Desktop Services applications with ThinManager. After reviewing the Appendix (do not complete as part of this lab), proceed to Section 3.



Overview

In this section, you will install and configure FactoryTalk View Site Edition Client software on the Remote Desktop Server. To do this, you will be performing the following tasks:

1. Install FactoryTalk View Site Edition Client in RD-Install Mode – Located in Lab Appendix for your reference
2. Configure the FactoryTalk Directory to Point to a Network Directory – Located in Lab Appendix for your reference

Section 3: Installation and Configuration of ThinManager

Overview

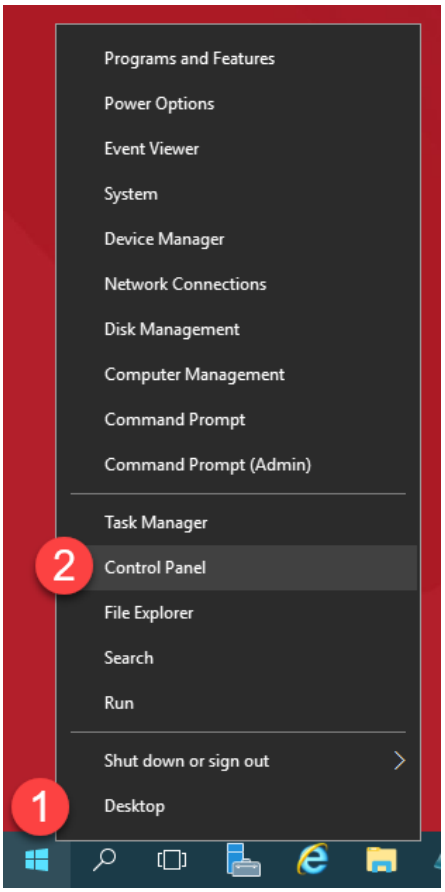
In this section, you will install ThinManager on the **RDS1** virtual machine. While ThinManager is most commonly installed on a **Remote Desktop Server**, it does not have to be. In fact, it could be installed on a workstation class machine, like **Windows 7** even. Basically, ThinManager does **not** have to be installed on a **Remote Desktop Server** in order to use that server as a source of content.

In this section, you will be performing the following tasks:

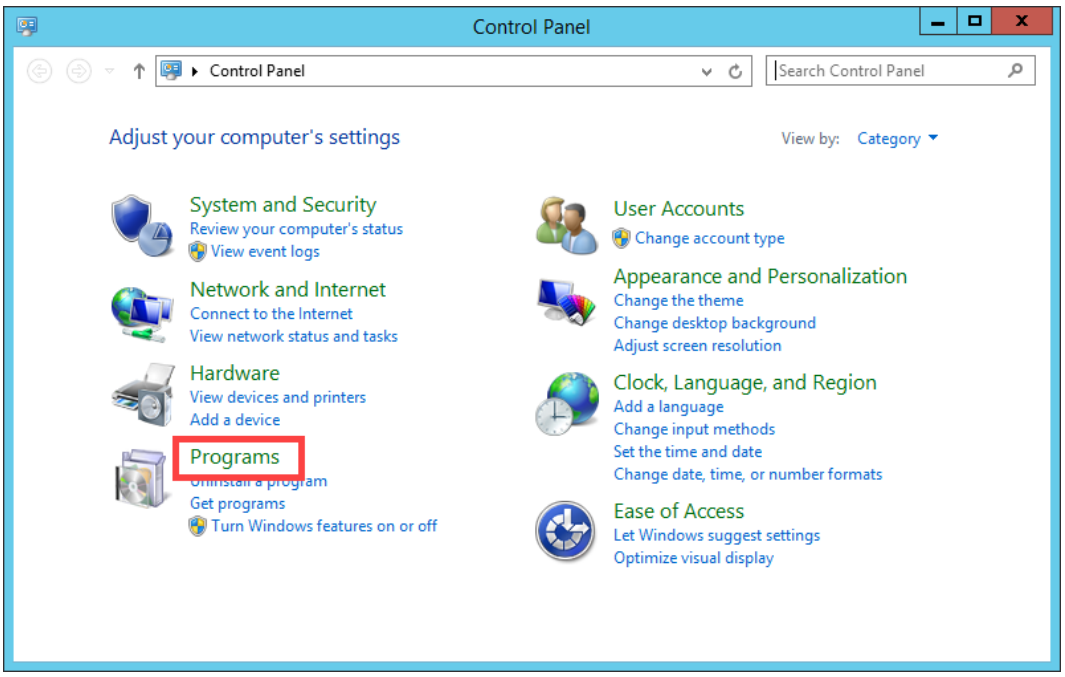
1. Installation of ThinManager
2. Apply FactoryTalk Activation for ThinManager
3. Apply Traditional Master License for ThinManager
4. Update TermCap Database

Installation of ThinManager

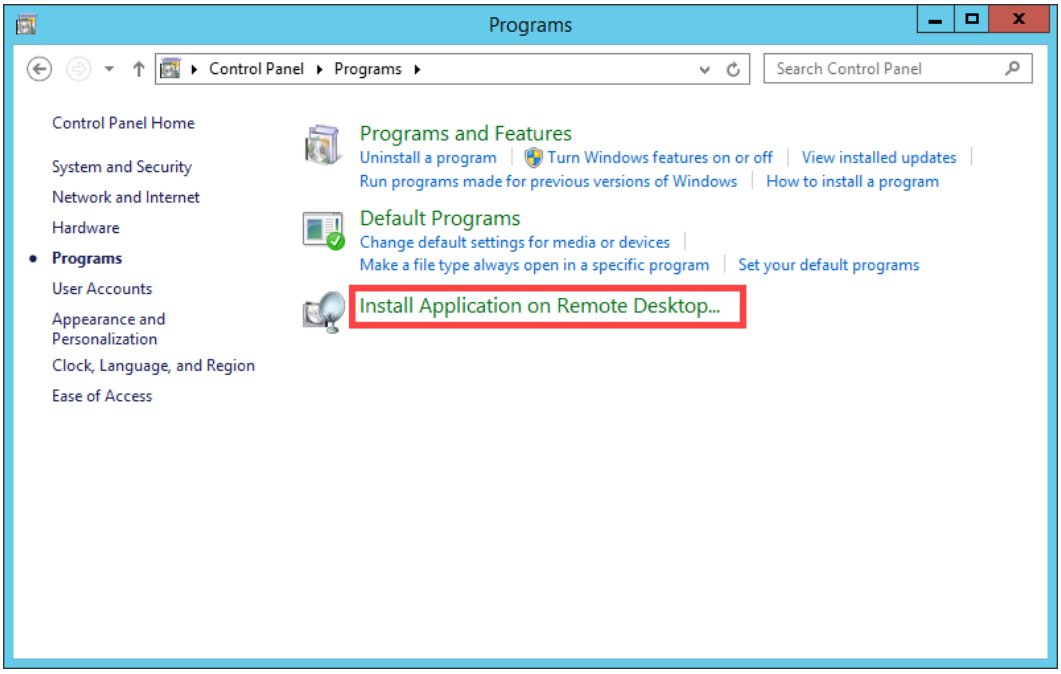
1. Right click the **Windows Start** button and click the **Control Panel** menu item.



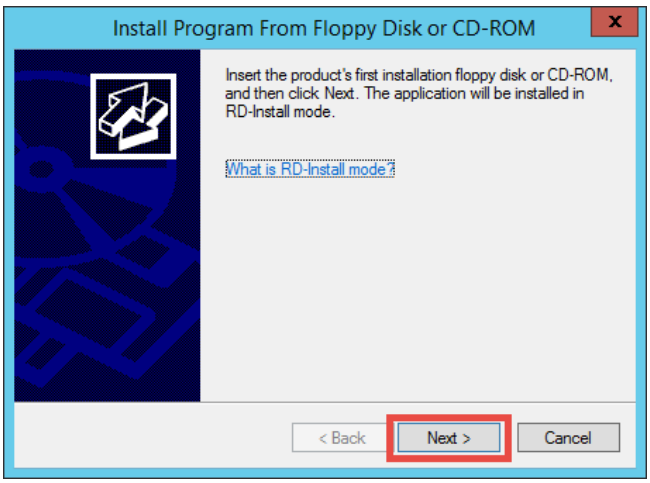
2. From the **Control** Panel, click the **Programs** link.



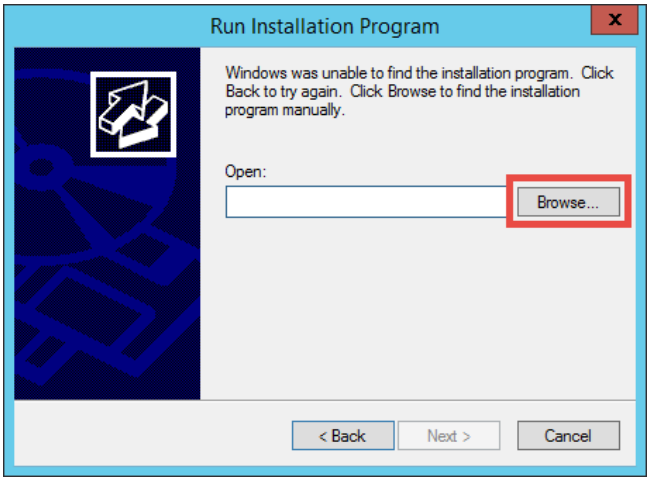
3. From the **Programs** page of the **Control Panel**, click the **Install Application on Remote Desktop…** link.



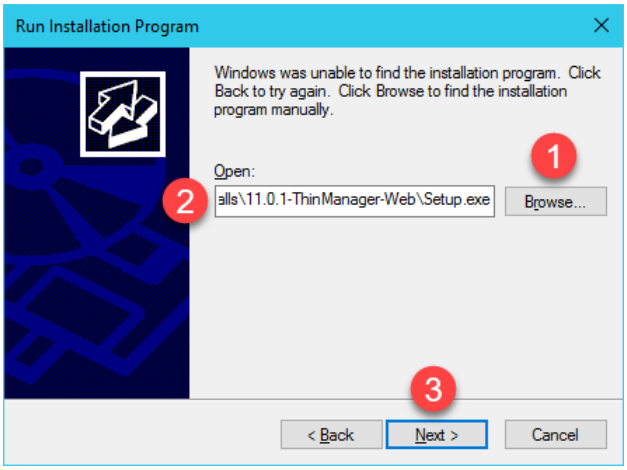
4. Click the **Next** button of the **Install Program From Floppy Disk or CD-ROM** wizard.



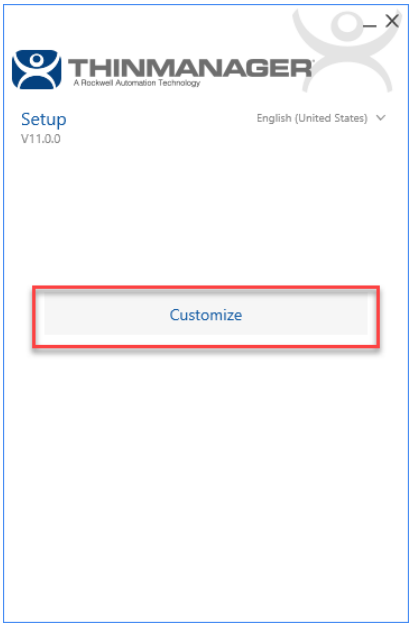
5. Click the **Browse…** button from the **Run Installation Program** page of the wizard.



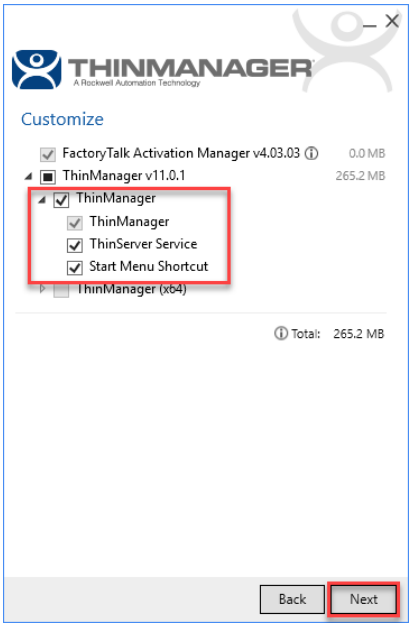
6. In the **Browse** dialog, browse to the folder **C:\Tools\Installs\11.0.1-ThinManager-Web**, select **Setup** and click **Open**. Click **Next>** to launch the ThinManager installation program.



7. Click the **Customize** button on the installer to set up the installation parameters.



8. Accept the default installation options to install the 32 bit version. Click **Next**.

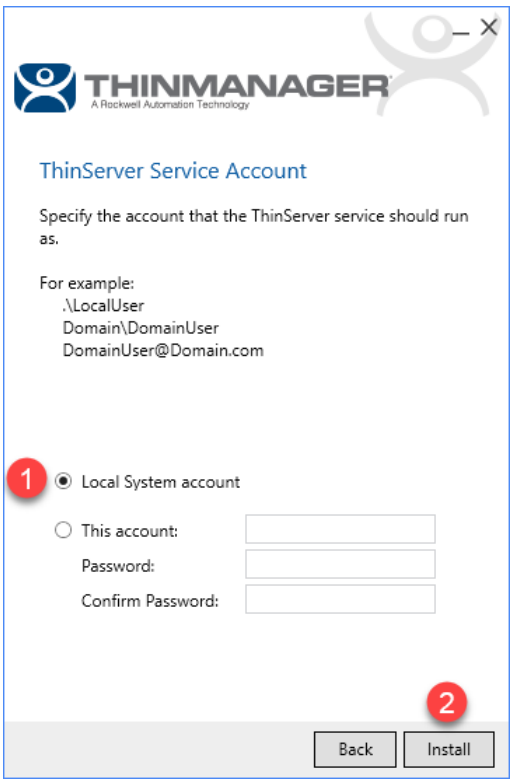


ThinManager v11 introduced support for FactoryTalk Activation. As this section will demonstrate, traditional ThinManager Master Licensing is still supported and is the default. In order to utilize FactoryTalk Activation, you must install FactoryTalk Activation Manager v4.03.03 or later, which has been pre-installed on your virtual machine to save time.

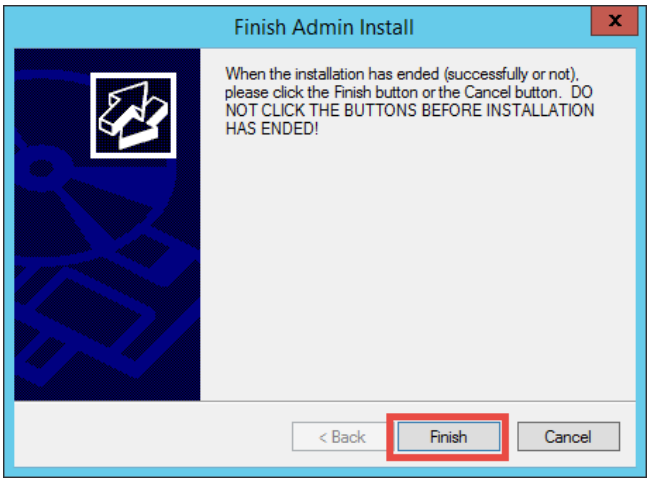
It should be noted that if you choose to install the x64 version of ThinManager you will be unable to preview IP cameras from the ThinManager user interface.

9. On the **ThinServer Service Account** page of the installation wizard, select **Local System account** and click the

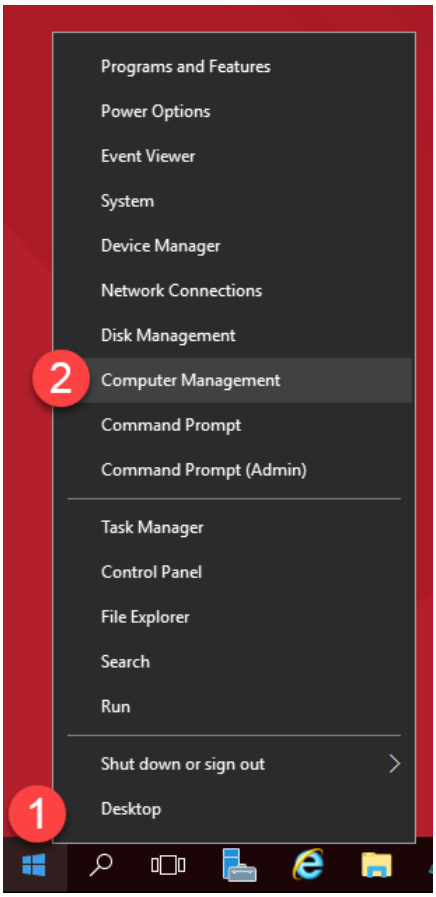
Install button.



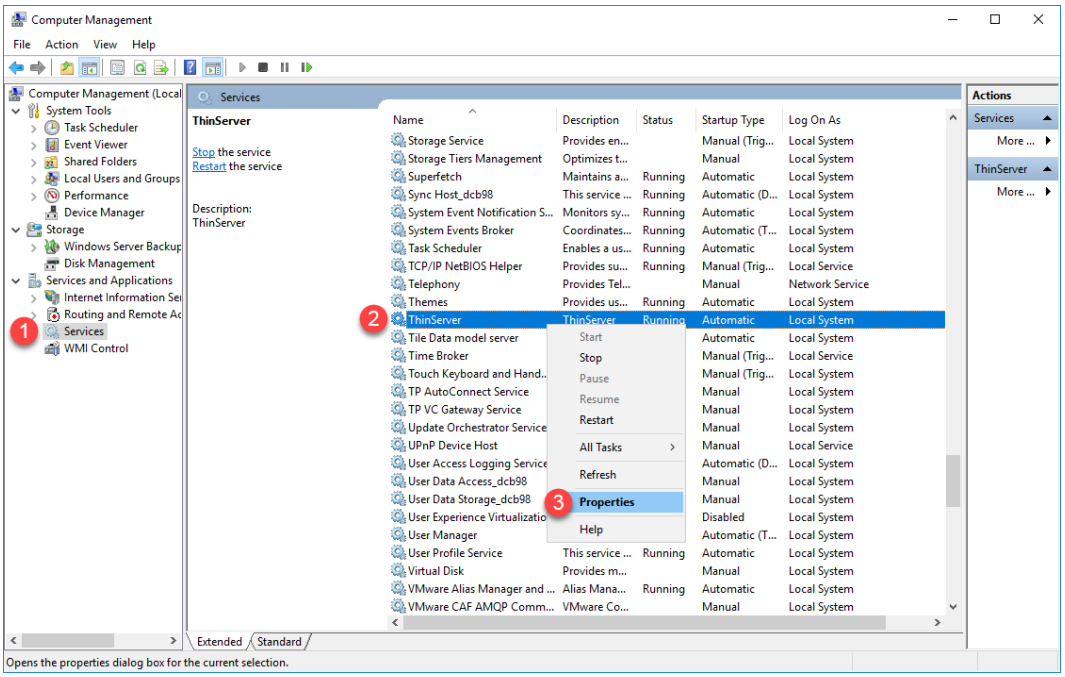
10. From the **End User License Agreements** page, click the **Accept all** button.
11. When the installation has finished click the **Close** button on the installer, followed by the **Finish** button on the Admin installer.



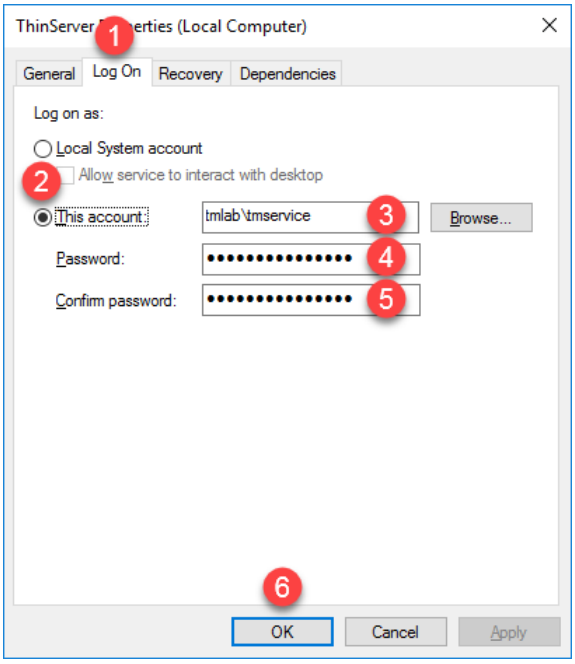
12. It is recommended to run the **ThinServer** service as a local **Administrator** account (in a domain environment, this would be a domain account that is a member of the local **Administrator** group). This account should also have local **Administrator permissions** on each **Remote Desktop Server** managed by ThinManager. In this lab, the **tmlab\tmservice** account has already been added to the local **Administrators** group on **RDS1** and **RDS2** for you. Let's now assign that account to the **ThinServer** service. Right click the **Windows Start** button and select **Computer Management**.



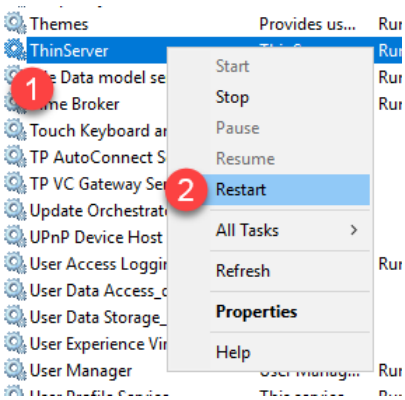
13. From the **Computer Management** console, expand the **Services and Applications** branch and select **Services**. From the Services list on the right side, scroll down to **ThinServer**, right click it and choose **Properties**.



14. From the **ThinServer Properties** window, select the **Log On** tab, then the **This account** radio button. Enter *tmlab\tmservice* in the **This account** textbox and *rw* in the **Password** and **Confirm Password** textboxes. Click the **OK** button. Click the **OK** button to the resulting message boxes.



15. Right click the **ThinServer** service one more time and select **Restart** in order to restart the service. Close the **Computer Management** console window. If still open, close the **Control Panel** as well.

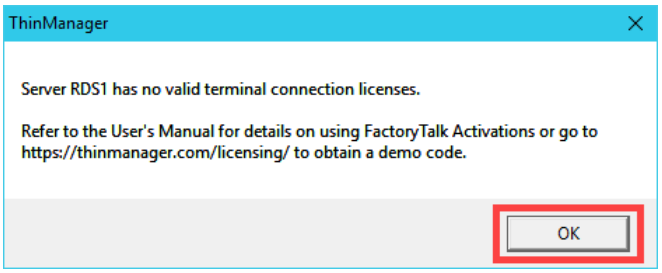


Apply FactoryTalk Activation for ThinManager

A ThinManager license/activation determines how many ThinManager terminals can be concurrently connected to ThinManager and whether ThinManager is enabled for **Redundancy**. **Redundancy** provides 2 installs of ThinManager whose configurations are automatically **synchronized**. **Redundancy** is different from **Failover**. **Failover** is included in every ThinManager license and provides the ability to automatically failover to multiple **Remote Desktop Servers** without any user intervention required at the client. **Automatic Remote Desktop Server Failover** will be demonstrated in Section 5. This lab will demonstrate how to setup **Redundancy**. In addition to the ThinManager installation just completed on **RDS1**, ThinManager has been pre-installed on **RDS2** for you.

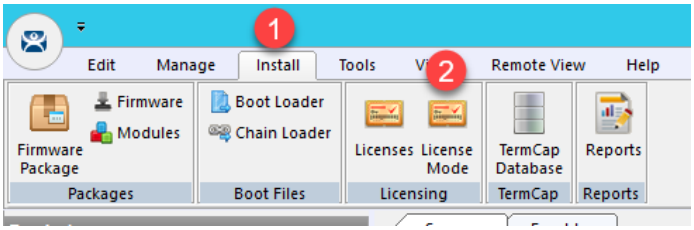
> Prior to version 11, ThinManager offered 2 **Redundancy** options: **Mirrored** and **Full**. To simplify, ThinManager now only offers **Full Redundancy**. If you are an existing **Mirrored Redundancy** user and are purchasing additional ThinManager licensing for your system, please contact insidesales@thinmanager.com to discuss upgrading your existing **Mirrored Redundancy** licensing to **Full Redundancy**.

1. From the **RDS1** virtual machine, double click the **ThinManager** shortcut on the desktop  .
2. Since we have yet to install a ThinManager license/activation, a message box alerts us. Click the **OK** button.

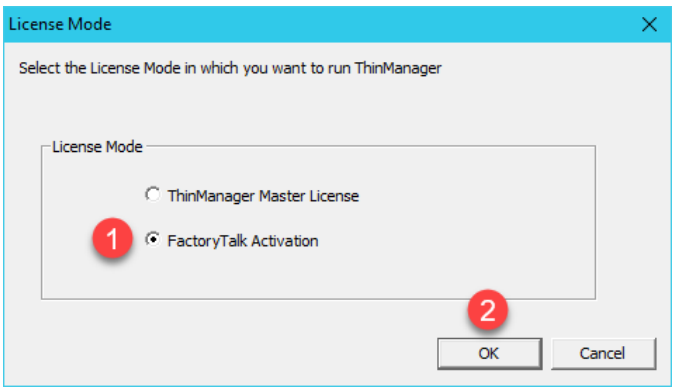


> As the message box indicates, a fully functional 30 day demo code can be obtained from the ThinManager website at http://downloads.thinmanager.com.

3. From the ThinManager **Admin Console**, click the **Install** ribbon, followed by the **License Mode** icon.

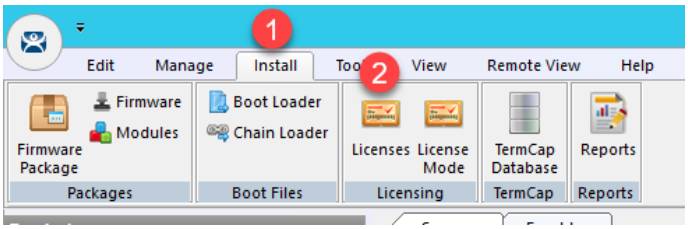


4. From the **License Mode** window, select the radio button for **FactoryTalk Activation** and click **OK**.

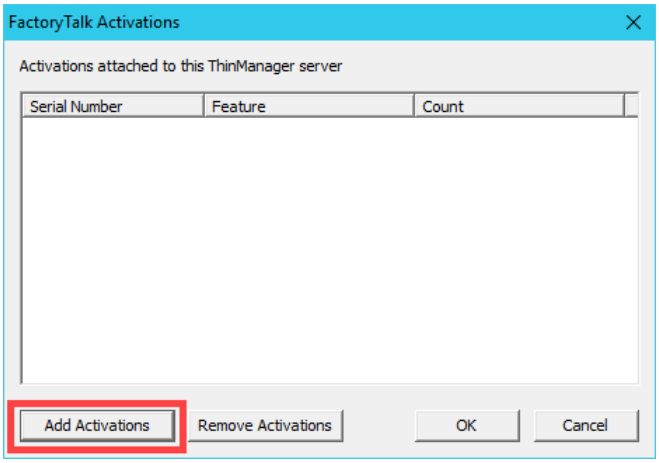


> As previously mentioned, ThinManager v11 adds support for FactoryTalk Activations as an alternative to traditional Master Licensing. Only one licensing mode can be enabled at a time. When using FactoryTalk Activation, licenses are downloaded to a machine in the same way as all other FactoryTalk activated products. Once an activation is downloaded, it must be assigned to a ThinManager server. For more information, refer to AID1083531 - FactoryTalk Activation with ThinManager. GoldMaster Activations are supported in this mode as well. For more information, please refer to AID1083532 - ThinManager Support for GoldMaster Activation.

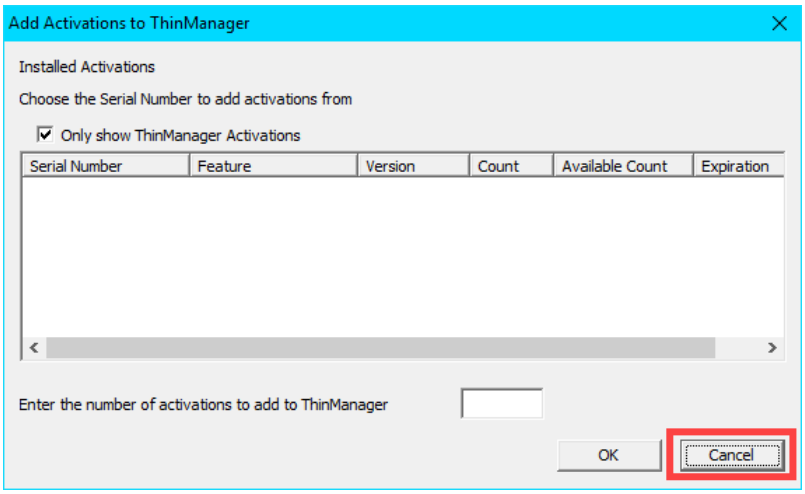
5. From the **Admin Console**, return to the **Install** tab and this time click the **Licenses** button.



6. From the **FactoryTalk Activations** window, click the **Add Activations** button.



7. With the way the Cloud lab images are hosted in the Amazon Elastic Cloud, we were unable to maintain the CodeMeter-based ThinManager FactoryTalk Activation once the Cloud lab image was launched, so you will not see any available activations. Click the **Cancel** button, then click the **Cancel** button again.



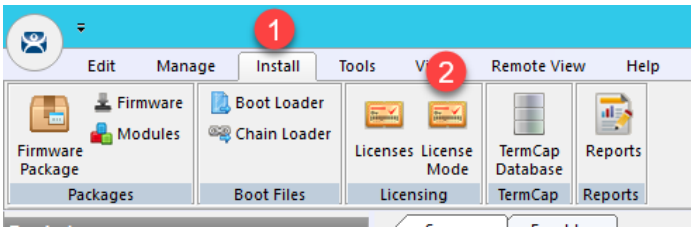
By default, ThinManager terminal connection license packs cannot be split up and applied to separate installations. If your ThinManager deployment requires a license pack to be split up, please inquire about ThinManager FLEX licensing, which enables this capability.

With **FactoryTalk Activation** and **ThinManager Redundancy**, you will need to assign an activation to both ThinManager installations. When you purchase a ThinManager license with **FactoryTalk Activation**, it will include an install count of 2 for this purpose – one for the **Primary ThinManager Server** and one for the **Secondary ThinManager Server**. Therefore, with a FactoryTalk Activated ThinManager license in a redundant deployment, you would follow the above steps on the **Primary ThinManager Server** as well as the **Secondary ThinManager Server**.

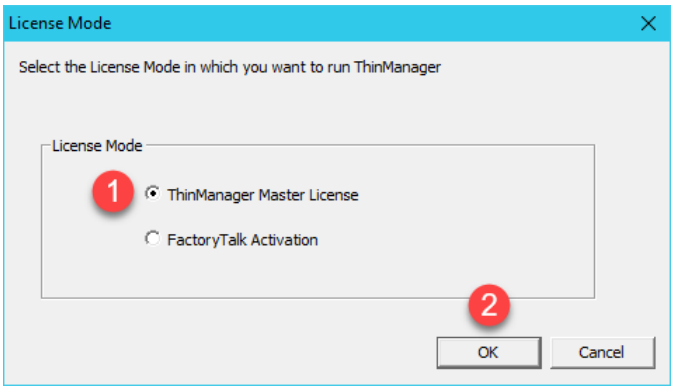
Apply Master License for ThinManager

With **ThinManager Traditional Master Licensing** in a redundant deployment, a single redundant license is automatically shared between redundant partners.

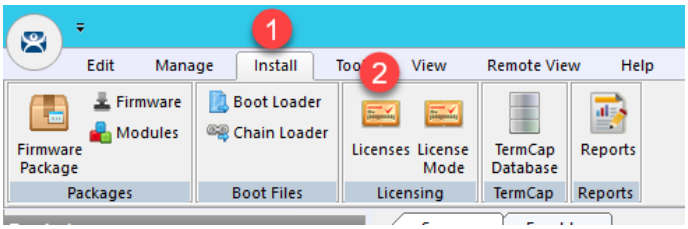
1. From the ThinManager **Admin Console**, click the **Install** ribbon, followed by the **License Mode** icon.



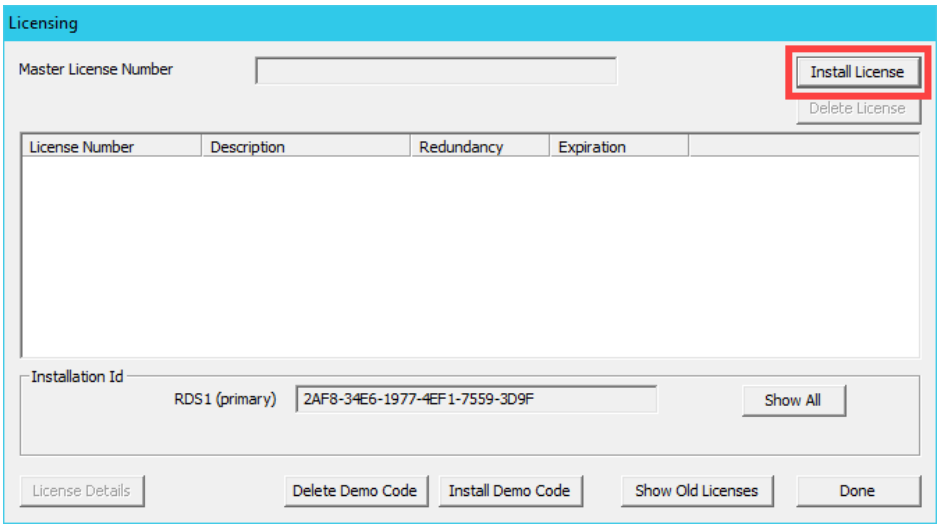
2. From the **License Mode** window, select the radio button for **ThinManager Master License** and click **OK**.



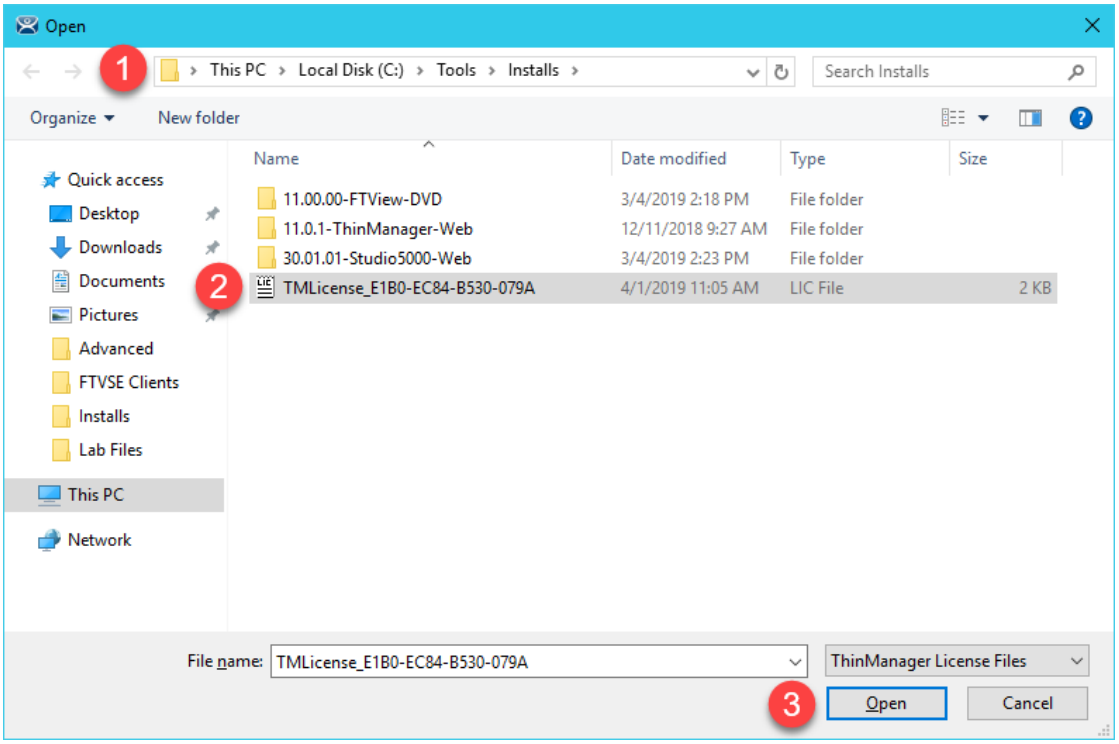
3. From the **Admin Console**, return to the **Install** tab and this time click the **Licenses** button.



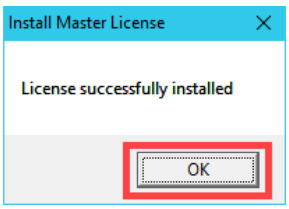
4. From the **Licensing** window, click the **Install License** button.



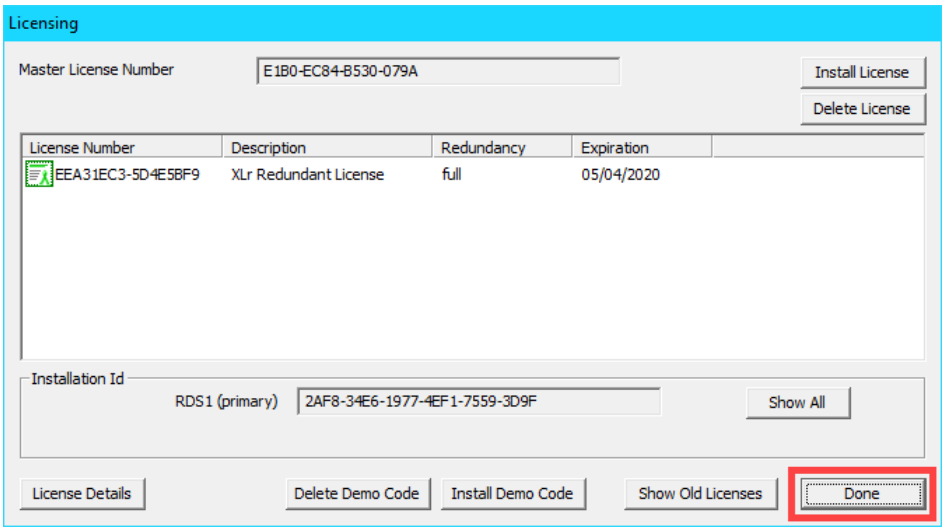
5. From the **Open** dialog, navigate to **C:\Tools\Installs** and select the **TMLicense_E1B0-EC84-B530-079A** file. Click the **Open** button.


Open
1
This PC › Local Disk (C:) › Tools › Installs ›
Search Installs
Organize
New folder
Quick access
Desktop
Downloads
Documents
Pictures
Advanced
FTVSE Clients
Installs
Lab Files
This PC
Network
Name
Date modified
Type
Size
11.00.00-FTView-DVD
3/4/2019 2:18 PM
File folder
11.0.1-ThinManager-Web
12/11/2018 9:27 AM
File folder
30.01.01-Studio5000-Web
3/4/2019 2:23 PM
File folder
2
TMLicense_E1B0-EC84-B530-079A
4/1/2019 11:05 AM
LIC File
2 KB
File name:
TMLicense_E1B0-EC84-B530-079A
ThinManager License Files
3
Open
Cancel

6. Click the **OK** button from the ensuing confirmation dialog box.

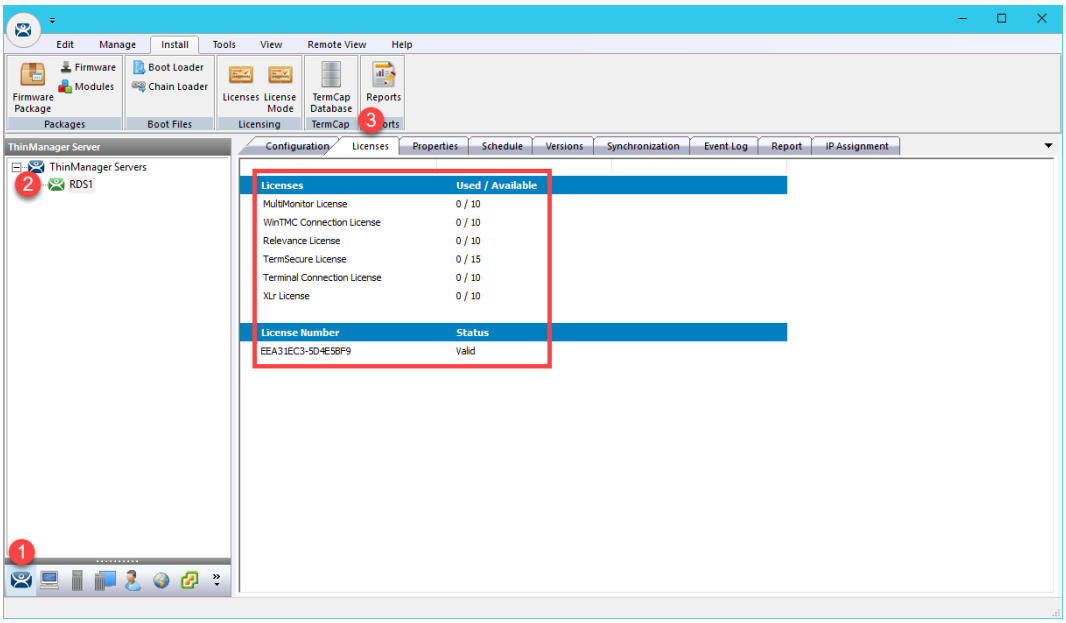


7. From the **Licensing** window, click the **Done** button.



8. **Close** the ThinManager **Admin Console** in order for ThinManager to properly recognize the features of the license and **Restart** it.

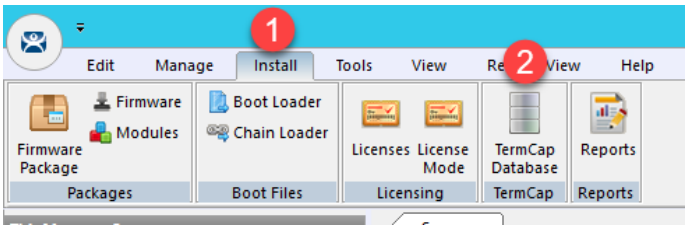
9. From the **Admin Console**, click the **ThinServer** icon in the tree selector, followed by **RDS1** from the **ThinManager Servers** tree, then the **Licenses** tab.



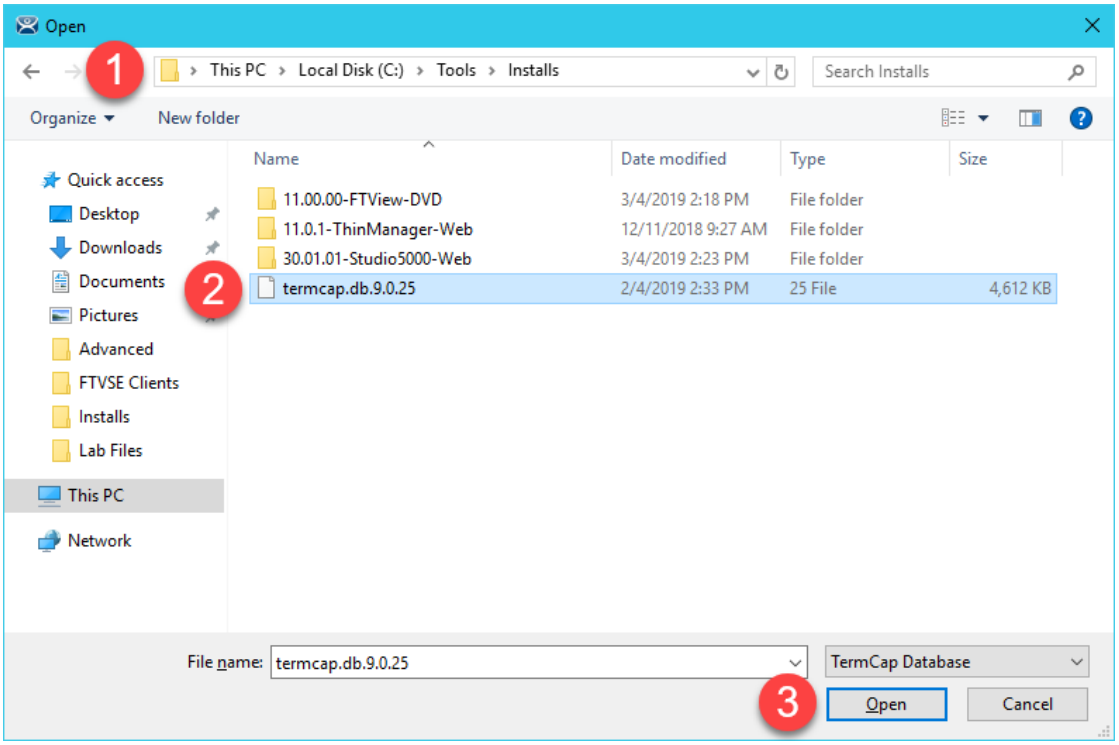
Update TermCap Database

Every version of ThinManager ships with an up-to-date version of the **Terminal Capabilities Database** (**TermCap**) at the time of release. The **TermCap Database** provides ThinManager with the configuration parameters for each thin client model. At each terminal connection, the **TermCap** database is utilized to perform an integrity check. If the configuration does not match the terminal specifications, ThinManager may reconfigure the terminal to an acceptable set of parameters. The images used in this lab were built with an up-to-date version of the **TermCap,** so an update is technically not necessary for this deployment of ThinManager, but it is worthwhile to become familiar with the process. In the following steps you will apply the latest **TermCap Database** to this installation.

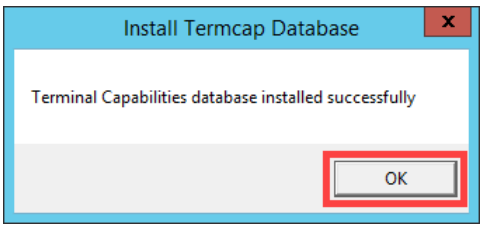
1. From ThinManager, click the **Install** ribbon followed by the **TermCap Database** icon.



2. From the **Open** dialog box, browse to **C:\Tools\Installs** and select the **termcap.db.9.0.25** file and click the **Open** button.



3. You should receive a successful confirmation message. Click the **OK** button.



This completes the section **Installation and Configuration of FactoryTalk View Site Edition Client on Remote Desktop Server**. Continue to the next section to start exploring the ThinManager fundamentals, **Display Servers**, **Display Clients** and **Terminals**.

Section 4: 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**X**ecution **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

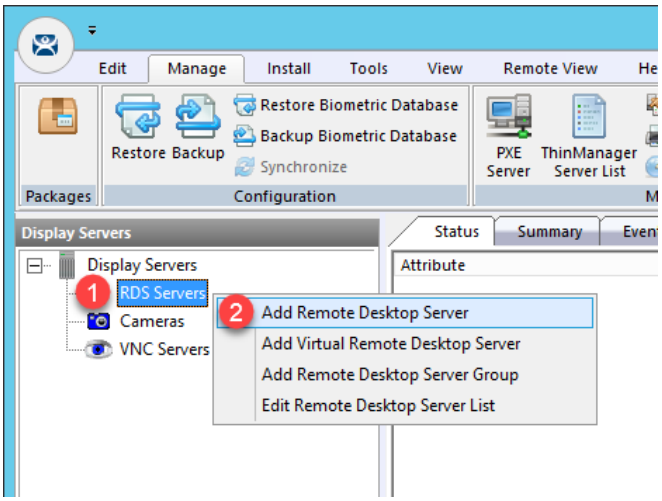
Register **RDS1** and **RDS2** as Display Servers in ThinManager.

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

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

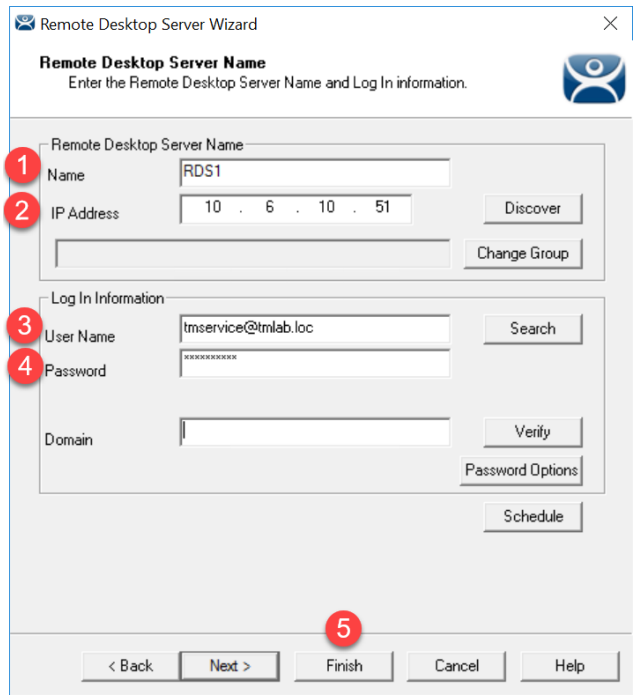
   The tree selector can be expanded or collapsed using the bar above directly above it.

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.



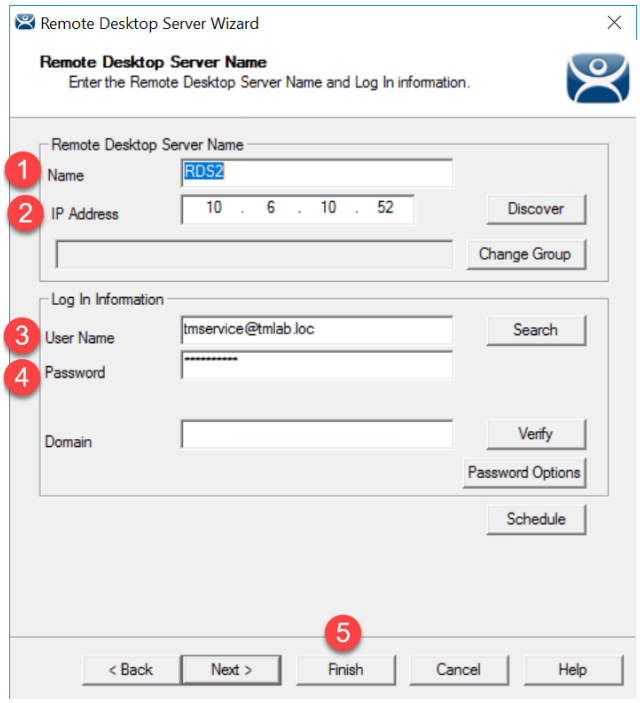
4. From the **Introduction** page of the **Remote Desktop Server Wizard**, click the **Next** button.
5. From the **Remote Desktop Server Name** page of the wizard, type *RDS1* in the **Name** field.
6. Click the **Discover** button. If the name is successfully resolved, the IP address of **RDS1** should 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.

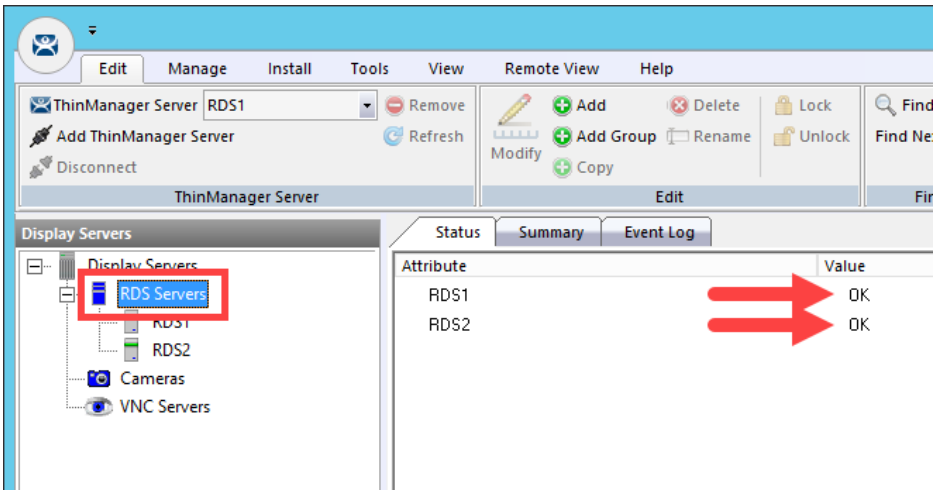


11. **RDS1** should now be added to the Remote Desktop Servers group. You may have to click the Display Servers branch to refresh the Remote Desktop Servers group.

12. Repeat steps 3 through 11, but this time register **RDS2**.



13. 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.

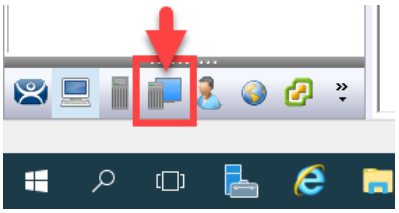


The credentials entered when configuring a Remote Desktop Server must have Administrative rights on the Remote Desktop Server. This is required for SmartSession and to populate the User, Sessions and Process tabs of the details pane, which are available when you click on the Remote Desktop Server of 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.

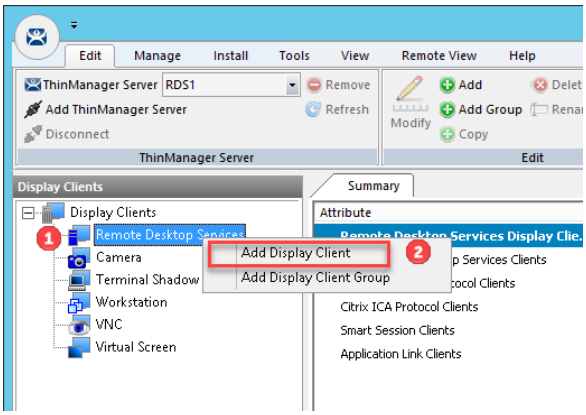
In order for ThinManager to connect to a Remote Desktop Server (like RDS1 in the example above), the provided Administrative credentials for that Remote Desktop Server in ThinManager should also be used as the ThinServer service credentials. The ThinServer service credentials on RDS1 are in fact configured 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

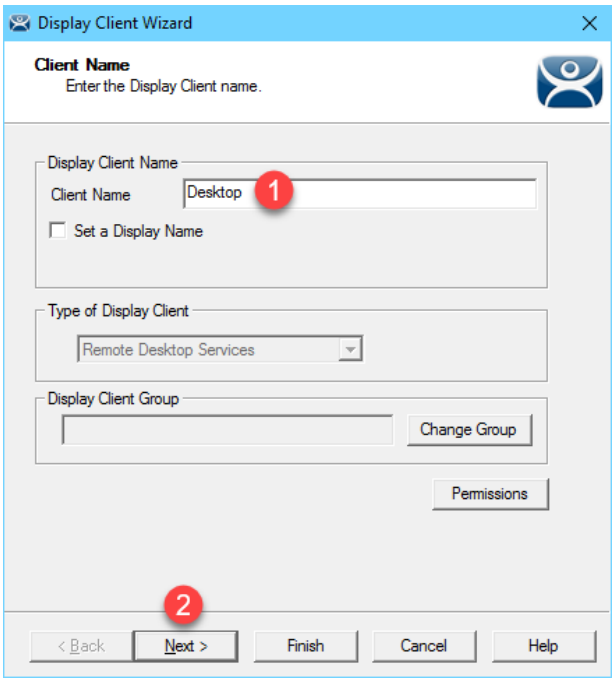
1. Click the **Display Clients**  icon from the ThinManager tree selector.



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**.

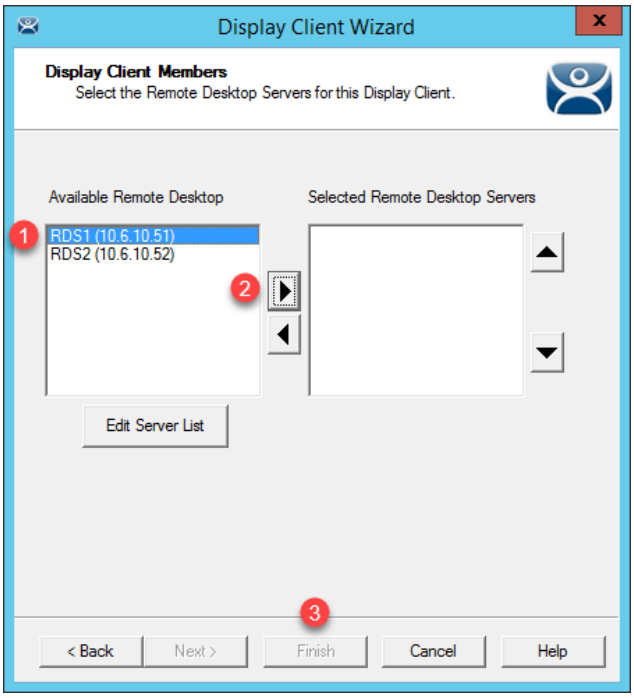


3. Type *Desktop* as the **Client Name** on the **Client Name** page of the wizard. Click the **Next** button.

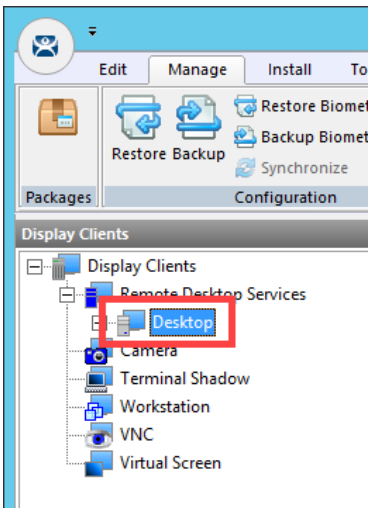


> The **Set a Display Name** checkbox is new for ThinManager 11 and provides the ability to assign an Alias to a Display Client that will be shown at the Terminal in the Display Client Selector instead of the **Client Name** entered. This feature requires firmware package 8.2 or newer. Firmware packages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

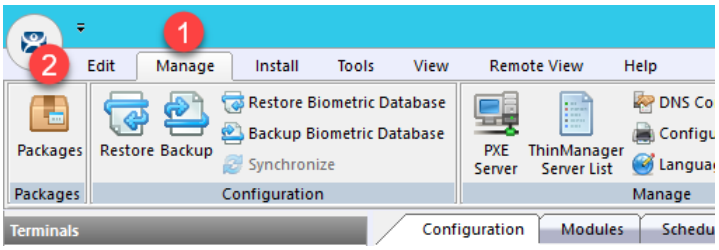


New in ThinManager 11, you can now create **Display Client Groups**. **Display Client Groups** provide the ability to better organize large quantities of content. You can create **Display Client Groups** much like folders in Windows Explorer, and then add **Display Clients** to the **Display Client Group**.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

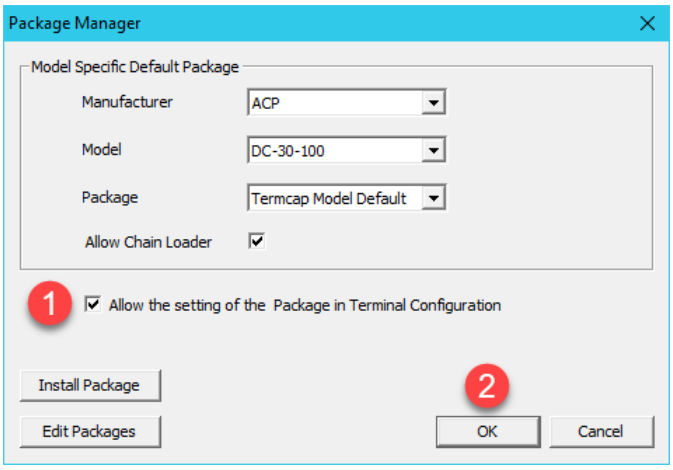
Create a Terminal Profile

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.

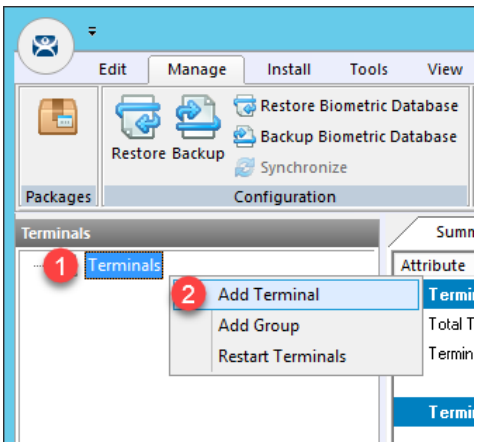


2. The **Package Manager** window enables firmware packages to be assigned in 2 different ways – by terminal model or on a terminal by terminal basis. We are going to utilize the latter. To enable this capability, check the **Allow the setting of the Package in Terminal Configuration** checkbox. Click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

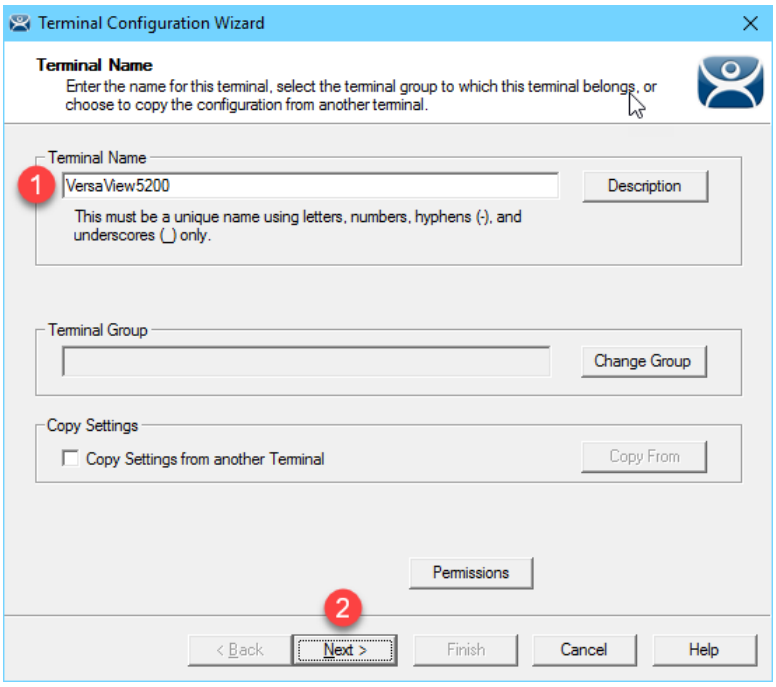


3. Click the **Terminals** icon  from the ThinManager tree selector.

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

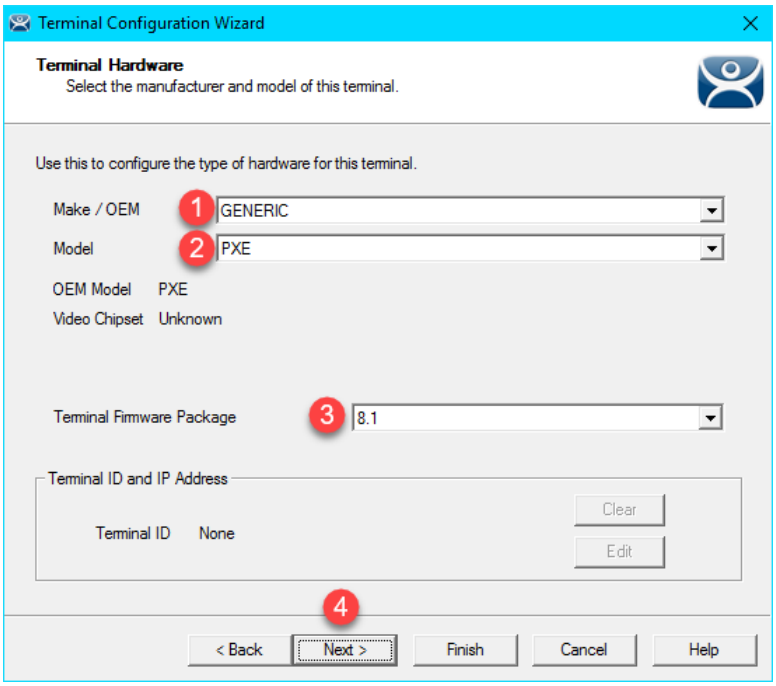


5. Type *VersaView5200* as the **Terminal Name** on the **Terminal Name** page of the wizard. Click the **Next** button.

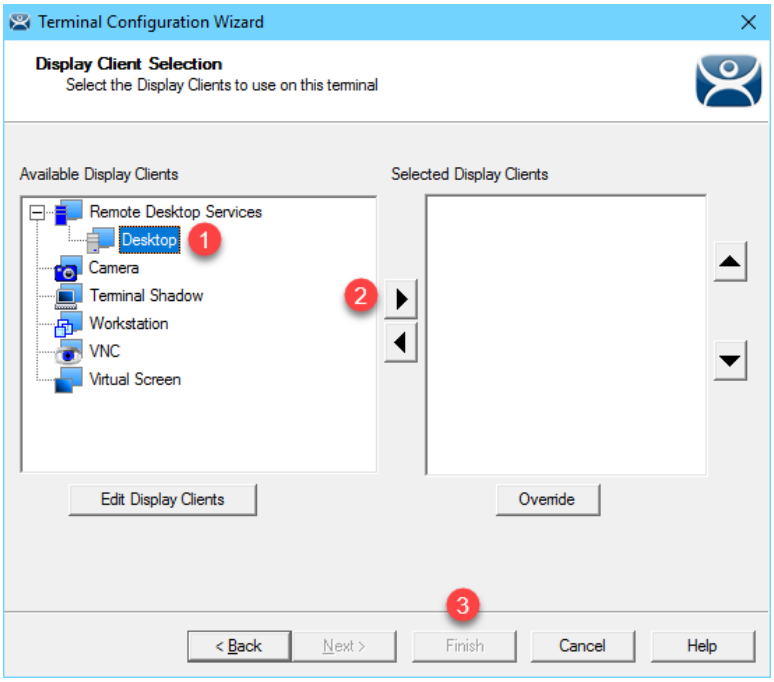


Clicking the Description button on the **Terminal Name** page of the wizard will not only allow you to enter a Description for the terminal, but also allow you to create **Custom Variables** for the terminal. **Custom Variables** were added in ThinManager 8.1. The **Custom Variable** can be used in the **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**.

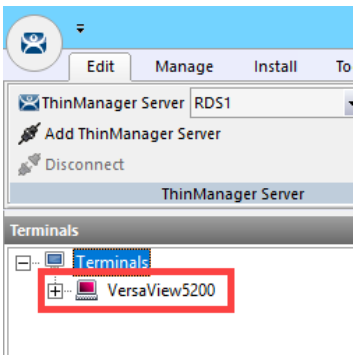
6. Accept the defaults of **Generic / PXE** from the **Make / OEM** and **Model** drop down lists, respectively. Select **8.1** from the **Terminal Firmware Package** drop down list. Click the **Next** button.



7. Click the **Next** button on the **Terminal Options** page of the wizard.
8. Click the **Next** button on the **Terminal Mode Selection** page of the wizard.
9. 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.



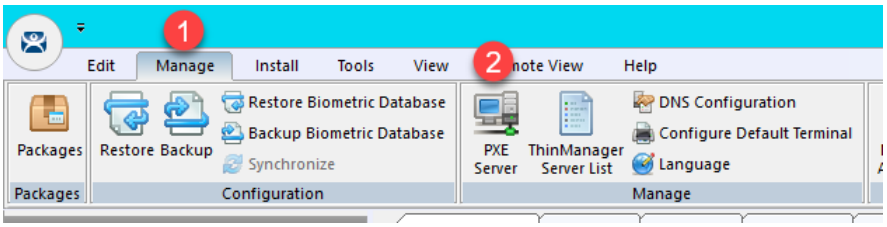
You can also create **Terminal Groups** in ThinManager. **Terminal Groups** provide 2 key capabilities: (1) terminal organization and (2) property inheritance. With terminal organization, you can create **Terminal Groups** much like folders in Windows Explorer, and then add **Terminals** to the **Terminal 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).

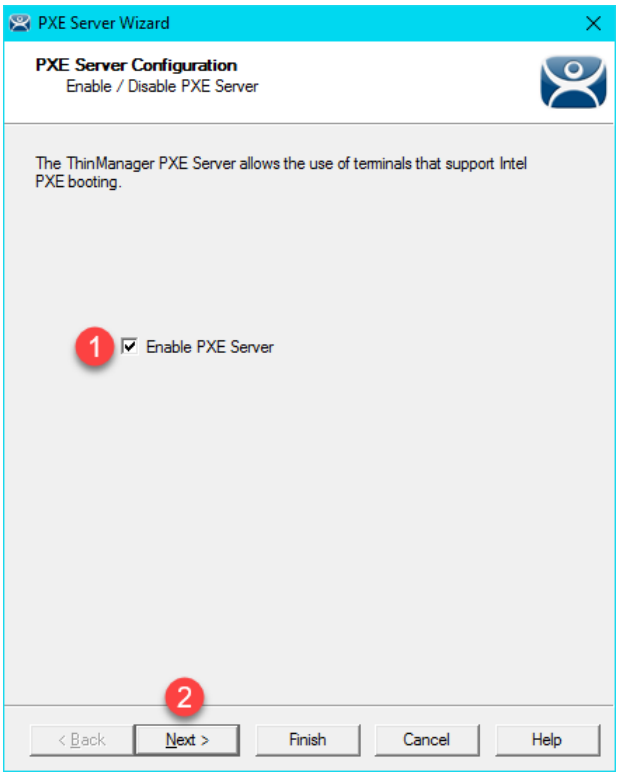
Configure PXE Server

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.

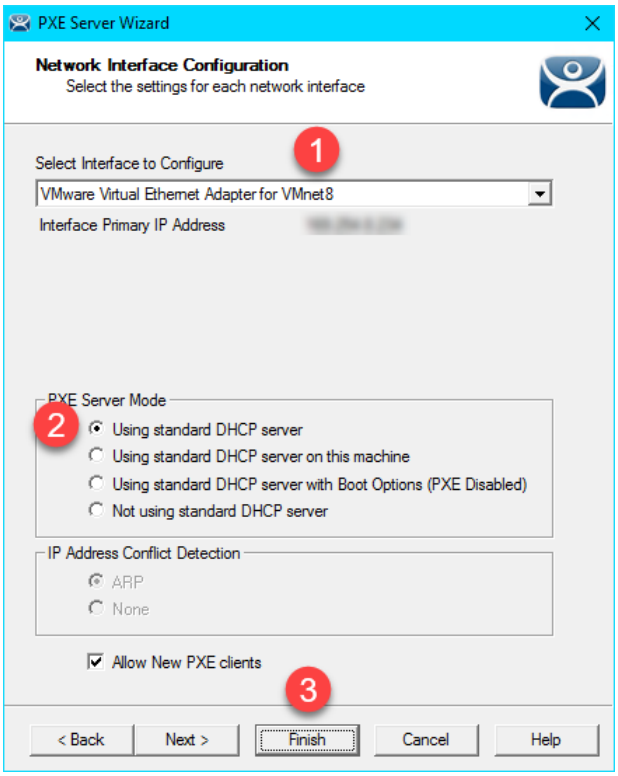
1. From the **ThinManager Admin Console**, select the **Manage** ribbon, followed by the **PXE Server** icon.



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



3. From the **Network Interface Configuration** page of the wizard, make sue **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:

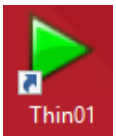
1. **Using standard DHCP server** – choose this when you have an existing DHCP server that you want to use for PXE, but you want ThinManager to provide the additional boot details, like the IP addresses of the ThinManager Server(s) and the name of the boot file. This is the preferred choice if you are using an existing DHCP server.
2. **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.
3. **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.
4. **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.

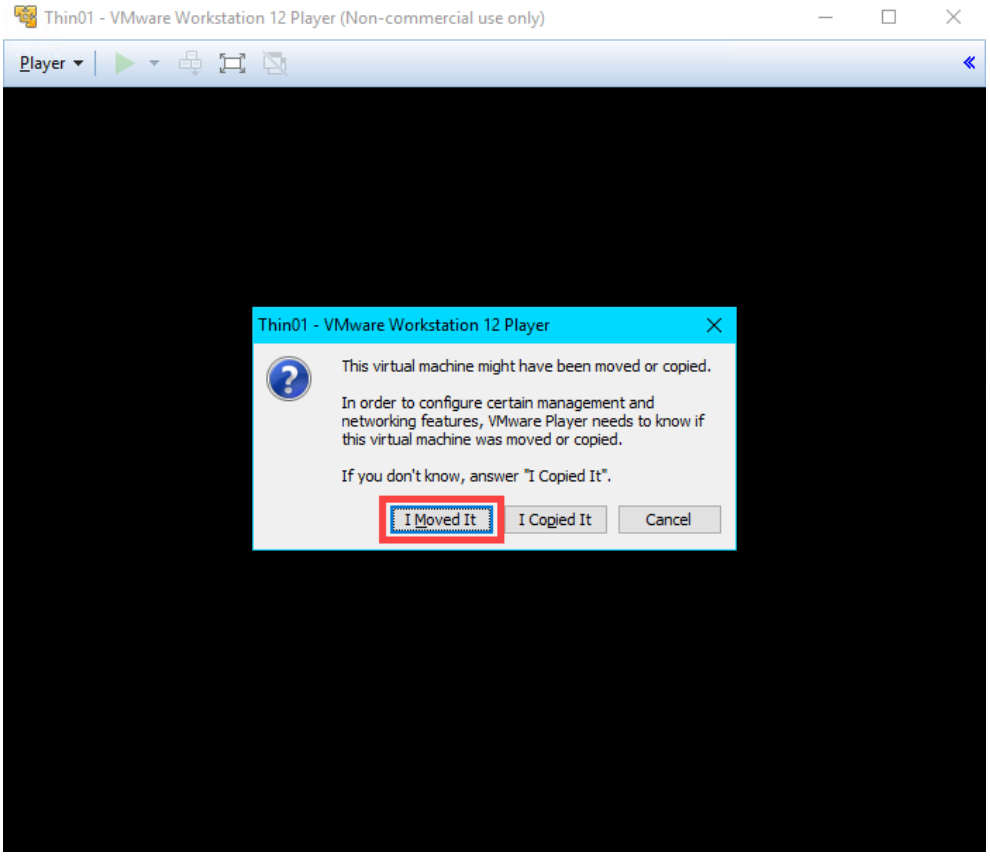


NOTE: Do not use the **VMWare Full Screen** option, as it has proven to be somewhat unstable in the cloud. It is ok to maximize the window.

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**.

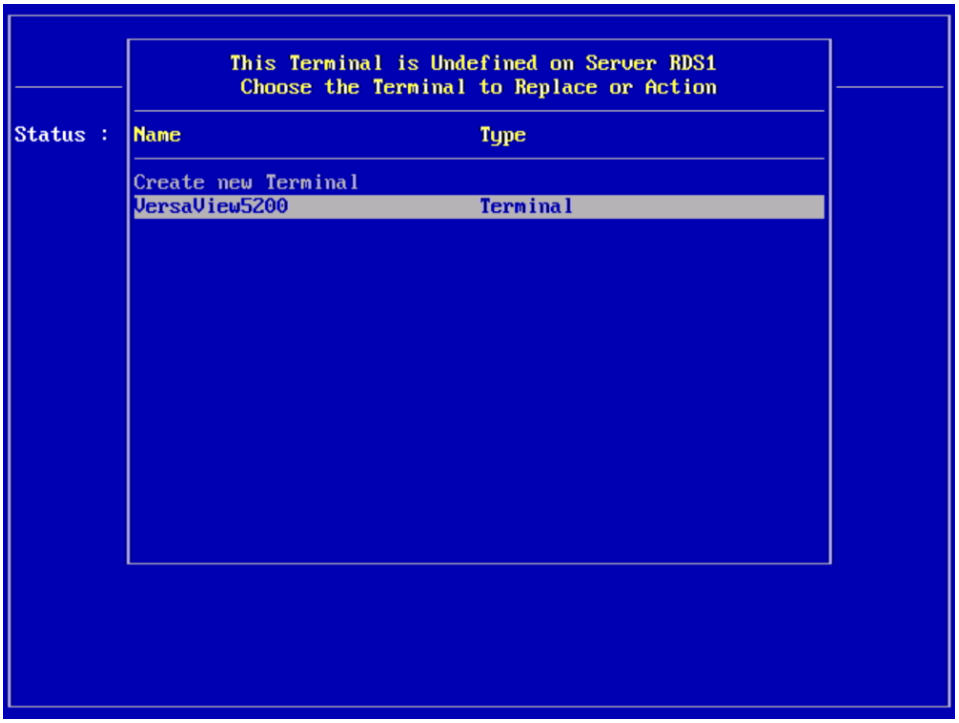
Since VMWare Tools cannot be installed within the virtual thin clients, the mouse pointer will get locked within each virtual machine when one of the virtual thin clients is active. To return the mouse pointer to the host, hit the CTRL+ALT key sequence.

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.

3. 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.

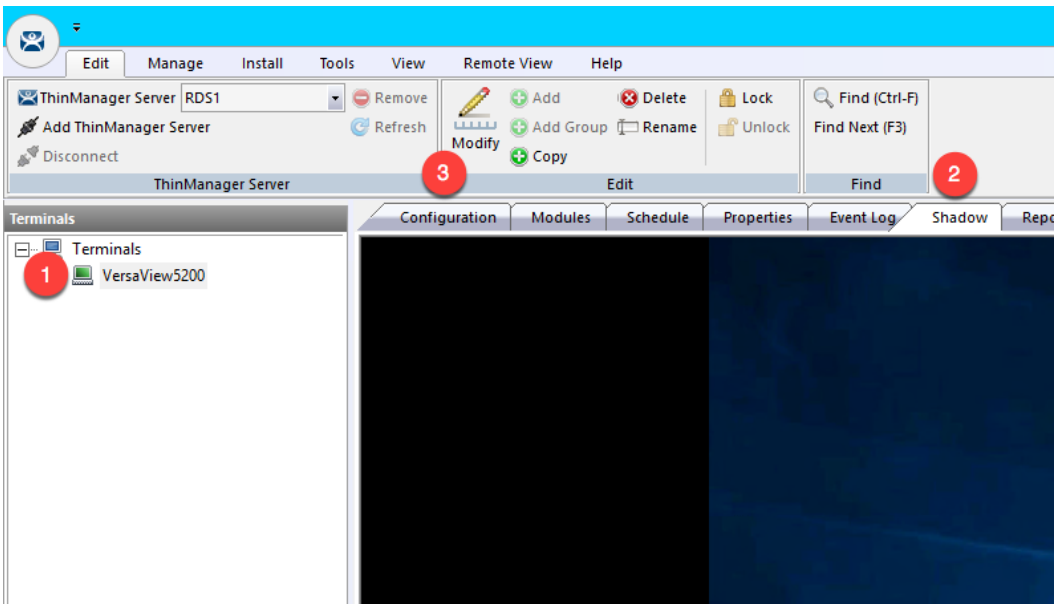
Additionally, you can control whether a Terminal Profile becomes available in this selection list. By default, a Terminal Profile becomes available for assignment when its associated terminal is offline. The **Allow replacement at terminal if off line** setting can be found on the **Terminal Options**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

4. 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**.

Checkpoint Question: https://thinmanager.com/cloudlabs/section04/

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 5: Configuring ThinManager Application Link and Failover for FactoryTalk View SE

Overview

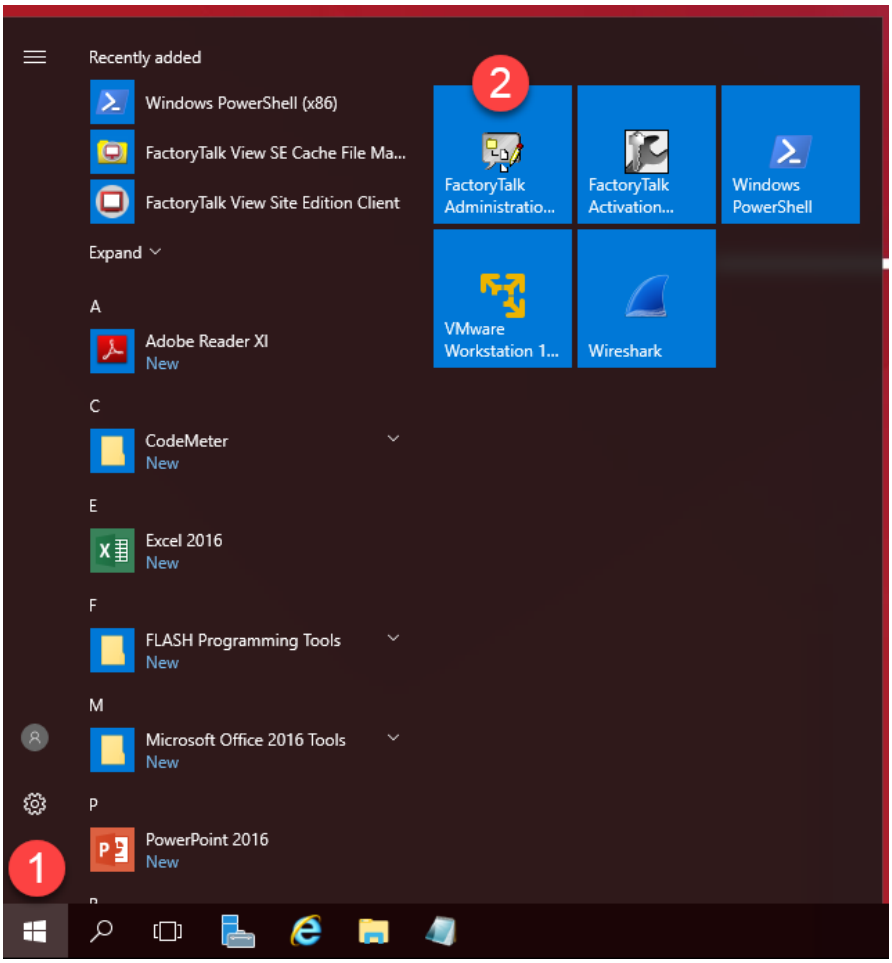
In the last lab section, you successfully delivered a Windows Desktop to the a virtual thin client using ThinManager. Typically, we go through great lengths to actually prevent access to the Windows Desktop on the plant floor, which is one reason why VDI is not always the best option for plant floor 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

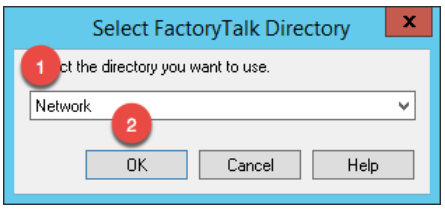
Add Terminal Names to FactoryTalk Directory

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.

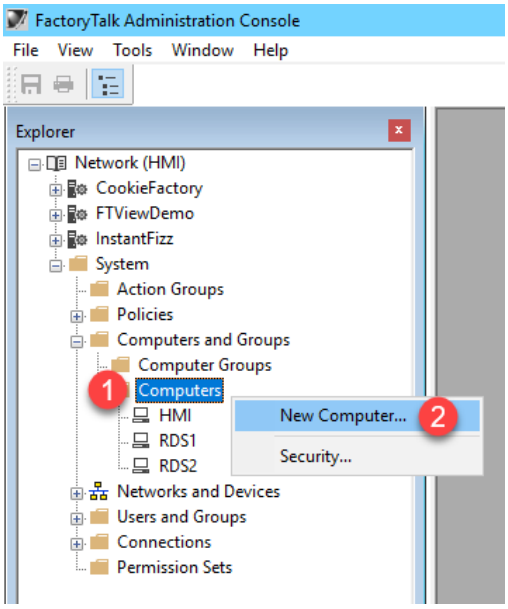
1. Click the **Windows Start** button from the **RDS1** host image – **NOT** the shadowed Desktop delivered to the thin client or the thin client itself.



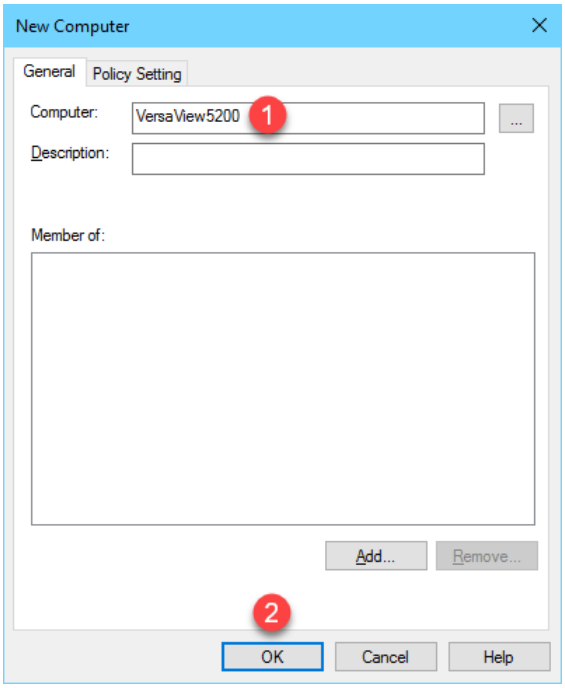
2. On the **Select FactoryTalk Directory** dialog, make sure **Network** is selected and click the **OK** button.



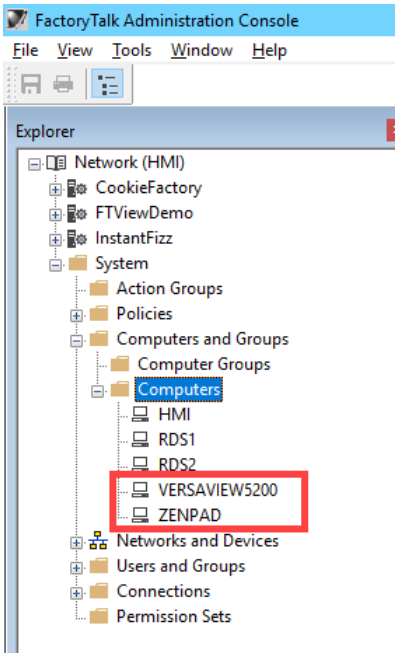
3. In the **Explorer** view, browse to **Network (THIS COMPUTER) →System→Computers and Groups→Computers**, right click **Computers** and select **New Computer…** from the menu.



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



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

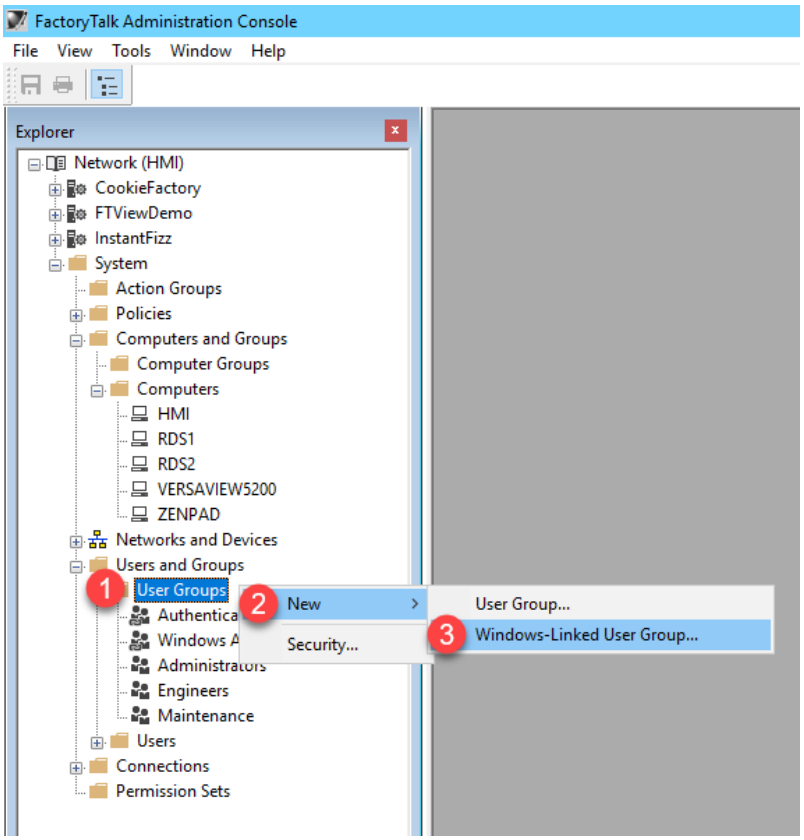


6. Keep the **FactoryTalk Administration Console** open for the next section.

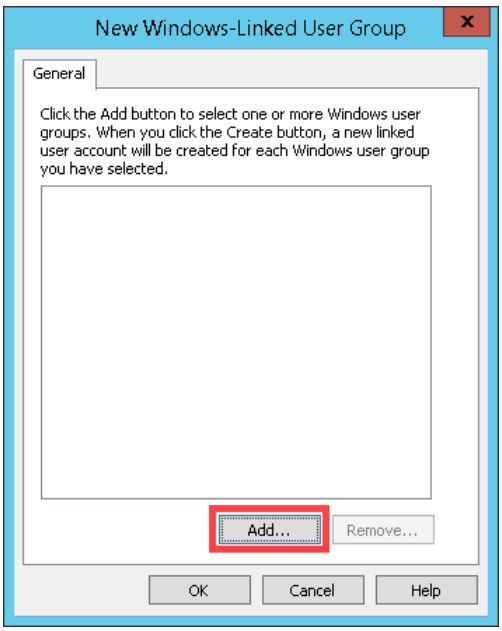
Add Windows Linked User Group to FactoryTalk Directory

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.

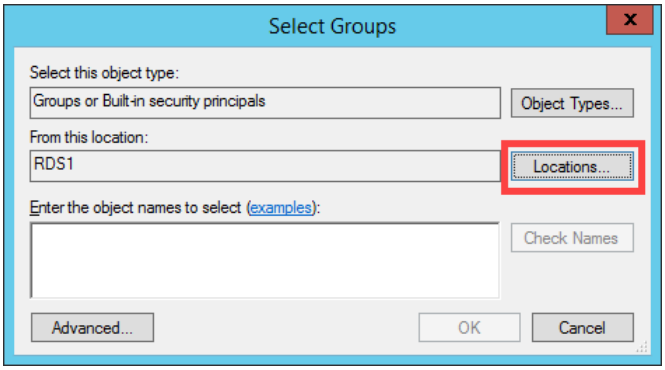
1. In the **Explorer** view, browse to **Network (THIS COMPUTER) →System→Users and Groups→User Groups**, right click **User Groups** and select **New | Windows-Linked User Group…** from the menu.



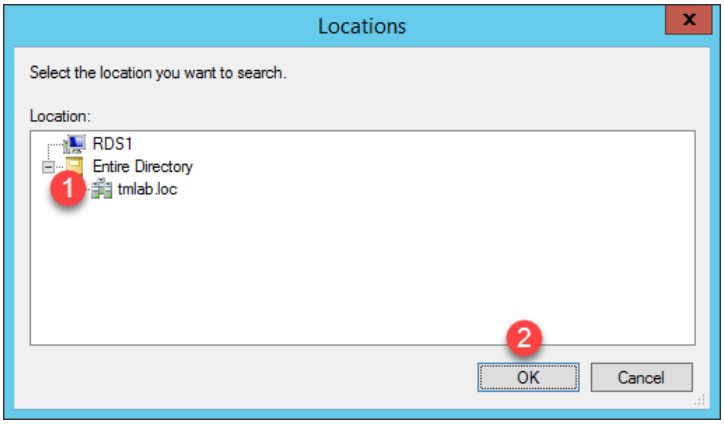
2. From the **New Windows-Linked User Group** popup, click the **Add** button.



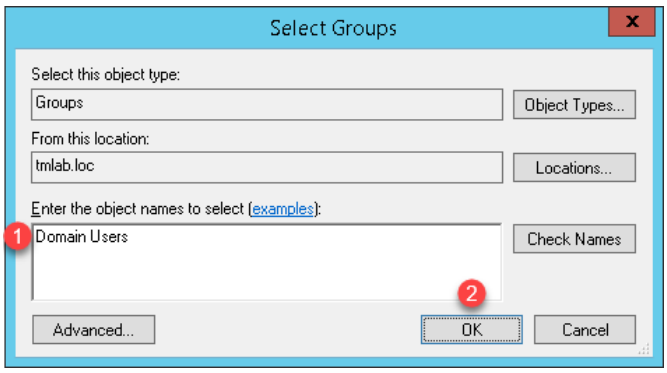
3. By default, this dialog box will show the local computer's user and groups, but we want to browse the **TMLAB** domain. From the **Select Groups** window, click the **Locations…** button.



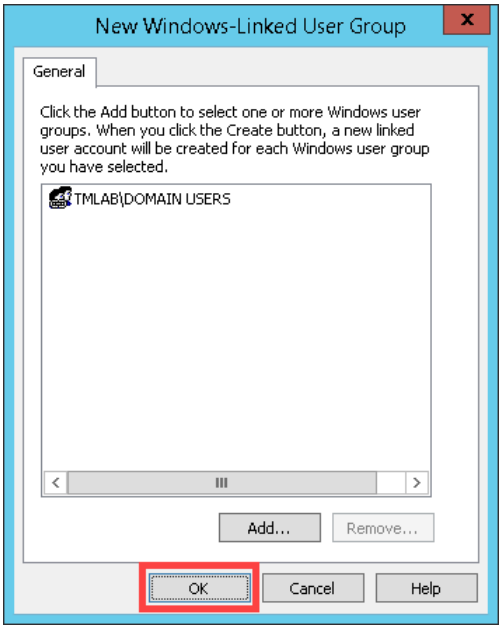
4. From the **Locations** selection box, expand the **Entire Directory** item and select the **tmlab.loc** item. Click the **OK** button.



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.

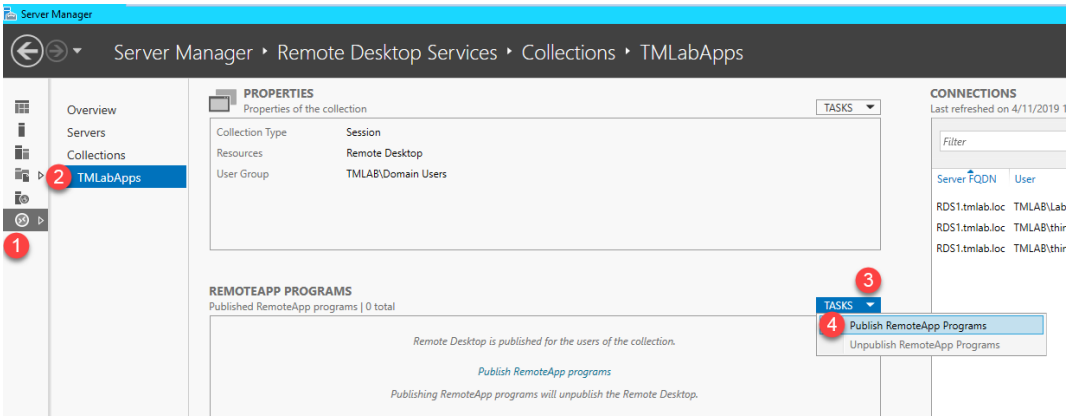
Create a RemoteApp for FactoryTalk View SE

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.

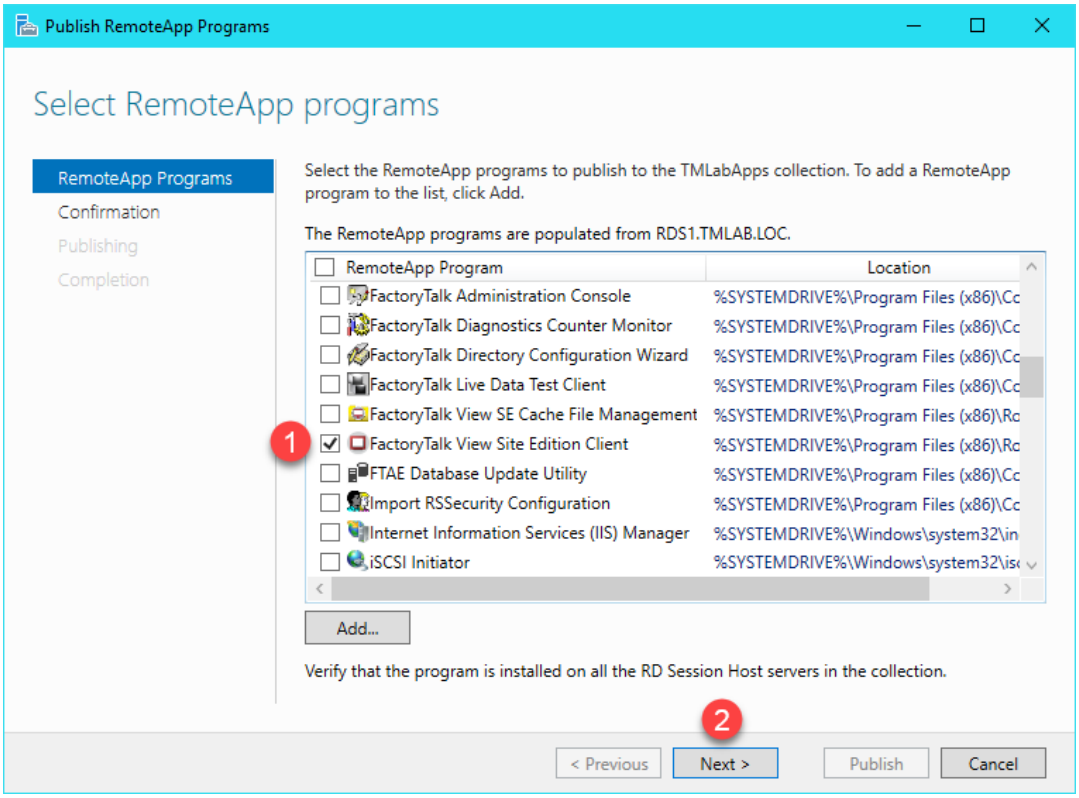
> While it is recommended that this default security measure be maintained, it can also be disabled through Local or Group Policy (from the Group Policy Editor: Default Domain Policy | Computer Configuration | Policies | Administrative Templates | Windows Components | Remote Desktop Services | Remote 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. **<u>MAKE SURE YOU CLICK THE SERVER MANAGER ICON ON THE RDS1 IMAGE AND NOT THE SHADOW OF THE THIN CLIENT.</u>**
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.

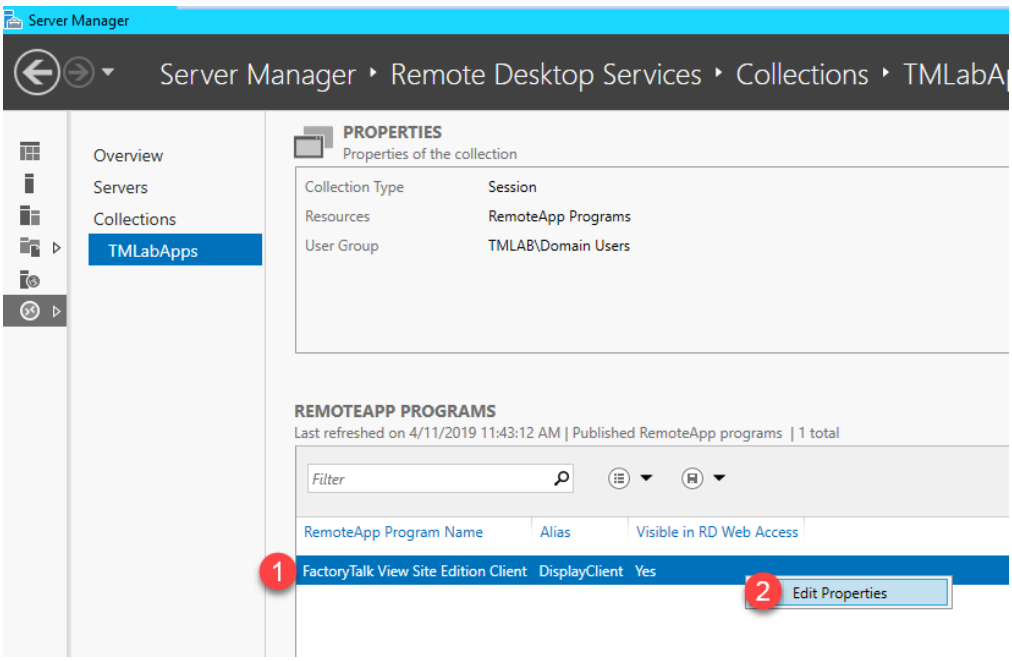


4. From the **Publish RemoteApp Programs** dialog, scroll down and check the **FactoryTalk View Site Edition Client** list item, followed by **Next>**.

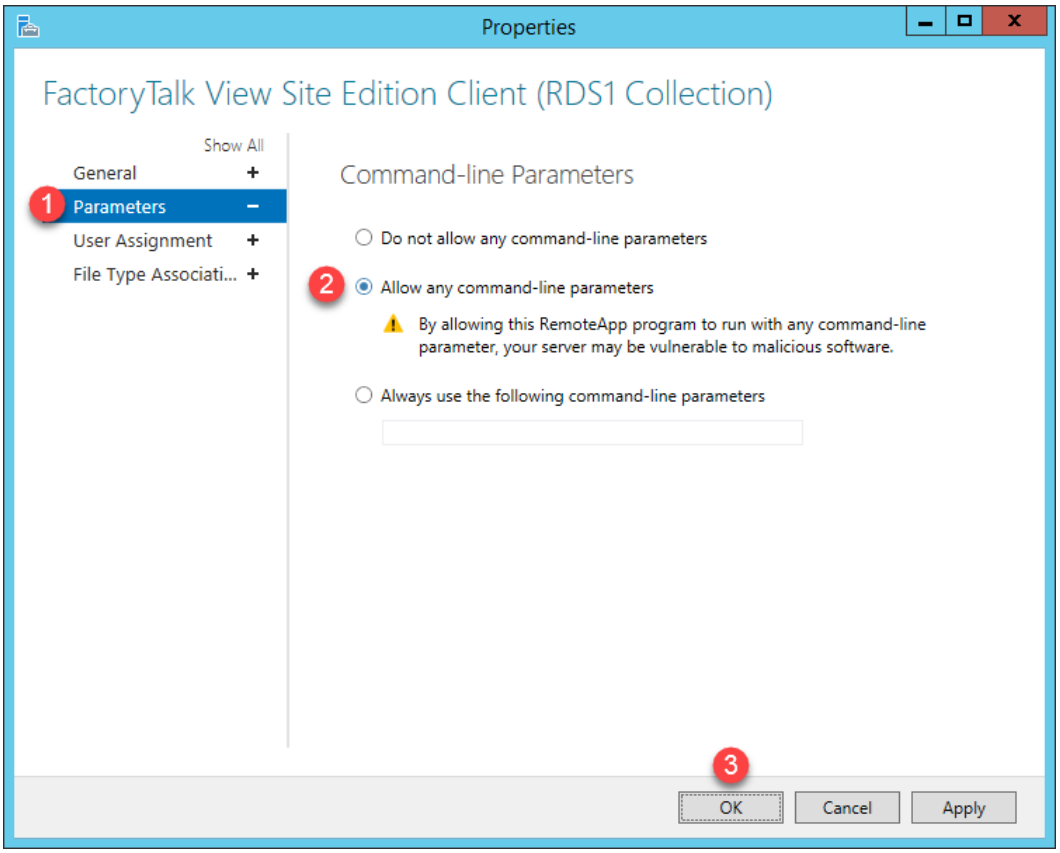


5. Click the **Publish** button on the **Confirmation** page.
6. Once **Status** changes to **Published**, click the **Close** button.

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



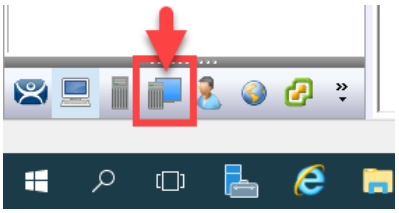
8. Select the **Parameters** panel item and then select the **Allow any command-line parameters** option. Click the **OK** button and the close **Server Manager**.



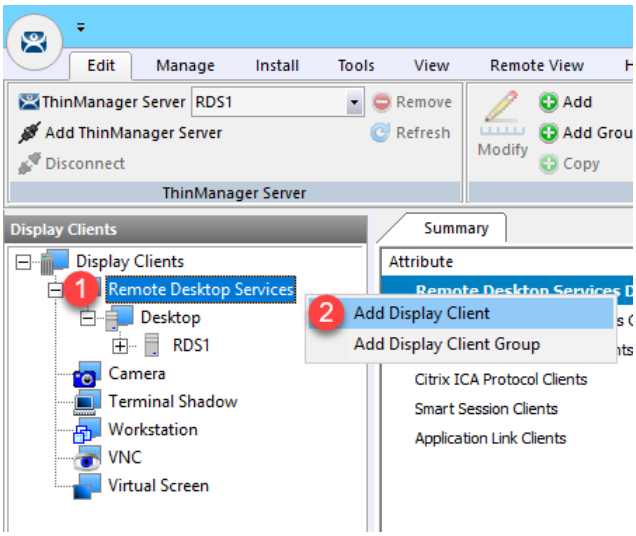
If your RemoteApp requires command line parameters, then selecting Allow any command-line parameters is less than secure than selecting Always use the following command-line parameters. We have chosen the less secure option for this lab as you will be creating several ThinManager Display Clients, each 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

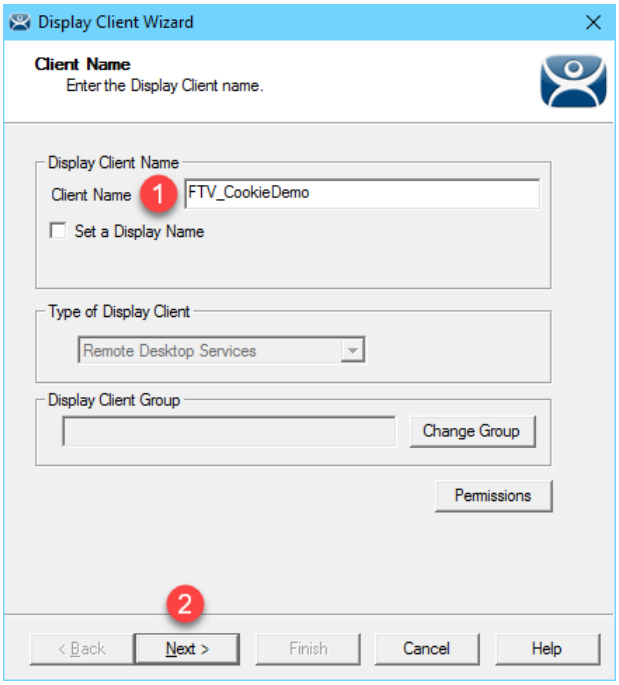
1. Return to ThinManager and click the **Display Clients** icon  from the ThinManager tree selector.



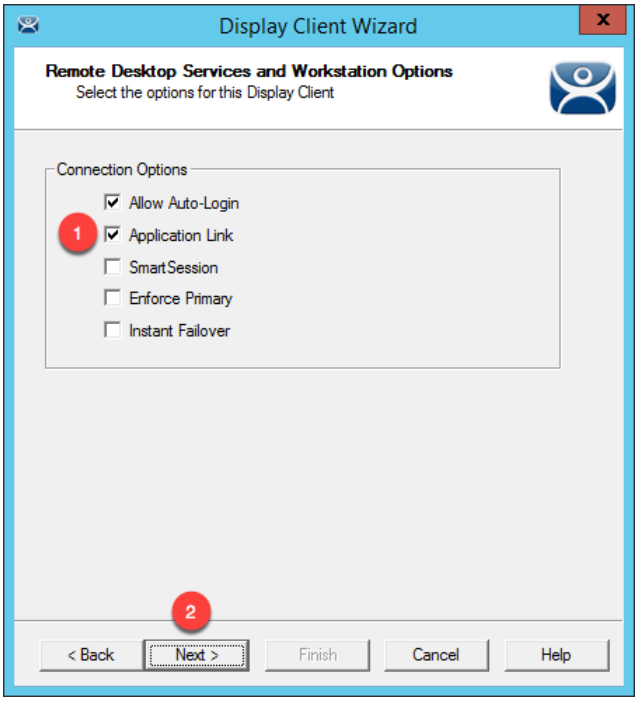
2. From the **Display Clients** tree, right click the **Remote Desktop Services** branch and select **Add Display Client**. This will launch the **Display Client Wizard**.



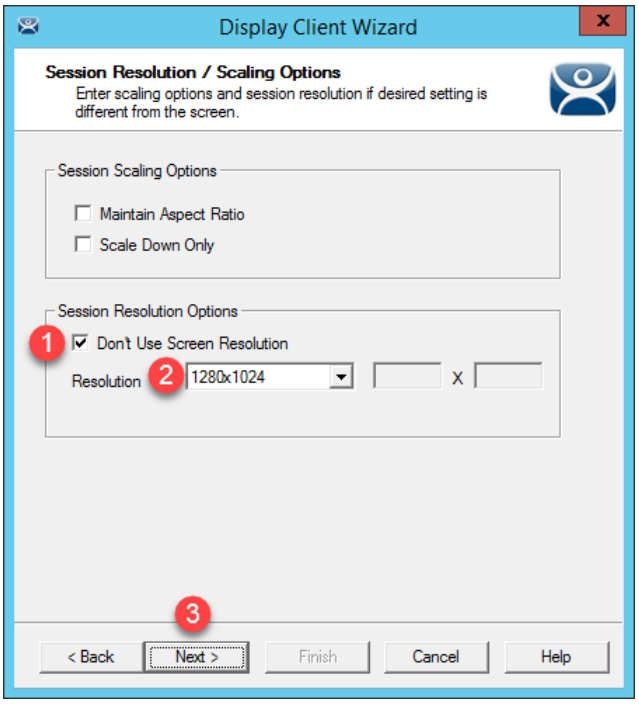
3. Type *FTV_CookieDemo* as the **Client Name** on the **Client Name** page of the wizard. Click the **Next** button.



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

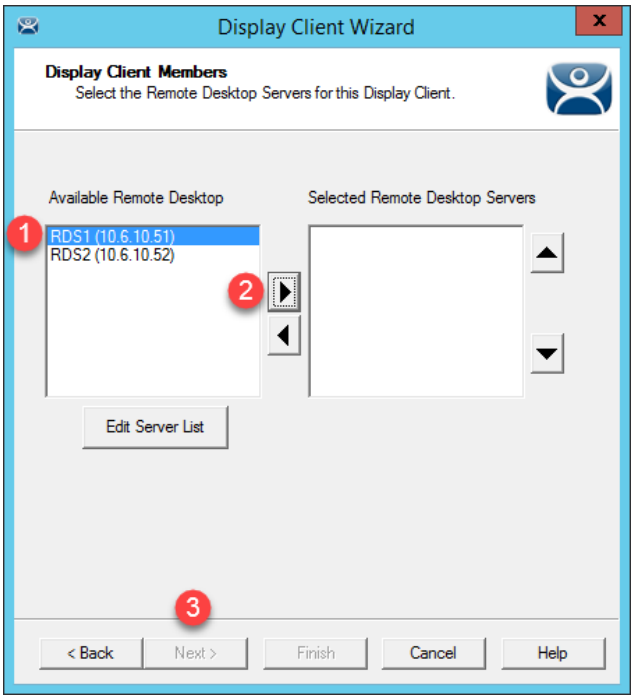


6. From the **Screen Resolution / Scaling Options** page of the wizard, check the box for **Don't Use Screen Resolution**, and select **1280x1024** from the **Resolution** drop down list. Click the **Next** button.



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**):

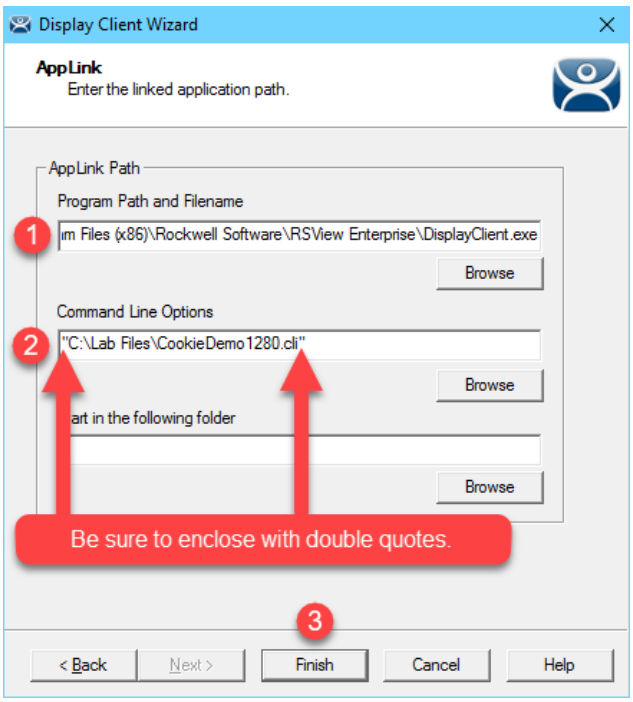
Program Path and Filename:

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

Command Line Options:

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

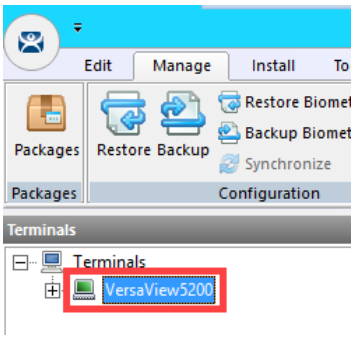
9. Make sure to enclose the **Command Line Options** path in double quotes. Click the **Finish** button.



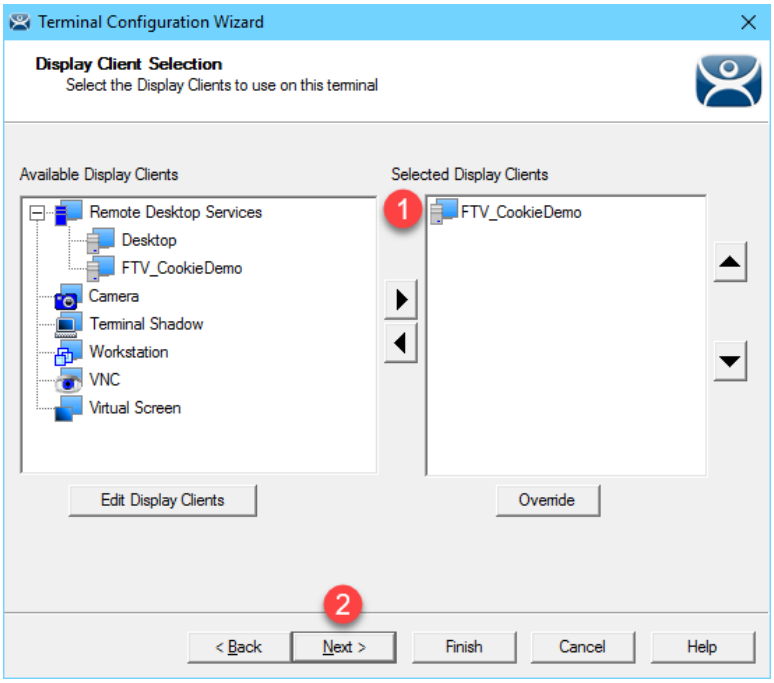
Apply New Display Client to Terminal

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**.

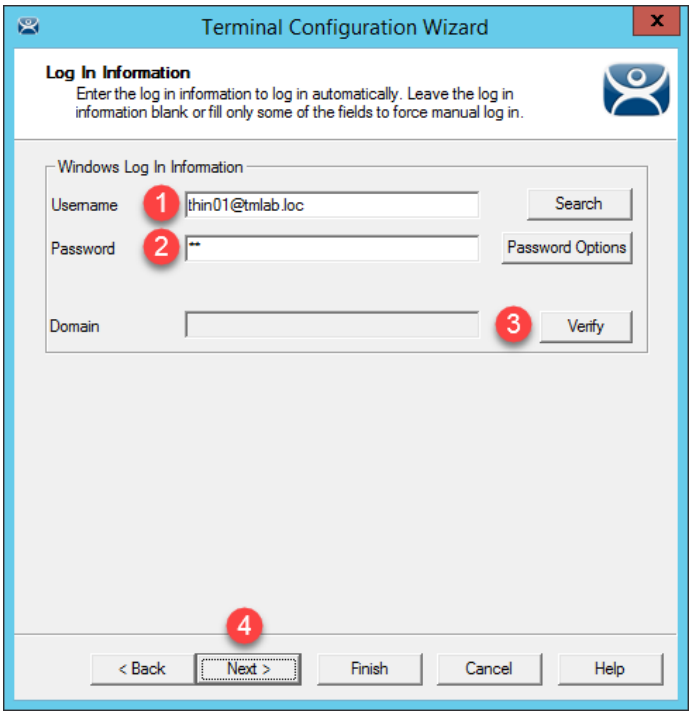


3. Click the **Next** button on the **Terminal Name** page of the wizard.
4. Click the **Next** button on the **Terminal Hardware** page of the wizard.
5. Click the **Next** button on the **Terminal Options** page of the wizard.
6. Click the **Next** button on the **Terminal Mode Selection** page of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

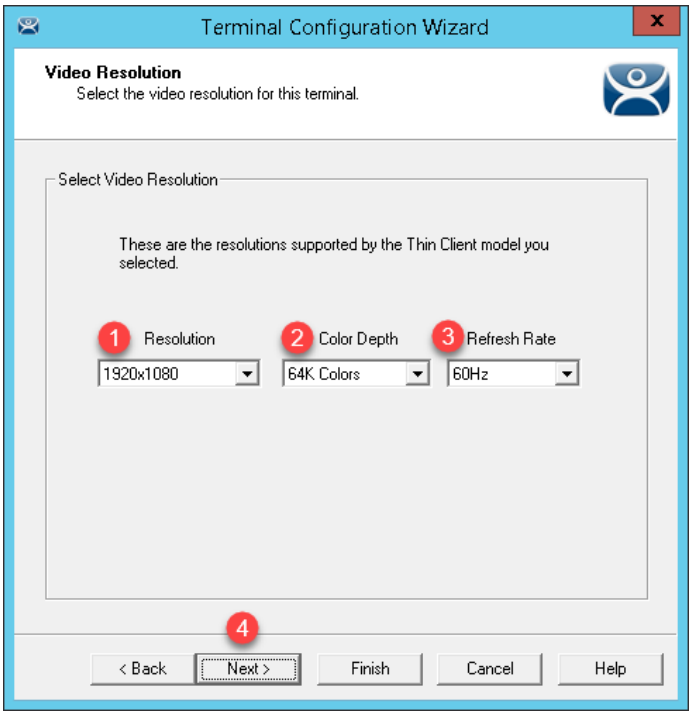


8. Click the **Next** button on the **Terminal Interface Options** page of the wizard.

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.

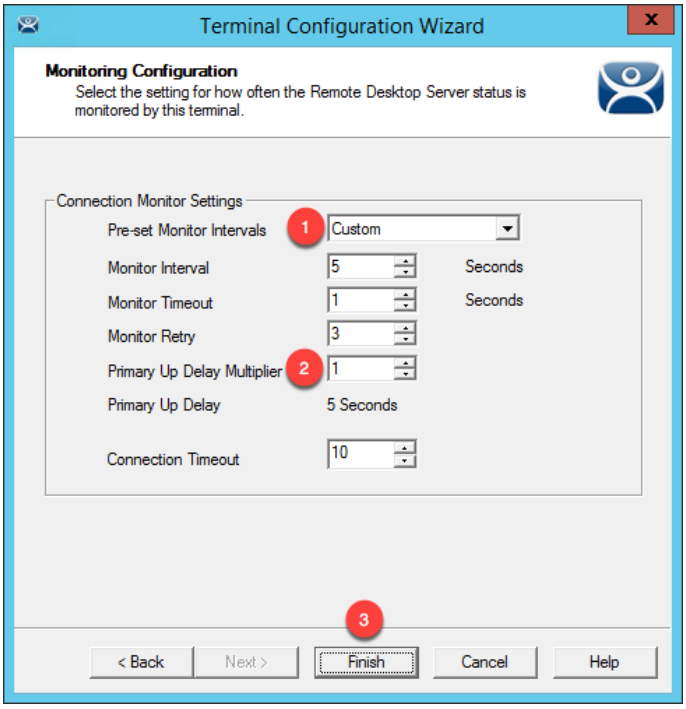


11. From the **Video Resolution** screen of the wizard, select **1920x1080** as the **Screen Resolution, 64K Colors** as the **Color Depth** and **60Hz** as the **Refresh Rate**. Click the **Next** button.

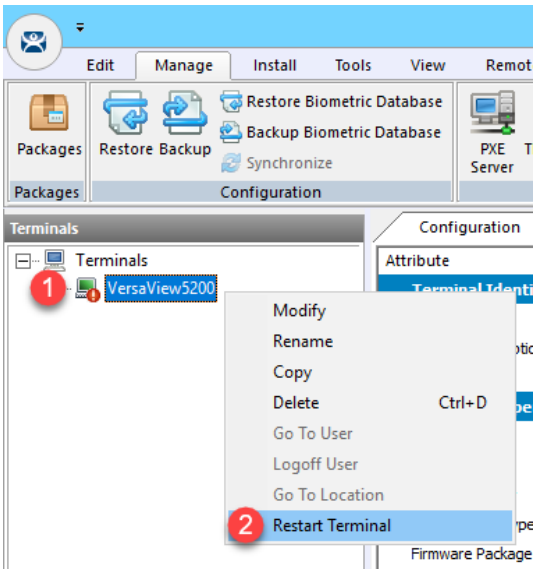


12. Click the **Next** button on the **Module Selection** page of the **Terminal Configuration Wizard**.
13. Click the **Next** button on the **ThinManager Server Monitor List** page of the **Terminal Configuration Wizard**.

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.



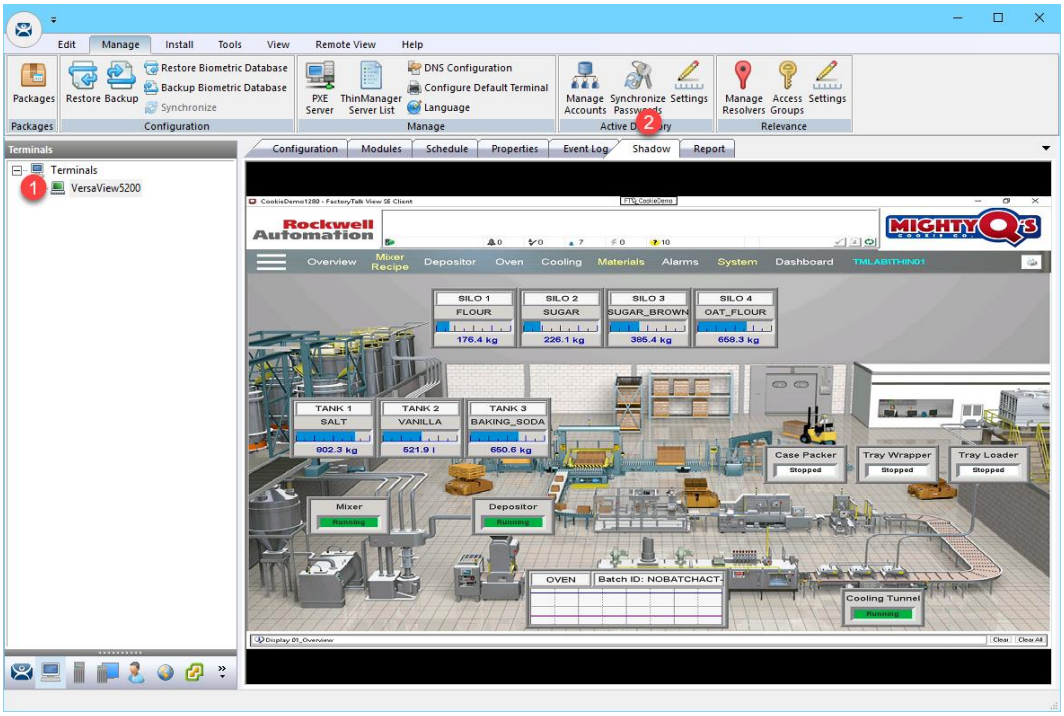
15. Right click the **VersaView5200** terminal from the **Terminals** tree and select **Restart Terminal** to apply the changes. Click **Yes** to restart the terminal.



> 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**.

16. 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.

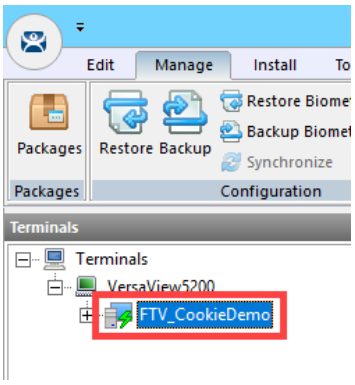
Once the application closes, you will see the desktop background with no Start menu bar for about 30 seconds before you are automatically logged out. When using AppLink, the user does not have access to any other programs or the desktop when connecting and once that application terminates, the user is 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.

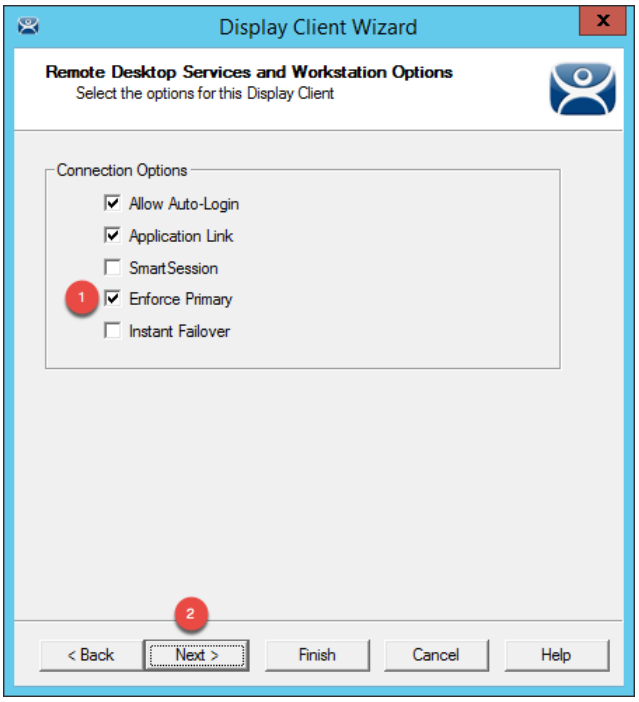
A module is a small driver that can be applied to a terminal to provide additional capabilities. For example, ThinManager includes 15 unique Touch Screen Modules, a Redundant Ethernet Module for thin clients with dual Ethernet ports (provides automatic failover of network interfaces connected to the 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**.

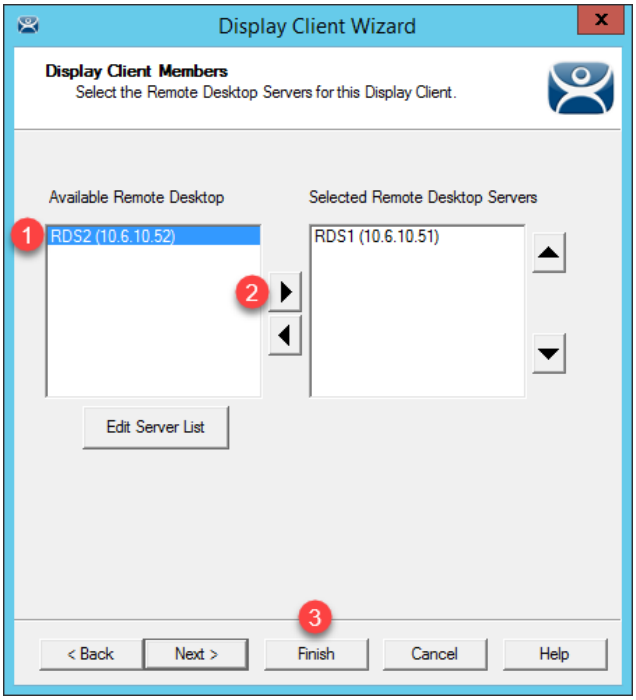


2. Click the **Next** button on the **Client Name** page of the wizard.
3. Click the **Next** button on the **Display Client Options** page of the wizard.
4. Check the **Enforce Primary** checkbox on the **Remote Desktop Services and Workstation Options** page of the wizard. Click the **Next** button.



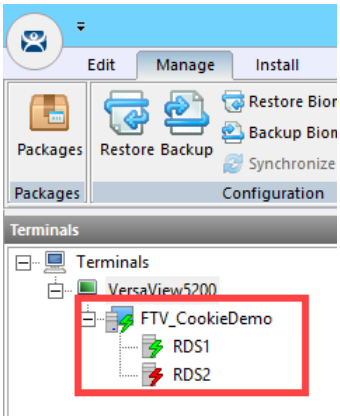
5. Click the **Next** button on the **Screen Resolution / Scaling Options** page of the wizard.

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.

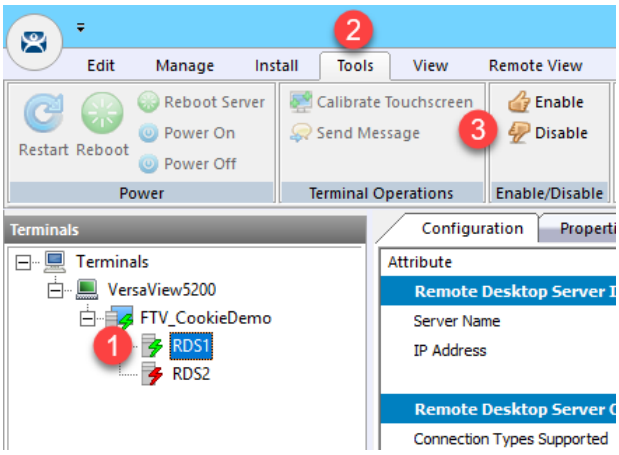


> By adding more than 1 Remote Desktop Server to the **Selected Remote Desktop Servers** list, you have added automatic Remote Desktop Server failover for this Display Client. The order of the servers listed determines the order of failover. In this case, **RDS1** would be the primary and **RDS2** would 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.

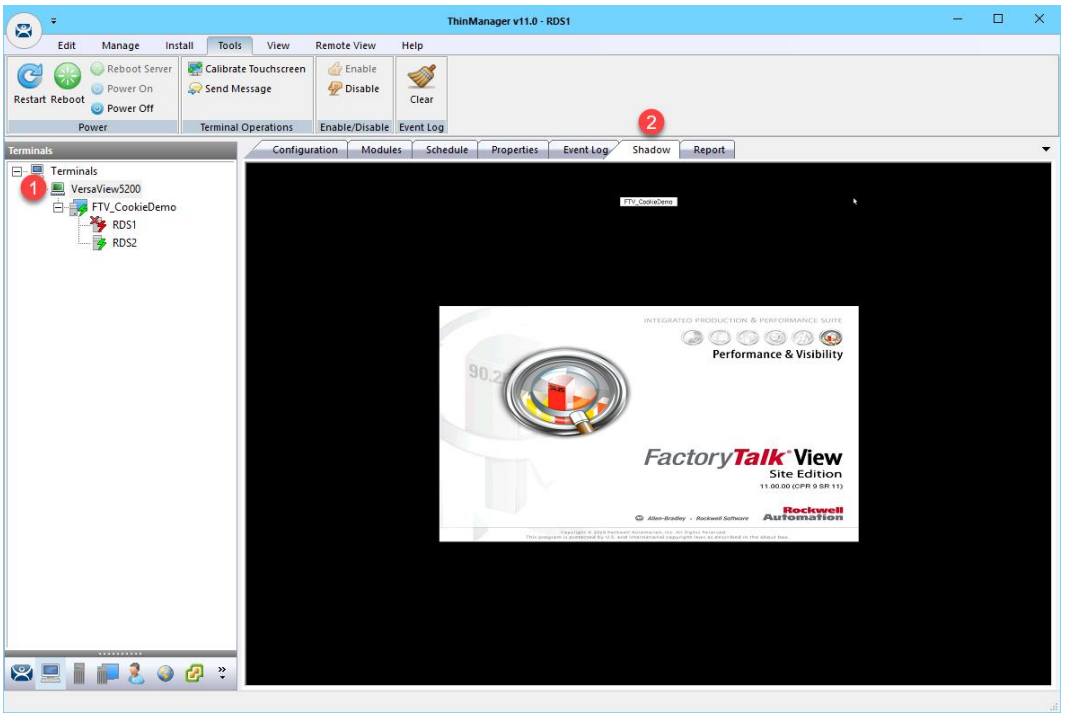
7. Right click the **VersaView5200** terminal and select **Restart Terminal** to apply the changes. Click **Yes** on the confirmation dialog box. If you expand the **VersaView5200** terminal, and then expand the **FTV_CookieDemo** Display Client, you will now see both **RDS1** and **RDS2** are listed. 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.



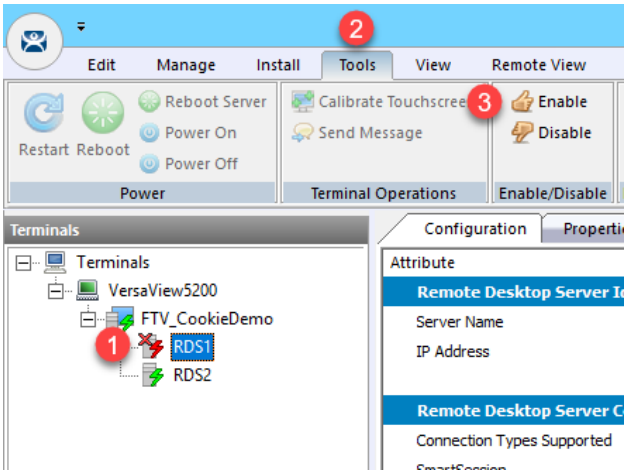
8. To force a failover to occur, we can manually disable the **RDS1** Remote Desktop Server from **ThinManager**. This will disconnect all Remote Desktop Server sessions connected to **RDS1**. From the **Terminals** tree, expand the **VersaView5200** terminal, and then expand the **FTV_CookieDemo** Display 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.



9. 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.



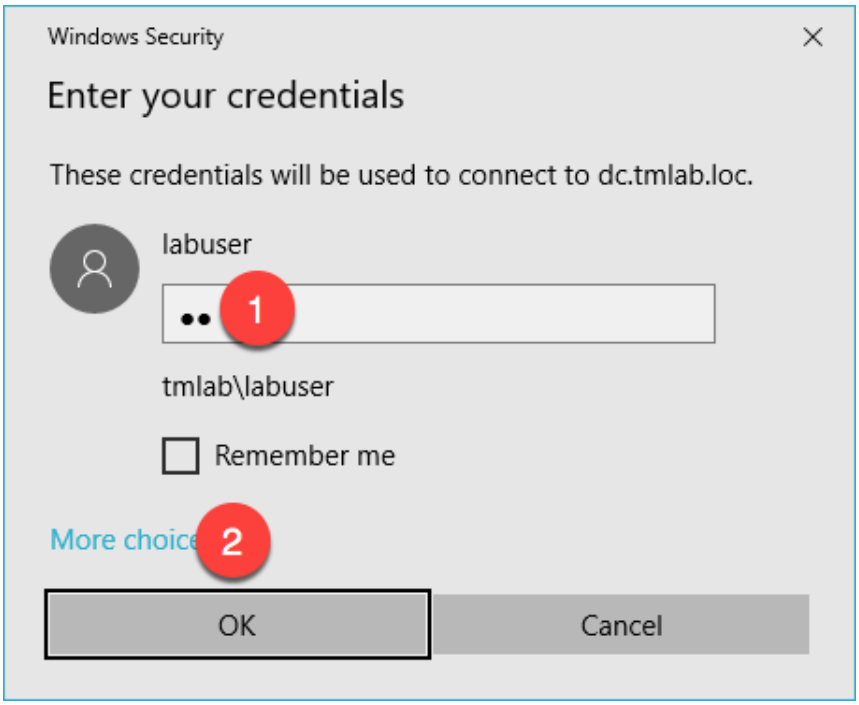
There are actually 2 types of automatic Remote Desktop Server failover supported by ThinManager. The one demonstrated above is called **Standard Failover**. With **Standard Failover**, the failover session is started on-demand. The other type is called **Instant Failover**, which differs by keeping sessions 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.

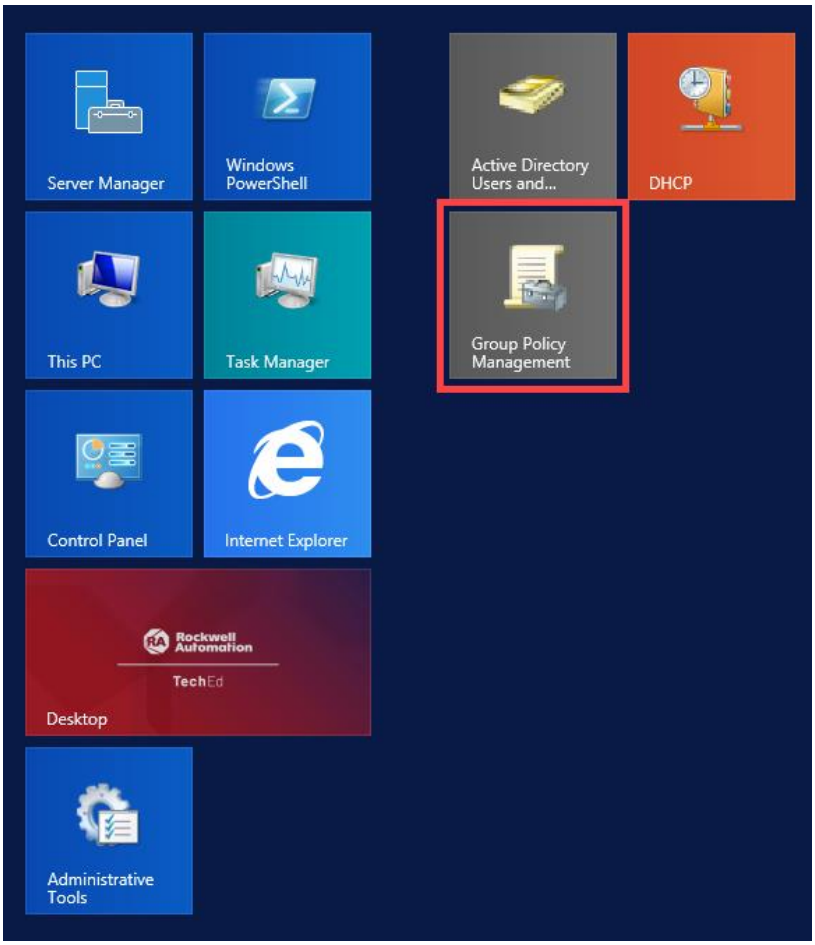
1. Minimize the **ThinManager Admin Console** if it is maximized and double click the **dc.tmlab.loc** shortcut on the desktop to launch a remote desktop session on the **DC** virtual image.

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

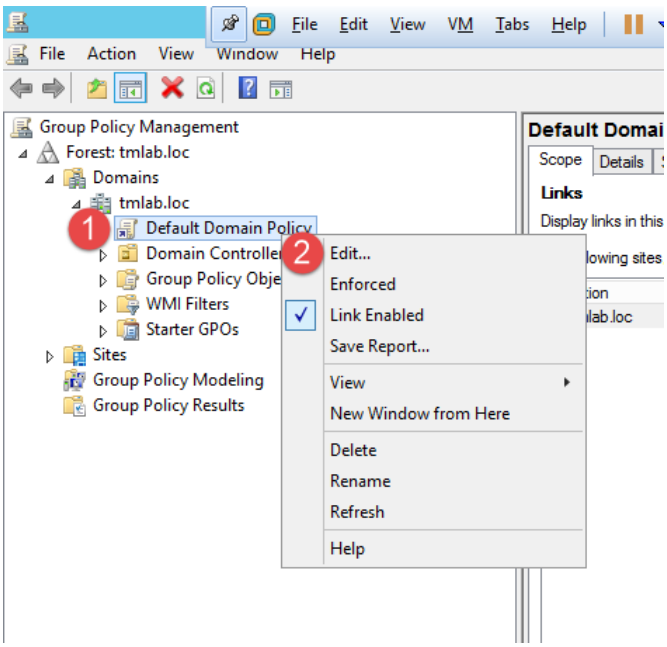


Note: If you cannot connect to DC via the shortcut, you may need to restart RDS1 from the Windows Desktop (Start > Power > Restart).

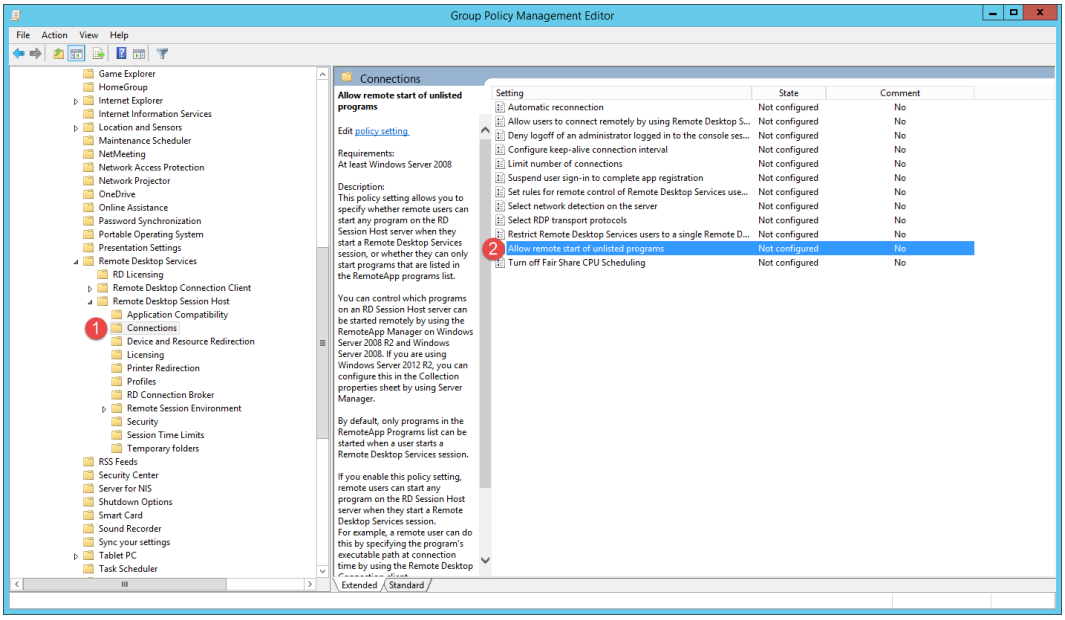
3. Click the **Windows Start** button.
4. From the **Windows Start Menu**, click the **Group Policy Management** icon.



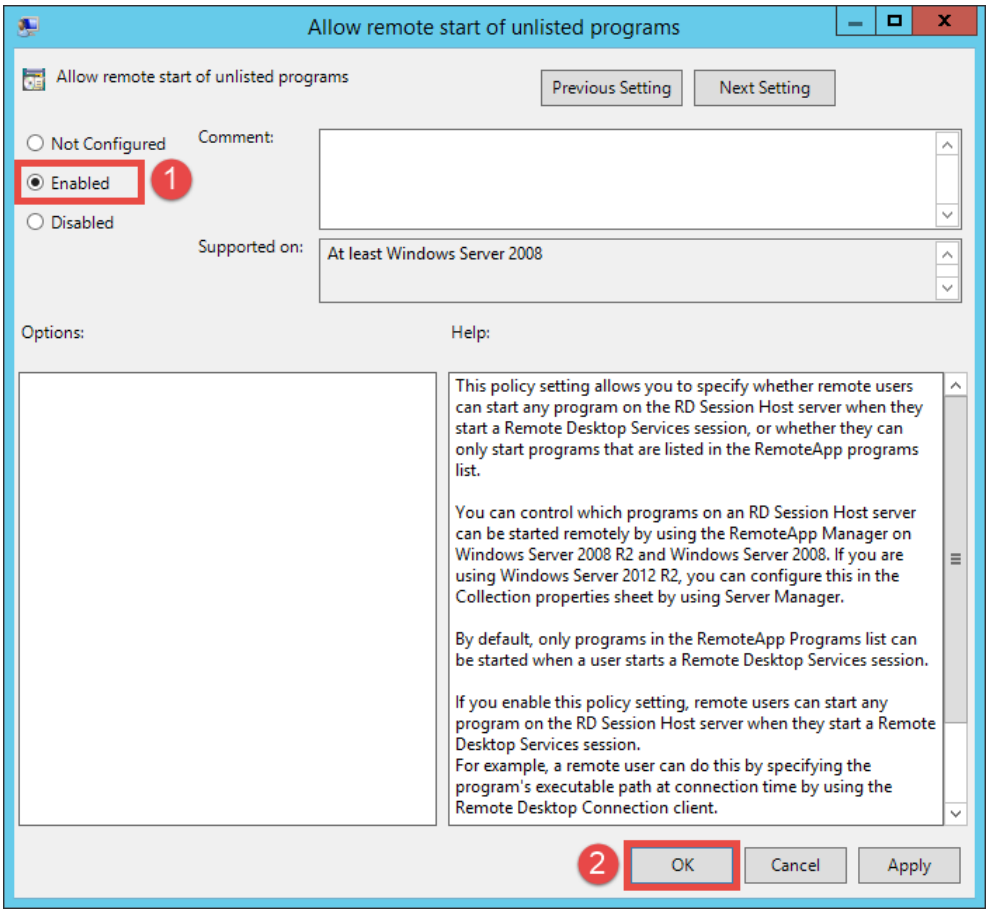
5. From the **Group Policy Editor**, right click the **Default Domain Policy** item and click **Edit…**



6. 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.

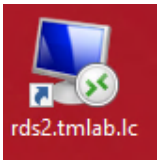


7. From the ensuing policy setting dialog box, click the **Enabled** option button followed by the **OK** button. Close the **Group Policy Management Editor** and the **Group Policy Management** window.

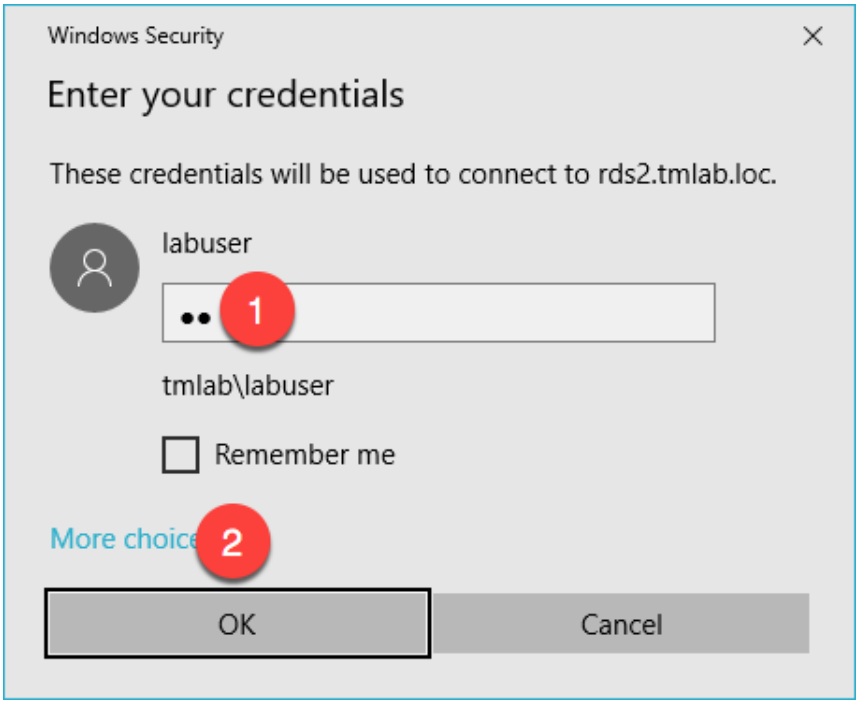


8. Close the remote desktop session on **dc.tmlab.loc**. Click **OK** to the confirmation dialog box.

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.

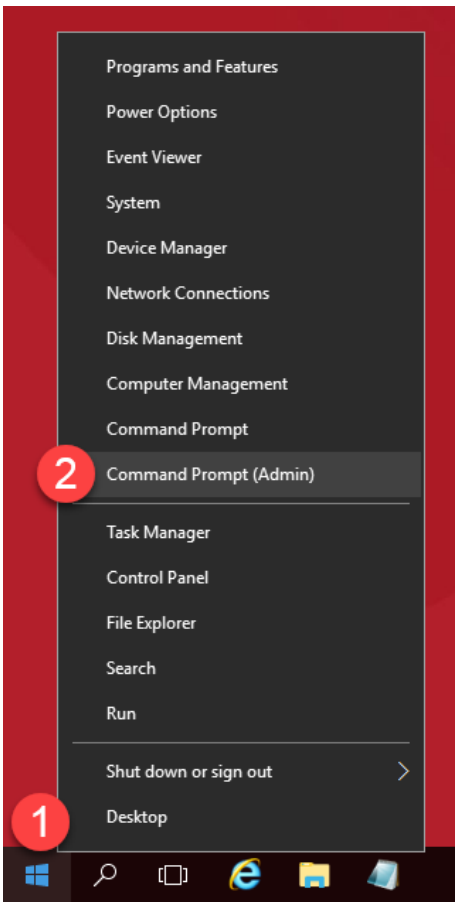


10. If you are presented with a login dialog box, make sure the username is *tmlab\labuser* and enter a password of *rw*.

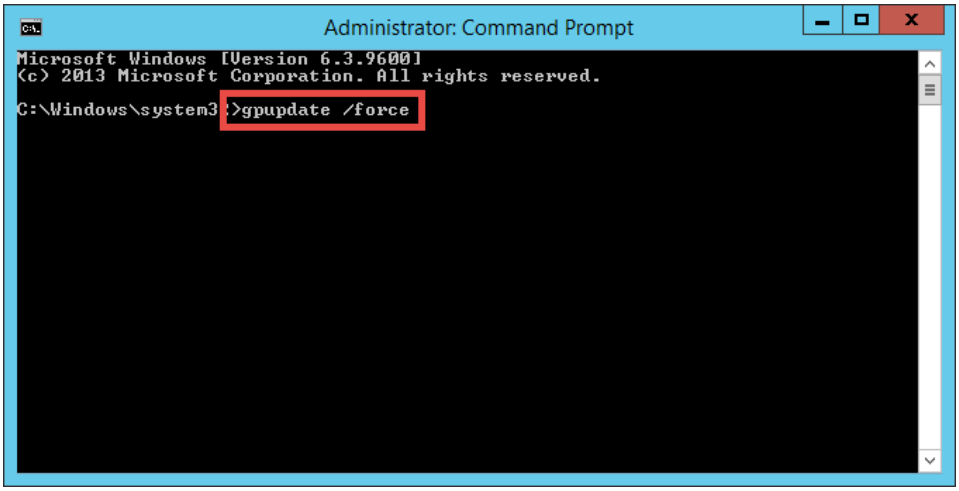


<u>Note:</u> If you cannot connect to RDS2 via the shortcut, you may need to restart RDS1 from the Windows Desktop (Start > Power > Restart).

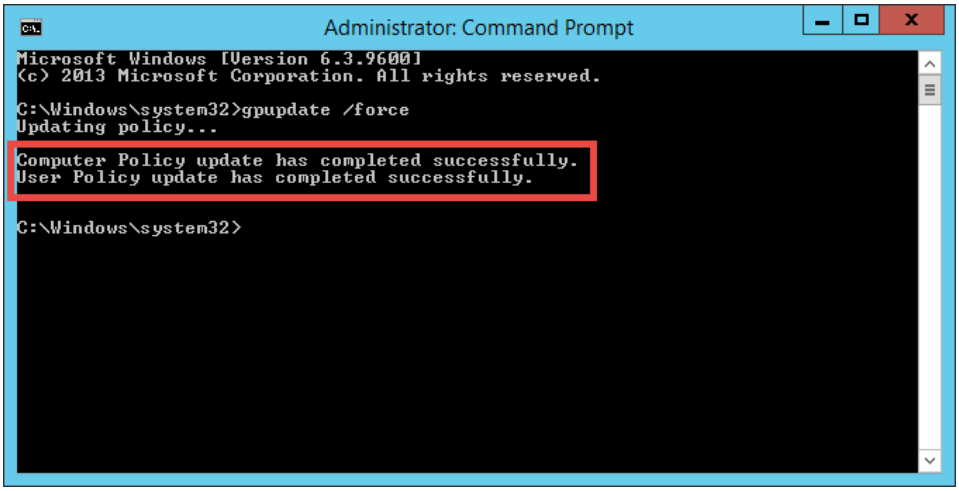
11. From **RDS2**, right click the **Windows Start Button** and click **Command Prompt** (**Admin**).



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



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



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

15. Repeat steps 11 – 13 from above on **RDS1**.

STOP **Checkpoint Question:** https://thinmanager.com/cloudlabs/section05/

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 6: Terminal Replacement in under 2 Minutes

Overview

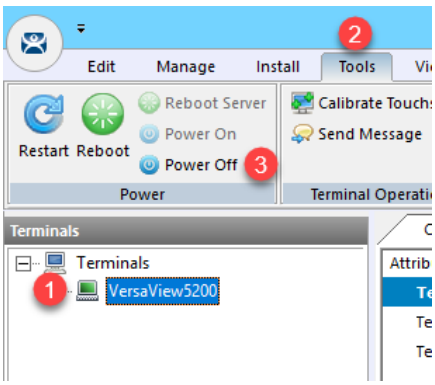
While industrial grade terminals like the **VersaView 5200** do not fail often (since it has no moving parts), it can be replaced in under 2 minutes when it does. Replacement starts by disconnecting the failed terminal and connecting the new terminal in its place. When the new terminal is powered up 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:

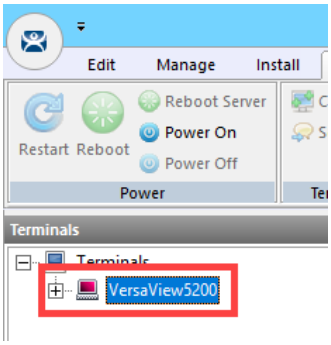
1. Power Down the Virtual Thin Client
2. Reassign the VersaView5200 Terminal Profile

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.

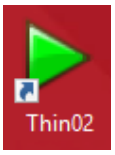


4. To confirm, the **VersaView5200** terminal icon in the **Terminals** tree should be **Red** before continuing. The **Thin01** virtual thin client will automatically close upon powering off.

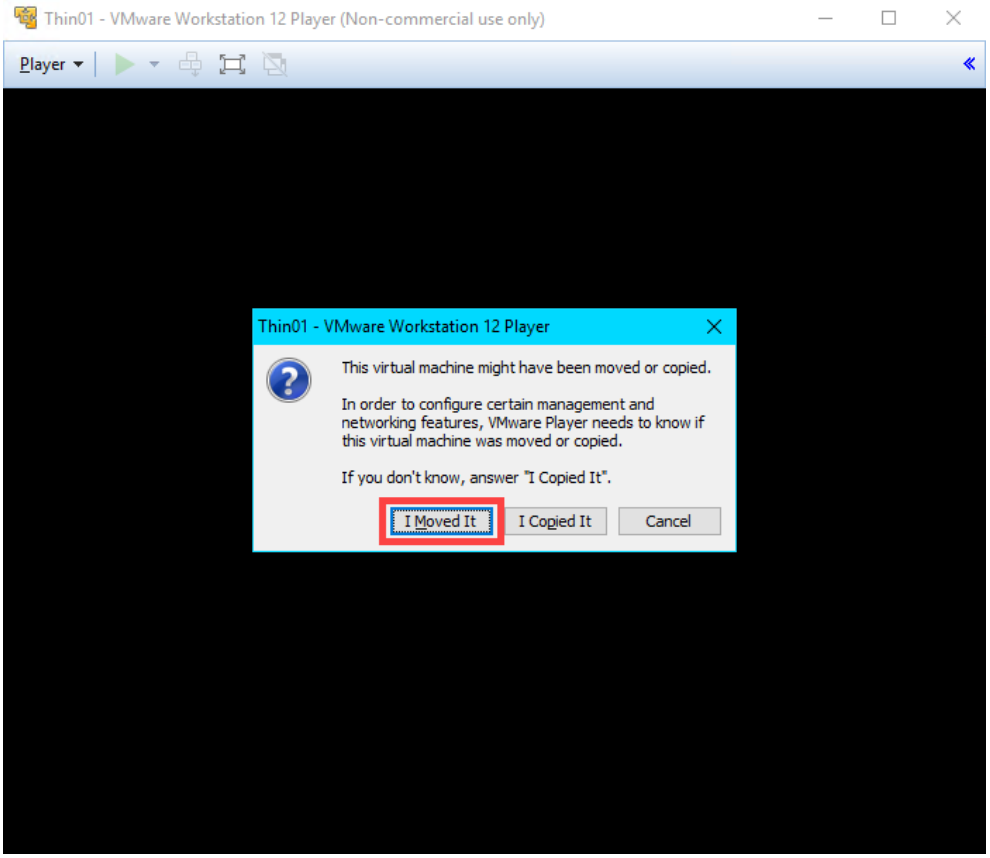


Reassign the VersaView5200 Terminal Profile

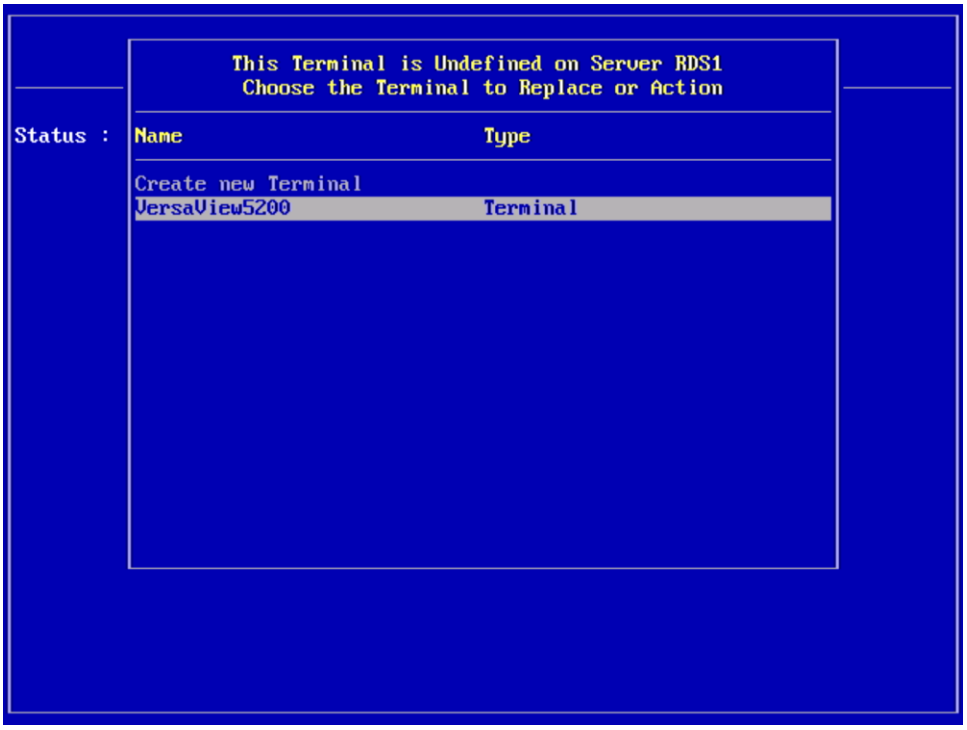
1. Double click the **Thin02** shortcut from the **RDS1** desktop. Since we are using virtual thin clients, you should think of this step as removing a failed physical thin client with a replacement thin client – as the



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

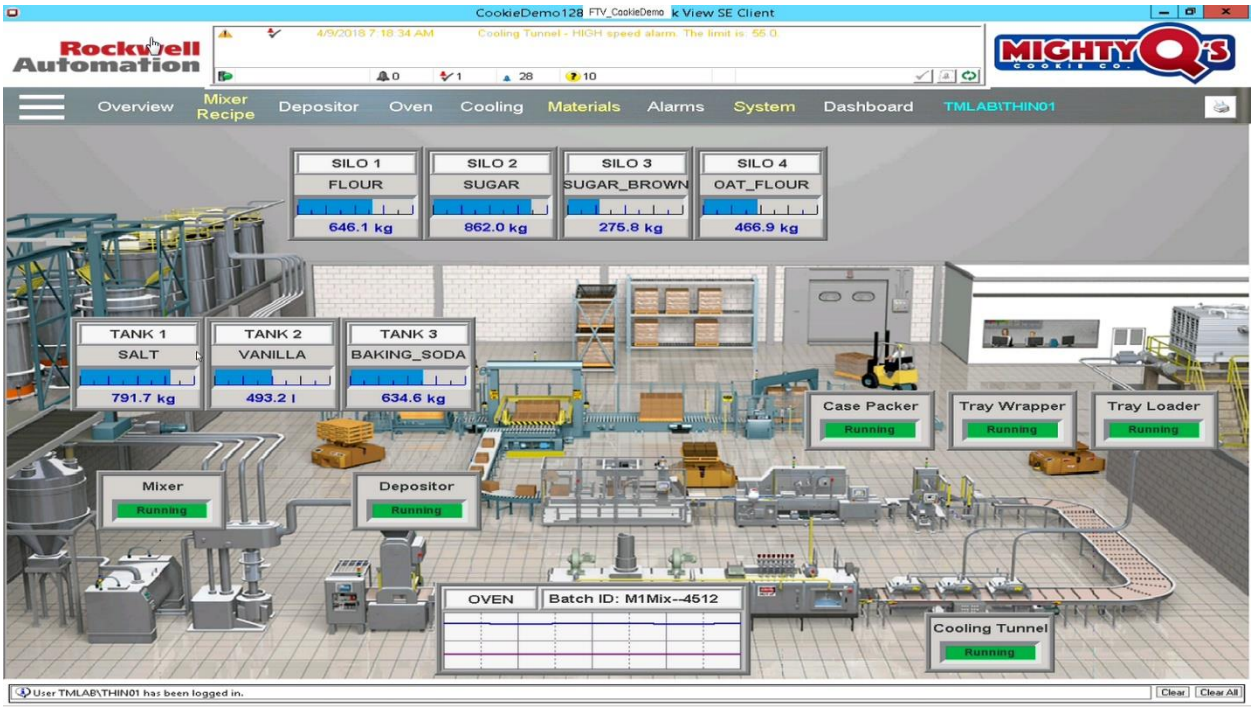


3. Upon powering up, the ThinManager firmware should get delivered to the replacement terminal. Because ThinManager does not have an existing terminal configuration that matches the **MAC address** of the replacement unit, you will be prompted to either **Create new Terminal** or select an existing terminal 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**.

4. You have now successfully replaced your thin client. Notice when the replacement unit received the **VersaView5200** terminal profile it was automatically reconnected to the Remote Desktop Server sessions that were being delivered to the replacement unit – literally, a bumpless transfer.



Checkpoint Question: https://thinmanager.com/cloudlabs/section06/

This completes the section **Terminal Replacement in Under 2 Minutes** of the lab. Continue on to deliver additional content and visualize it using tiling mode.

Section 7: 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:

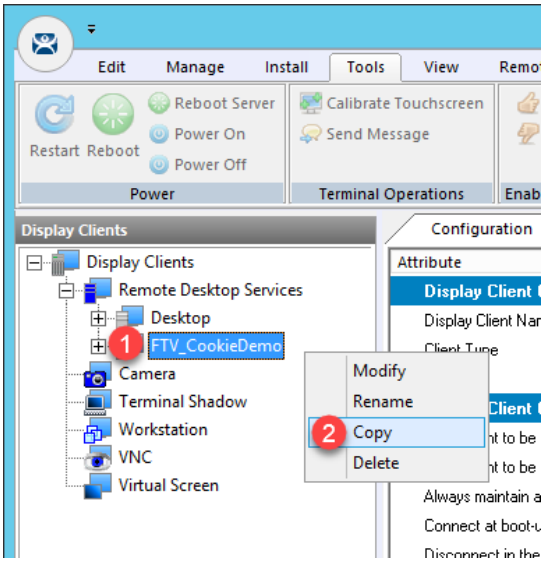
1. Create InstantFizz Remote Desktop Services Display Client
2. Create Excel Remote Desktop Services Display Client
3. Create SuperJuice VNC Display Client
4. Create Camera Display Client
5. Apply Display Clients to Terminal and Enable Tiling
6. FactoryTalk View SE Client Licensing Benefits
7. Remove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

Create InstantFizz Remote Desktop Services Display Client

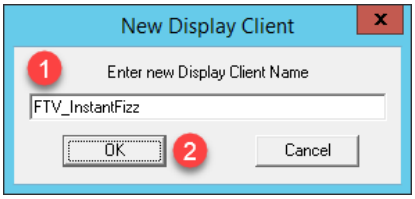
We are going to copy the **FTV_CookieDemo** Display Client to create another View SE Display Client, but this time to launch a different View SE application. We won't need Automatic Remote Desktop Failover, so we will disable this from the copied terminal profile.

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

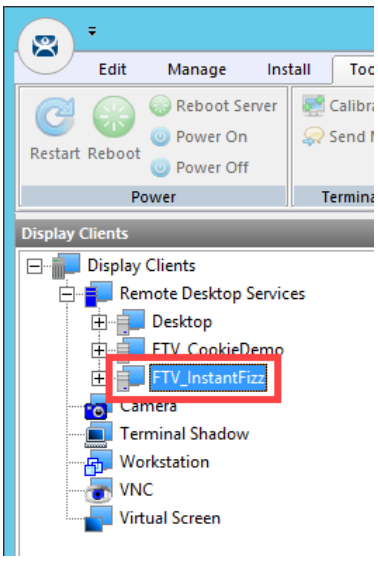
2. From the **Display Clients** tree, expand the **Remote Desktop Services** branch and right click the **FTV_CookieDemo** item and select **Copy**.



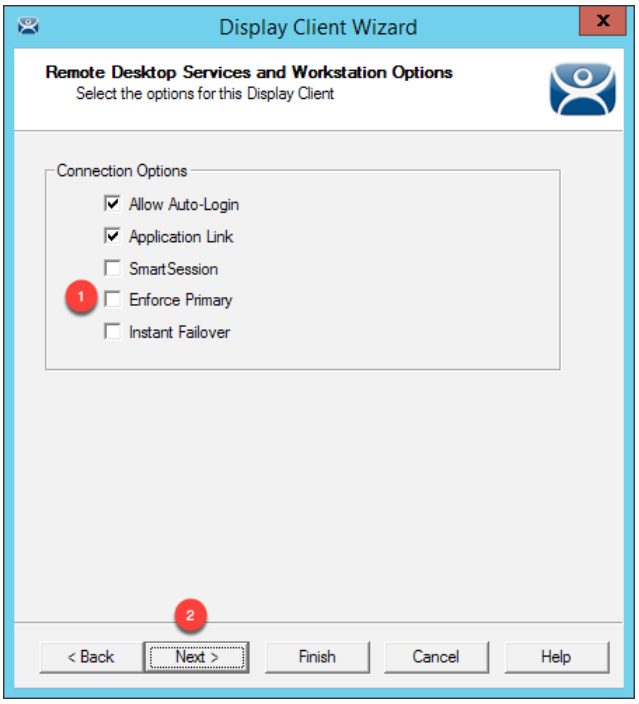
3. Type *FTV_InstantFizz* in the **Enter new Display Client Name** text box and click the **OK** button.



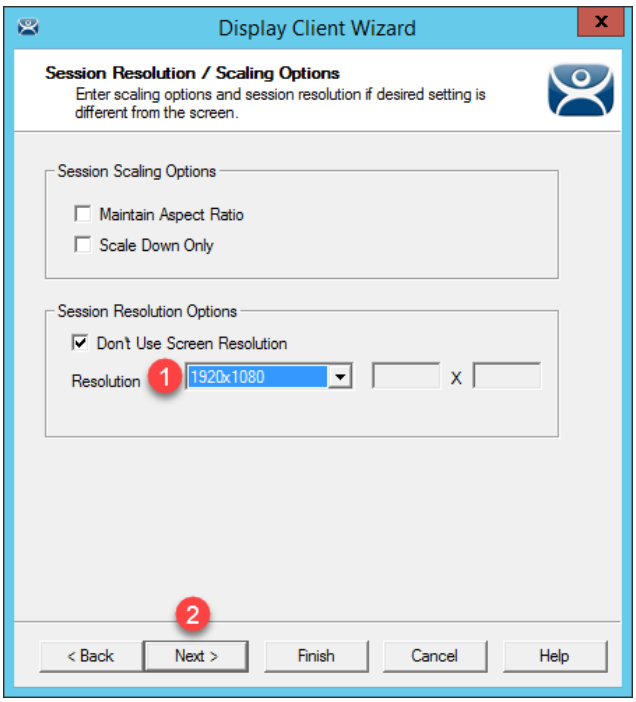
4. Double click the **FTV_InstantFizz Display Client** item.



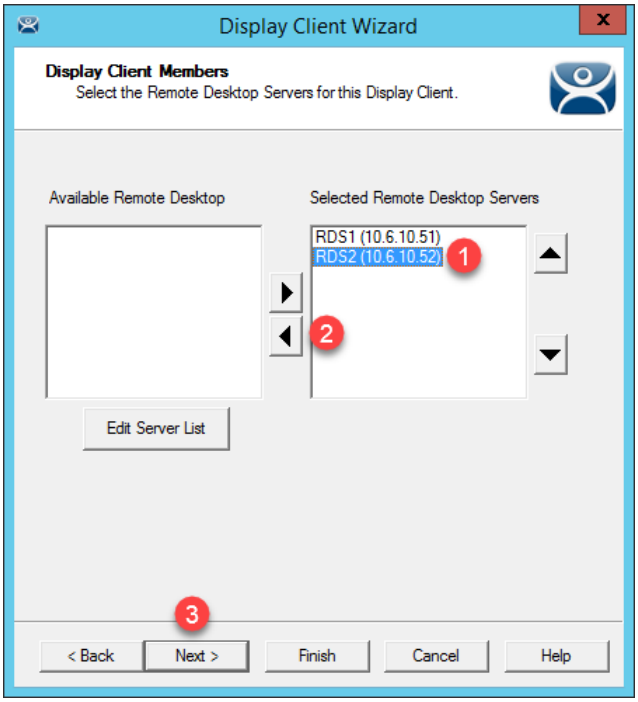
5. From the **Client Name** page of the wizard, click the **Next** button.
6. From the **Display Client Options** page of the wizard, click the **Next** button.
7. From the **Remote Desktop Services and Workstation Options** page of the wizard, uncheck the **Enforce Primary** checkbox and click the **Next**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



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

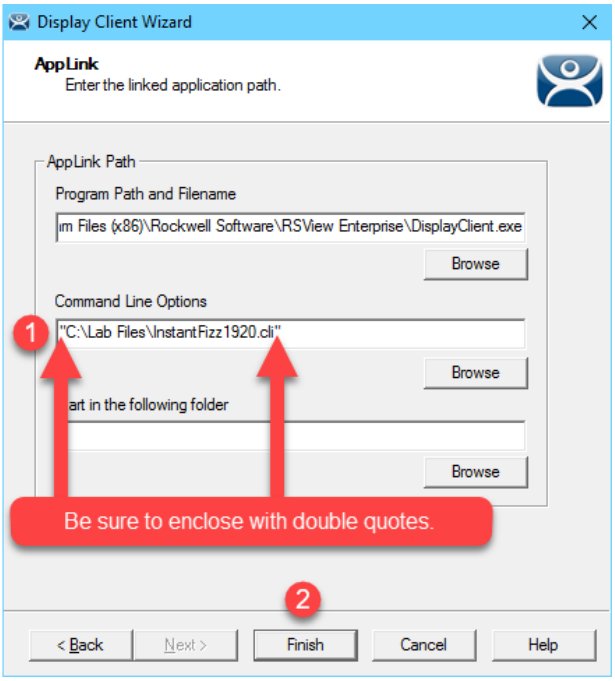


9. From the **Display Client Members** page of the wizard, select **RDS2** from the **Selected** list and click the **Left** arrow button to remove it. Click the **Next** button.



10. 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"
```



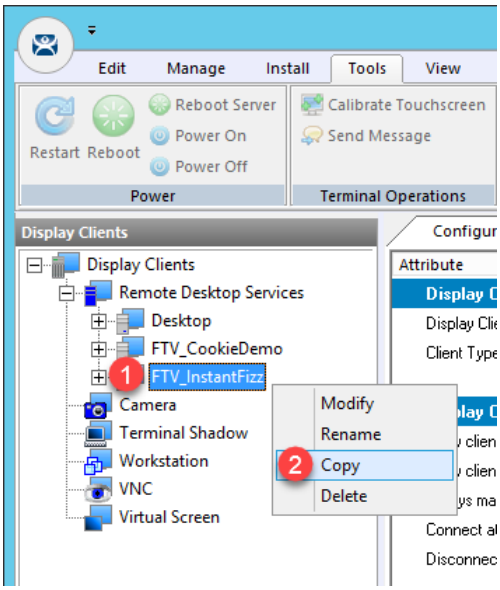
11. Click the **Finish** button.

> 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.

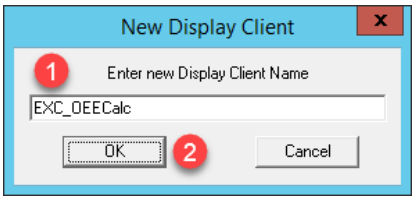
Create Excel Remote Desktop Services Display Client

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

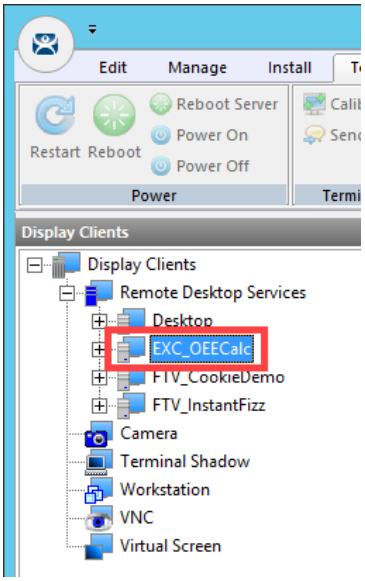
1. From the **Display Clients** tree, expand the **Remote Desktop Services** branch and right click the **FTV_InstantFizz** item and select **Copy**.



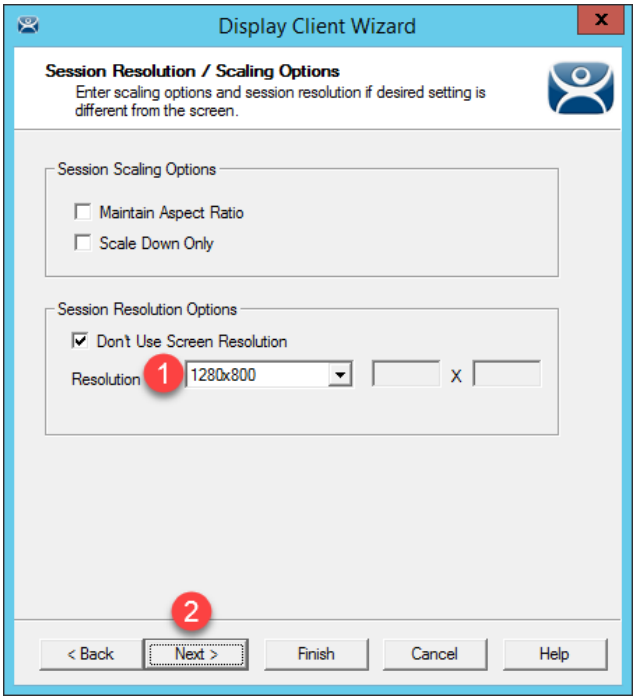
2. Type *EXC_OEECalc* in the **Enter new Display Client Name** text box and click the **OK** button.



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.



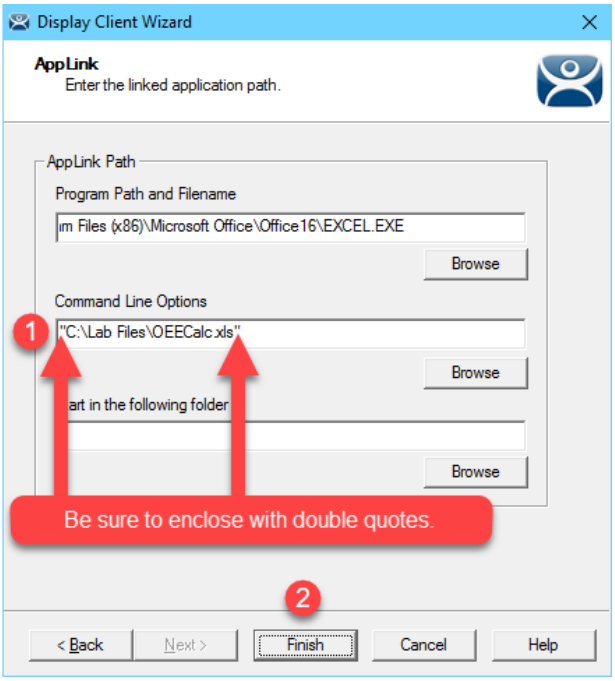
8. From the **Display Client Members** page of the wizard, click the **Next** button.
9. From the **AppLink** page of the wizard, replace the **Program Path and Filename** and the **Command Line Options** paths with the ones below (you can also copy and paste this path from the **LabPaths.txt** file 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"`

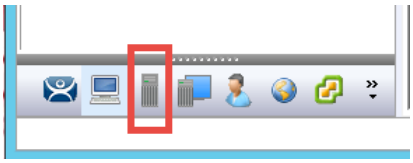


10. Click the **Finish** button.

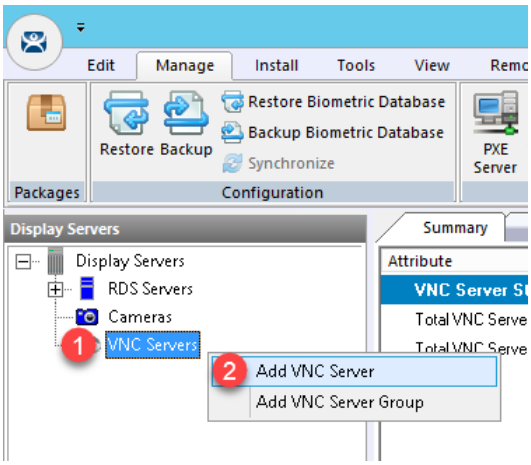
Create SuperJuice VNC Display Client

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.

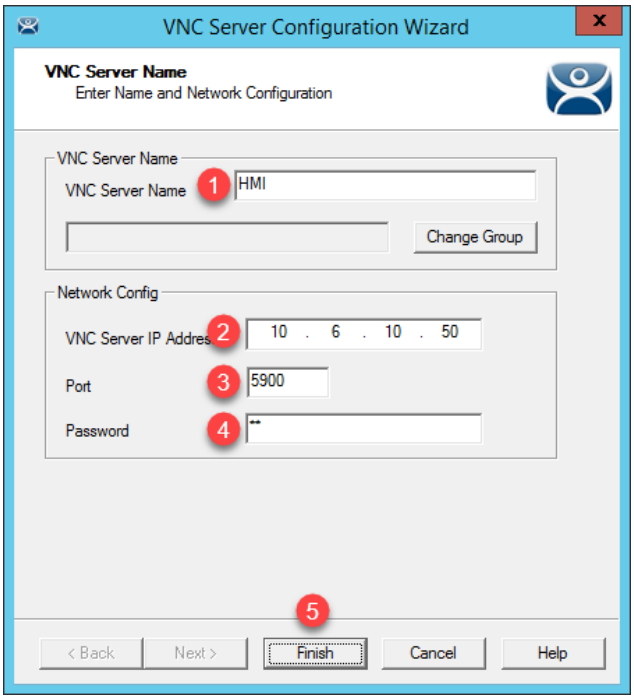
1. Click the **Display Servers** icon  in the ThinManager tree selector.



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**.

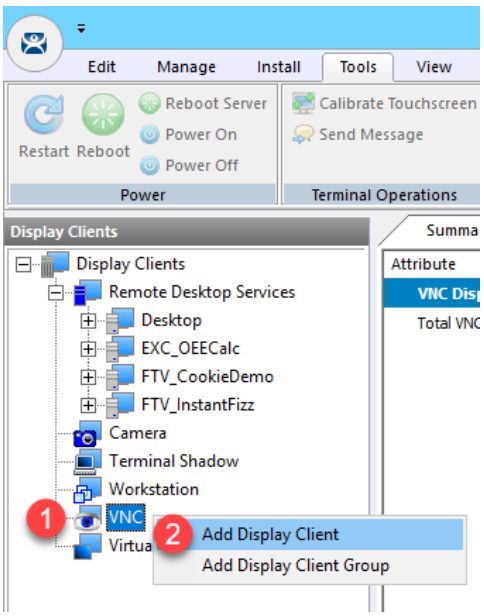


3. From the **VNC Server Name** page of the wizard, enter *HMI* in the **VNC Server Name** text box. Enter *10.6.10.50* in the **VNC Server IP Address** text box. Keep **5900** as the **Port**, and enter *rw* in the **Password** field. Click the **Finish** button.

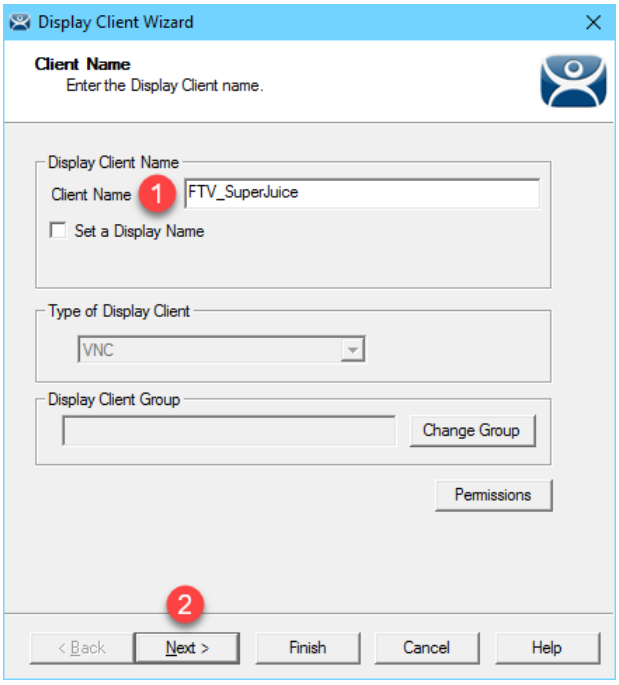


4. Click the **Display Clients**  icon from the ThinManager tree selector.

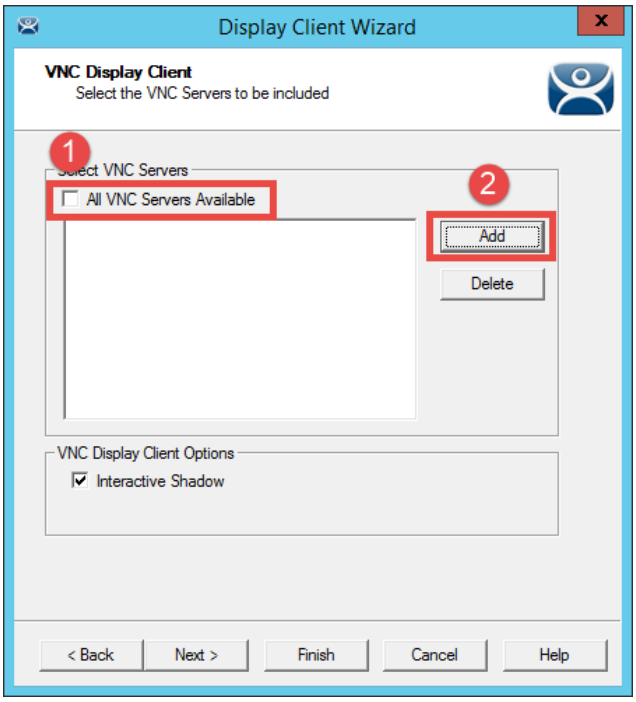
5. Expand the **Display Clients** tree, right click the **VNC** branch and select **Add Display Client**.



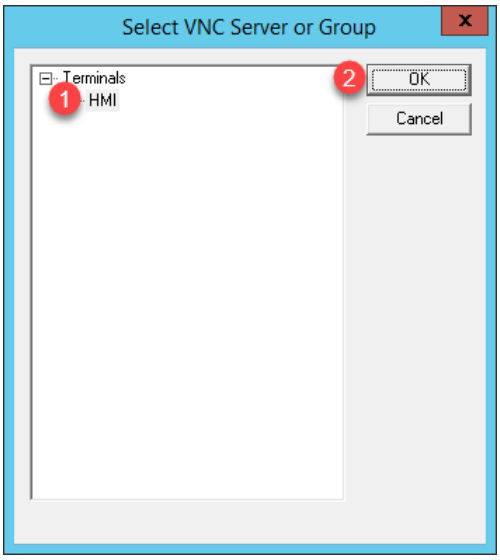
6. From the **Client Name** page of the wizard, enter *FTV_SuperJuice* as the **Client Name**. Click the **Next** button.



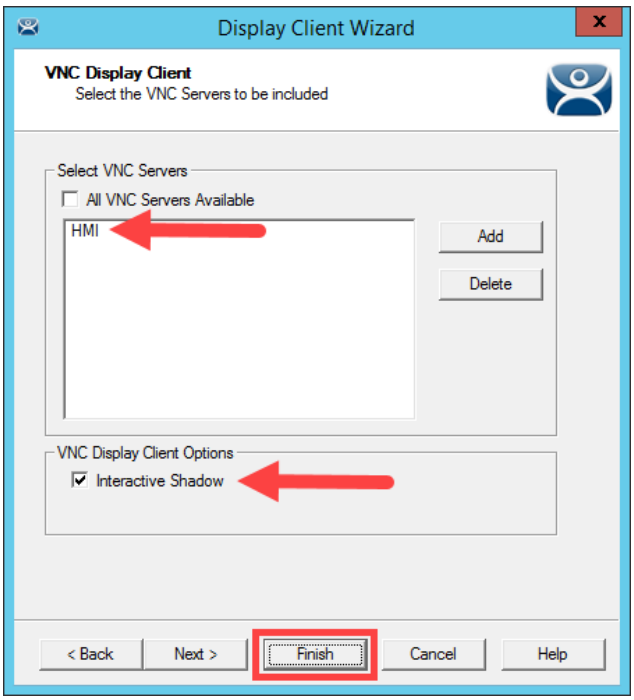
7. From the **Display Client Options** page of the wizard, click the **Next** button.
8. From the **VNC Display Client** page of the wizard, <u>un</u>check the **All VNC Servers Available** checkbox and then click **Add** button.



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



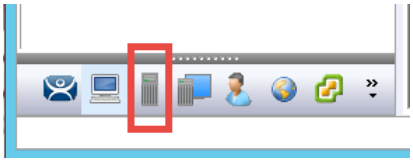
10. Back on the **VNC Display Client** page, keep the check for **Interactive Shadow** and click the **Finish** button.



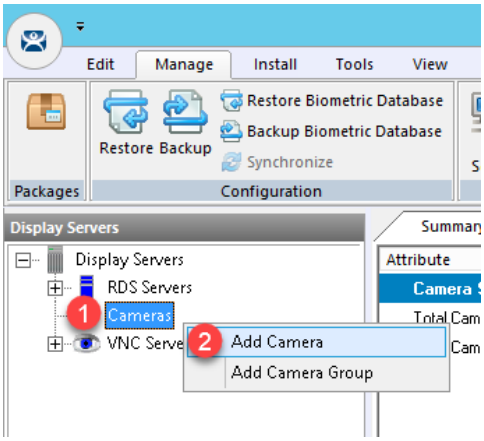
Create Camera Display Client

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).

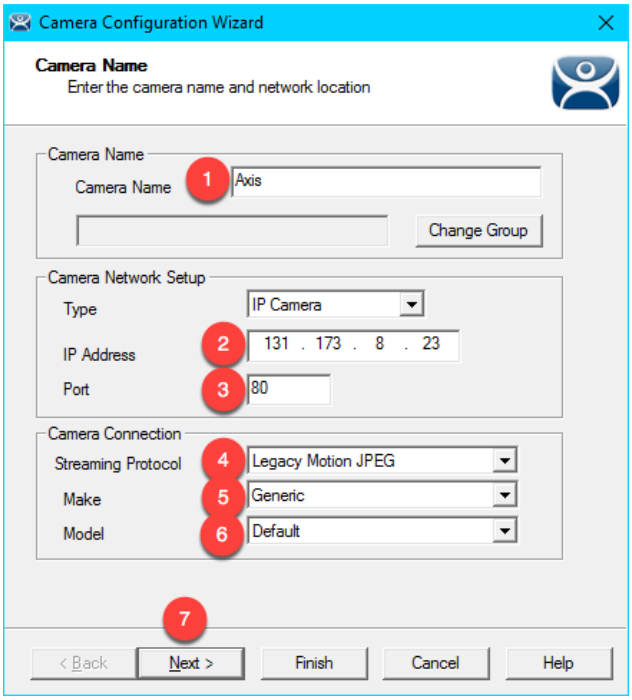
1. Click the **Display Servers** icon in the ThinManager tree selector.



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

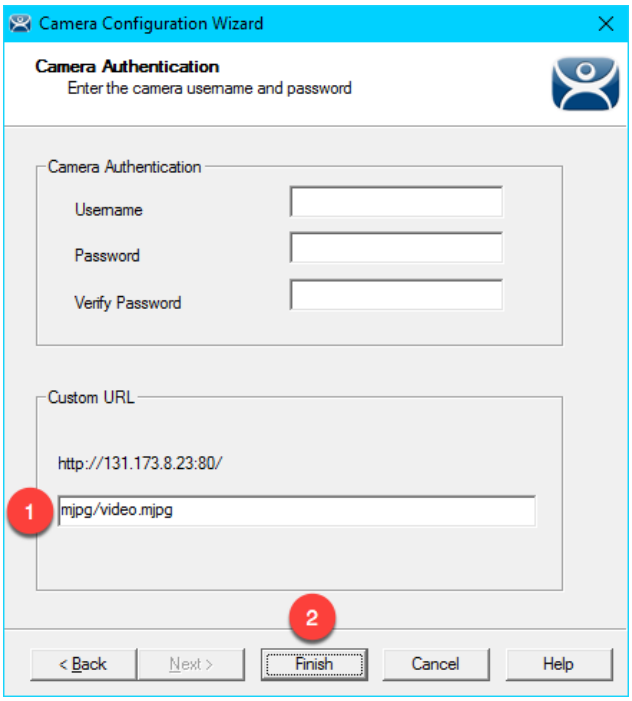


3. From the **Camera Name** page of the wizard, enter/select the following and then click the **Next** button.
   - **Camera Name** = *Axis*
   - **IP Address** = *131.173.8.23*
   - **Port** = *80*
   - **Streaming Protocol** = Legacy Motion JPEG
   - **Make** = Generic
   - **Model** = Default



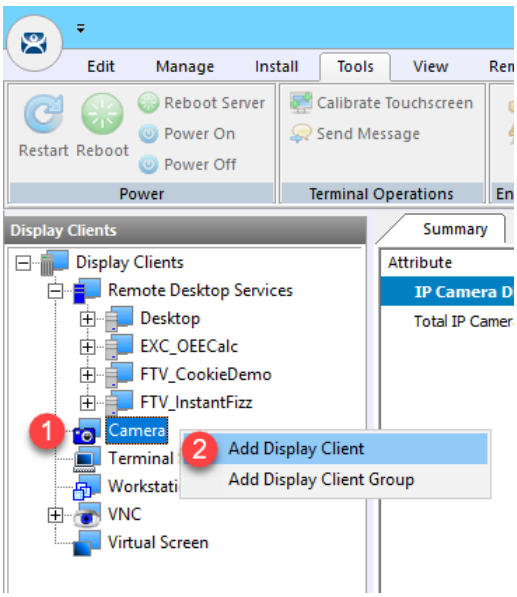
This is a public facing IP camera located at Osnabrück University in Lower Saxony, Germany. The camera is focused on a Foucault pendulum, a device named after the French physicist Léon Foucault. It was created to demonstrate the Earth's rotation. While the camera performs reasonably well over the Internet,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

4. 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.

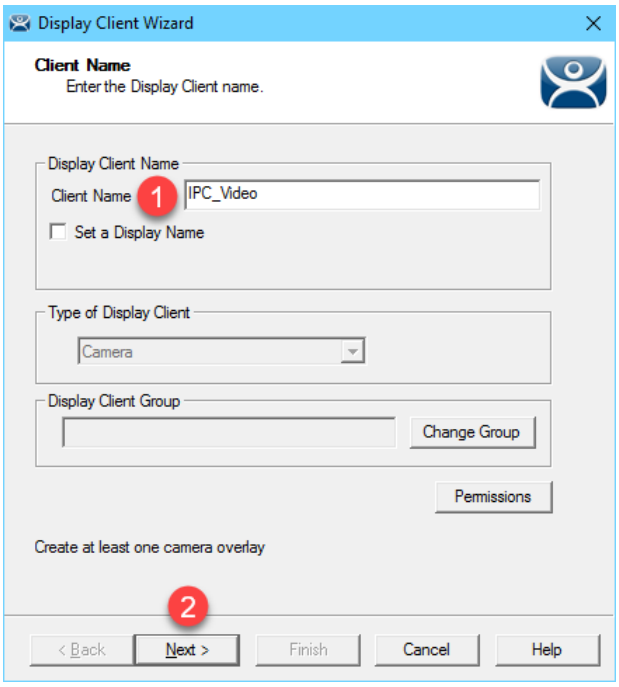


5. Click the **Display Clients**  icon from the ThinManager tree selector.

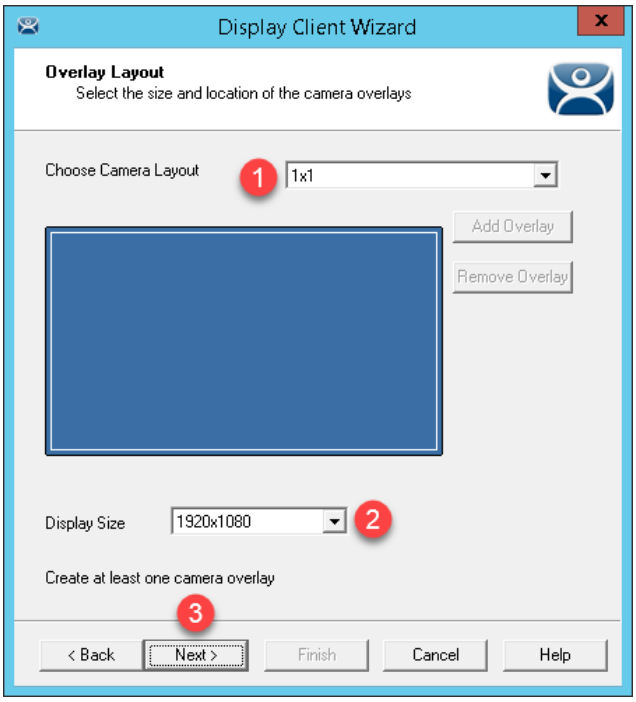
6. Expand the **Display Clients** tree, right click the **Camera** branch and select **Add Display Client**.



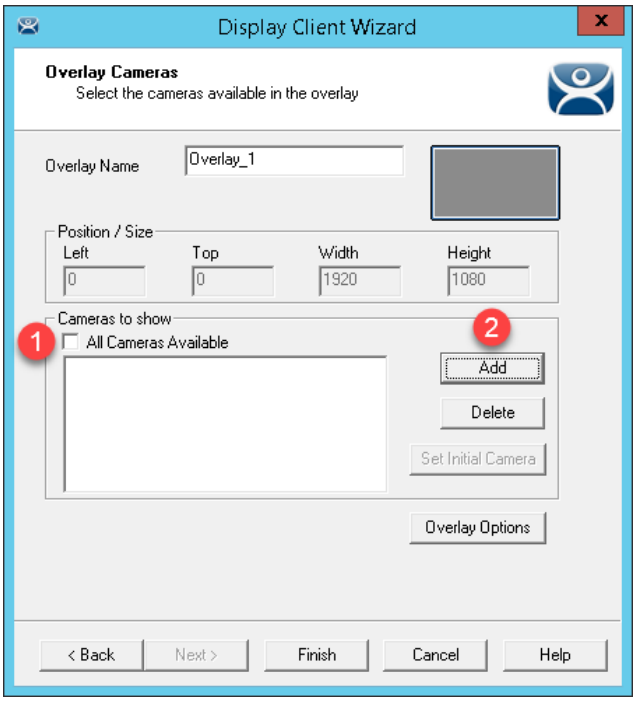
7. From the **Client Name** page of the wizard, enter *IPC_Video* as the **Client Name**. Click the **Next** button.



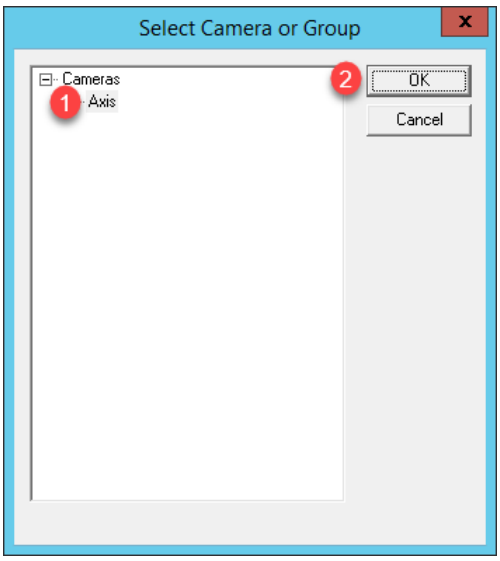
8. From the **Display Client Options** page of the wizard, click the **Next** button.
9. From the **Overlay Layout** page of the wizard, select **1x1** from the **Choose Camera Layout** drop down list and select **1920x1080** from the **Display Size** drop down list. Click the **Next** button.



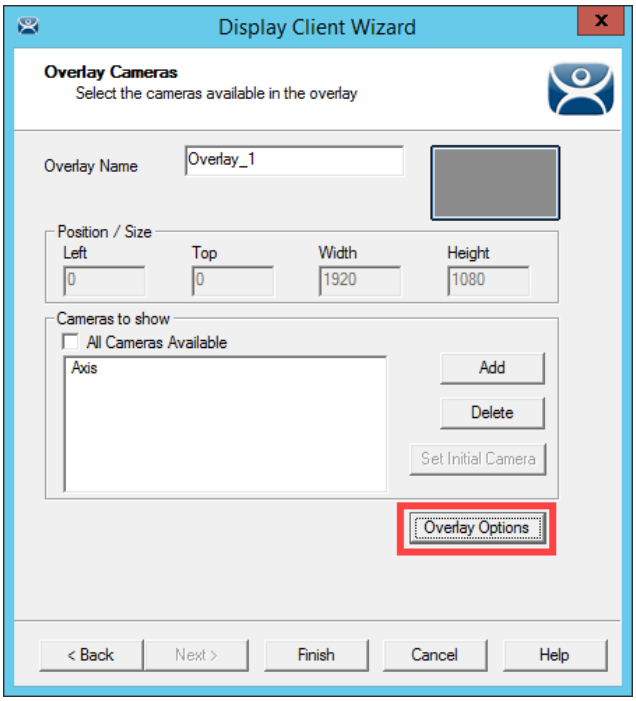
10. From the **Overlay Cameras** page of the wizard, **un**-check the **All Cameras Available** checkbox and click the **Add** button.



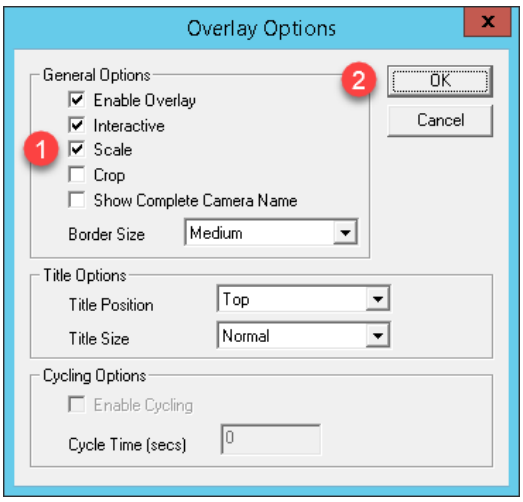
11. From the **Select Camera or Group** window, select the **Axis** item and click the **OK** button.



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.

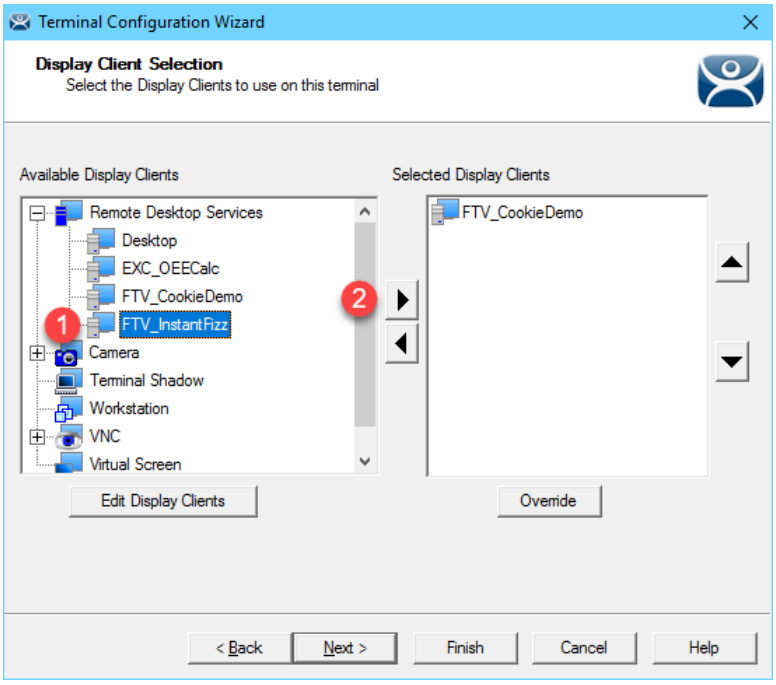


ThinManager also supports USB Cameras as sources of content. A camera's video stream can be delivered as its own Display Client, or as an overlay to an existing Display Client. ThinManager supports real time streaming protocols (RTSP) like H.264. RTSP can be decoded by the terminal's CPU or for certain 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.

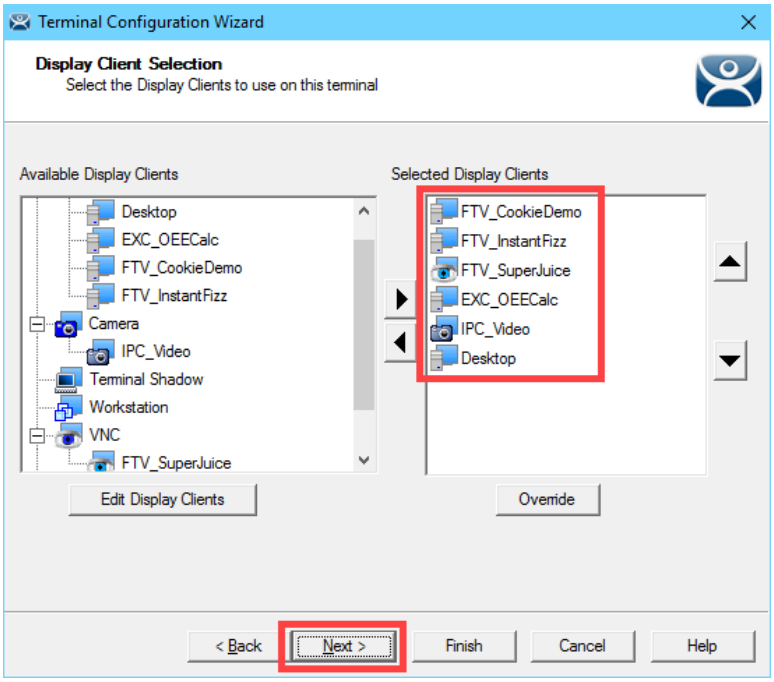
Apply Display Clients to Terminal and Enable Tiling

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

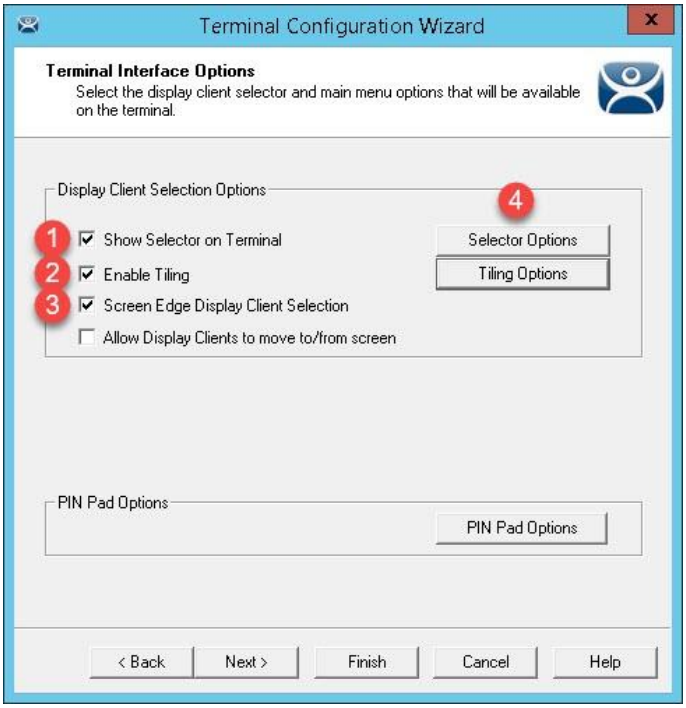
2. From the **Terminals** tree, double click the **VersaView5200** terminal to launch the **Terminal Configuration Wizard**.
3. Click the **Next** button on the **Terminal Name** page of the wizard.
4. Click the **Next** button on the **Terminal Hardware** page of the wizard.
5. Click the **Next** button 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.



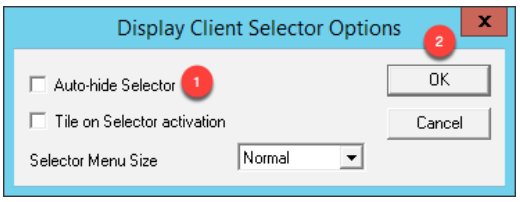
8. Repeat the previous step for the **FTV_SuperJuice, EXC_OEECalc, IPC_Video** and **Desktop Display Clients**. Click the **Next** button.



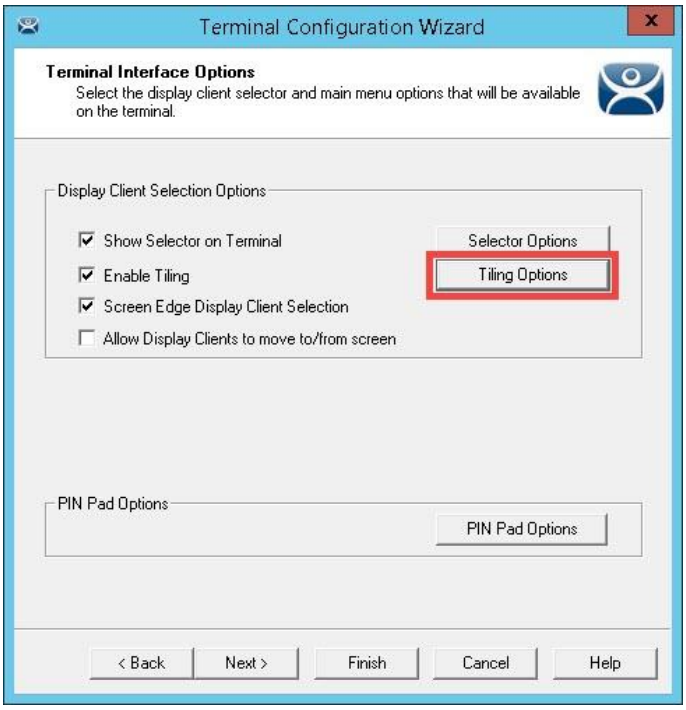
9. On the **Terminal Interface Options** page of the wizard, make sure **Show Selector on Terminal, Enable Tiling and Screen Edge Display Client Selection** are checked. Click the **Selector Options** button.



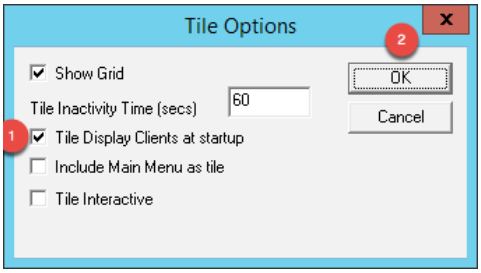
10. Click on the **Selector Options** button. **Un**check **Auto-hide Selector** and click the **OK** button.



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

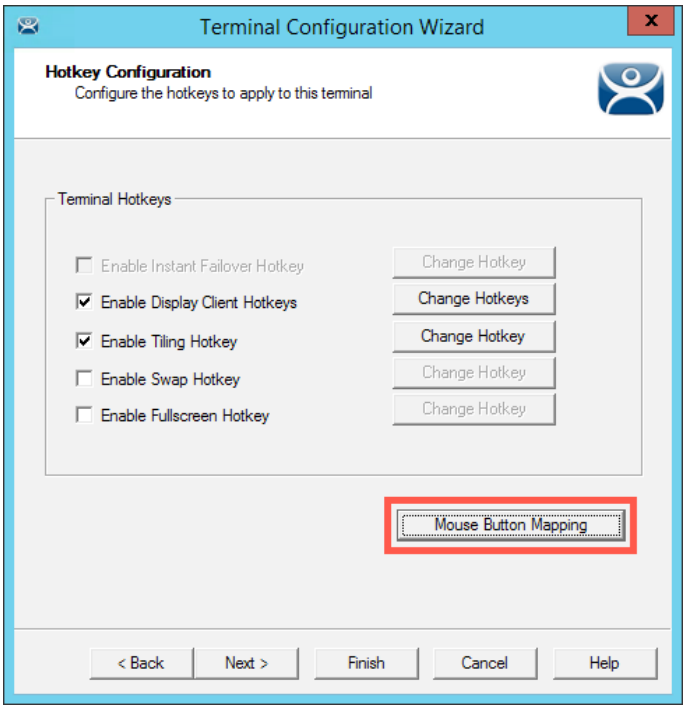


12. Make sure **Show Grid** is checked, and also check **Tile Display Clients at startup**. Click the **OK** button.

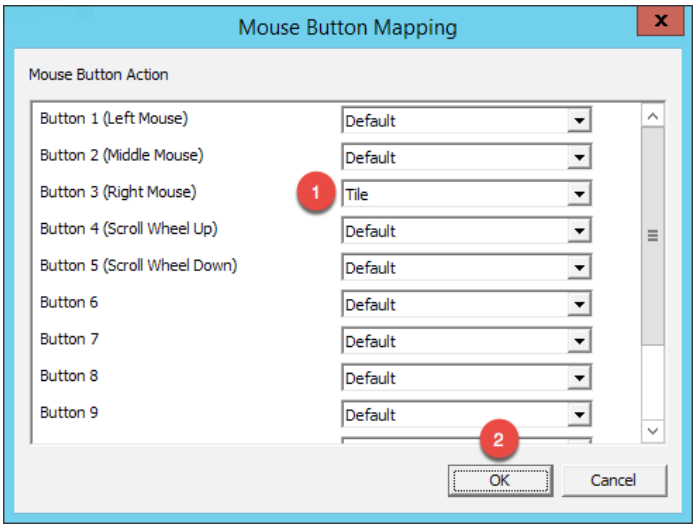


13. Click the **Next** button when you return to the **Terminal Interface Options** page of the wizard.

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.

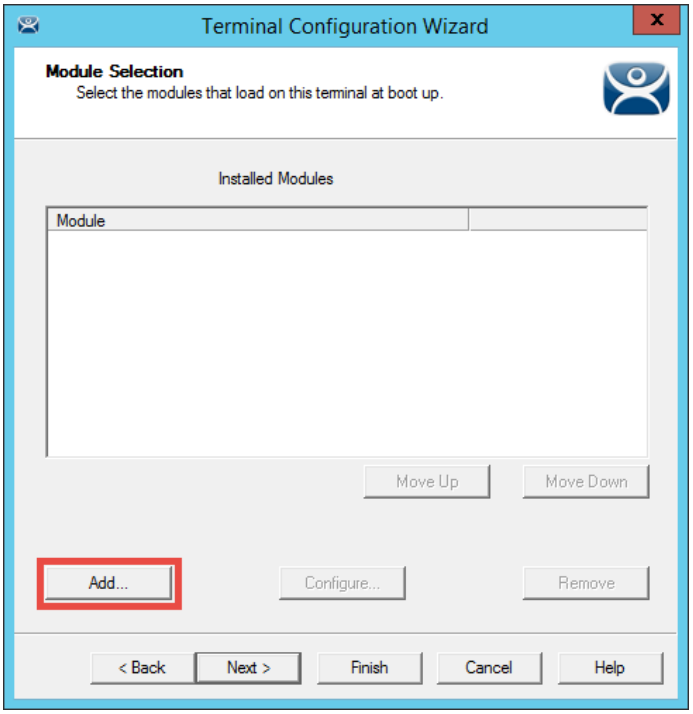


15. From the **Mouse Button Mapping** dialog box, select **Tile** from the **Button 3 (Right Mouse)** drop down list. Click the **OK** button followed by the **Next** button.

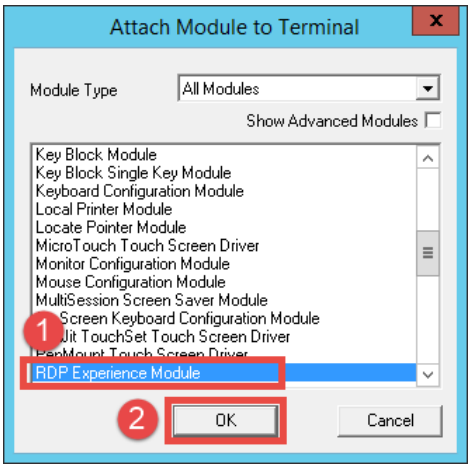


ThinManager 9 introduced more mouse button mapping options, including all mouse button types to a number of new mouse button actions like Swap and Full Screen, both of which are applicable to Virtual Screens, which will be introduced in the next section.

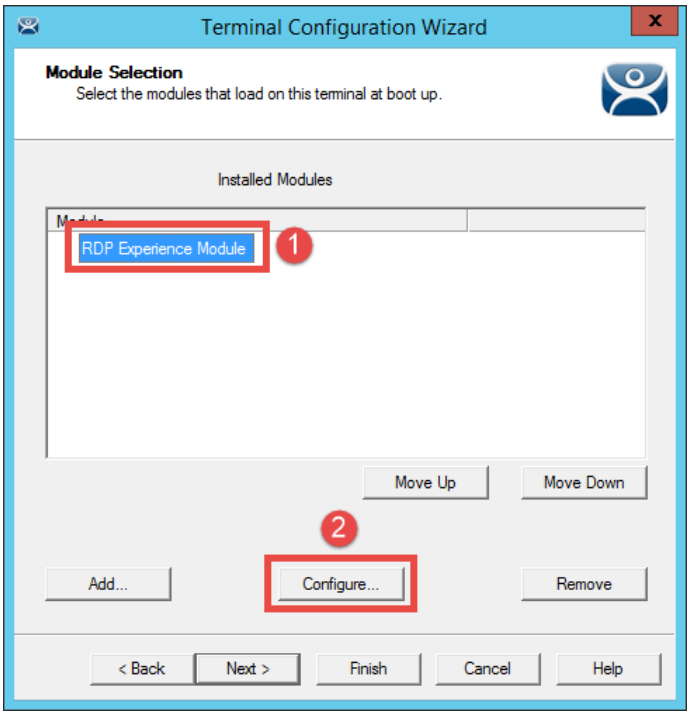
16. From the **Log In Information** page of the wizard, click the **Next** button.
17. From the **Video Resolution** page of the wizard, click the **Next** button.
18. From the **Module Selection** page of the wizard, click the **Add…** button.



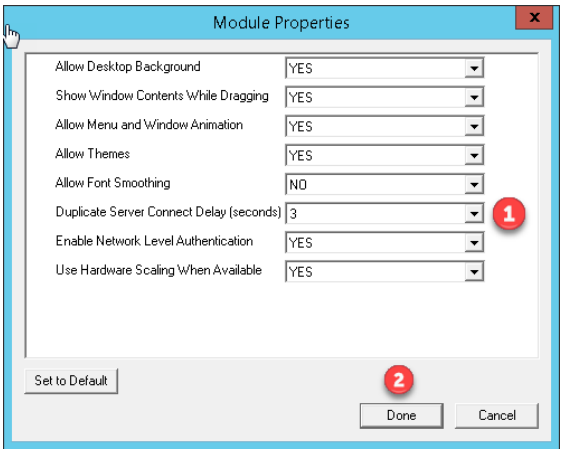
19. From the **Attach Module to Terminal** dialog box, scroll down and select the **RDP Experience Module** and click the **OK** button.



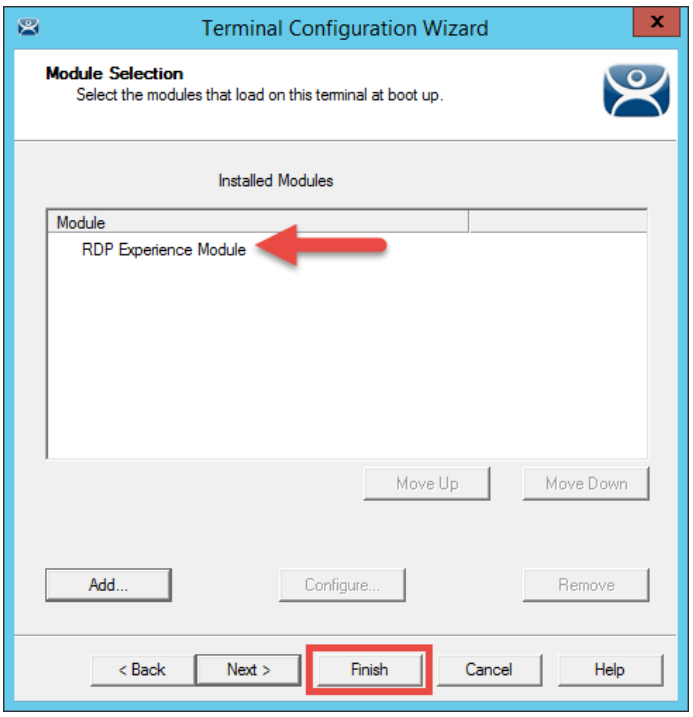
20. Back on the **Module Selection** page of the wizard, select the **RDP Experience Module** and click the **Configure** button.



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



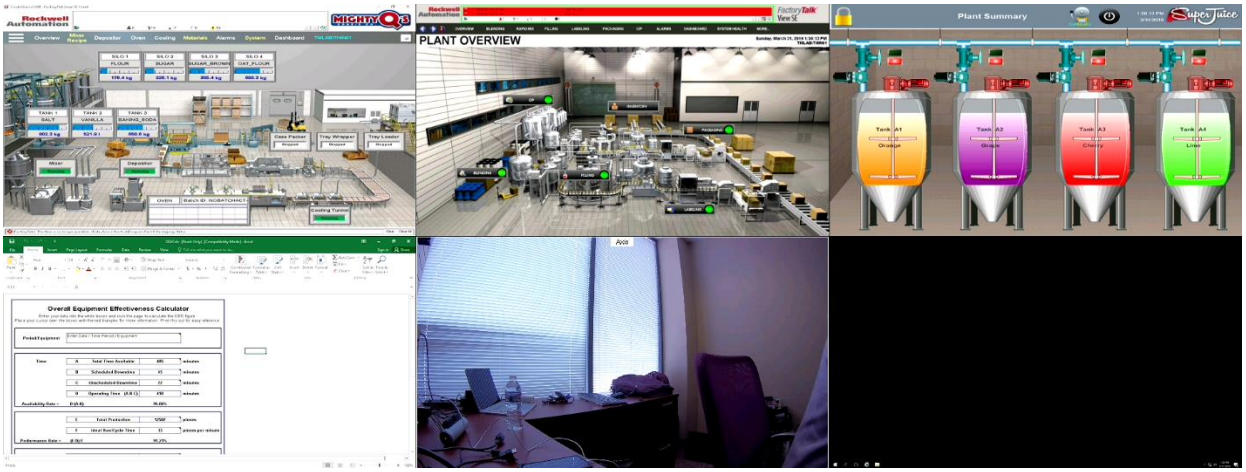
22. Back on the **Module Selection** page of the wizard, click the **Finish** button.



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**. **<u>If you see an Activation window in Microsoft Excel, just ignore it.</u>**



> 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**.

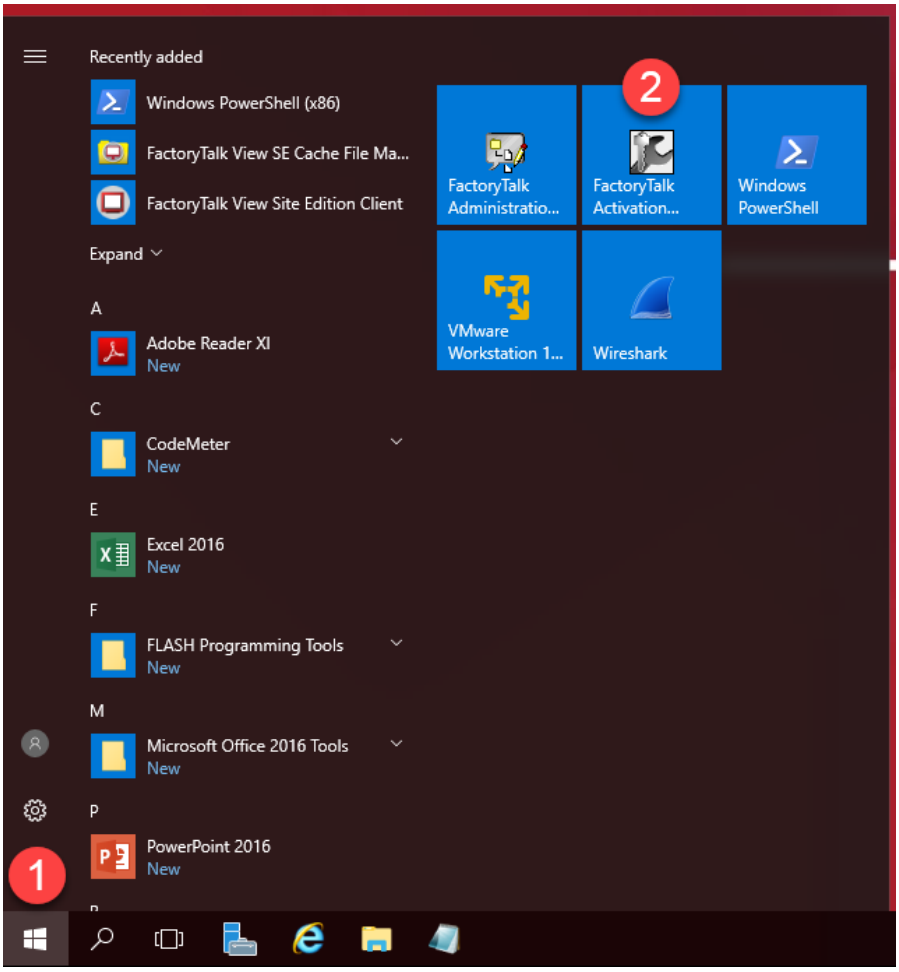
> You can deploy up to 25 (a 5x5 Grid) **Display Clients** using **Tiling Mode** to a single monitor. If you are not using **Tiling Mode**, there is no limit to the number of **Display Clients** that can be applied to a single monitor. All of the processing required for this content is not occurring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

FactoryTalk View SE Client Licensing Benefits

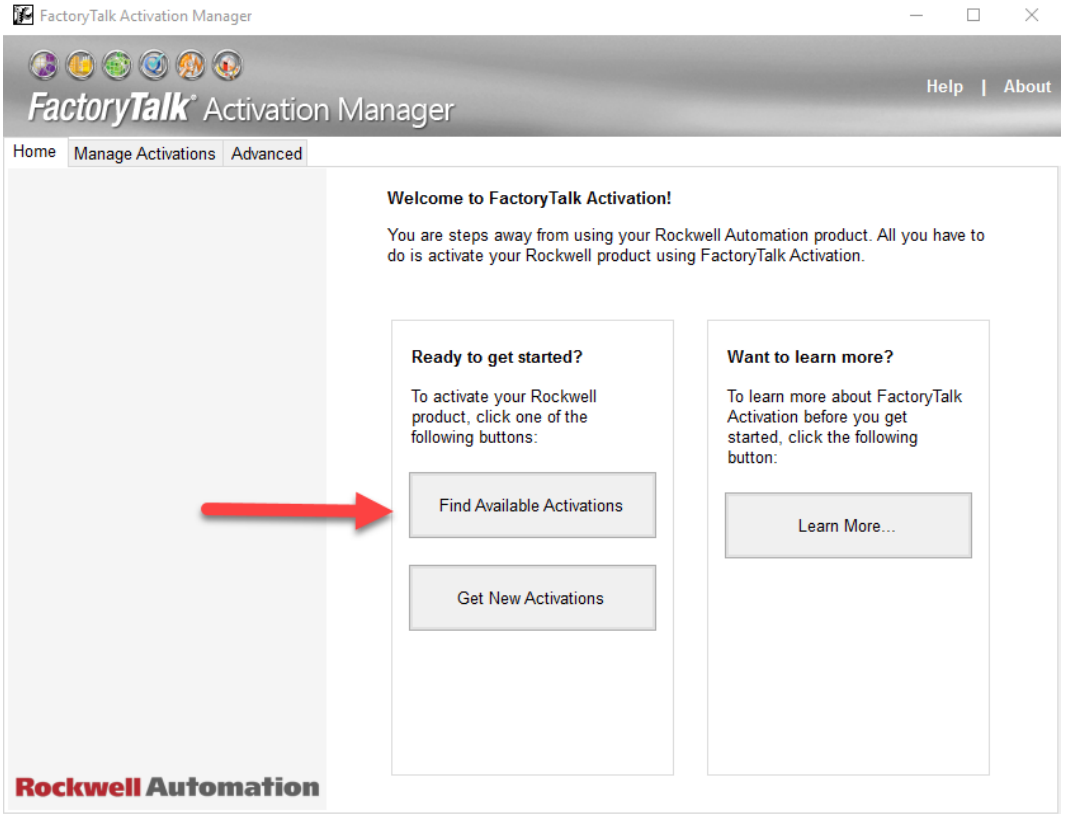
The FactoryTalk View Site Edition Client consumes one SE Client license for each unique session running on a Remote Desktop Server that launches **DisplayClient.exe** in a distributed architecture. With the release of ThinManager 11.0 and FactoryTalk View SE 11.0, a single FactoryTalk View SE Client 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.

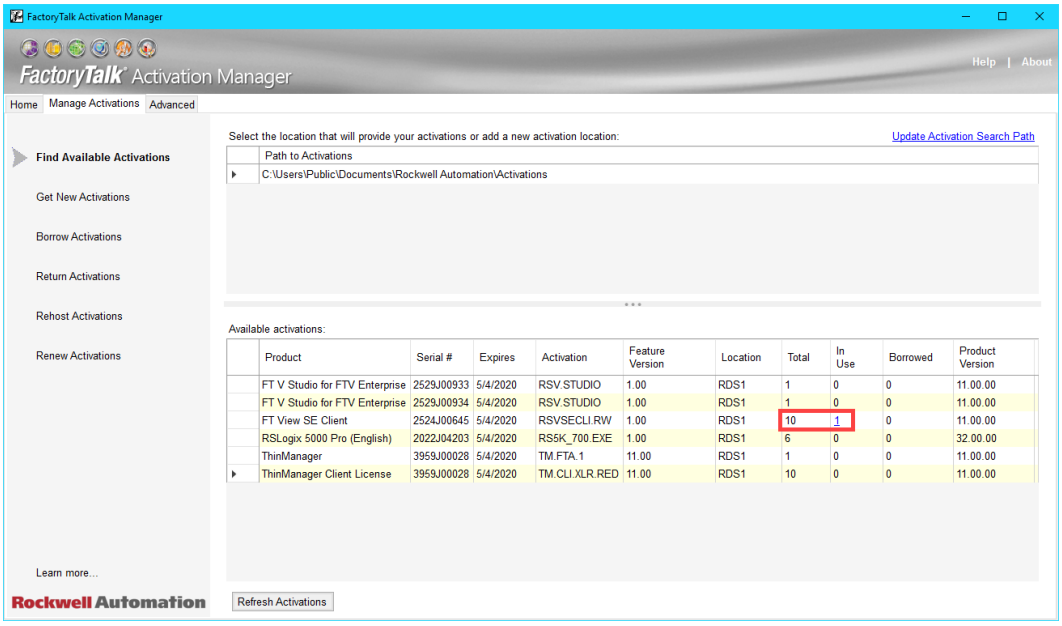
1. From the **Start Menu** click the **FactoryTalk Activation Manager** icon.



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



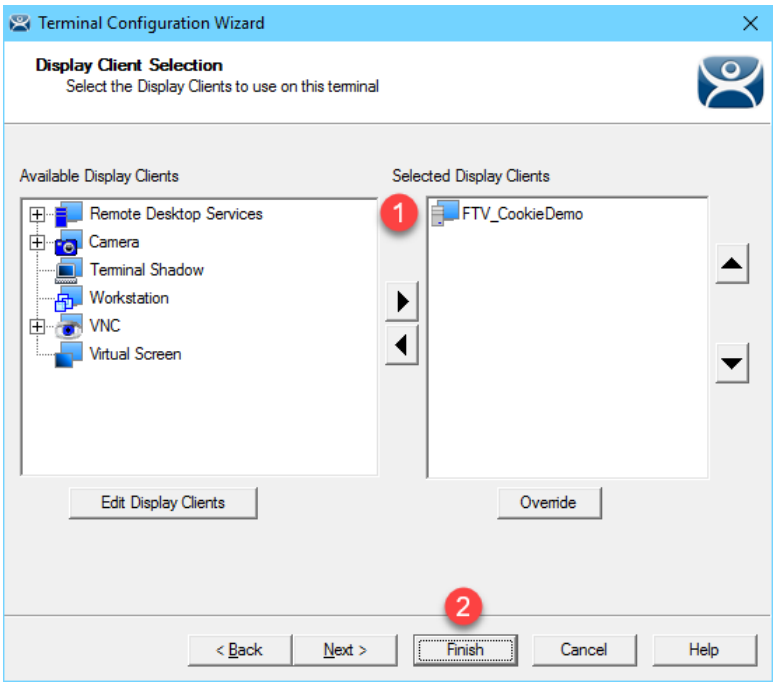
3. Here you will see all the FactoryTalk Activations for the local server. Find the **FactoryTalk View SE Client** item in the list and notice that only 1 of the 10 SE Client licenses is currently in use despite running 2 separate sessions of the **FactoryTalk View SE Client** on the virtual thin client.



4. 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.

Checkpoint Question: https://thinmanager.com/cloudlabs/section07/

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

Section 8: 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:

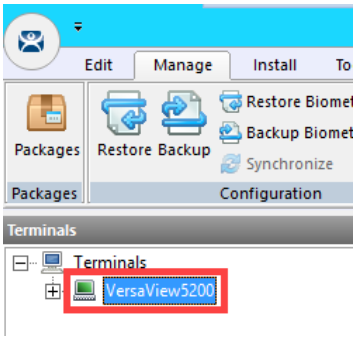
1. Split Content across Multiple Monitors
2. Create Virtual Screen Display Client
3. Apply Virtual Screen to Terminal
4. Add Virtual Screen Swapping

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**.

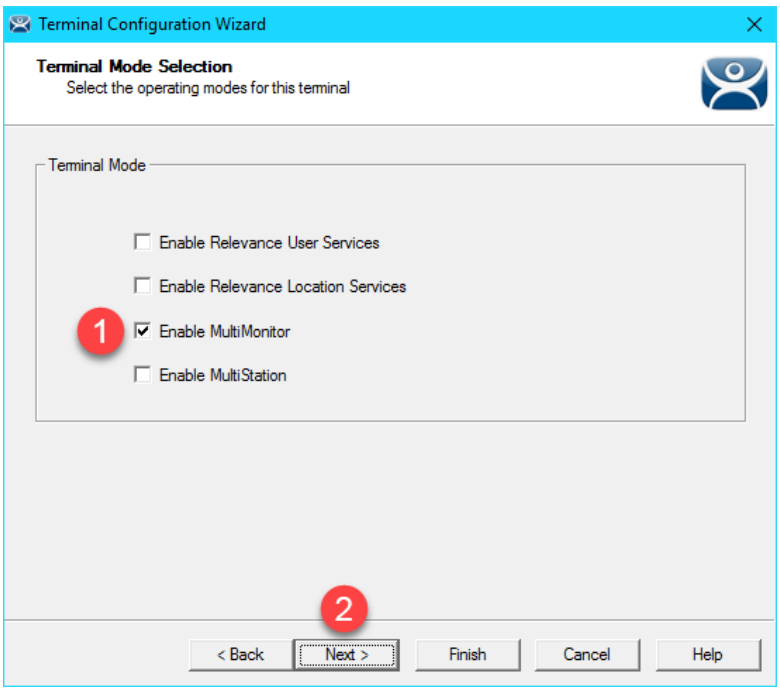
1. If not already there, return to **ThinManager** on **RDS1**.
2. Click the **Terminals** tree selector icon.

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

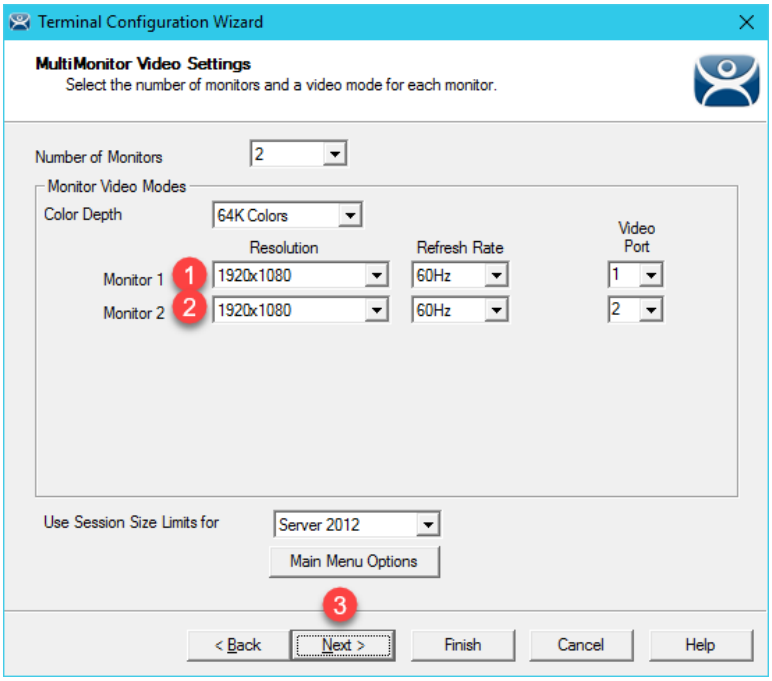


4. Click the **Next** button on the **Terminal Name** page of the wizard.
5. Click the **Next** button on the **Terminal Hardware** page of the wizard.
6. Click the **Next** button on the **Terminal Options** page of the wizard.

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.

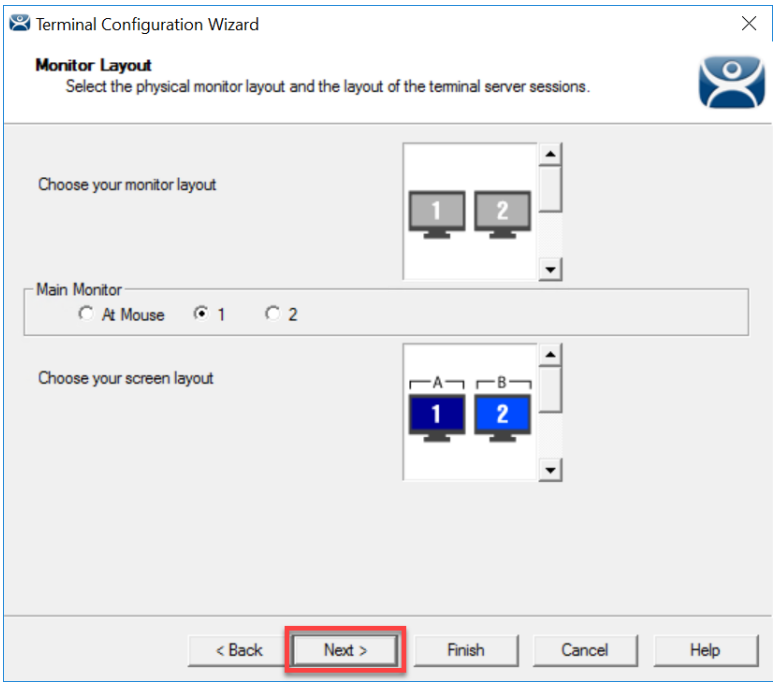


> The **Use Session Size Limits for** drop down list allows you to specify either **Server 2012** or **Server 2008 R2** session size limits. Prior to Windows Server 2012, the maximum screen resolution for an RDP session was 4096 x 2048. Windows Server 2012 has increased this maximum to 8192 x 8192.

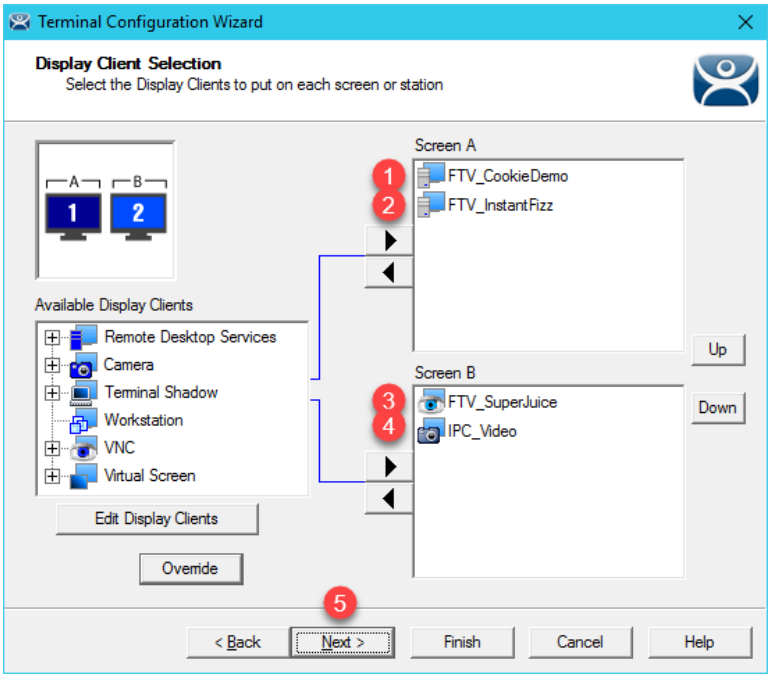
9. From the **Monitor Layout** wizard, accept the defaults. This is where you tell ThinManager how your monitors are physically oriented via the **Monitor Layout** section, as well as how to treat each individual monitor via the **Screen**

Layout section. Click the **Next** button.

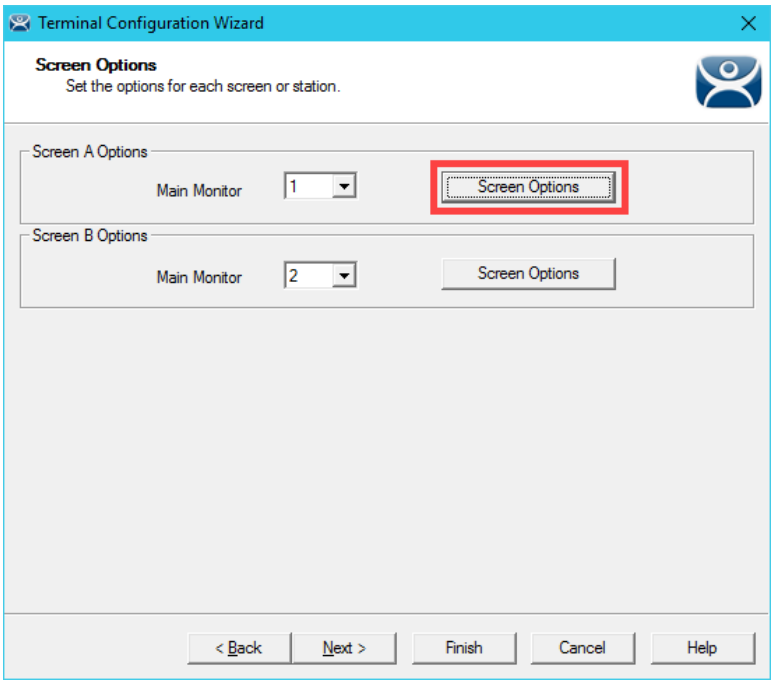
Screens are treated individually by default, which is referred to as **Screening**. Or the screens can be combined logically, which is referred to as **Spanning**.



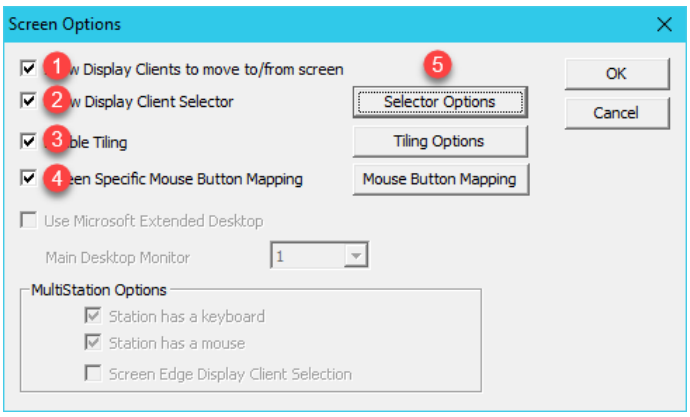
10. Select **FTV_CookieDemo** from the **Available Display Clients** list and click the **Right Arrow** button for **Screen A** to move it to the **Selected Display Clients** list. Repeat this step to move the **FTV_InstantFizz Display Client** to **Screen A** as well. Select **FTV_SuperJuice** from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



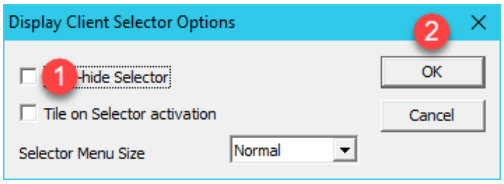
11. On the **Screen Options** page of the wizard, click the **Screen Options** button for **Screen A**.



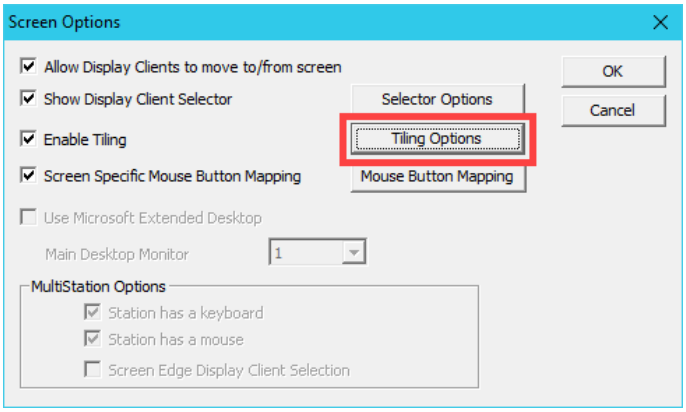
12. Make sure **Show Display Client Selector, Enable Tiling, Allow Display Clients to move to/from screen** and **Screen Specific Mouse Button Mapping** checkboxes are checked. Click the **Selector Options** button.



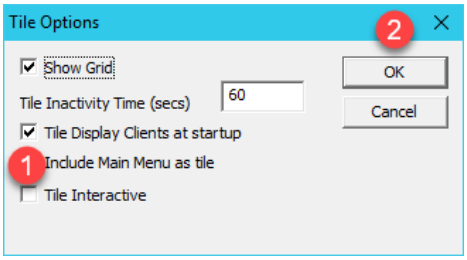
13. From the **Display Client Selector Options** popup, uncheck **Auto-hide Selector** and click the **OK** button.



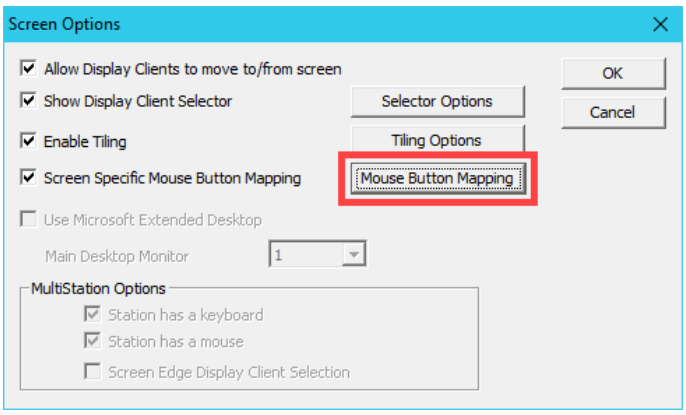
14. Back on the **Screen Options** popup, now click the **Tiling Options** button.



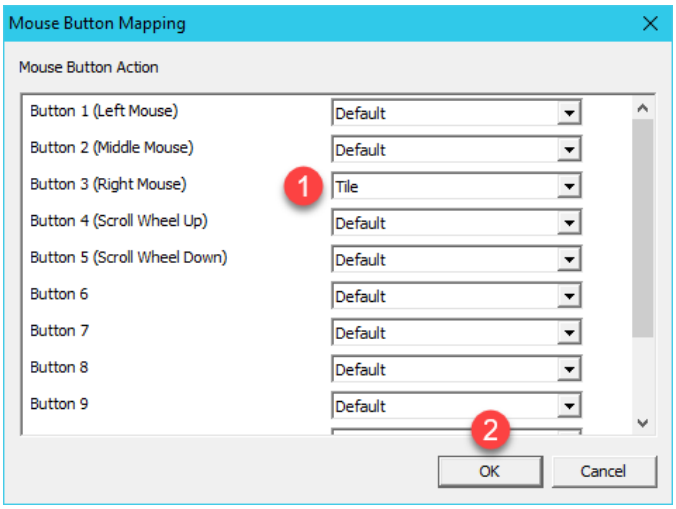
15. From the **Tile Options** popup, check the **Tile Display Clients and startup** check box. Click the **OK** button on the **Tile Options** popup.



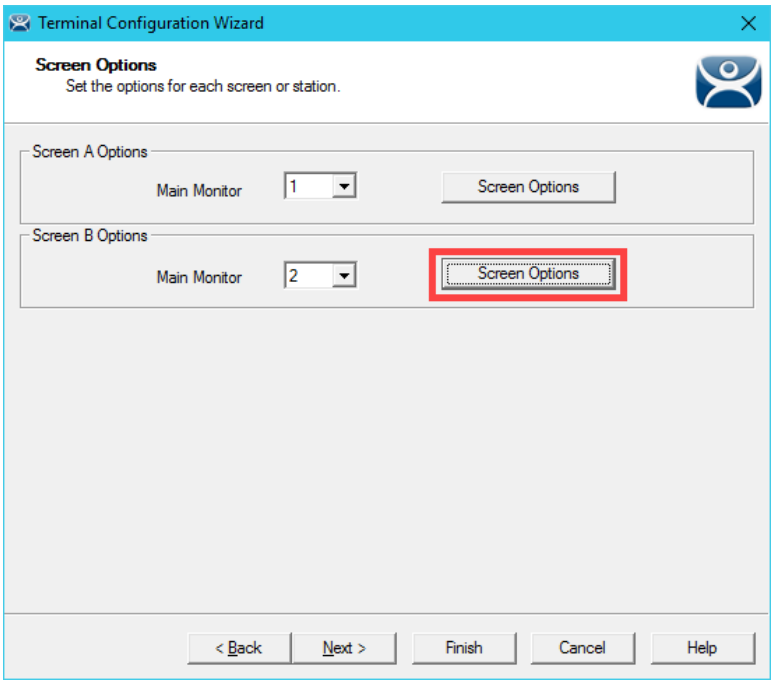
16. Click the **Mouse Button Mapping** button on the **Screen Options** popup.



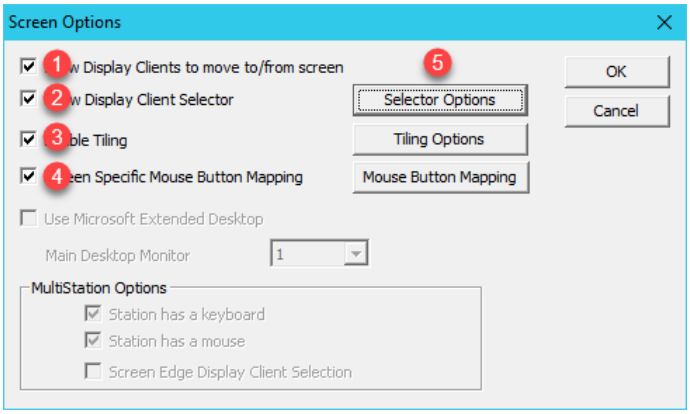
17. From the **Mouse Button Mapping** dialog box, select **Tile** from the **Button 3 (Right Mouse)** drop down list. Click the **OK** button.



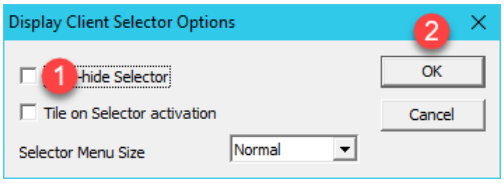
18. Click the **OK** button on the **Screen Options** popup.
19. Back on the **Screen Options** page of the wizard, click the **Screen Options** button for **Screen B**.



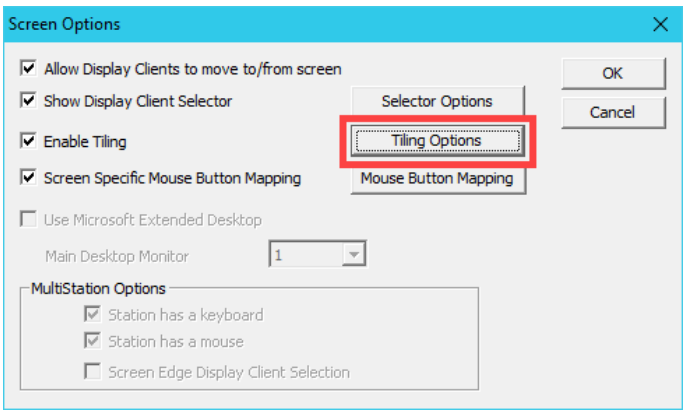
20. Make sure **Show Screen Specific Mouse Button Mapping** checkboxes are checked. Click the **Selector Options** button.



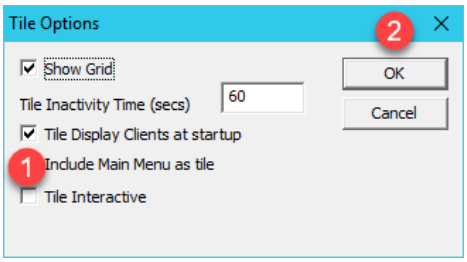
21. From the **Display Client Selector Options** popup, uncheck **Auto-hide Selector** and click the **OK** button.



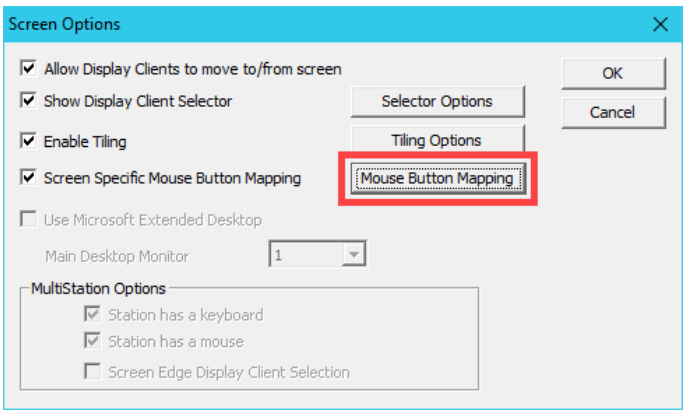
22. Back on the **Screen Options** popup, now click the **Tiling Options** button.



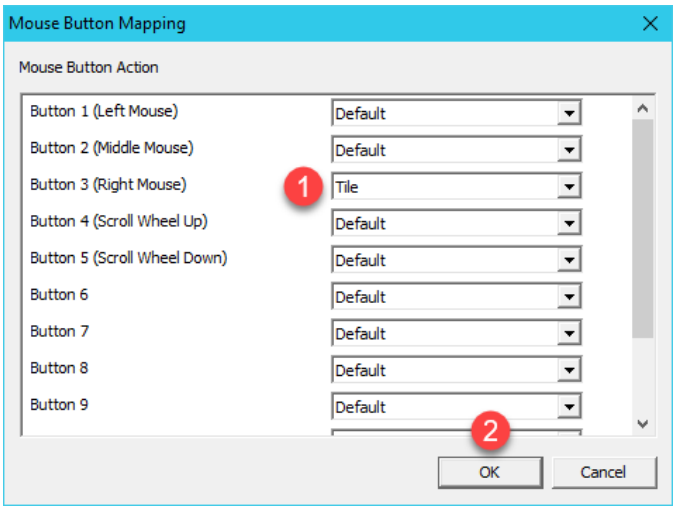
23. From the **Tile Options** popup, check the **Tile Display Clients and startup** check box. Click the **OK** button on the **Tile Options** popup.



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.

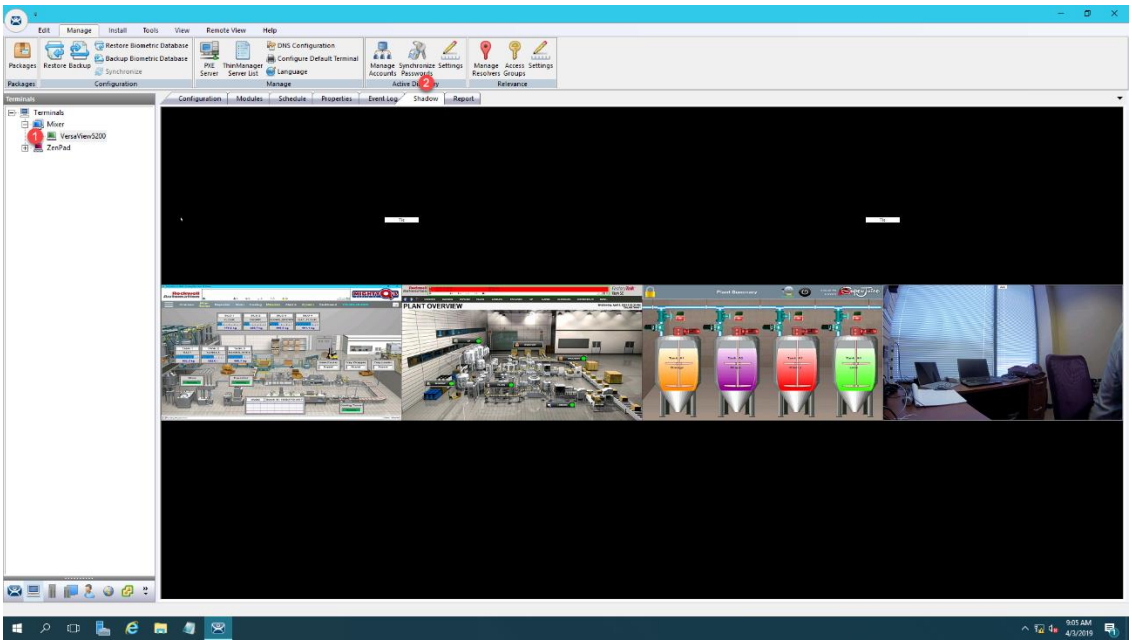


26. Click the **OK** button on the **Screen Options** popup.

27. Click the **Finish** button.

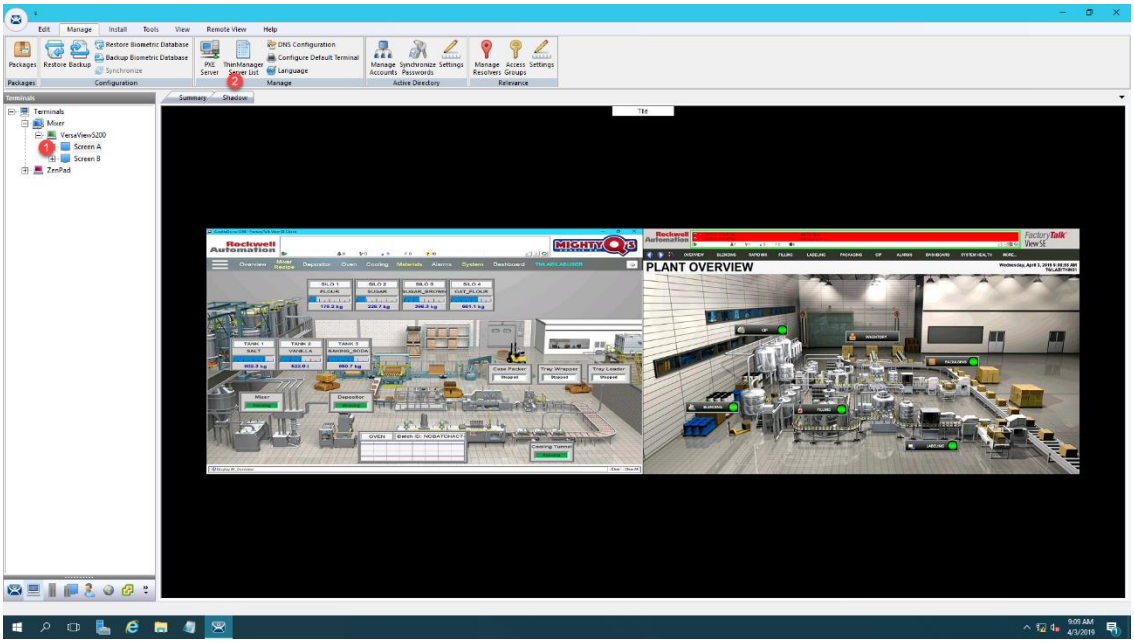
28. Right click the **VersaView5200** terminal from the **Terminals** tree and select **Restart Terminal** to apply the changes. Click **Yes** to the confirmation dialog.

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**.

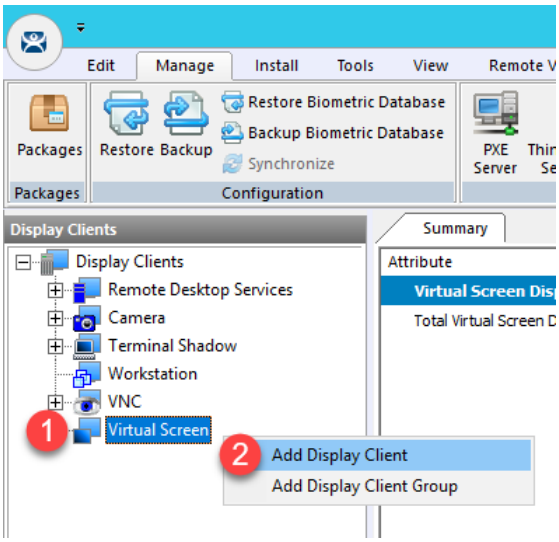


MultiMonitor combined with **Tiling** and/or **Virtual Screens** are extremely powerful tools that really elevate the user experience at the terminal. They are especially valuable in **Control Room** settings, or anywhere centralized monitoring is desired. As previously mentioned, some thin clients can 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.

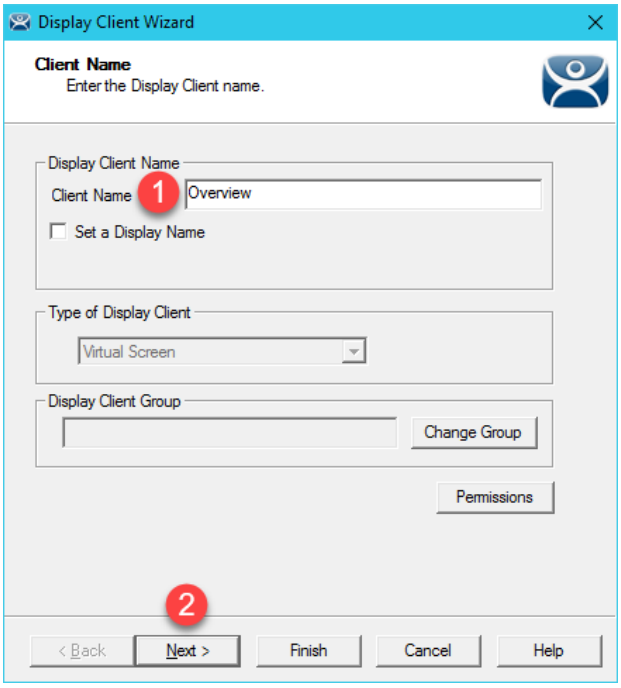
Create Virtual Screen Display Client

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

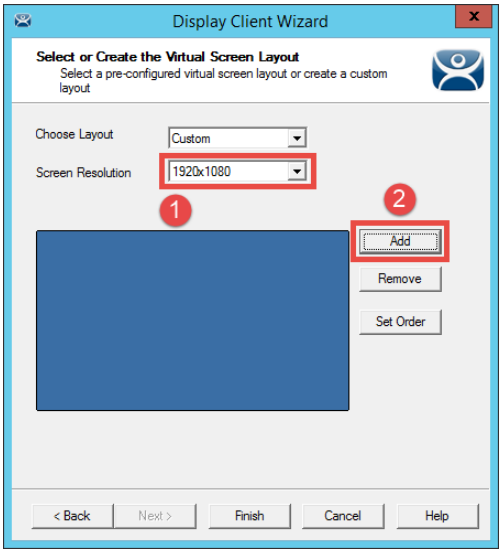
2. Right click the **Virtual Screen** branch and select the **Add Display Client** item.



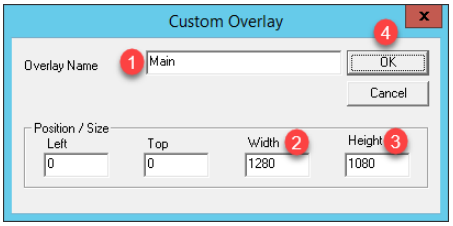
3. From the **Client Name** page of the wizard, enter *Overview* as the **Client Name**. Click the **Next** button.



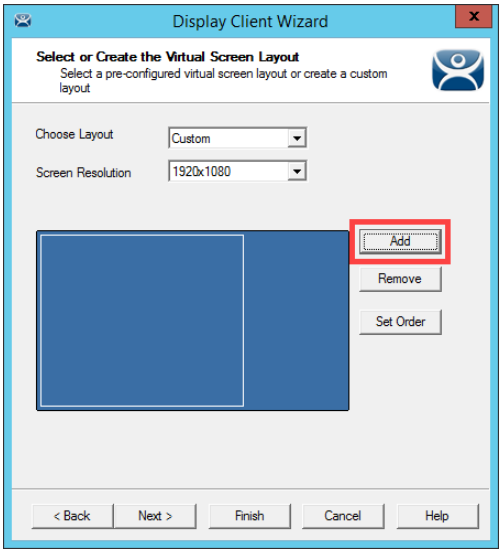
4. From the **Display Client Options** page of the wizard, click the **Next** button.
5. From the **Select or Create the Virtual Screen Layout** page of the wizard, select **1920x1080** from the **Screen Resolution** drop down list and then click the **Add** button.



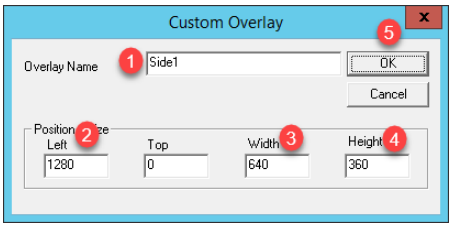
6. From the **Custom Overlay** dialog box, enter *Main* as the **Overlay Name**, keep *0* in the **Left** field, keep *0* in the **Top** field, *1280* in the **Width** field and *1080* in the **Height** field. Click the **OK** button.



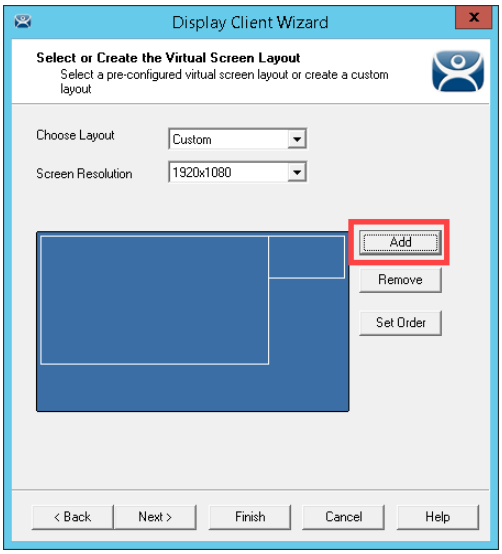
7. Back at the **Select or Create the Virtual Screen Layout** page of the wizard, click the **Add** button again to add another overlay.



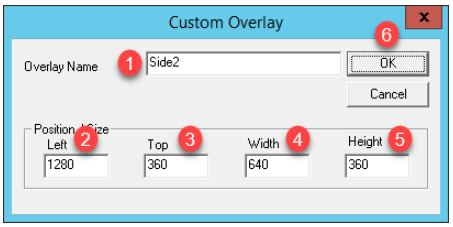
8. From the **Custom Overlay** dialog box, enter *Side1* as the **Overlay Name**, *1280* in the **Left** field, *0* in the **Top** field, *640* in the **Width** field and *360* in the **Height** field. Click the **OK** button.



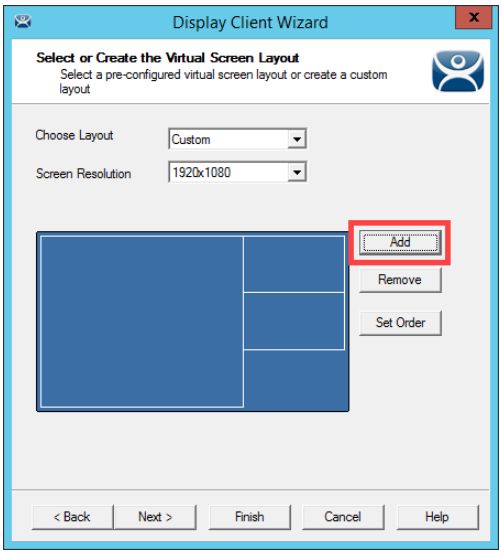
9. Back at the **Select or Create the Virtual Screen Layout** page of the wizard, click the **Add** button again to add another overlay.



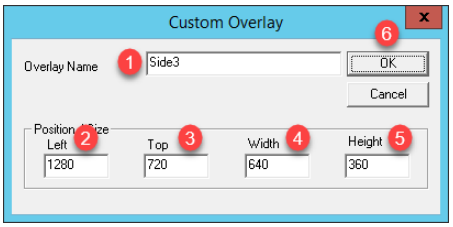
10. From the **Custom Overlay** dialog box, enter *Side2* as the **Overlay Name**, *1280* in the **Left** field, *360* in the **Top** field, *640* in the **Width** field and *360* in the **Height** field. Click the **OK** button.



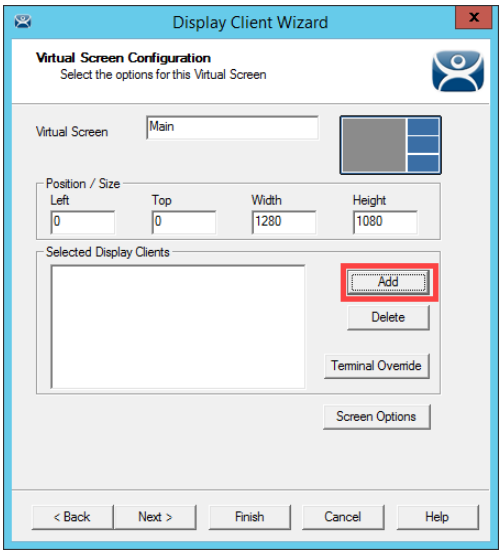
11. Back at the **Select or Create the Virtual Screen Layout** page of the wizard, click the **Add** button again to add another overlay.



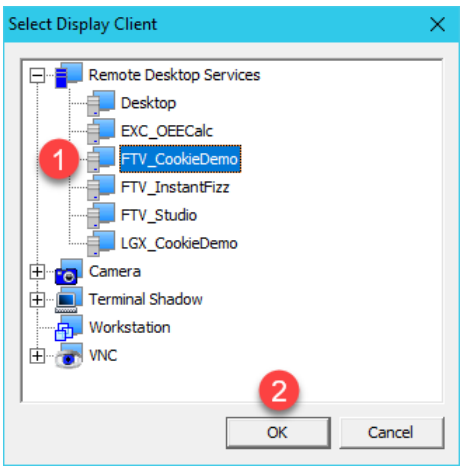
12. From the **Custom Overlay** dialog box, enter *Side3* as the **Overlay Name**, *1280* in the **Left** field, *720* in the **Top** field, *640* in the **Width** field and *360* in the **Height** field. Click the **OK** button, followed by the **Next** button.



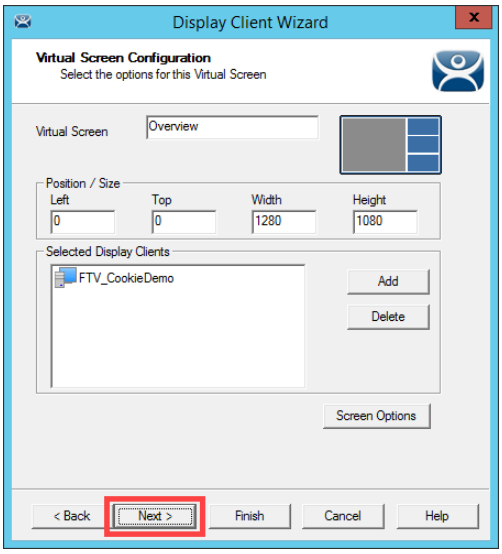
13. We will now assign content to each of the Virtual Screens created, starting with the **Main** Virtual Screen. Click the **Add** button in the **Selected Display Clients** frame.



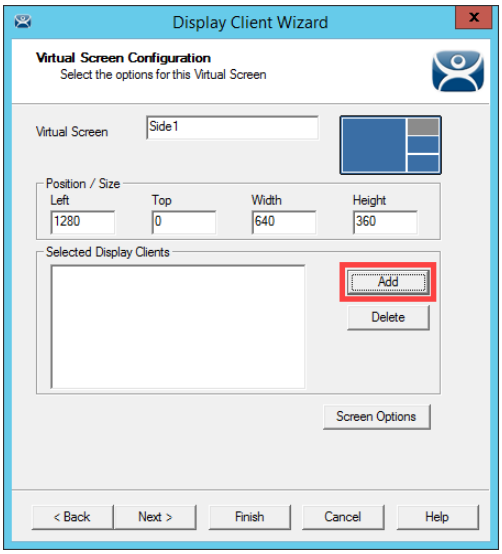
14. Select the **FTV_CookieDemo** item from the list and click the **OK** button.



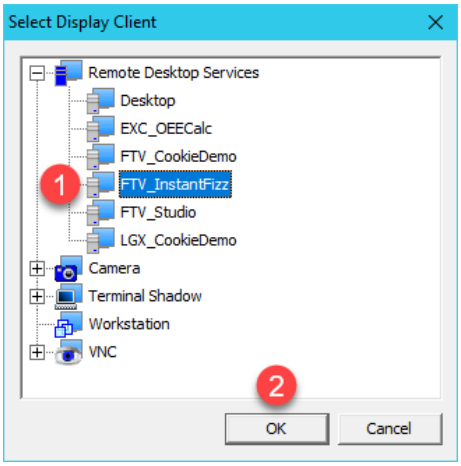
15. Back at the **Virtual Screen Configuration** page of the wizard, click the **Next** button.



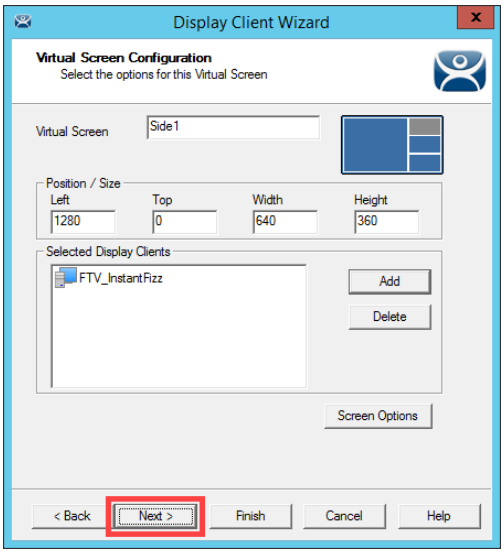
16. Now for the **Side1** Virtual Screen, click the **Add** button.



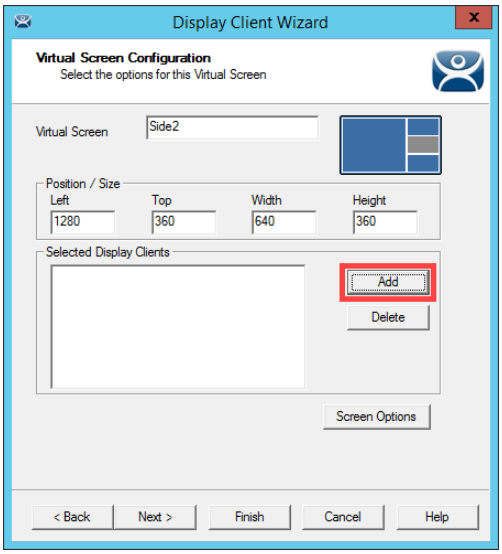
17. Select the **FTV_InstantFizz** item from the list and click the **OK** button.



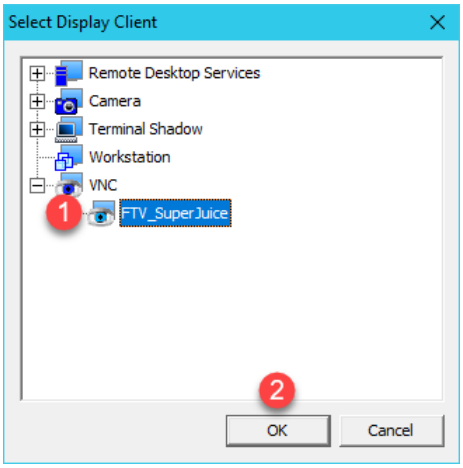
18. Back at the **Virtual Screen Configuration** page of the wizard, click the **Next** button.



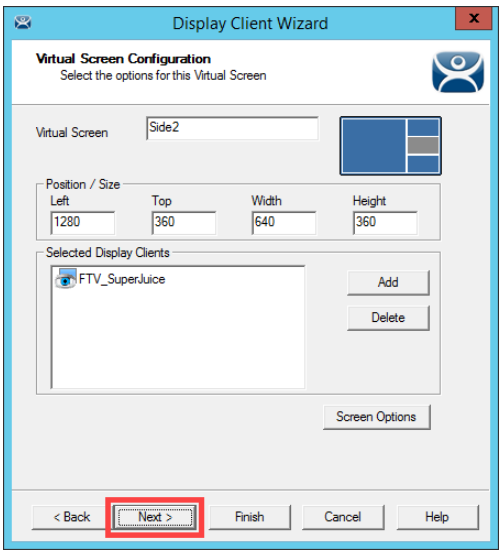
19. Now for the **Side2** Virtual Screen, click the **Add** button.



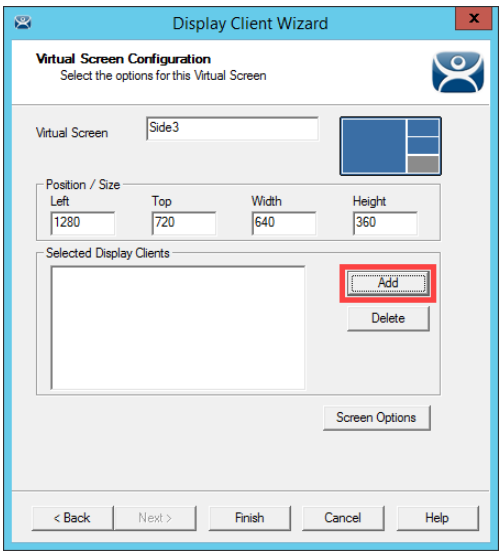
20. Select the **FTV_SuperJuice** item from the list and click the **OK** button.



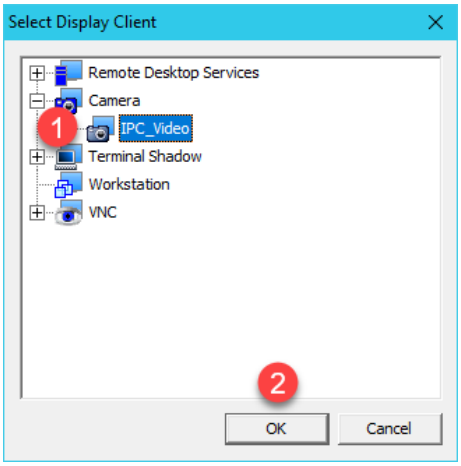
21. Back at the **Virtual Screen Configuration** page of the wizard, click the **Next** button.



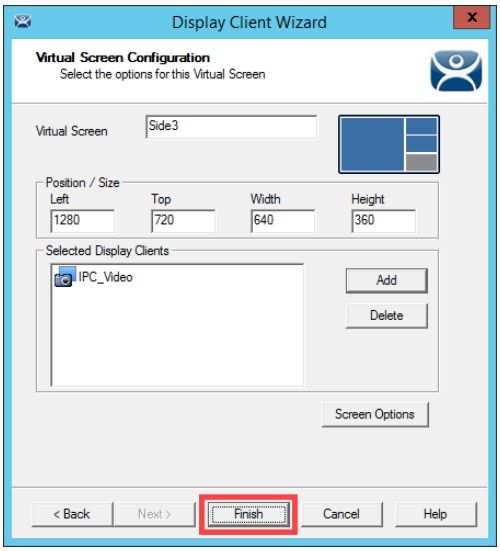
22. Now for the **Side3** Virtual Screen, click the **Add** button.



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



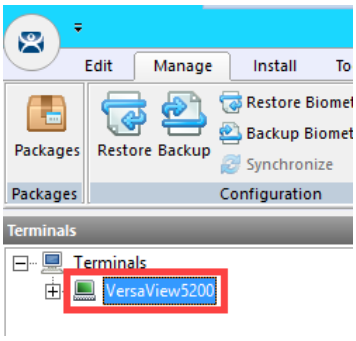
24. Back at the **Virtual Screen Configuration** page of the wizard, click the **Finish** button.



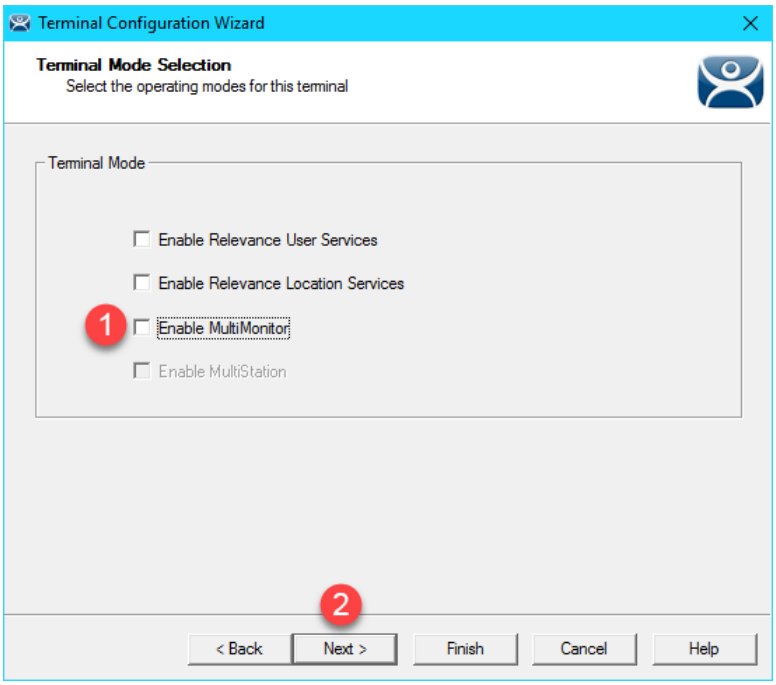
Apply Virtual Screen to Terminal

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

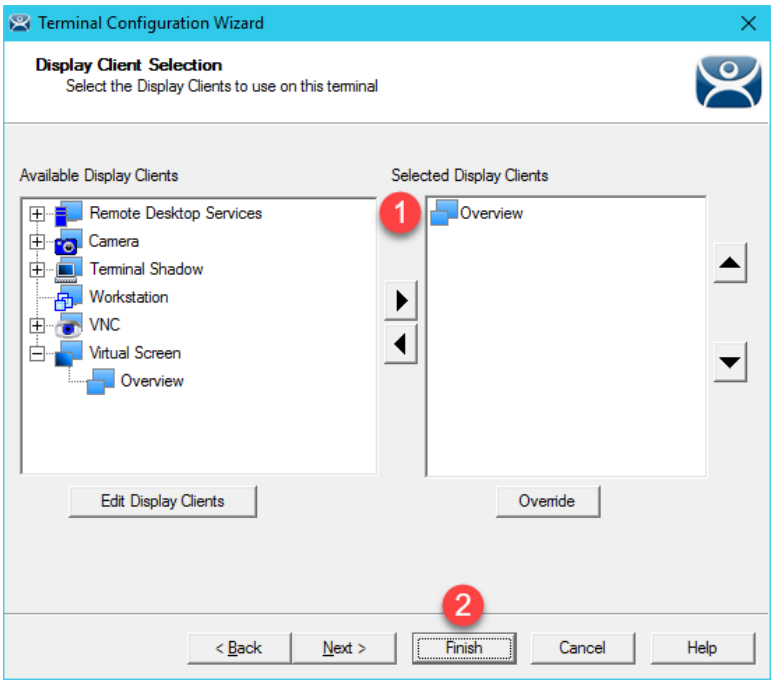
2. Double click the **VersaView5200** terminal.



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**.



7. 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.



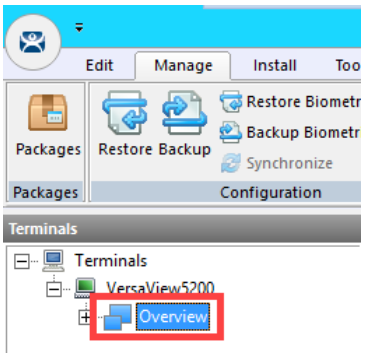
8. Right click the **VersaView5200** terminal and select the **Restart Terminal** item. Click the **Yes** button to confirm.

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.

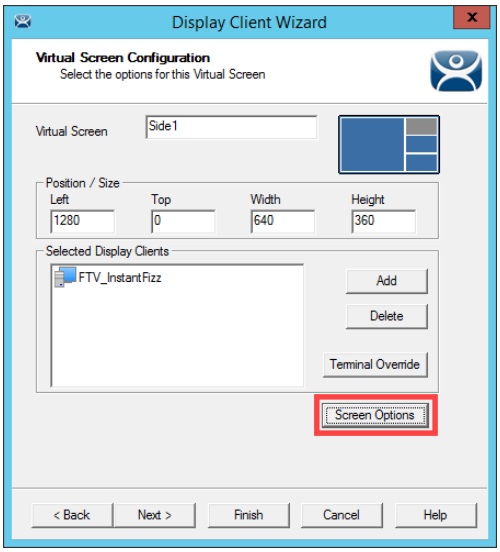
ThinManager 8.1 added support for 4K monitors. For thin clients with the graphics horsepower to drive a 4K display (3840x2160), you can, for example, carve up the 4K display into 4 separate 1920x1080 quadrants and treat them as individual displays within **ThinManager using Virtual Screening**.

Add Virtual Screen Swapping

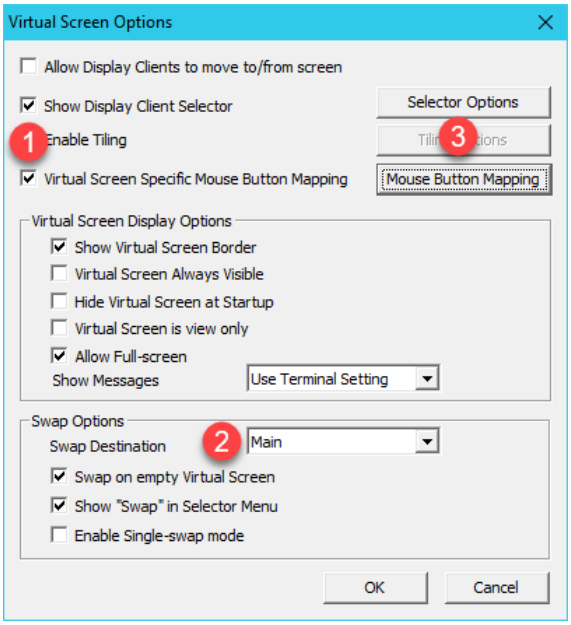
1. From the **Terminals** tree, expand the **VersaView5200** terminal and then double click the **Overview Virtual Screen Display Client** to launch the **Display Client Wizard**.



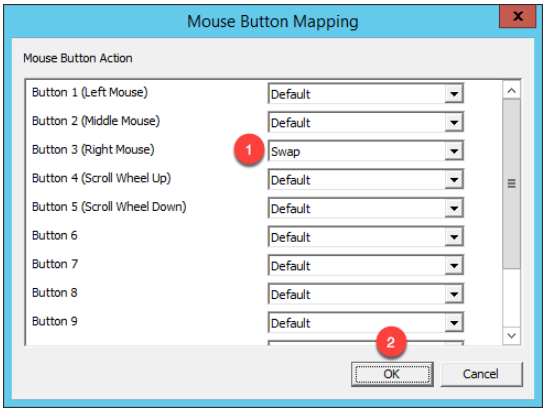
2. From the **Client Name** page of the wizard, click the **Next** button.
3. From the **Display Client Options** page of the wizard, click the **Next** button.
4. From the **Select or Create the Virtual Screen Layout** page of the wizard, click the **Next** button.
5. From the **Main Virtual Screen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



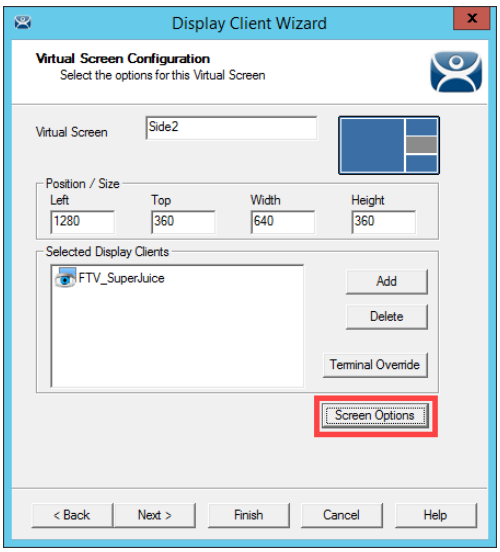
7. From the **Virtual Screen Options** dialog, check the **Virtual Screen Specific Mouse Button Mapping** checkbox, and select **Main** from the **Swap Destination** drop down list. Click the **Mouse Button Mapping** button.



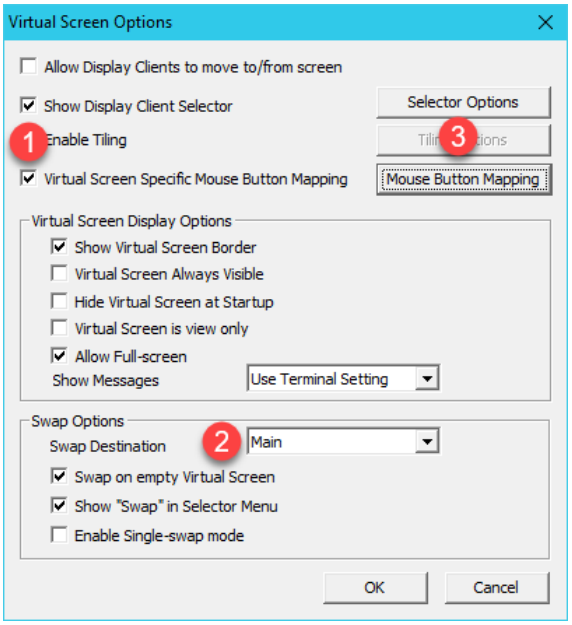
8. From the **Mouse Button Mapping** dialog, select **Swap** from the **Button 3 (Right Mouse)** drop down list. Click the **OK** button twice, followed by the **Next** button.



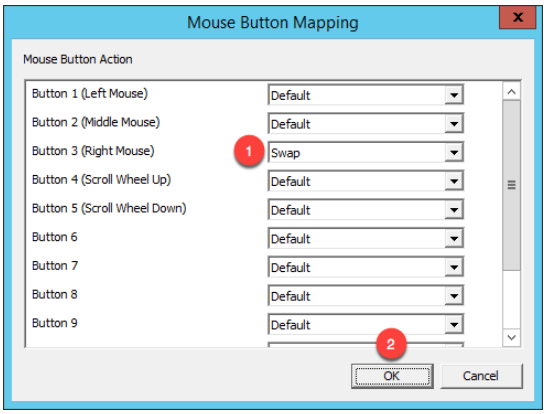
9. Back at the **Side 2 Virtual Screen Configuration** page of the wizard, click the **Screen Options** button.



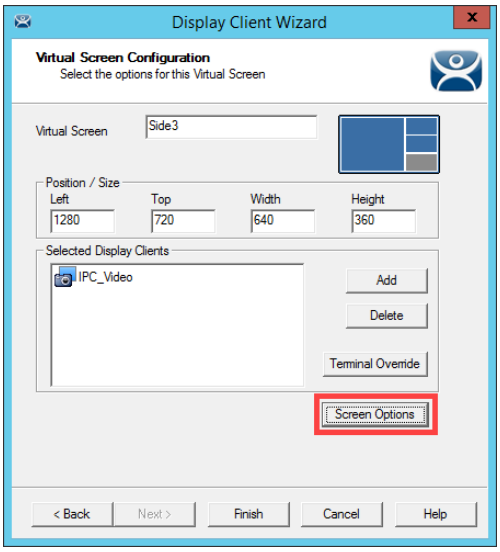
10. From the **Virtual Screen Options** dialog, check the **Virtual Screen Specific Mouse Button Mapping** checkbox, and select **Main** from the **Swap Destination** drop down list. Click the **Mouse Button Mapping** button.



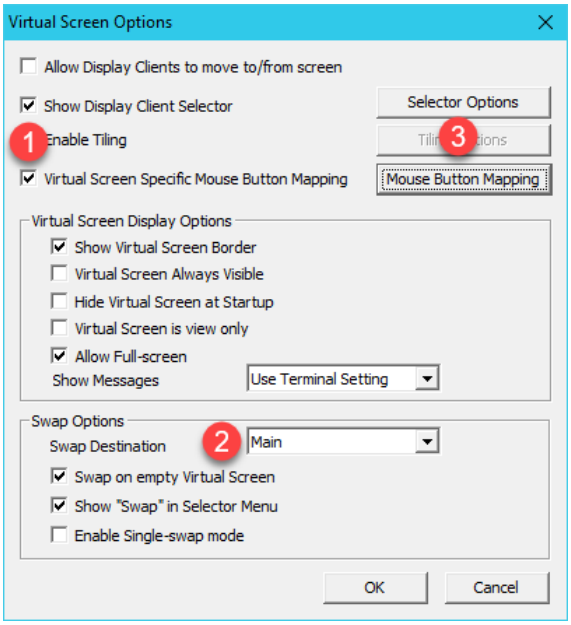
11. From the **Mouse Button Mapping** dialog, select **Swap** from the **Button 3 (Right Mouse)** drop down list. Click the **OK** button twice, followed by the **Next** button.



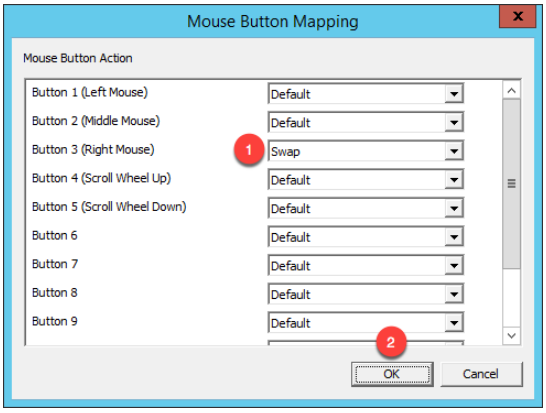
12. Back at the **Side 3 Virtual Screen Configuration** page of the wizard, click the **Screen Options** button.



13. 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.



14. 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.



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

16. Select the **Shadow** tab to see the results. **Right click** on any of the 3 side virtual screens to test the swapping capability.

STOP **Checkpoint Question:** https://thinmanager.com/cloudlabs/section08/

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 9: Relevance User Services - User Based Content Delivery

Overview

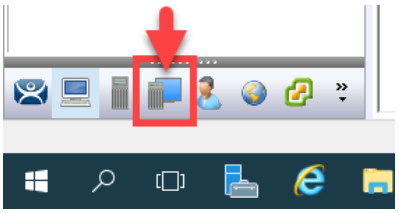
Up to this point in the lab, you have assigned default content to the **Terminal's Profile**. In other words, the content is owned by the terminal and is the same regardless of who is physically at the terminal. You can control a user's access within each application at the terminal by requiring them 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:

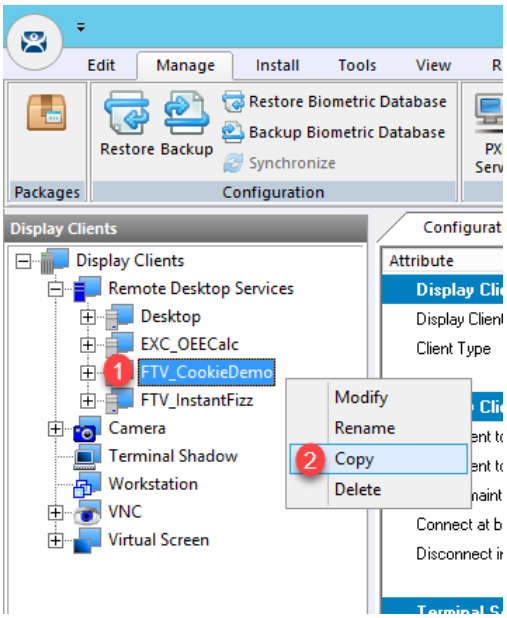
1. Create a View Studio Display Client
2. Create an Engineer User Group
3. Create an Engineer User
4. Enable User Services for Terminal
5. Login as Engineer User
6. Add RF IDeas Badge Reader
7. Configure ThinManager to Cache Password
8. Add Multifactor Authentication with a PIN and Password Storage
9.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

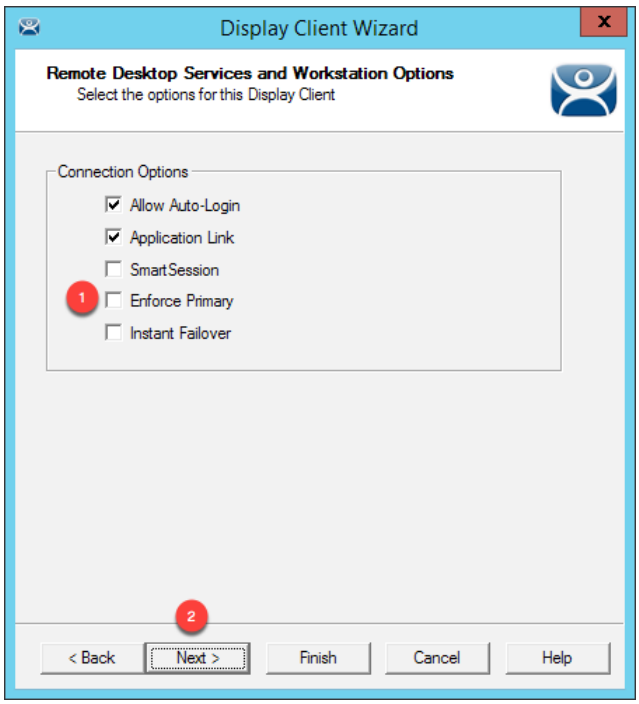


2. From the **Display Clients** tree, expand the **Remote Desktop Services** branch and right click the **FTV_CookieDemo** item and select **Copy**.

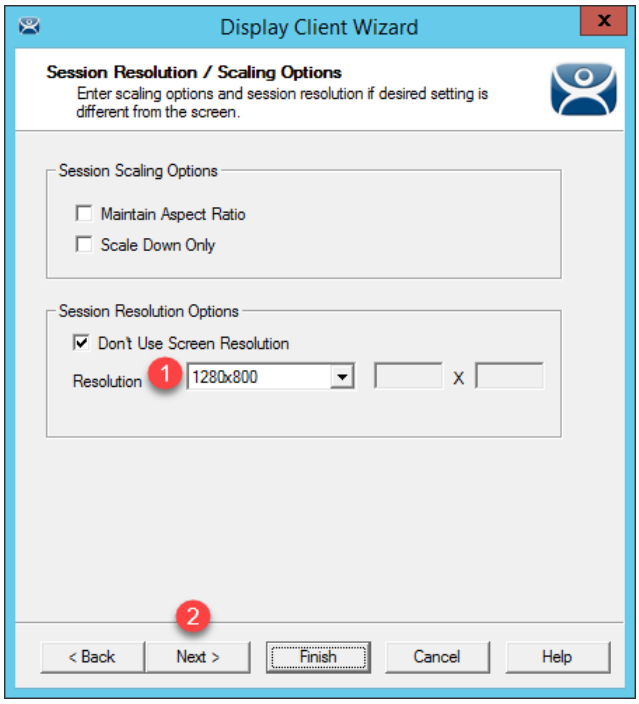


3. Type *FTV_Studio* in the **Enter new Display Client Name** text box and click the **OK** button.
4. Double click the new **FTV_Studio Display Client** item.
5. Click the **Next** button on the **Client Name** page of the wizard.
6. Click the **Next** button on the **Display Client Options** page of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

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

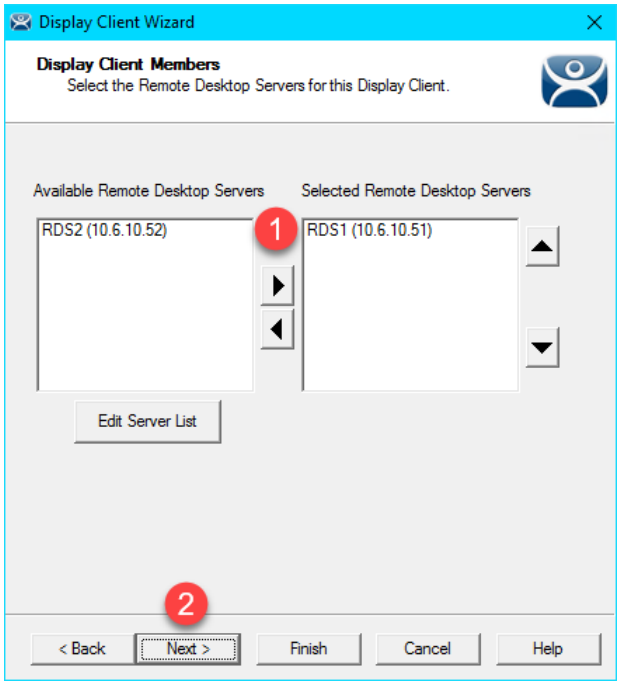


8. From the **Screen Resolution / Scaling Options** page of the wizard, change the **Resolution** to **1280x800**. Click the **Next** button.



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

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


Display Client Wizard
Display Client Members
Select the Remote Desktop Servers for this Display Client.
Available Remote Desktop Servers
Selected Remote Desktop Servers
RDS2 (10.6.10.52)
RDS1 (10.6.10.51)
1
Edit Server List
2
< Back
Next >
Finish
Cancel
Help

10. 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**):

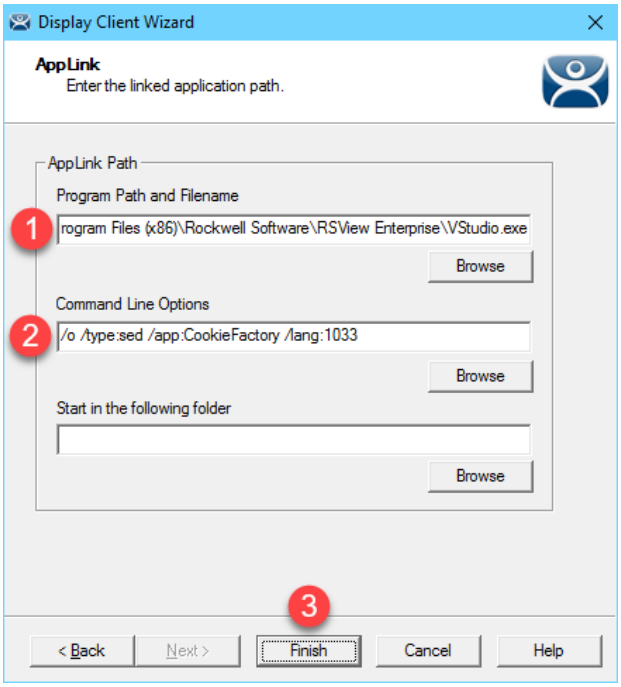
    Program Path and Filename:

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

    Command Line Options:

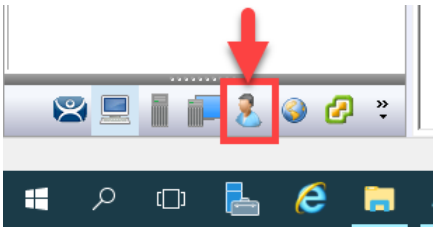
    `/o /type:sed /app:CookieFactory /lang:1033`

    Click the **Finish** button.

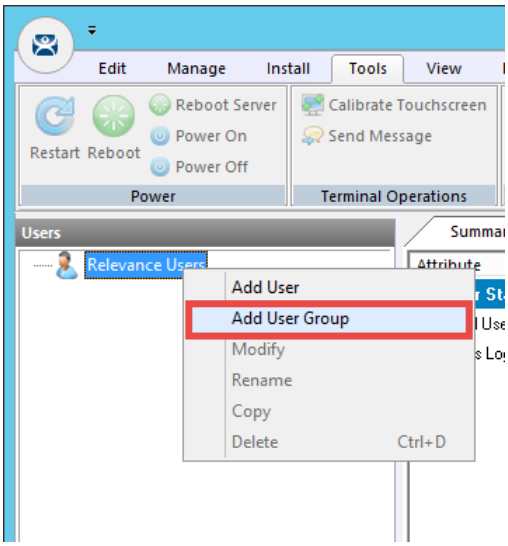


Create an Engineer User Group

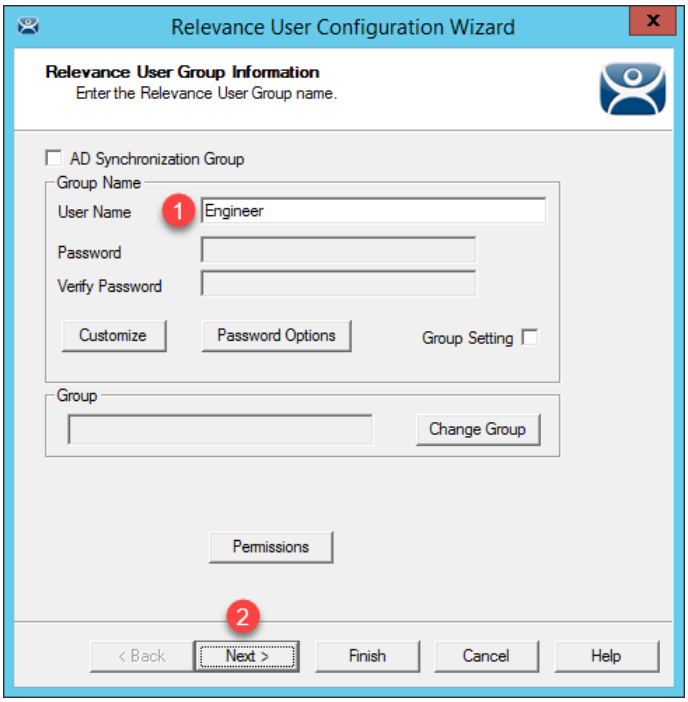
1. Click the **Users** icon  in the ThinManager tree selector.



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**.

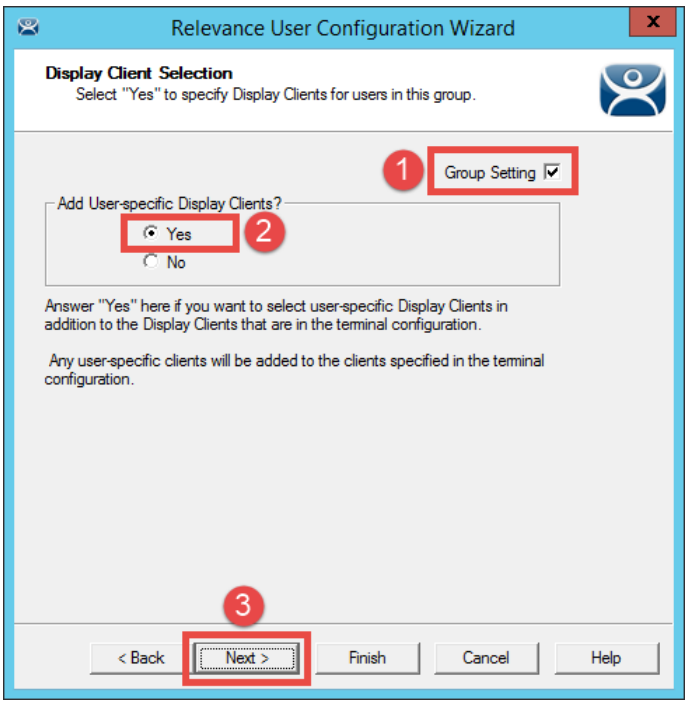


3. From the **Relevance User Group Information** page of the wizard, enter *Engineer* as the **User Name** in the **Group Name** frame. Click the **Next** button.



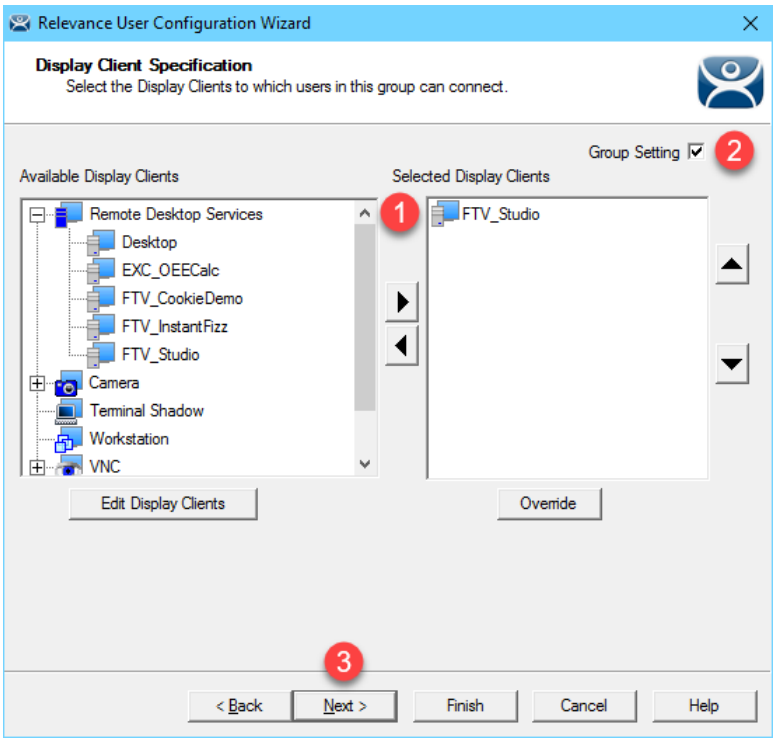
ThinManager 8 included much tighter integration with Active Directory. For example, a Relevance User Group can be automatically synchronized with an Active Directory group. In doing so, ThinManager would automatically create Relevance Users for each member of the synchronized Active Directory group. 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.

4. 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.



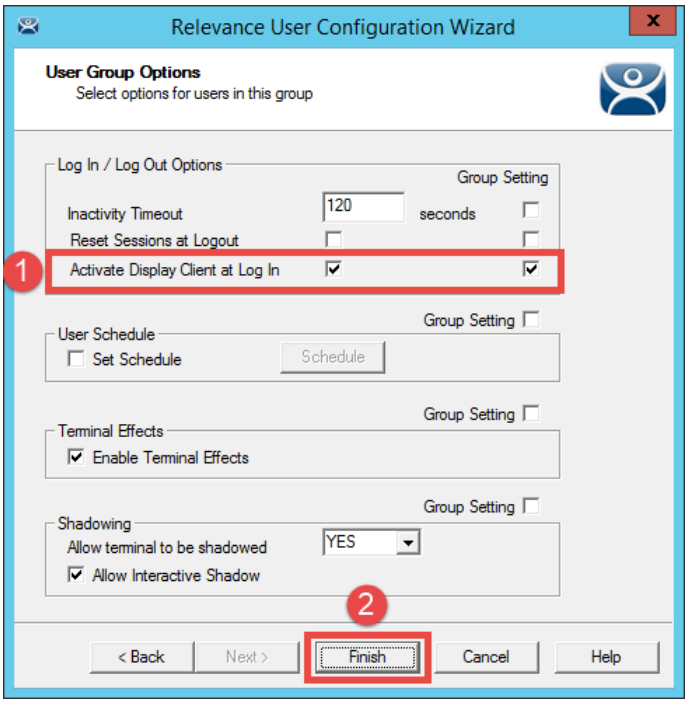
Clicking the Group Setting checkbox will pass the setting onto members of the group.

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.



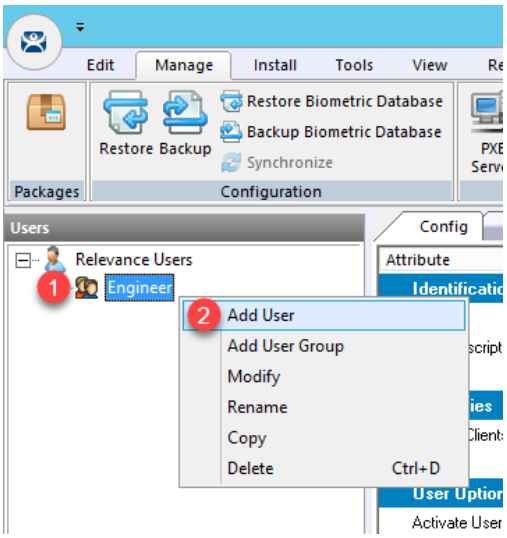
6. From the **Windows Log In Information** page of the wizard, click the **Next** button.
7. From the **Terminal Interface Options** page of the wizard, note that you can override the default **Terminal** settings by making changes here. Leave the default settings in place. Click the **Next** button.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

9. 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.

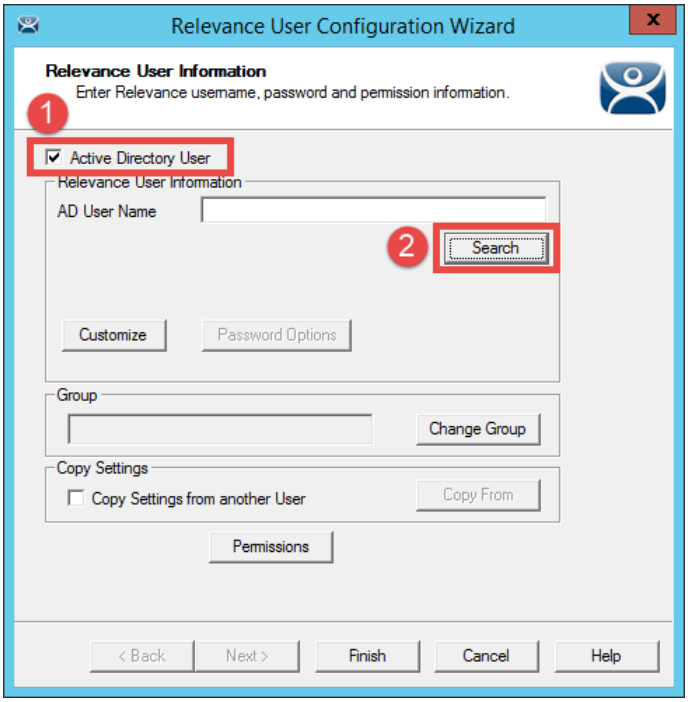


Create an Engineer User

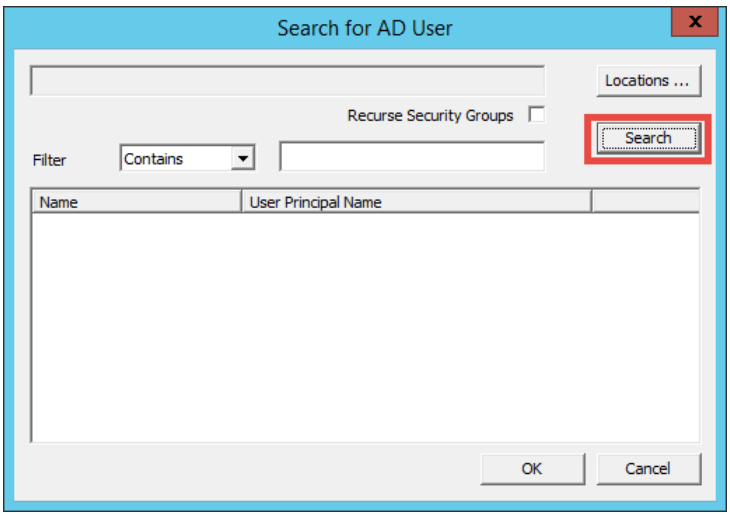
1. Expand the **Relevance Users** node.
2. Right click the newly created **Engineer User Group** and select **Add User**. This will launch the **Relevance User Configuration** wizard.



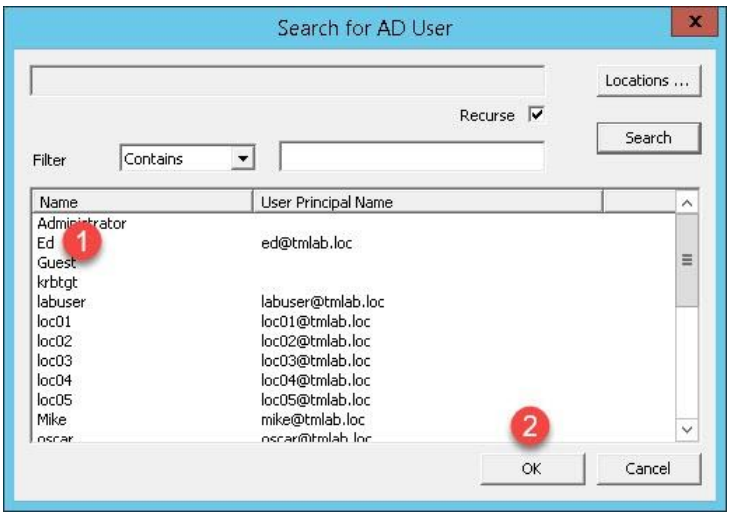
3. From the **Relevance User Information** page of the wizard, check the **Active Directory User** checkbox if it is not already checked. Click the **Search** button.



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

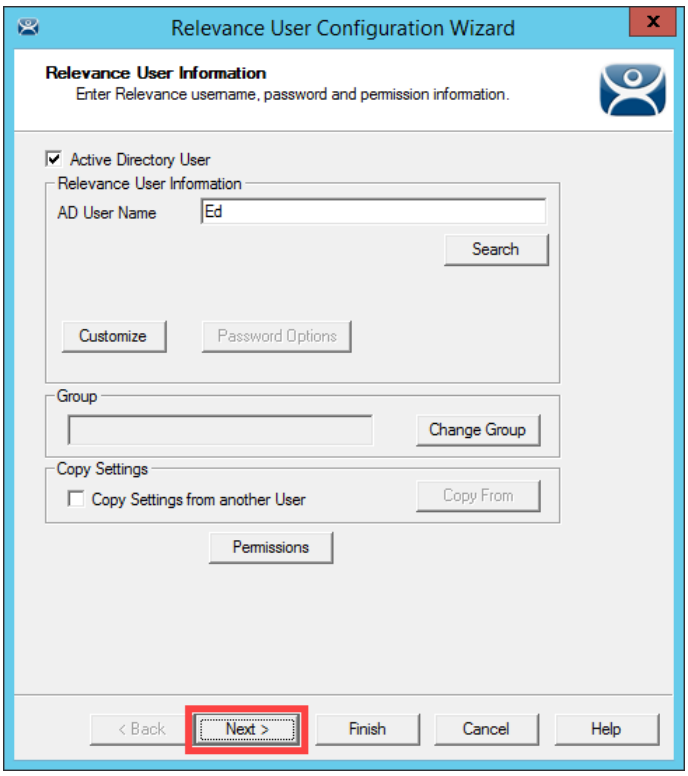


5. Select **Ed** from the user list and then click the **OK** button.



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.



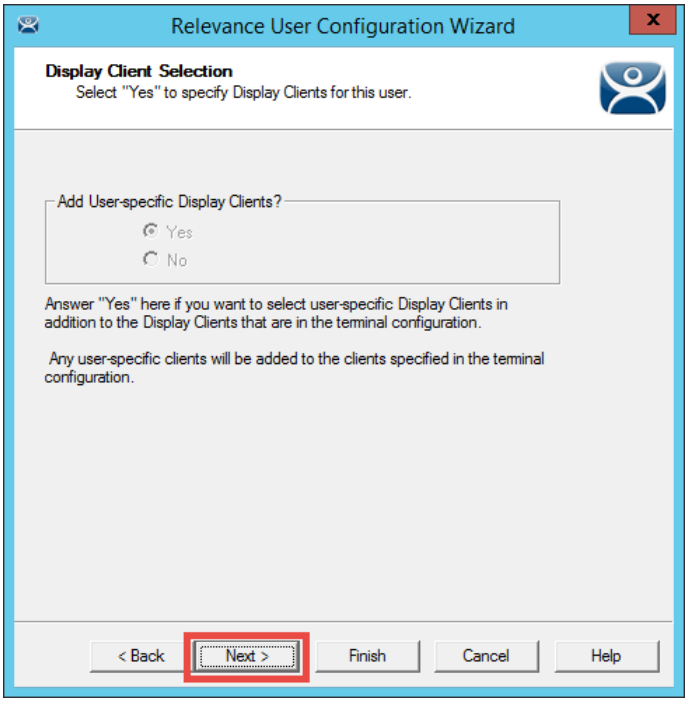
7. From the **Active Directory Password** page of the wizard click the **Next** button.

> 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.

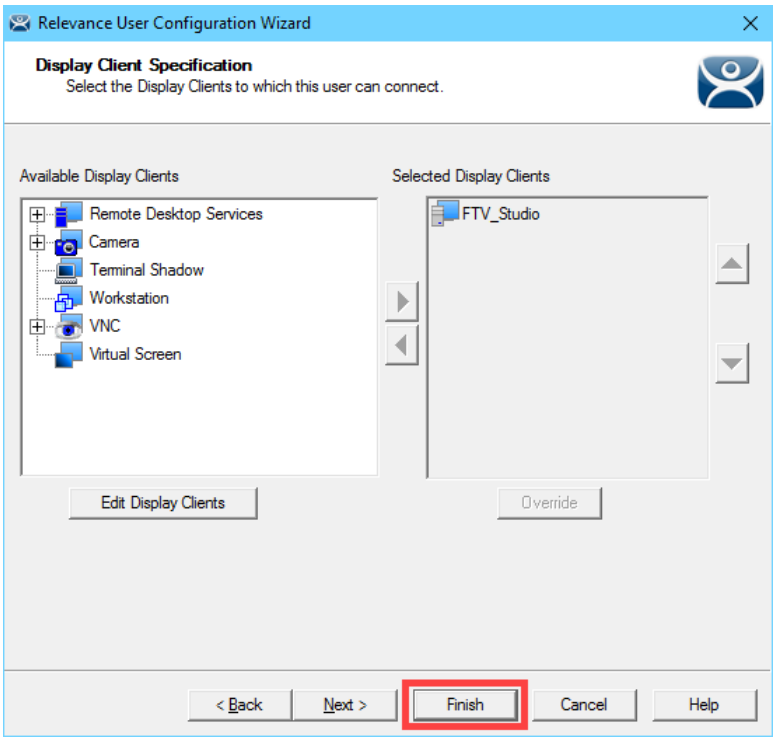
8. From the **Card / Badge Information** page of the wizard, click the **Next** button. We will incorporate an RF IDeas badge reader shortly.

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.



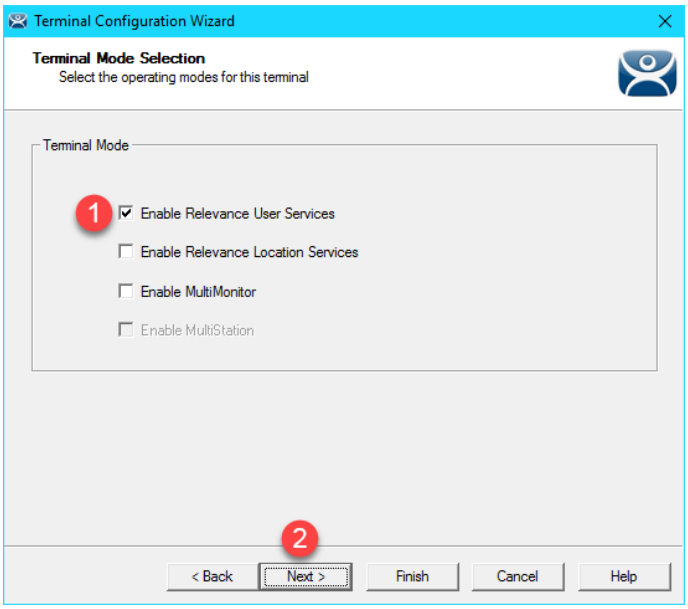
11. From the **Display Client Specification** page of the wizard, notice that the selection is disabled here as well. Click the **Finish** button.



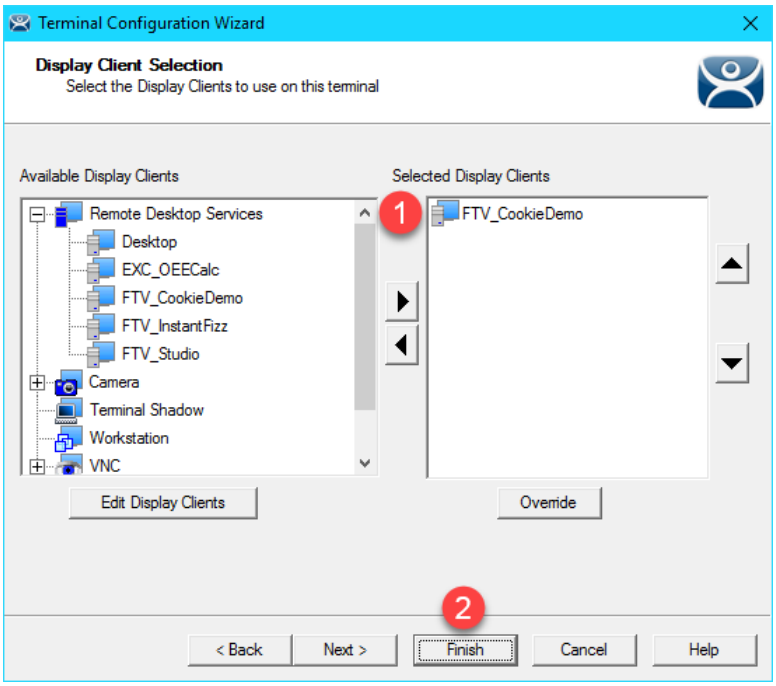
Enable User Services for Terminal

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.



7. 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**.

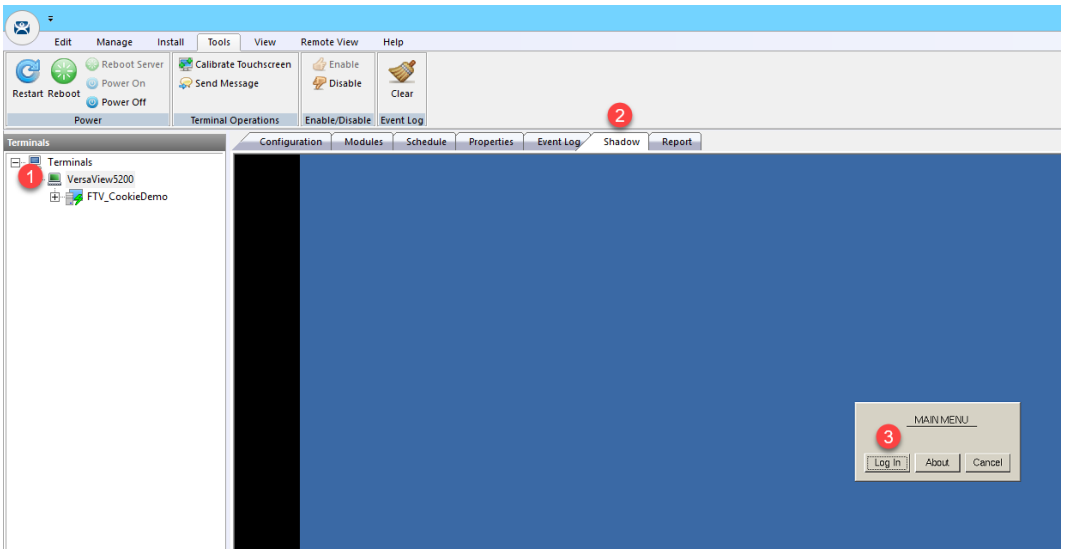


8. Right click **VersaView5200** and select **Restart Terminal** to apply the change.

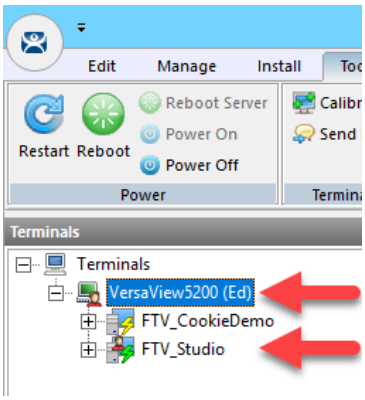
> When deploying **Relevance Users** for the first time, Enabling **Relevance User Services** at the **Terminal** is a commonly missed step. Without Enabling **Relevance User Services** at the terminals where you want to enable Relevance User logins, the Login option will not be available from the **Main 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

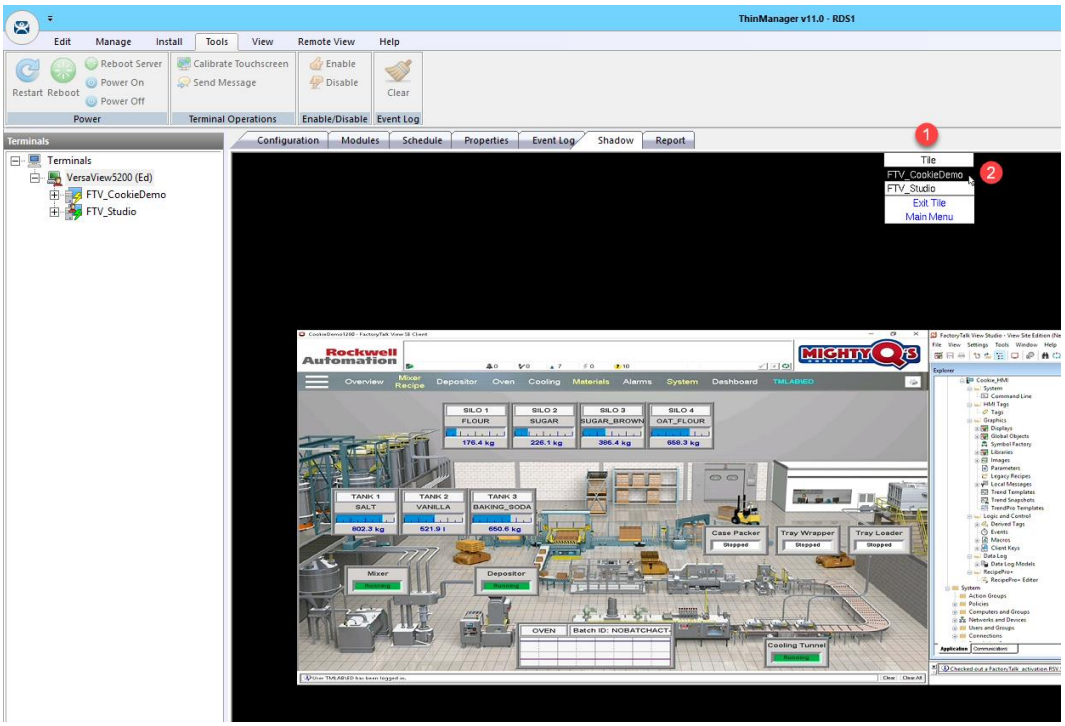
1. From the **Terminals** icon  in the ThinManager tree selector, select **VersaView5200**.
2. Click the **Shadow** tab from the Details Pane.
3. Hit CTRL-m to access the **Main Menu**.
4. From the **Main Menu**, click the **Log In** button.



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.



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



9. 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**.

10. Click the **Display Client Selector** once more and this time select **Main Menu**.

11. 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.

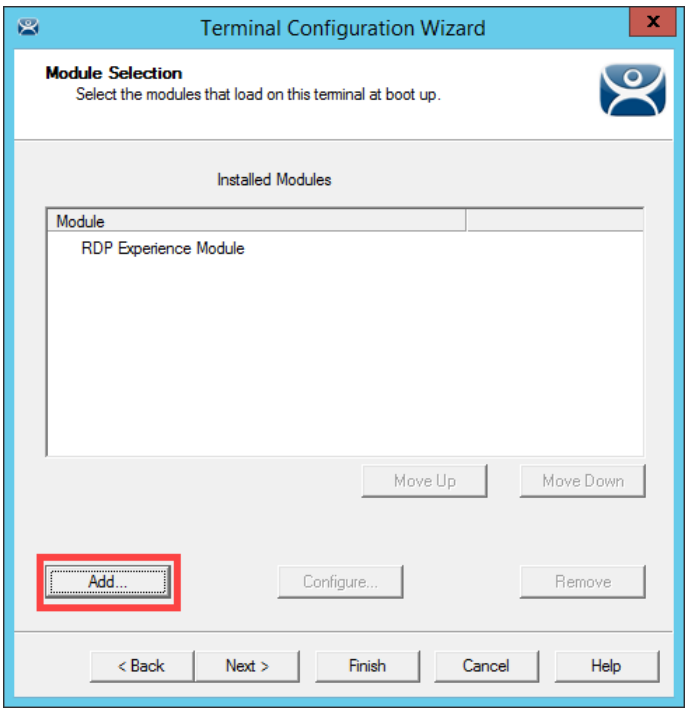
ThinManager ships with the TermMon ActiveX control that can be utilized by any ActiveX container, like FactoryTalk View SE. The ActiveX extends most of the ThinManager feature set to the ActiveX container, so you can then programmatically control many elements of ThinManager right from FactoryTalk View 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

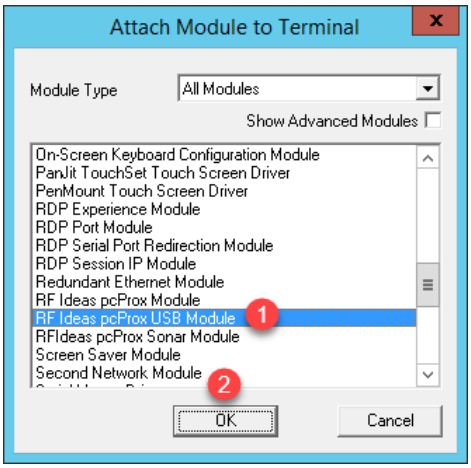
An RF IDeas Badge Reader could be connected to a physical thin client via USB. Since we are using a virtual thin client, we will be unable to test the results of this section, but will still go through the steps to add the module.

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.

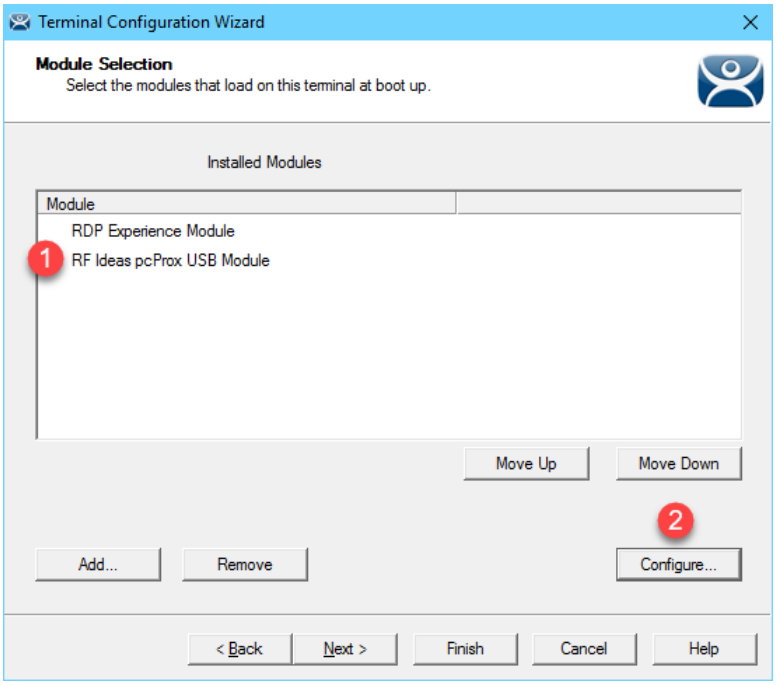


12. From **Attach Module to Terminal** dialog box, select the **RF Ideas pcProx USB Module** and click the **OK** button.

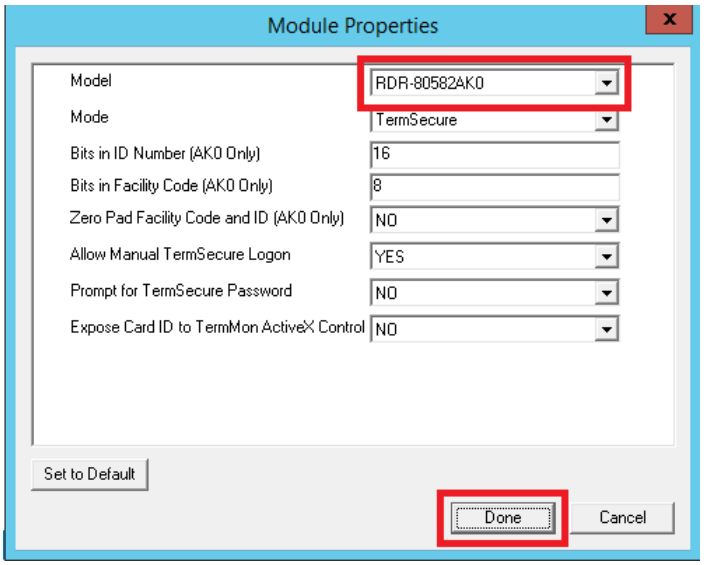


The release of ThinManager 11 includes the new USB ID Reader Module, which enables ThinManager to support generic Badge Reader modules that act as a keyboard emulator.

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



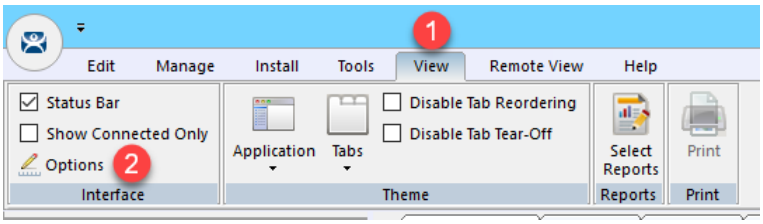
14. From the **Module Properties** dialog box, select **RDR-80582AK0** from the **Model** drop down list and click the **Done** button.



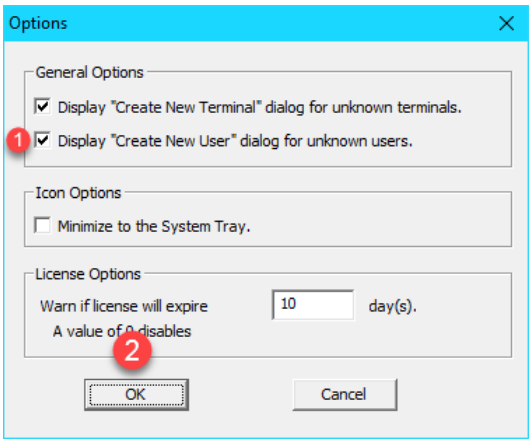
15. Back at the **Module Selection** page of the wizard, click the **Finish** button.

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.

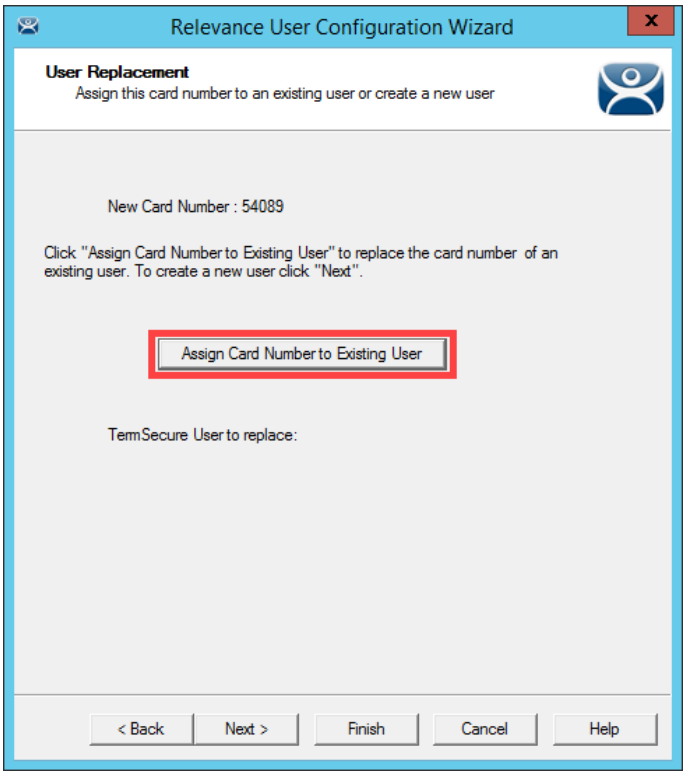


18. From the **Options** window, check the **Display "Create New User" dialog for unknown users** and click the **OK** button.



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

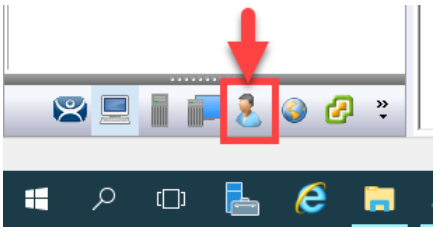
20. If this was a new badge to ThinManager, you would be presented with the option to assign it to a user. **NOTE:** Since you do not have a badge reader in the Cloud lab, you will not see this window appear.



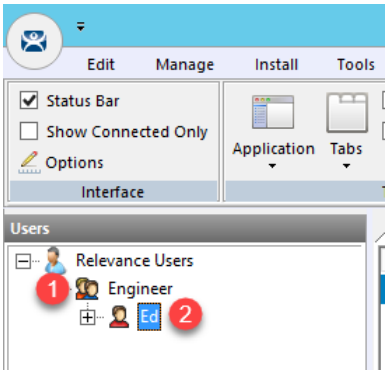
Configure ThinManager to Cache Password

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.

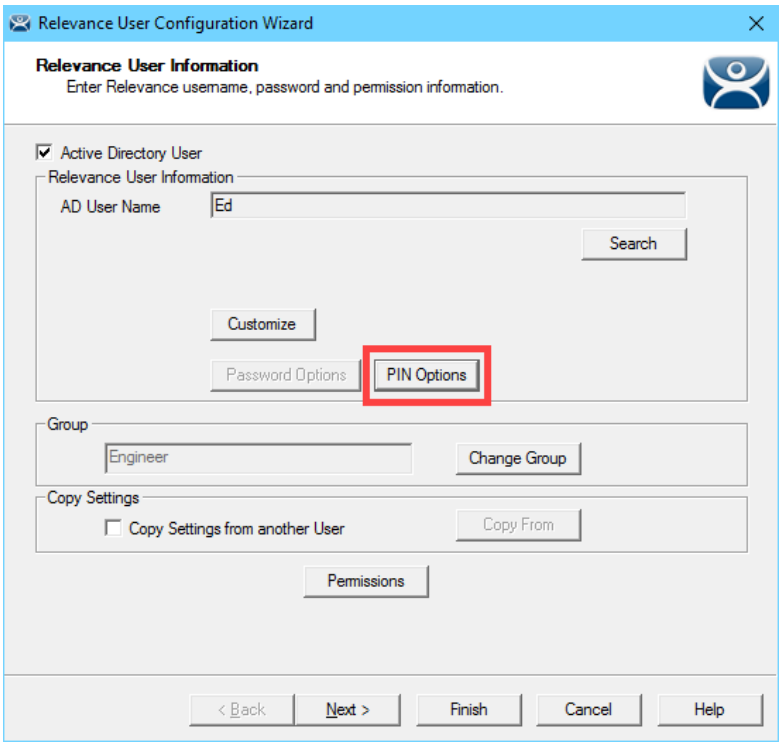
1. Click the **Users** icon  in the ThinManager tree selector.



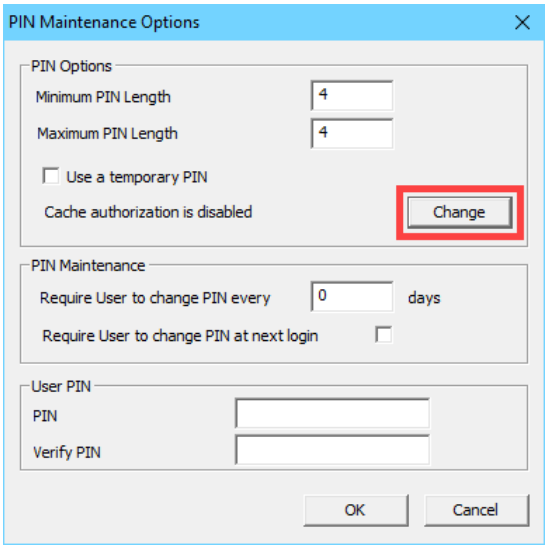
2. Expand the **Engineer** group and double click the icon for **Ed**.



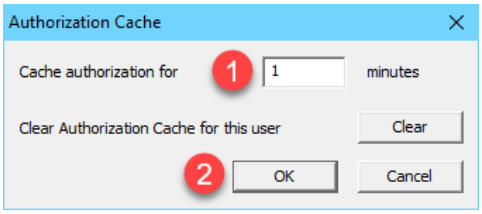
3. Click the **PIN Options** button on the **Relevance User Information** page of the wizard.



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



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



6. 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.

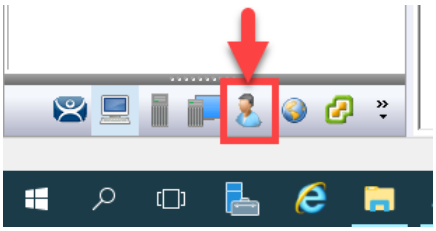
7. Return to the shadow of the **VersaView5200** terminal, hit CTRL-m on the keyboard to open the **Main Menu**.
8. Click the **Log In** button.
9. Enter *ed* as the **User Name** with a **Password** of *rw* as before to login as Ed.
10. Hit CTRL-m on the keyboard to open the **Main Menu** again, and click the **Log Off** button.
11. 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.
12. 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

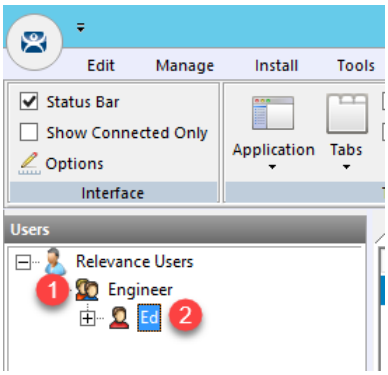
As part of ThinManager 10, a permanent or temporary PIN can be assigned to Relevance Users as an additional option for authenticating.

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.

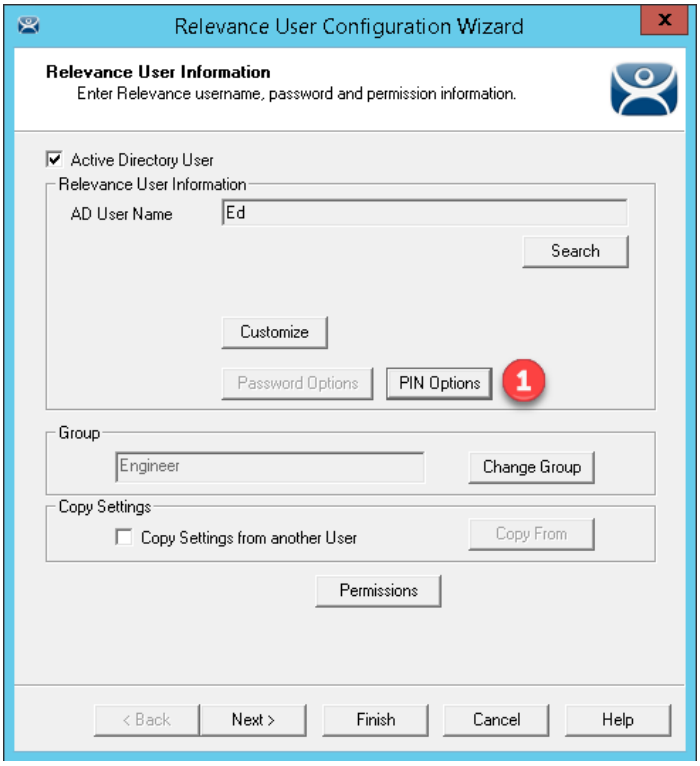
1. Click the **Users** icon  in the ThinManager tree selector.



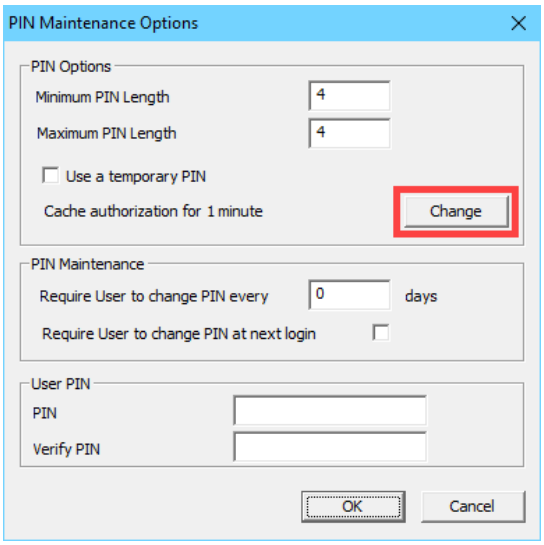
2. Expand the **Engineer** group and double click the icon for **Ed**.



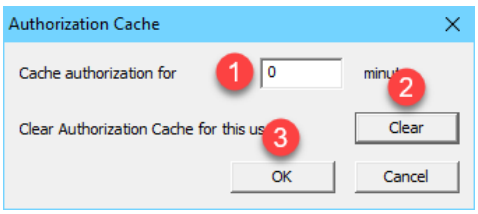
3. Click the **PIN Options** button on the **Relevance User Information** page of the wizard.



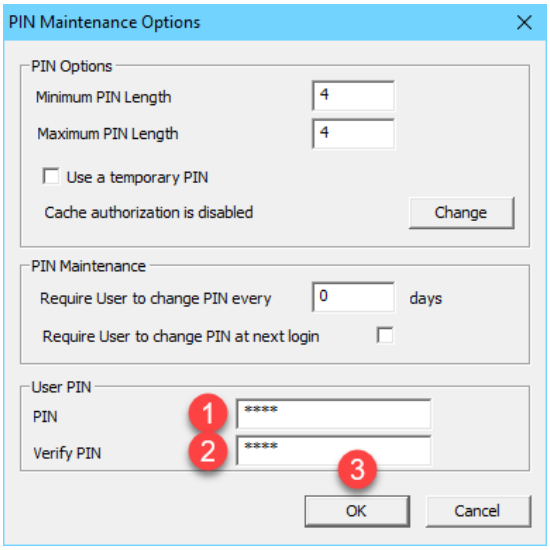
4. Click the **Change** button within the **PIN Options** frame.



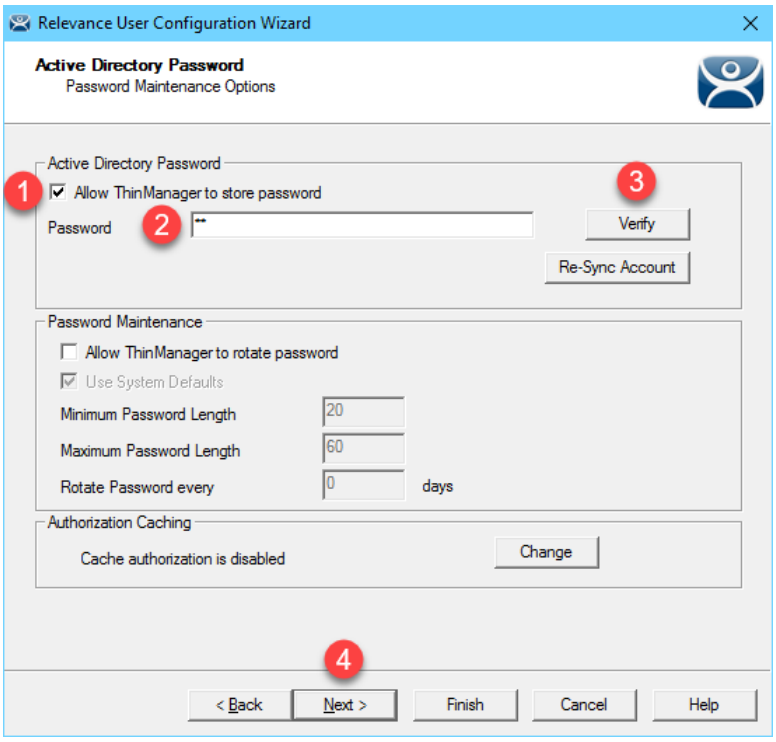
5. Enter a *0* for the **Cache authorization for** textbox and click the **Clear** button next to the **Clear Authorization Cache for this user** to reset the cache. Confirm the **Clear User Authorization Cache** prompt and click **OK**.



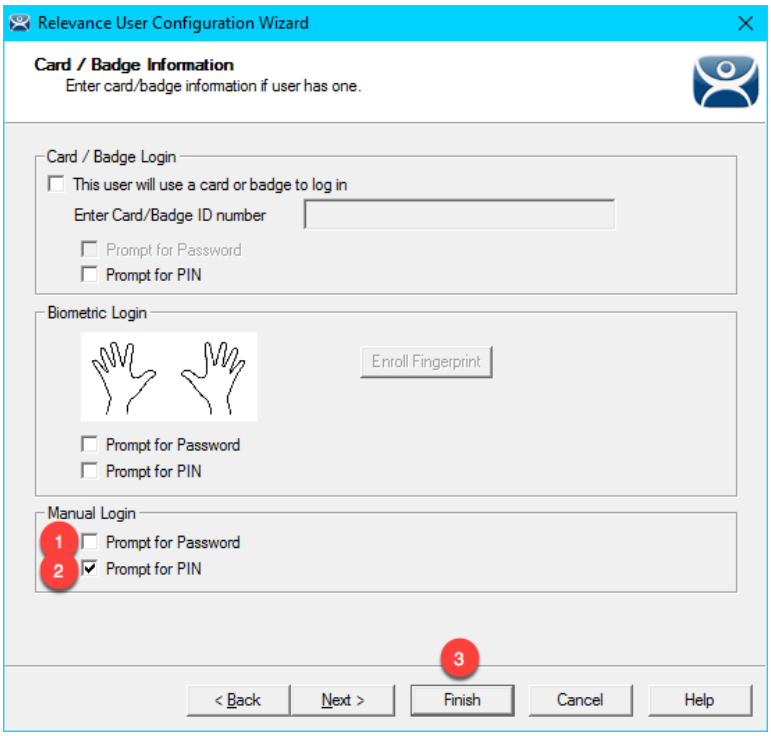
6. Enter *1234* in the **PIN** field within the **User PIN** frame and re-enter in the **Verify PIN** field. Click the **OK** button, followed by the **Next** button.



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**.



8. 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.



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

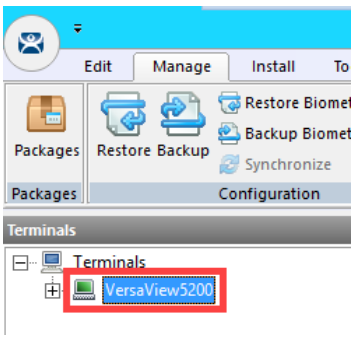
> In the example above, we set a permanent PIN for Ed. We could have just as easily required a temporary PIN that Ed would create for himself at the terminal. We could also require him to change this PIN on a scheduled interval.

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.

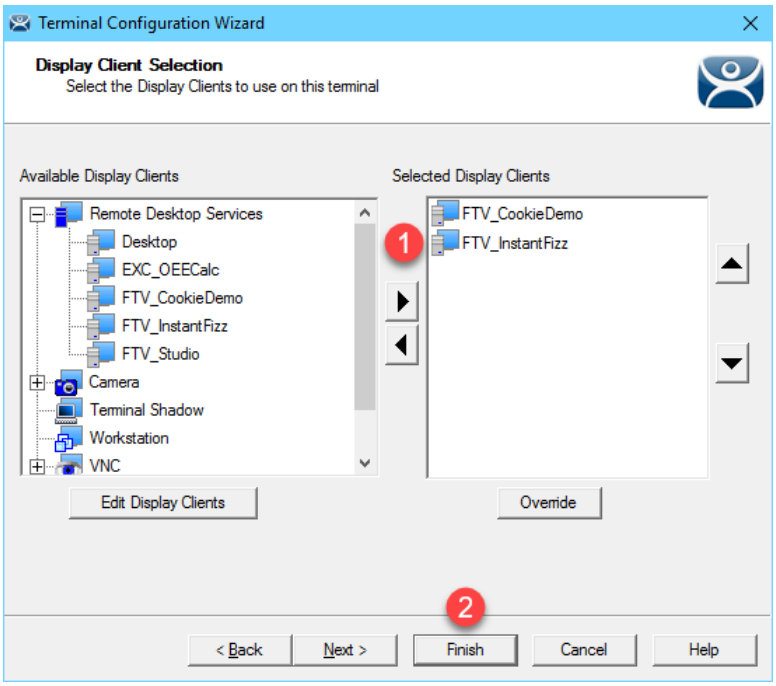
In the next steps you will configure ThinManager to deliver (2) separate FactoryTalk View SE Display Clients to the virtual thin client in tile mode. The **tmlab\thin01** user will automatically establish the two sessions, as this is the domain user that is assigned to the **VersaView5200** terminal 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.

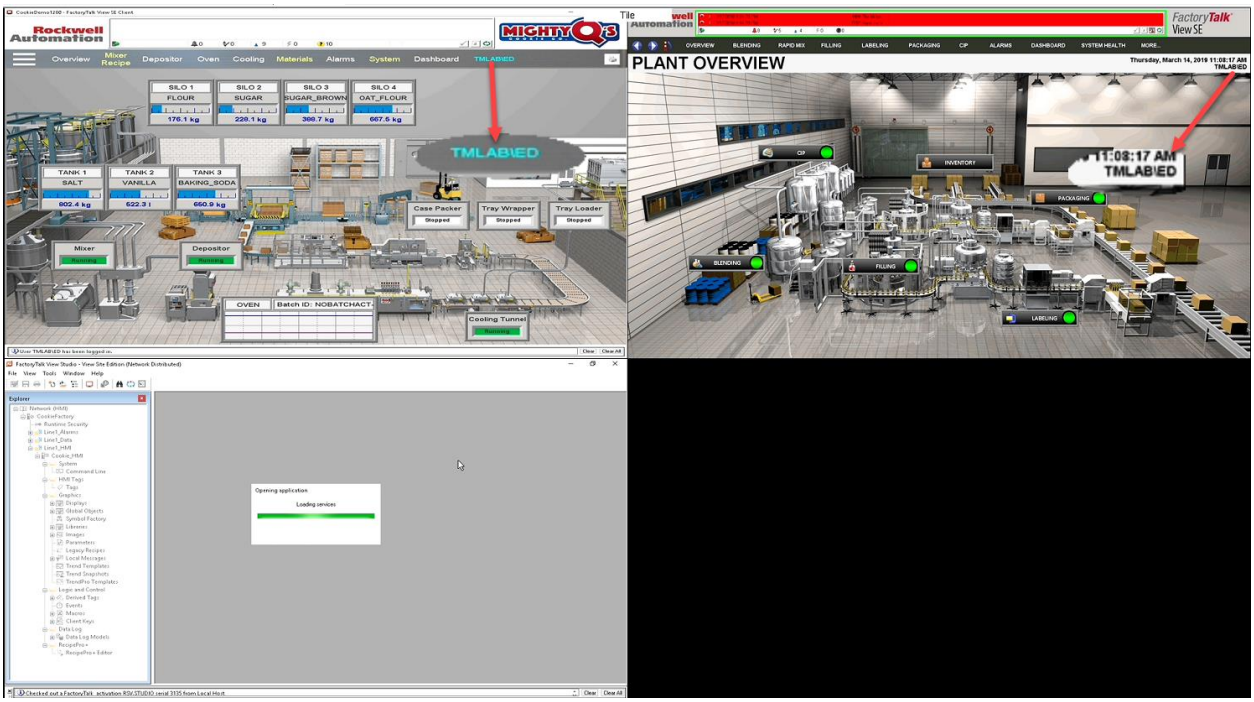
6. From the **Display Client Selection** page of the wizard, select **FTV_InstantFizz** from the **Available Display Clients** list and click the **Right Arrow** button to move it to the **Selected Display Clients** list, click the **Finish** button.



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

8. Shadow the **VersaView5200** terminal and confirm that user **tmlab\thin01** 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 **tml1ab\ed** user automatically logged into both **FactoryTalk View SE** display clients, and that the **FTV_Studio** client is delivered in tile mode.

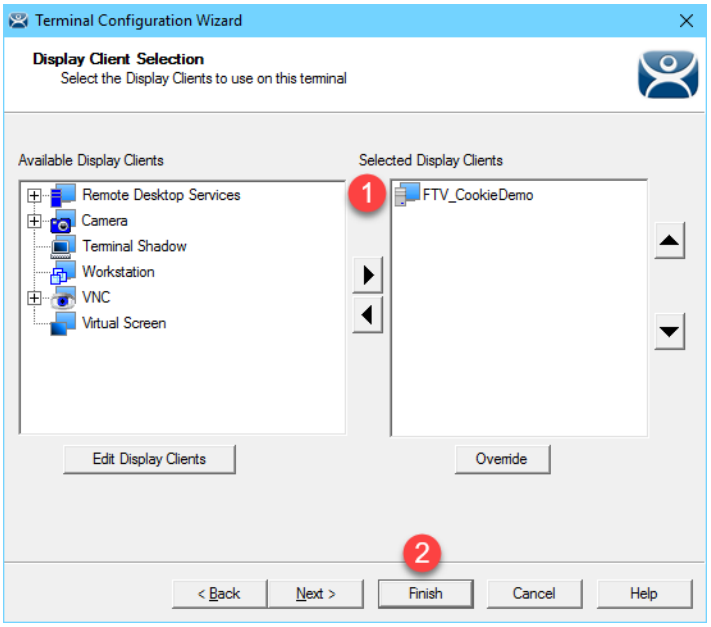


12. Hit CTRL-m on the keyboard again to open the **Main Menu**.
13. Click the **Log Off** button.
14. Verify that the **tmlab\thin01** user is logged back into the tiled FactoryTalk View SE display clients.

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_InstantFizz 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.

Checkpoint Question: https://thinmanager.com/cloudlabs/section09/

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

Section 10: 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 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

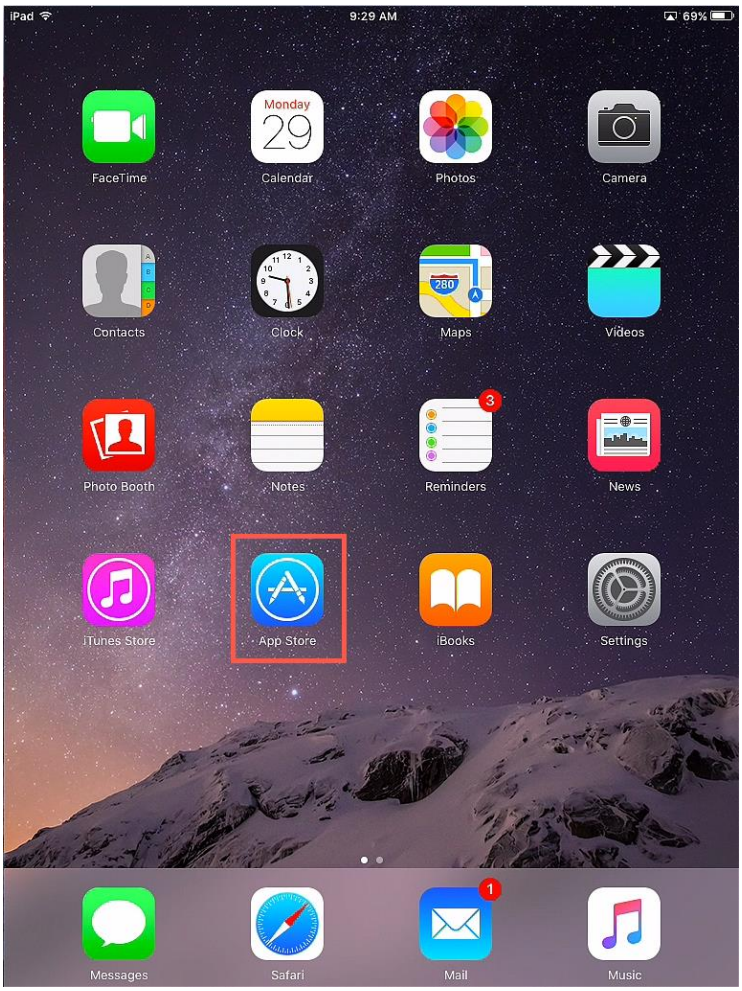
QR Codes are essentially more robust alphanumeric versions of barcodes. QR Codes can be generated and printed from several websites. Bluetooth Beacons are essentially proximity sensors for mobile devices. They offer a tunable signal strength, and hence range, from 0 to approximately 50 meters. ThinManager 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.

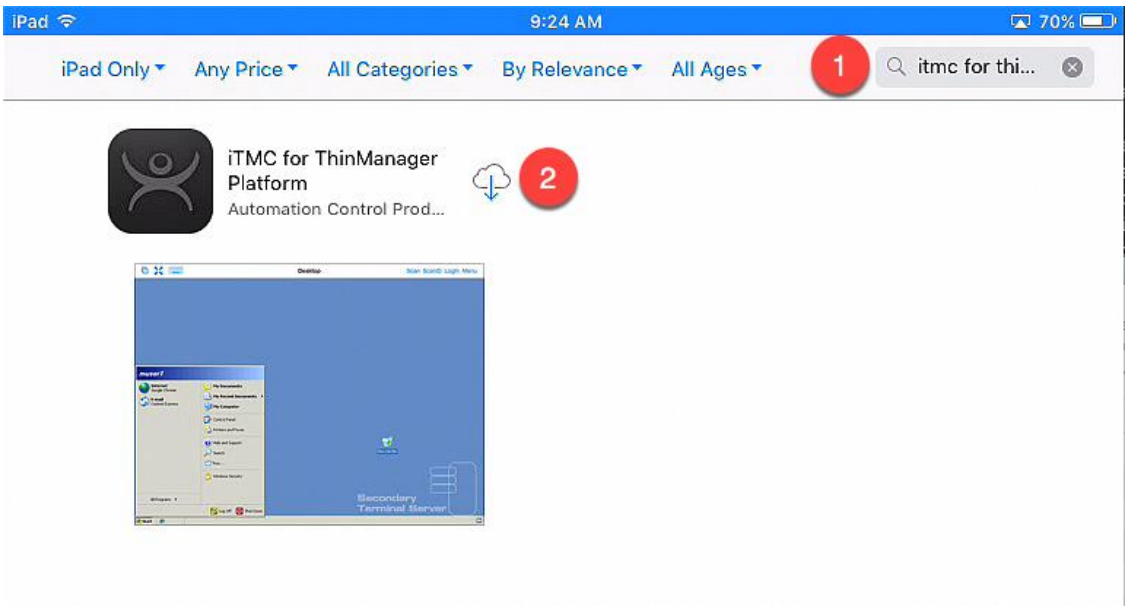
Install iTMC on Your Mobile Device (iOS Users)

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 to **Install aTMC on Your Mobile Device (Android Users)** below.

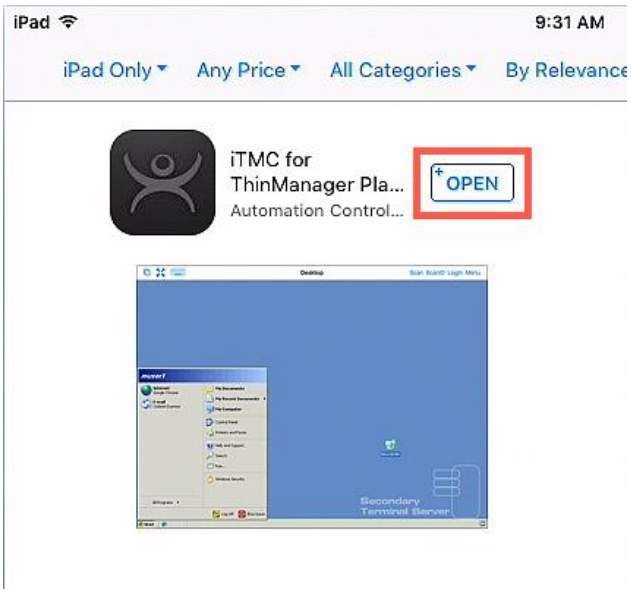
1. Launch the App Store from your iOS device.



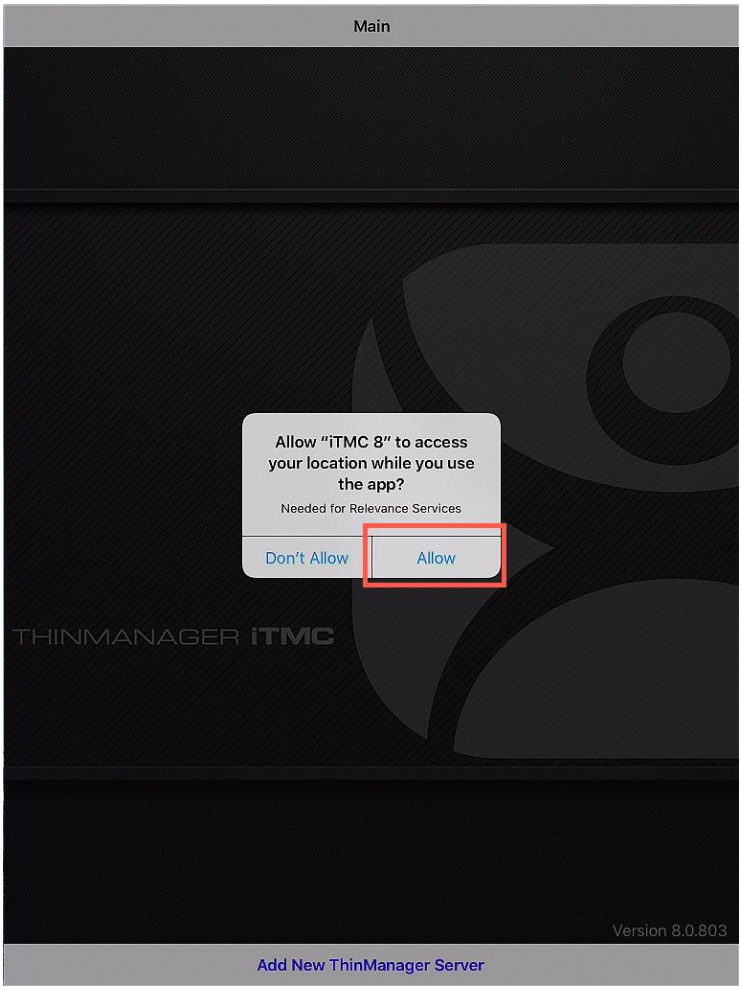
2. In the **Search** field, enter *iTMC for ThinManager Platform*. Touch the **Download** icon.



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

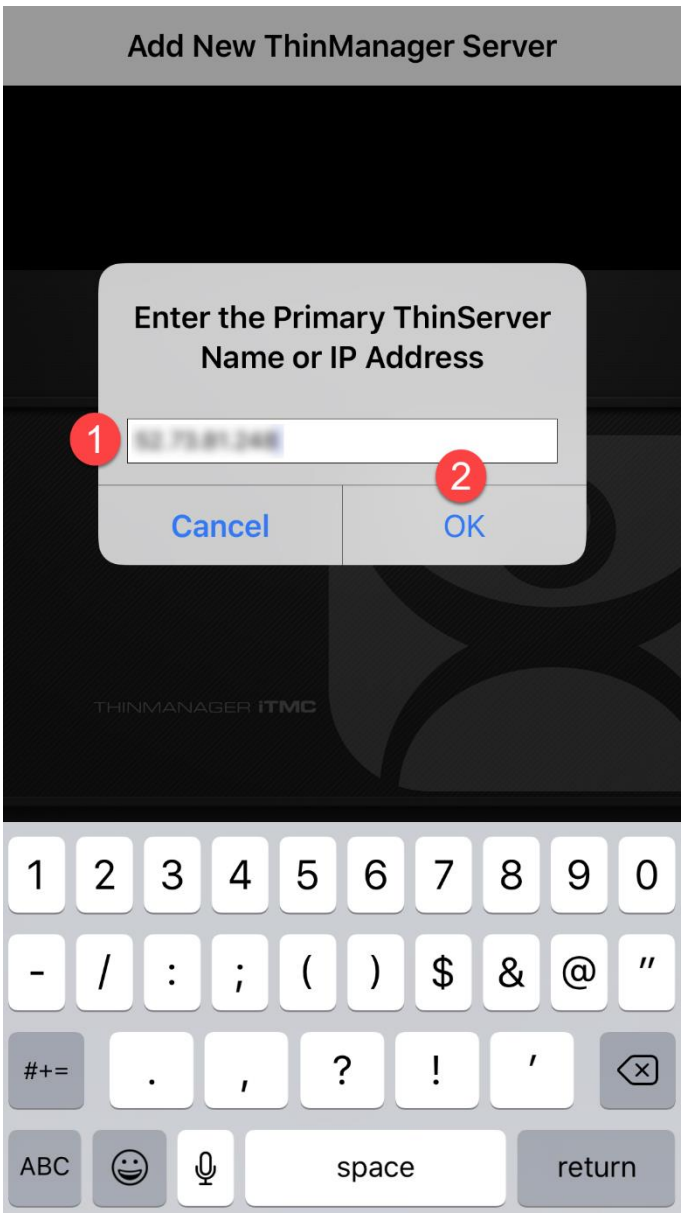


4. Launch **iTMC**. If it requests to access to your location while using the app, touch the **Allow** button.

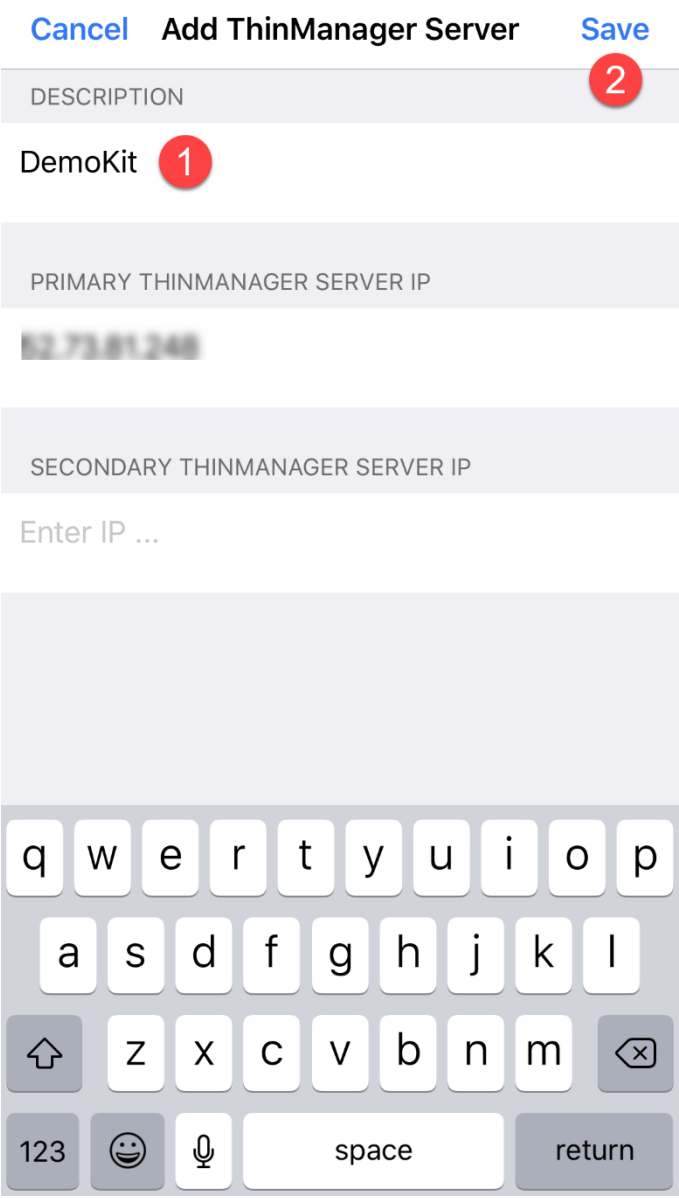


iOS treats Bluetooth beacons as Location Services devices, so if you intend to use beacons with an iOS device, you will need to enable Location Services for iTMC.

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



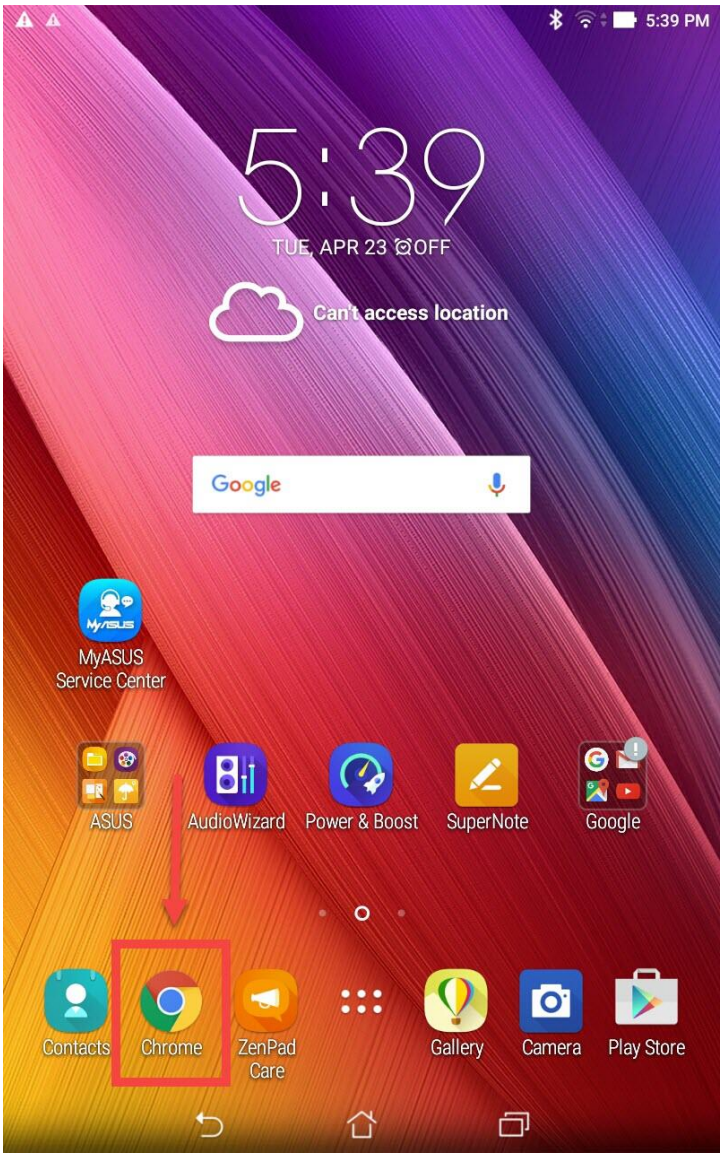
6. Enter a **Description** for this connection and touch the **Save** button.



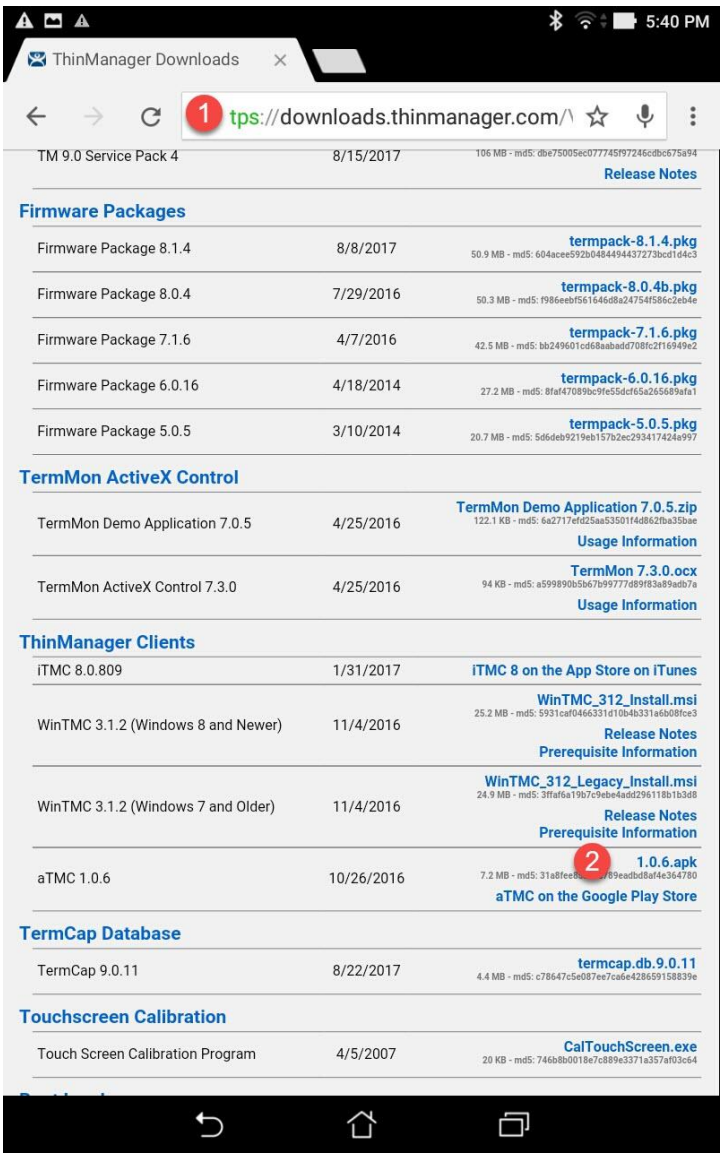
Install aTMC on Your Mobile Device (Android Users)

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 you mobile device has an Internet connection and open Chrome.

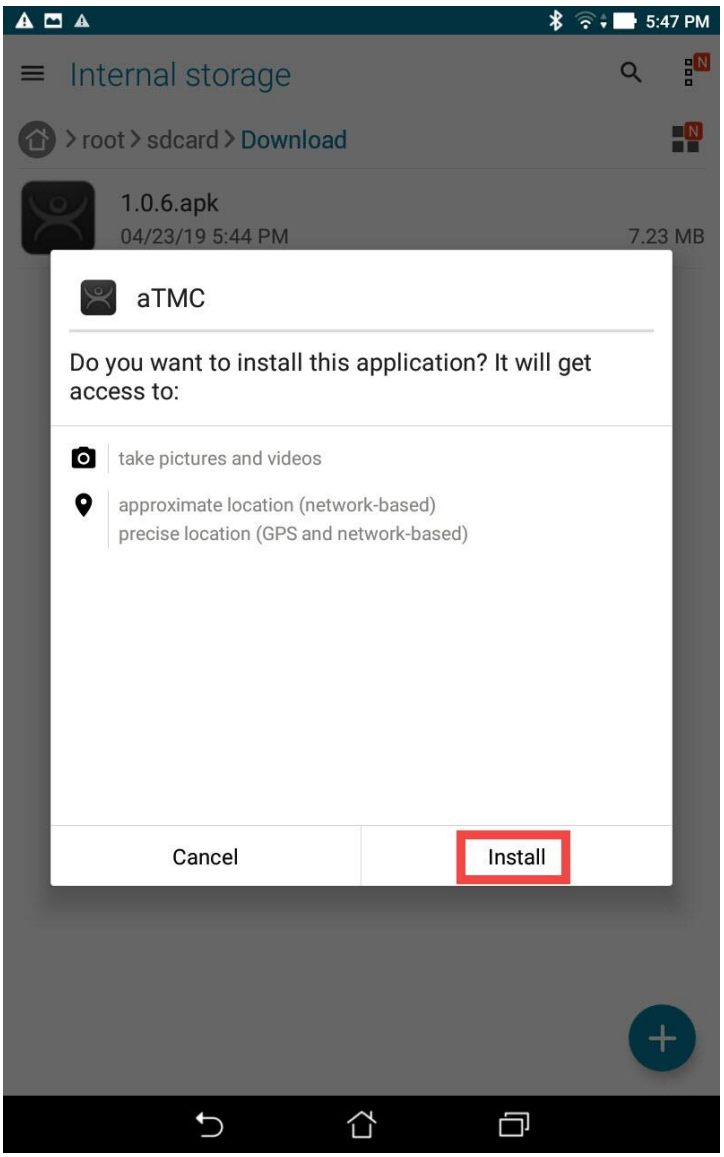


2. From **Chrome**, enter the following **URL**: *downloads.thinmanager.com*. Touch on the **aTMC** download link (1.0.6.apk in the screen shot below, but you may see a newer version which is ok).

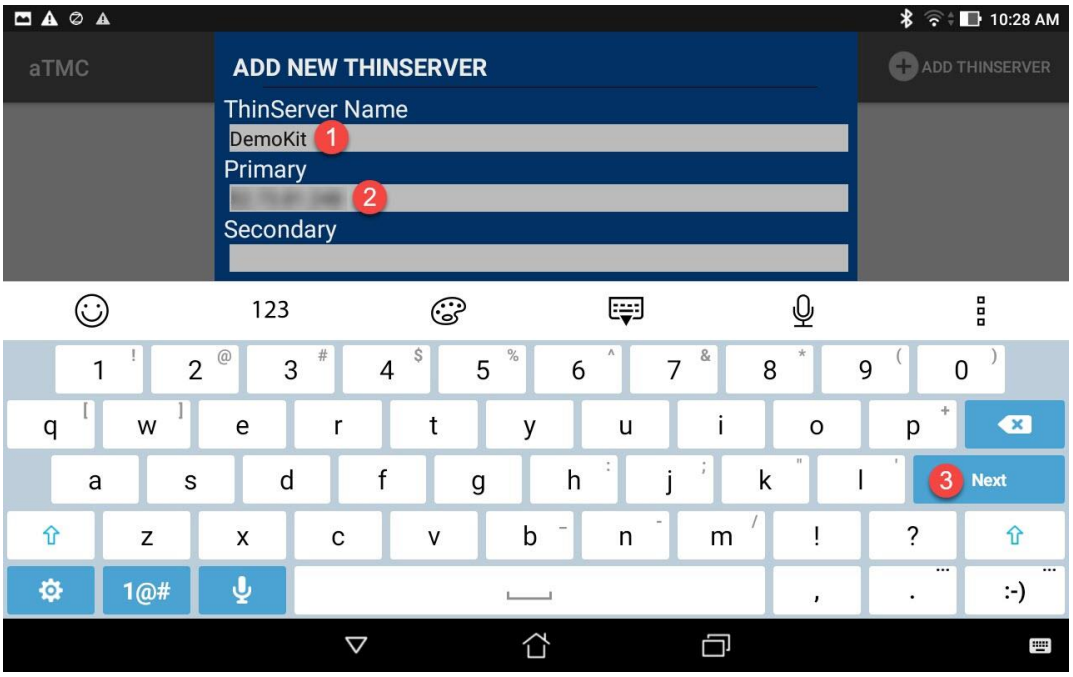


aTMC can also be downloaded from the Google Play Store.

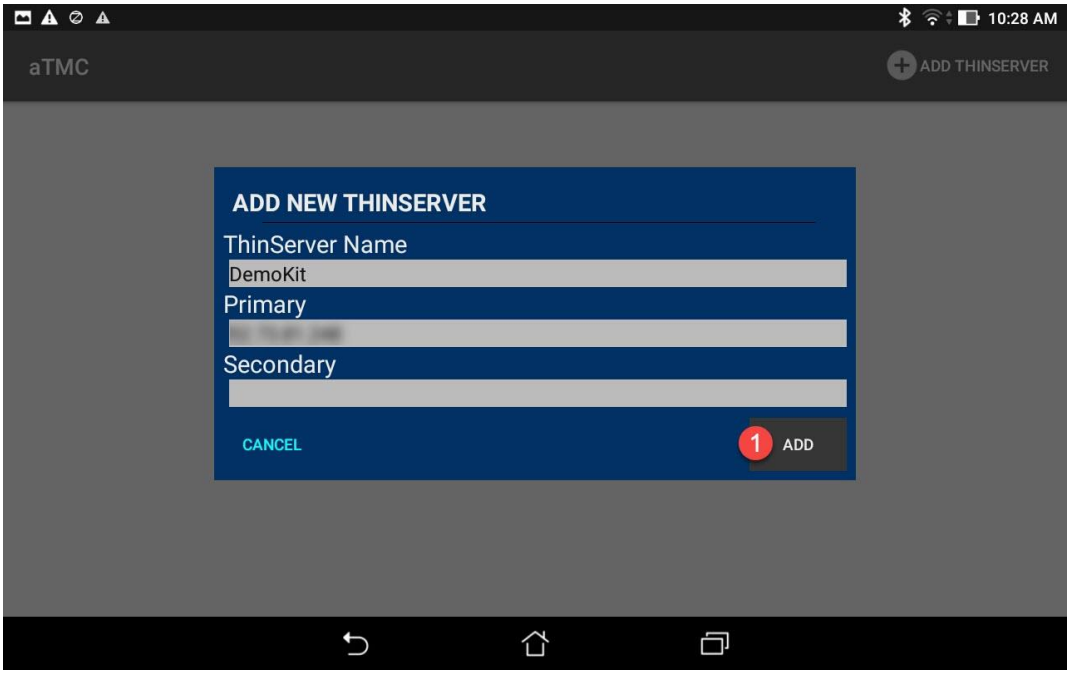
3. Once **aTMC** is downloaded, install it.



4. 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.

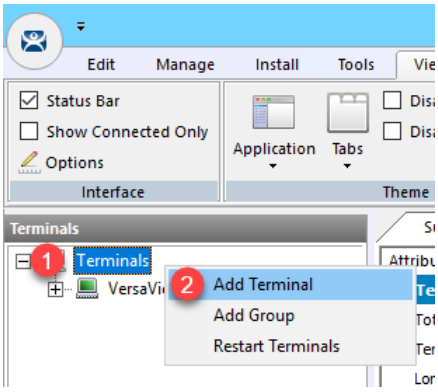


5. Click the **Add** button.

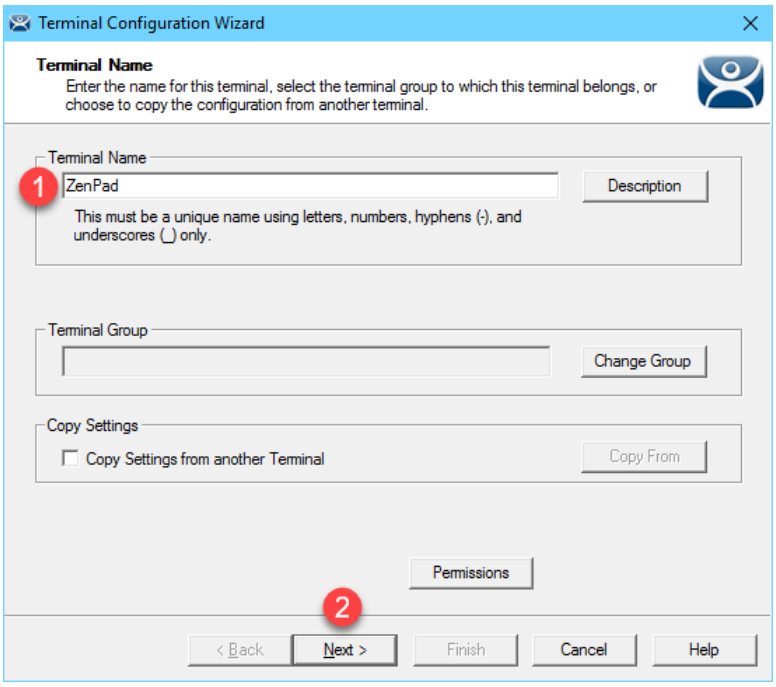


Create Terminal Profile for Mobile Device

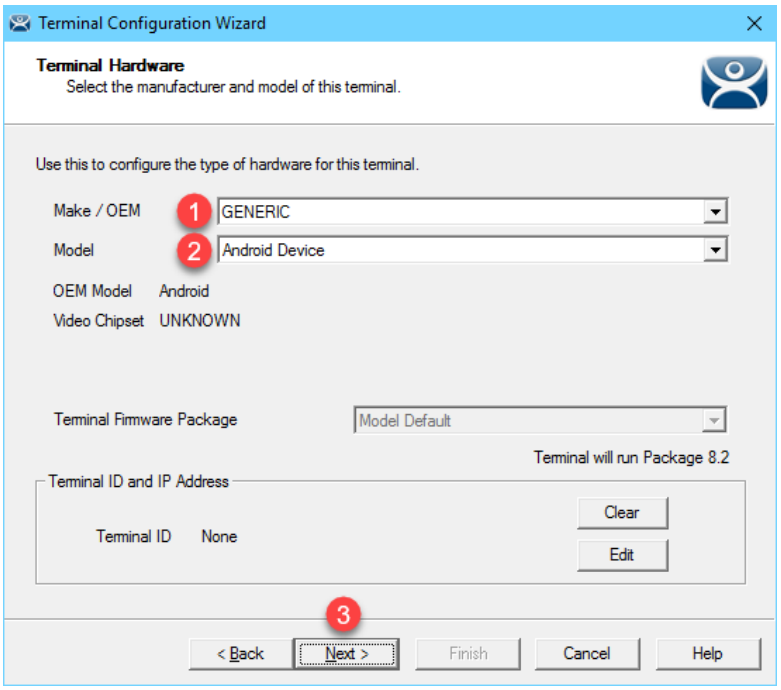
1. Click the **Terminals** icon  from the ThinManager tree selector.
2. From the **Terminals** tree, right click the **Terminals** node and select **Add Terminal**. This will launch the **Terminal Configuration Wizard**.



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

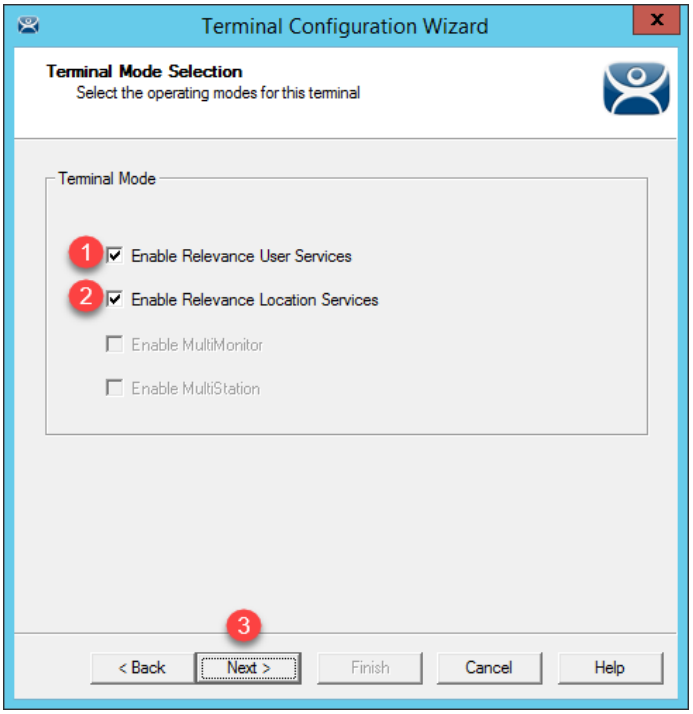


4. Select **Generic** from the **Make/OEM** drop down list and **Android Device** from the **Model** drop down list. Click the **Next** button.

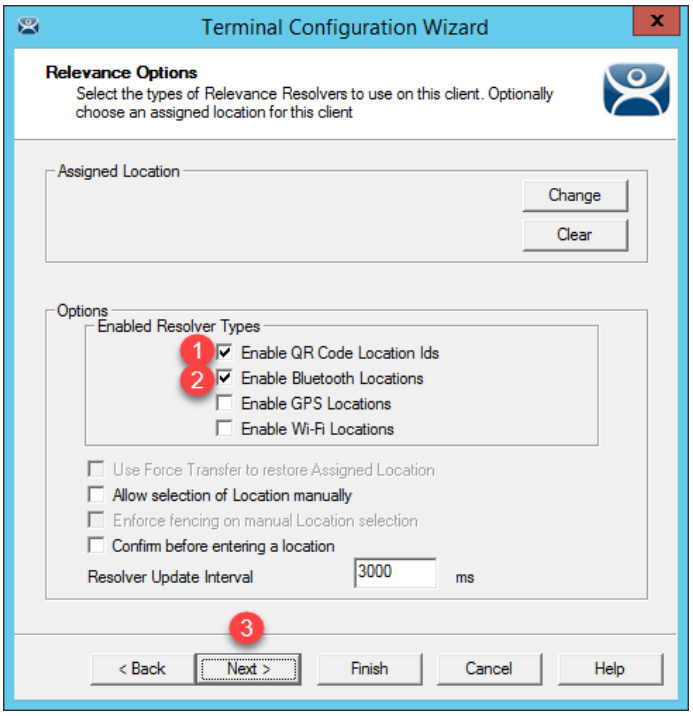


If you are using an iOS device in the lab, you would select **Apple** as the **Make / OEM** and **iOS Device** as the **Model**.

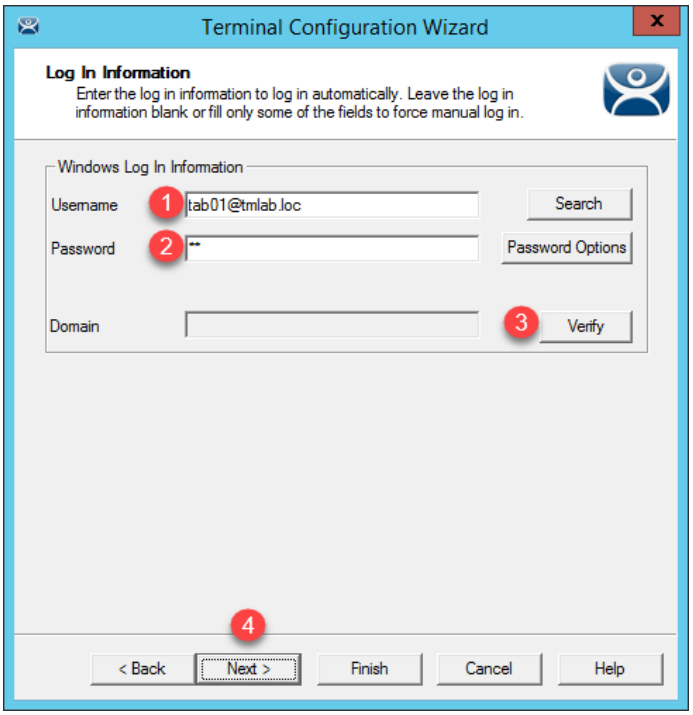
5. Click the **Next** button on the **Terminal Options** page of the wizard.
6. Check the **Use Display Clients**, **Enable Relevance User Services**, and **Enable Relevance Location Services** checkboxes on the **Terminal Mode Selection** page of the wizard. Click the **Next** button.



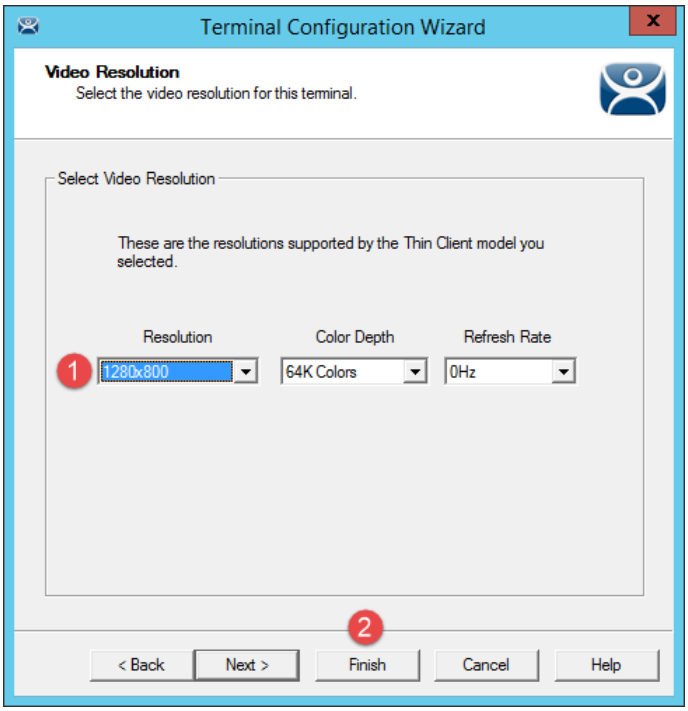
7. Click the **Next** button from the **Display Client Selection** page of the wizard.
8. Click the **Next** button on the **Terminal Interface Options** page of the wizard.
9. Check the **Enable QR Code Location Ids** and **Enable Bluetooth Locations** checkboxes from the **Relevance Options** page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



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.



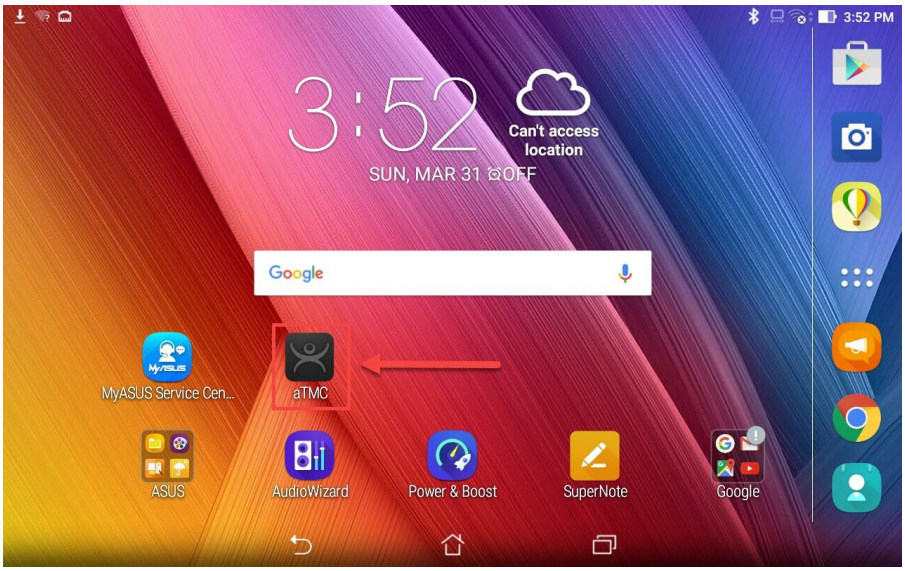
11. From the **Video Resolution** screen of the wizard, select **1280x800** as the **Resolution**, and keep other default settings. Click the **Finish** button.



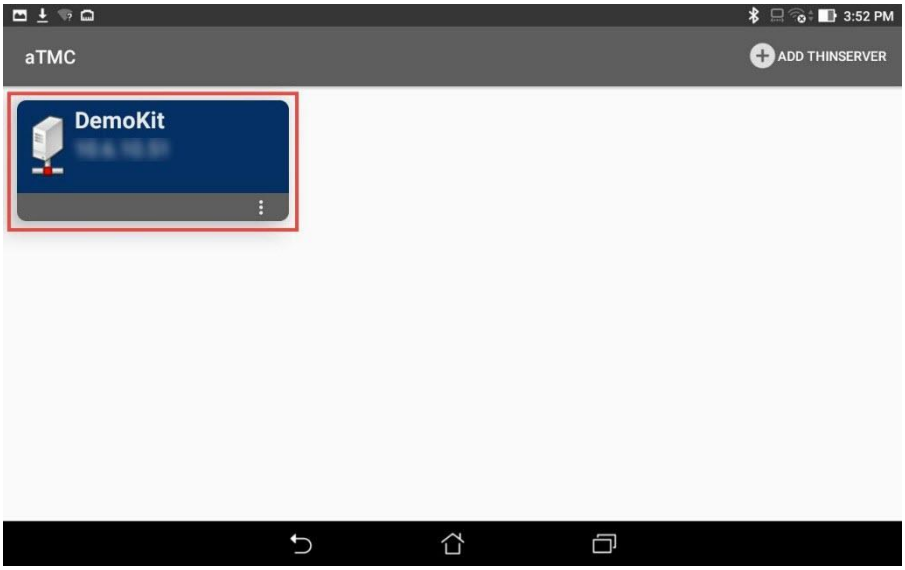
Assign Terminal Profile to Mobile Device

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.

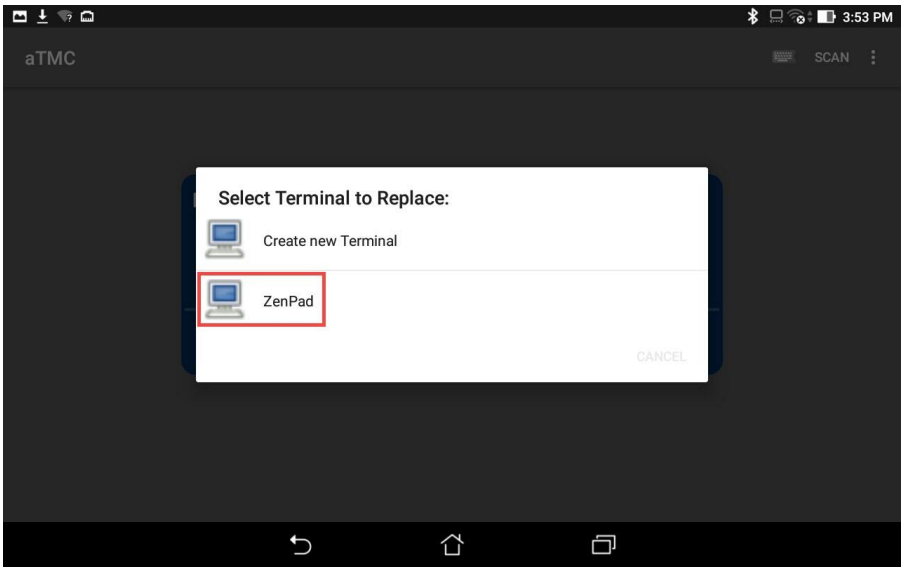
1. Launch **aTMC** from your mobile device.



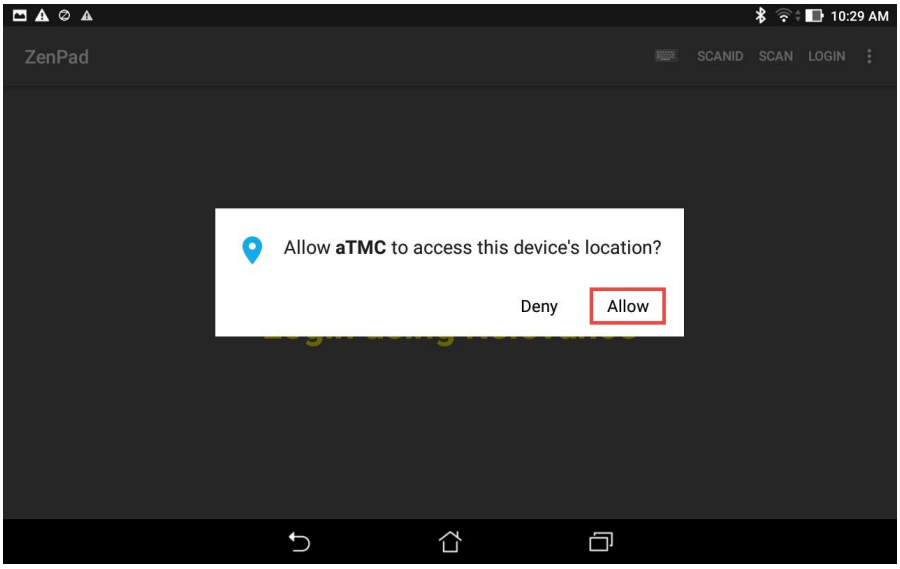
2. Touch the **DemoKit ThinServer** to connect to it.



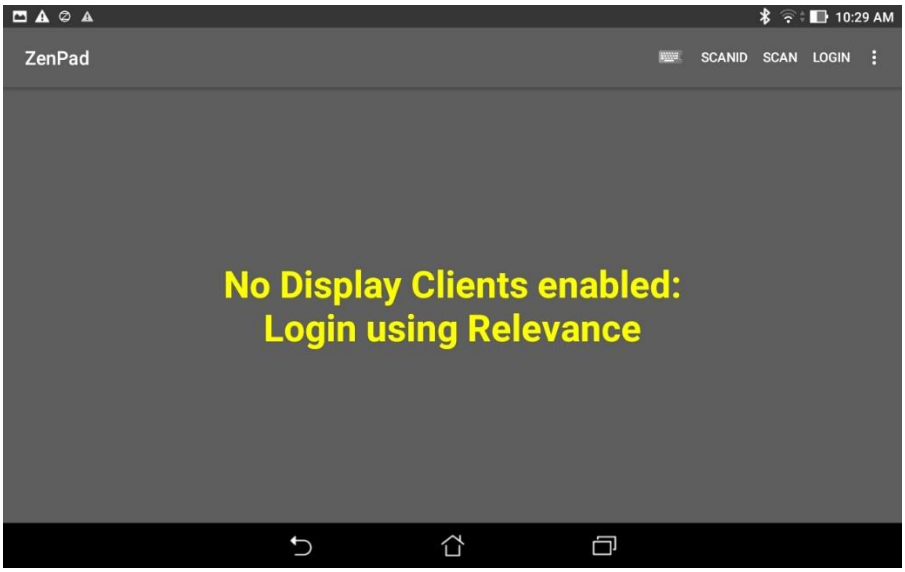
3. Since we have not assigned a **Terminal Profile** to the **ZenPad** yet, **aTMC** will prompt us to assign one of the available profiles to it. Touch the **ZenPad** profile that we created in the previous steps.



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.



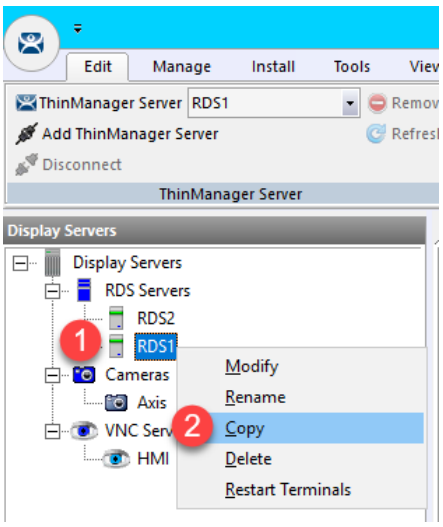
Create Public Display Server

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.

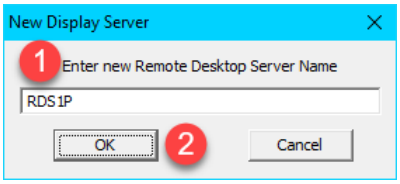
1. Click the **Display Servers** icon in the ThinManager tree selector.

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

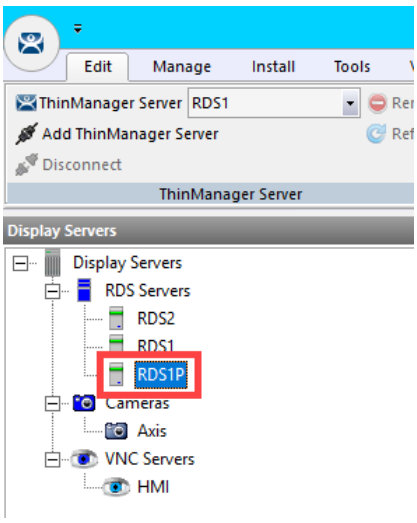
2. From the **Display Servers** tree, expand the **RDS Servers** branch, right click **RDS1** and click **Copy**.



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

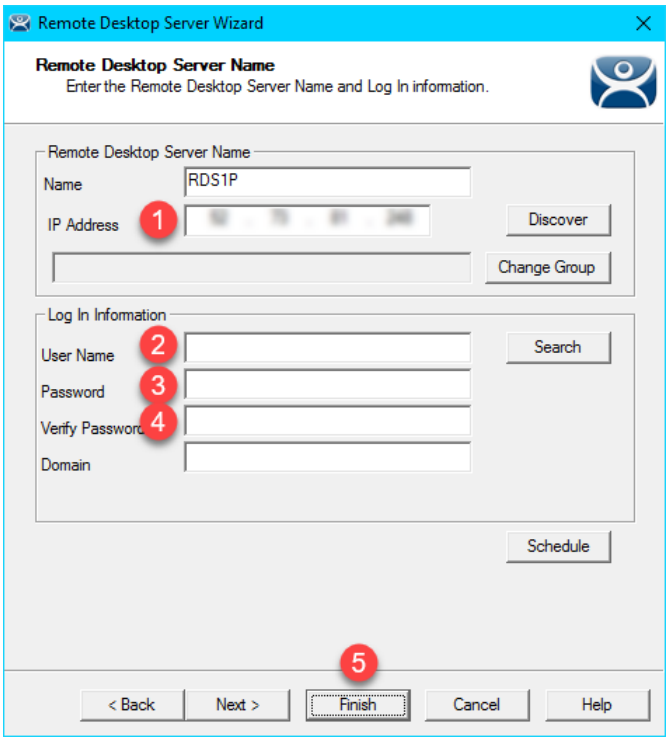


4. Double click the newly created **Display Server RDS1P**.



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, <u>delete</u> the **User Name**, **Password** and **Verify Password** entries. Click the **Finish** button.

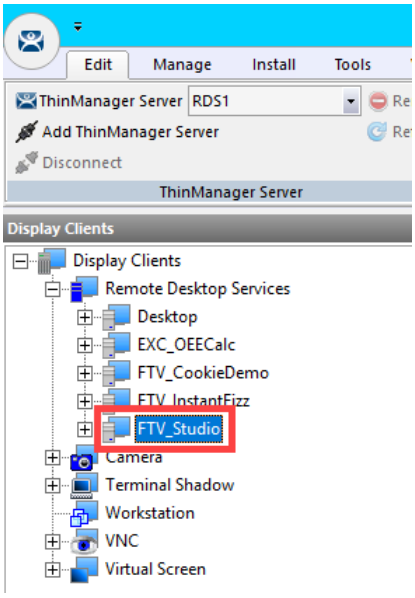


Reassign Display Client to Public Display Server

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**.

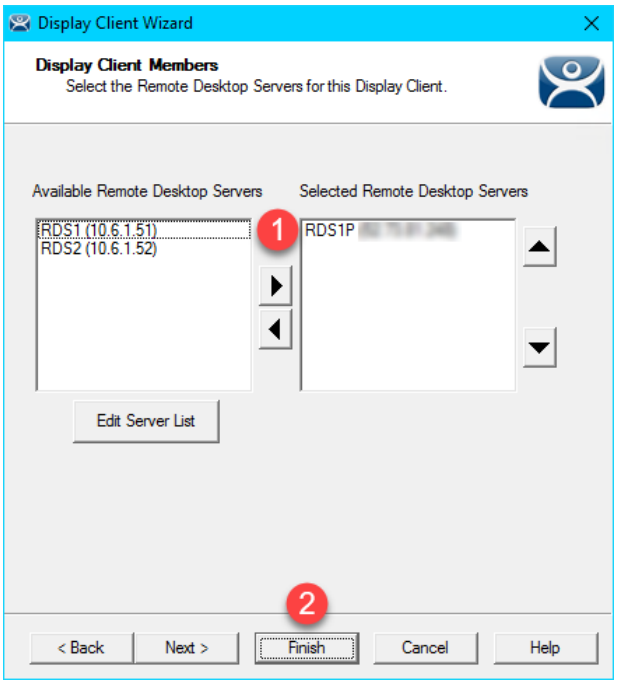
1. From ThinManager, click the **Display Clients** icon  from the ThinManager tree selector.

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



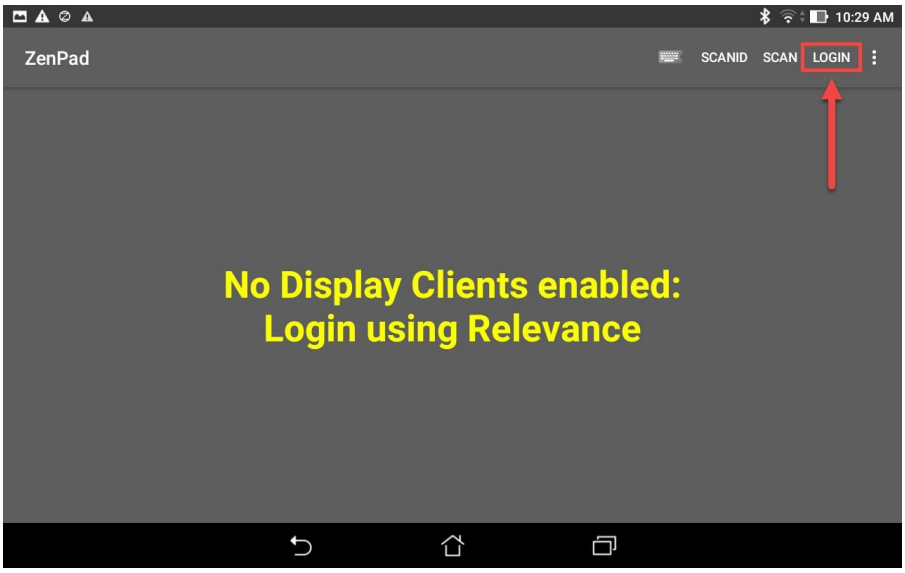
3. Click the **Next** button from the **Client Name** page of the wizard.
4. Click the **Next** button from the **Display Client Options** page of the wizard.
5. Click the **Next** button from the **Remote Desktop Services and Workstation Options** page of the wizard.
6. Click the **Next** button from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

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

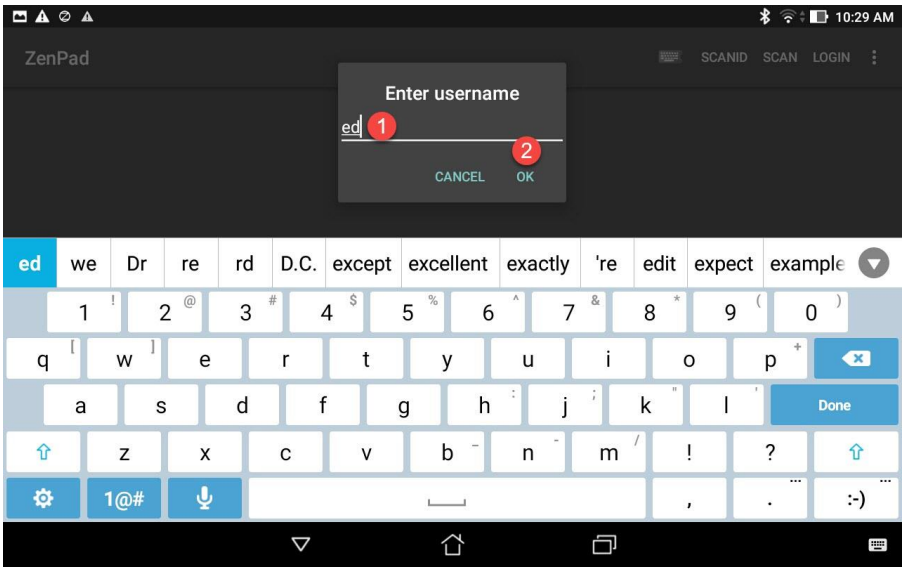


Login as Engineer User

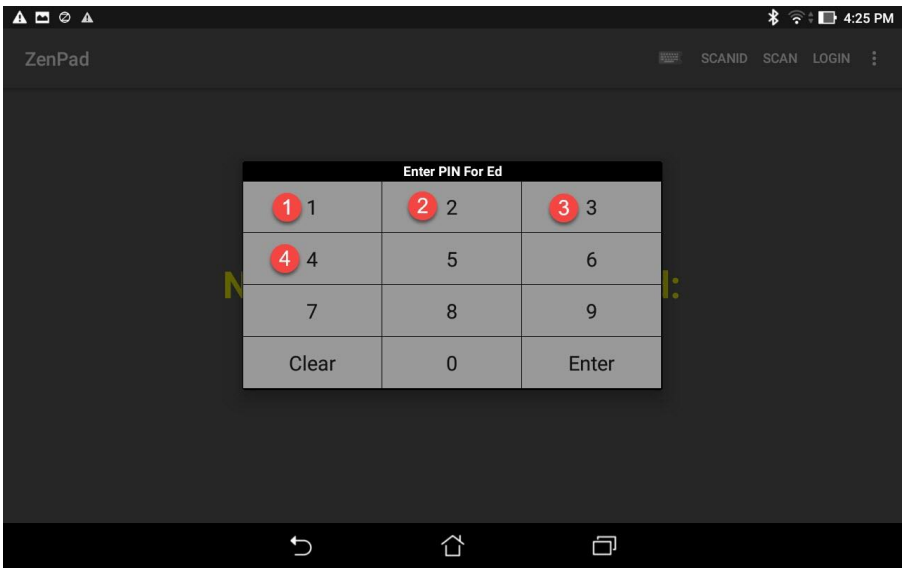
1. From the **aTMC** application, touch the **LOGIN** button in the top right corner.



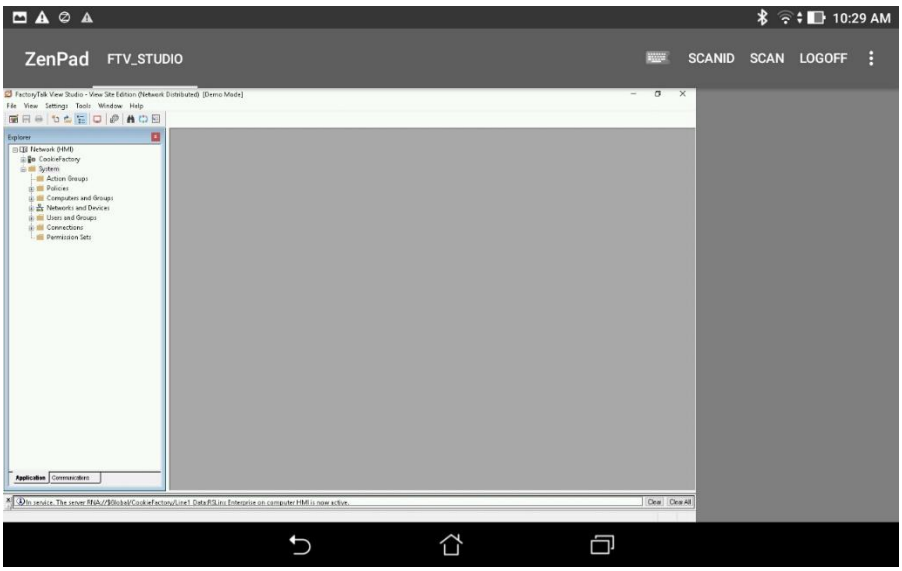
2. Enter *ed* as the **username** and touch the **Ok** button.



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.

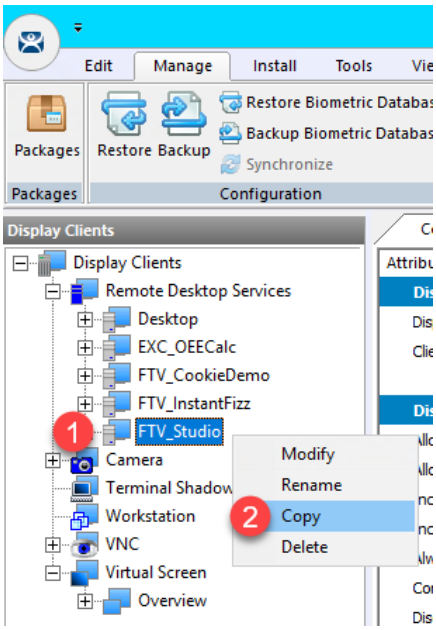
> Other tablet gestures are supported as well. Pinch and zoom works as expected. Once zoomed in, you can pan around the screen using two fingers on the tablet. You can also perform a 2 finger hold down, which will toggle the on screen keyboard.

Create Logix Designer Display Client

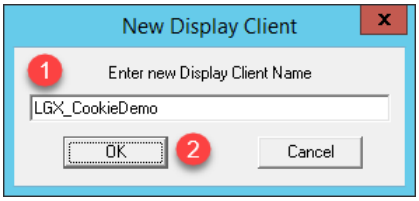
In these last sections of the lab, we are going to set ThinManager up to deliver **Logix Designer** to the **ZenPad** just by simply scanning a QR Code. The first step is to create the **Display Client** for **Logix Designer**.

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

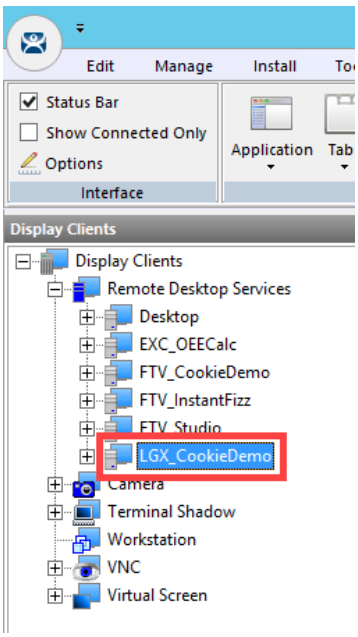
2. From the **Display Clients** tree, expand the **Remote Desktop Services** branch and right click the **FTV_Studio** item and select **Copy**.



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.

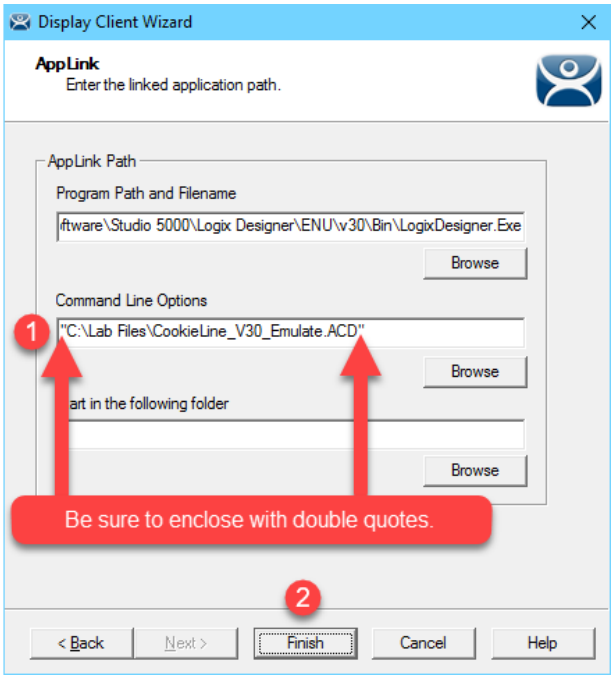
10. From the **AppLink** page of the wizard, replace the **Program Path and Filename** and the **Command Line Options** paths with the ones below (you can also copy and paste this path from the **LabPaths.txt** file by right clicking the **Notepad** icon pinned to the start bar and selecting **LabPaths.txt**):

    Program Path and Filename:

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

    Command Line Options:

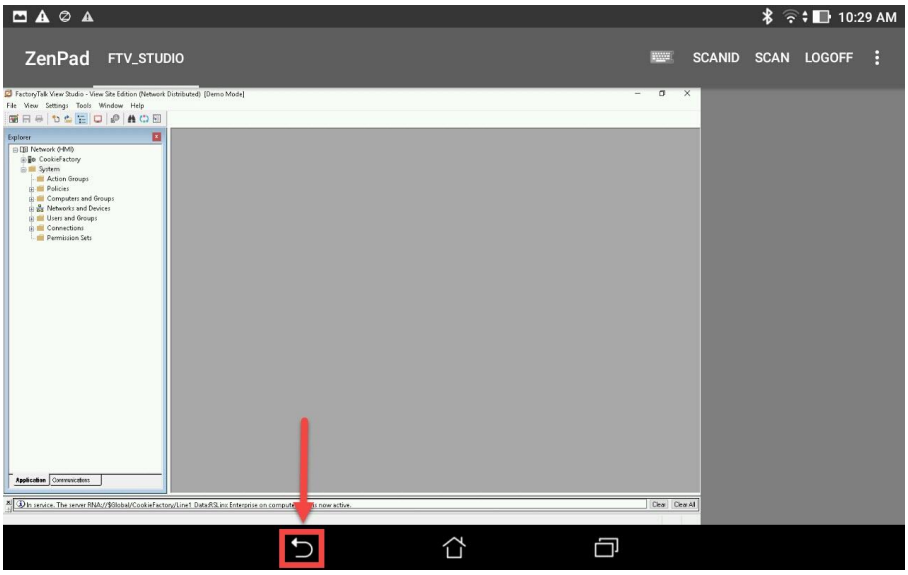
    ```
    "C:\Lab Files\CookieLine_V30_Emulate.ACD"
    ```



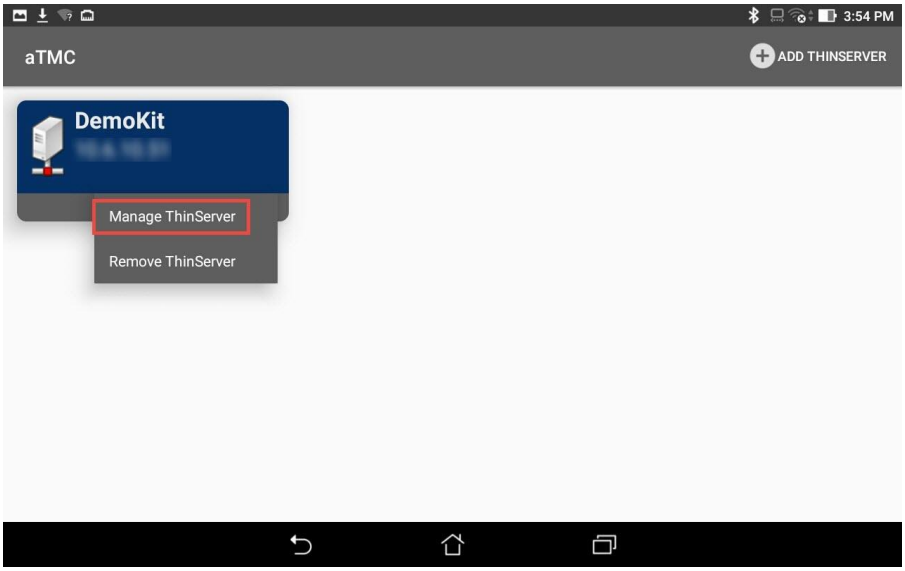
11. Click the **Finish** button.

Register QR Code Location Resolver from Mobile Device

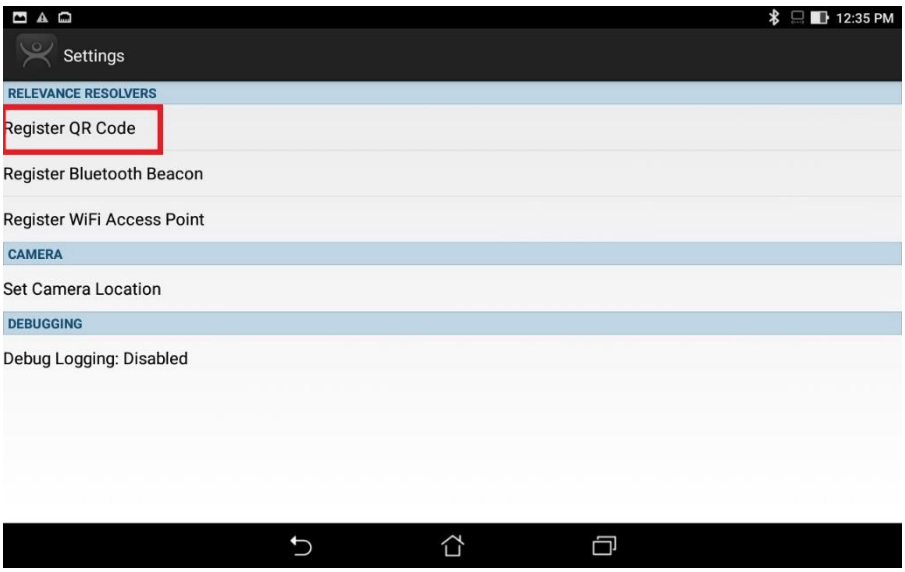
1. From aTMC, touch the **Back** button to return to the aTMC **Main Menu**. Touch **Yes** on the confirmation dialog.



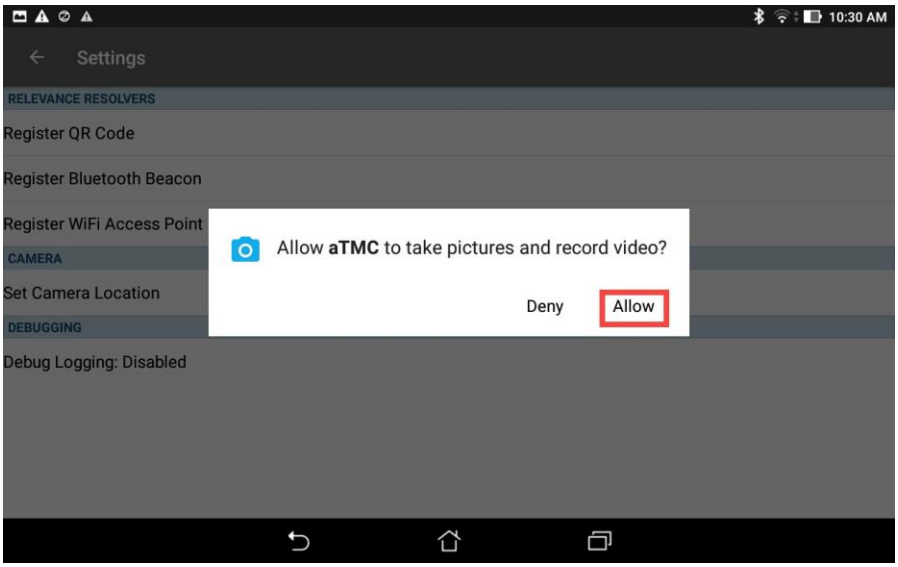
2. From the aTMC **Main Menu**, touch the **Settings** button (3 vertical dots below the **DemoKit** button), followed by the **Manage ThinServer** button.



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

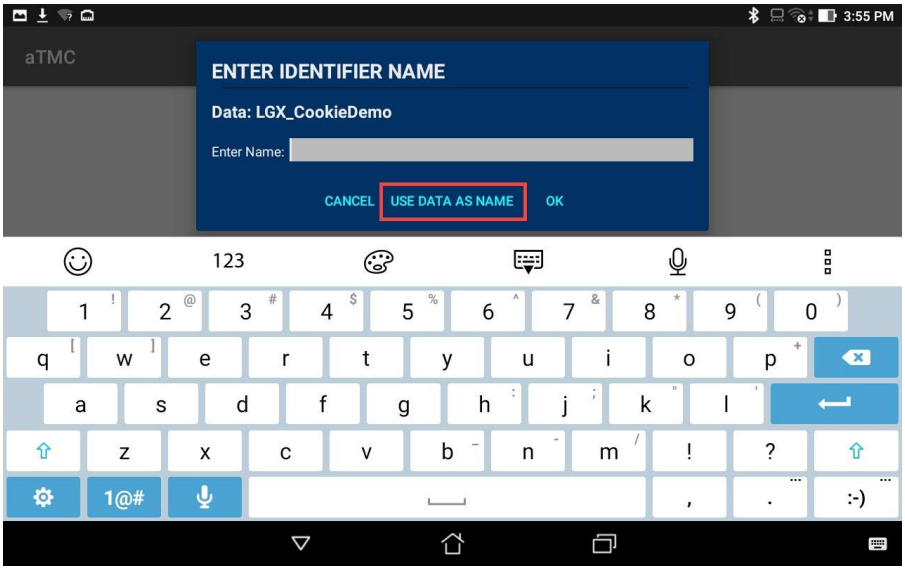


4. If you receive a prompt requesting permission for **aTMC** to take pictures and record video, touch the **Allow** button.



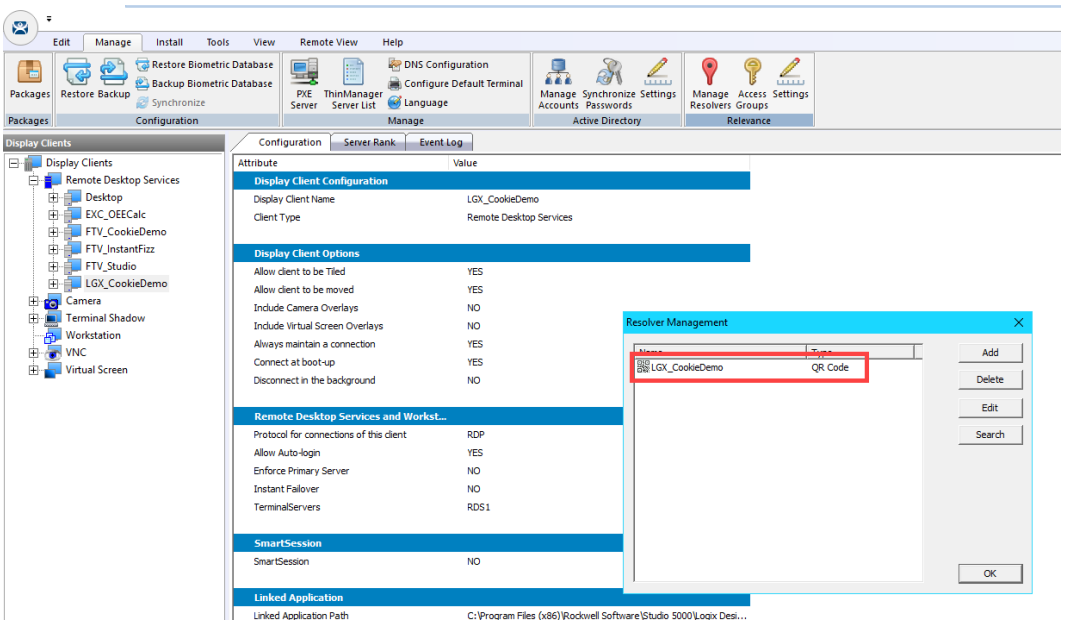
5. A camera window will appear. Point the Tablet camera at the **QR Code** below.

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.**

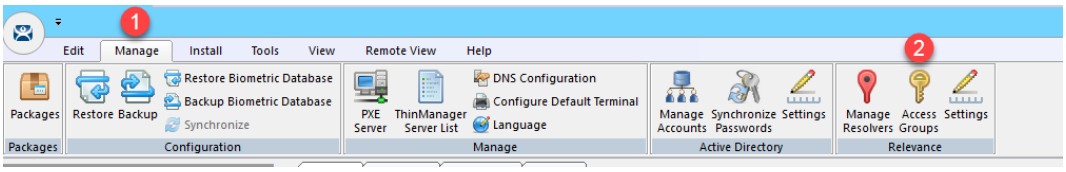
8. To confirm the creation of the **Location Resolver**, return to **ThinManager** on **RDS1**, click the **Manage** ribbon, followed by the **Manage Resolvers** icon. You should see a new **QR Code** resolver named **LGX_CookieDemo** in the **Resolver Management** window. Click the **OK** button.



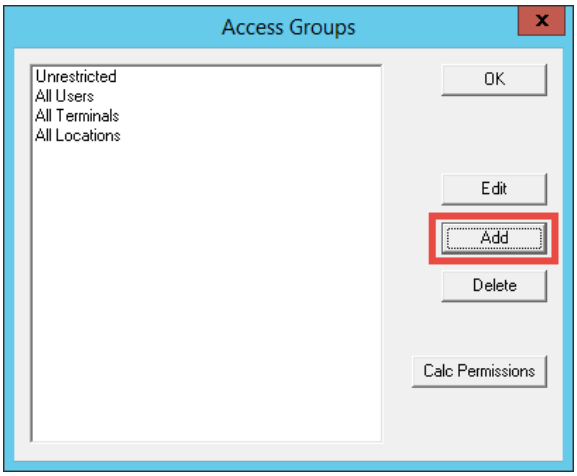
Create Engineer Access Group

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.

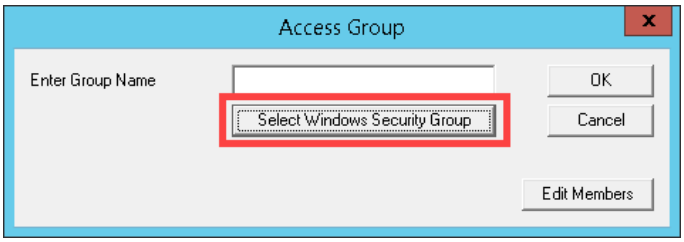
1. Click the **Manage** ribbon, followed by the **Access Groups** icon.



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

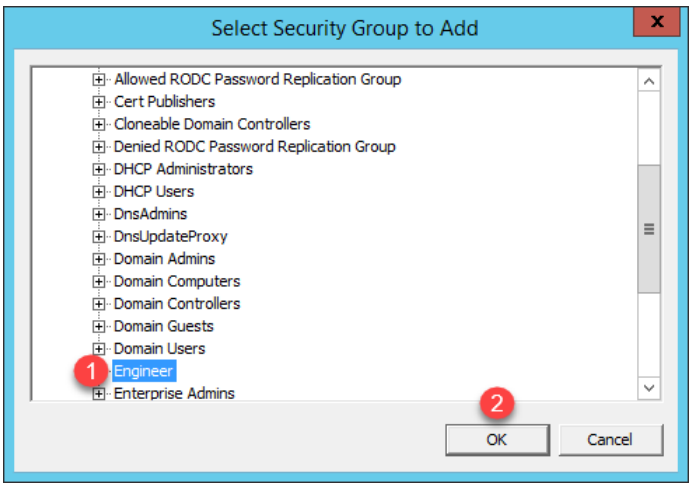


3. Click the **Select Windows Security Group** button.



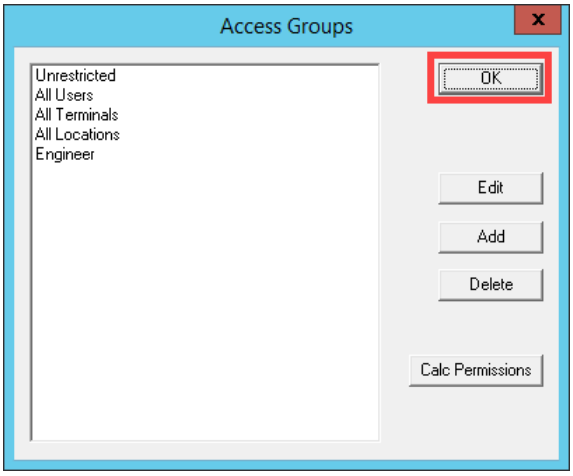
> The Select Windows Security Group provides the ability to link an Access Group to a Widows Security Group. Therefore, you could manage access to ThinManager resources (Terminals, Display Clients, etc.) through Windows Security Groups as well. You could also use the TermMon ActiveX within an ActiveX 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.



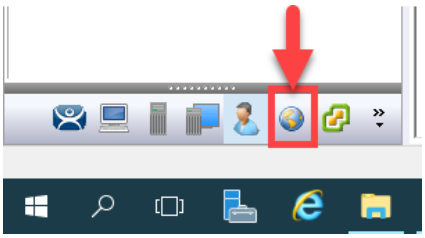
5. From the **Access Group** window, click the **OK** button.

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

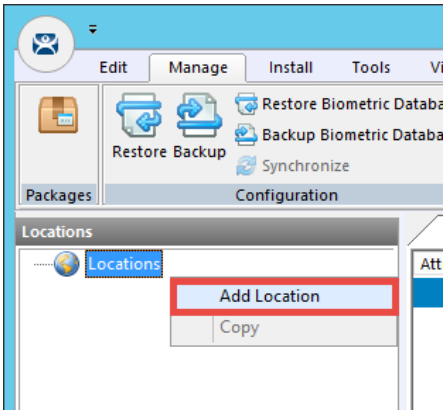


Create Relevance Location for Logix PLC

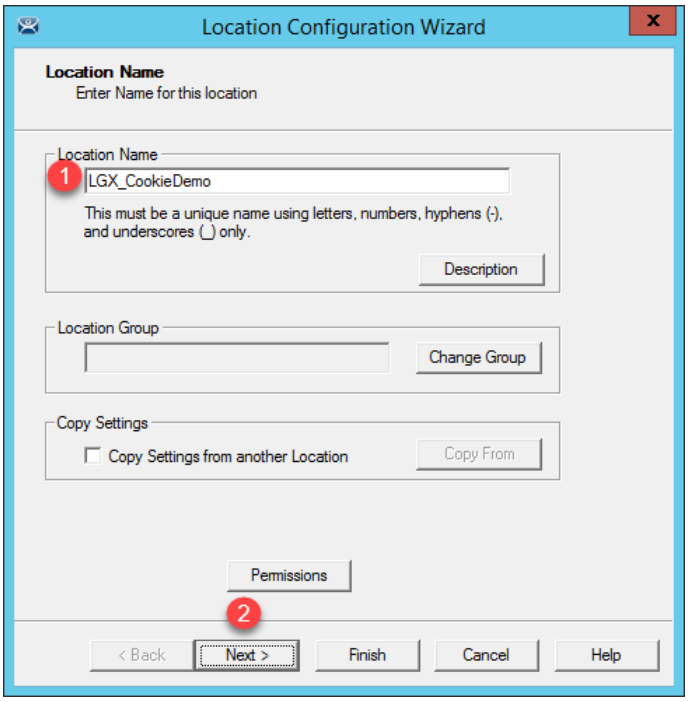
1. Click the **Locations** icon  in the tree selector.



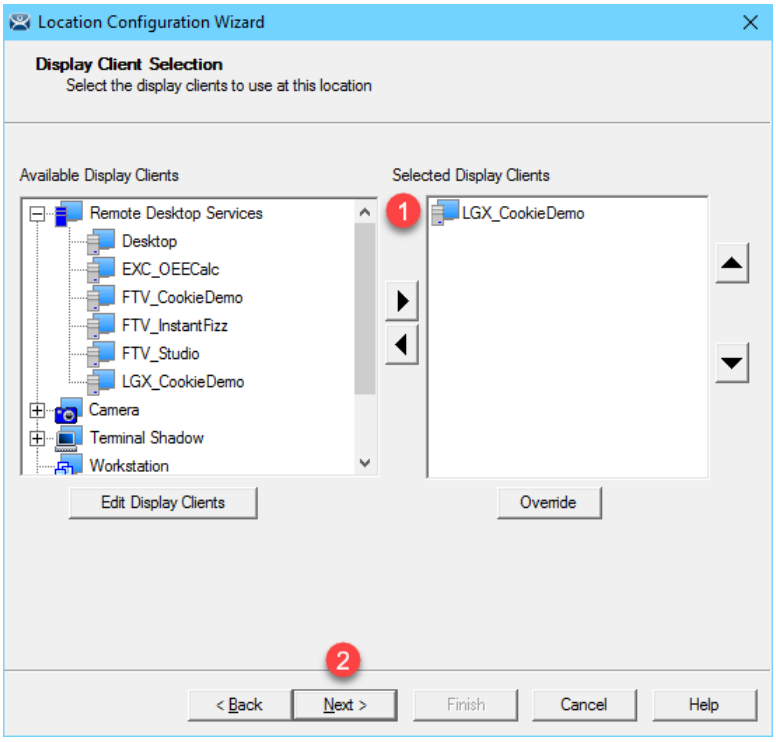
2. From the ensuing **Locations** tree, right click the **Locations** tree node and select **Add Location**.



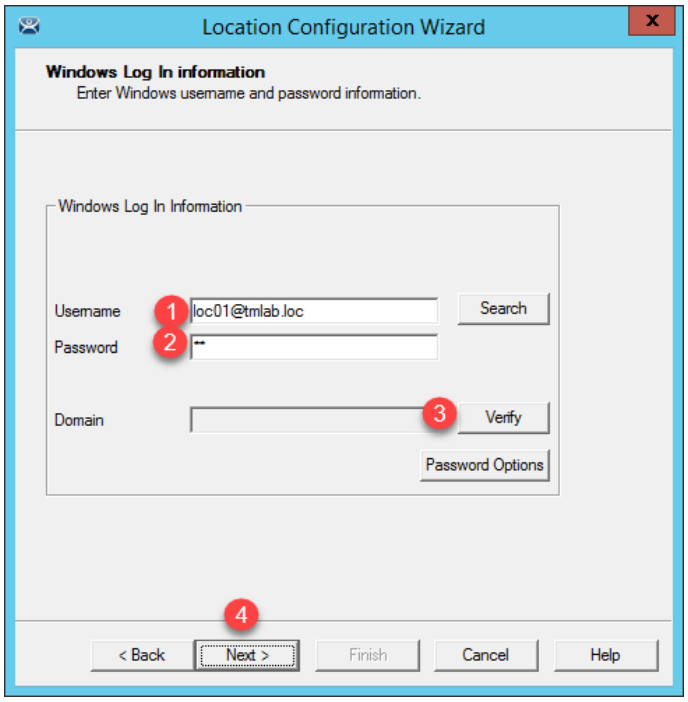
3. From the **Location Name** page of the **Location Configuration Wizard**, enter *LGX_CookieDemo* as the **Location Name**. Click the **Next** button.



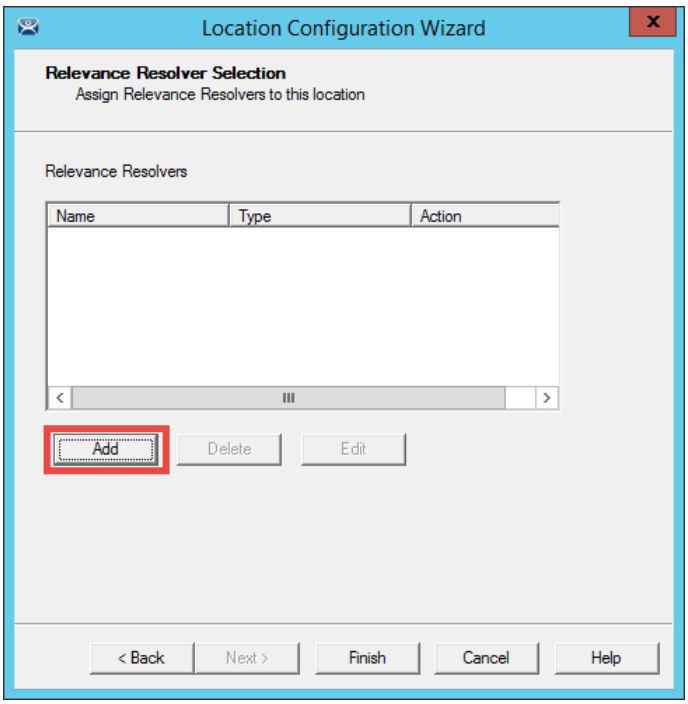
4. From the **Location Options** page of the wizard, click the **Next** button.
5. From the **Display Client Selection** page of the wizard, select the **LGX_CookieDemo Display Client** and click the **Right** arrow button to move it to the **Selected Display Clients** list, click **Next**.



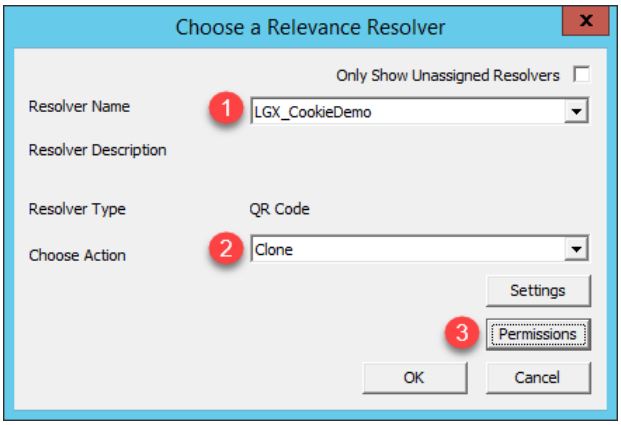
6. From the **Windows Log In information**, enter *loc01@tmlab.loc* as the **Username** and *rw* as the **Password**. Click the **Verify** button to confirm the credentials are valid. Click the **Next** button.



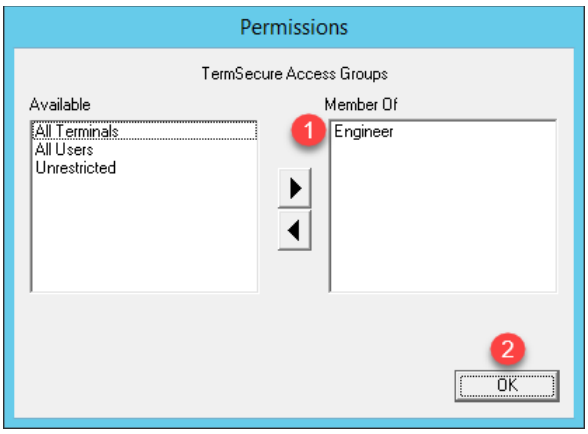
7. From the **Relevance Resolver Location** page of the wizard, click the **Add** button.



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.

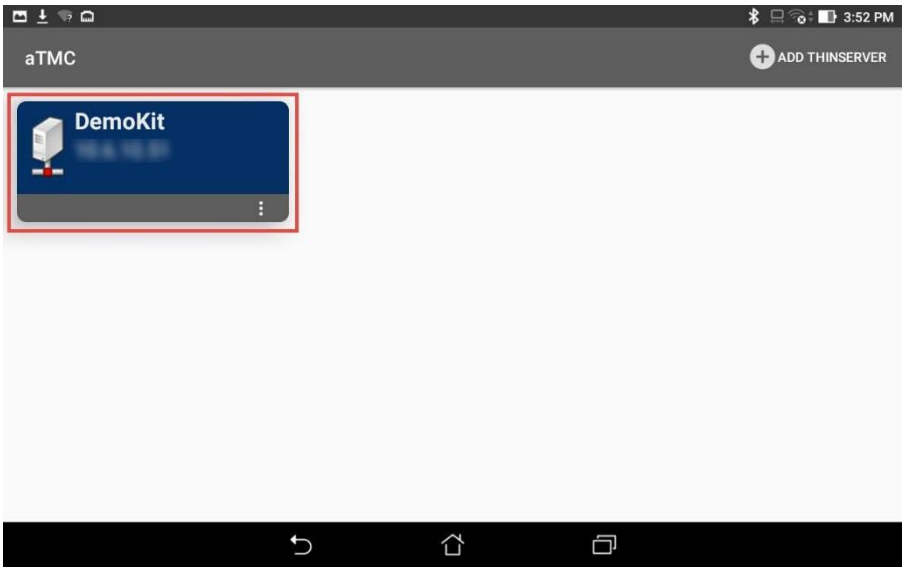


9. From the **Permissions** window, remove **Unrestricted** from the **Member Of** list, and move **Engineer** to the **Member Of** list. Click the **OK** button **twice**, followed by the **Finish** button.

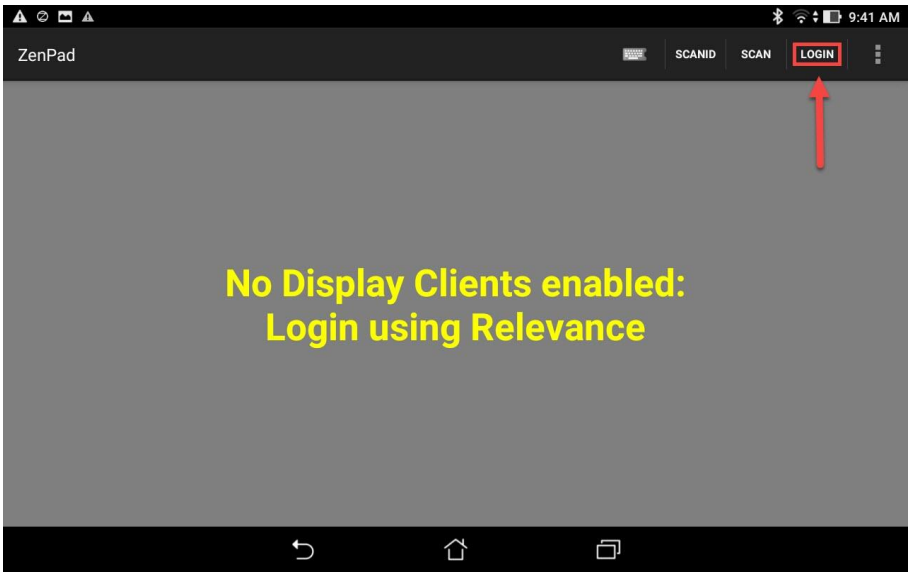


Resolve to Location from Mobile Device

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.

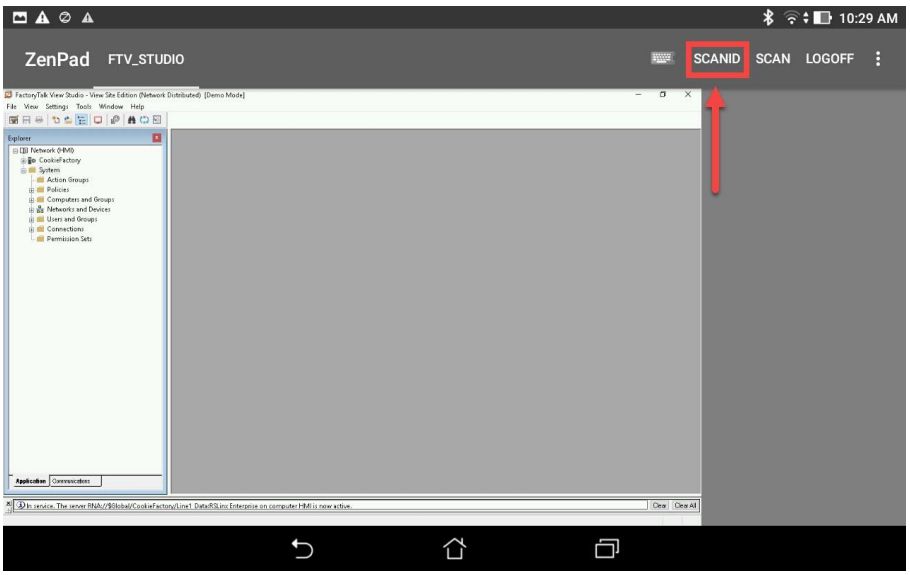


2. If not already logged in as **Ed**, touch the **LOGIN** button and enter a **username** of *ed* and a PIN of *1234*.



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

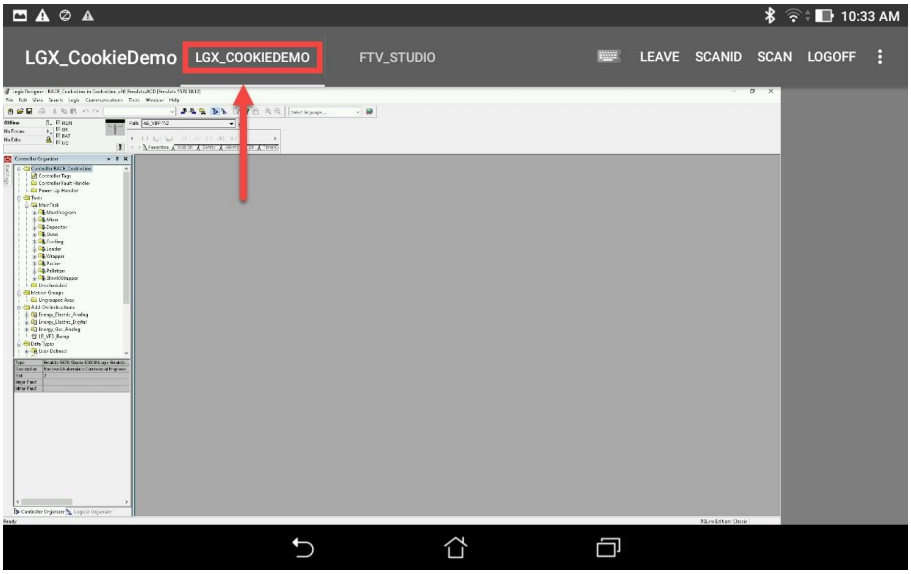
3. Once logged in as Ed, touch the **SCANID** button in the top right corner.



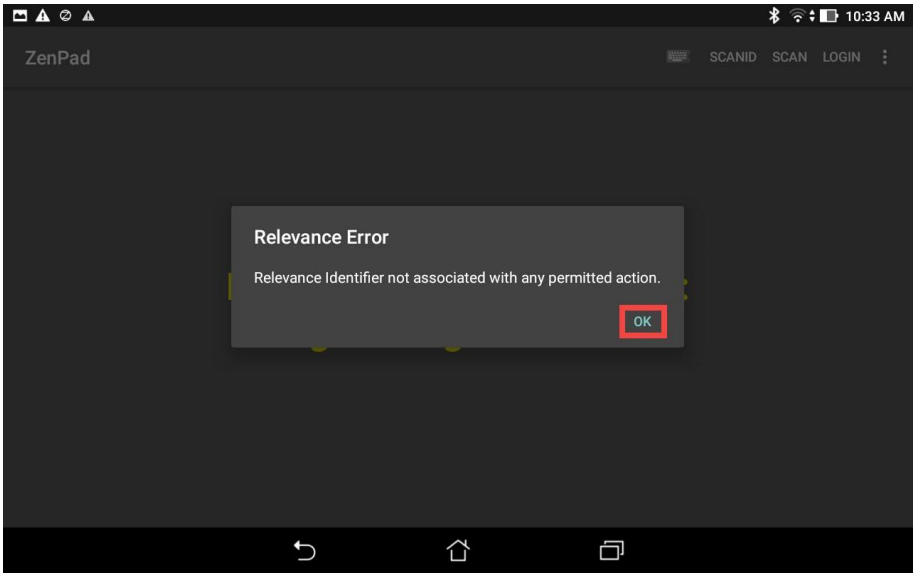
There is also a SCAN button available to the right of SCANID that enables the scanning of barcodes within the delivered applications.

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

5. 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**.



6. 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.



Checkpoint Question: https://thinmanager.com/cloudlabs/section10/

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

Section 11: ThinManager Redundancy and Firewall Configuration

Overview

With ThinManager installed on both **RDS1** and **RDS2** servers, we can now enable automatic synchronization to provide ThinManager redundancy. With redundancy enabled, we will be able to utilize **Windows Firewalls** to demonstrate how the ThinManager firmware and terminal profiles are delivered over the network. On **RDS1**, we will turn on **Windows Firewalls** and open the necessary ports required by ThinManager to communicate. After learning about ThinManager redundancy and firewall configurations, we will disable the secondary ThinManager server for the remainder of the lab sections.

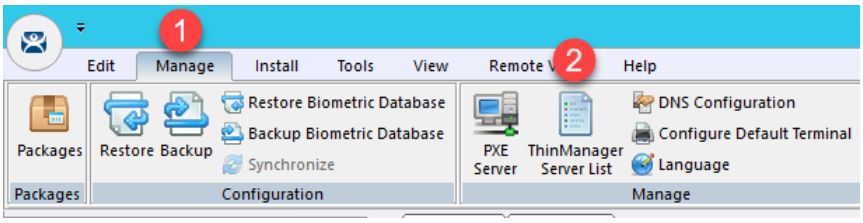
In this section, you will be performing the following tasks:

1. Configure Automatic Synchronization
2. Add Remote ThinManager Server
3. Disable Automatic Synchronization
4. Turn On Windows Firewall on RDS1
5. Configure Windows Firewall on RDS1
6. Disable Secondary ThinManager Server

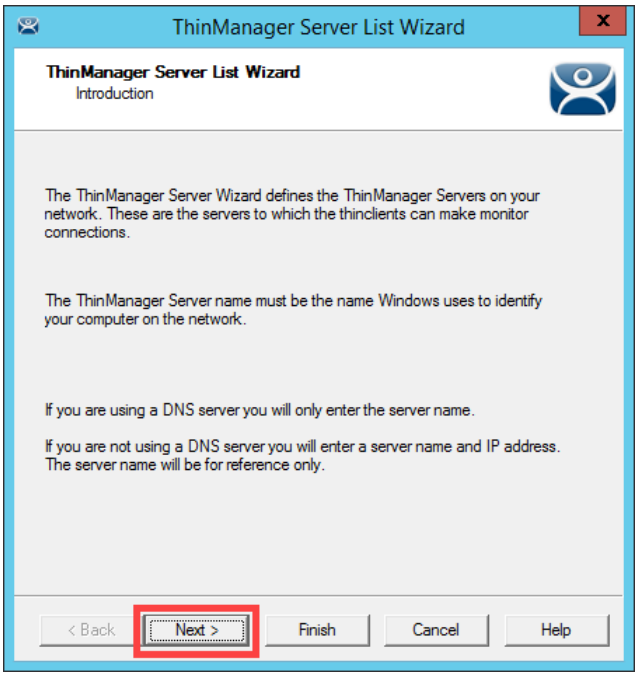
Configure Automatic Synchronization

As previously mentioned, automatic synchronization is generally used in **Redundant** deployments. It automatically synchronizes the ThinManager configurations between two ThinManager installations so that either ThinManager installation can boot terminals and deliver terminal profiles. In the subsequent steps, you will configure **RDS1** and **RDS2** to be synchronization partners.

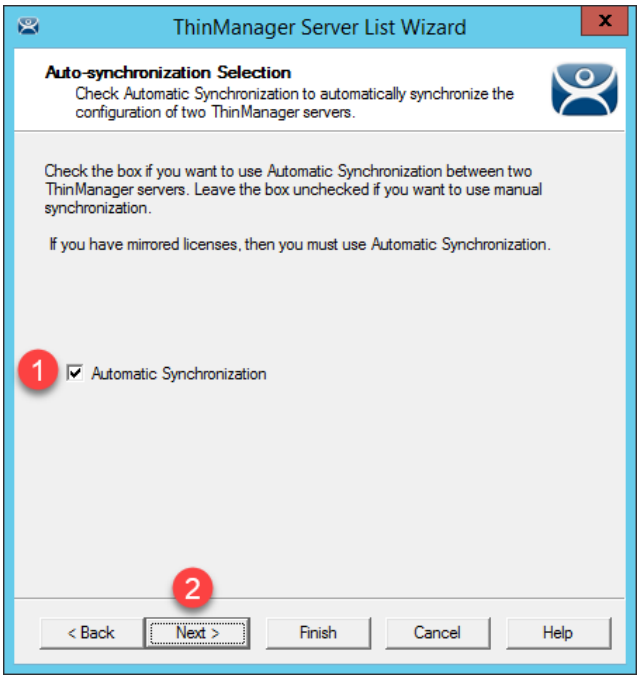
1. From ThinManager, click the **Manage** ribbon followed by the **ThinManager Server List** icon.



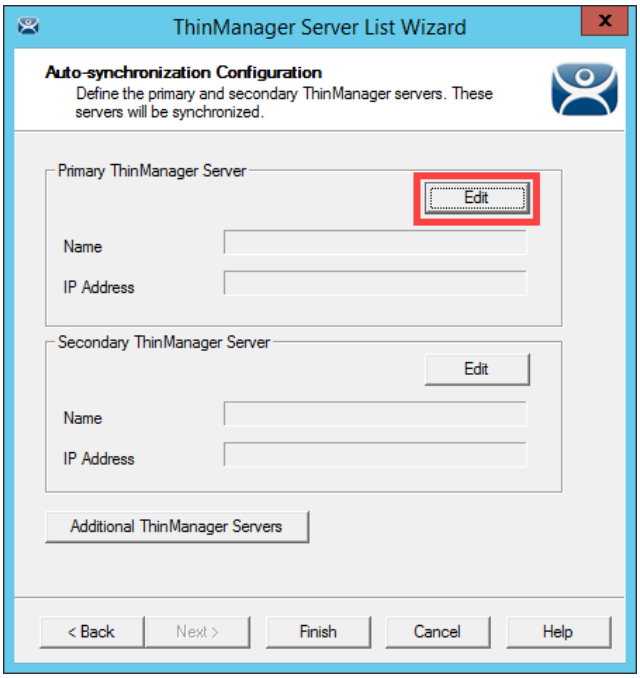
2. The **ThinManager Server List Wizard** will launch. Click the **Next** button from the **Introduction** page of the wizard.



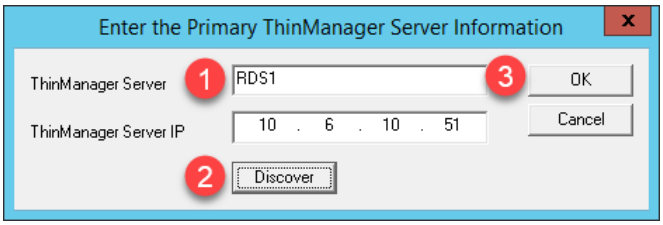
3. From the **Auto-synchronization Selection** page of the wizard, check the **Automatic Synchronization** checkbox and click the **Next** button.



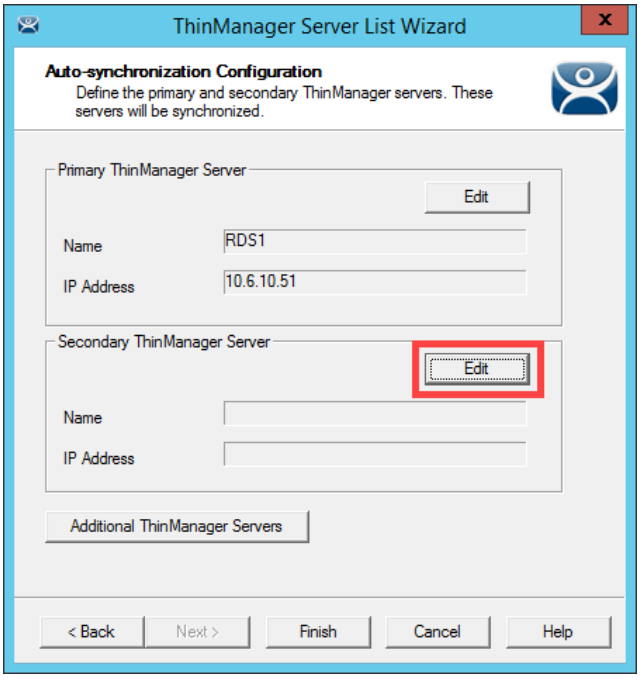
4. From the **Auto-synchronization Configuration** page of the wizard, click the **Edit** button in the **Primary ThinManager Server** frame.



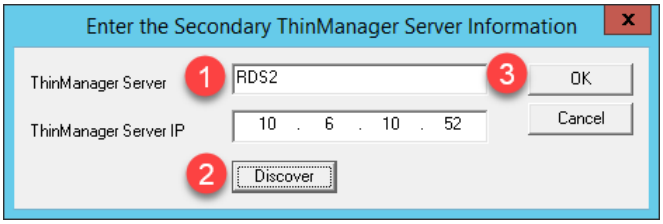
5. Enter *RDS1* in the **ThinManager Server** field, followed by the **Discover** button, which should auto-fill the **IP Address** of **RDS1** in the **ThinManager Server IP** Field. Click the **OK** button.



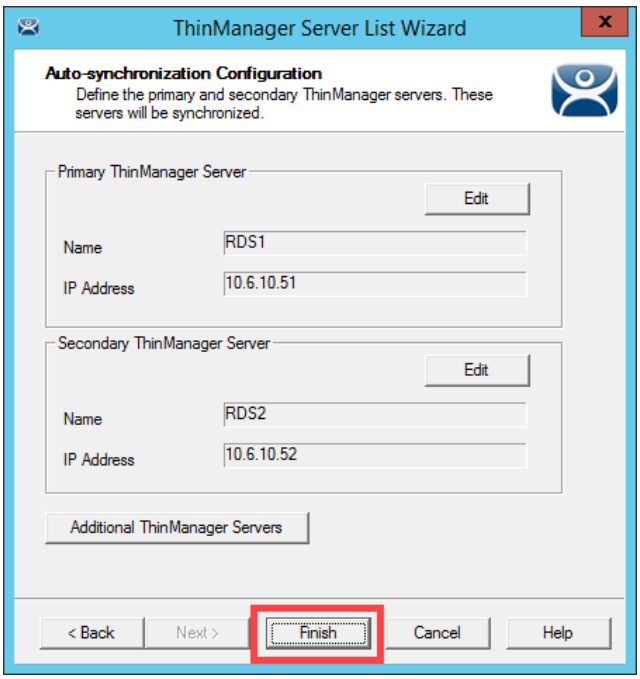
6. Back on the **Auto-synchronization Configuration** page of the wizard, click the **Edit** button from the **Secondary ThinManager Server** frame of the wizard.



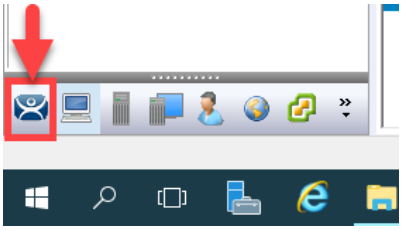
7. Enter *RDS2* in the **ThinManager Server** field, followed by the **Discover** button, which should auto-fill the **IP Address** of **RDS2** in the **ThinManager Server IP** Field. Click the **OK** button.



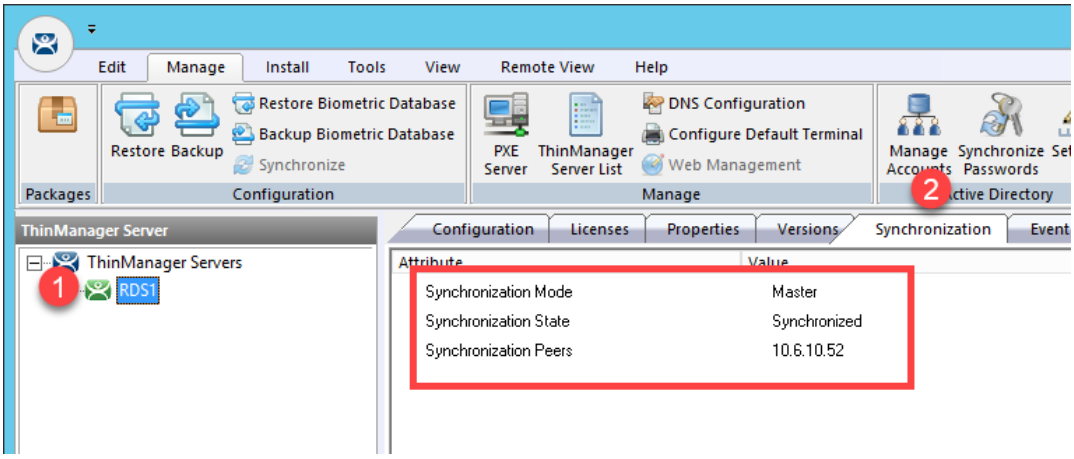
8. Back on the **Auto-synchronization Configuration** page of the wizard, click the **Finish** button.



9. To check the state of the synchronization, click the **ThinManager** icon from the button bar.



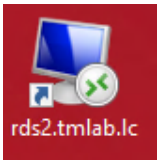
10. From the **ThinManager Server** tree, select **RDS1**, followed by the **Synchronization** tab. You should see a **Synchronization State** of **Synchronized**.



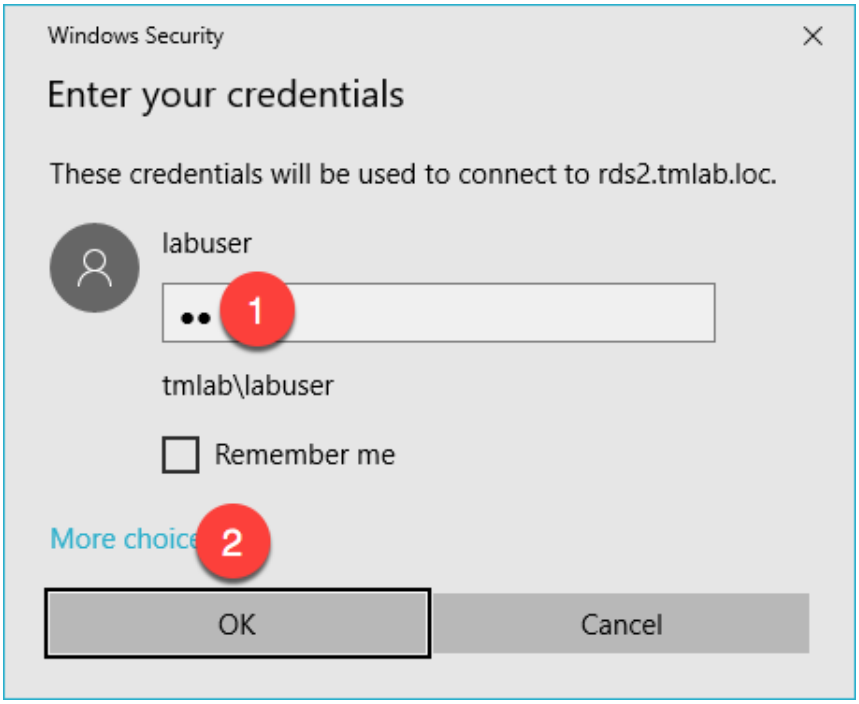
If the Synchronization State does not immediately show Synchronized, simply click on another tab, and return to the Synchronization tab to refresh its state.

Since the first synchronization was initiated from RDS1, it becomes the initial Master. Subsequently, the ThinServer that has been up and running the longest will assume the role of Master.

11. To further confirm the synchronization state, double click the **rds2.tmlab.loc** shortcut on the **RDS1** desktop.

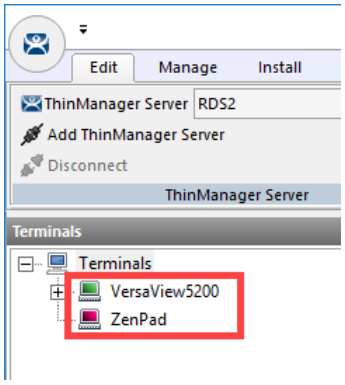


12. If you are presented with a login dialog box, make sure the username is *tmlab\labuser* and enter a password of *rw*. Click the **OK** button.



13. From the **RDS2** desktop, double click the **ThinManager** shortcut on the desktop.

14. Notice that the ThinManager configuration on **RDS2** now has terminals configured since it has been **synchronized** with the configuration from **RDS1**. Close the **ThinManager Admin Console**.

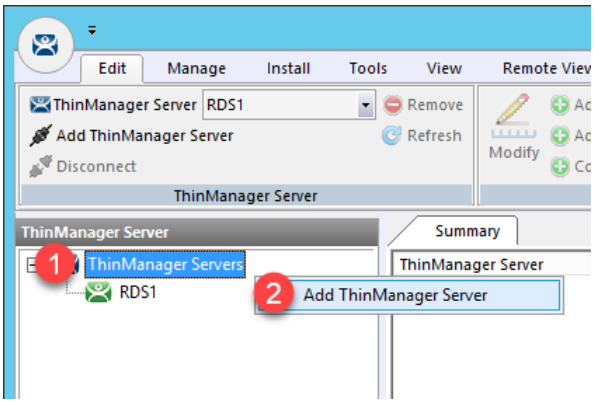


15. Close the remote desktop session on **RDS2**. Click the **OK** button if you are presented with a confirmation dialog box.

Add Remote ThinManager Server

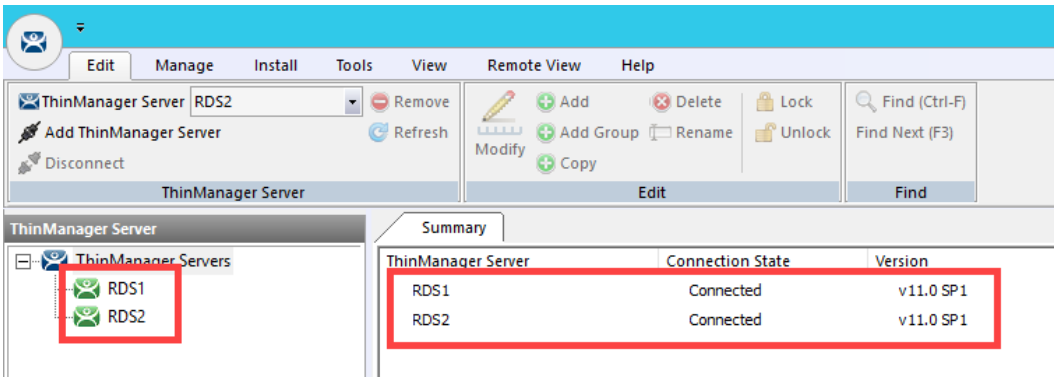
The ThinManager **Administrative Console** can manage not only the **ThinServer** installed on its machine, but also remote **ThinServers** installed on remote machines. Keep in mind that the **Administrative Console** does not have to be installed on the same machine as the **ThinServer** service, although it often is. So, you could have a number of remote **ThinServers**, all of which could be remotely managed by a single **ThinManager Administrative Console**. With that said, only a pair of **ThinServers** can have their configurations **synchronized**.

1. From the **ThinManager Server** tree, right click the **ThinManager Servers** item and select **Add ThinManager Server**.

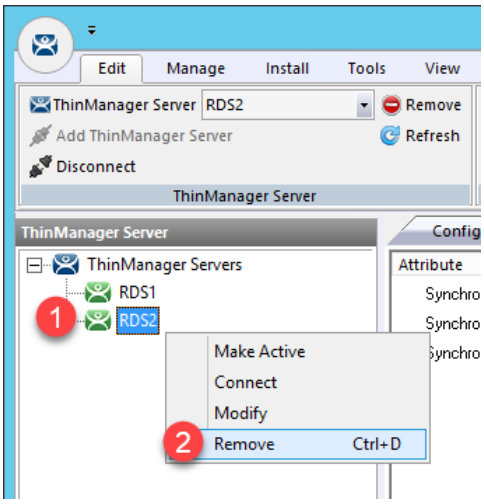


2. From the **ThinManager** popup window, enter *RDS2* in the **Enter ThinManager Server** field and click the **OK** button.

3. Notice that **RDS2** has now been added to the **ThinManager Admin Console**. You could now manage the ThinManager configuration of **RDS2** remotely from **RDS1**.



4. Since **RDS1** and **RDS2** are **synchronization** partners, managing **RDS2** from **RDS1** isn't all that useful (since their configurations will always be the same), but it is useful to see how easily this accomplished. With that said, let's remove **RDS2** from the **Admin Console** on **RDS1**.

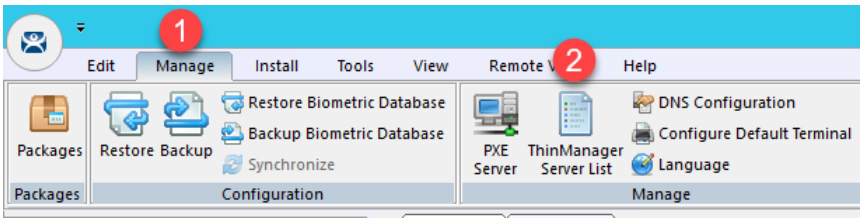


5. From the ensuing confirmation dialog box, click the **Yes** button.

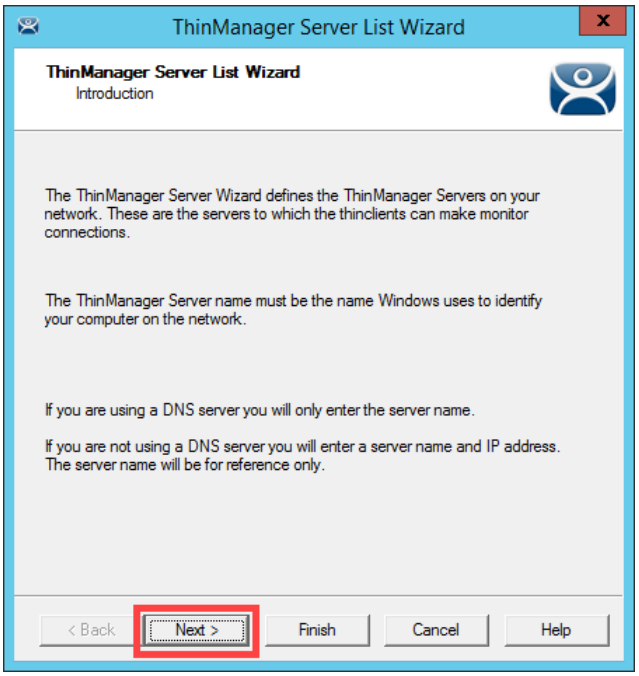
Disable Automatic Synchronization

We will disable automatic synchronization to prepare for the remaining advanced lab section(s).

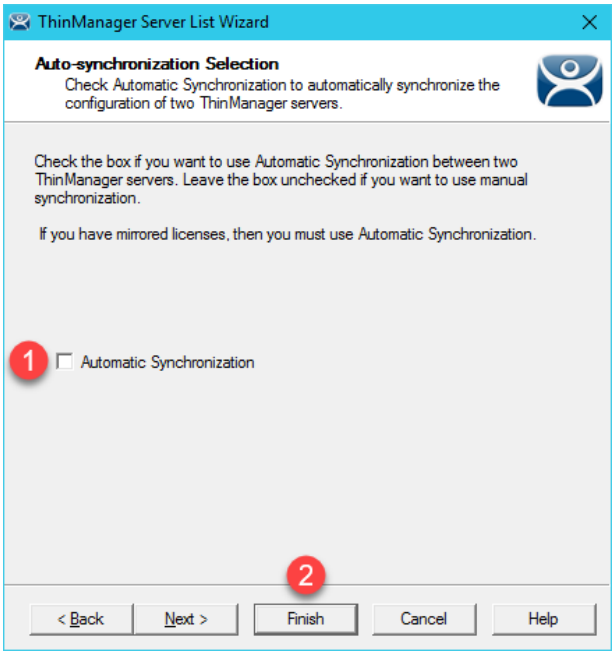
1. From ThinManager, click the **Manage** ribbon followed by the **ThinManager Server List** icon.



2. The **ThinManager Server List Wizard** will launch. Click the **Next** button from the **Introduction** page of the wizard.



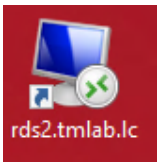
3. From the **Auto-synchronization Selection** page of the wizard, uncheck the **Automatic Synchronization** checkbox and click the **Finish** button.



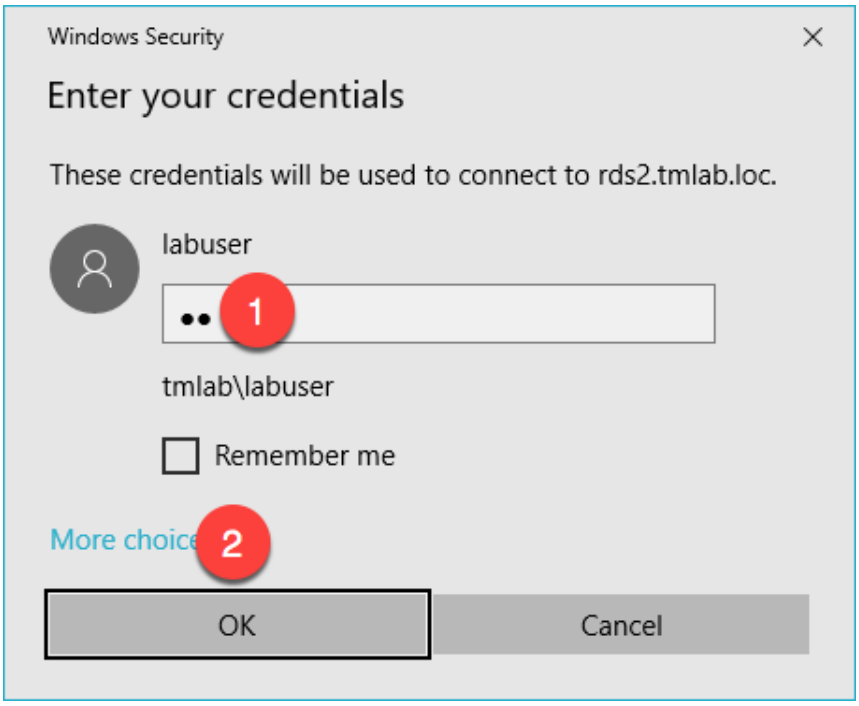
Disable Secondary ThinManager Server

We will disable the secondary ThinManager server for the remainder of the lab sections as well.

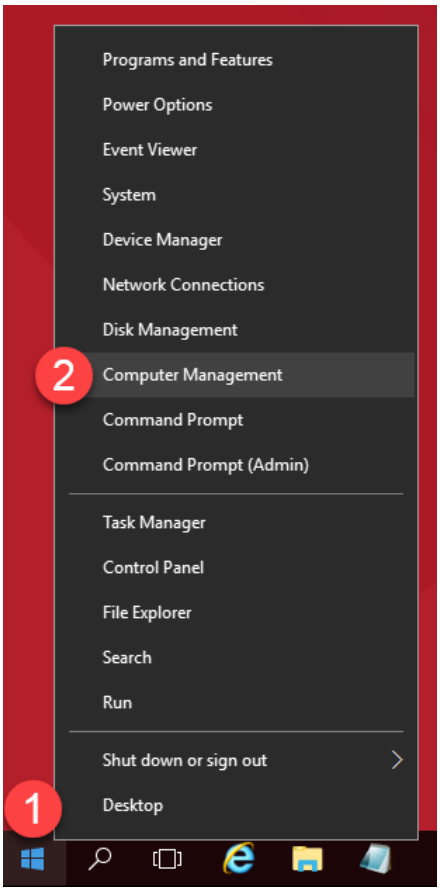
1. Double click the **rds2.tmlab.loc** shortcut on the **RDS1** desktop.



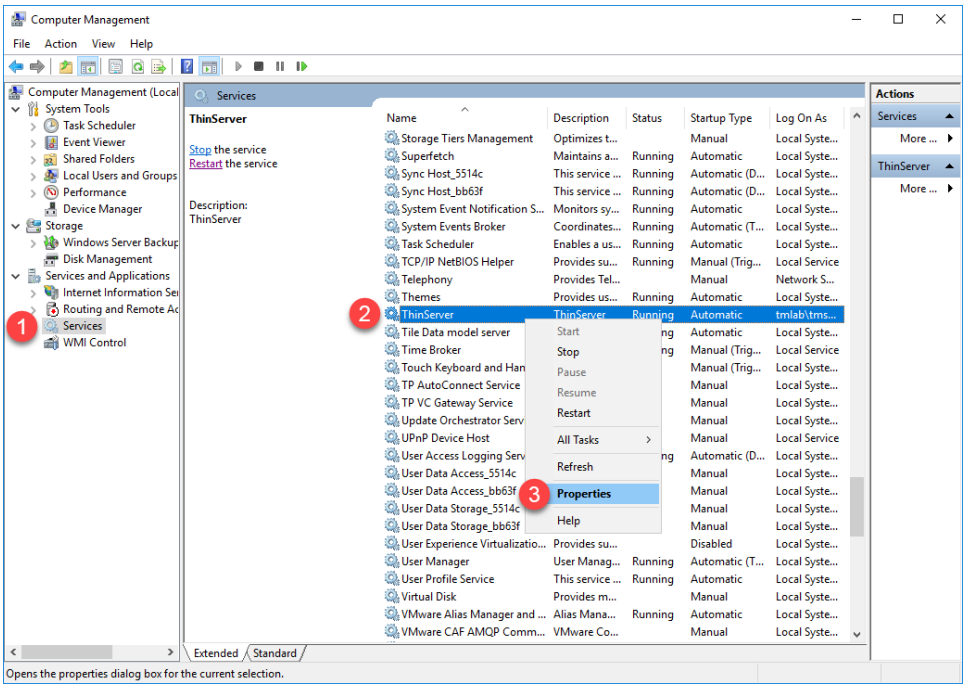
2. If you are presented with a login dialog box, make sure the username is *tmlab\labuser* and enter a password of *rw*. Click the **OK** button.



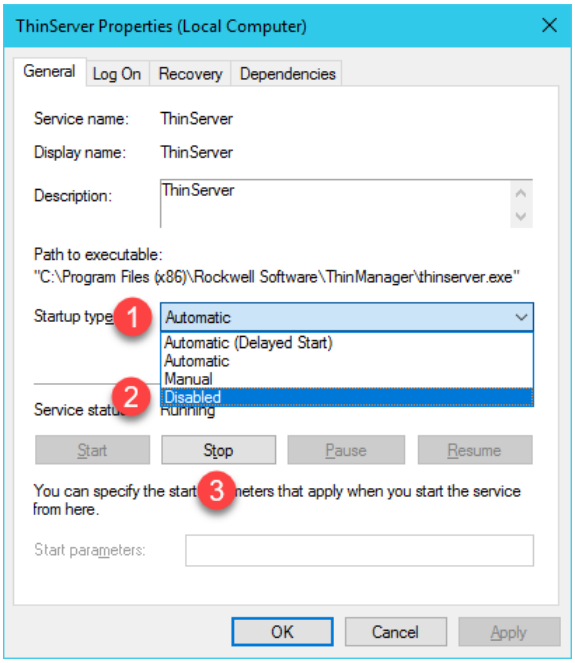
3. Close the **ThinManager Admin Console** if it is open.
4. Right-click the **Windows Start** button and select **Computer Management**.



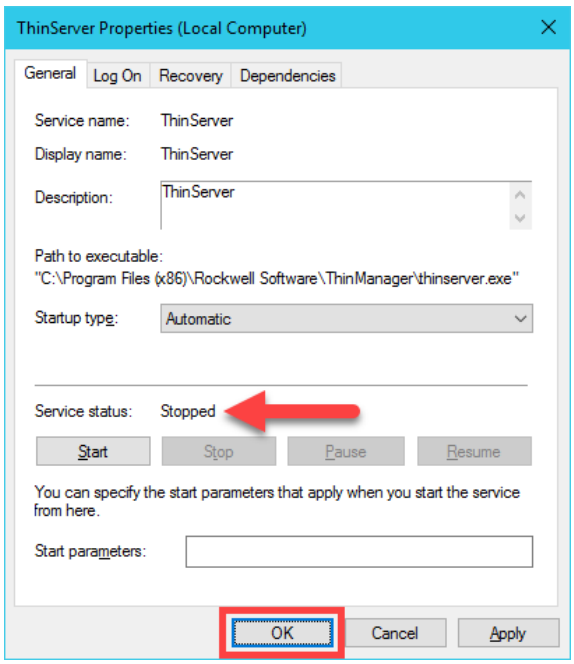
5. Expand the **Services and Applications** node and select the **Services** management console. Scroll down to find the **ThinServer** service, right-click and select **Properties.**



6. On the **General** tab, click the **Startup type** drop down list and select **Disabled**, then click the **Stop** button.



7. Confirm it has stopped and click **OK.**

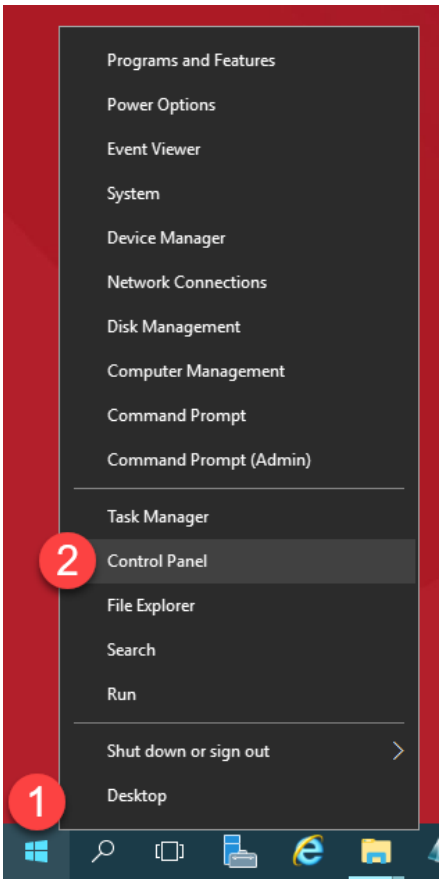


8. You have successfully disabled the **Secondary ThinManager Server**. The remaining lab sections can be completed with a single **ThinManager Server**. Close out of the **Computer Management** console on **RDS2**.

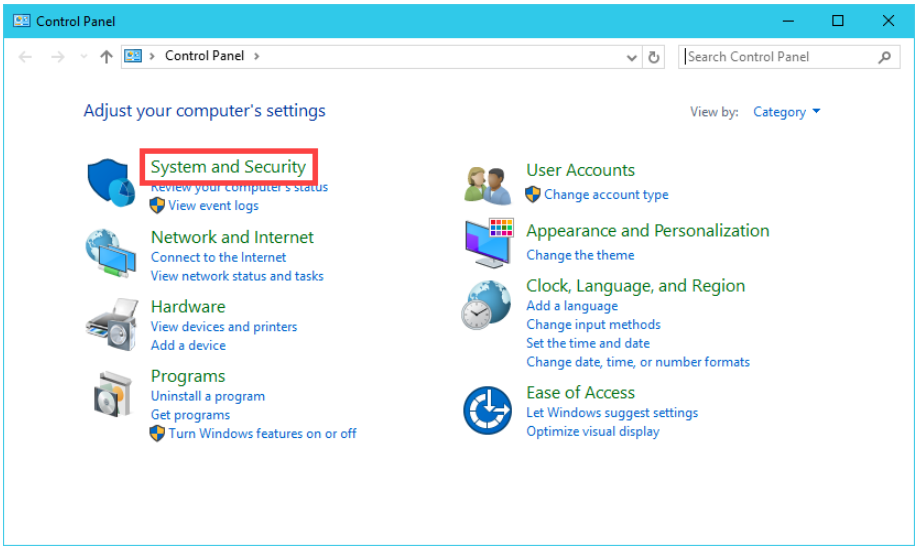
9. Close the remote desktop session on **rds2.tmlab.loc** to return to **RDS1**. Click the **OK** button if presented with a confirmation dialog box.

Turn On Windows Firewall on RDS1

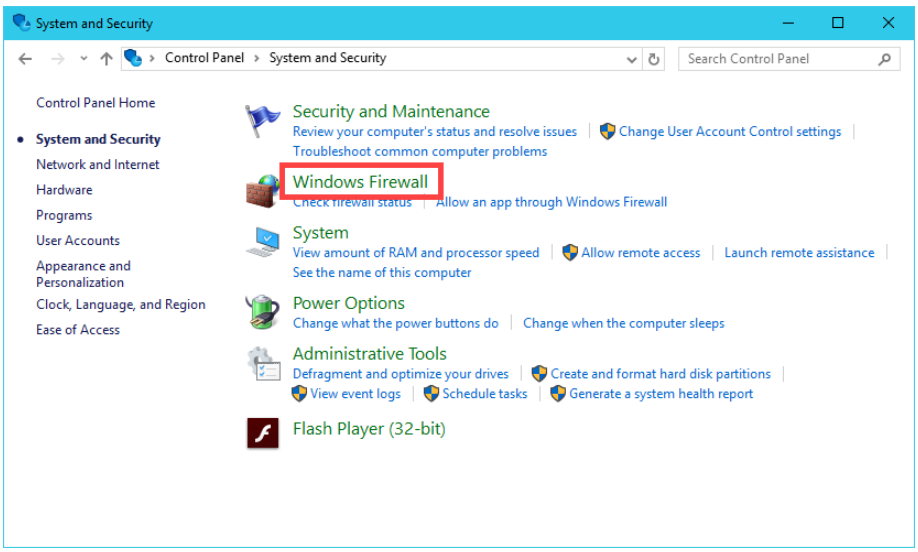
1. With the **VersaView5200** virtual thin client still powered on, right click the **Windows Start Button** on **RDS1** and select **Control Panel**.



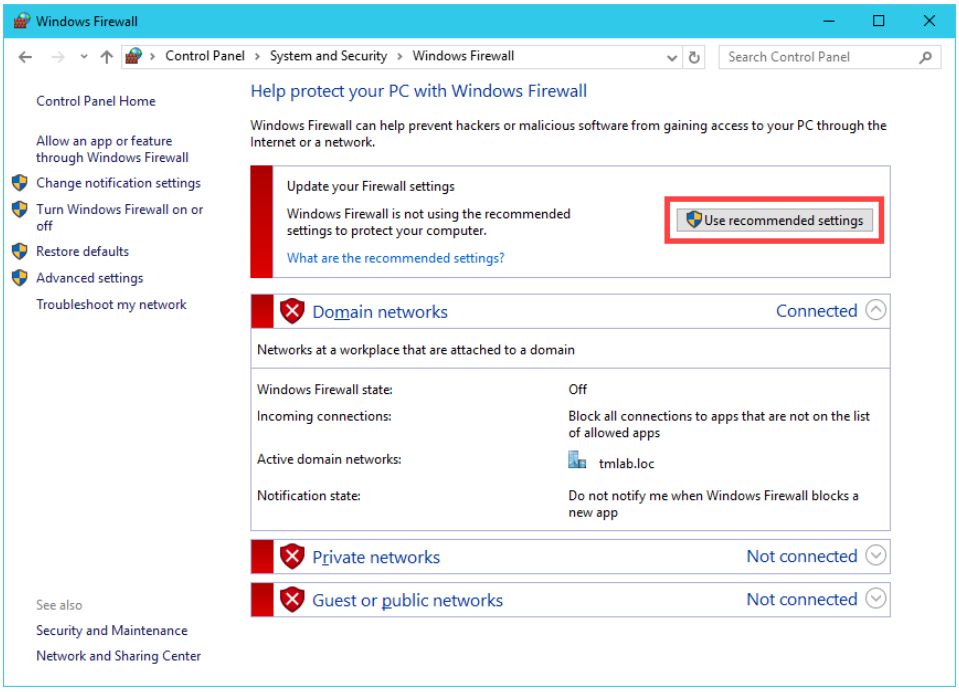
2. From the **Control Panel**, click the **System and Security** link.



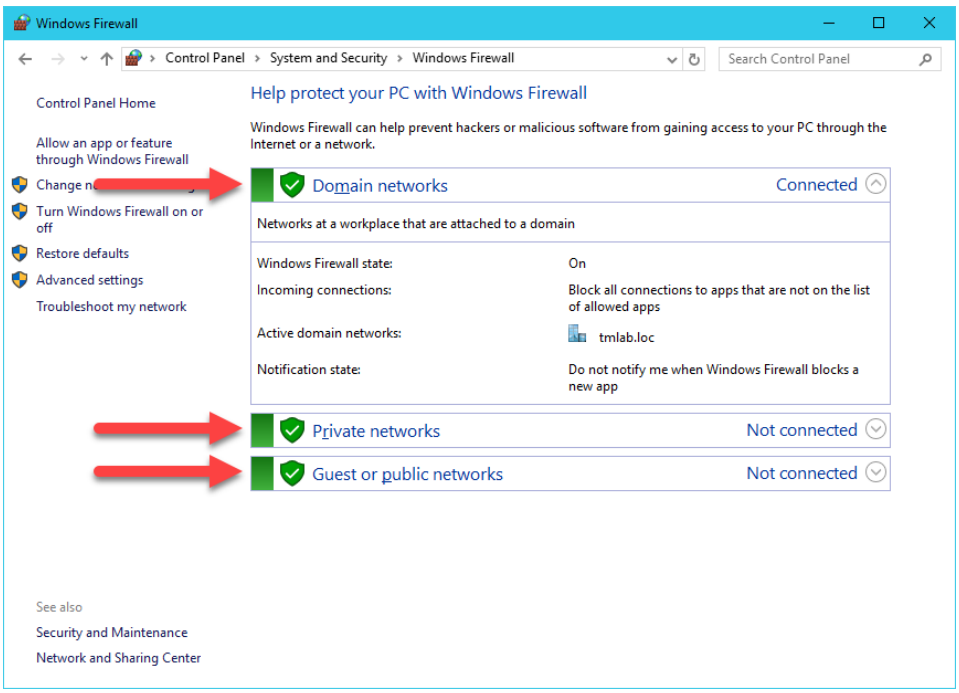
3. From the **System and Security** page of the **Control Panel**, click the **Windows Firewall** link.



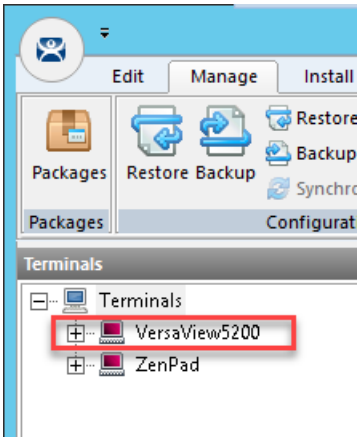
4. From the **Windows Firewall** page of the **Control Panel**, click the **Use recommended settings** button.



5. The result should be the 3 **domain profiles**, **Domain**, **Private** and **Public**, should all be **Turned On** and **Green**.



6. If you return to **ThinManager**, and select the **Terminals** button bar icon, you should see the **VersaView5200** terminal icon is now **Red**, indicating that we have lost our **Terminal Monitor Connection** with our virtual thin client, since that traffic is now being blocked by the **Windows Firewall**. The virtual thin client can still receive its content from its source (**RDS1**) via **TCP3389**, which is opened by default on the **Windows Firewall**.

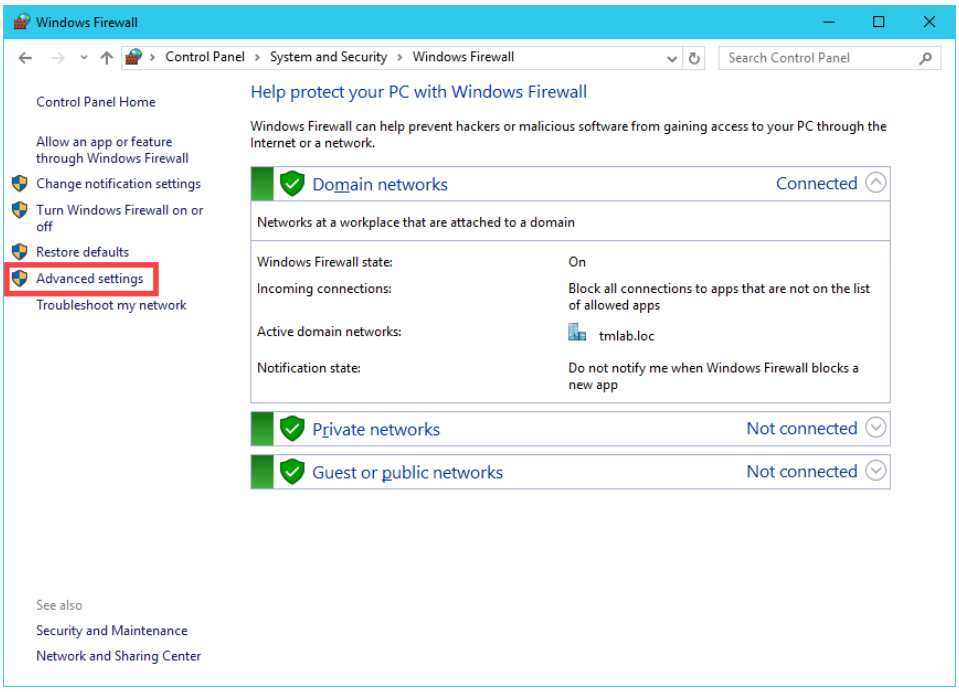


> If you had a physical thin client and attempted to reboot it at this point, it would still be able to boot but not from the ThinManager installed on **RDS1**, instead **RDS2** would respond to the PXE request and boot the terminal. Unfortunately, we are unable to demonstrate this in the Cloud as the DHCP request from the virtual thin client does not make it to **RDS2** due to networking restrictions.

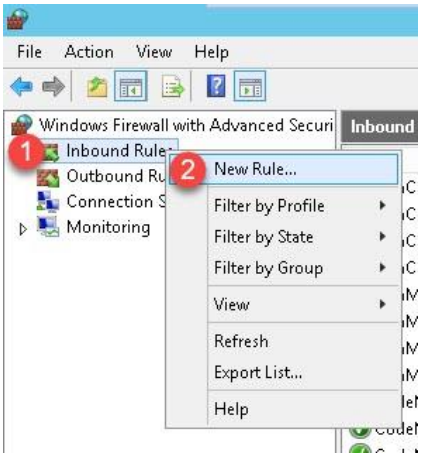
Configure Windows Firewall on RDS1

Now, let's configure the **Windows Firewall** on **RDS1** to permit the required traffic to restore our communication between ThinManager and the virtual thin client.

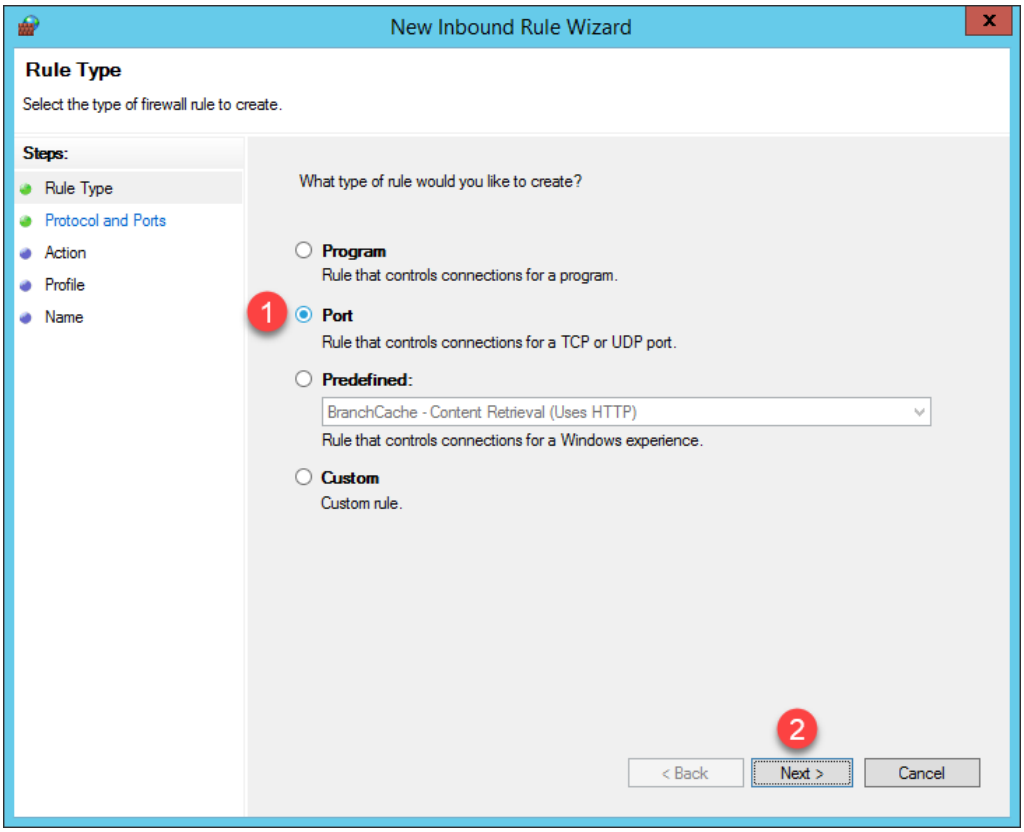
1. Return to the **Windows Firewall** page of the **Control Panel** on **RDS1** and click the **Advanced Settings** link.



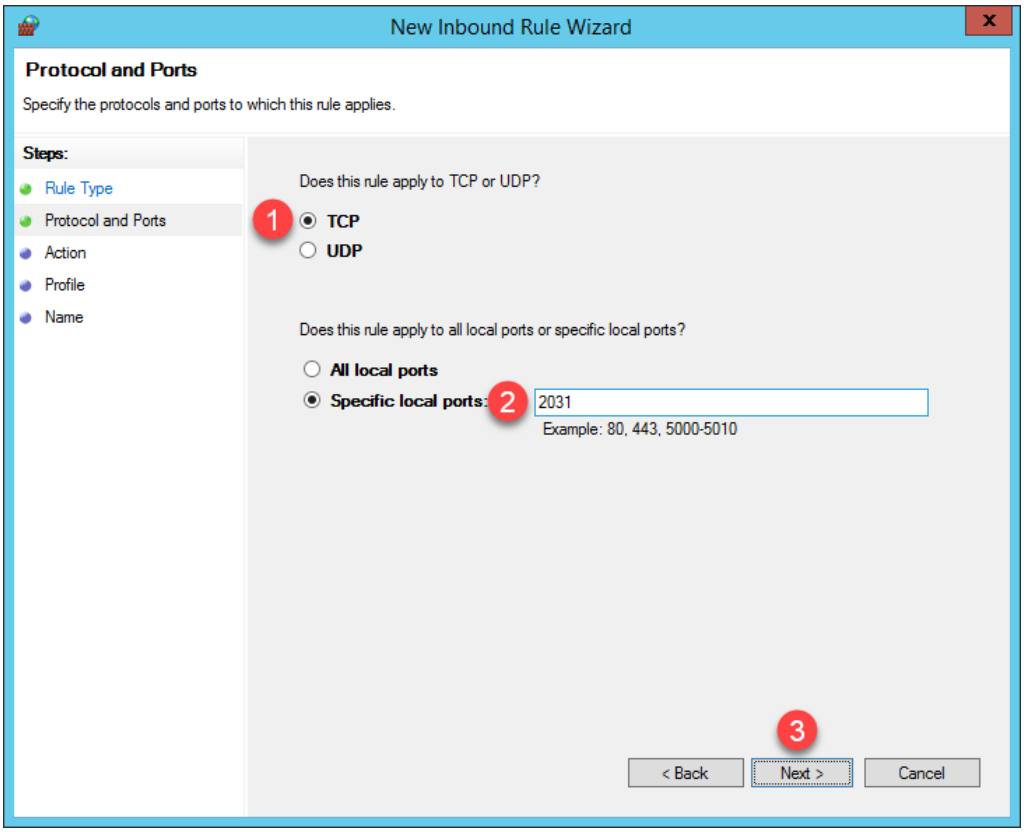
2. From the **Windows Firewall and Advanced Security** window, right click the **Inbound Rules** tree item and select **New Rule..**



3. From the **Rule Type** panel of the **New Inbound Rule Wizard**, select the **Port** radio button, followed by the **Next** button.

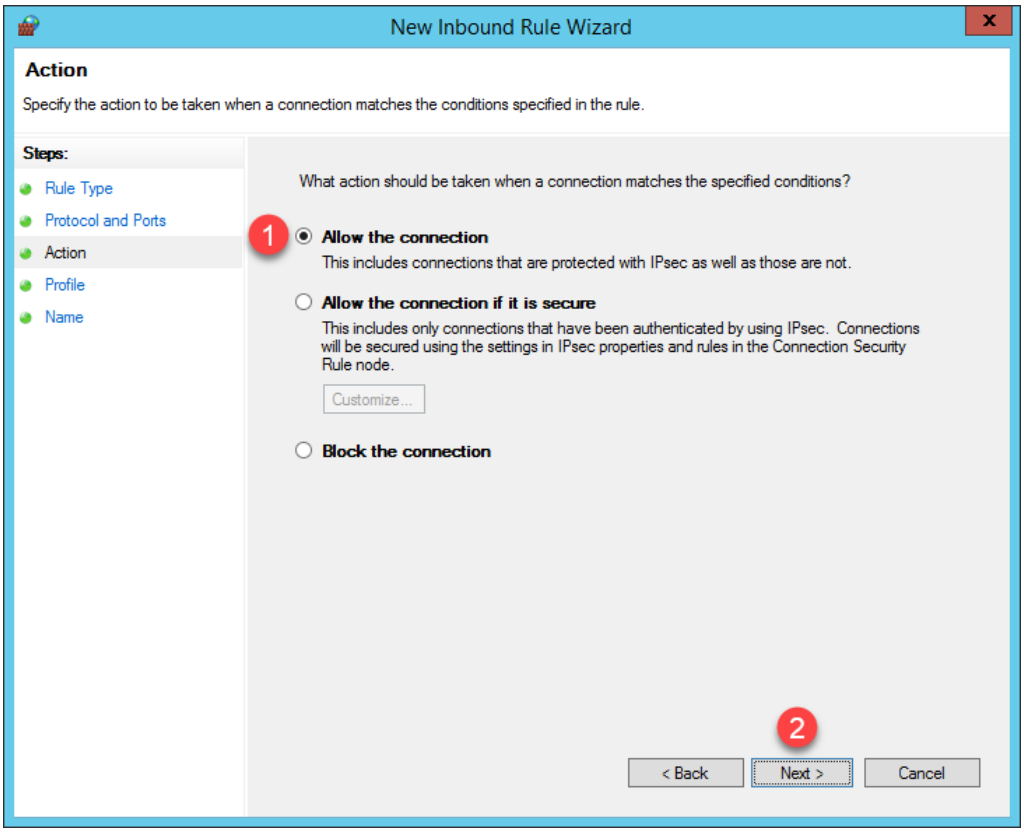


4. From the **Protocol and Ports** panel of the **New Inbound Rule Wizard**, select the **TCP** radio button and enter *2031* in the **Specified local ports** field. Click the **Next** button.

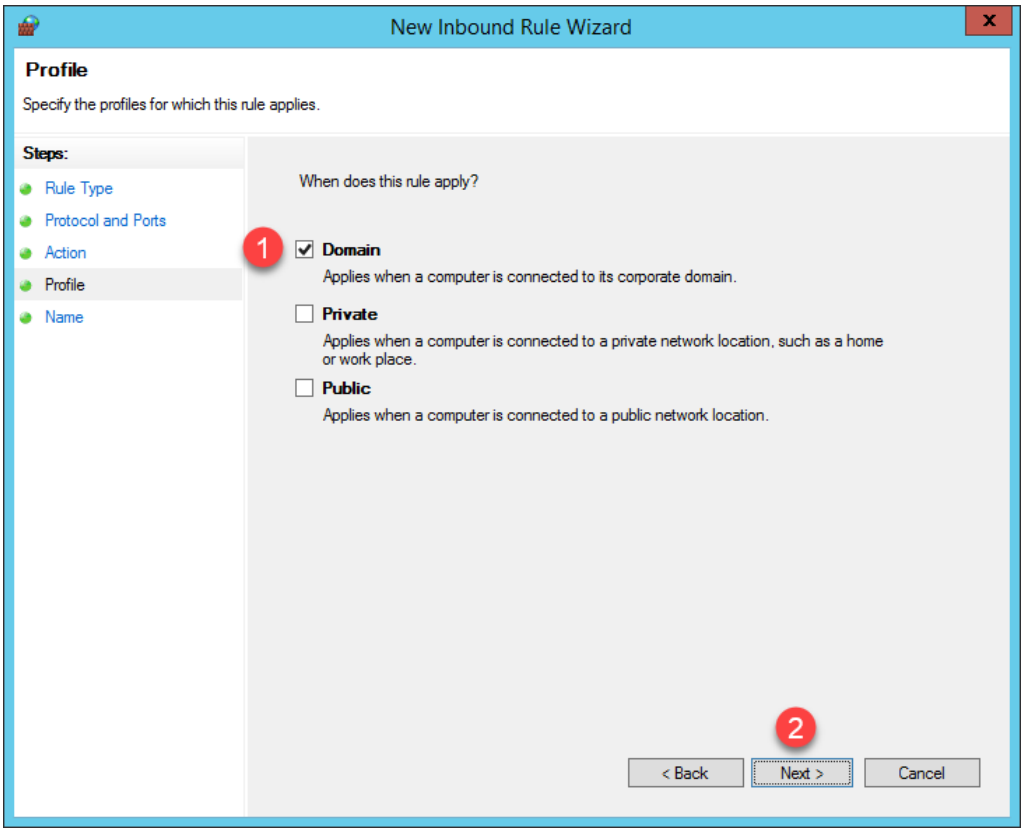


TCP Port 2031 is required by ThinManager for the Terminal Monitor Connection as well as for the delivery of the Terminal Profile to the terminal when it is booting up.

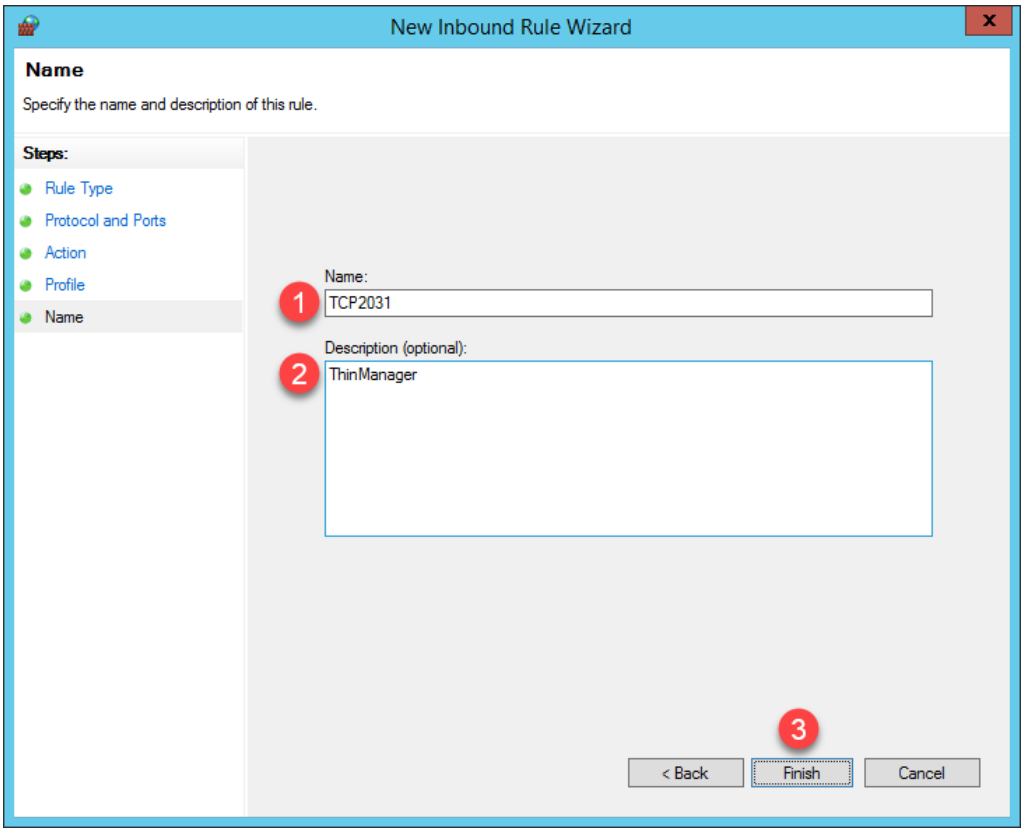
5. From the **Action** panel of the **New Inbound Rule Wizard**, select the **Allow the connection** radio button and click the **Next** button.



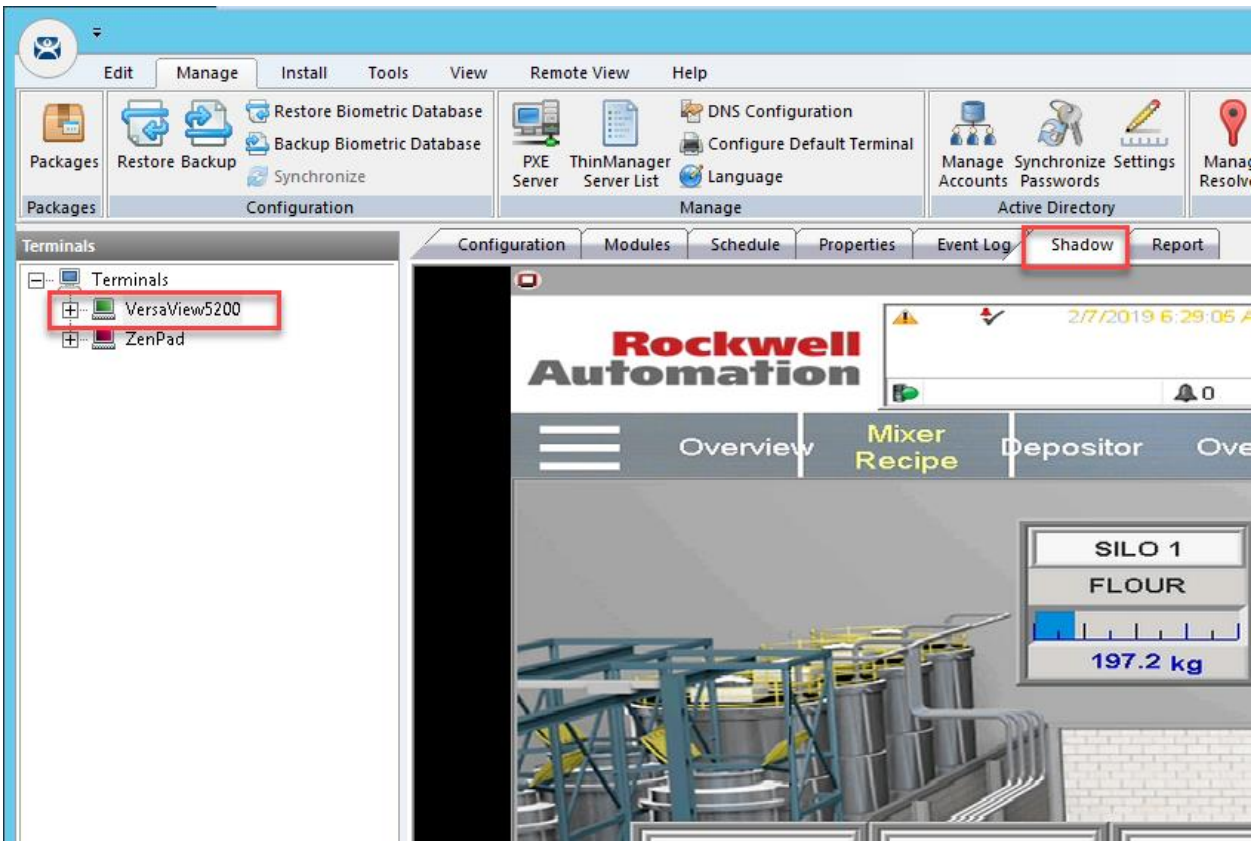
6. From the **Profile** panel of the **New Inbound Rule Wizard**, check the **Domain** checkbox and **un**-check the **Private** and **Public** checkboxes. Click the **Next** button.



7. From the **Name** panel of the **New Inbound Rule Wizard**, enter *TCP2031* as the **Name** and *ThinManager* as the **Description**. Click the **Finish** button.

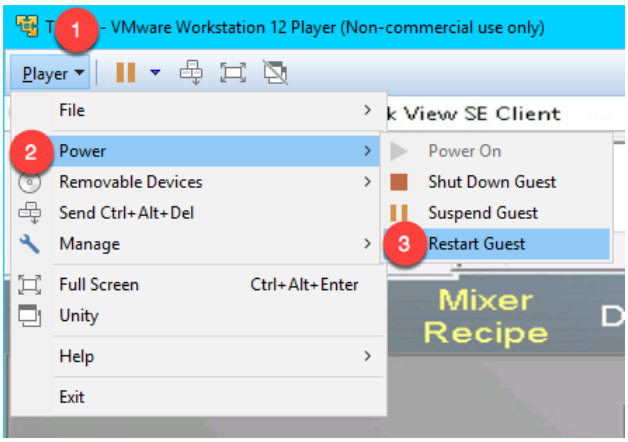


8. If you return to ThinManager, you should see the **Terminal Monitor Connection** is restored for **VersaView5200** since its icon has returned to **Green**. Terminal shadowing should be restored as well.

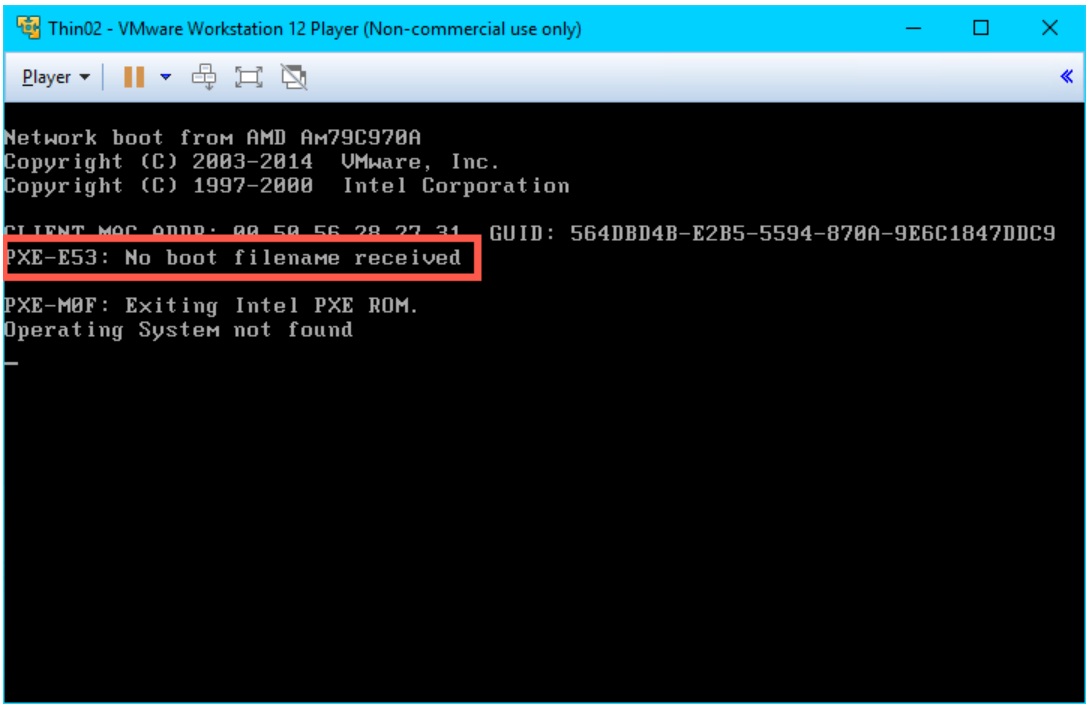


Terminal **shadowing** actually uses **TCP5900** for communication. This **outbound port** on **RDS1** was already enabled, but the **Terminal Monitor Connection** is first required before being able to establish a **shadow**.

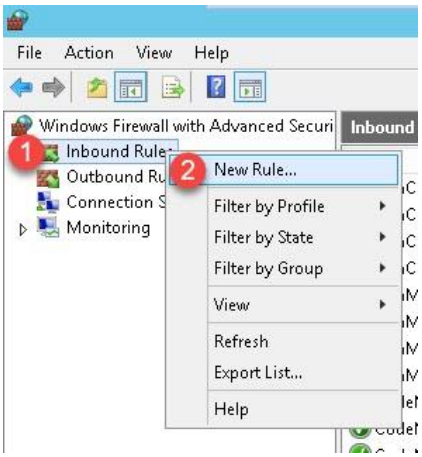
9. Switch to the virtual thin client so we can restart it and watch the boot process. Click the **Player** drop down, followed by the **Power** menu item then the **Restart Guest** item. Click the **Yes** button to the confirmation dialog box.



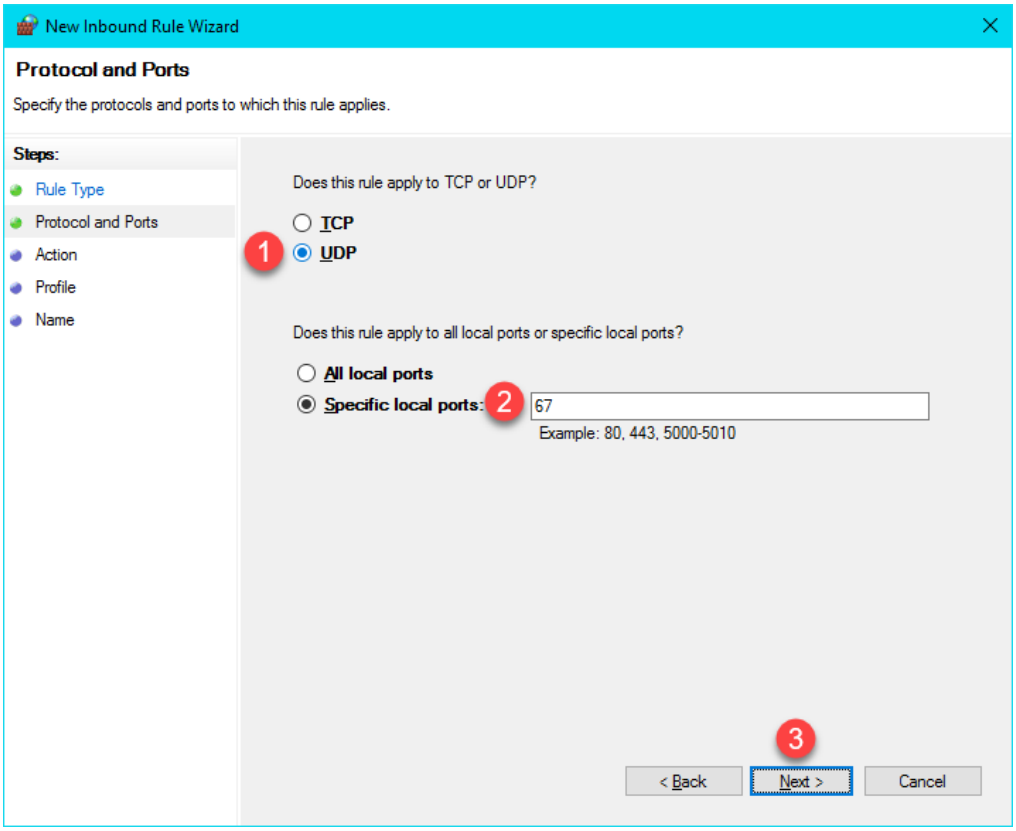
10. After a few seconds of attempting to acquire a **DHCP** address, the **PXE** boot process will timeout. Recall we configured **ThinManager** to use a Standard DHCP Server. Since **VMWare Player** is configured for **NAT**, it will issue the IP address. The error indicates that it probably received the IP address, but that is only 1 part of the **PXE** boot process – the virtual thin client also needs the boot server IP address(es) and the boot filename, which is supposed to be supplied by **ThinManager** in our current configuration. We will need to address this requirement in the Windows firewall.



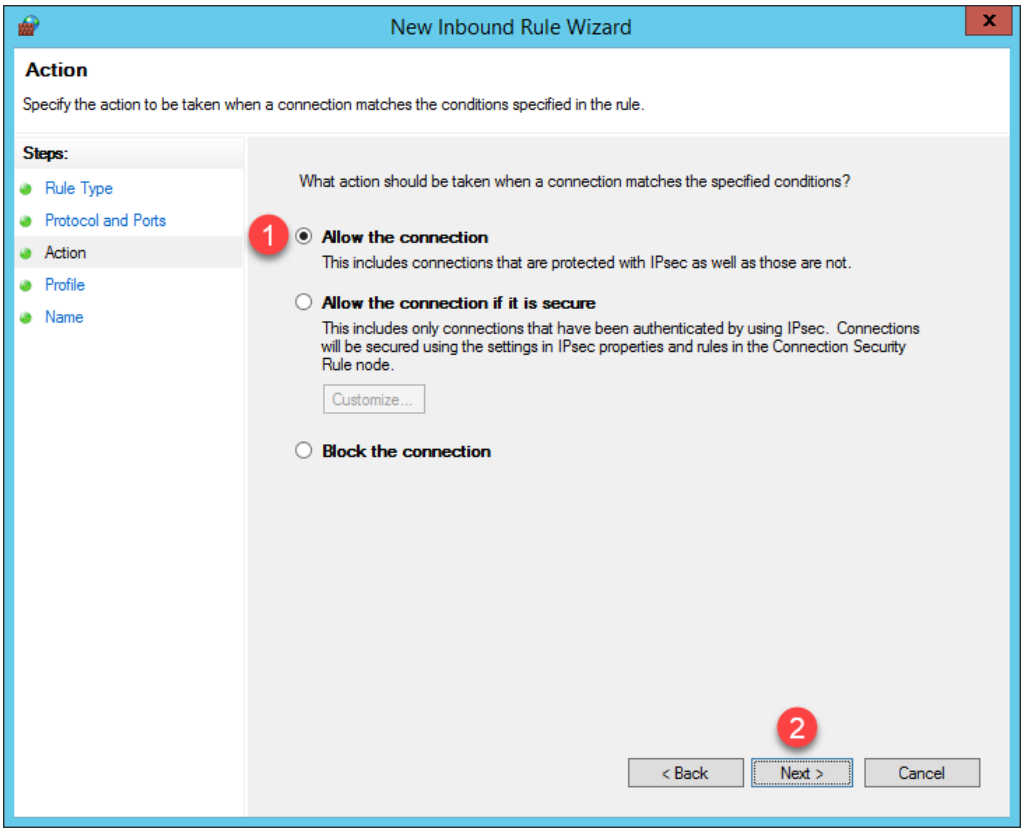
11. While we have addressed the **Terminal Monitor Connection** issue, the virtual thin client will still be unable to boot from **RDS1** with the current **Firewall** configuration. To address this, return to the **Windows Firewall and Advanced Security** window, right click the **Inbound Rules** tree item and select **New Rule..**



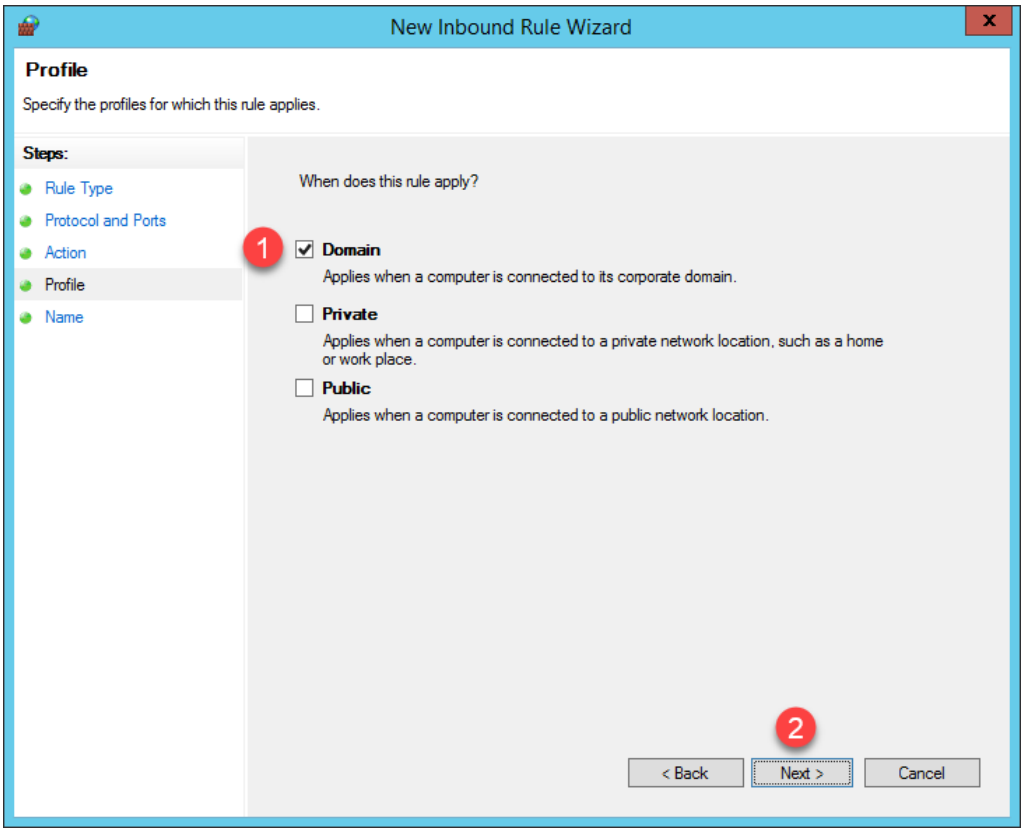
12. From the **Protocol and Ports** panel of the **New Inbound Rule Wizard**, select the **UDP** radio button and enter *67* in the **Specified local ports** field. Click the **Next** button.



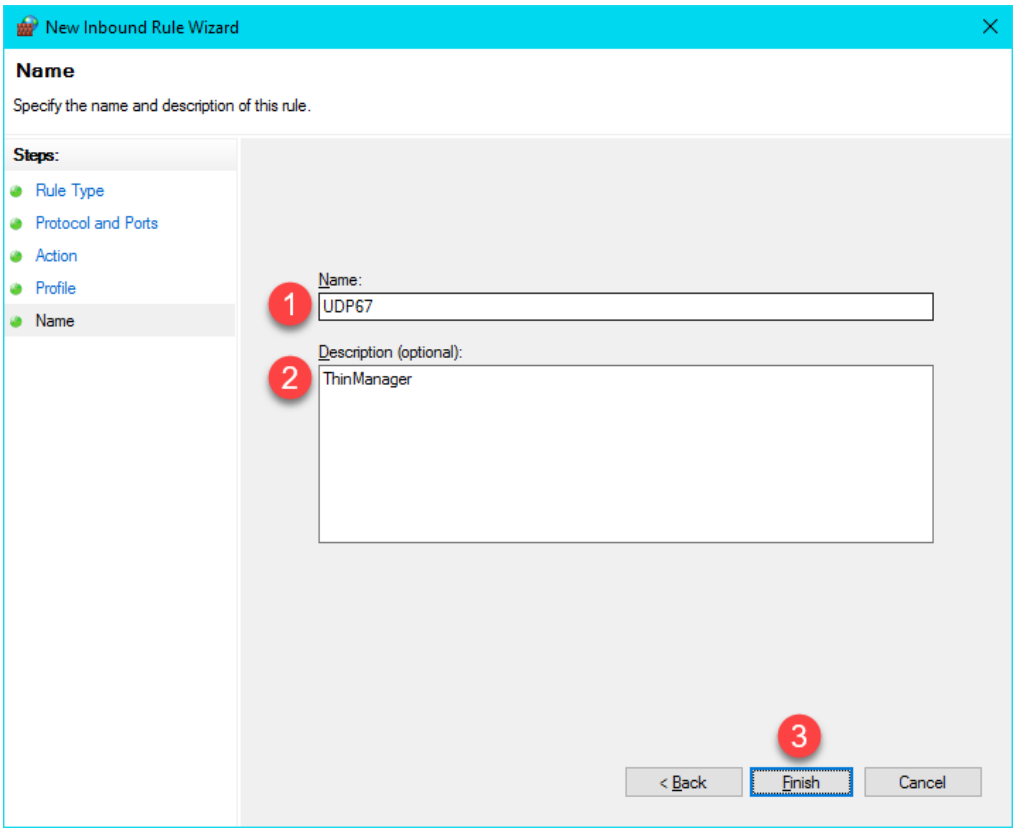
13. From the **Action** panel of the **New Inbound Rule Wizard**, select the **Allow the connection** radio button and click the **Next** button.



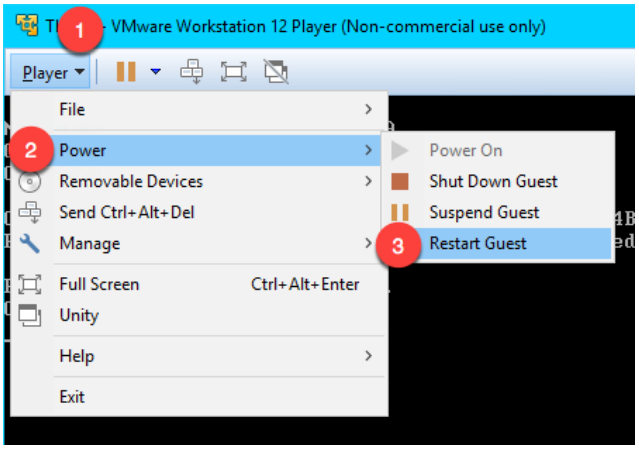
14. From the **Profile** panel of the **New Inbound Rule Wizard**, check the **Domain** checkbox and **un**-check the **Private** and **Public** checkboxes. Click the **Next** button.



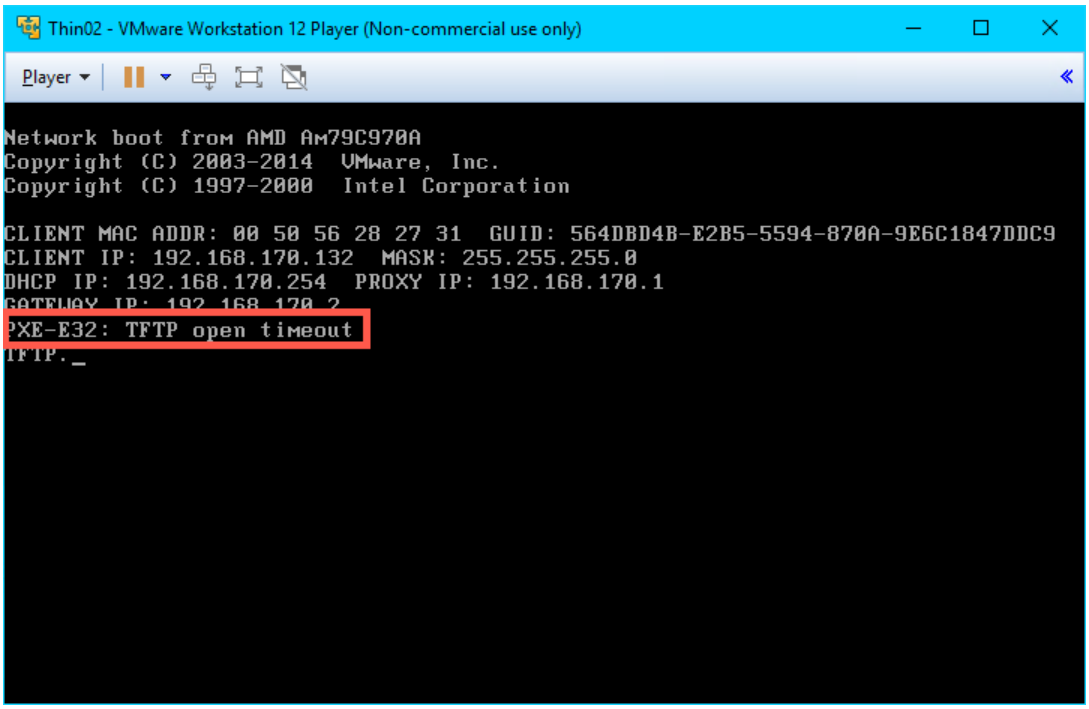
15. From the **Name** panel of the **New Inbound Rule Wizard**, enter *UDP67* as the **Name** and *ThinManager* as the **Description**. Click the **Finish** button. Leave the **Windows Firewall with Advanced Security** window open.



16. Let's see the result of this firewall change. Return to the virtual thin client, click the **Player** drop dropdown, followed by the **Power** menu item then the **Restart Guest** item. Click the **Yes** button on the confirmation dialog box.

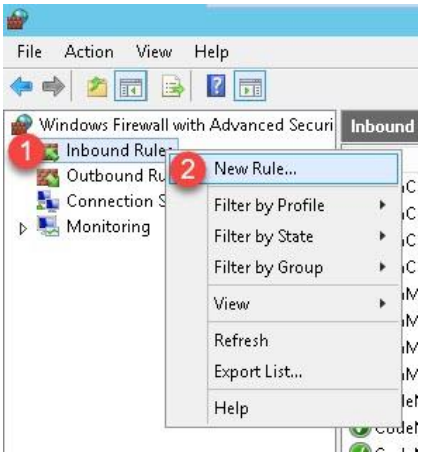


17. This time, the virtual thin client receives an IP address, but now it appears to timeout during the **TFTP** stage of the boot process. Once again, this is due to our firewall blocking this traffic.

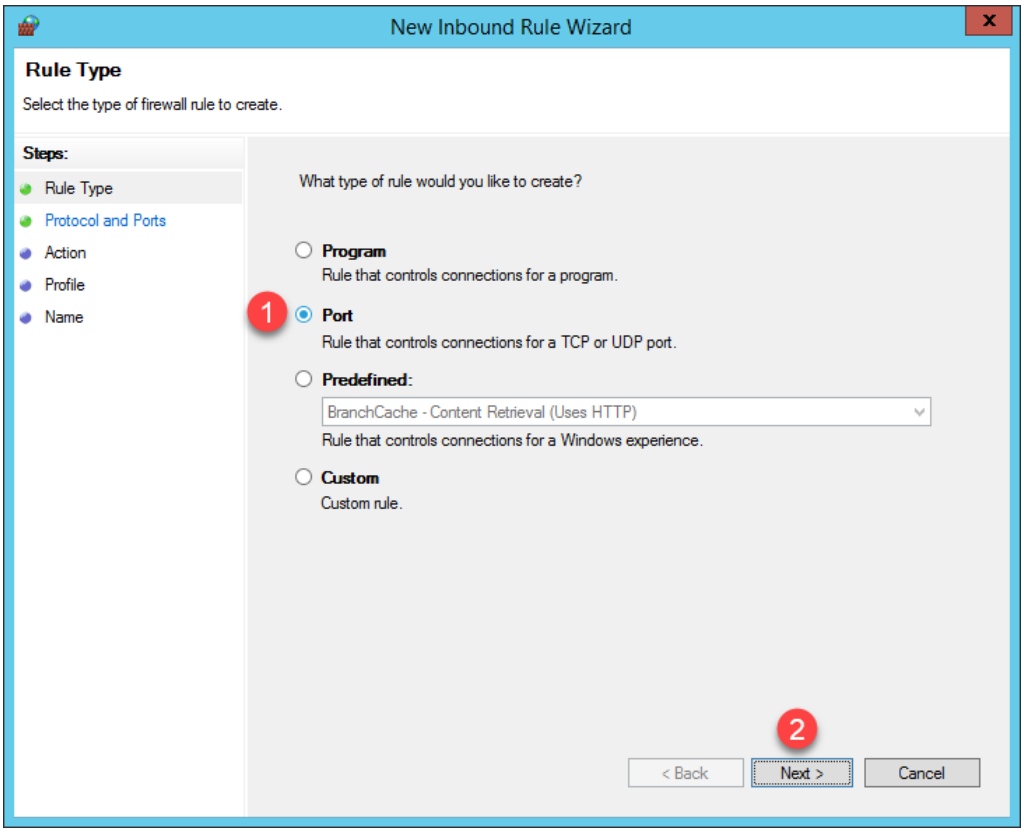


> Your IP addresses will most likely be different. The 192.168.x.y subnet is being issued by **VMWare Player** since the virtual thin client is configured for **NAT**.

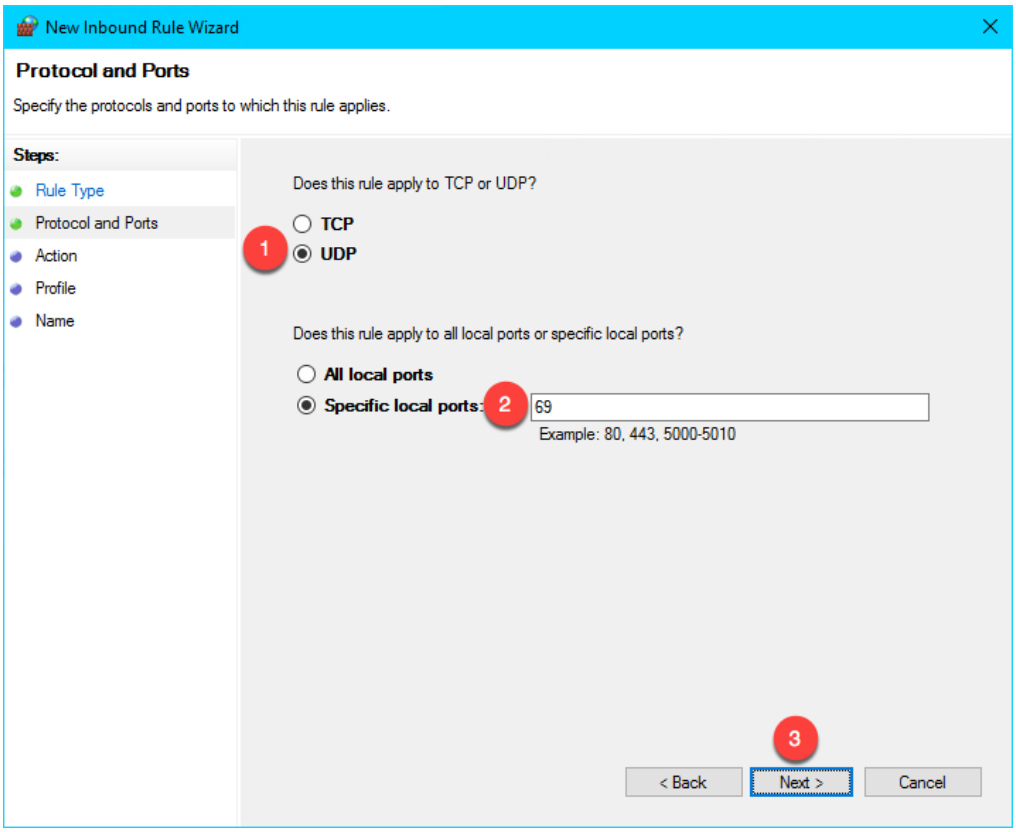
18. To address this, return to the **Windows Firewall and Advanced Security** window, right click the **Inbound Rules** tree item and select **New Rule..**



19. From the **Rule Type** panel of the **New Inbound Rule Wizard**, select the **Port** radio button, followed by the **Next** button.

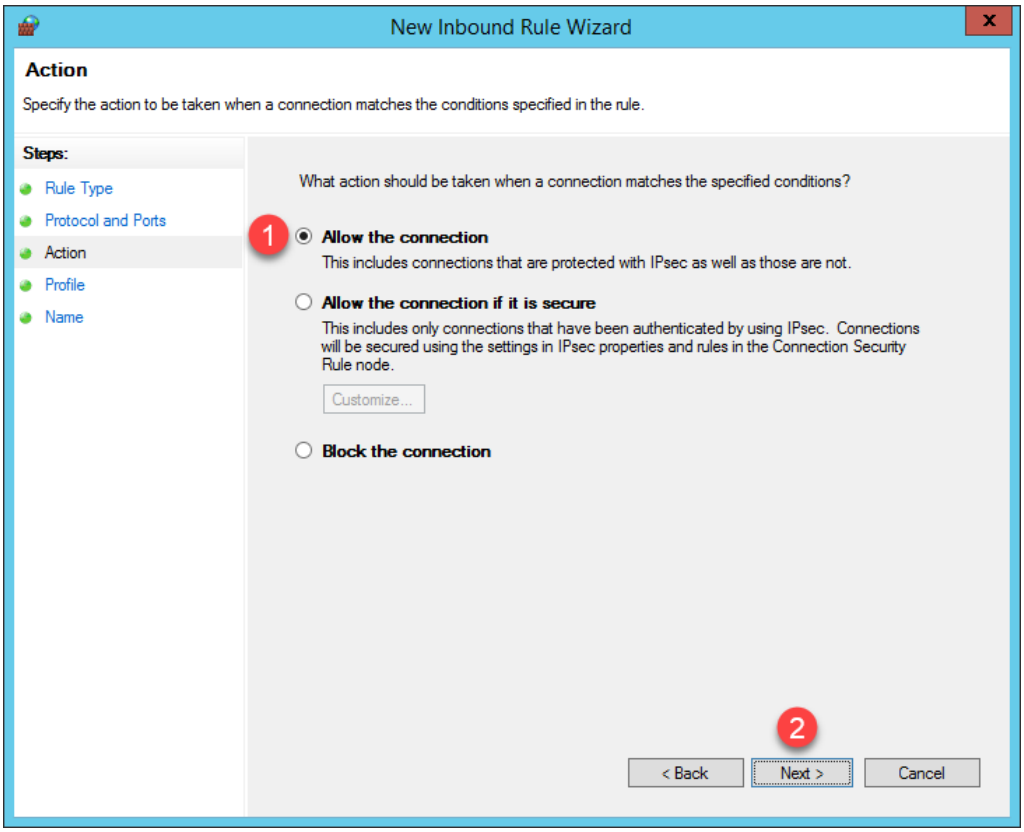


20. From the **Protocol and Ports** panel of the **New Inbound Rule Wizard**, select the **UDP** radio button and enter *69* in the **Specified local ports** field. Click the **Next** button.

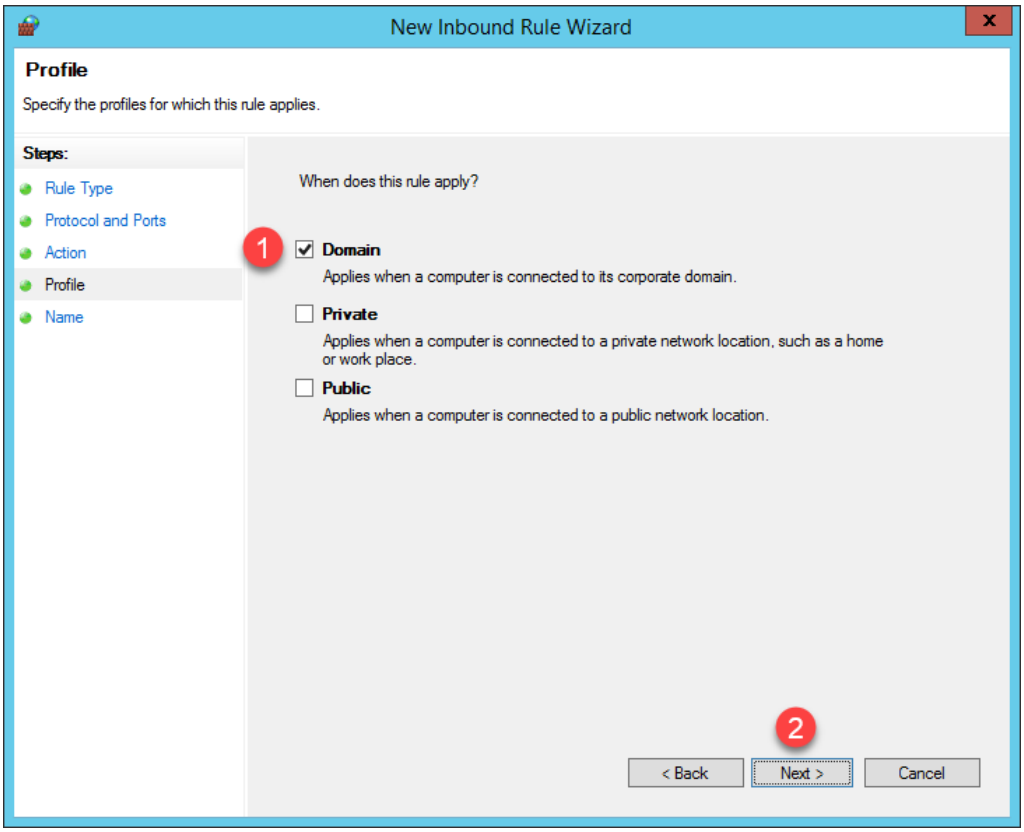


UDP Port 69 is required by ThinManager to transfer the **firmware** to **ThinManager Compatible** terminals (PXE), like the virtual thin client(s) in this Cloud lab. This transfer is accomplished using **Trivial File Transfer Protocol** (**TFTP**). **ThinManager Readey** terminals, which have the **ThinManager BIOS extension image** embedded in them by the vendor, also use **TFTP** but requires a different port. Namely, **UDP 69** for **TFTP** of the **firmware**.

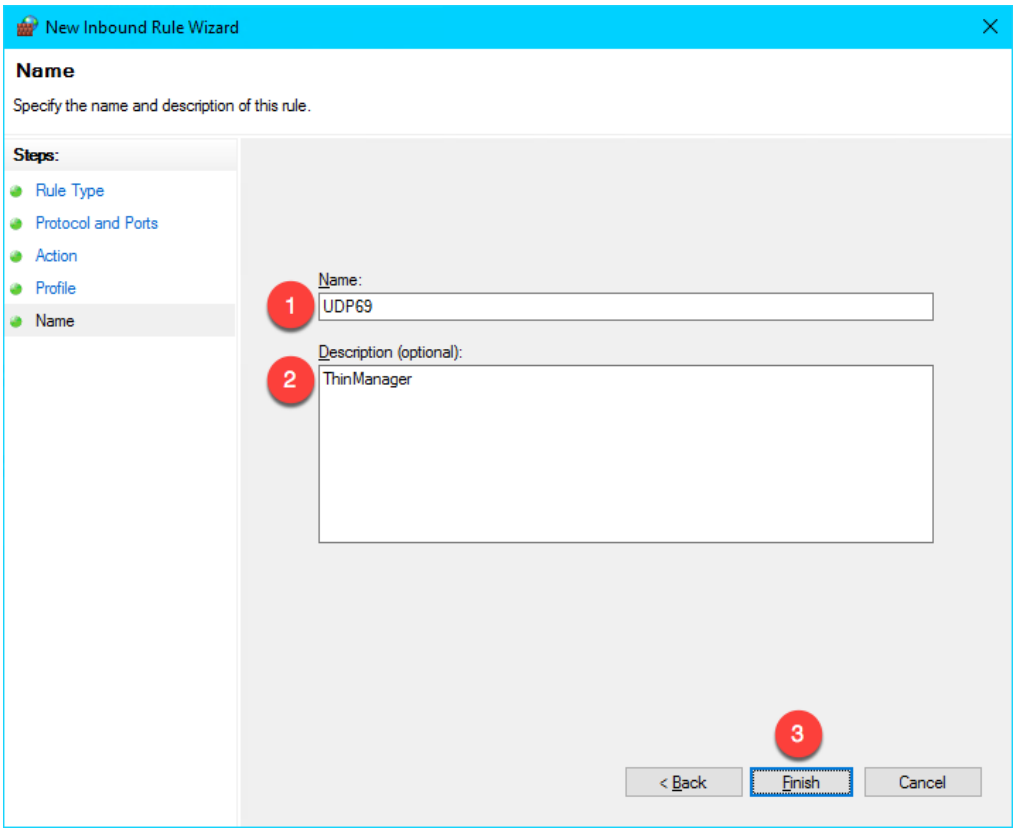
21. From the **Action** panel of the **New Inbound Rule Wizard**, select the **Allow the connection** radio button and click the **Next** button.



22. From the **Profile** panel of the **New Inbound Rule Wizard**, check the **Domain** checkbox and **un**-check the **Private** and **Public** checkboxes. Click the **Next** button.

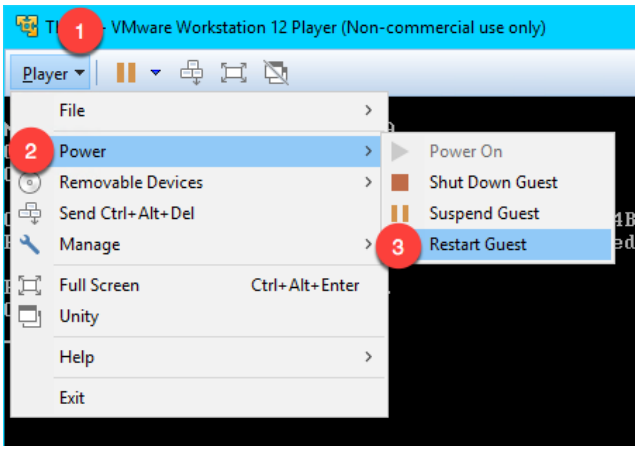


23. From the **Name** panel of the **New Inbound Rule Wizard**, enter *UDP69* as the **Name** and *ThinManager* as the **Description**. Click the **Finish** button.

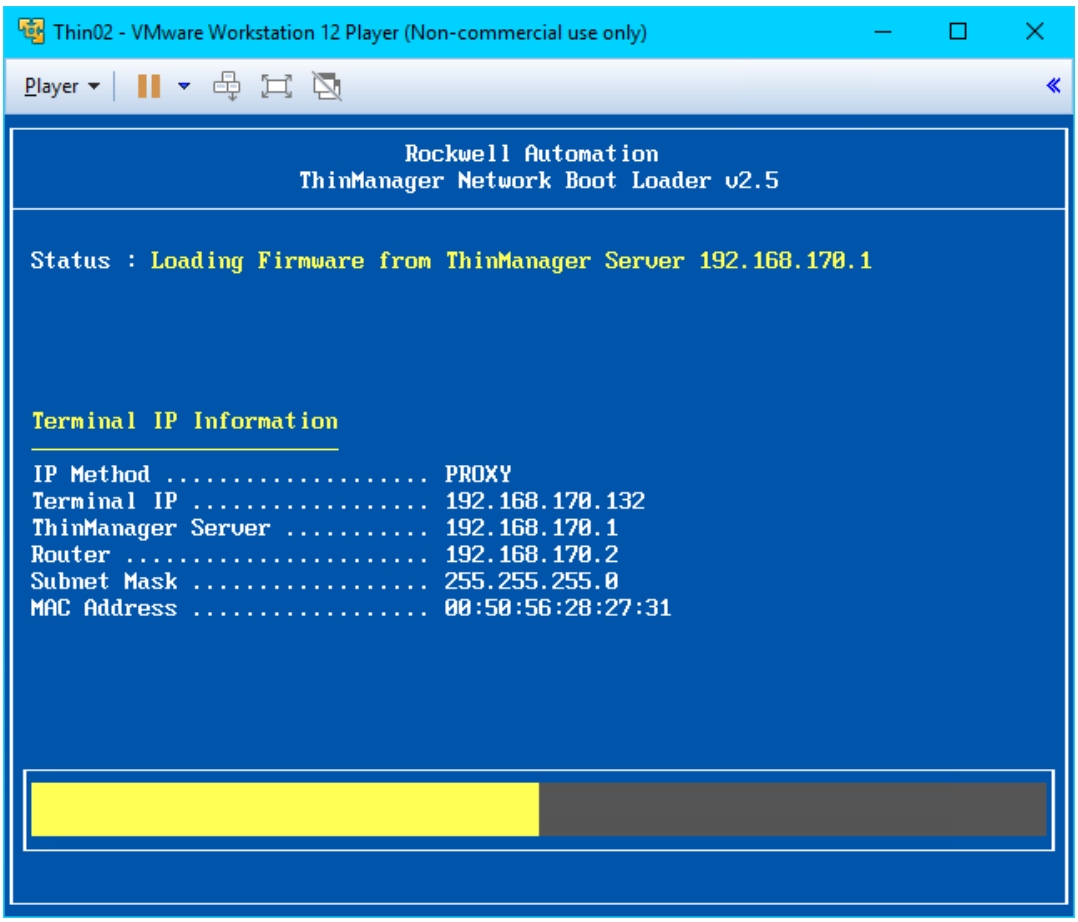


24. Close the **Windows Firewall with Advanced Security** window and the **Control Panel**.

25. Once again return to the virtual thin client, click the **Player** drop down, followed by the **Power** menu item then the **Restart Guest** item.



26. This time, the virtual thin client should complete the boot process.



In addition to the communication ports mentioned in the above steps, **TCP3389** is essential for the **Remote Desktop Protocol** traffic between the **RDS Servers** and the client devices. This port was pre-configured in the **Firewall Rules** when the **Remote Desktop Services** role was added in Section 1. Sometimes it is desired to change the default **RDP** port. This can be accomplished on the **RDS Server** side by modifying a registry entry at:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\TerminalServer\WinStations\RDP-Tcp\PortNumber

…and then on the Client side by adding the **RDP Port Module** to the ThinManager **Terminal Profile**. **ThinManager Modules** will be covered in Section 12.

Also keep in mind that you may have hardware-based firewalls to consider and configure accordingly.

One final word on **Firewalls**, ThinManager 9.0 introduced a **Firewall Compatible TFTP** option. Why is this important? As just mentioned, both **ThinManager Ready** and **ThinManager Compatible Terminals** use **TFTP** (Trivial File Transfer Protocol) to transfer the ThinManager **firmware** to thin/zero clients. The **TFTP** conversation starts at the client side on a specific port (UDP4900 for **ThinManager Ready** terminals, UDP69 for **ThinManager Compatible** terminals). By default, the **ThinManager Server** will respond on a random port per the **TFTP** specification. The random nature of this response can make **firewall** configuration (hardware and/or software) challenging. Most managed **firewalls** can be configured for **TFTP** and intelligently handle the opening and closing of random ports. If not, then a fairly broad range of ports must be opened, which is generally not desirable. By enabling the **Firewall Compatible TFTP** option, ThinManager will respond on the same port initiated by the client (UDP4900 for **ThinManager Ready** terminals, UDP69 for **ThinManager Compatible** terminals), making **firewall** configuration much simpler. This option is available from the **ThinManager Server Configuration Wizard** which is accessible by double clicking the **ThinManager Server** of interest from the **ThinManager Servers** tree.

STOP **Checkpoint Question:** https://thinmanager.com/cloudlabs/section11/

This completes the section **ThinManager Redundancy and Firewall Configuration**. Please continue on to learn more about **Modules**.

Section 12: Modules

Overview

The concept of **modules** was introduced earlier in the lab. **Firmware Packages** were introduced as part of the product as a way to **package** the **firmware** and its associated **modules** in a single unit. A **module** is essentially like a driver that provides additional capability to the **Terminal**. There are **modules** for touchscreen controllers, badge readers and redundant Ethernet, just to name a few. **Modules** will be explored in more detail in this section by experimenting with some of the ones that can be demonstrated in a Cloud environment. Unfortunately, the more common Modules like the USB Touch Screen Driver, Redundant Ethernet Module are not demonstrable in this format.

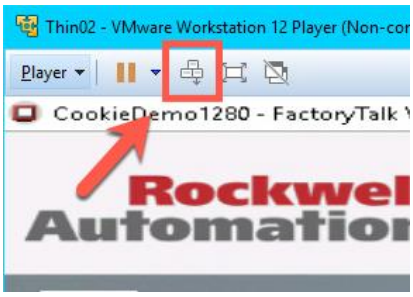
In this section, you will be performing the following tasks:

1. Key Block Module
2. Locate Pointer Module
3. MultiSession Screen Saver Module

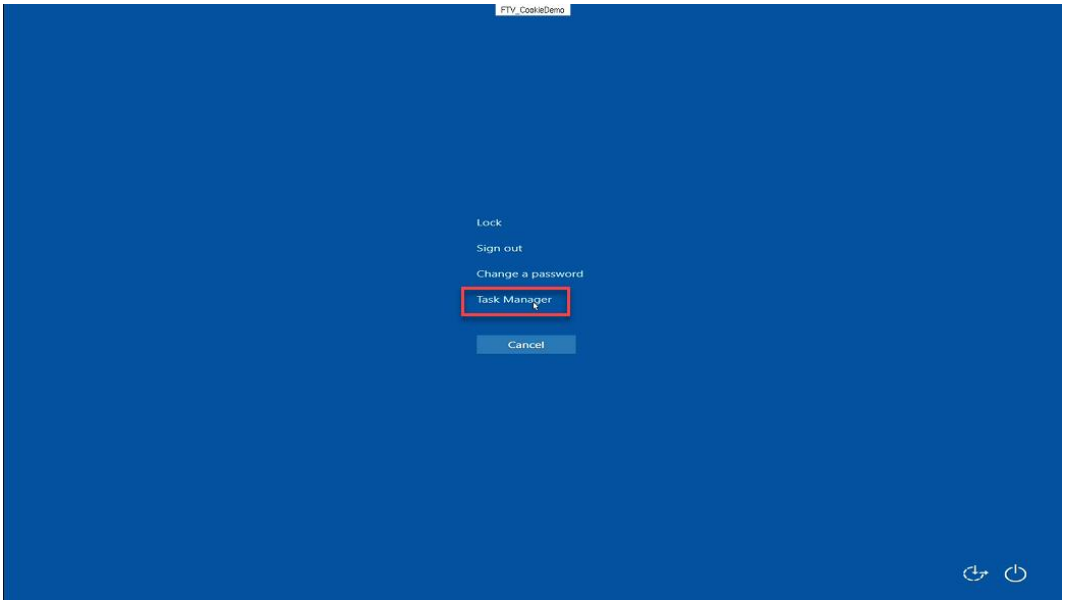
Key Block Module

Let's explore some of the more commonly used ThinManager **Modules**.

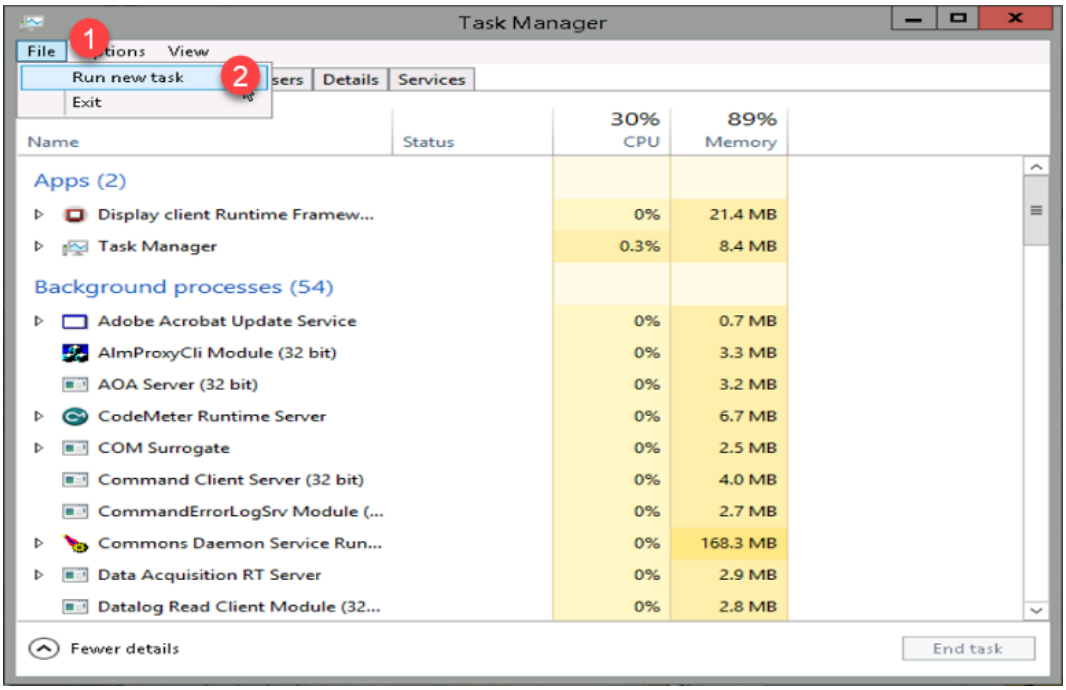
1. From the virtual thin client hit the **CTRL-ALT-DEL** icon in the toolbar to send that key sequence to the virtual thin client.



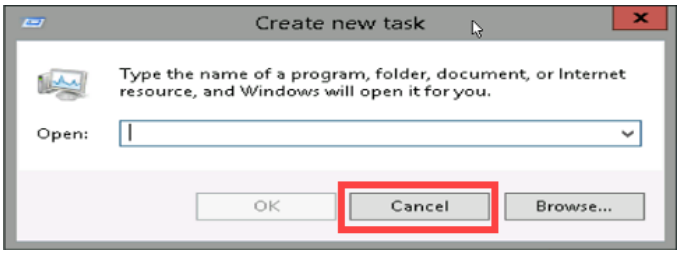
2. Notice this results in the ability to **Lock**, **Sign out**, **Change a password** or even access **Task Manager**! Click the **Task Manager** link.



3. From the **Task Manager** window, click the **More details** button at the bottom left, then select the **File** menu item, followed by the **Run new task** item.

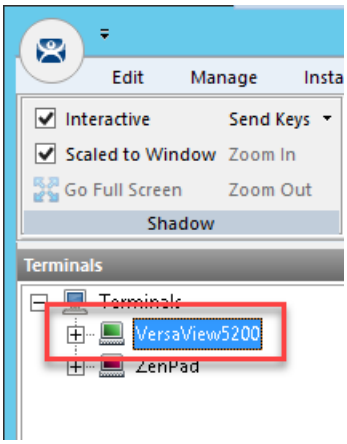


4. At this point, we have effectively defeated the intent of using **Application Link** (eliminating access to other elements within the **Windows Desktop**) in ThinManager, as the user could launch any application they wish – on the **Remote Desktop Server** no less! Click the **Cancel** button and close **Task Manager** on the virtual thin client.



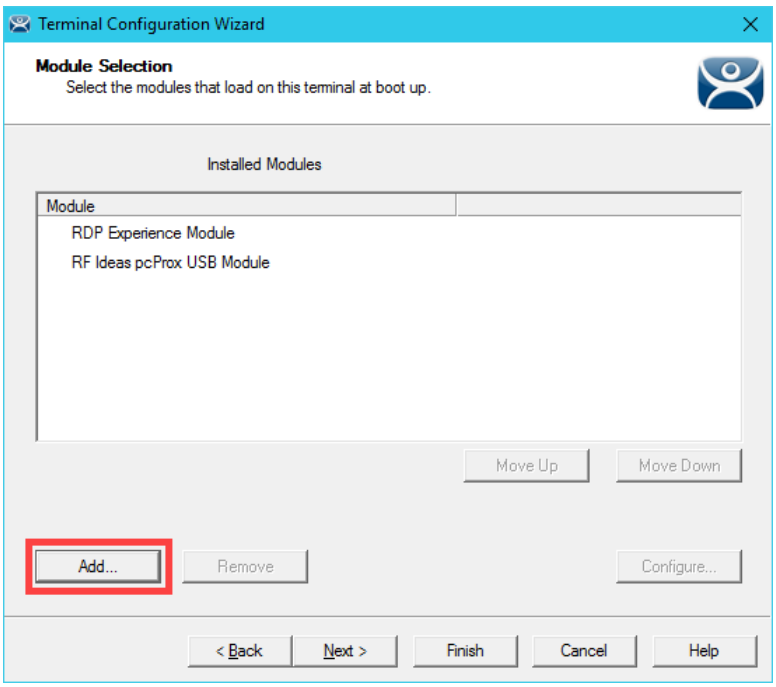
5. Return to the **ThinManager Admin Console**. Click the **Terminals** tree selector icon.

6. This problem is easily rectified using the **Key Block Module** in ThinManager. Double click the **VersaView5200** terminal.

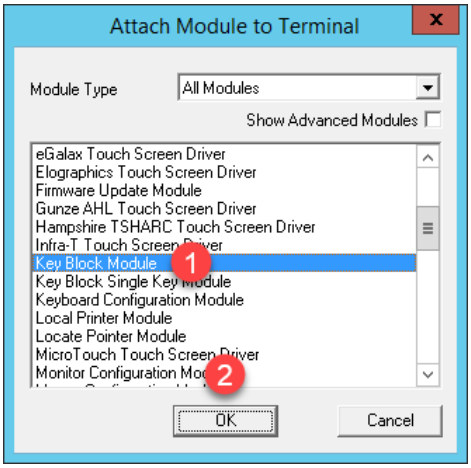


7. Click the **Next** button on the **Terminal Name** page of the wizard.
8. Click the **Next** button on the **Terminal Hardware** page of the wizard.
9. Click the **Next** button on the **Terminal Options** page of the wizard.
10. Click the **Next** button on the **Terminal Mode Selection** page of the wizard.
11. Click the **Next** button on the **Display Client Selection** page of the wizard.
12. Click the **Next** button on the **Terminal Interface Options** page of the wizard.
13. Click the **Next** button on the **Hotkey Configuration** page of the wizard.
14. Click the **Next** button on the **Log In Information** page of the wizard.
15. Click the **Next** button on the **Video Resolution** page of the wizard.

16. Click the **Add…** button on the **Module Selection** page of the wizard.

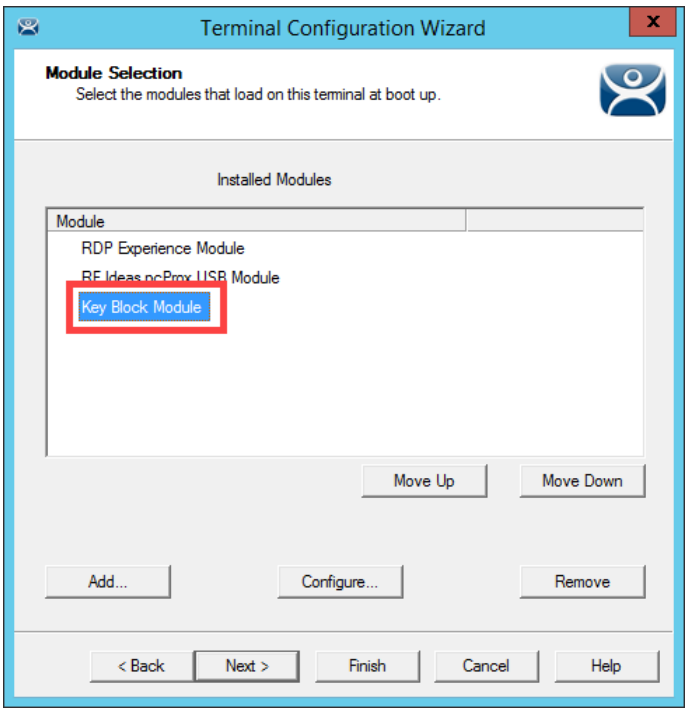


17. Scroll down and select the **Key Block Module**. Click the **OK** button.

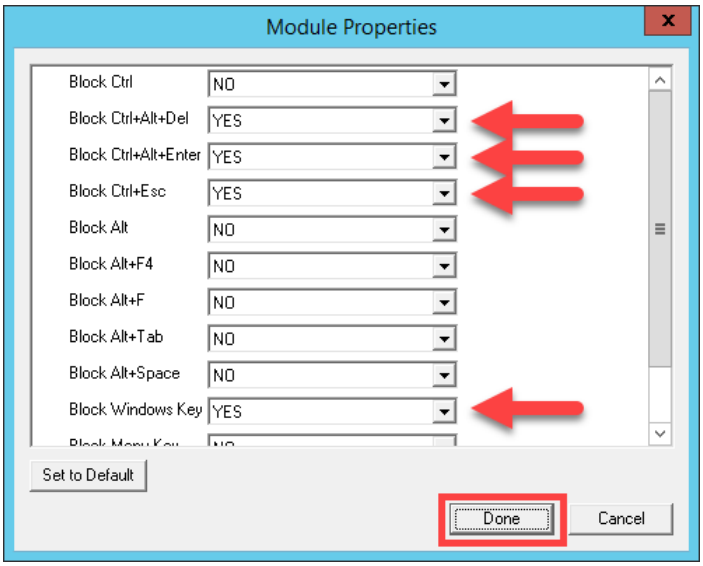


> You may notice the **Key Block Single Key Module** and the **Keyboard Configuration Module** as well. The **Key Block Single Key Module** allows you to block specific keys, like CTRL-B, or any other combination, like ALT-S. The **Keyboard Configuration Module** provides the ability to set the initial state of the **Num Lock**, **Caps Lock**, etc., **Repeat Delay** and **Rate** as well as **Keyboard Layout** options.

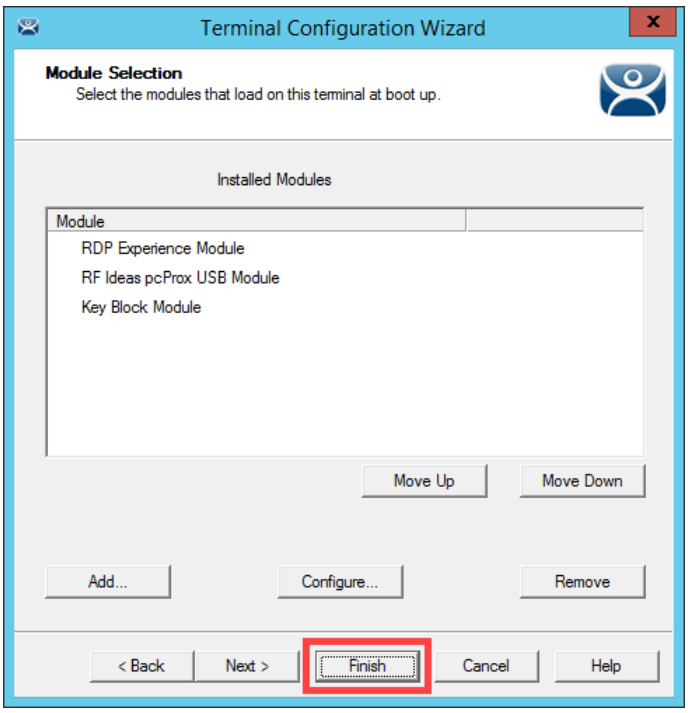
18. Double click the **Key Block Module** item in the **Installed Modules** list to configure it.



19. Notice the default **Block** settings. Accept the defaults and click the **Done** button.

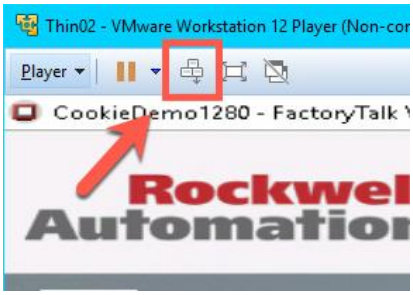


20. Click the **Finish** button.



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

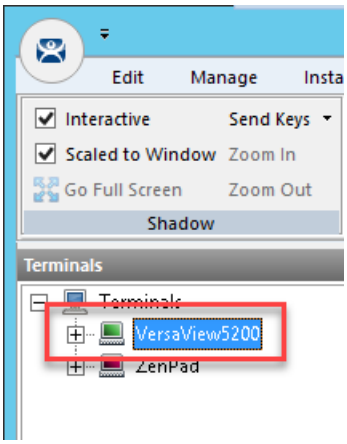
22. Return to the virtual thin client and click the **CTRL-ALT-DEL** icon from the toolbar again to verify it is now blocked.



Locate Pointer Module

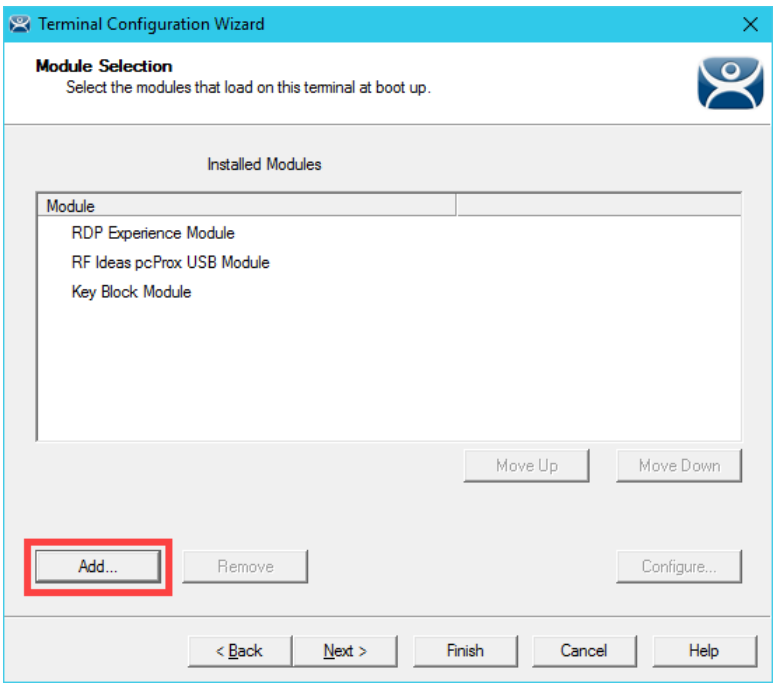
The Locate Pointer Module is very useful on high resolution screens and/or with MultiMonitor deployments.

1. Double click the **VersaView5200** terminal.

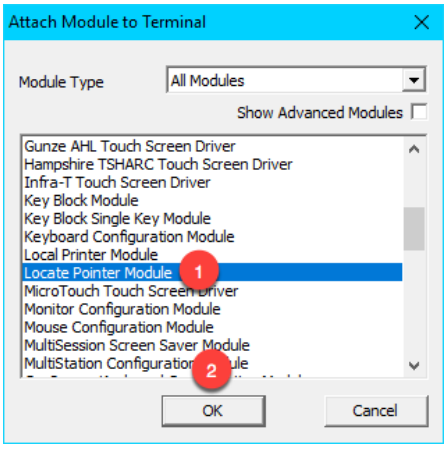


2. Click the **Next** button on the **Terminal Name** page of the wizard.
3. Click the **Next** button on the **Terminal Hardware** page of the wizard.
4. Click the **Next** button on the **Terminal Options** page of the wizard.
5. Click the **Next** button on the **Terminal Mode Selection** page of 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 on the **Log In Information** page of the wizard.
10. Click the **Next** button on the **Video Resolution** page of the wizard.

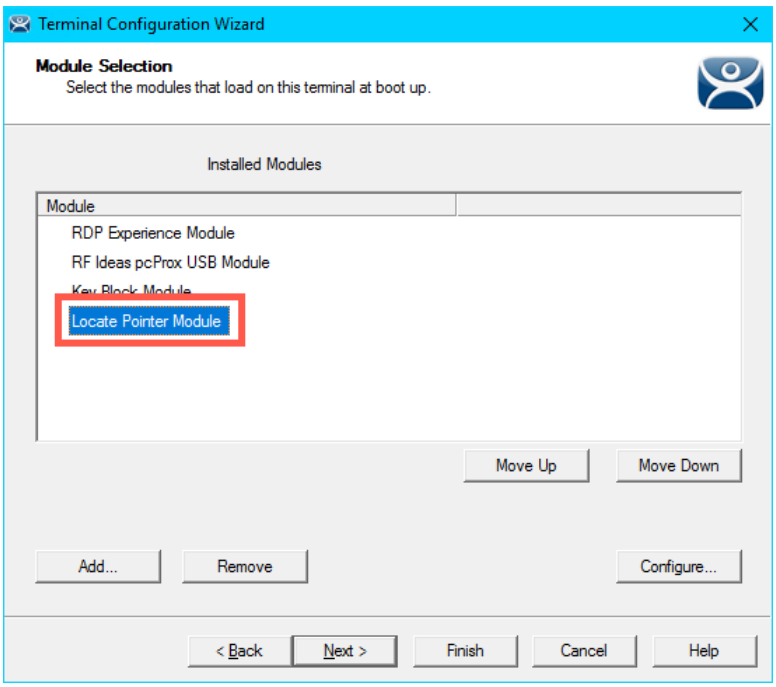
11. Click the **Add…** button on the **Module Selection** page of the wizard.



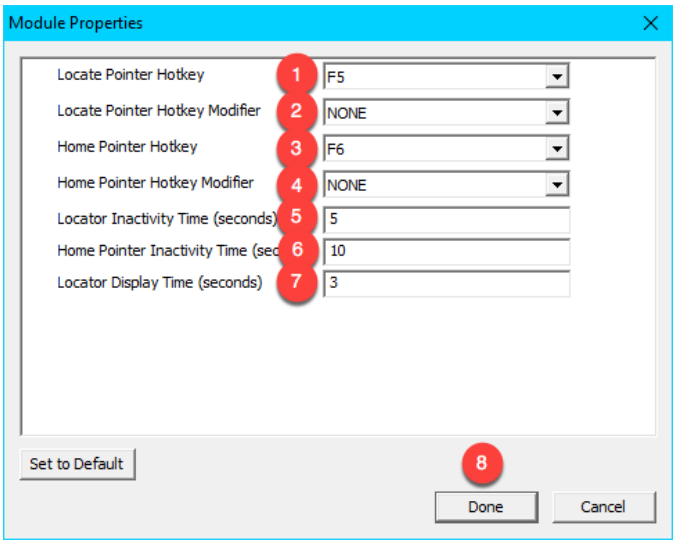
12. Scroll down and select the **Locate Pointer Module**. Click the **OK** button.



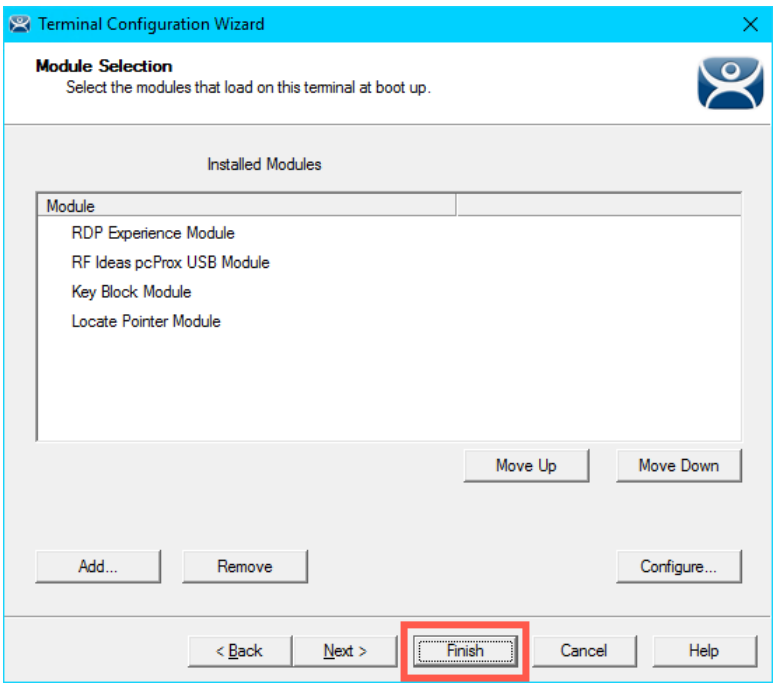
13. Back at the **Module Selection** page of the wizard, double click the **Locate Pointer Module**.



14. From the **Module Properties** page of the wizard, match the settings in the screen shot below and click the **Done** button.

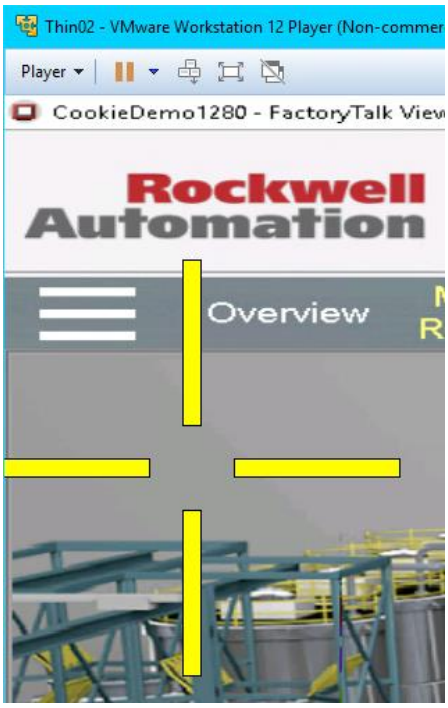


15. From the **Module Selection** page of the wizard, click the **Finish** button.



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

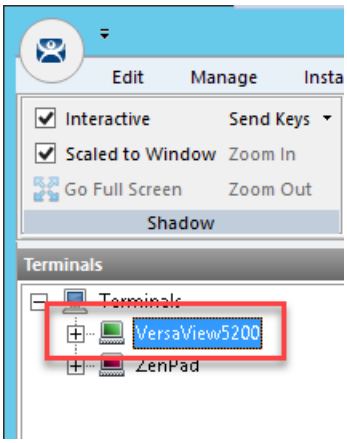
17. Return to the virtual thin client, click in an open area of the screen to ensure the focus is there, then hit the *F5* key on your keyboard. You should see a large crosshair indicating the location of your pointer. If you quickly hit the *F6* key, the pointer locator will move to the center of the screen.



MultiSession Screen Saver Module

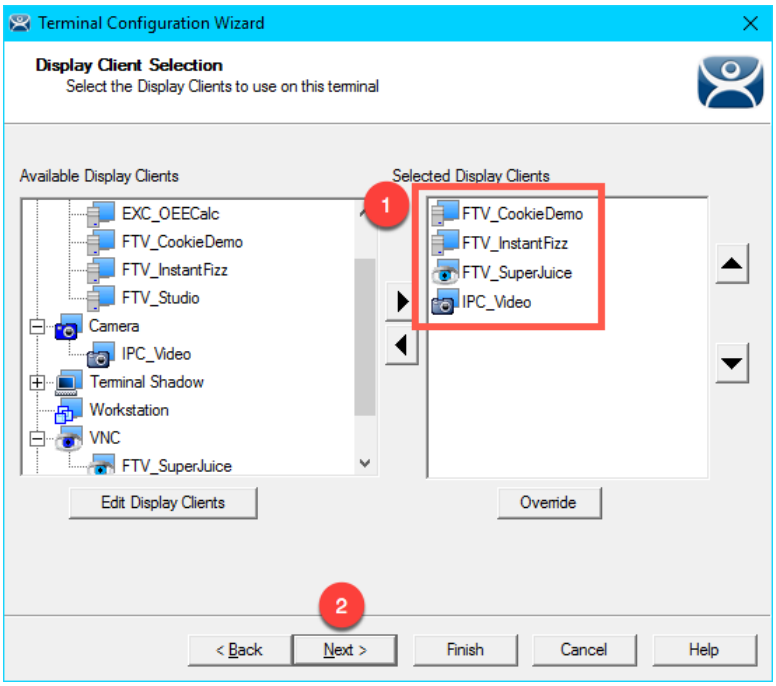
If you recall from Section 7 , **MultiSession** is the term used to define when we deliver more than one **Display Client** to a **Terminal**. We used **Tiling Mode** and **Virtual Screens** to demonstrate the **Visualization** options for **MultiSession**. The **MultiSession Screen Saver Module** operates like a **Screen Saver** in that it can be configured to be triggered after a specific amount of inactivity at the terminal. It can be set to cycle through the **MultiSession Display Clients** on a configurable interval, or it can be set to return to the main **MultiSession Display Client**.

1. Double click the **VersaView5200** terminal.



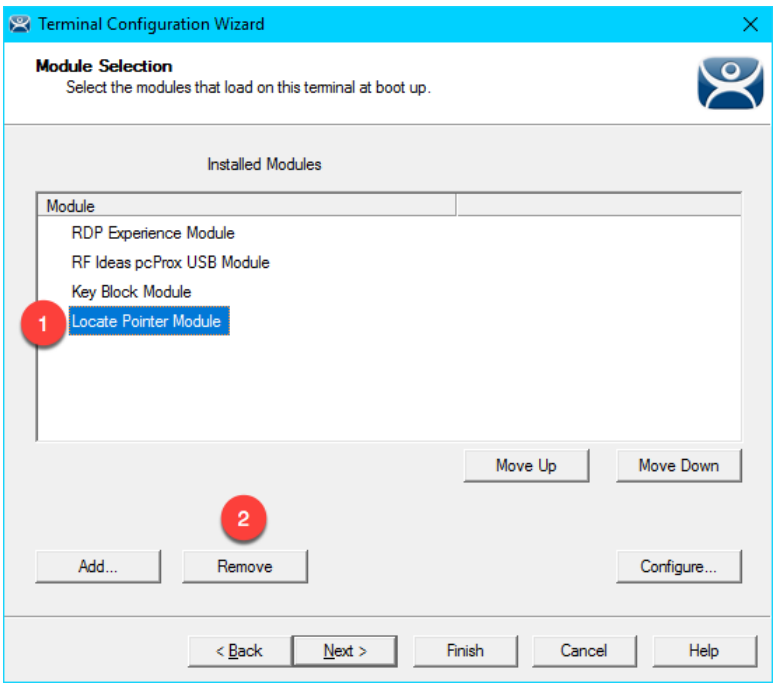
2. Click the **Next** button on the **Terminal Name** page of the wizard.
3. Click the **Next** button on the **Terminal Hardware** page of the wizard.
4. Click the **Next** button on the **Terminal Options** page of the wizard.
5. Click the **Next** button on the **Terminal Mode Selection** page of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

6. From the **Display Client Selection** page of the wizard, make sure you have the **FTV_CookieDemo**, **FTV_InstantFizz**, **FTV_SuperJuice** and **IPC_Video Display Clients** added to the **Selected Display Clients** listbox. Click the **Next** button.

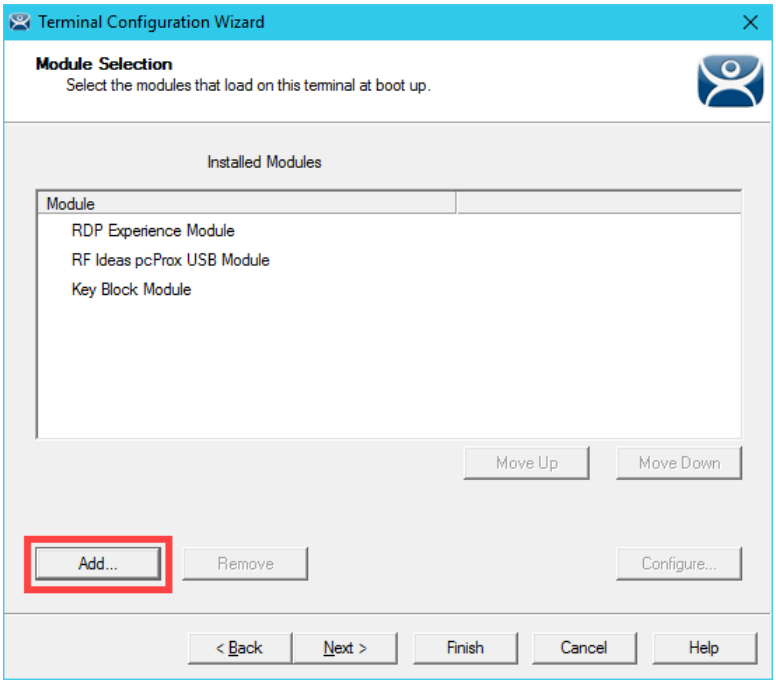


7. Click the **Next** button on the **Terminal Interface Options** page of the wizard.
8. Click the **Next** button on the **Hotkey Configuration** page of the wizard.
9. Click the **Next** button on the **Log In Information** page of the wizard.
10. Click the **Next** button on the **Video Resolution** page of the wizard.

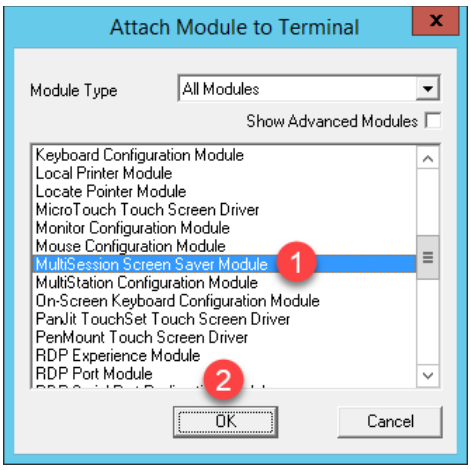
11. Let's remove the **Locate Pointer Module** by selecting it and then clicking the **Remove** button.



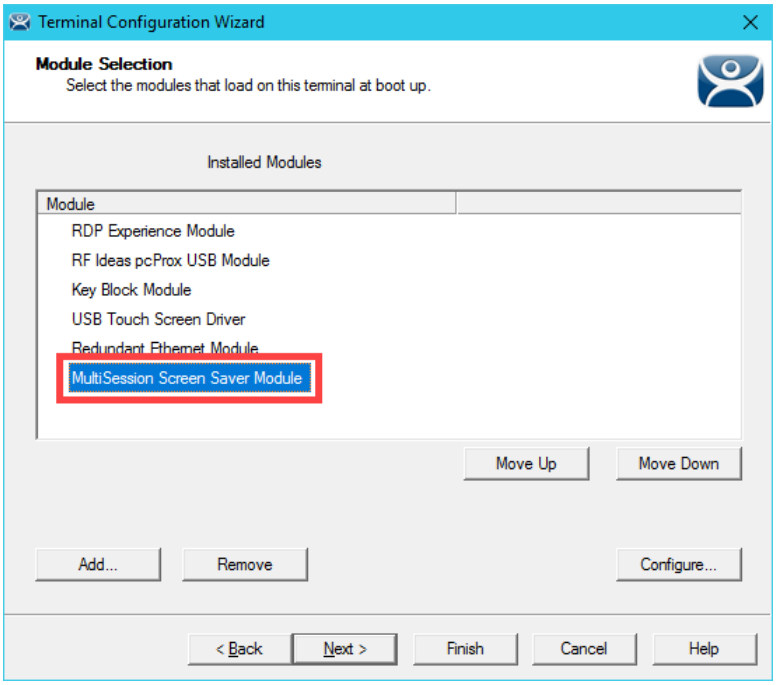
12. Click the **Add…** button on the **Module Selection** page of the wizard.



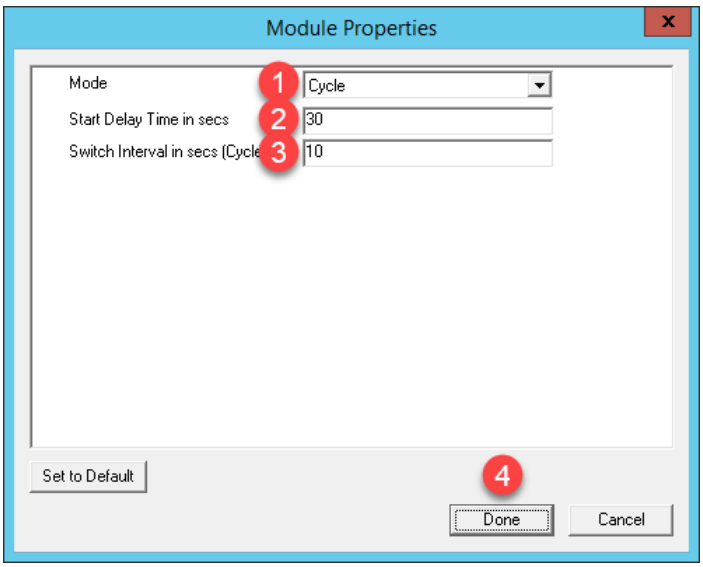
13. From the **Attach Module to Terminal** window, select the **MultiSession Screen Saver Module** and click the **OK** button.



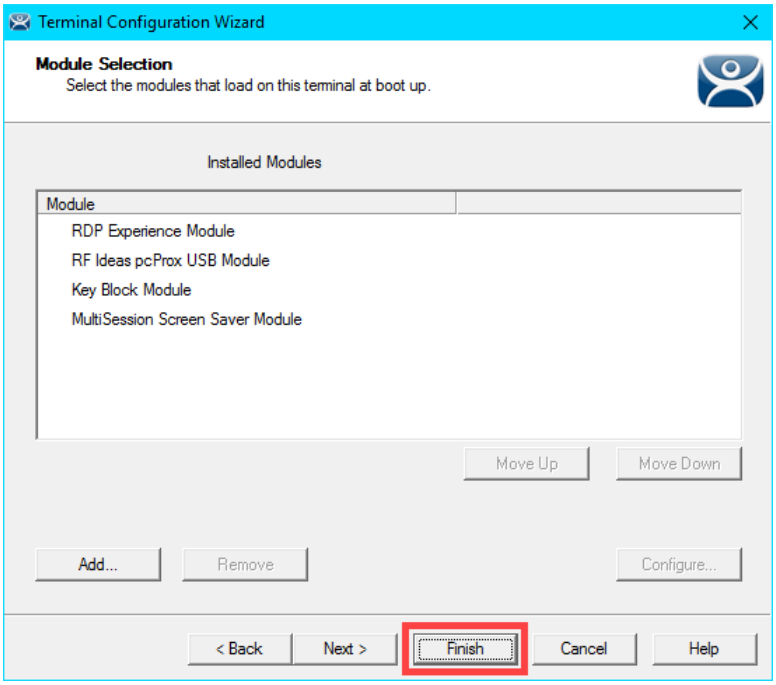
14. Double click the **MultiSession Screen Saver Module** from the **Installed Modules** list.



15. Keep the **Mode** set to **Cycle**, enter *30* in the **Start Delay Time in secs** field, enter *10* in the **Switch Interval in secs (Cycle)** field, and click the **Done** button.



16. Click the **Finish** button.



17. Right click the **VersaView5200** terminal and select the **Restart Terminal** item. Click the **Yes** button to confirm.
18. Once **VersaView5200** reboots, do not interact with the virtual thin client for approximately 30 seconds. The **MultiSession Screen Saver Module** should trigger and begin cycling through the **Display Clients** every 10 seconds.

> Another commonly used module is the **Custom Video Mode Module**. If you have connected a display to your ThinManager-managed terminal and it appears to boot properly, but the end result is a blank screen that can still be shadowed from the **Admin Console**, try applying the **Custom Video Mode Module** with default settings to your terminal's configuration, and reboot your terminal. This module will change the default video timings used by the ThinManager firmware.

Checkpoint Question: https://thinmanager.com/cloudlabs/section12/

This completes the **Modules** section. Please continue on to the **Terminal Groups, Overrides, Schedules and Mouse Button Mapping** section or jump to any of the remaining sections.

Section 13: Terminal Groups, Overrides, Schedules and Mouse Button Mapping

Overview

This section is a bit of a catch-all for some under-utilized, but very effective and powerful features of ThinManager.

In this section, you will be performing the following tasks:

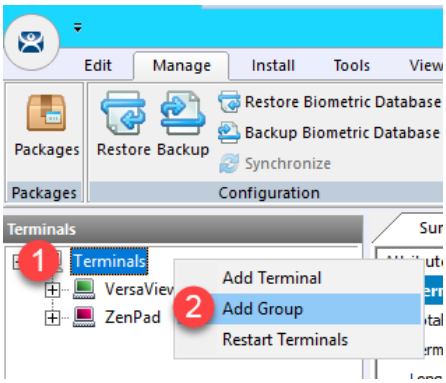
1. Terminal Groups
2. Overrides
3. Schedules
4. Mouse Button Mapping
5. Remove Override and Mouse Button Mapping

Terminal Groups

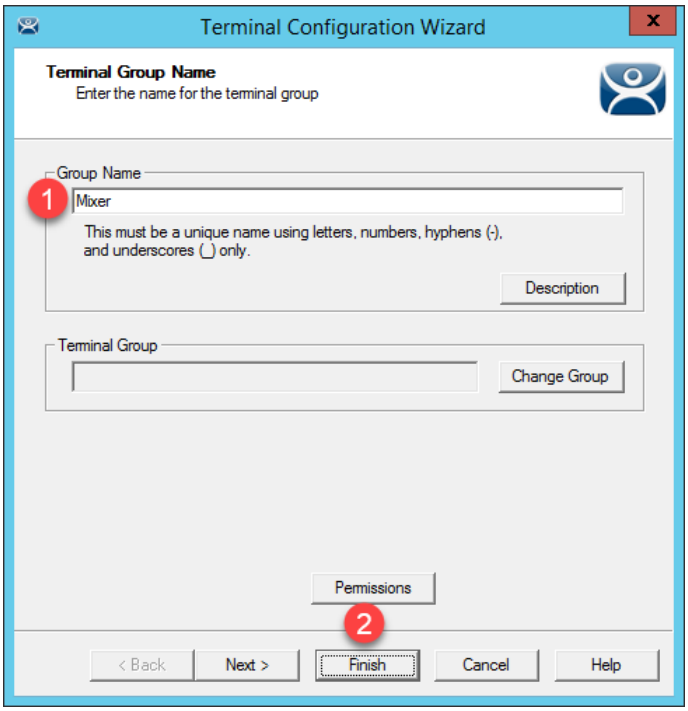
Terminal Groups provide 2 key capabilities: (1) terminal organization and (2) settings inheritance. With terminal organization, you can create **Terminal Groups** much like folders in Windows Explorer, and then add **Terminals** to the **Terminal Group**. The other key benefit of **Terminal Groups** is that you can assign **Terminal** settings 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.

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

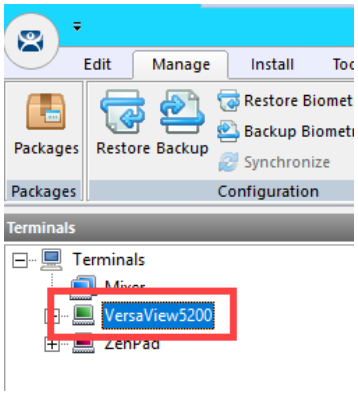
2. Right click the **Terminals** root item in the **Terminals tree** and select **Add Group**.



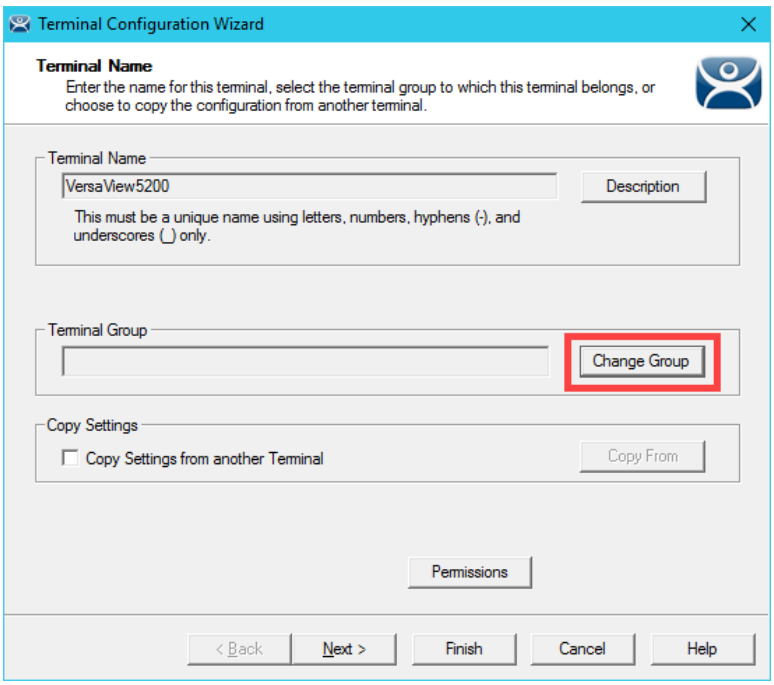
3. From the **Terminal Group Name** of the **Terminal Configuration Wizard**, enter *Mixer* as the **Group Name**. Click the **Finish** button.



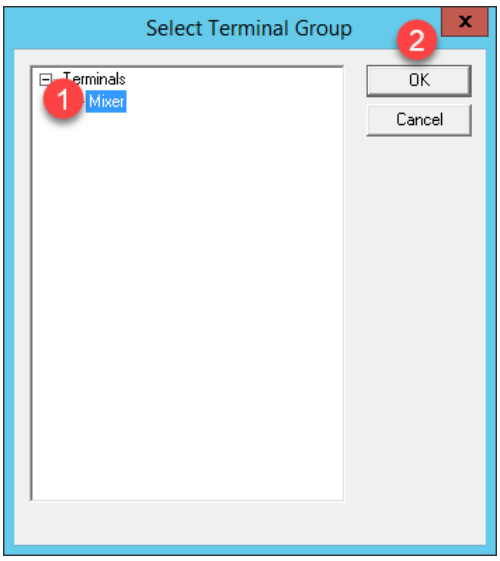
4. Double click the **VersaView5200** terminal.



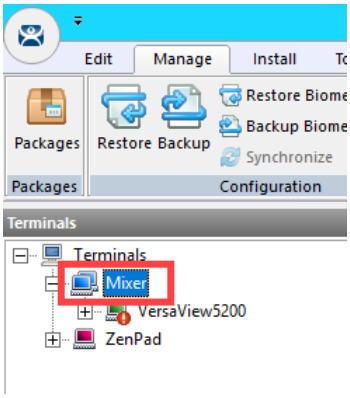
5. From the **Terminal Name** page of the **Terminal Configuration Wizard**, click the **Change Group** button.



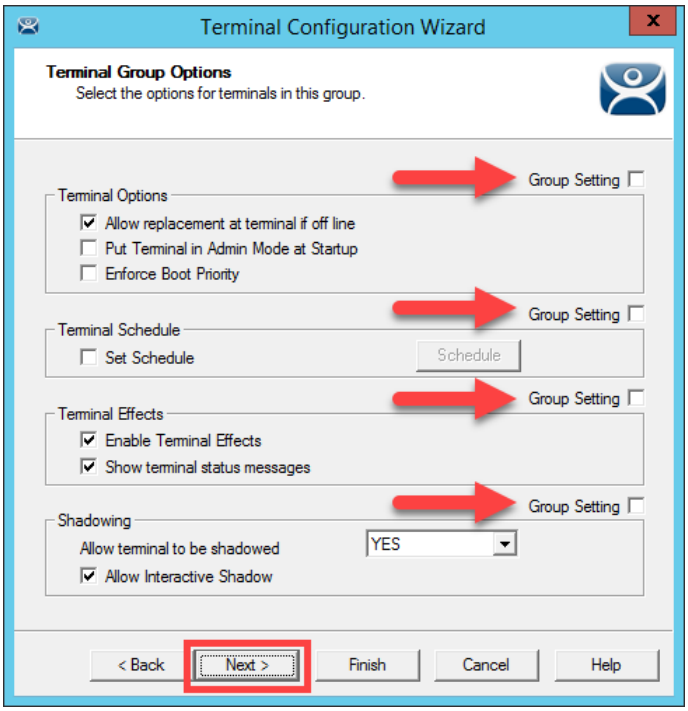
6. From the **Select Terminal Group** window, select **Mixer** and click the **OK** button.



7. Click the **Finish** button.
8. Let's say we would like all of the **Terminals** added to the **Mixer Terminal Group** to have the **Key Block Module**. Instead of assigning it to each individual **Terminal Profile**, we will add it to the **Terminal Group**. Double click the **Mixer Terminal Group**.



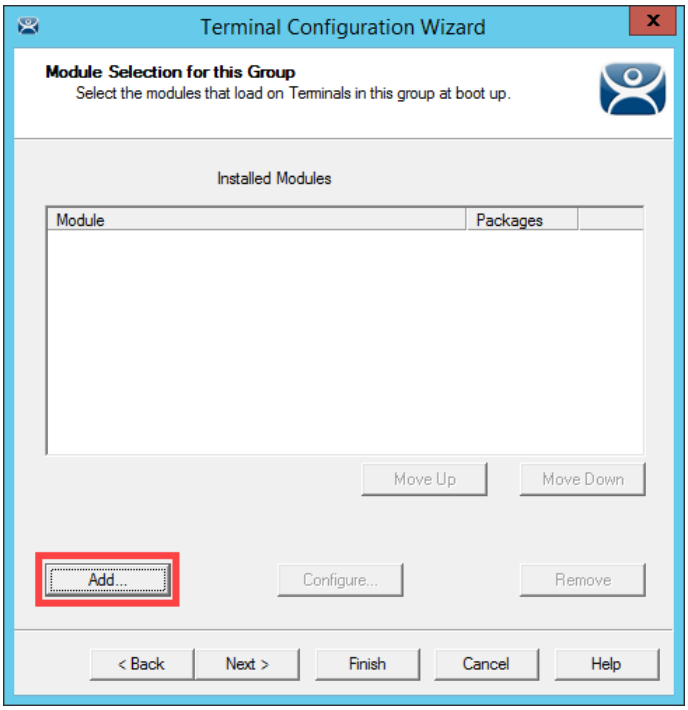
9. Click the **Next** button from the **Terminal Group Name** of the **Terminal Configuration Wizard**.
10. From the **Terminal Group Options** page of the wizard, notice the **Group Setting** checkboxes. Checking any of those checkboxes will result in that setting or group of settings to be inherited by the **Terminal** members of the **Terminal Group**. Do not check any of them – just click the **Next** button.



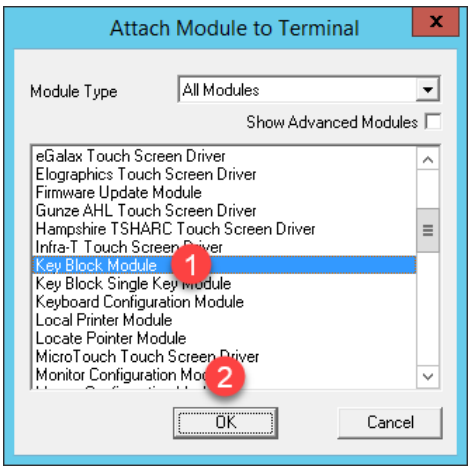
11. Click the **Next** button on the **Terminal Mode Selection** page of the wizard.
12. Click the **Next** button from the **Terminal Mode Selection** page of the wizard.
13. Click the **Next** button on the **Display Client Selection** page of the wizard.
14. Click the **Next** button on the **Terminal Interface Options** page of the wizard.
15. Click the **Next** button on the **Hotkey Configuration** page of the wizard.
16. Click the **Next** button on the **Log In Information** page of the wizard.
17. Click the **Next** button on the **Group Video Resolution** page of the wizard.
18. Click the **Next** button on the **WinTMC** page of the wizard.

> **WinTMC** is an application that can be installed on a **Windows OS** (like Windows 7/Vista/8/10) that essentially emulates a ThinManager Client. You would create a **Terminal Profile** for a **WinTMC** client in much the same way that you would for an actual thin/zero client.

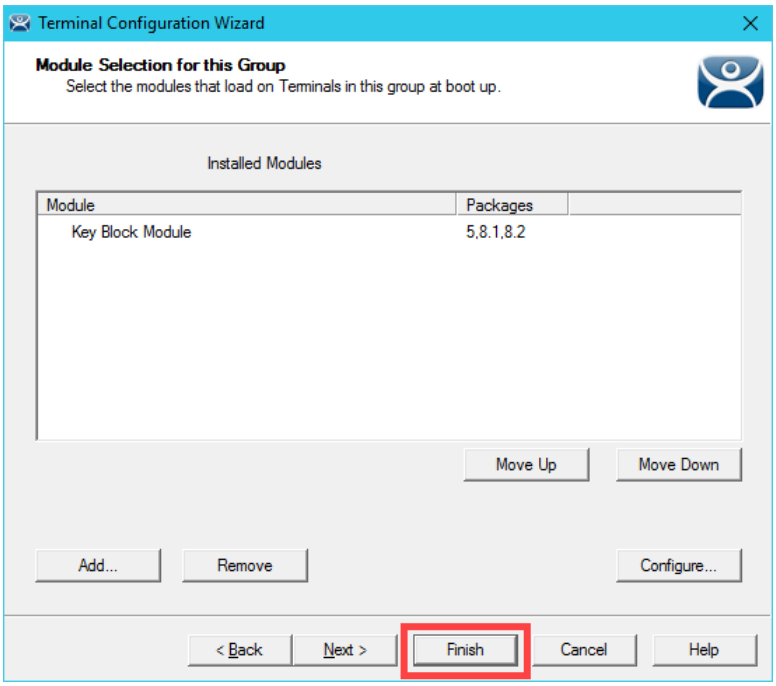
19. Click the **Next** button from the **Mobile Device Group Options** page of the wizard.
20. Click the **Add…** button from the **Module Selection for this Group** page of the wizard.



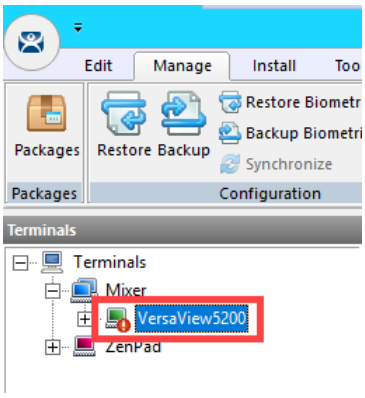
21. Scroll down and select the **Key Block Module**. Click the **OK** button.



22. Click the **Finish** button.



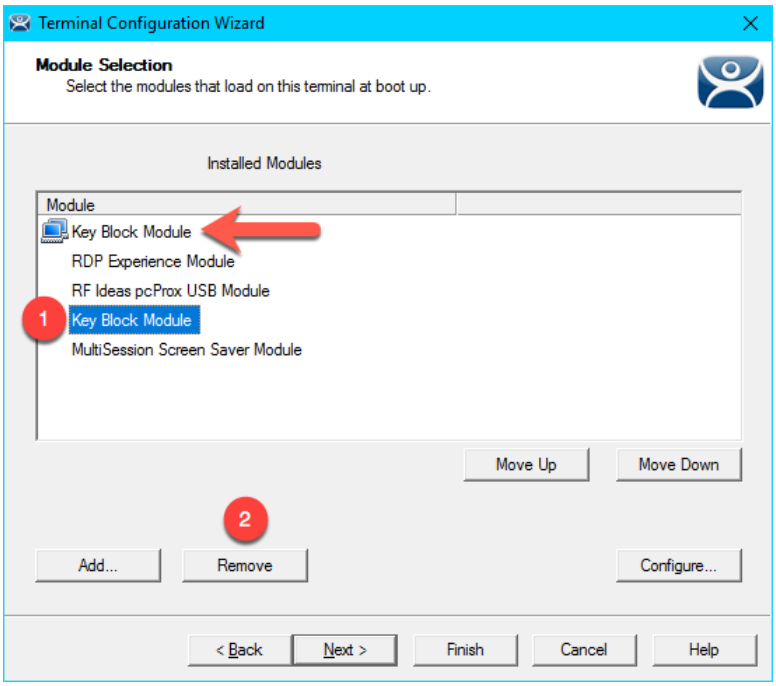
23. Double click on the **VersaView5200** terminal.



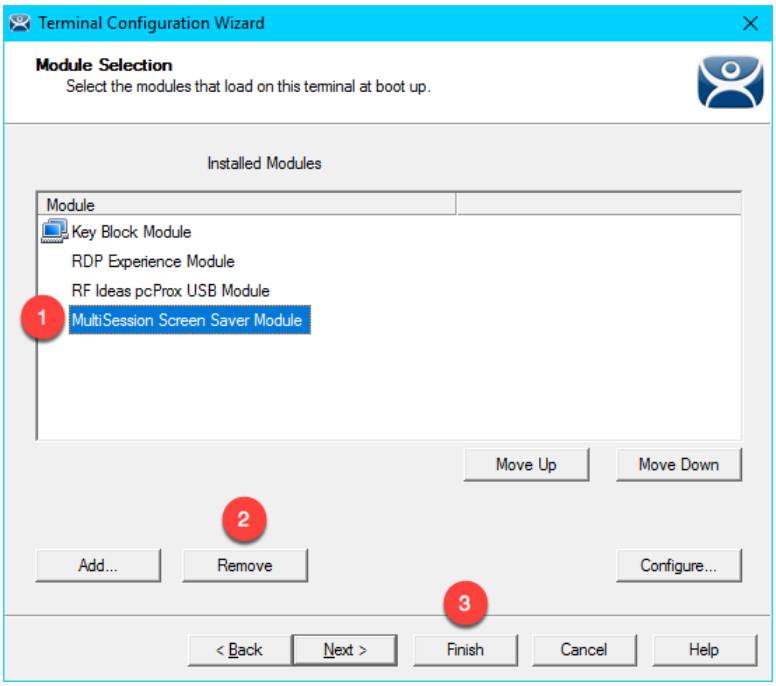
24. Click the **Next** button on the **Terminal Name** page of the wizard.

25. Click the **Next** button on the **Terminal Hardware** page of the wizard.

26. Click the **Next** button on the **Terminal Options** page of the wizard.
27. Click the **Next** button on the **Terminal Mode Selection** page of the wizard.
28. Click the **Next** button on the **Display Client Selection** page of the wizard.
29. Click the **Next** button on the **Terminal Interface Options** page of the wizard.
30. Click the **Next** button on the **Hotkey Configuration** page of the wizard.
31. Click the **Next** button on the **Log In Information** page of the wizard.
32. Click the **Next** button on the **Video Resolution** page of the wizard.
33. From the **Module Selection** page of the wizard, notice the group-inherited **Key Block Module** (indicated with the **Group** icon). Select the other **Key Block Module** listed. This is the one added in **Modules** lab section to this specific **Terminal Profile**. Click the **Remove** button.

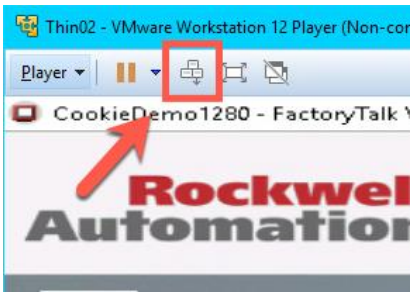


34. While still on the **Module Selection** page of the wizard, remove the **MultiSession Screen Saver Module** followed by the **Finish** button.



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

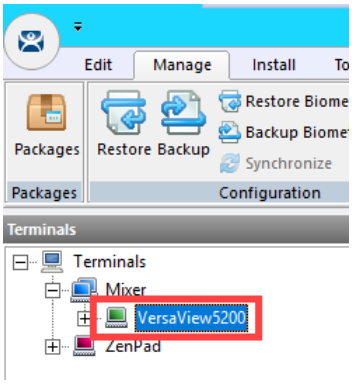
36. Confirm that **CTRL-ALT-DEL** is still blocked, and therefore proving that the **Key Block Module** is successfully inherited from the **Mixer Terminal Group**.



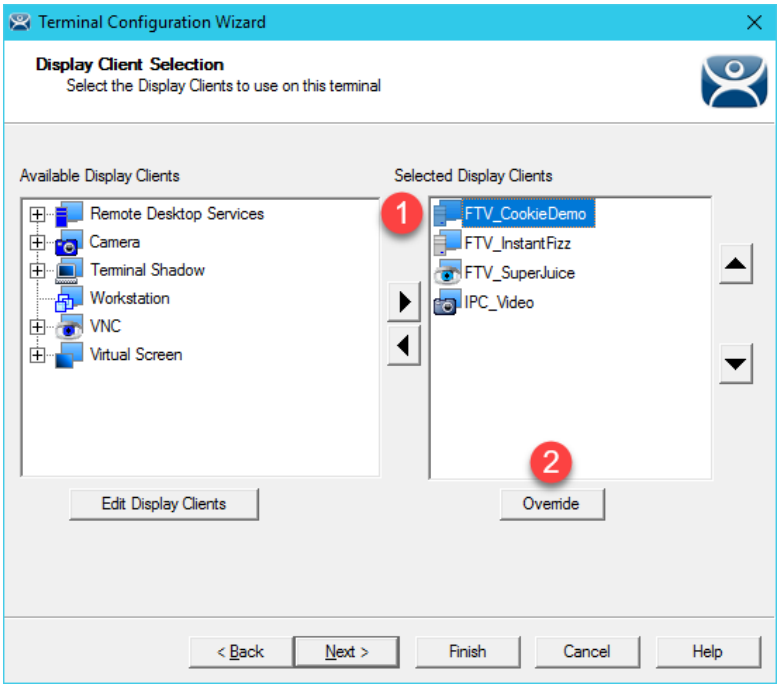
Overrides

The **Override** feature allows you to change the default behavior of a **Display Client** when applied to a **Terminal**. For instance, maybe you need a particular **Display Client** to launch as a different user than what is assigned to the **Terminal Profile**. This can be accomplished using the **Override** feature.

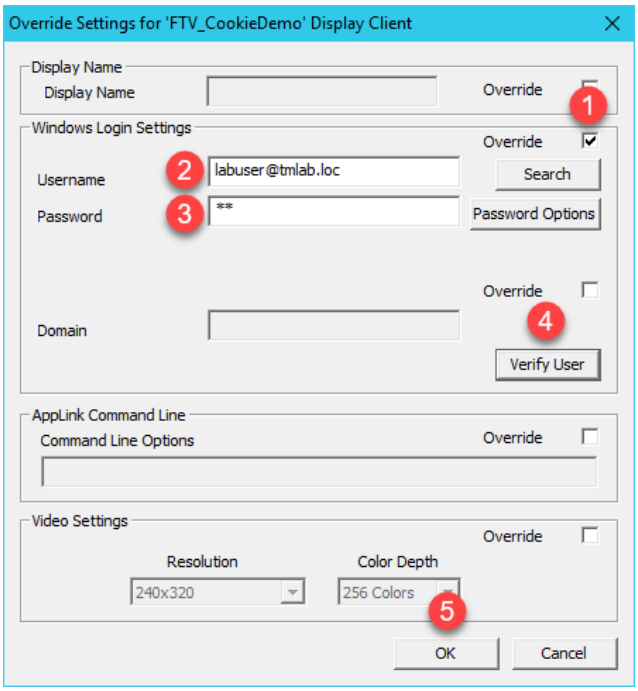
1. Double click the **VersaView5200** terminal.



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. Select the **FTV_CookieDemo Display Client** from the **Selected Display Clients** list and click the **Override** button.

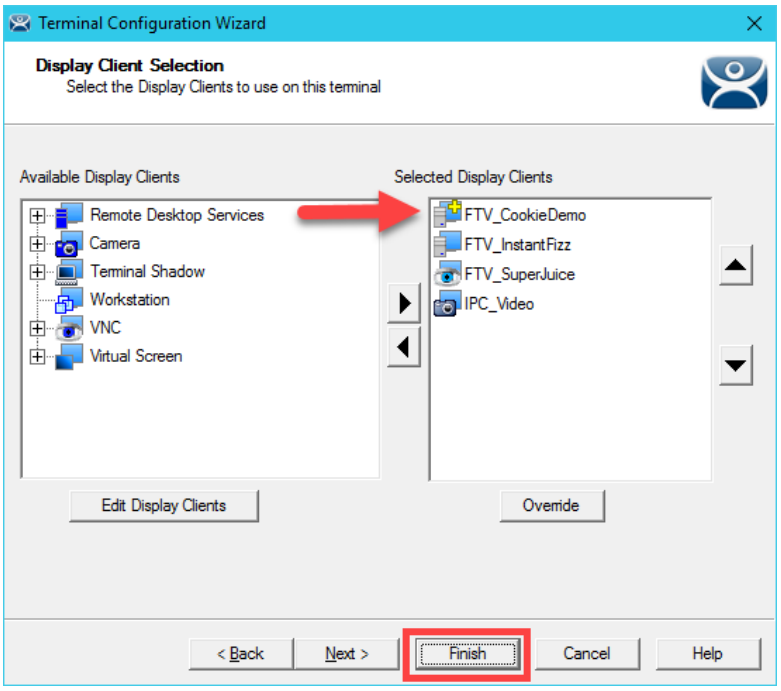


7. From the **Override Settings** window, check the **Override** checkbox on the **Windows Login Settings** frame, enter *labuser@tmlab.loc* as the **Username**, enter *rw* as the **Password**. Click the **Verify User** button to confirm the credentials entered. Click the **OK** button twice.



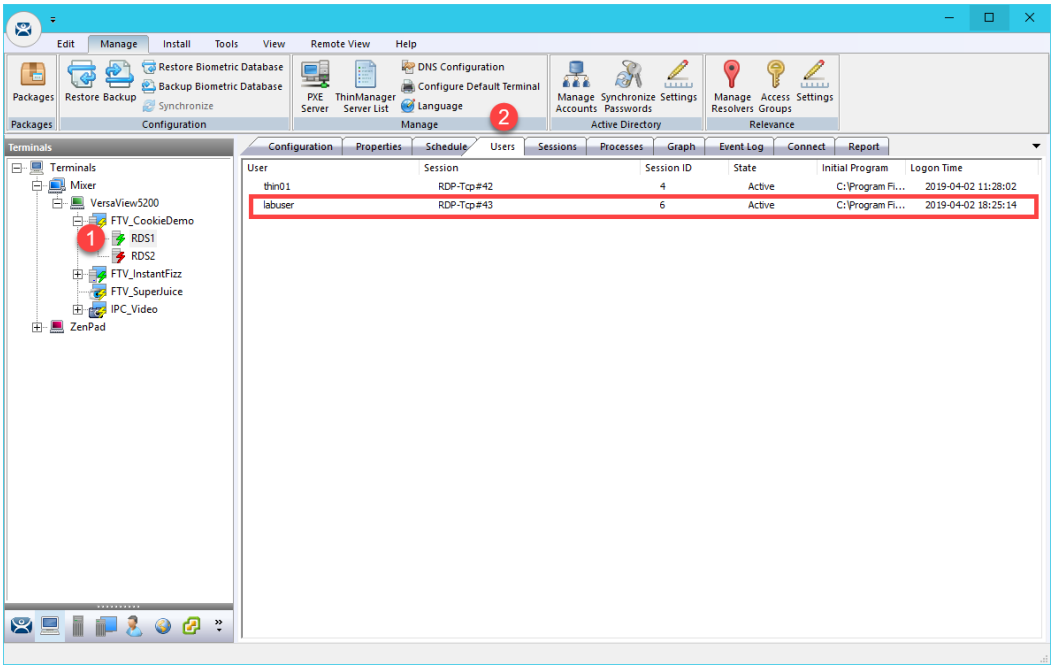
> In addition to user credentials, the **Domain** can be overridden, along with the **AppLink Command Line** and **Video Settings**.

8. Notice the **Display Client** icon has changed for **FTV_CookieDemo**, indicating that an **Override** has been applied to it for this **Terminal**. Click the **Finish** button.



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

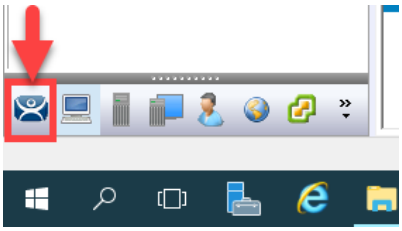
10. At the virtual thin client, you should see a new instance of the **FTV_CookieDemo** launching. Instead of launching as the user assigned to the **VersaView5200 Terminal Profile** (thin01@tmlab.loc), it is now launched as labuser@tmlab.loc. Navigate to **Terminals->Mixer->VersaView5200->FTV_CookieDemo** from the **Terminals** tree and select the **RDS1** node, followed by the **Users** tab. Here you will see the new session launched with the **labuser** credentials.



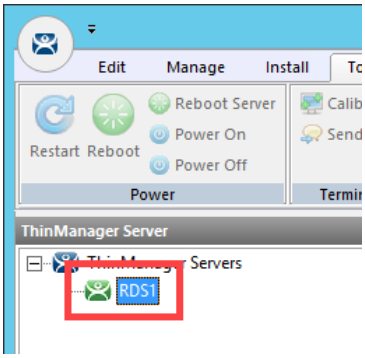
Schedules

ThinManager has a rich scheduling environment that can be applied to **Terminals**, **Remote Desktop Servers** and **Relevance Users**. For example, maybe certain **Terminals** should only be available at certain times of the day and/or certain days of the week. The same can be applied to **Relevance Users**. So, **Schedules** can be used to further enhance your **Security** initiatives. You can also schedule automatic ThinManager configuration backups, or regular **Touchscreen Calibrations!**

1. From ThinManager, click the **ThinManager** icon in the button bar.

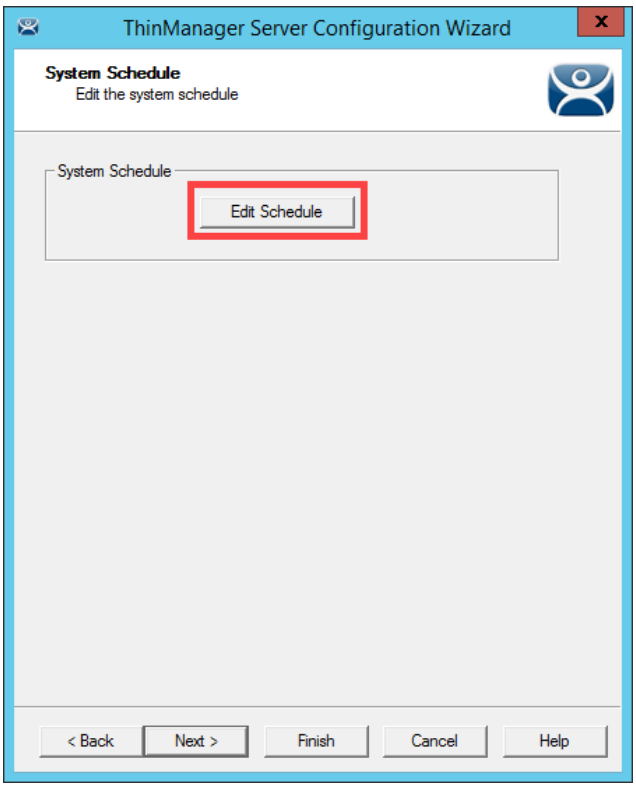


2. Double click the **RDS1** item in the **ThinManager Servers** tree.

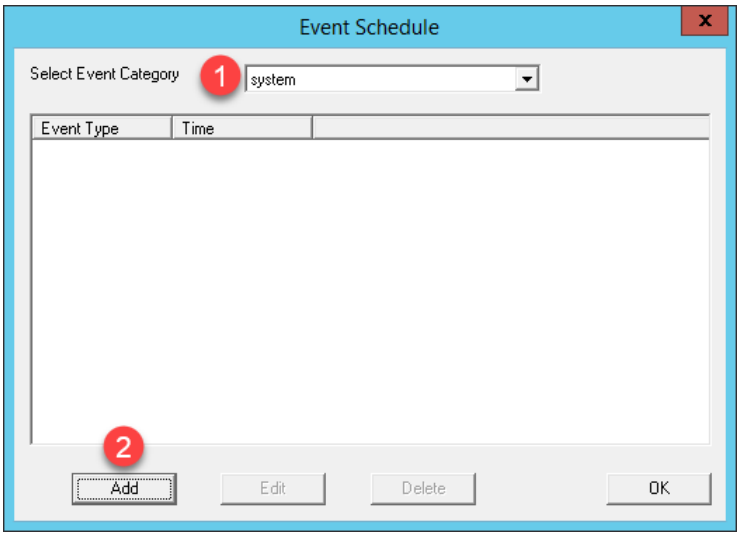


3. Click the **Next** button on the **Introduction** page of the **ThinManager Server Configuration Wizard**.
4. Click the **Next** button on the **Unknown Terminals** page of the wizard.
5. Click the **Next** button on the **Terminal Replacement** page of the wizard.
6. Click the **Next** button on the **Historical Logging** page of the wizard.

7. Click the **Edit Schedule** button on the **System Schedule** page of the wizard.

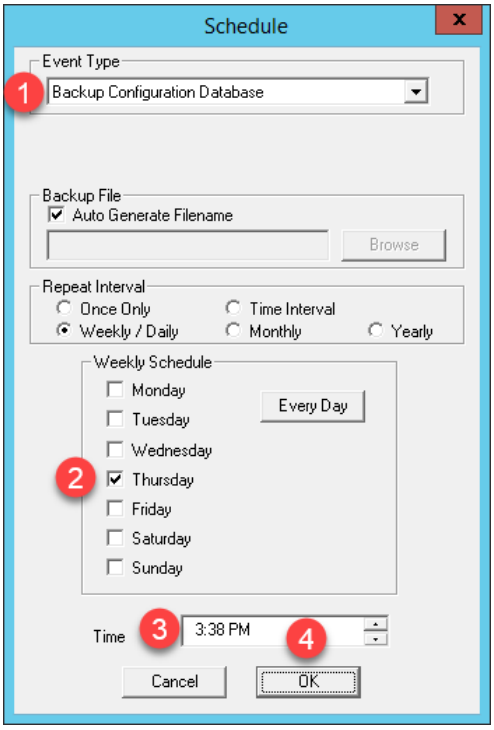


8. From the **Event Schedule** window, select **system** from the **Select Event Category** drop down list and click the **Add** button.

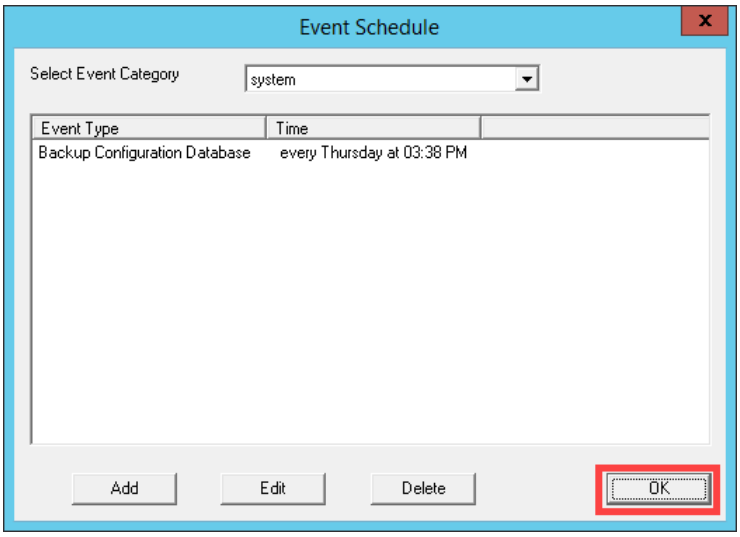


You may notice that is you select **terminal**, **terminalserver** or **user** from the drop down list, the **Add** button will become disabled. That is because **schedules** for these items are created on their respective objects. For example, to set a **terminal schedule** you would do that using the **Terminal Configuration Wizard** of the targeted terminal. This could also be accomplished at a **Terminal Group** level as well. You could then **Edit** or **Delete** those schedules from this dialog box.

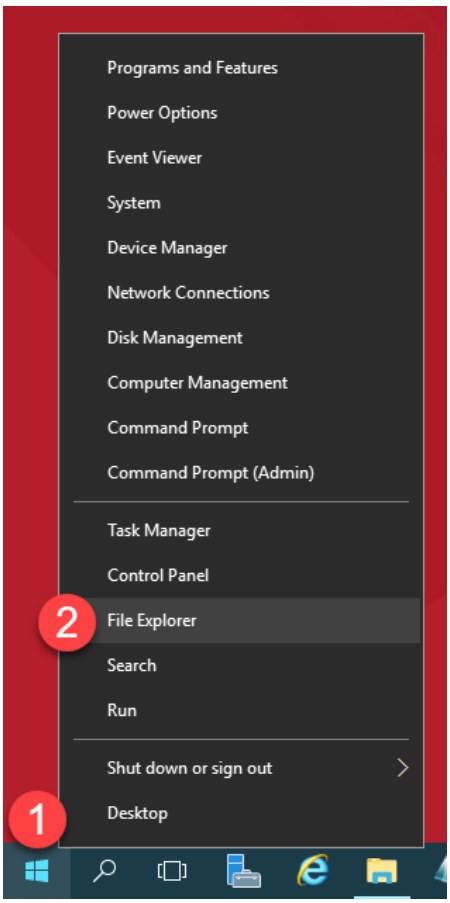
9. Select **Backup Configuration Database** from the **Event Type** drop down list. Leave **Auto Generate Filename** checked. Leave the **Weekly / Daily** radio button selected. Check today's day (**Thursday** in the screen shot) checkbox in the **Weekly Schedule** frame and set the time to 2 minutes past the current time of the **RDS1** virtual machine's time (**3:38 PM** in the screen shot). Click the **OK** button.



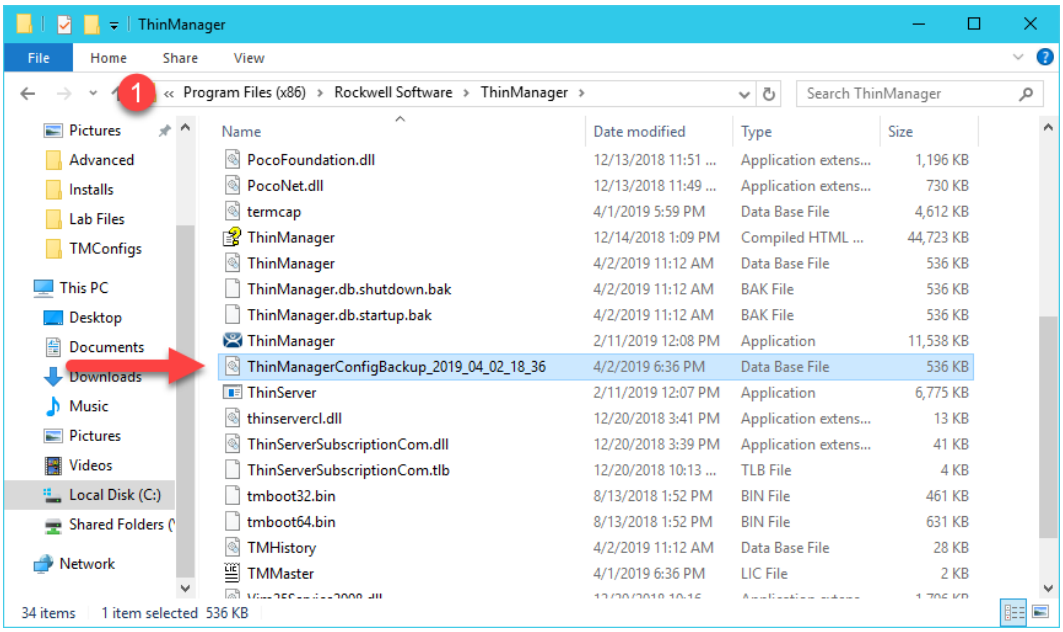
10. Click the **OK** button followed by the **Finish** button.



11. When the time on **RDS1** reaches the set schedule from above, right click the **Windows Start Button**, and select the **File Explorer** item.



12. Navigate to the following folder: **C:\Program Files (x86)\Rockwell Software\ThinManager**. You should see a new ThinManager configuration backup there. Close the **File Explorer** and return to **ThinManager**.



Mouse Button Mapping

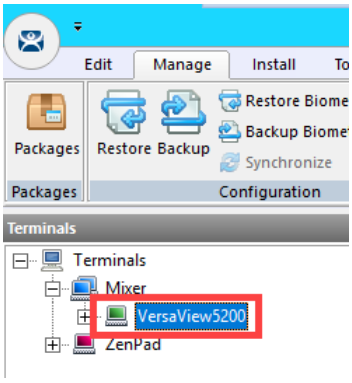
Enhanced **mouse button mapping** was added with the release of ThinManager 9.0. You can assign and perform the following ThinManager-related actions to any mouse button.

- Calibrate Touchscreen
- Tile
- Swap
- Full Screen
- Go To Next Display Client
- Go To Previous Display Client
- Log On Relevance User
- Main Menu
- Scroll Up
- Scroll Down
- Virtual Keyboard

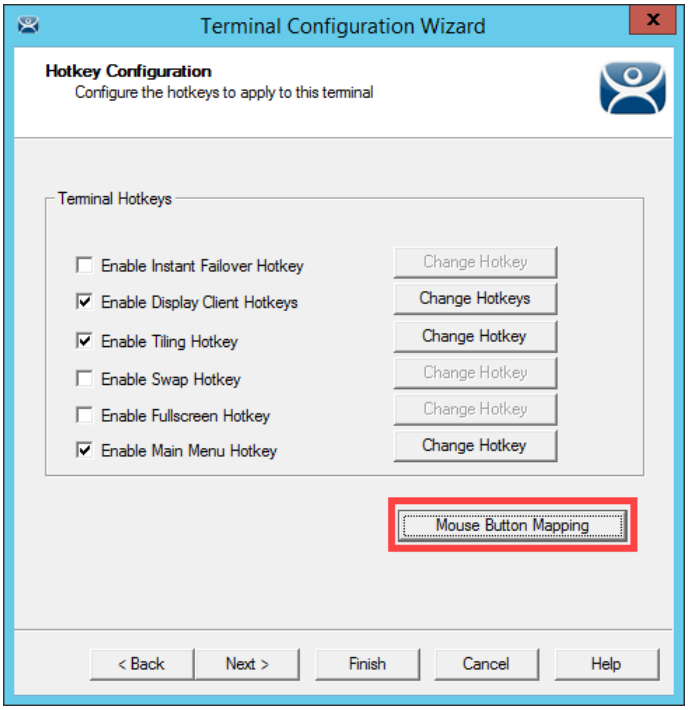
Different actions can be defined for different physical or **Virtual Screens**.

1. Click the **Terminals** icon from the button bar.

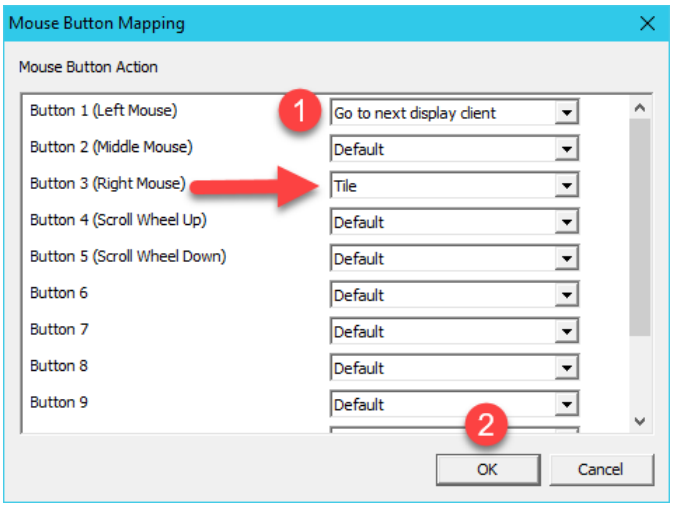
2. Double click the **VersaView5200** terminal.



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. Click the **Next** button on the **Terminal Mode Selection** page of the wizard.
7. Click the **Next** button on the **Display Client Selection** page of the wizard.
8. Click the **Next** button on the **Terminal Interface Options** page of the wizard.
9. Click the **Mouse Button Mapping** button on the **Hotkey Configuration** page of the wizard.



10. Earlier, we assigned the **Tile** action to the **Right Mouse** button. Change **Button 1 (Left Mouse)** to **Go to next display client**. Click the **OK** button.

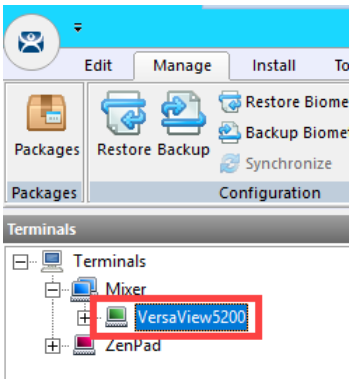


11. Click the **Finish** button.
12. Right click the **VersaView5200** terminal and select the **Restart Terminal** item. Click the **Yes** button to confirm.
13. At the virtual thin client, verify that a **Left Click** (or touch) switches to the next **Display Client**.

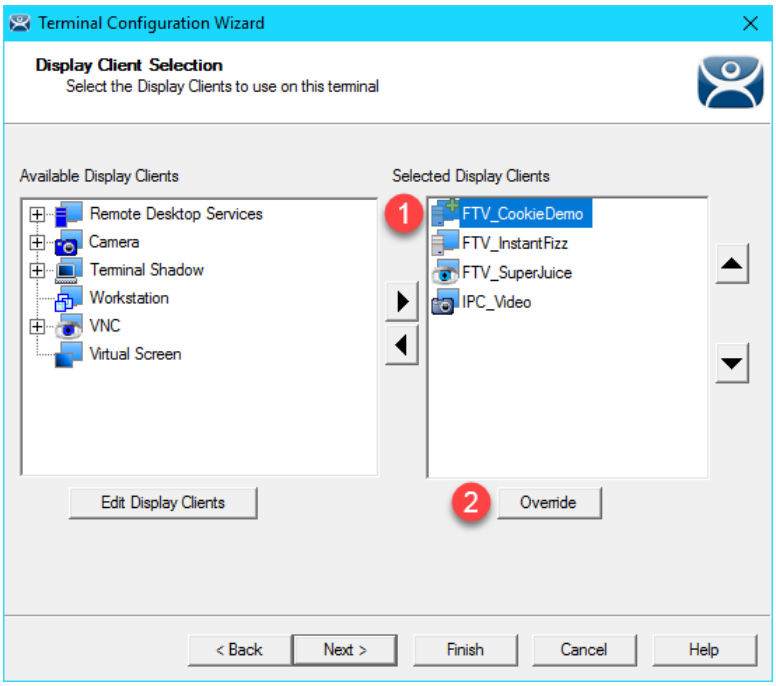
Remove Override and Mouse Button Mapping

Since we will not need these settings in the remaining lab sections, let's remove them before continuing.

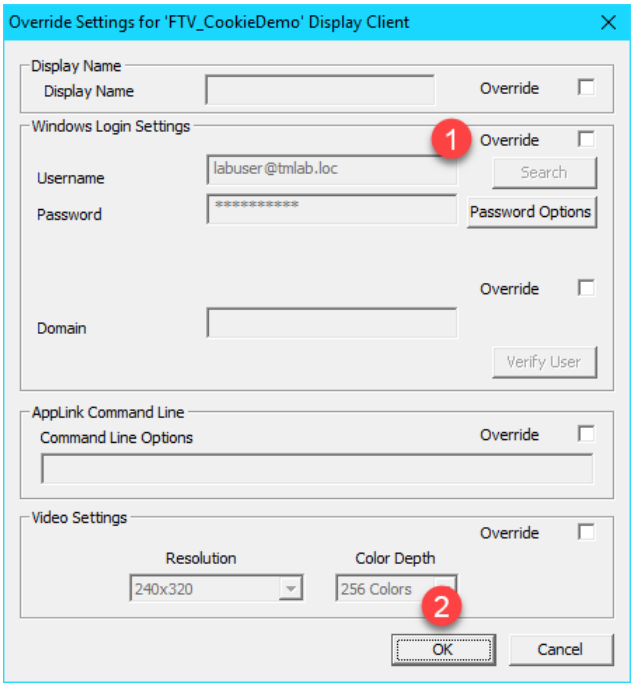
1. Double click the **VersaView5200** terminal.



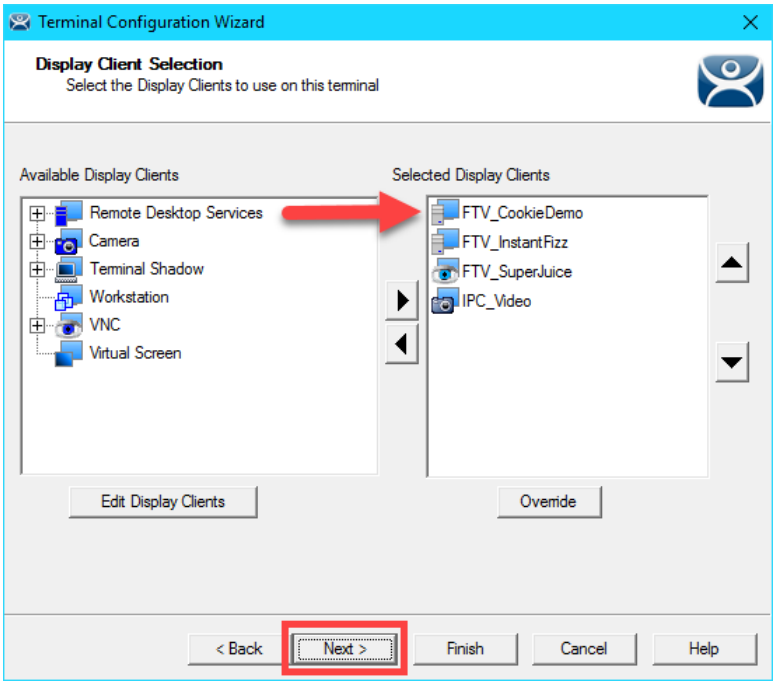
2. Click the **Next** button on the **Terminal Name** page of the wizard.
3. Click the **Next** button on the **Terminal Hardware** page of the wizard.
4. Click the **Next** button on the **Terminal Options** page of the wizard.
5. Click the **Next** button on the **Terminal Mode Selection** page of the wizard.
6. From the **Display Client Selection** page of the wizard, select the **FTV_CookieDemo Display Client** and click the **Override** button.



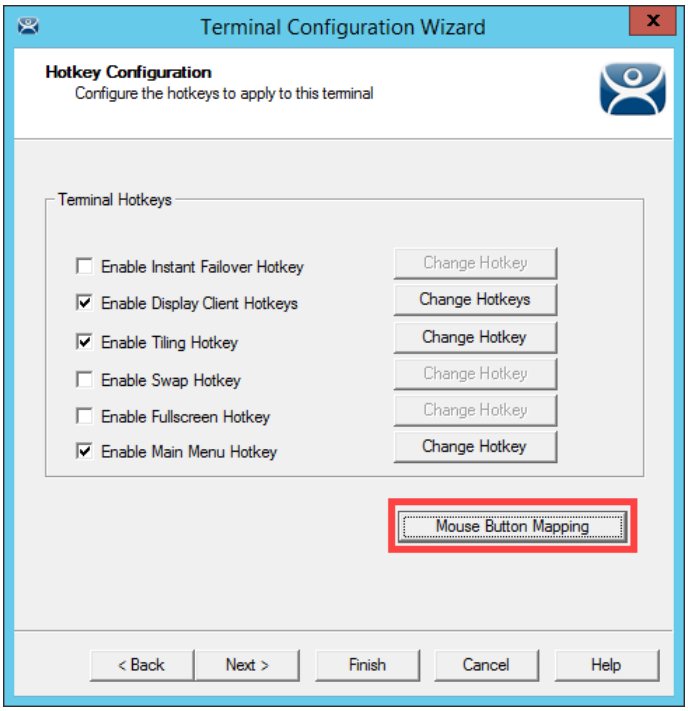
7. From the **Override Settings** window, **un**-check the **Override** checkbox and click the **OK** button.



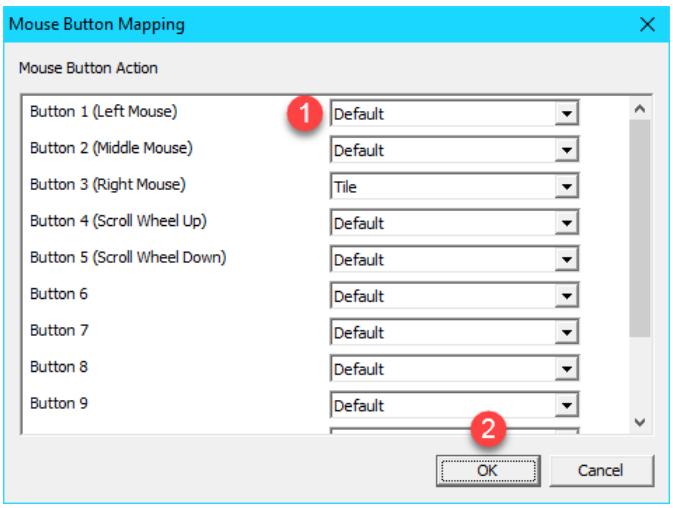
8. From the **Display Client Selection** page of the wizard, notice the **FTV_CookieDemo Display Client** no longer has the **Override** icon assigned to it. Click the **Next** button.



9. Click the **Next** button on the **Terminal Interface Options** page of the wizard.
10. Click the **Mouse Button Mapping** button on the **Hotkey Configuration** page of the wizard.



11. Return **Button 1 (Left Mouse)** to **Default**. Click the **OK** button.



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

Checkpoint Question: https://thinmanager.com/cloudlabs/section13/

This completes the section **Terminal Groups, Overrides, Schedules and Mouse Button Mapping**. Please continue on to the **Securing the ThinManager Adin Console** section of the lab.

Section 14: Securing the ThinManager Admin Console

Overview

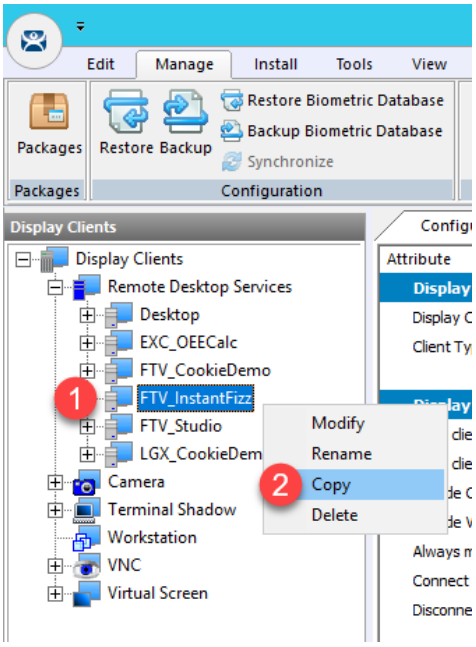
By default, only local administrator user accounts can access the **ThinManager Admin Console**. For ThinManager systems on an **Active Directory** (AD) domain, AD users who will administer the ThinManager system must initially be added to the local Administrators group on the ThinManager server. To add access for other local or domain accounts, **ThinManager Security Groups** can be configured to allow varying levels of access and control to the Admin Console. In this section we will explore requirements for an AD user to gain access and rights in the **ThinManager Admin Console**.

1. Create ThinManager Admin Console Display Client
2. Assign Admin Console Display Client to Terminal
3. ThinManager Security Groups

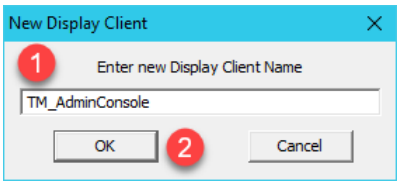
Create ThinManager Admin Console Display Client

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

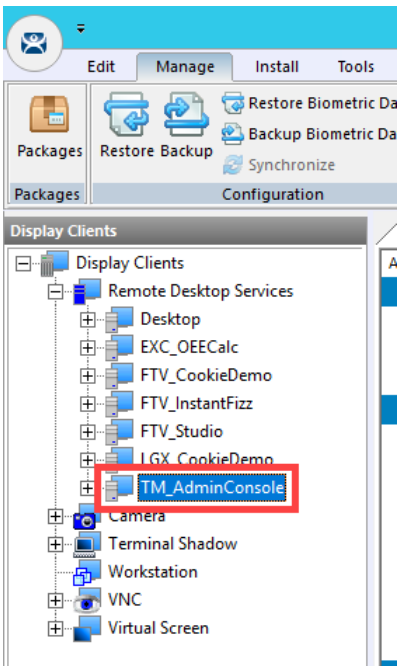
2. Expand the **Remote Desktop Services** tree item, right click the **FTV_InstantFizz Display Client** and select **Copy**.



3. From the **New Display Client** dialog box, enter *TM_AdminConsole* and click the **OK** button.



4. Double click the **TM_AdminConsole Display Client**.



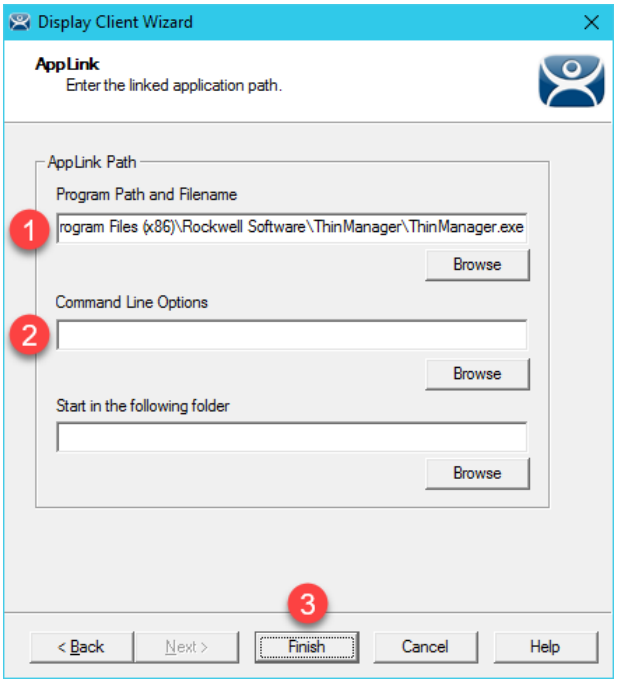
5. From the **Client Name** page of the wizard, click the **Next** button.
6. From the **Display Client Options** page of the wizard, click the **Next** button.
7. From the **Remote Desktop Services and Workstation Options** page of the wizard, click the **Next** button.
8. From the **Screen Resolution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

10. From the **AppLink** page of the wizard, enter the following path for the **Program Path and Filename** field (you can also copy this from the **LabPaths.txt** file). Clear the **Command Line Options** text box. Click the **Finish** button.

    Program Path and Filename:

    `C:\Program Files (x86)\Rockwell Software\ThinManager\ThinManager.exe`

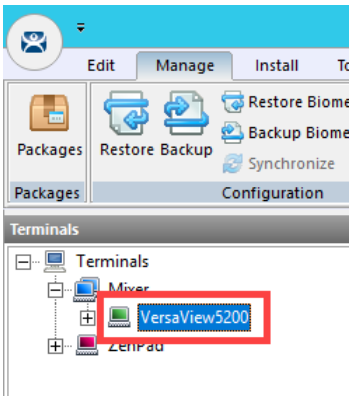
    Command Line Options:



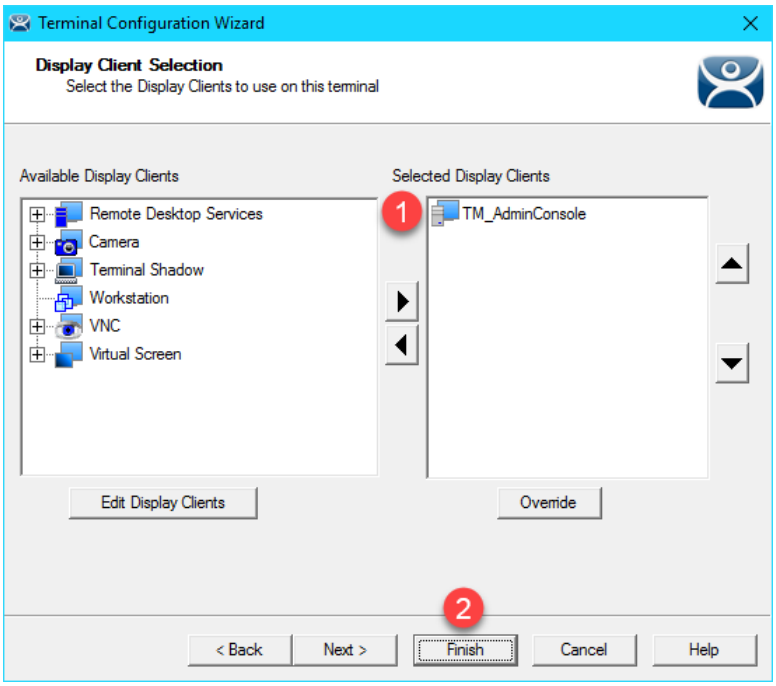
Assign Admin Console Display Client to Terminal

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

2. From the **Terminals** tree, double click the **VersaView5200** terminal



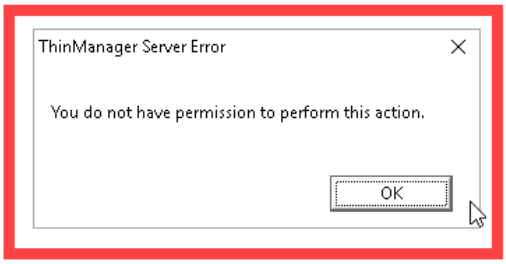
3. Click the **Next** button from the **Terminal Name** page of the wizard.
4. Click the **Next** button from the **Terminal Hardware** page of the wizard.
5. Click the **Next** button from the **Terminal Options** page of the wizard.
6. Click the **Next** button from the **Terminal Mode Selection** page of the wizard.
7. On the **Display Client Selection** page, remove the existing **Display Clients** from the **Selected Display Clients** list box, and add the **TM_AdminConsole Display Client**. Click the **Finish** button.



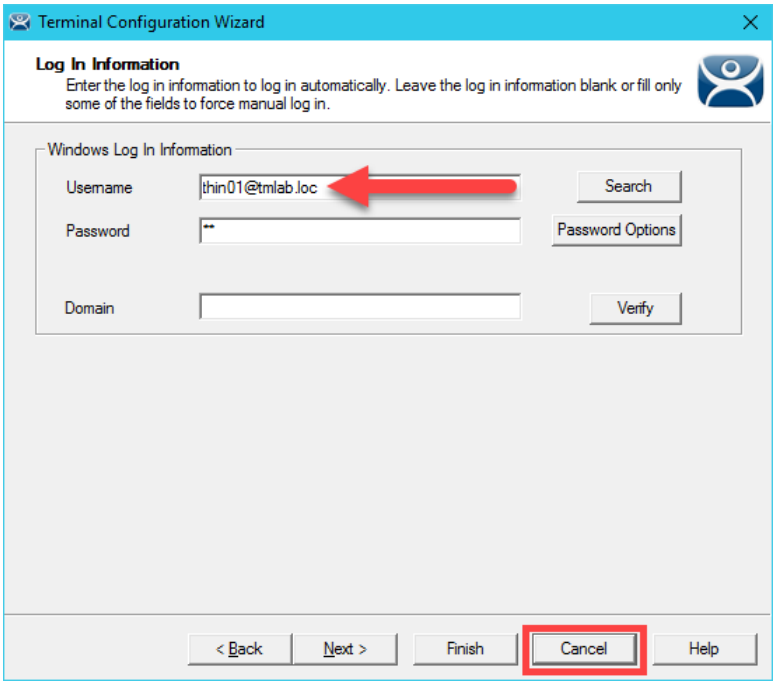
8. Right click the **VersaView5200** terminal from the **Terminals** tree and select **Restart Terminal** to apply the changes.

Click **Yes** to the confirmation dialog.

9. After the terminal has restarted and launched the **TM_AdminConsole Display Client**, you will see a permissions error message at the virtual thin client. By default, only local **Administrators** have access to the **ThinManager Admin Console**.



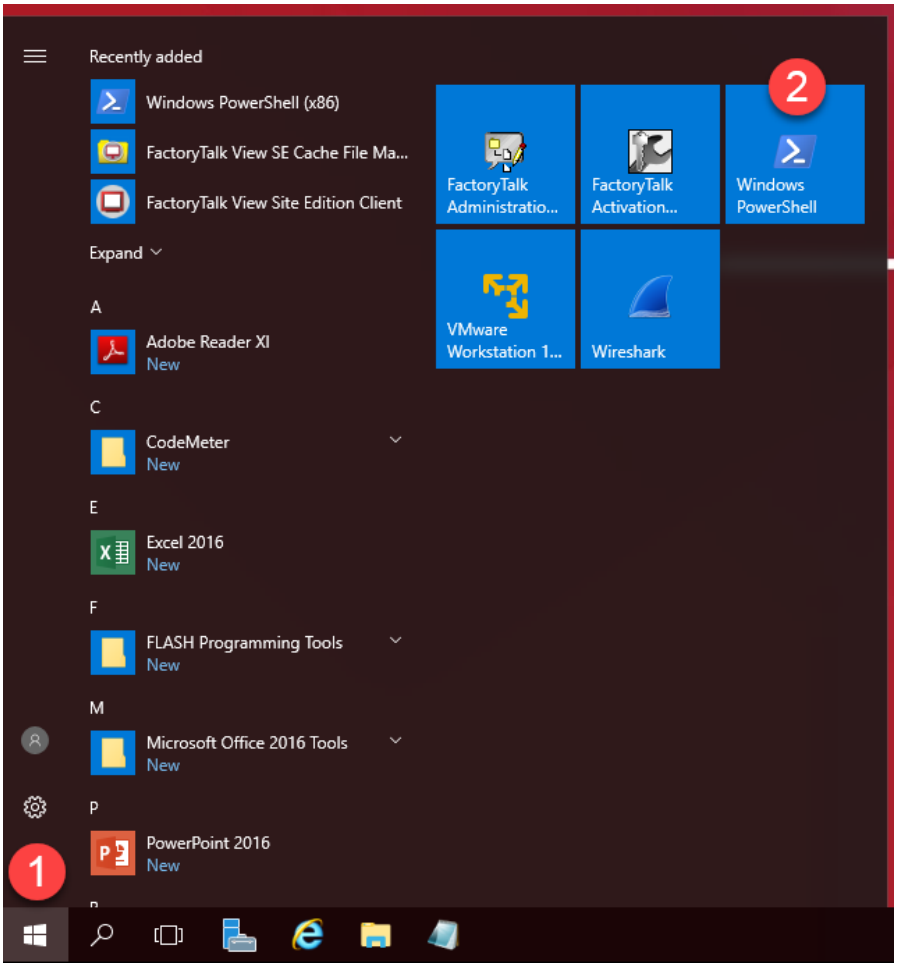
10. Recall that the user account assigned to the **VersaView5200** terminal is **thin01@tmlab.loc**. You can verify this by double clicking the **VersaView5200** terminal profile and advancing through the **Terminal Configuration Wizard** until you reach the **Log In Information** page. Since the **thin01@tmlab.loc** user account is not a member of the local Administrators group, it cannot launch the **Admin Console** by default. Click the **Cancel** button.



ThinManager Security Groups

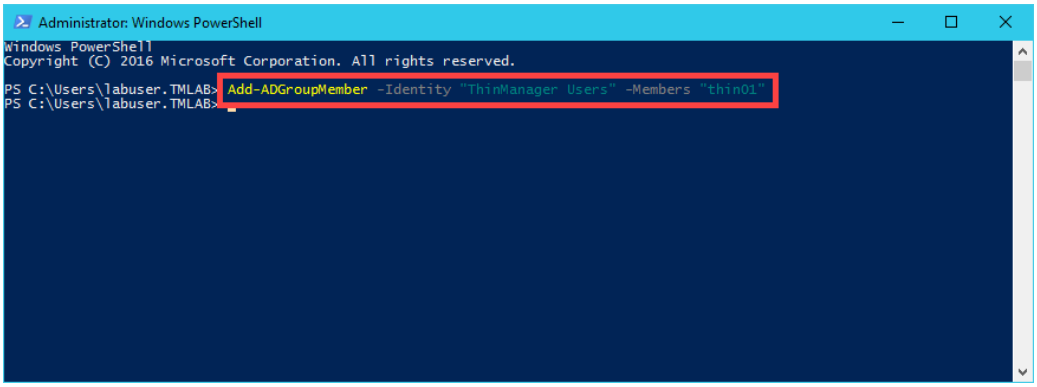
The Windows Security Groups utilized in this section of the lab have been pre-created within Active Directory. If you do not have a domain, these Security Groups could also be Local Security Groups.

1. We would like to add the **thin01@tmlab.loc** user to the **Active Directory Security Group ThinManager Users**. To do so, click the **Windows Start Button**, right click **Windows Power Shell** and select **Run as Administrator**.



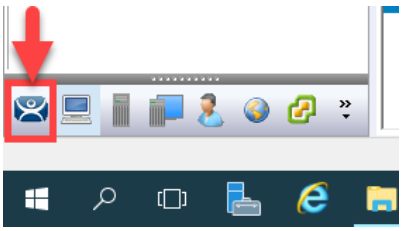
2. In the **PowerShell** window, enter the following command (you can also copy this from the **LabPaths.txt** file) and hit ENTER. This will add the **thin01** user to the **ThinManager Shadow Users ActiveDirectory Security Group**. Once completed, close the **PowerShell** window.

```
Add-ADGroupMember -Identity "ThinManager Users" -Members "thin01"
```

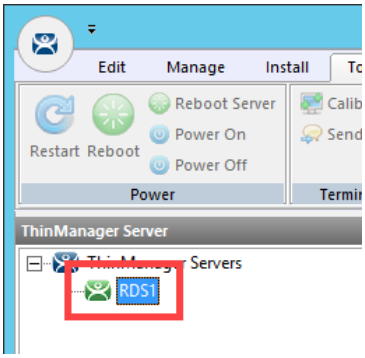


The **ServerManager PowerShell** module was preinstalled on **RDS1** as well as the **ActiveDirectory PowerShell** feature.

3. From ThinManager, click the **ThinManager** icon in the button bar.

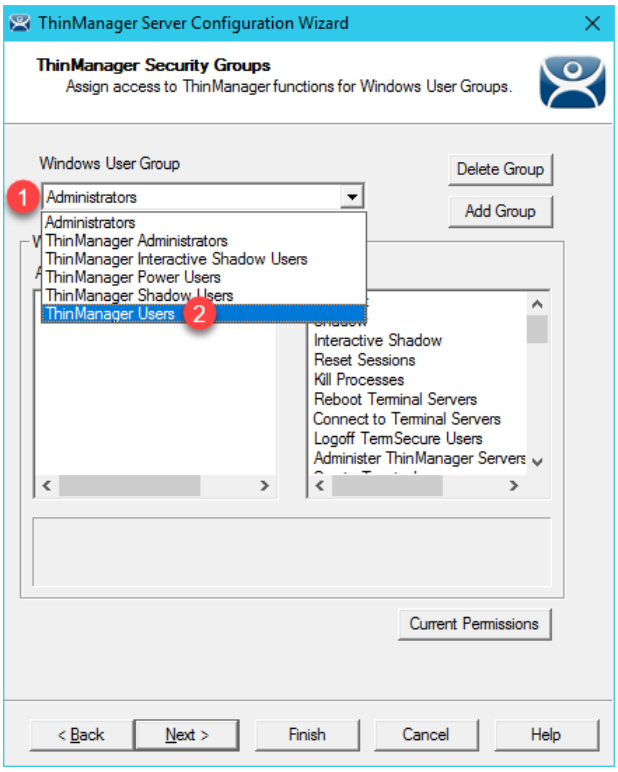


4. Double click the **RDS1** item in the **ThinManager Servers** tree.

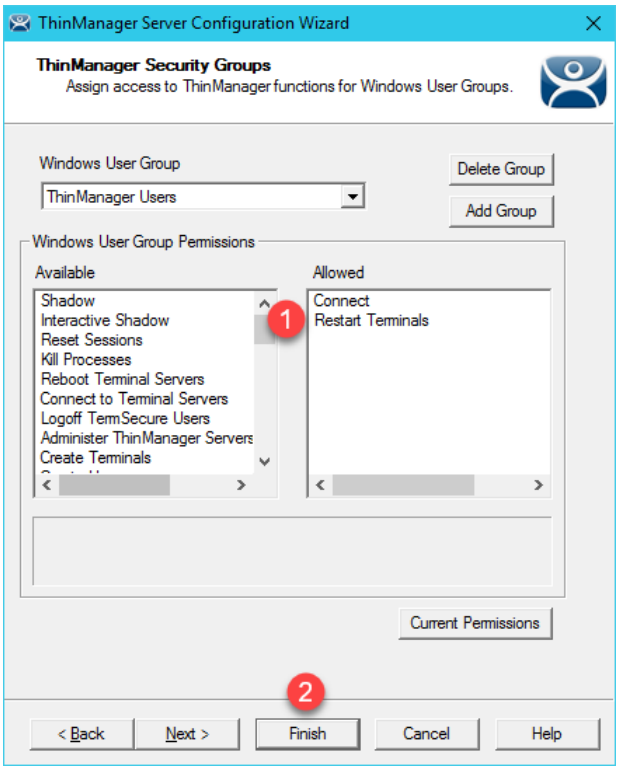


5. Click the **Next** button on the **Introduction** page of the **ThinManager Server Configuration Wizard**.
6. Click the **Next** button on the **Unknown Terminals** page of the wizard.
7. Click the **Next** button on the **Terminal Replacement** page of the wizard.
8. Click the **Next** button on the **Historical Logging** page of the wizard.
9. Click the **Next** button on the **System Schedule** page of the wizard.

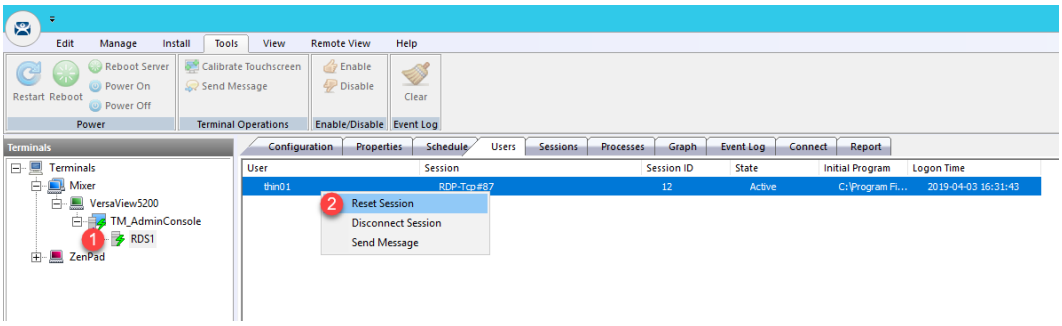
10. From the **ThinManager Security Groups** page of the wizard, notice that the pre-selected **Administrators** group has every **Available** list box **permission** in the **Allowed** list box. This indicates that, by default, members of the local **Administrators** group where **ThinManager** is installed have full permissions within the **Admin Console**. Click the **Windows User Group** drop down list and select **ThinManager Users**. As can be viewed from the **ThinManager Security Groups** page of the wizard, the available permissions are quite granular.



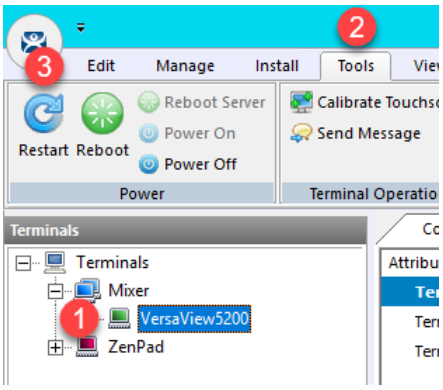
11. The **ThinManager Users** group is permitted to **Connect** only by default and can essentially do nothing else within the **Admin Console**. Scroll to the **Restart Terminals** permission and double click it to add it to the **Allowed** list. Click the **Finish** button.



12. Now that **thin01@tmlab.loc** is a member of the **ThinManager Users ActiveDirectory Security Group**, let's reset the session associated with the **TM_AdminConsole Display Client**. From the **Terminals** tree, navigate to **Terminals->Mixer->VersaView5200->TM_AdminConsole** and select **RDS1**. With **RDS1** selected, select the **Users** tab, right click the session listed and select **Reset Session**. This will reset the **TM_AdminConsole** session on the virtual thin client.



13. Return to the virtual thin client. The **TM_AdminConsole Display Client** should now be delivered. Since right click is being mapped to Tiling in the **VersaView5200** terminal profile, we will use an alternative way to perform a **Restart Terminal** action. Select the **VersaView5200** terminal then select the **Tools** ribbon followed by clicking the **Restart** icon. Click **Yes** to the confirmation dialog box. The terminal should restart since the **thin01@tmlab.loc** user account is a member of the **ThinManager Users** security group, which now has the **Restart Terminals** permission.



> Adding users to **Security Groups** as we did in this lab section do not immediately get recognized within **ThinManager**, since there is no way to be notified of these changes through **Active Directory**. **ThinManager** does check for **Security Group** membership updates every 4 minutes or any time a change is made in **ThinManager** to one of its **Security Groups** (i.e.: a permission is added/removed from an existing **Security Group**). You can also force an update by restarting the **ThinServer** service. Since we made a change to the **ThinManager Users** group (by adding the **Restart Terminals** permission), **ThinManager** refreshed its **Security Group** membership and detected that **thin01@tmlab.loc** had been added to the **ThinManager Users** group.

This completes the **Securing the ThinManager Admin Console** section of the lab. Please continue on to the **ThinManager SmartSession** section of the lab.

Section 15: ThinManager SmartSession

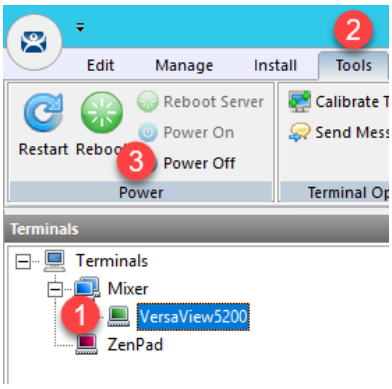
Overview

With **SmartSession**, **Remote Desktop Services Display Clients** will be started on the least loaded **Display Server** assigned to the **Display Client**. ThinManager determines the least loaded **Display Server** by performing a load calculation based on the **CPU** and **RAM** utilization along with the **number of sessions** running on each **Display Server**. Once a **Display Client** is launched on a **Display Server**, ThinManager does not attempt to move it dynamically to maintain a balanced load (i.e.: this calculation and determination only occurs when a **Display Client** is launched). In this section we will configure the RDS1 and RDS2 **Display Servers** to utilize **SmartSession** to balance session loading as a **FactoryTalk View SE Client** application is deployed multiple times to the virtual thin client.

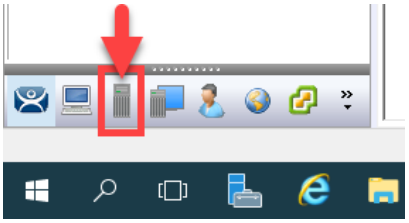
1. Power Off Terminal and Reset Sessions
2. Configure Display Servers for SmartSession
3. Create Display Clients for SmartSession
4. Assign Display Clients with SmartSession to Terminal
5. Power Off Terminal and Reset Sessions

Power Off Terminal and Reset Sessions

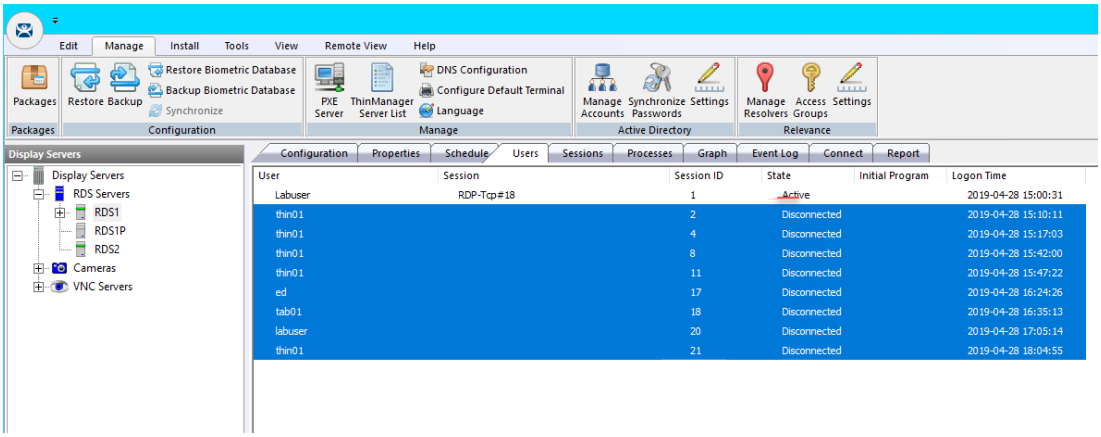
1. Power off the virtual thin client by selecting the **VersaView5200** terminal, followed by the **Tools** ribbon, then click the **Power Off** icon.



2. Navigate to the **Display Servers** tab in the **ThinManager Admin Console**.

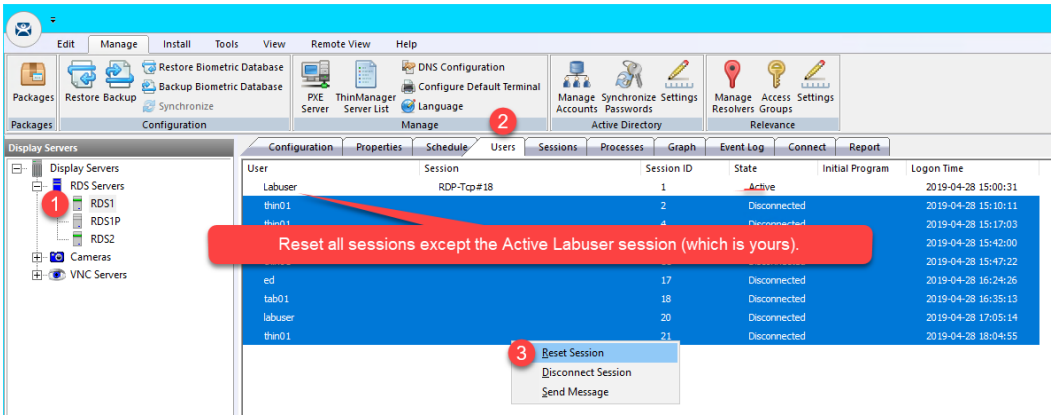


3. Expand **RDS Servers,** select **RDS1** and click the **Users** tab. Here you will see information about all of the user sessions established on **RDS1**. You may see more and/or different sessions than the screen shot below.

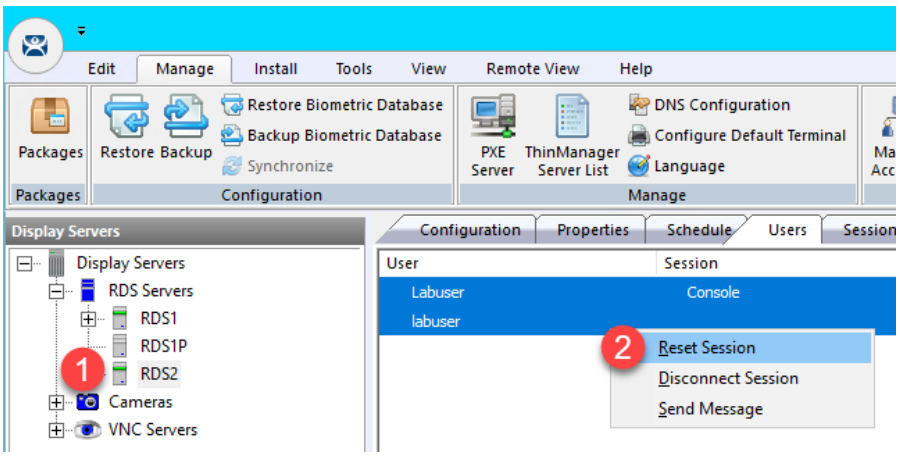


> In order for **ThinManager** to gather this session information from a **Remote Desktop Server**, you must assign an account to the **ThinServer** service that is a member of the local **Administrator** group on the **ThinManager Server**. This same account also needs to be assigned to the **Remote Desktop Server Display Server**. This can be done by double clicking the **Display Server** and advancing to the **Remote Desktop Server Name** page of the wizard and entering the account's credentials in the **Log In Information** frame. In an **Active Directory** deployment, this should be a domain account, and should be assigned to the **ThinServer** service on both **ThinManager** installations (if using **Redundancy**) and assigned to every **Remote Desktop Server Display Server**. These steps have already been completed for you in the lab.

4. Select all of the sessions except the **Active** session for the User **Labuser** (this is your current session into **RDS1**). Right click the other sessions select **Reset Session.** Click the **Yes** button on the confirmation dialog box. **NOTE:** The list of sessions running at your lab station may differ from the screen shot below. None of the sessions should relaunch since we have powered down the virtual thin client.



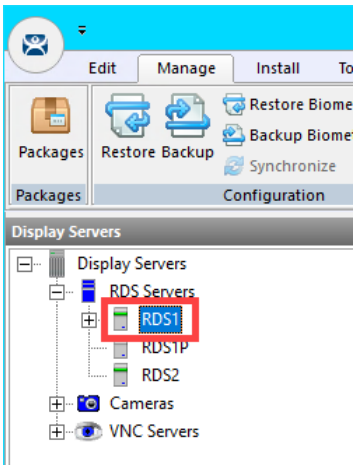
5. Now select **RDS2**, and once again click the **Users** tab. Reset all sessions.



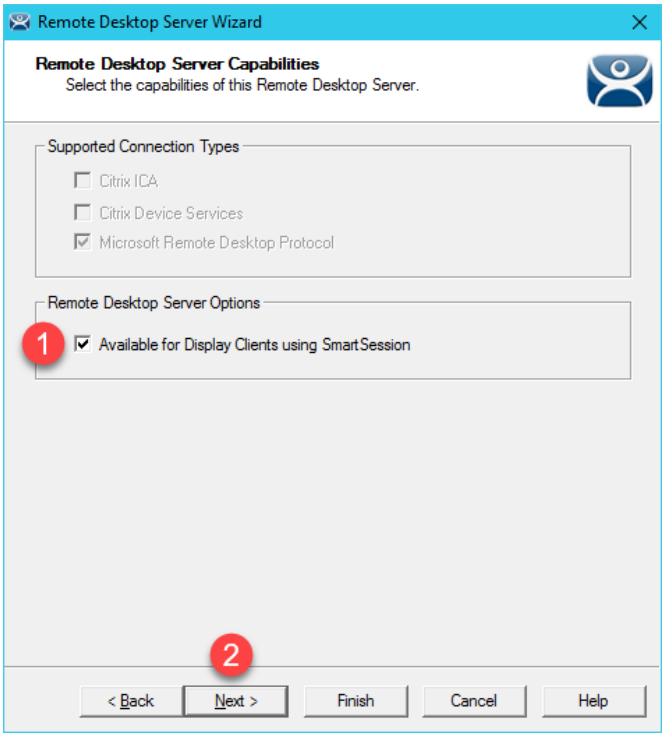
Configure Display Servers for SmartSession

In this section, we will enable **SmartSession** on the **RDS1** and **RDS2 Display Servers** and review the configuration options.

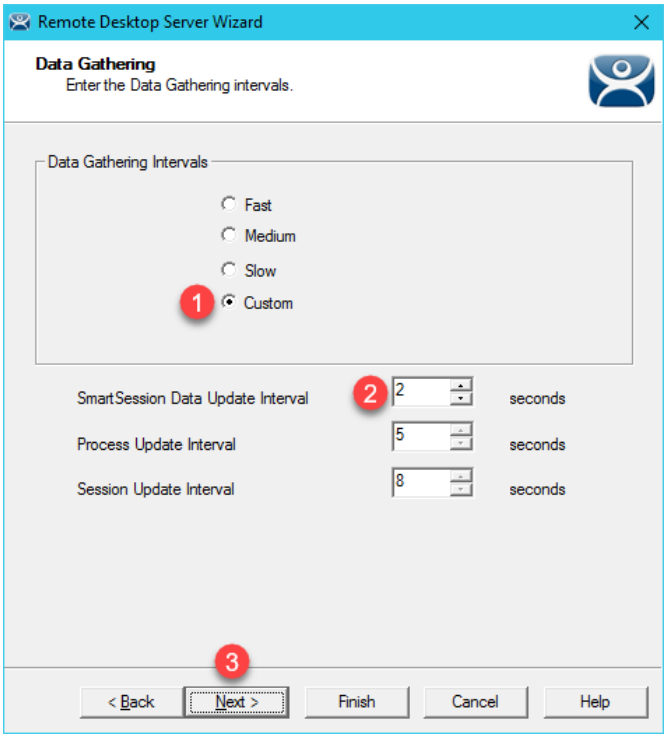
1. Double click **RDS1** Display Server to begin configuration.



2. Click the **Next** button on the **Introduction** page of the wizard.
3. Click the **Next** button on the **Remote Desktop Server Name** page of the wizard.
4. From the **Remote Desktop Server Capabilities** page, check the **Available for Display Clients using SmartSession** checkbox. Click **Next** the button.

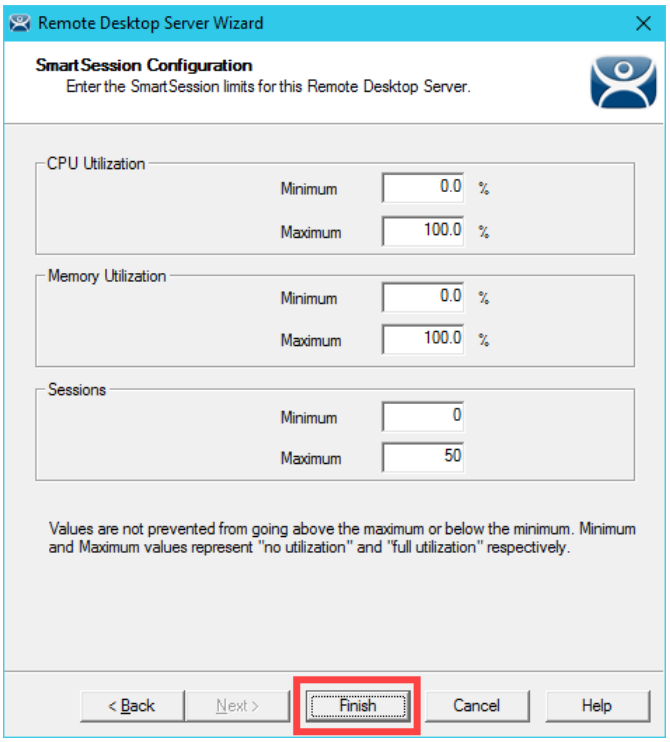


5. On the **Data Gathering** page of the wizard, select the **Custom** radio button and reduce the **SmartSession Data Update Interval** to **2** seconds. Click the **Next** button.



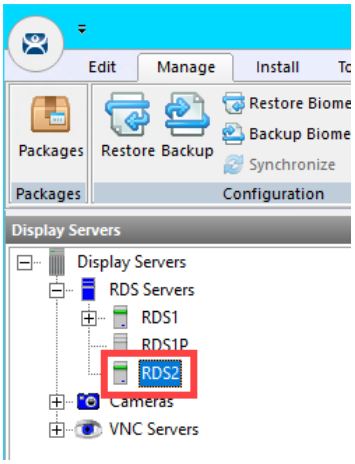
Smart Session Data Update Interval is the amount of time between the retrieval of SmartSession data – CPU usage, memory usage, and session count, from the Remote Desktop Server. This setting affects the update speed of the **Server Rankings** used in **SmartSession** load balancing. Faster rates will lead to quicker updates but will add more network traffic.

6. On the **SmartSession Configuration** page we will leave the default settings for the lab. The limits configured on this page make up the 0% to 100% scale used to gauge each utilization marker. Click the **Finish** button.



An example of why the defaults might be changed: You may want to consider the RDS server to be at 100% utilization when 25 sessions are running, instead of the default 50. Or you may want to consider the RDS server at 100% utilization when 70% of memory is consumed, instead of 100%.

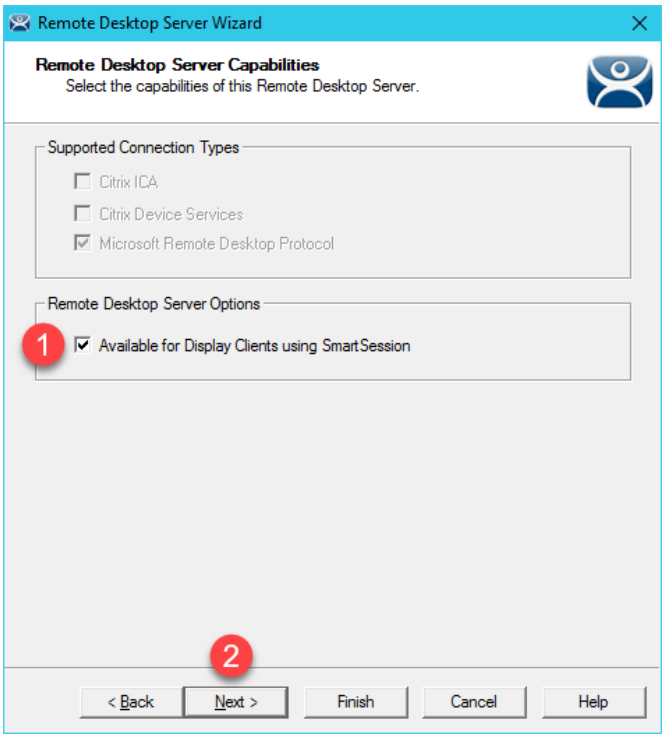
7. Double click **RDS2** Display Server to begin configuration.



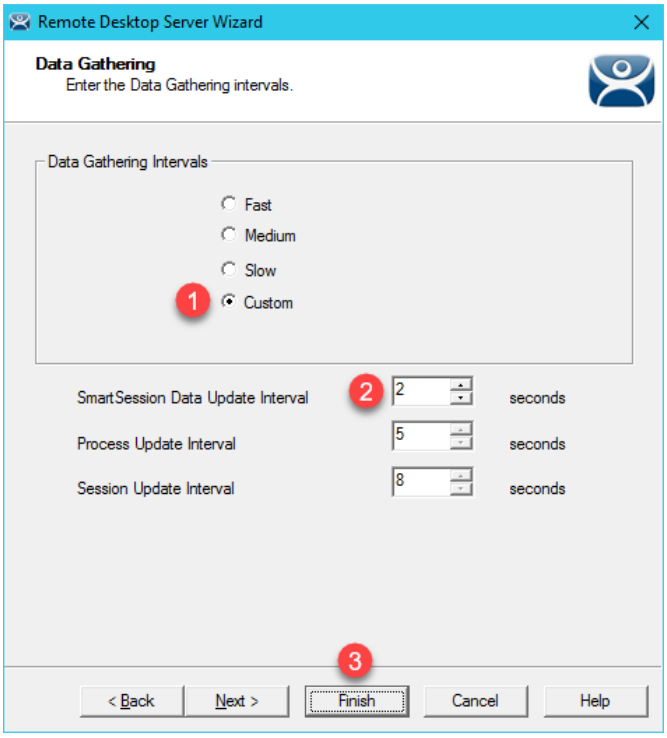
8. Click the **Next** button on the **Introduction** page of the wizard.

9. Click the **Next** button on the **Remote Desktop Server Name** page of the wizard.

10. From the **Remote Desktop Server Capabilities** page, check the **Available for Display Clients using SmartSession** checkbox. Click **Next** the button.



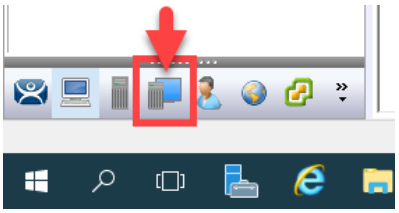
11. On the **Data Gathering** page, select the **Custom** radio button and reduce the **SmartSession Data Update Interval** to **2** seconds. Click the **Finish** button.



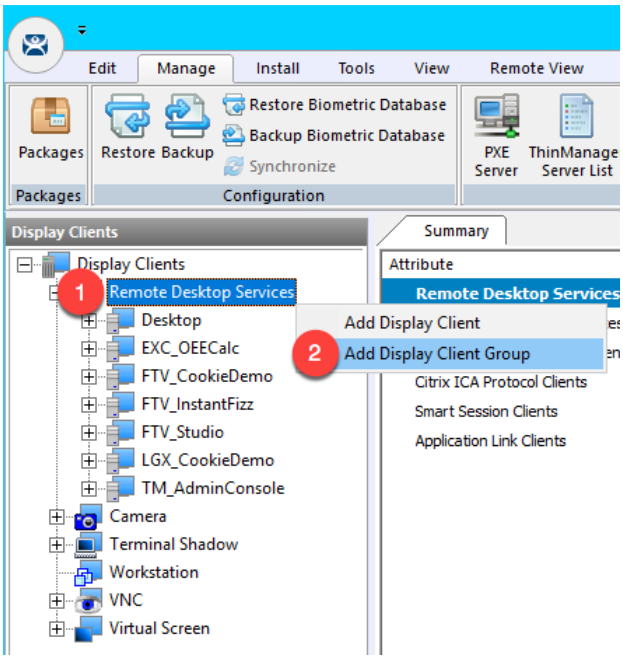
Create Display Clients for SmartSession

To demonstrate, we will assign six **FactoryTalk View SE Display Clients** configured for **SmartSession** to the virtual thin client. The end result will be three sessions running on RDS1 and three running on RDS2.

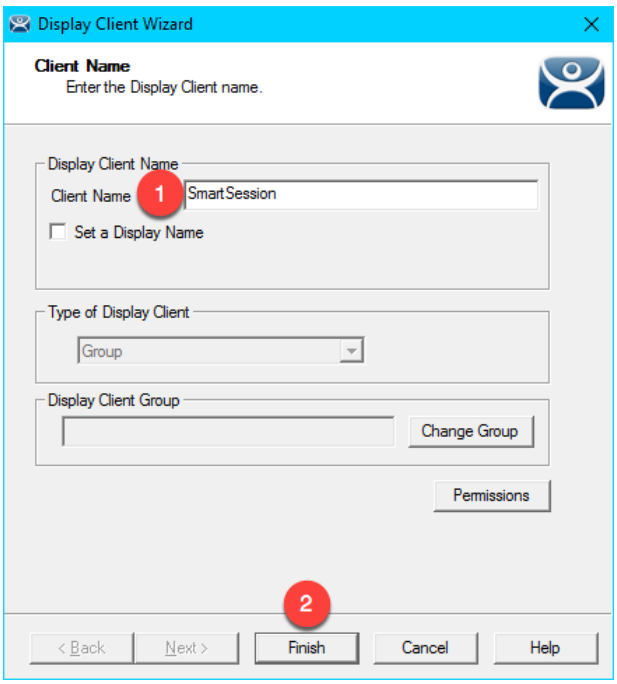
1. From ThinManager, click the **Display Clients** tree selector.



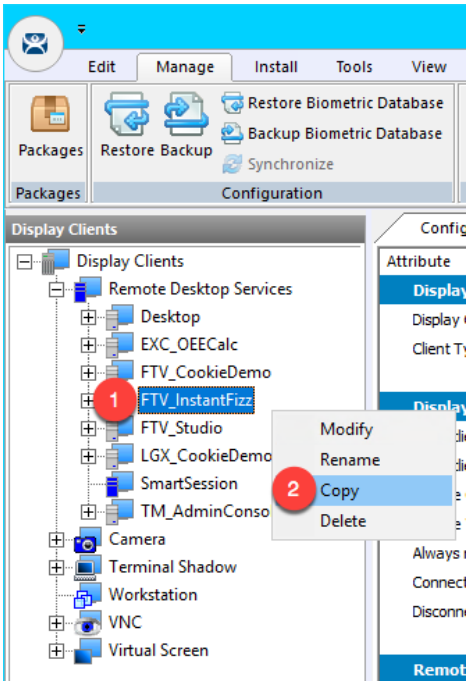
2. First, let's create a **Display Client Group** for our new **SmartSession Display Clients**. Right click the **Remote Desktop Services** tree item and select **Add Display Client Group**.



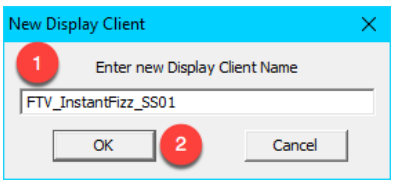
3. From the **Client Name** page of the wizard, enter *SmartSession* as the **Client Name**. Click the **Finish** button.



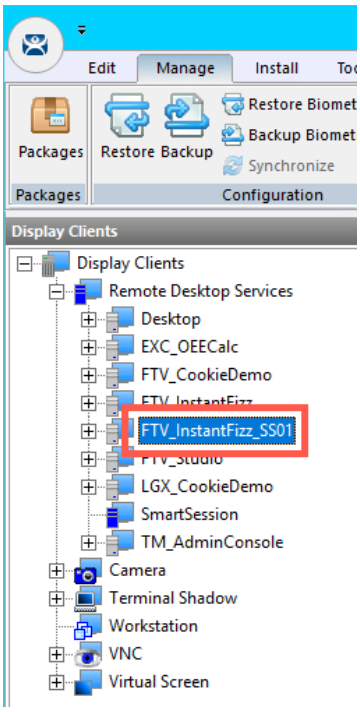
4. Since the **FTV_InstantFizz Display Client** is most like the new **Display Client** we want to create, right click it and select **Copy**.



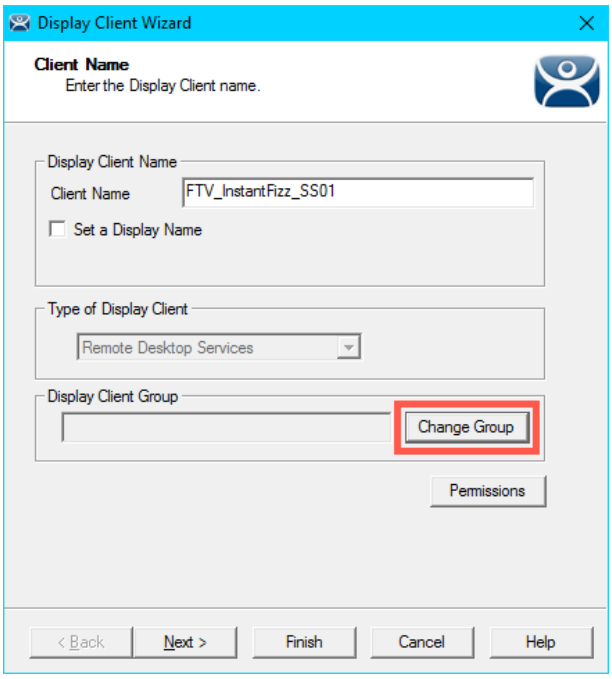
5. From the **New Display Client** dialog box, enter *FTV_InstantFizz_SS01* and click the **OK** button.



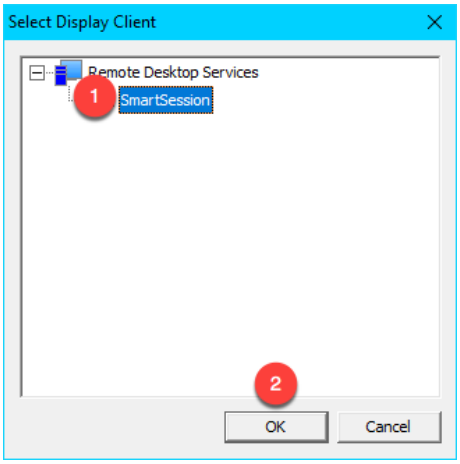
6. Double click newly created **FTV_InstantFizz_SS01 Display Client**.



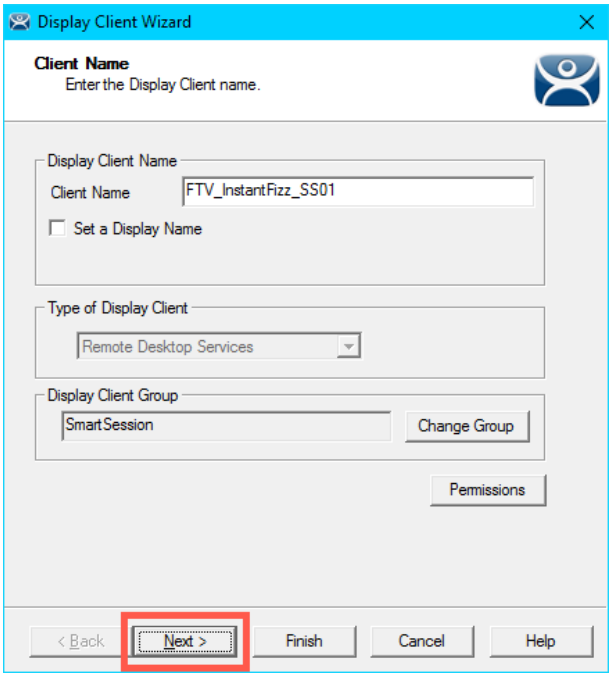
7. From the **Client Name** page of the wizard, click the **Change Group** button.



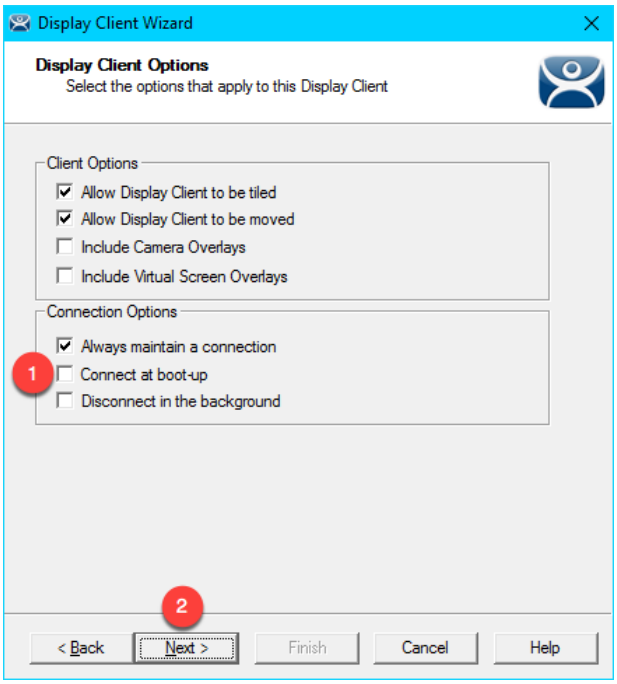
8. From the **Select Display Client** window, select the **SmartSession Display Client Group** and click the **OK** button.



9. Back at the **Client Name** page of the wizard, click the **Next** button.

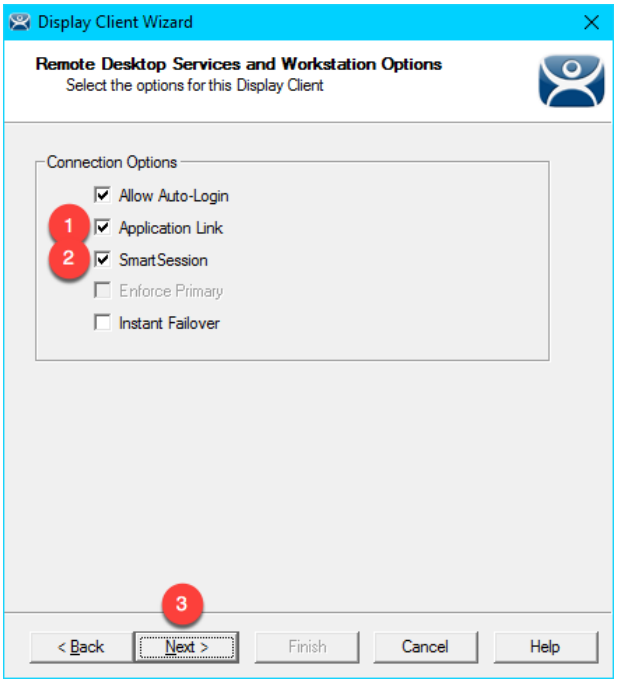


10. From the **Display Client Options** page of the wizard, **un**-check the **Connect at boot-up** checkbox. Click the **Next** button.



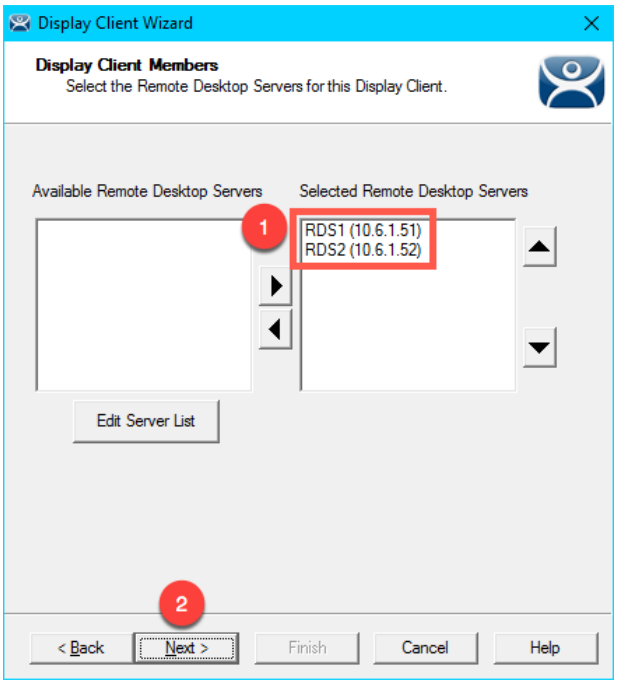
> The **Connect at boot-up** checkbox controls whether the **Display Client** will automatically connect and initiate a Remote Desktop Server session when the terminal boots up. We don't want this to happen in this section because we want to control the timing of when the **Display Clients** launch to demonstrate **SmartSession**.

11. From the **Remote Desktop Services and Workstation Options** page of the wizard, make sure the **Application Link** checkbox and the **Smart Session** checkbox are both checked. Click the **Next** button.

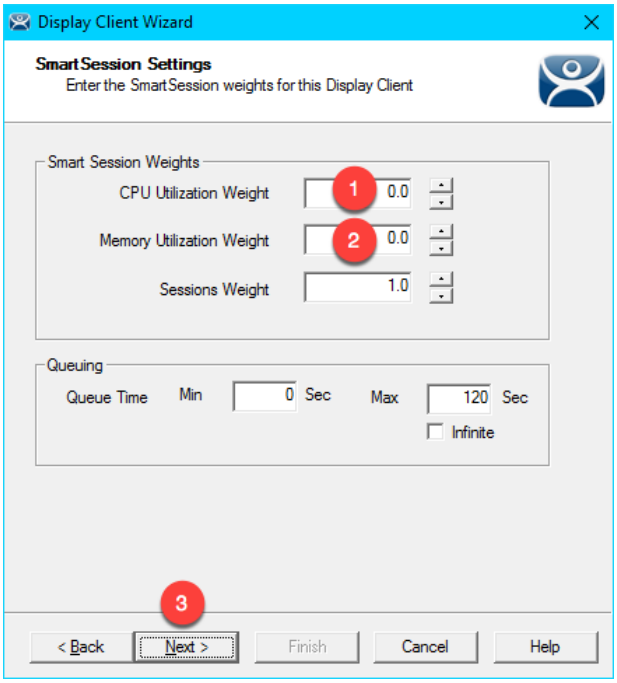


12. Click the **Next** button on the **Session Resolution / Scaling Options** page of the wizard.

13. From the **Display Client Members** page of the wizard, move both **RDS1** and **RDS2** to the **Selected Remote Desktop Servers** listbox. Click the **Next** button.



14. We will adjust the **SmartSession Weights** to affect how the load is calculated for this **Display Client**. Enter a *0.0* for the **CPU Utilization Weight** category and enter a *0.0* for the **Memory Utilization Weight** category. Leave the **Sessions Weight** category at 1.0. Click the **Finish** button. By setting the CPU and Memory weights to 0.0 in the previous step, we will only use **number of sessions** to determine load. The default behavior is to equally factor CPU and memory utilization into the equation as well, however we will modify the weights in this way to put more emphasis on number of sessions.



The formula that ThinManager uses to calculate **SmartSession** load balancing per application is

SmartSession Load = (CPU weight **X** the CPU Use **%) + (**Memory weight **X** Memory Use **%) + (**Session weight **X** Session Number **%)**

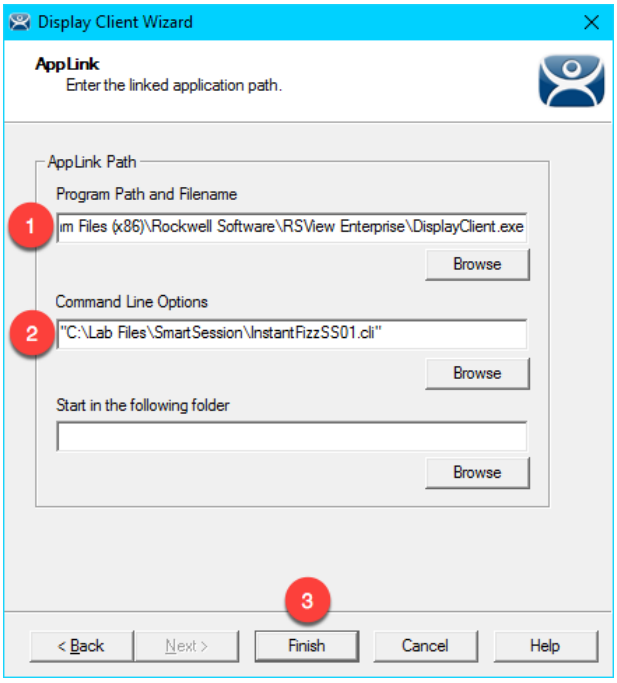
15. From the **AppLink** page of the wizard, enter the following path for the **Program Path and Filename** field and **Command Line Options** field and click the **Finish** button (you can also copy and paste these paths from the **LabPaths.txt** file by right clicking the **Notepad** icon pinned to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

    Program Path and Filename:

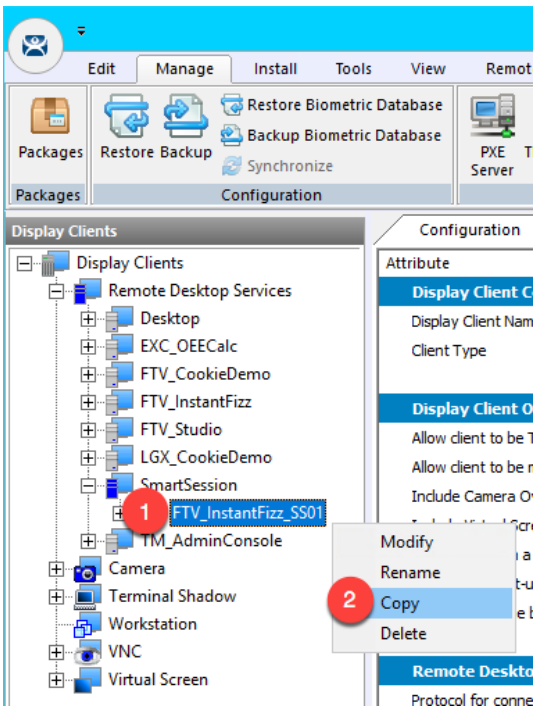
    `C:\Program Files (x86)\Rockwell Software\RSView Enterprise\DisplayClient.exe`

    Command Line Options:

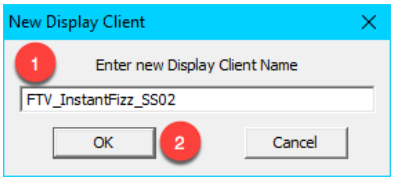
    `"C:\Lab Files\SmartSession\InstantFizzSS01.cli"`



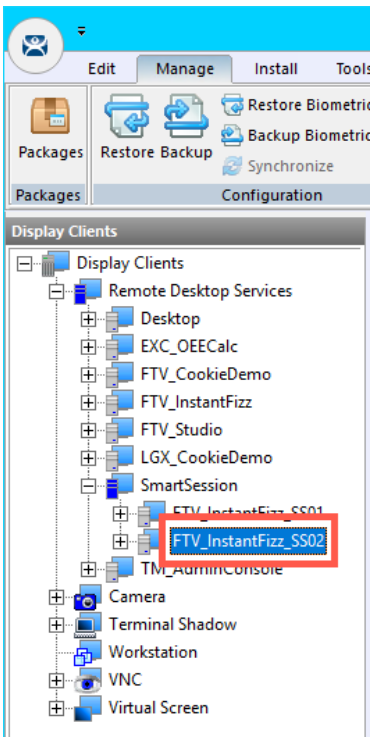
16. Right click the **FTV_InstantFizz_SS01 Display Client** and choose **Copy**.



17. From the **New Display Client** dialog, enter *FTV_InstantFizz_SS02* and click the **OK** button.



18. Double click the **FTV_InstantFizz_SS02 Display Client**.



19. From the **Client Name** page of the wizard, click the **Next** button.
20. From the **Display Client Options** page of the wizard, click the **Next** button.
21. From the **Remote Desktop Services and Workstation Options** page of the wizard, click the **Next** button.
22. From the **Screen Resolution / Scaling Options** page of the wizard, click the **Next** button.
23. From the **Display Client Members** page of the wizard, click the **Next** button.

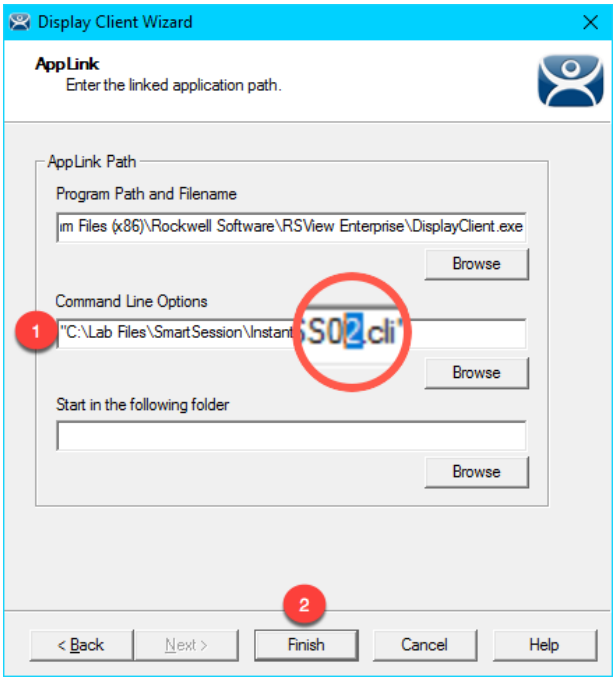
24. From the **AppLink** page of the wizard, update the **Command Line Options** per below and click the **Finish** button (you can also copy and paste this path from the **LabPaths.txt** file by right clicking the **Notepad** icon pinned to the start bar and selecting **LabPaths.txt**):

Program Path and Filename:

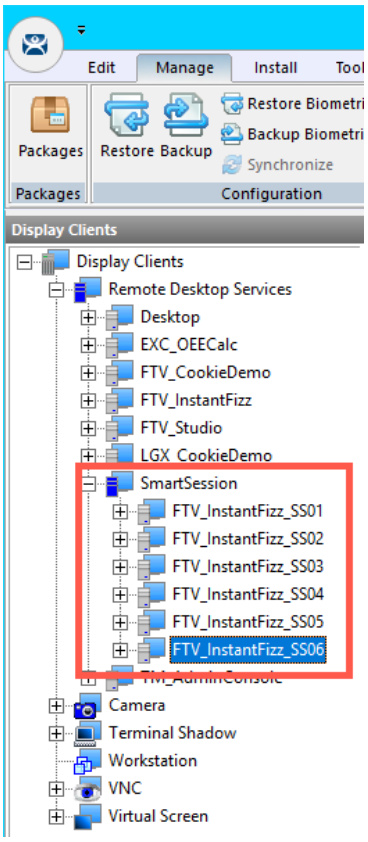
```
C:\Program Files (x86)\RSView Enterprise\DisplayClient.exe
```

Command Line Options:

```
"C:\Lab Files\SmartSession\InstantFizzSS02.cli"
```



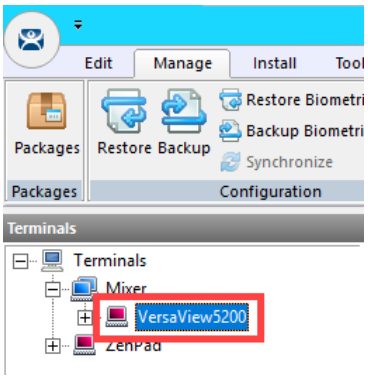
25. Repeat steps 16-24 to create 4 more Display Clients: **FTV_InstantFizz_SS03**, **FTV_InstantFizz_SS04**, **FTV_InstantFizz_SS05** and **FTV_InstantFizz_SS06**. When complete, you should have **Display Client Group** called **SmartSession**, with 6 **Display Clients** inside it.



Assign Display Clients with SmartSession to Terminal

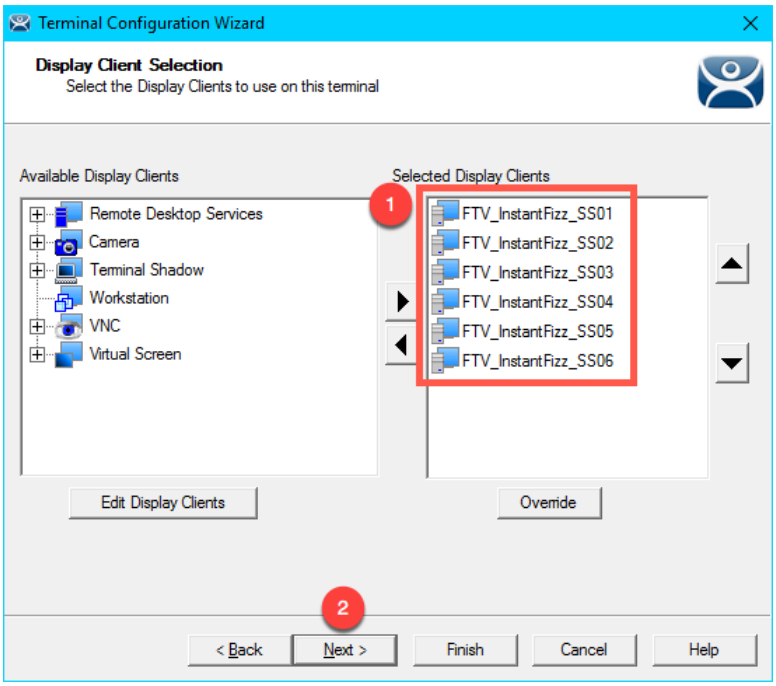
1. Click the **Terminals** tree selector icon.

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

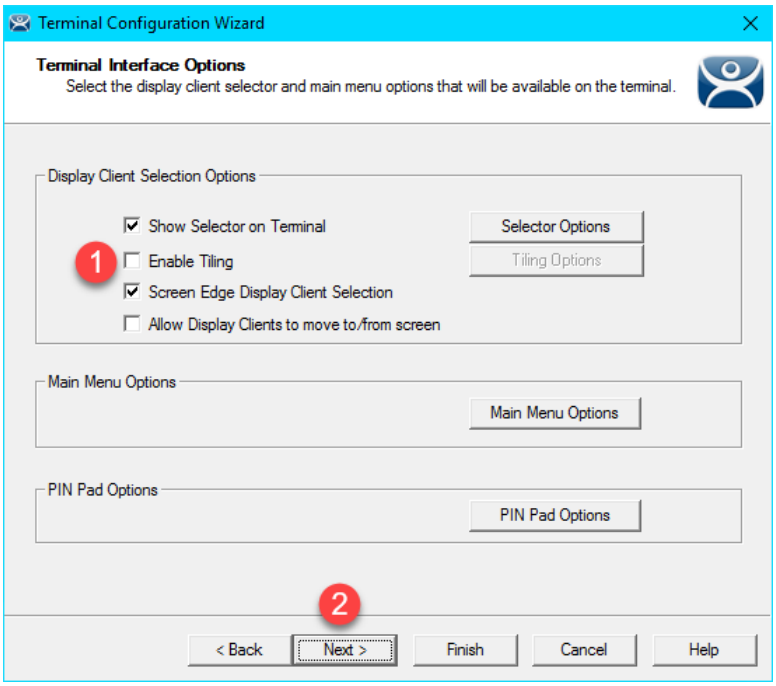


3. Click the **Next** button on the **Terminal Name** page of the wizard.
4. Click the **Next** button on the **Terminal Hardware** page of the wizard.
5. Click the **Next** button on the **Terminal Options** page of the wizard.
6. Click the **Next** button from the **Terminal Mode Selection** page of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

7. On the **Display Client Selection** page, remove any existing **Display Clients** and assign each of the **FTV_InstantFizz_SS0x Display Clients** to the **Selected Display Clients** list box. Click the **Next** button.

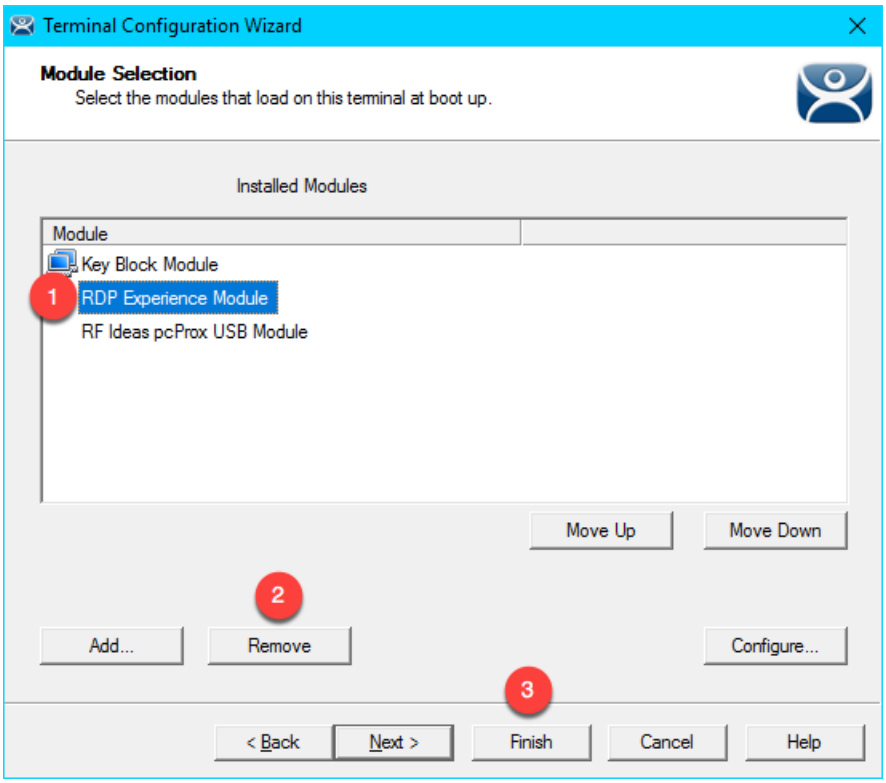


8. From the **Terminal Interface Options** page of the wizard, **<u>un-check</u>** the **Enable Tiling** checkbox. Click the **Next** button.



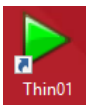
9. Click the **Next** button on the **Hotkey Configuration** page of the wizard.
10. Click the **Next** button on the **Log In Information** page of the wizard.
11. Click the **Next** button on the **Video Resolution** page of the wizard.

12. From the **Module Selection** page of the wizard, select the **RDP Experience Module** and click the **Remove** button. Click the **Finish** button.

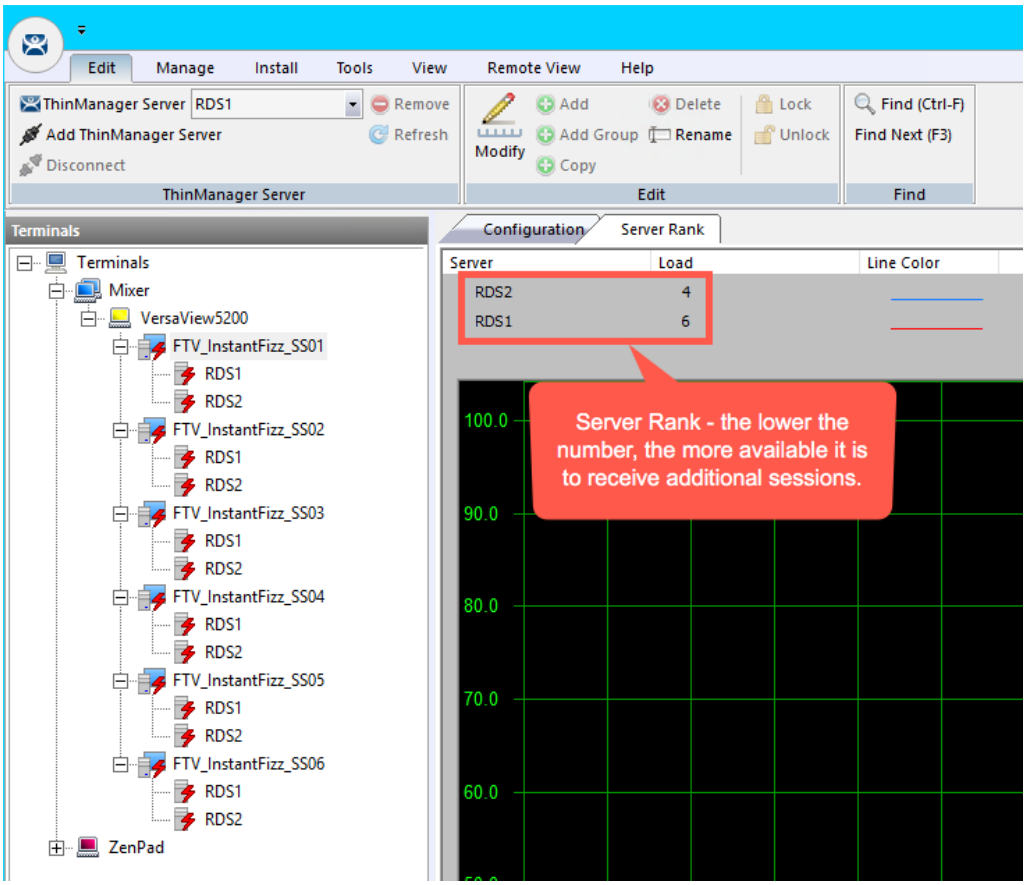


We previously used the **RDP Experience Module** as an alternative way to stagger the starting of multiple sessions on the virtual thin client using the **Duplicate Server Connect Delay (seconds)** property. In general, a non-zero value for this property can result in unexpected results with **SmartSession**.

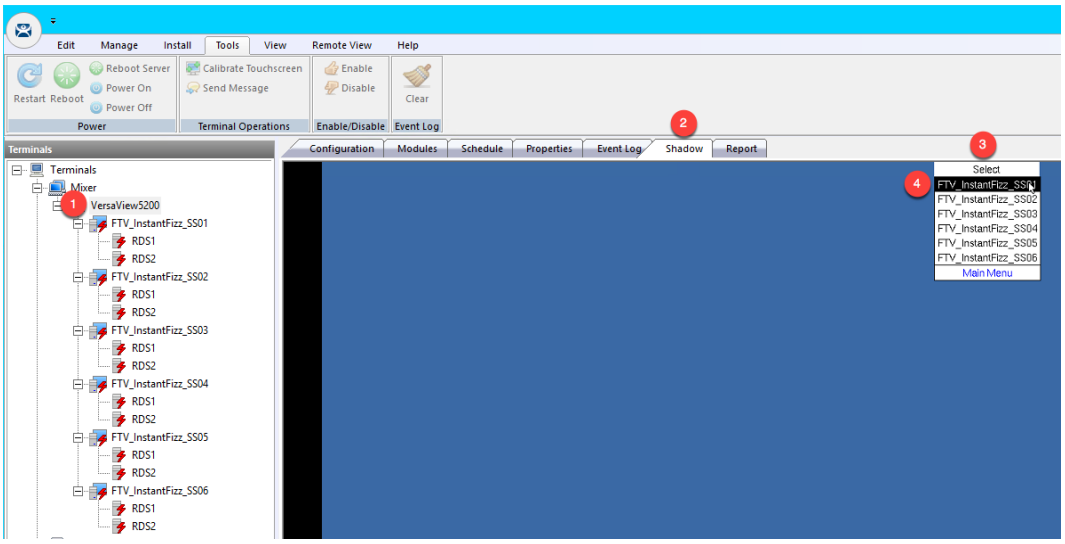
13. Double click the **Thin01** shortcut on the **RDS1** desktop to launch the virtual thin client.



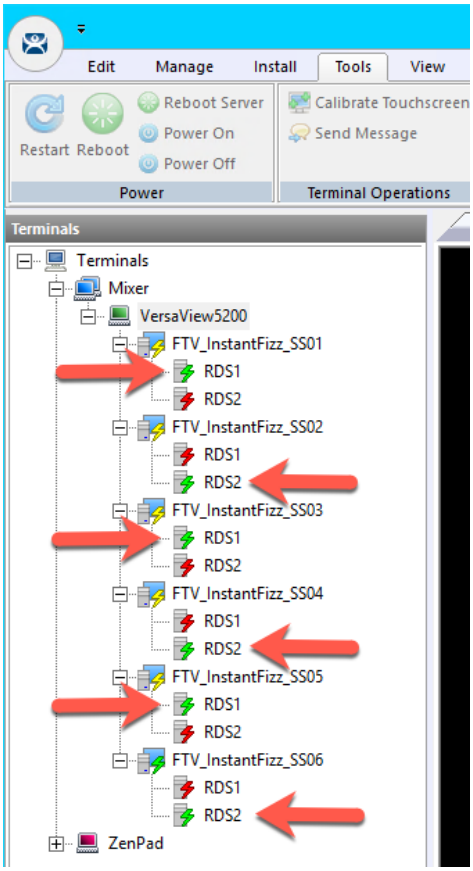
14. While the **VersaView5200** terminal boots, click the plus next to each of the **FTV_InstantFizz_SS0x Display Clients** to enable viewing of the **RDS1** and **RDS2** servers. Select the **FTV_InstantFizz_SS01 Display Client** and then click the **Server Rank** tab. This console view will allow you to monitor how the six **Display Clients** are distributed across the **RDS1** and **RDS2 Display Servers**. Only **FTV_InstantFizz_SS01** was configured to automatically start. The remaining **InstantFizzSS0x Display Clients** were configured not to **Connect at boot-up** (this is configured in the **Display Client Wizard**). This was done in order to stagger the connections of the **Display Clients**. **RDS1** should have a higher rank initially since you are connected to it via **RDP** for your remote session.



15. From the virtual thin client or a shadow of **VersaView5200**, click and hold the **DisplayClient Selector** and hover over **FTV_InstantFizz_SS01** and release your mouse button to launch it.

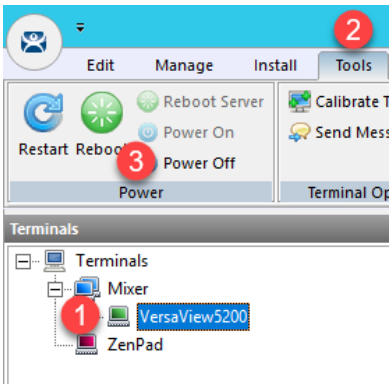


16. Repeat the process in the previous step by selecting the other **Display Clients** to launch them, waiting a few seconds in between. You should see the **Display Clients** alternate between **RDS1** and **RDS2** as **Smart Session** attempts to balance the load based on number of sessions running on each.

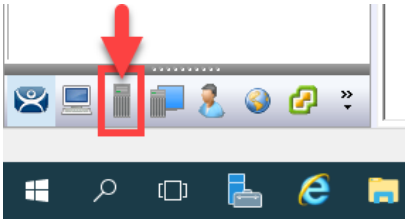


Power off Terminal and Reset Sessions

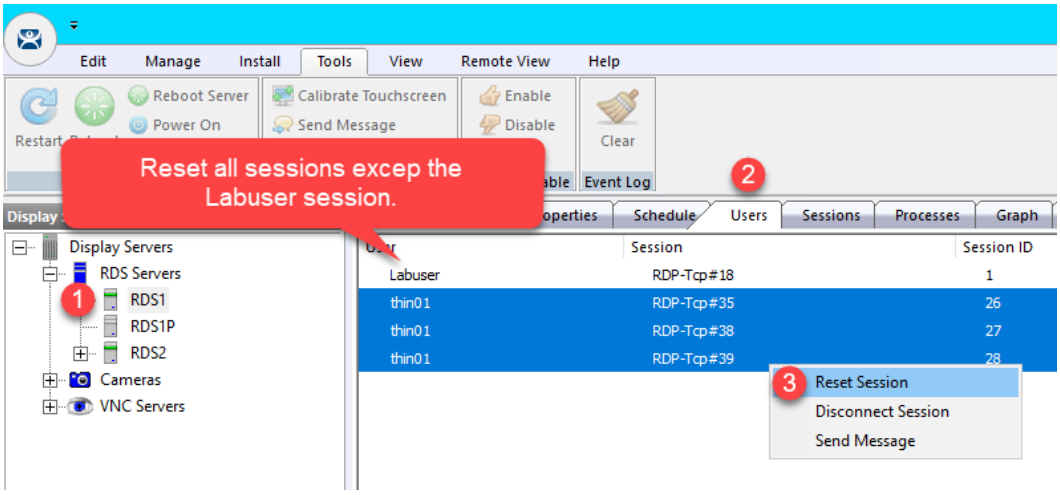
1. Power off the virtual thin client by selecting the **VersaView5200** terminal, followed by the **Tools** ribbon, then click the **Power Off** icon.



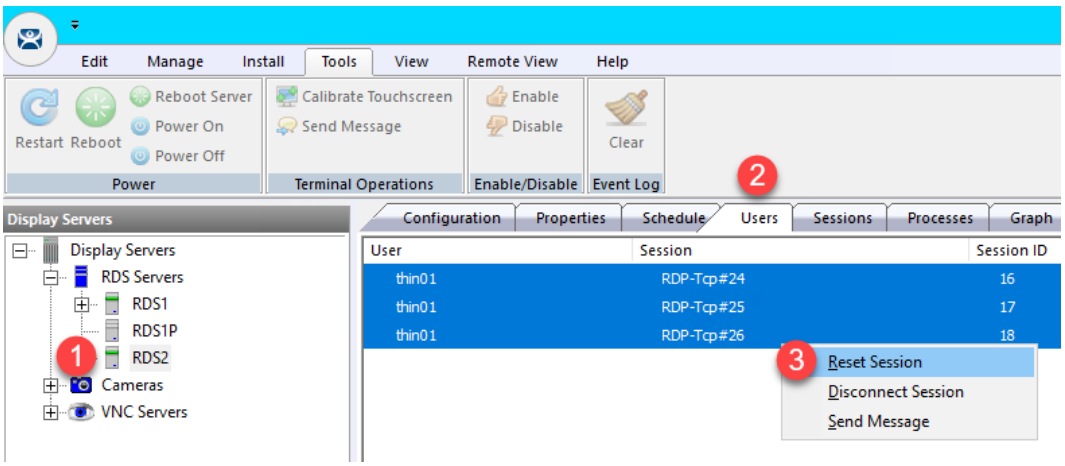
2. Navigate to the **Display Servers** tab in the ThinManager Administration Console.



3. Expand **RDS Servers,** select **RDS1** and click the **Users** tab. Select all of the user sessions except for the **Active labuser** user (this is your session into RDS1), right click and select **Reset Session**.

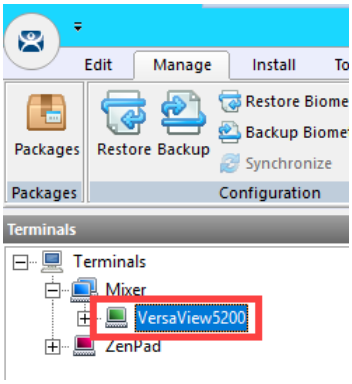


4. Now select **RDS2** and click the **Users** tab. Reset all sessions.



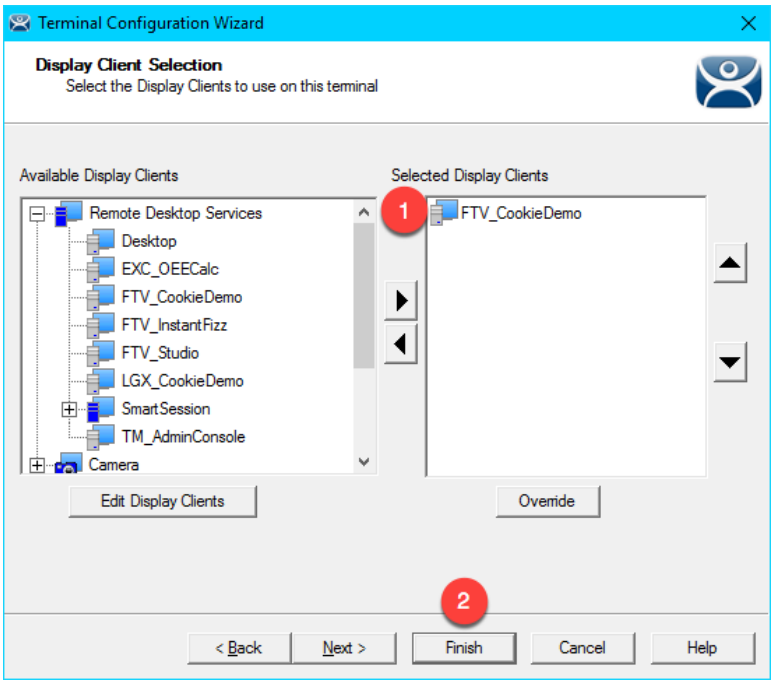
5. Click the **Terminals** tree selector icon.

6. Double click the **VersaView5200** terminal.



7. Click the **Next** button on the **Terminal Name** page of the wizard.
8. Click the **Next** button on the **Terminal Hardware** page of the wizard.
9. Click the **Next** button on the **Terminal Options** page of the wizard.
10. Click the **Next** button on the **Terminal Mode Selection** page of the wizard.

11. From the **Display Client Selection** page of wizard, remove all of the **Display Clients** from the **Selected Display Clients** list. Select the **FTV_CookieDemo 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.



This completes the section **RDS Load Balancing with ThinManager SmartSession** of the lab. Please continue on to the **Language Support** section of the lab.

Section 16: Language Support

Overview

Prior to version 11, **ThinManager** offered multi-language support only **within** **Remote Desktop Server** sessions delivered to **ThinManager-managed terminals**. This was accomplished using the **Keyboard Configuration Module** which supports 43 different languages. However, this **module** only permits localized keyboard entry **within** the **Remote Desktop Server session**. This means that only **English** keyboards are supported within ThinManager firmware dialog boxes with this module – like **Relevance User** login prompts, etc. Similarly, object names for **Terminals, Display Clients**, etc. within the **ThinManager Admin Console** could only be named with English characters. These localization limitations have been greatly improved with the release of ThinManager v11.

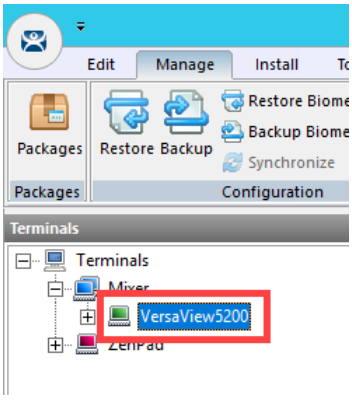
1. Keyboard Configuration Module
2. Default Language Selection and Firmware Package 8.2
3. Terminal Language Selection
4. Remove Language Selection Module

Keyboard Configuration Module

As previously mentioned, the **Keyboard Configuration Module** enables a ThinManager managed thin client to support non-English keyboard input, but only within Remote Desktop Server sessions. This section will show how to apply and configure the **Keyboard Configuration Module** for this purpose, but since we only have English keyboards at your lab stations, we will be unable to demonstrate the results. The **Keyboard Configuration Module** does **not** require ThinManager v11.

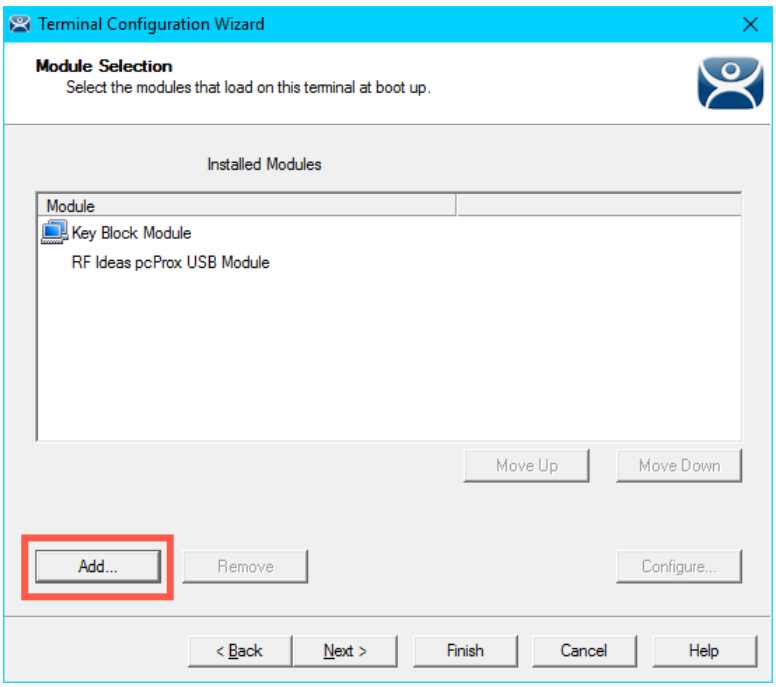
1. Click the **Terminals** tree selector icon.

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

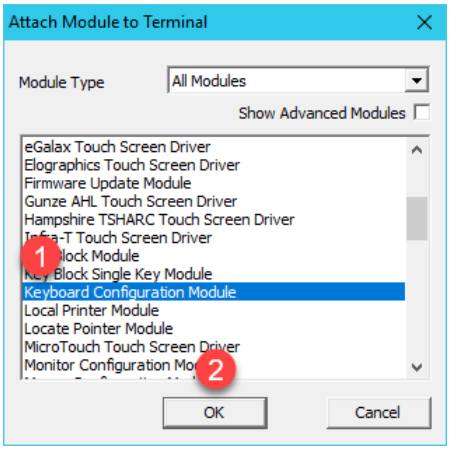


3. Click the **Next** button on the **Terminal Name** page of the wizard.
4. Click the **Next** button on the **Terminal Hardware** page of the wizard.
5. Click the **Next** button on the **Terminal Options** page of the wizard.
6. Click the **Next** button on the **Terminal Mode Selection** page of the wizard.
7. Click the **Next** button on the **Display Client Selection** page of the wizard.
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. Click the **Next** button on the **Log In Information** page of the wizard.
11. Click the **Next** button on the **Video Resolution** page of the wizard.

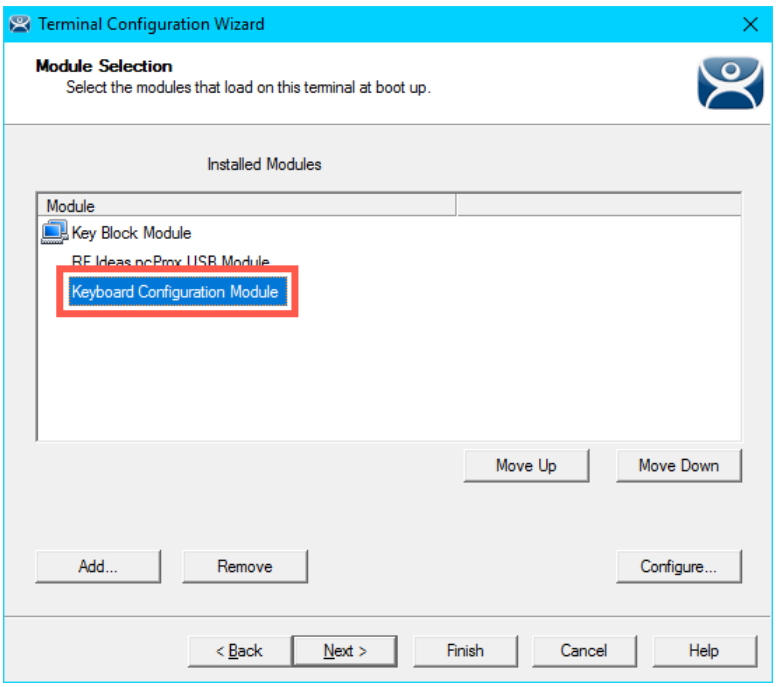
12. Click the **Add…** button on the **Module Selection** page of the wizard.



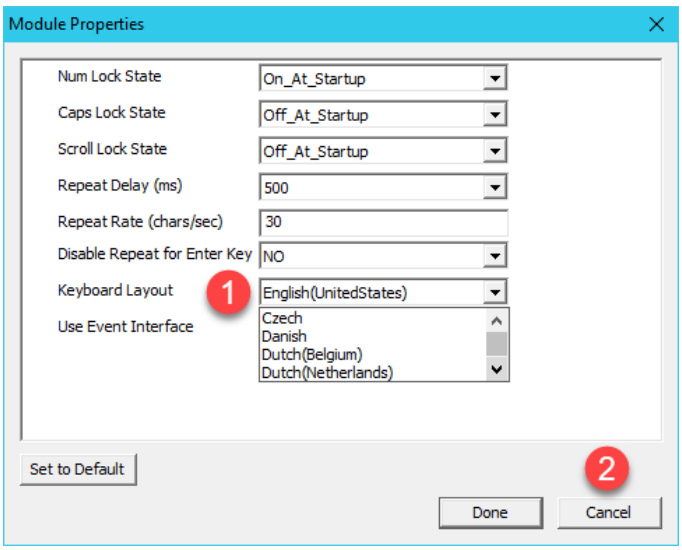
13. From the **Attach Module to Terminal** window, select the **Keyboard Configuration Module** and click the **OK** button.



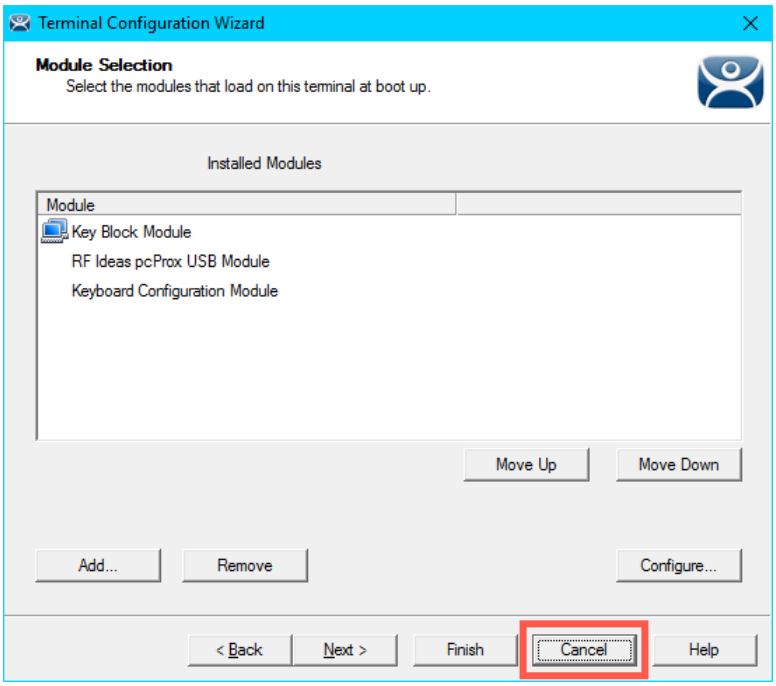
14. Back at the **Module Selection** page of the wizard, double click the **Keyboard Configuration Module**.



15. From the **Module Properties** window, you will see that you can set general keyboard properties for the terminal. Click the **Keyboard Layout** drop down list and review the available languages. Just to reiterate, selecting a language from this drop down list will support that language within any Remote Desktop Server sessions delivered to the ThinManager-managed terminal to which this module is applied. Click the **Cancel** button.



16. Again, since we have an English keyboard connected to our virtual thin client, we cannot see the results of selecting a different language, so click the **Cancel** button.



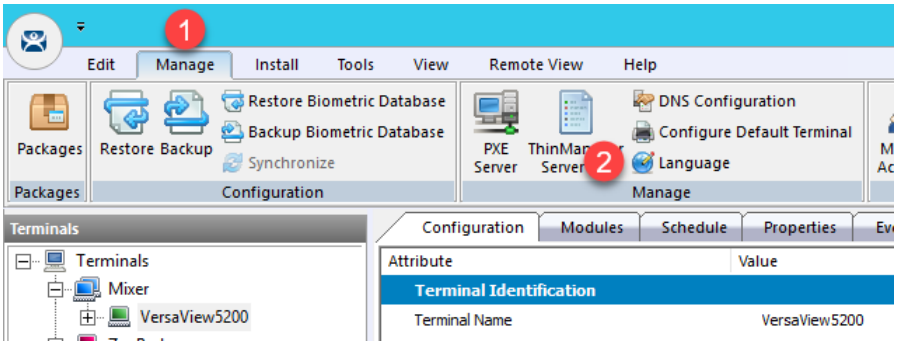
Default Language Selection and Firmware Package 8.2

With ThinManager v11, the Windows components of ThinManager and associated Firmware Package (8.2 or newer) have been updated to accept Unicode characters, enabling broader support for non-English characters. With ThinManager 11.0 and Firmware Package 8.2, a new **Language Selection Module** enables support for the following languages:

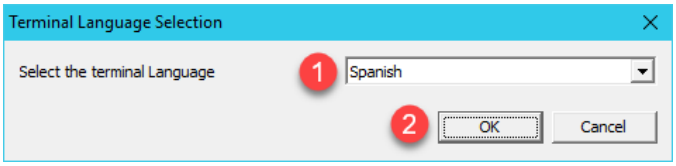
- French
- French (Swiss)
- German
- German (Swiss)
- Russian
- Spanish

Unlike the **Keyboard Configuration Module**, the **Language Selection Module** will allow you to enter any of these Languages listed above not only within the **Remote Desktop Server session** but also within ThinManager firmware specific input fields, like **Relevance User Services** username and password fields. With **Firmware Package 8.2**, the **On-Screen Keyboard Configuration Module** has been updated to support these languages as well. With regard to Interactive Shadowing from the Admin Console, if your ThinManager Host Operating System is set to the same language as the Terminal being shadowed, you will be able to provide keyboard input via an interactive shadow in the Languages listed above seamlessly into both Remote Desktop Server sessions as well as ThinManager firmware specific input fields. Lastly, ThinManager 11.0 with Firmware Package 8.2 supports non-English characters for ThinManager objects like Display Servers, Display Clients, Terminals, Locations, etc. While we will continue to add support for additional languages, if you need support for a language that is not provided, you may still use the **Keyboard Configuration Module**, but this would limit language support to within the Remote Desktop Server sessions as explained in the previous section.

1. Let's set the default language for all of the terminals configured to run **Firmware Package 8.2** or newer. From the **ThinManager Admin Console**, select the **Manage** ribbon followed by the **Language** icon.

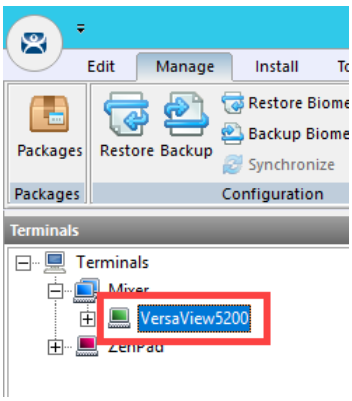


2. From the **Terminal Language Selection** window, select **Spanish** from the drop down list and click the **OK** button.



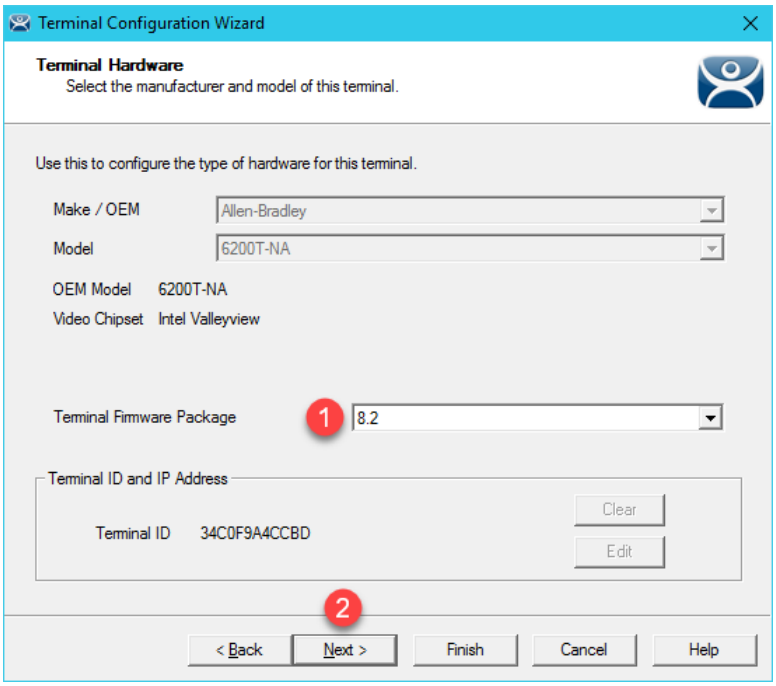
> The **Terminal Language** drop down list will only be populated with languages if you are running ThinManager 11 and have **Firmware Package 8.2** or newer installed.

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. From the **Terminal Hardware** page of the wizard, click the **Terminal Firmware Package** drop down list and select **8.2**. Click the **Next** button.



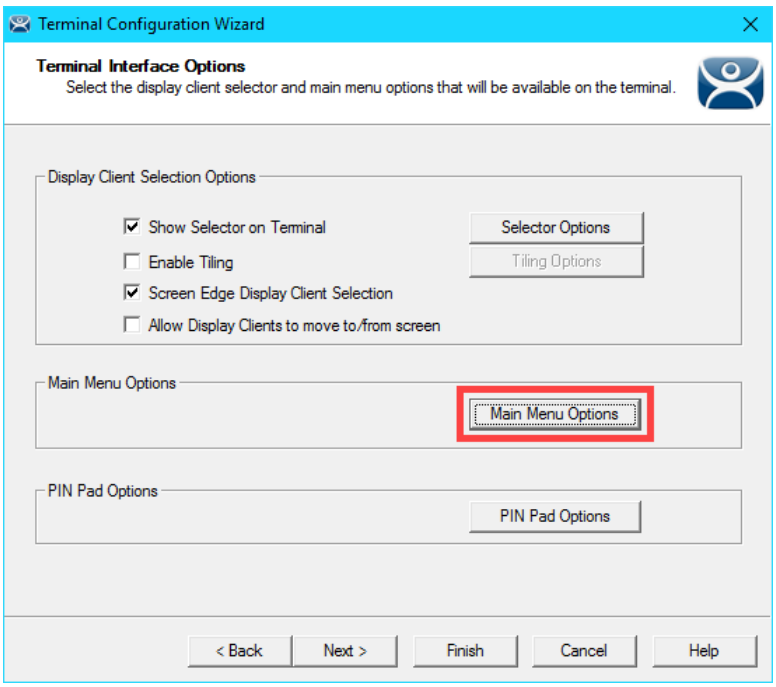
> In **ThinManager**, a **Firmware Package** is a version of **Firmware** along with the **Modules** that are associated with it. As previously mentioned, a **Module** provides some additional functionality to the **Firmware**, like a touchscreen or badge reader driver, etc. Individual Modules can be updated independent of a **Firmware Package**.

6. Click the **Next** button on the **Terminal Options** page of the wizard.

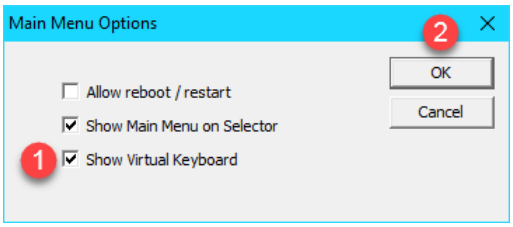
7. Click the **Next** button on the **Terminal Mode Selection** page of the wizard.

8. Click the **Next** button on the **Display Client Selection** page of the wizard.

9. From the **Terminal Interface Options** page of the wizard, click the **Main Menu Options** button.

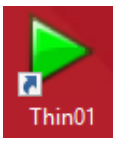


10. From the **Main Menu Options** window, check the **Show Virtual Keyboard** checkbox. Click the **OK** button, followed by the **Finish** button.

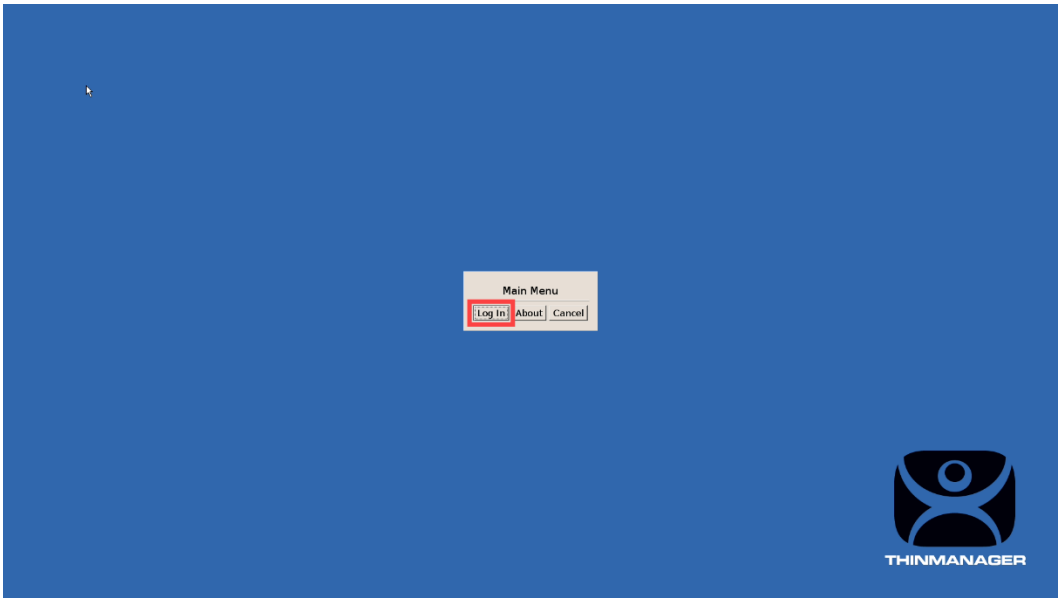


The **Virtual Keyboard** will automatically popup when an input from the ThinManager firmware is required (i.e.: Relevance User username or password entry).

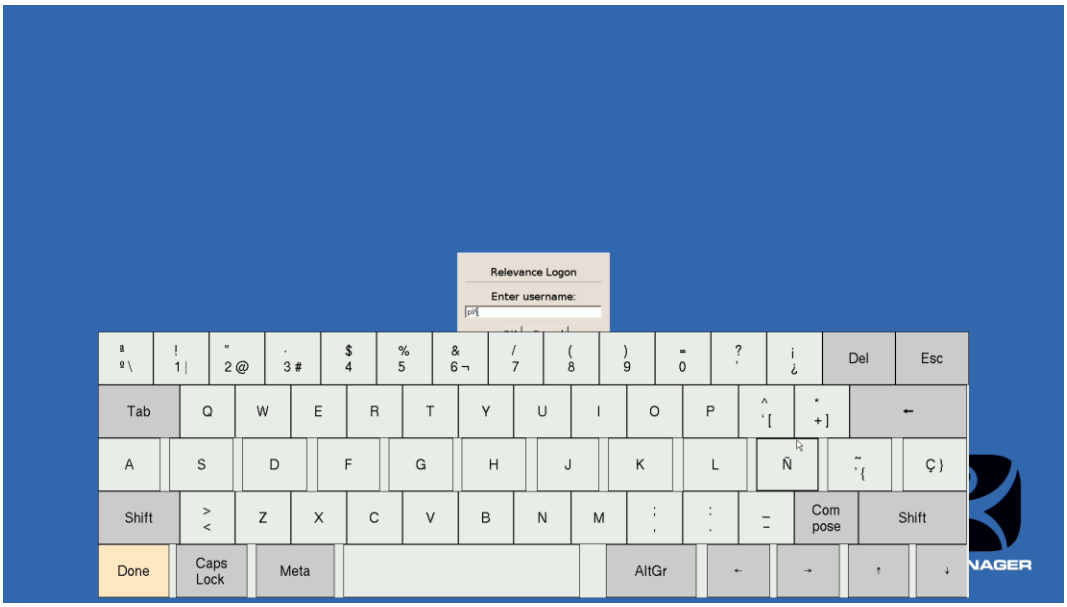
11. Double click the virtual thin client **Thin01** from your desktop to launch it.



12. Once the **VersaView5200** terminal reboots, hit **CTRL-m** on the keyboard either on the virtual thin client or a shadow of it to launch the terminal's **Main Menu**. Touch the **Log In** button.



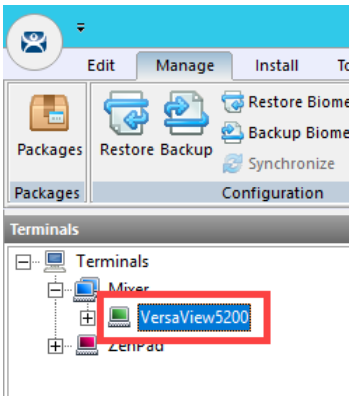
13. This should launch a **Spanish On Screen Keyboard** and allow you to enter a non-English character as part of the **Relevance Username**. After a few seconds, the **Relevance Logon** dialog box will time out.



Terminal Language Selection

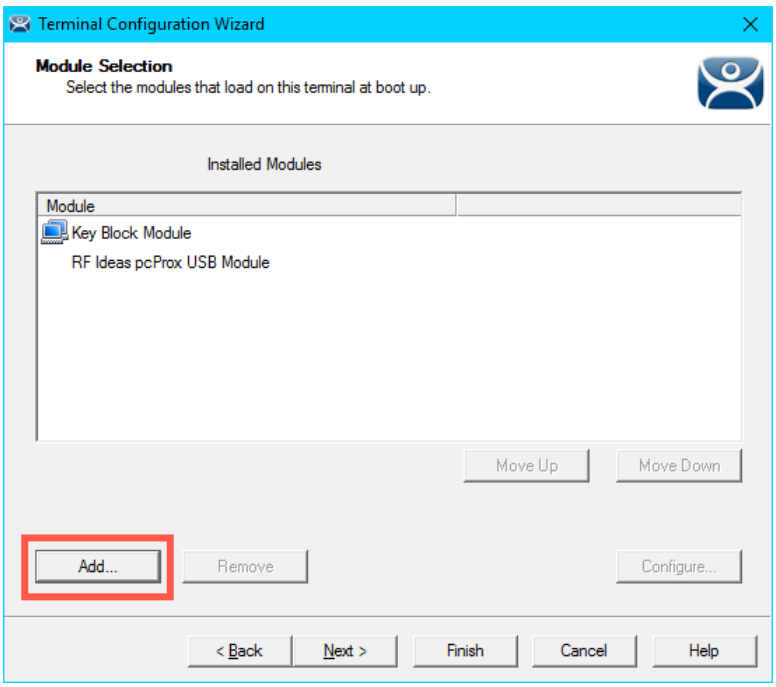
If you need to assign different languages to different terminals, this can be accomplished using the **Language Selection Module** which is included in **Firmware Package 8.2**.

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

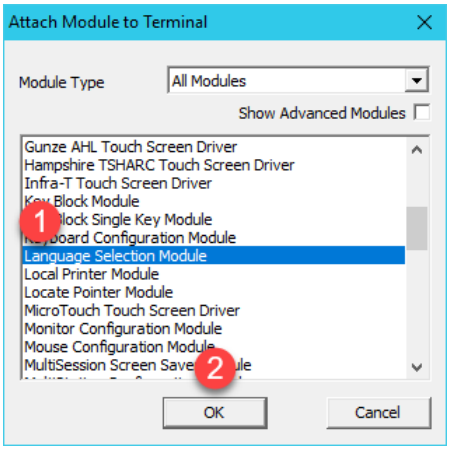


2. Click the **Next** button on the **Terminal Name** page of the wizard.
3. Click the **Next** button on the **Terminal Hardware** page of the wizard.
4. Click the **Next** button on the **Terminal Options** page of the wizard.
5. Click the **Next** button on the **Terminal Mode Selection** page of 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 on the **Log In Information** page of the wizard.
10. Click the **Next** button on the **Video Resolution** page of the wizard.

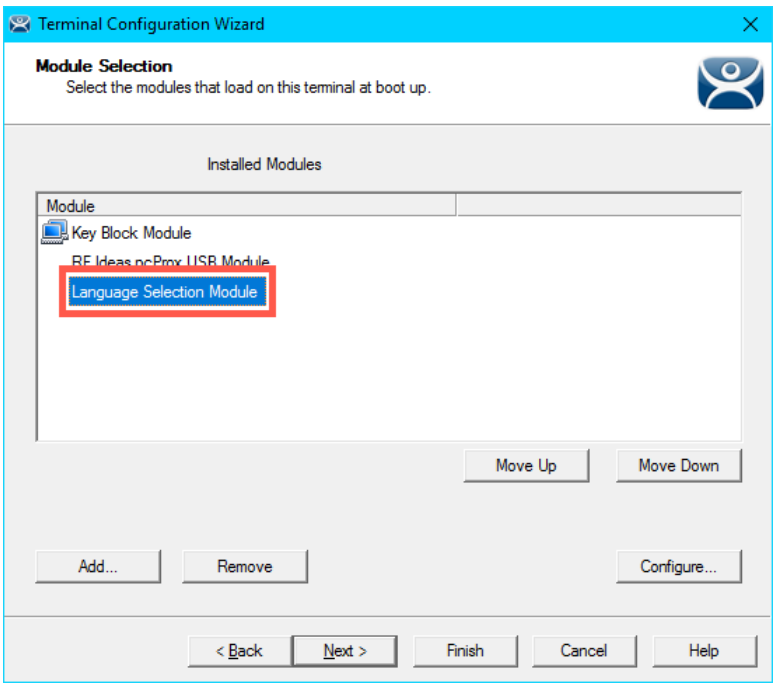
11. From the **Module Selection** page of the wizard, click the **Add…** button.



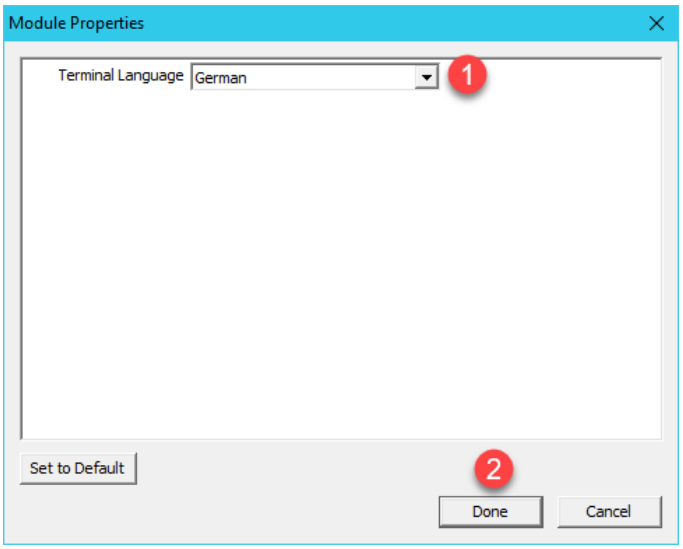
12. From the **Attach Module to Terminal** window, select the **Language Selection Module**.



13. Back at the **Module Selection** page of the wizard, double click the **Language Selection Module**.

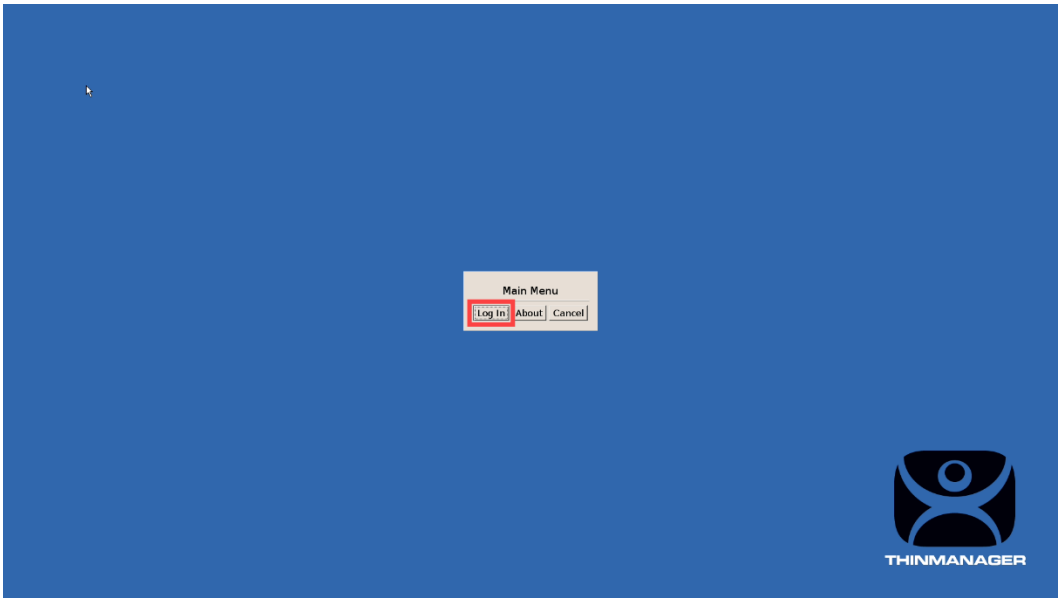


14. From the **Module Properties** window, select **German** from the **Terminal Language** drop down list and click the **Done** button, followed by the **Finish** button.

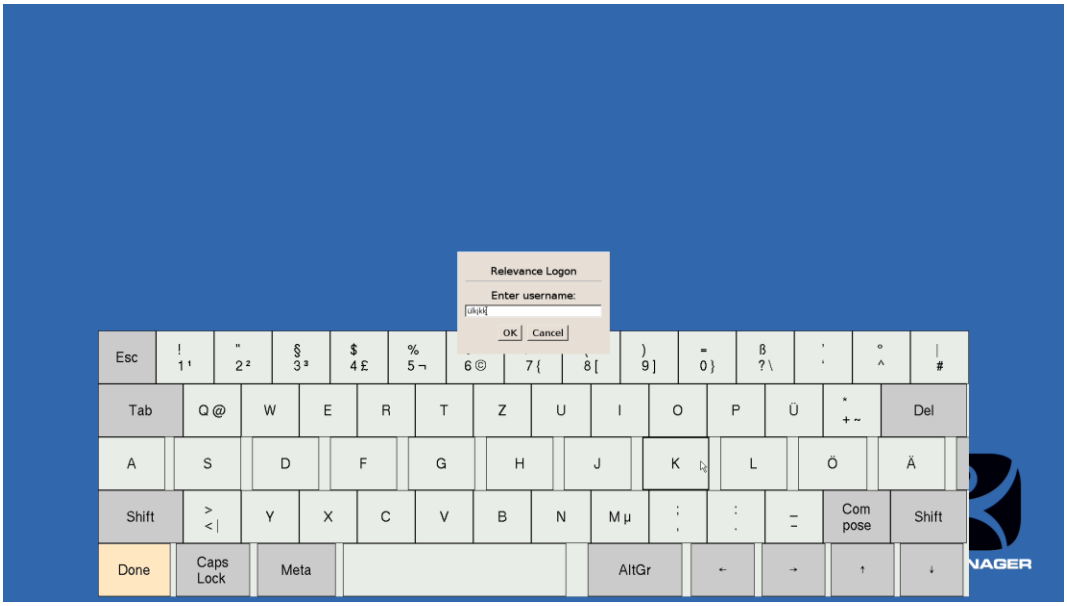


As previously noted, the **Language Selection Module** is only available on terminal's that have **Firmware Package 8.2** or newer applied to them.

15. Right click the **VersaView5200** terminal from the **Terminals** tree and select **Restart Terminal** to apply the changes. Click **Yes** to the confirmation dialog.
16. Once the terminal restarts, hit CTRL-m on the keyboard at the virtual thin client to launch the terminal's **Main Menu**. Touch the **Log In** button.



17. This should launch a **German On Screen Keyboard** and allow you to enter a non-English character as part of the **Relevance Username**. After a few seconds, the **Relevance Logon** dialog box will time out.



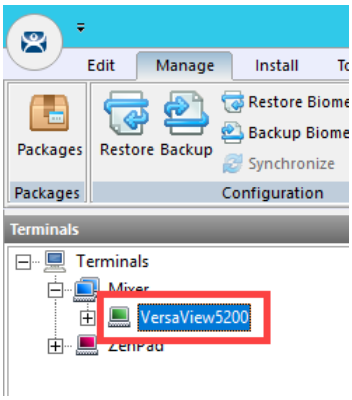
Also as previously mentioned, additional languages will continue to be added to the new **Language Selection** capability that is part of ThinManager v11. Additional languages will be added to **Firmware Packages 8.2** or newer and will be deployable by simply downloading, installing and deploying the updated **Firmware Package**.

Please refer to AID1084359 – ThinManager Language Support which summarizes most of the information from this section for future reference and will be updated as new languages are released.

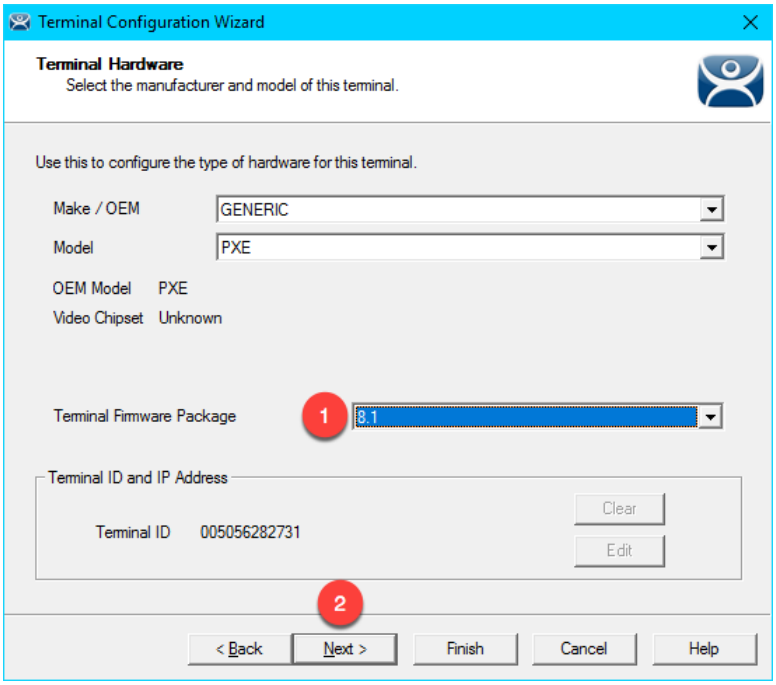
Remove Language Selection Module

We will complete the remaining lab sections with an English keyboard, so we can remove **Firmware Package 8.2** and the **Language Selection Module**.

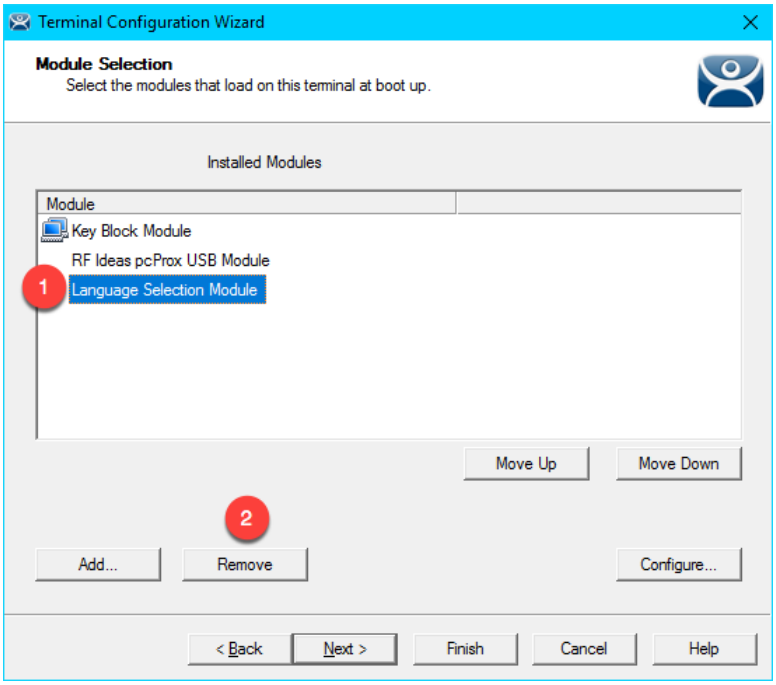
1. From the **Terminals** tree, double click the **VersaView5200** terminal to launch the **Terminal Configuration Wizard**.



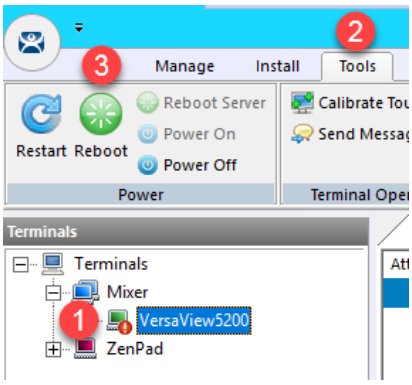
2. Click the **Next** button on the **Terminal Name** page of the wizard.
3. From the **Terminal Hardware** page of the wizard, select **8.1** from the **Terminal Firmware Package** drop down list.



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 on the **Log In Information** page of the wizard.
10. Click the **Next** button on the **Video Resolution** page of the wizard.
11. From the **Module Selection** page of the wizard, select the **Language Selection Module** and click the **Remove** button, followed by the **Finish** button.



12. From the **Terminals** tree, select the **VersaView5200** terminal, followed by the **Tools** ribbon, then click the **Reboot** icon. You can continue to the next section while the terminal completes its reboot process.



This completes the **Language Support** section of the lab. Please continue on to the **Relevance and Geo-Fencing** section of the lab.

Section 17: Relevance Location Services - Geo-Fencing

Overview

Location based content delivery was introduced in the Section 10, where we created a simple **Location Resolver** using a **QR Code**. Scanning the **QR Code** as a member of our Maintenance group delivered Logix Designer with an associated ACD file to our mobile (yet tethered!) device. A **QR Code** is one of four **Location Resolver** technologies currently supported by ThinManager. Additionally, **Bluetooth Beacons**, WiFi Access Points and GPS can be used to define **Locations** in ThinManager. In this section of the lab, we are going to create a **geo-fence** using a **Bluetooth Beacon**, such that certain content will be available within the **geo-fence**, but unavailable outside of it. We are also going to present some unique ways that our tablet can interact with our thin client.

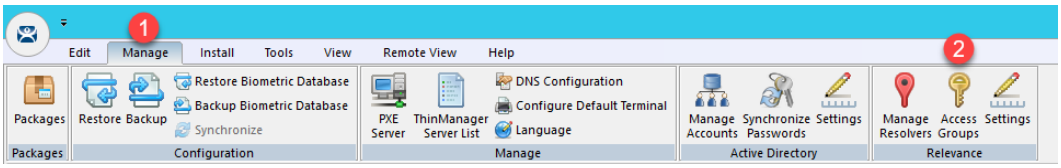
In this section, you will be performing the following tasks:

1. Create a Maintenance Access Group
2. Create a Maintenance User Group
3. Create a Maintenance User
4. Register a Bluetooth Beacon Location Resolver
5. Register a QR Code Location Resolver
6. Create Parent (Geo-Fence) Location
7. Create Child Location
8. Assign Default Location to Terminal
9. Reassign Display Client to Public Display Server
10. See the Results
11. Remove Default Location from Terminal

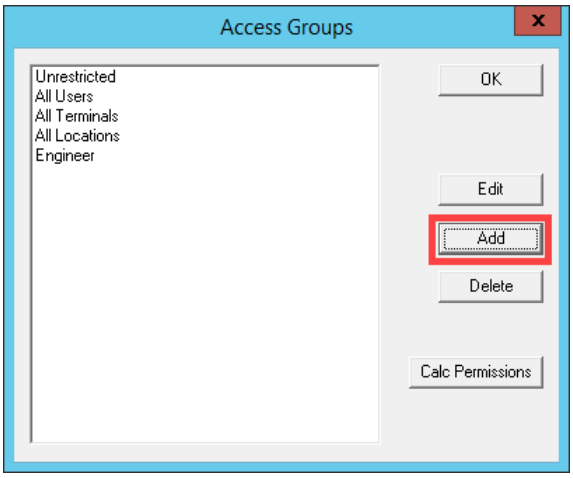
Create Maintenance Access Group

Access Groups are used to control access to **Terminals**, **Display Clients** and/or **Locations**. We previously created an Engineer **Access Group** in the Section 10. We will create another **Access Group** for Maintenance now.

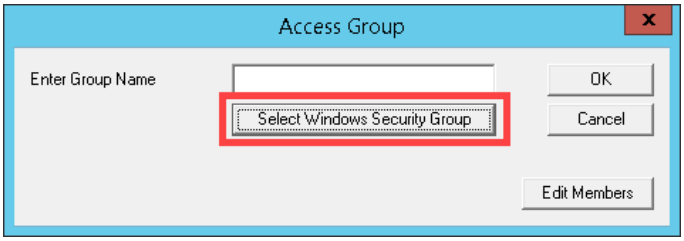
1. Click the **Manage** ribbon, followed by the **Access Groups** icon.



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

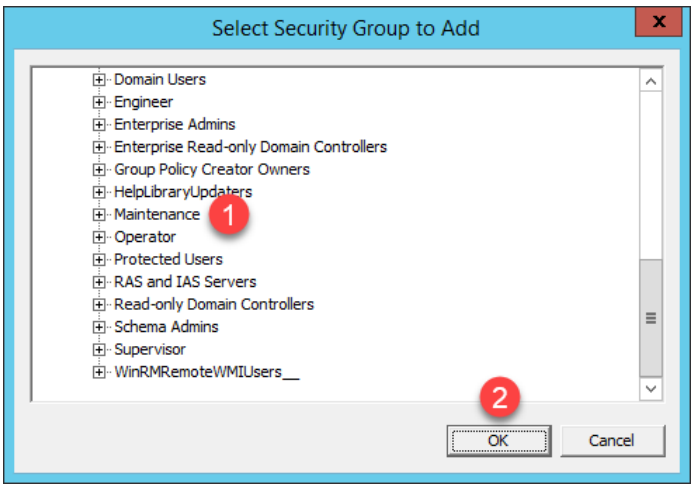


3. Click the **Select Windows Security Group** button.

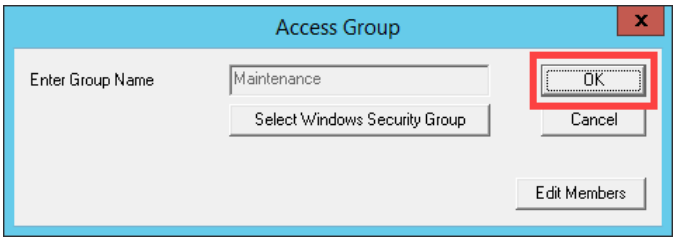


The Select Windows Security Group provides the ability to link an **Access Group** to a **Widows Security Group**. Therefore, you could manage access to ThinManager resources (**Terminals**, **Display Clients**, etc.) through **Windows Security Groups** as well. You could also use the **TermMon ActiveX** 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.

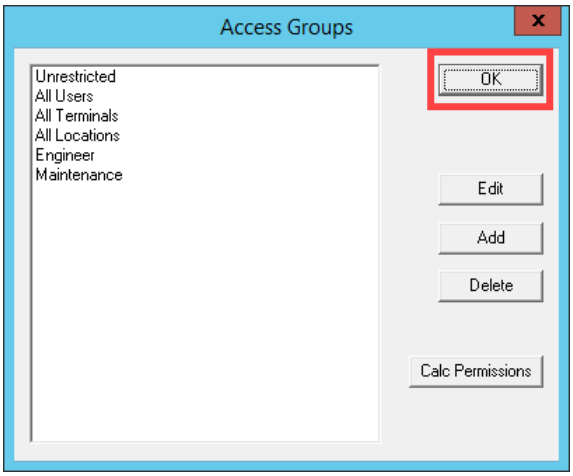
4. From the **Select Security Group to Add** window, expand the **Users** item and select the **Maintenance** group, followed by the **OK** button.



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

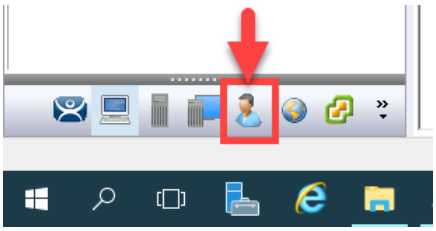


6. From the **Access Groups** window, click the **OK** button.

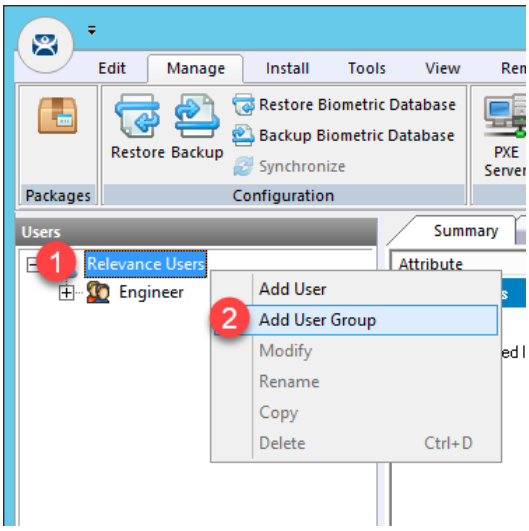


Create Maintenance User Group

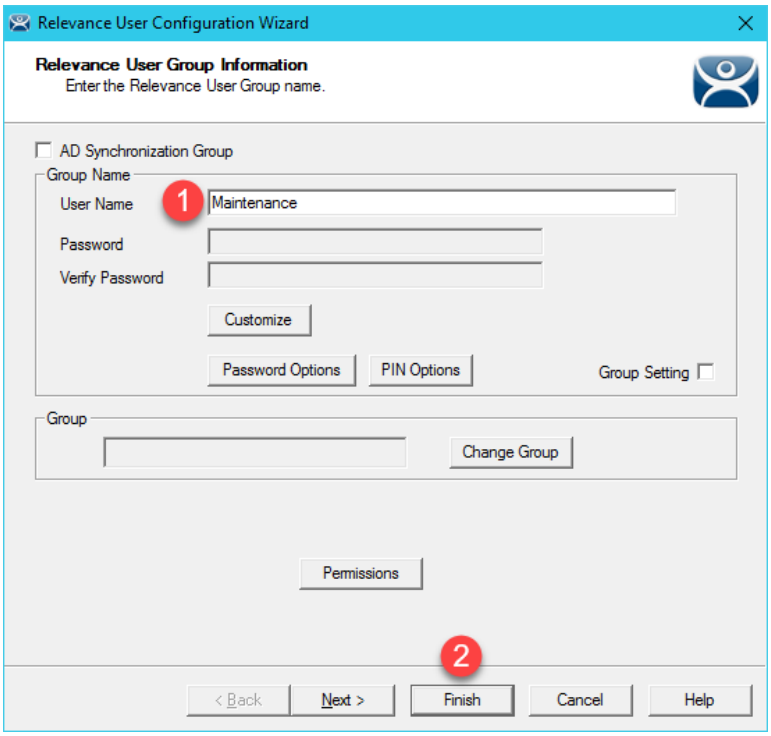
1. Click the **Users** icon  in the ThinManager tree selector.



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**.

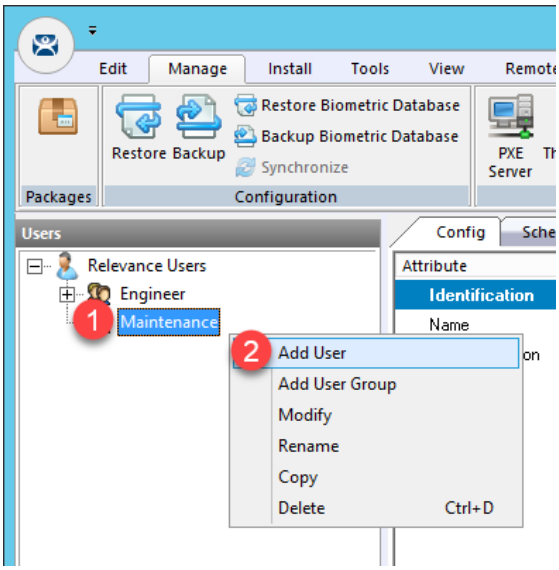


3. From the **Relevance User Group Information** page of the wizard, enter *Maintenance* as the **User Name** in the **Group Name** frame. Click the **Finish** button.

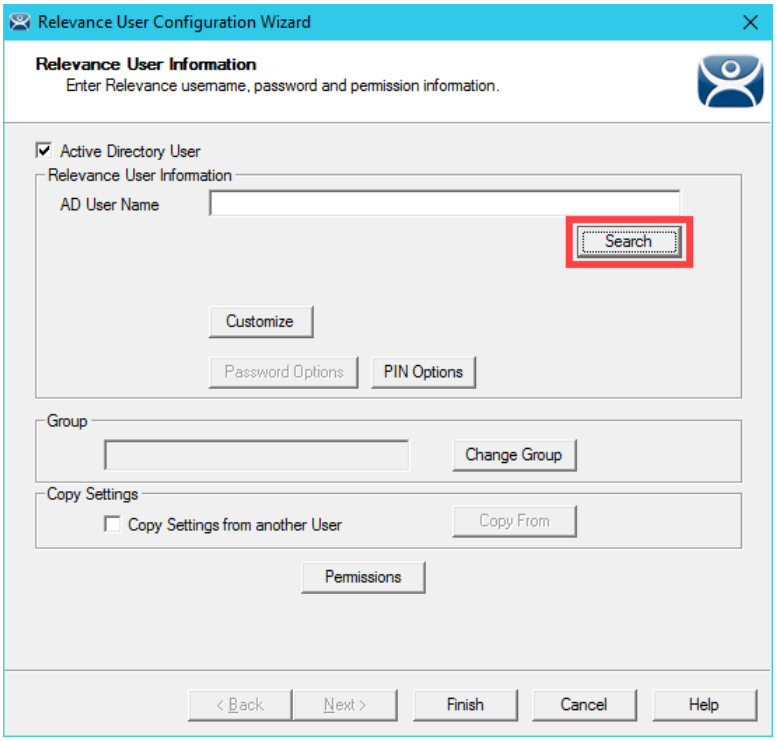


Create Maintenance User

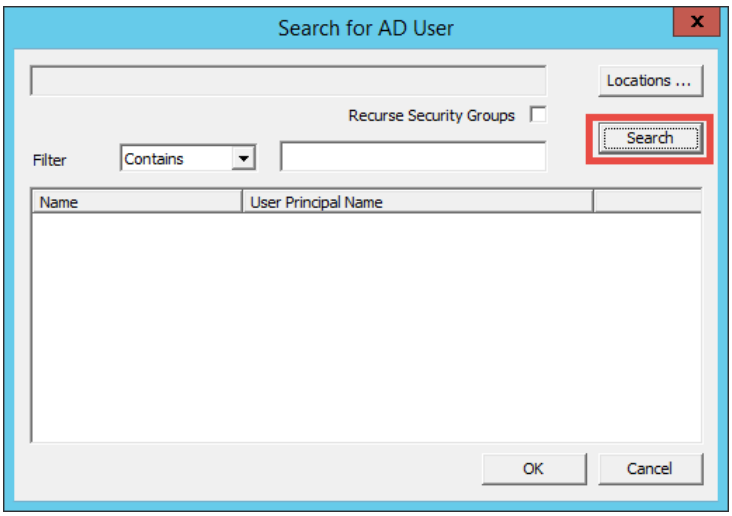
1. Expand the **Relevance Users** node.
2. Right click the newly created **Maintenance User Group** and select **Add User**. This will launch the **Relevance User Configuration** wizard.



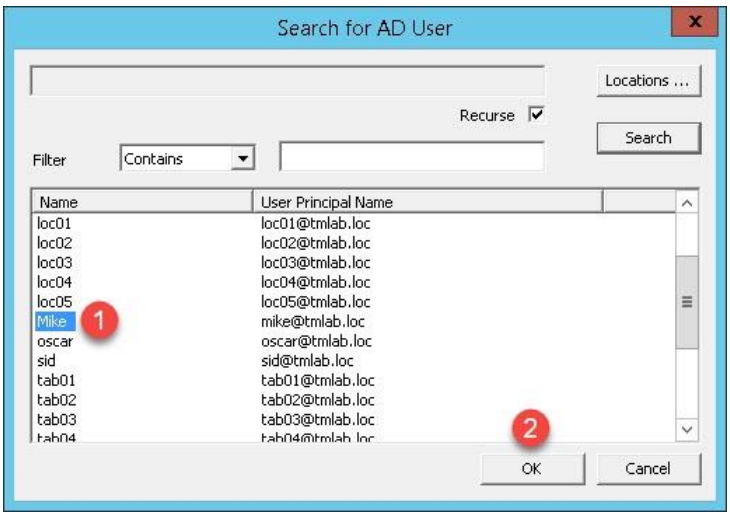
3. From the **Relevance User Information** page of the wizard, check the **Active Directory User** checkbox if it is not already checked. Click the **Search** button.



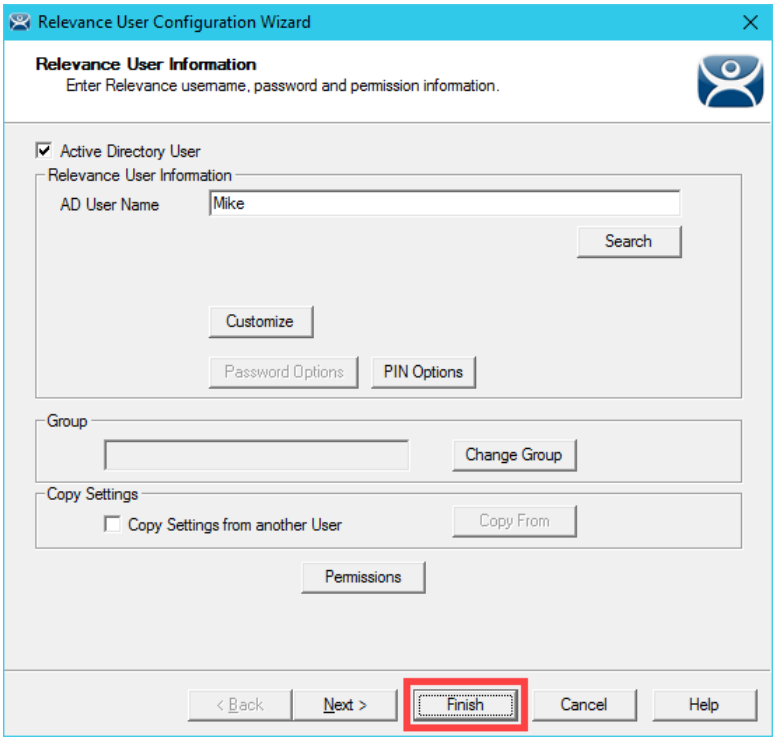
4. From the **Search for AD User** dialog box, click the **Search** button.



5. Select **Mike** from the user list and then click the **OK** button.



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

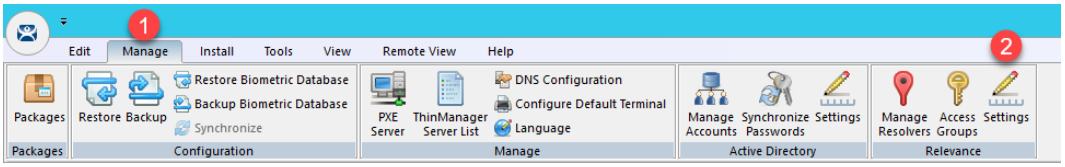


Register a Bluetooth Beacon Location Resolver

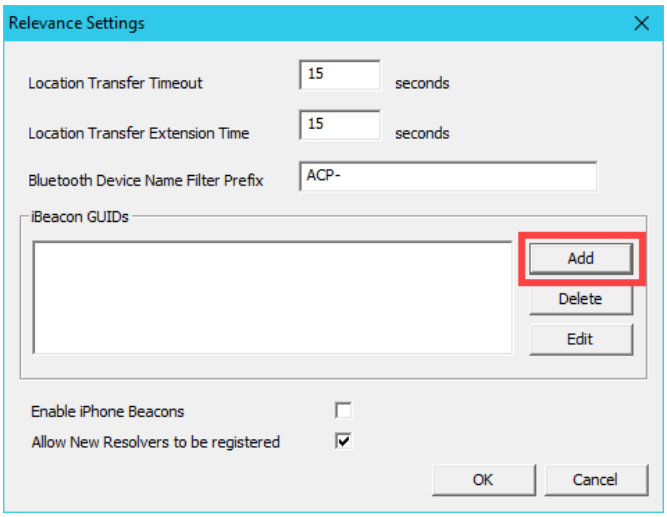
A **Bluetooth Beacon** uses **Bluetooth Low Energy** (**BTLE**) to transmit a signal continuously, hence the name beacon. This signal includes a **Received Signal Strength Indicator** (**RSSI**). Version 4.0 of the Bluetooth Standard, which a majority of today's mobile devices support, included support for **BTLE**. The closer the mobile device is to the **Bluetooth Beacon**, the stronger the signal strength (less negative). The further away the mobile device is from the **Bluetooth Beacon**, the weaker the signal strength (more negative). This signal strength can be used within ThinManager to create a **Location** that is defined by an entry and exit point, each represented by a specific signal strength value. We will use a common **Bluetooth Beacon** for the lab that will be used as our **geo-fence**.

Since this is a Cloud lab, we will not have access to a Bluetooth Beacon, but we will walk through the process of manually registering an **iBeacon**. With an actual beacon, you would be able to register it using a ThinManager mobile client like aTMC, iTMC or WinTMC. First, in order for ThinManager to use an **iBeacon**, you must tell ThinManager the **Universally Unique Identifier** (**UUID**) of the **beacon**. For Radius Network **beacons**, you can use their free App called **RadBeacon** to configure their **beacons**.

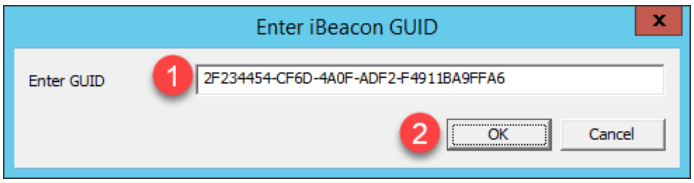
1. From ThinManager, click the **Manage** ribbon followed by the **Settings** icon within the **Relevance** group.



2. From the **Relevance Settings** window, click the **Add** button in the **iBeacon GUIDs** frame.

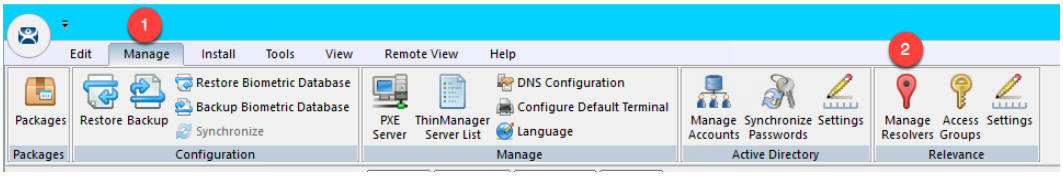


3. Enter the following in the **GUID** field *2F234454-CF6D-4A0F-ADF2-F4911BA9FFA6* (you can also copy and paste this path from the **LabPaths.txt** file by right clicking the **Notepad** icon pinned to the start bar and selecting **LabPaths.txt**). Click the **OK** button.

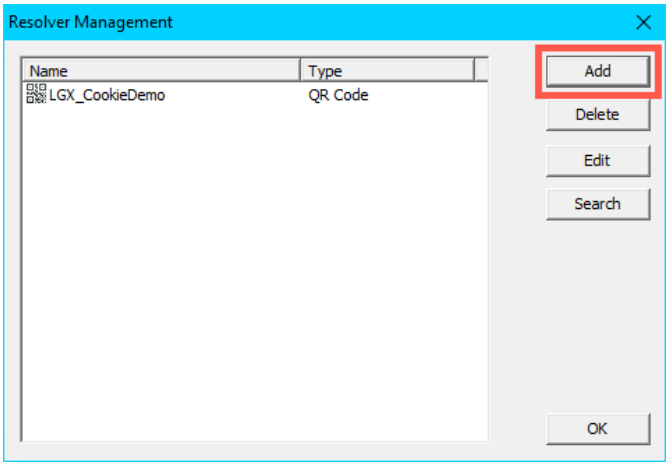


4. Click the **OK** button.

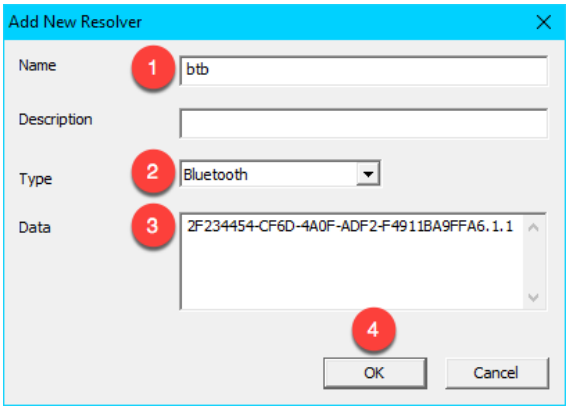
5. Click the **Manage** ribbon followed by the **Manage Resolvers** icon.



7. From the **Resolver Management** window, click the **Add** button.

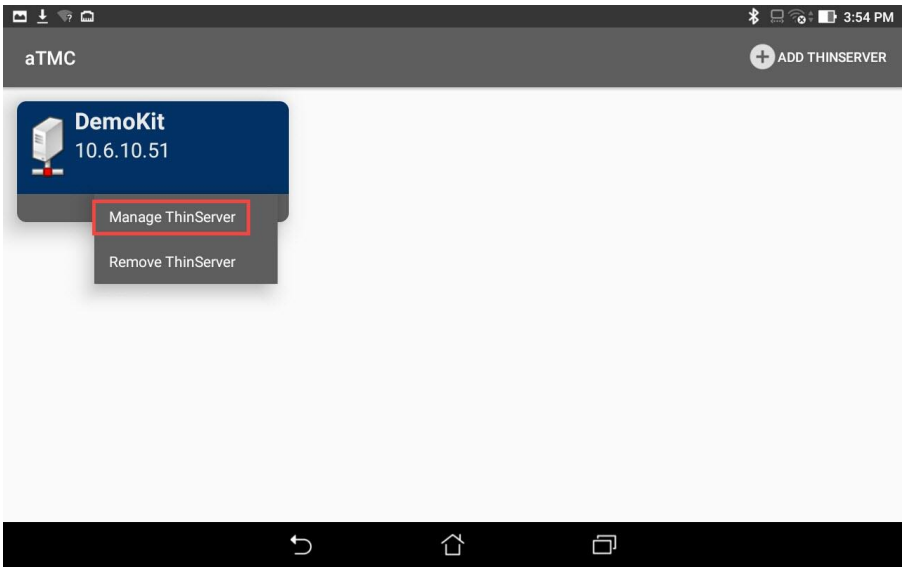


8. From the **Add New Resolver** window, enter *btb* as the **Name**, select **Bluetooth** as the **Type** and enter or copy/paste *2F234454-CF6D-4A0F-ADF2-F4911BA9FFA6.1.1* into the **Data** field. Click the **OK** button followed by the **OK** button again.

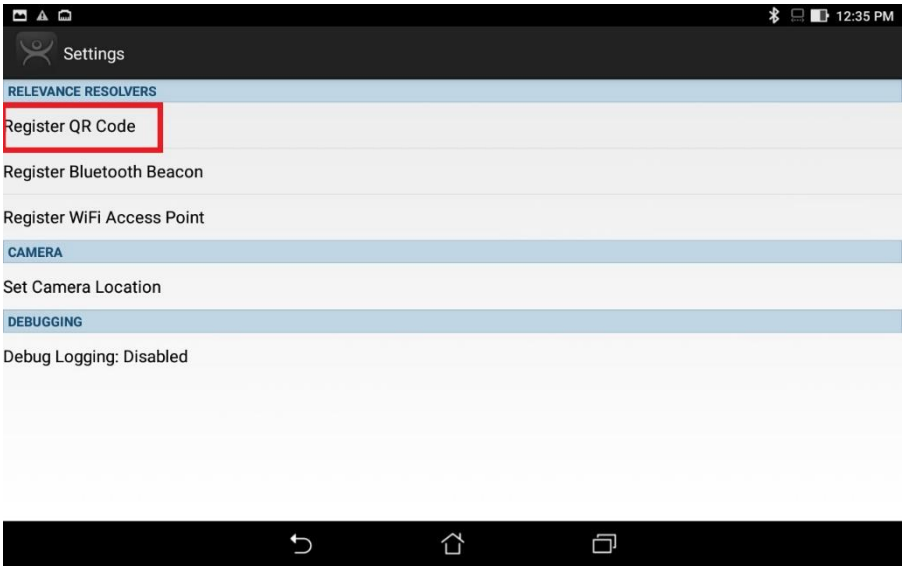


Register a QR Code Location Resolver

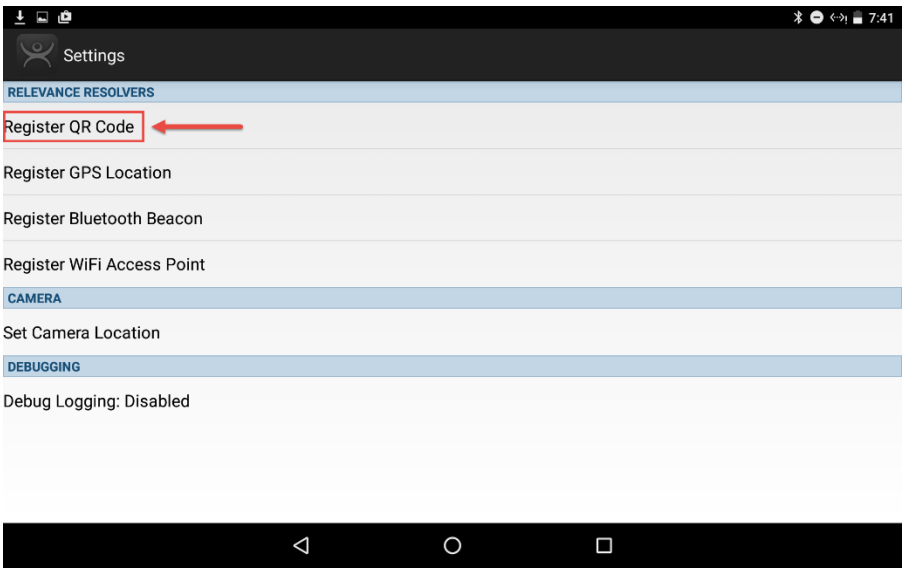
1. From the aTMC **Main Menu**, touch the **Settings** button (3 vertical dots below the **DemoKit** button), followed by the **Manage ThinServer** button.



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

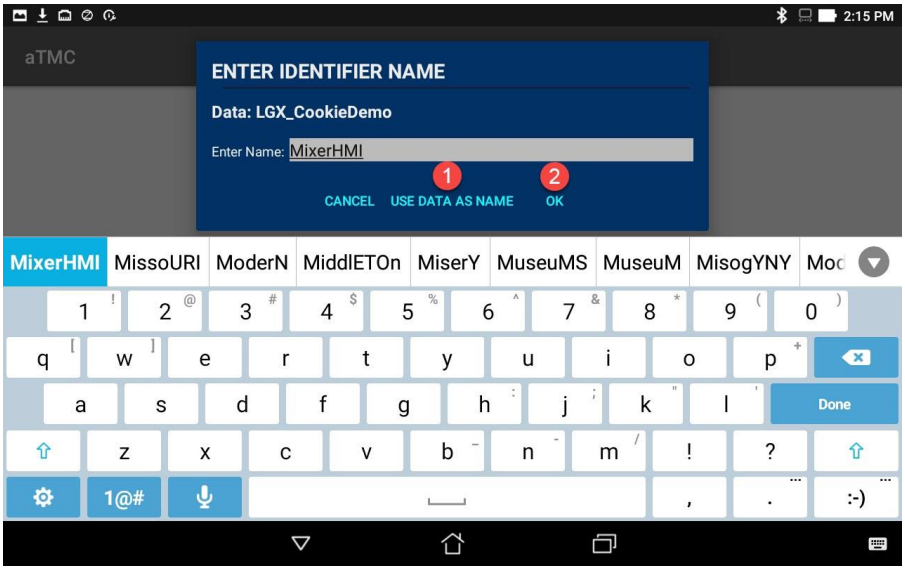


3. Back at the **aTMC Settings** window, touch the **Register QR Code** button.

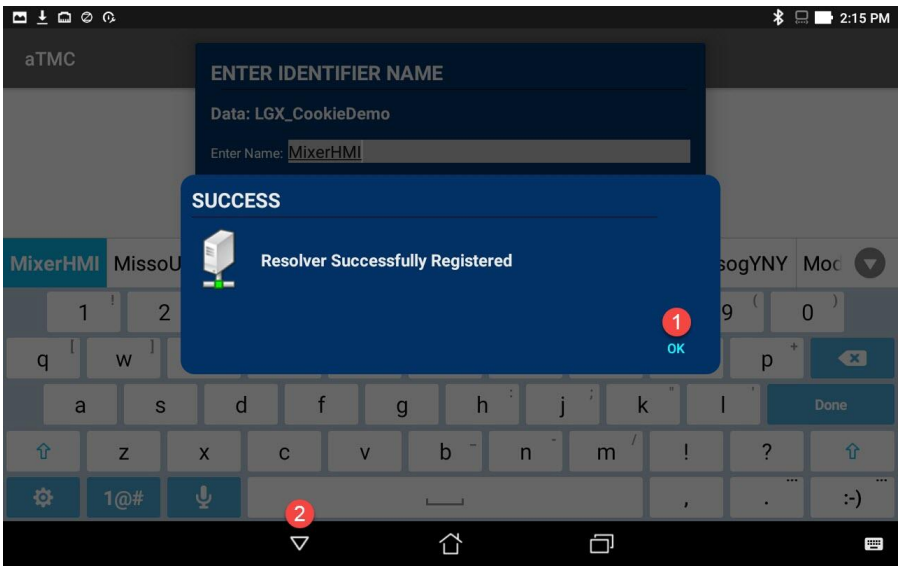


4. A camera window will appear. Point the Tablet camera at the **QR Code** below.

5. 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** (**MixerHMI**). Touch the **OK** button.



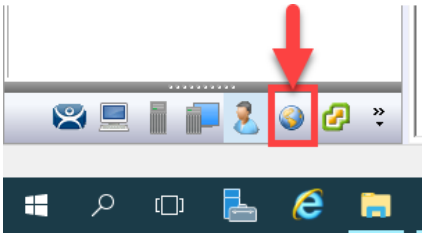
6. You should receive a successful confirmation dialog. Touch the **OK** button, followed by the **Back** button to return to the **Main Menu.**



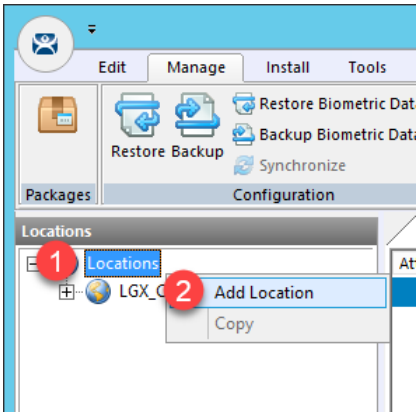
Create Parent (Geo-Fence) Location

The example you are about to create will require two **Locations** in ThinManager. One will be the **Parent** representing the **geo-fence**, to which the **Bluetooth Beacon Location Resolver** will be assigned. The second will be the **Child** to which we will assign the **CookieDemo Display Client** and the **QR Code Location Resolver**.

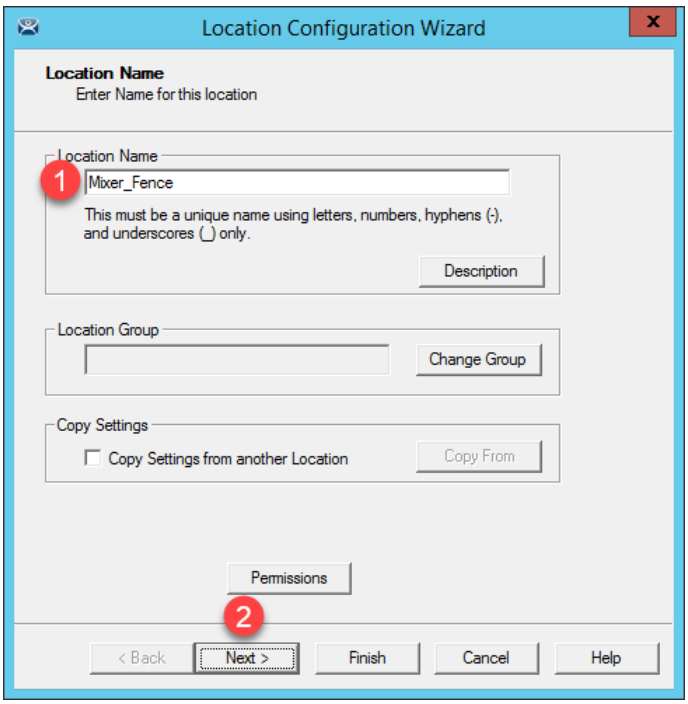
1. Click the **Locations** icon  in the tree selector. This icon will only be present if you have a **Relevance** license activated.



2. Right click the **Locations** tree item and select **Add Location**.



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



4. From the **Location Options** page of the wizard, keep the defaults and click the **Next** button.

> Due to the fact that you are tethered, we will not actually be enforcing the Fence in this example. If we wanted to enforce the fence, we would check the **Enforce Location Fencing** checkbox.

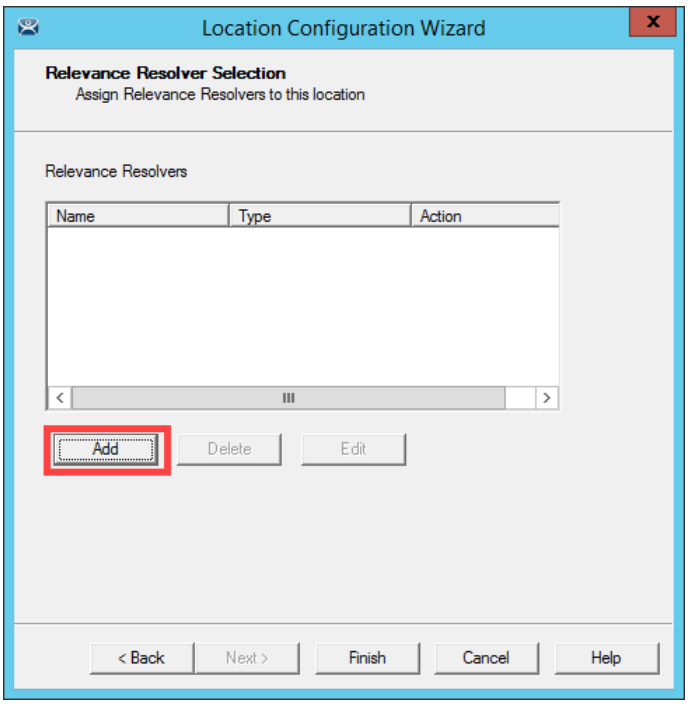
5. Click the **Next** button on the **Display Client Selection** page of the wizard.

> If we assigned a **Display Client** here it would be automatically delivered to the tablet when within the defined range of the **Beacon**, and automatically removed when outside the range of the **Beacon**. For the example we are building, we want to require the scan of a **QR Code** while within range of the **Beacon** to trigger the content delivery.

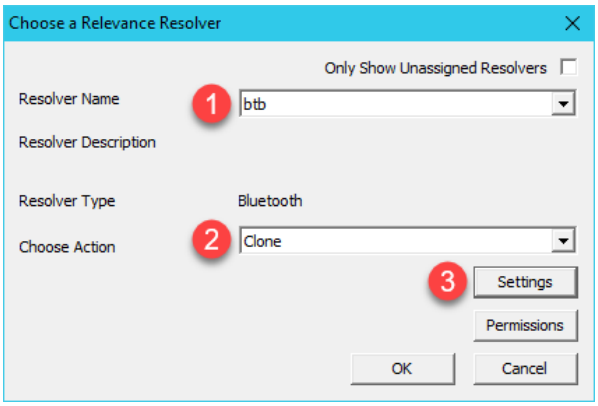
6. Click the **Next** button on the **Windows Log In Information** page of the wizard.

> Since we have not assigned a Display Client to this Location, we don't need to provide Login Credentials.

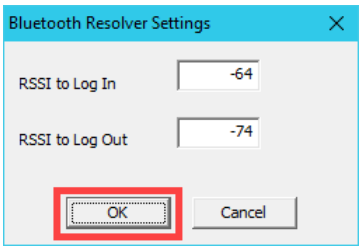
7. Click the **Add** button from the **Relevance Resolver Selection** page of the wizard.



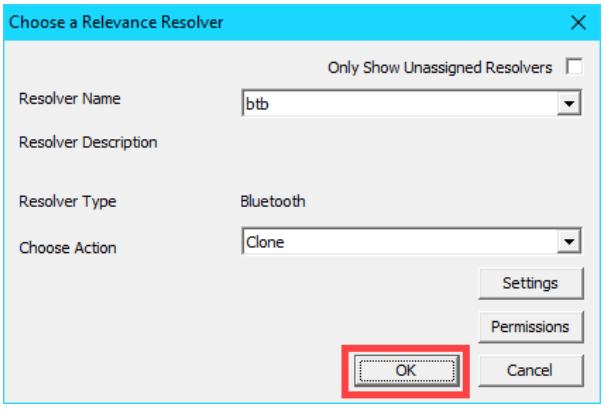
8. Select **btb** from the **Resolver Name** drop down list and **Clone** from the **Choose Action** page of the wizard. Click the **Settings** button.



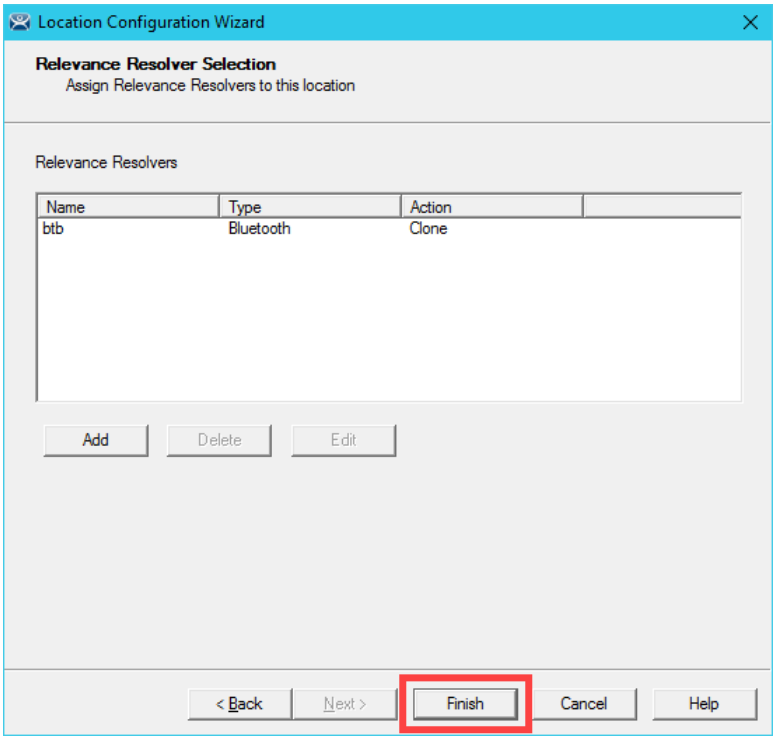
9. The **RSSI to Log In** value is the one captured when you registered the Beacon. The **RSSI to Log Out** is just 10 less than the **RSSI to Log In.** For the purposes of this lab, do not change the values. Click the **OK** button.



10. Click the **OK** button again.



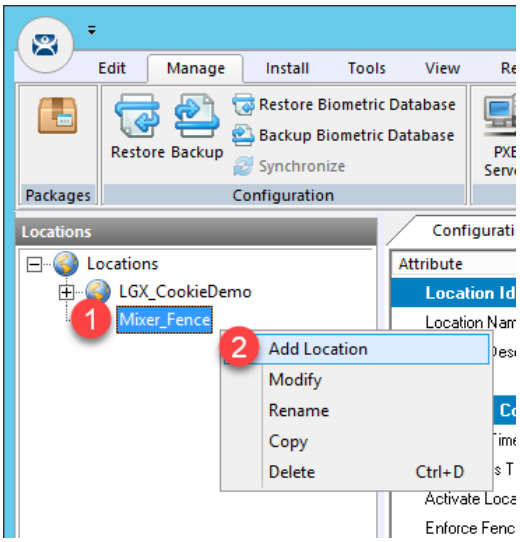
11. Click the **Finish** button.



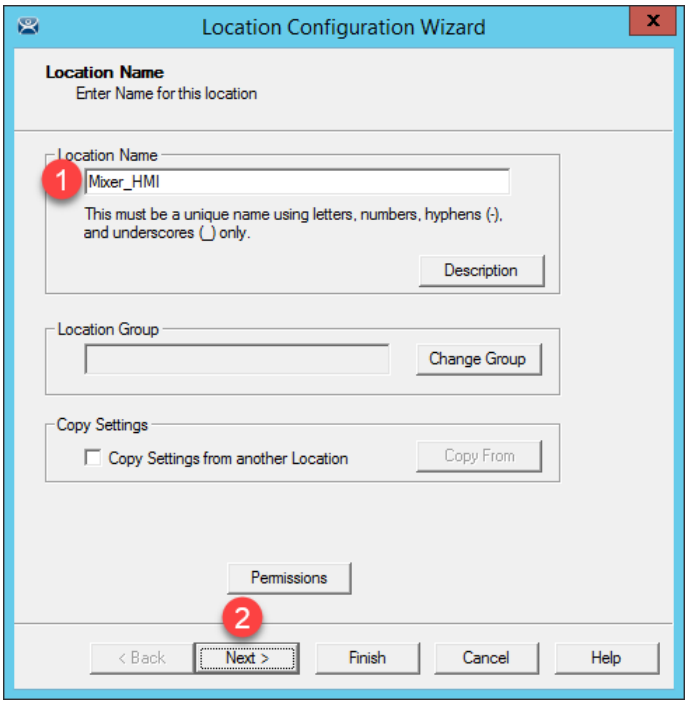
Create Child Location

We will assign the **CookieDemo Display Client** to the **Child Location** and the **QR Code Location Resolver** we just registered.

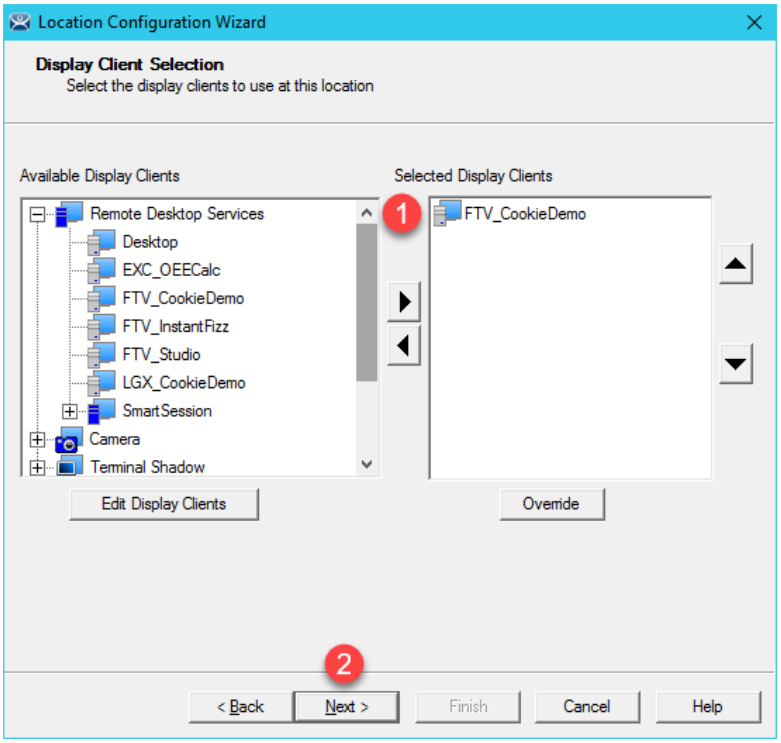
1. Right click the **Mixer_Fence** location and select the **Add Location** item.



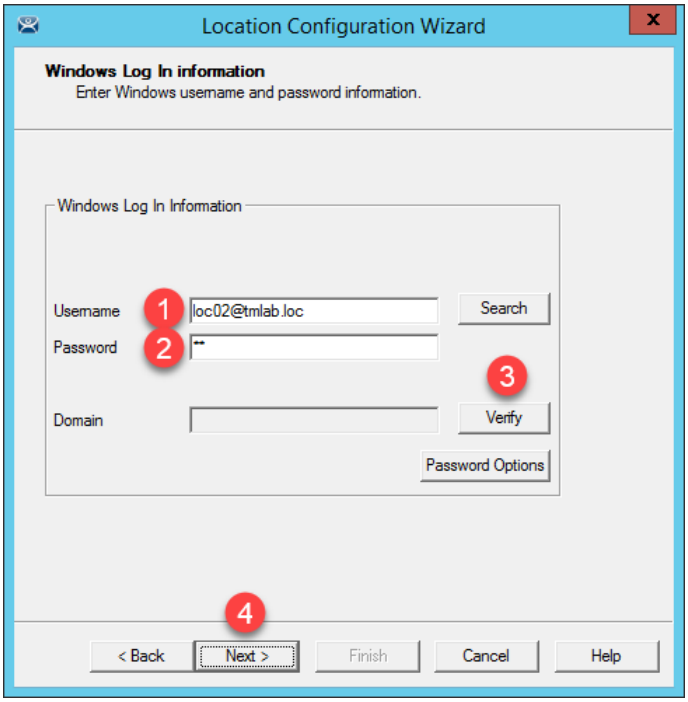
2. From the **Location Name** page of the **Location Configuration Wizard**, enter *Mixer_HMI* as the **Location Name**. Click the **Next** button.



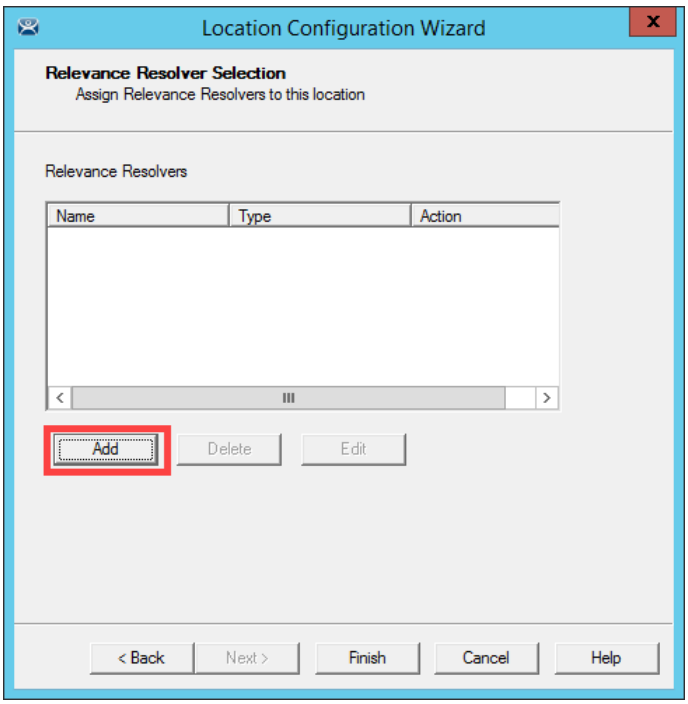
3. Click the **Next** button on the **Location Options** page of the wizard.
4. From the **Display Client Selection** page of the wizard, remove all existing **Display Clients** and move the **FTV_CookieDemo Display Client** to the **Selected Display Clients** list. Click the **Next** button.



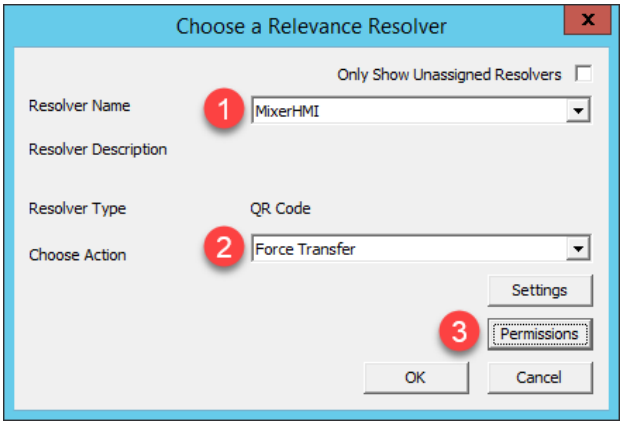
5. From the **Windows Log In Information** page of the wizard, enter *loc02@tmlab.loc* as the **Username** and *rw* as the **Password**. Click the **Verify** button to validate the credentials entered. Click the **Next** button.



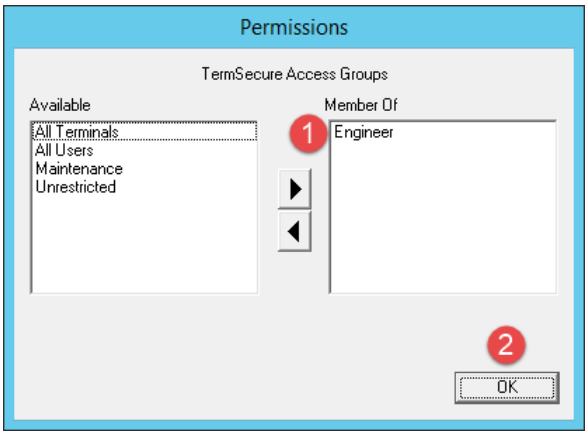
6. From the **Relevance Resolver Selection** page of the wizard, click the **Add** button.



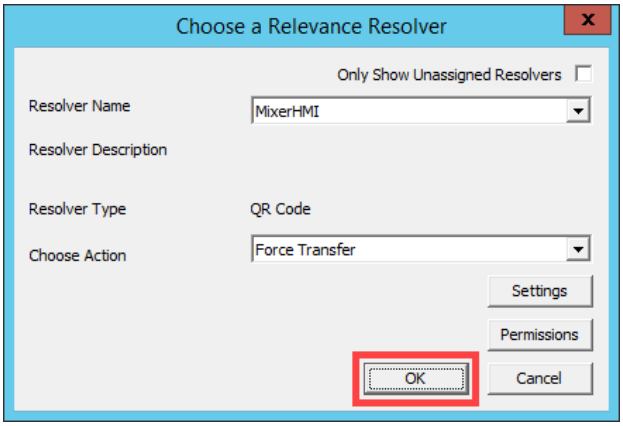
7. Select **MixerHMI** as the **Resolver Name** and **Force Transfer** as the **Choose Action**. Click the **Permissions** button.



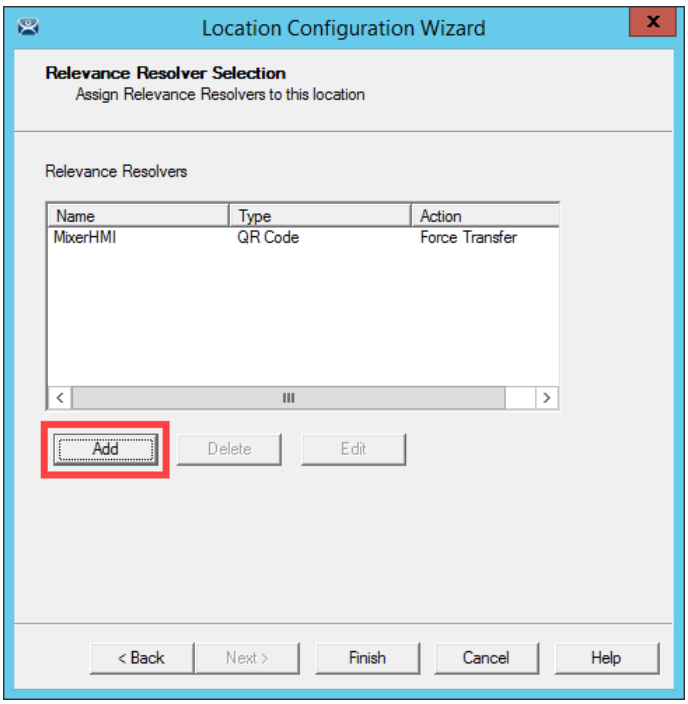
8. From the **Permissions** window, remove **Unrestricted** from the **Member Of** list and add **Engineer**. Click the **OK** button.



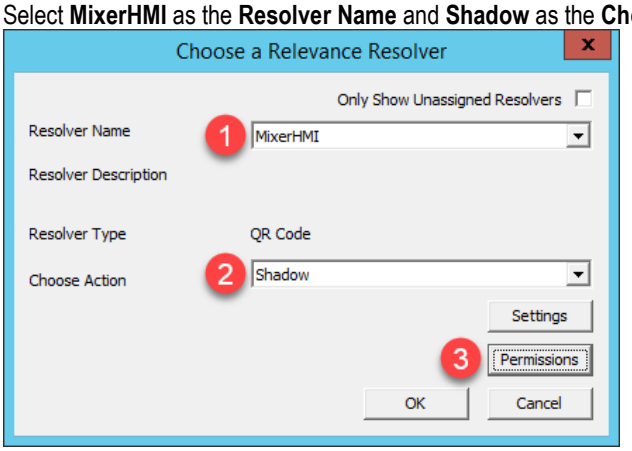
9. Click the **OK** button.



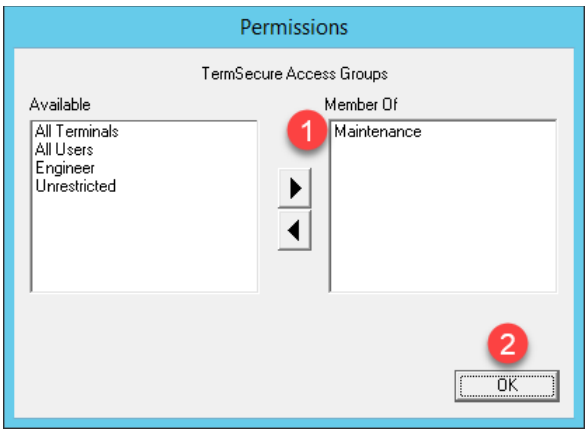
10. Click the **Add** button.



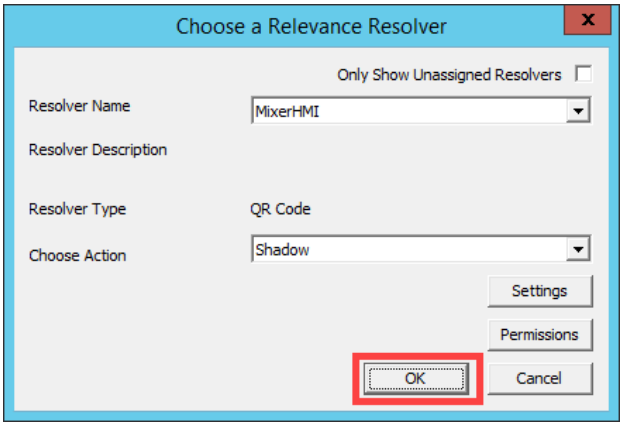
11. Select **MixerHMI** as the **Resolver Name** and **Shadow** as the **Choose Action**. Click the **Permissions** button.



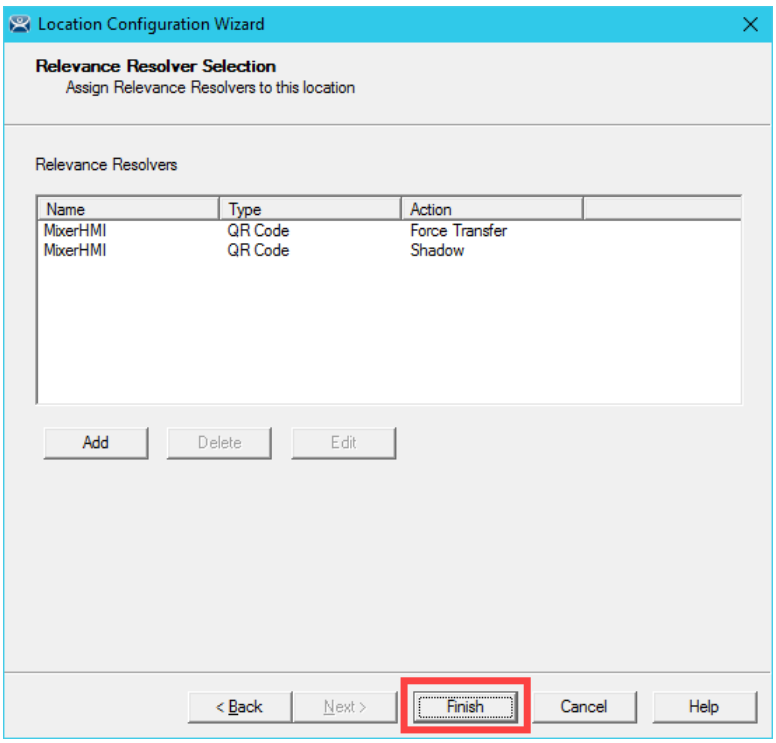
12. From the **Permissions** window, remove **Unrestricted** from the **Member Of** list and add **Maintenance**. Click the **OK** button.



13. Click the **OK** button.



14. Click the **Finish** button.



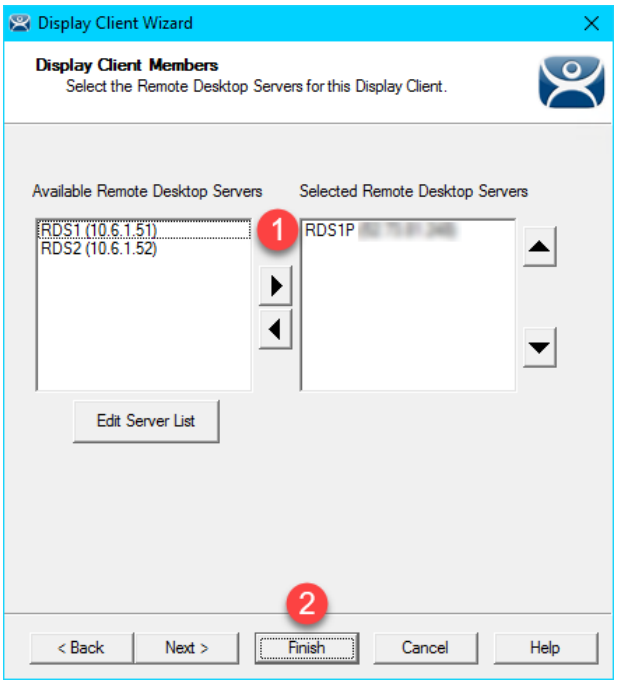
Reassign Display Client to Public Display Server

When we created the **FTV_CookieDemo Display Client** in the previous sections, we assigned the **RDS1** and **RDS2 Display Servers** to it, which have private IP addresses of 10.6.10.51 and 10.6.10.52, respectively. These IP addresses will not be reachable by your remote tablet, so we will reassign the **Display Client** 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_CookieDemo 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.

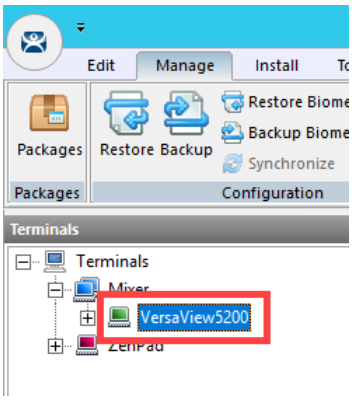
7. From the **Display Client Members** page of the wizard, remote **RDS2** from the **Selected Remote Desktop Servers** list box and add **RDS1P** instead. Click the **Finish** button.



Assign Default Location to Terminal

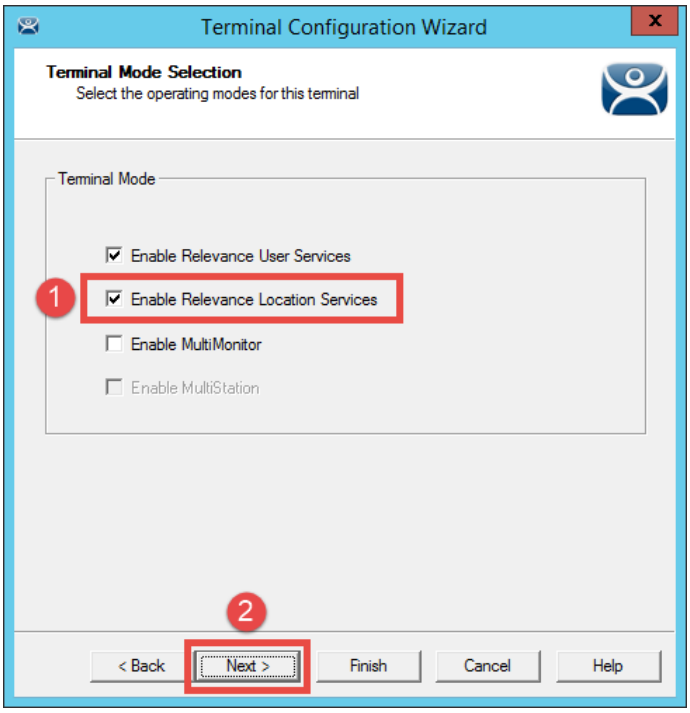
1. Click the **Terminals** tree selector icon.

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

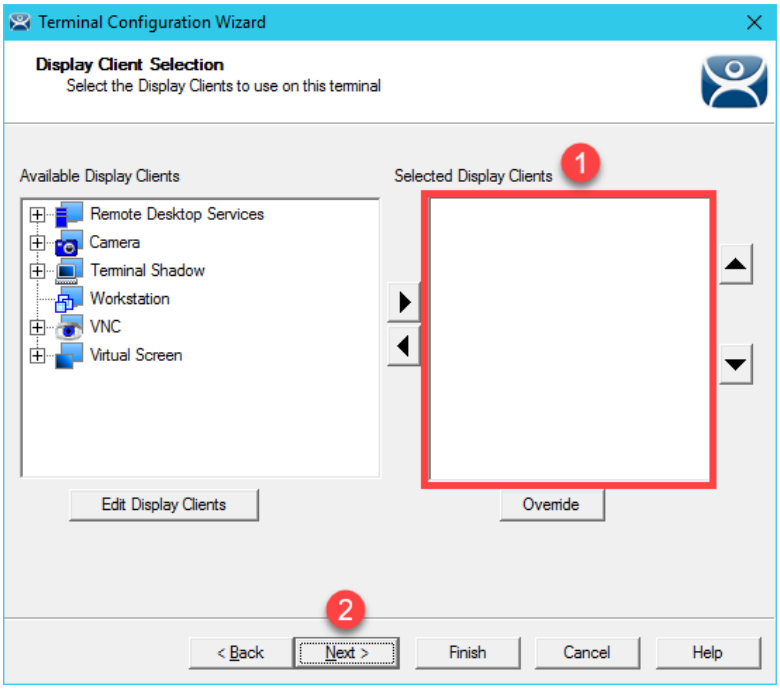


3. Click the **Next** button on the **Terminal Name** page of the wizard.
4. Click the **Next** button on the **Terminal Hardware** page of the wizard.
5. Click the **Next** button on the **Terminal Options** page of the wizard.

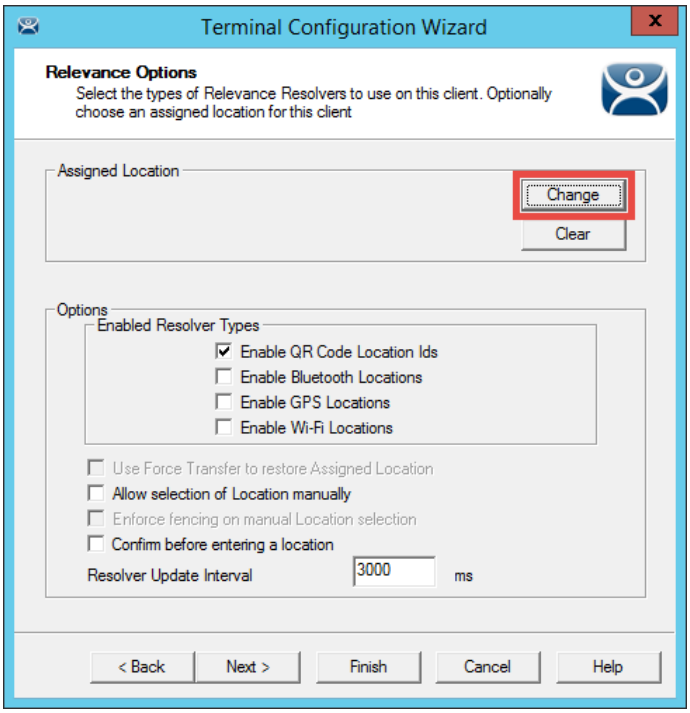
6. From the **Terminal Mode Selection** page of the wizard, make sure **Enable Relevance User Services** is checked. Also check the **Enable Relevance Location Services**. This is required to use this **Terminal** with **Relevance**. Click the **Next** button.



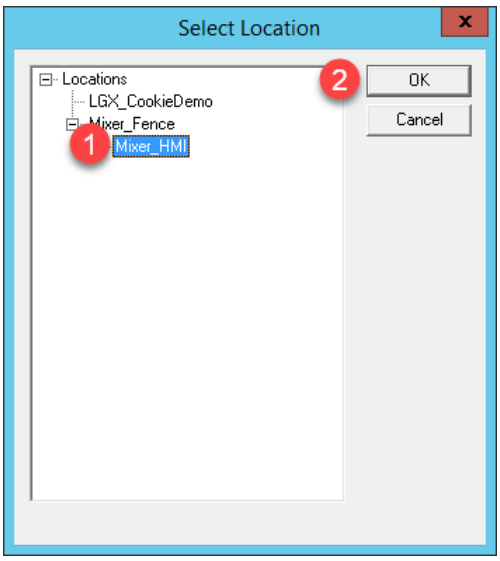
7. Ensure all **Display Clients** are removed from the **Selected Display Clients** list. Click the **Next** button.



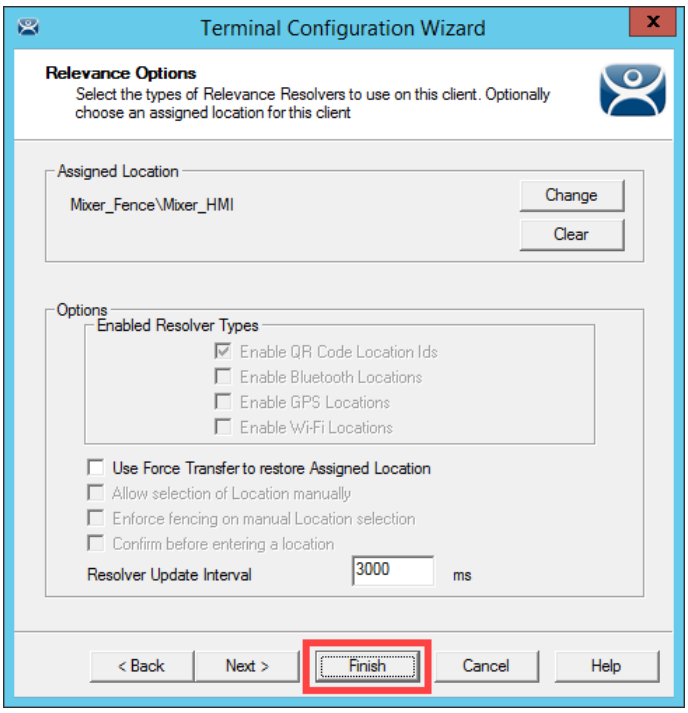
8. From the **Terminal Interface Options** page of the wizard, click the **Next** button.
9. From the **Relevance Options** page of the wizard, click the **Change** button.



10. From the **Select Location** popup, select **Mixer_HMI**. Click the **OK** button.



11. Click the **Finish** button.



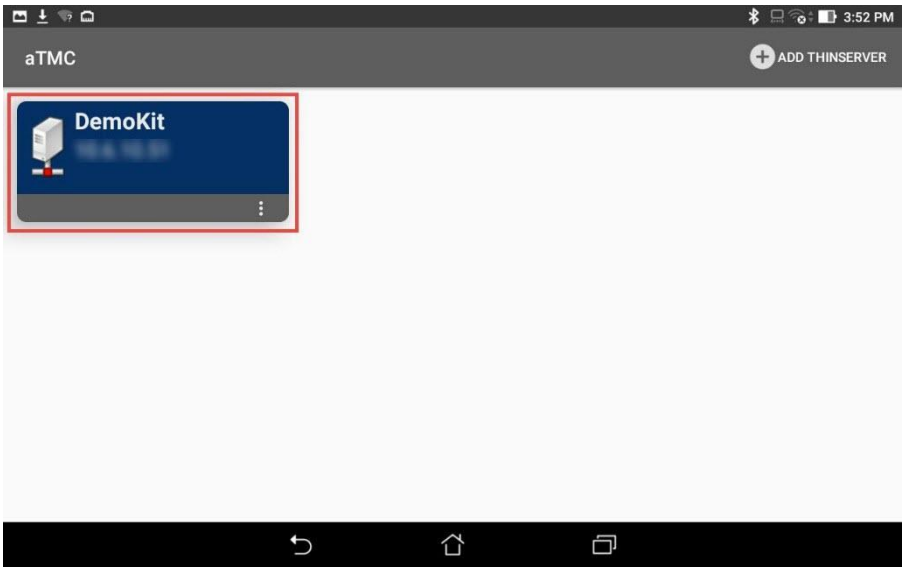
Notice the **Allow selection of Location manually** checkbox. With this checked, the **Terminal** to which this profile is assigned will be able to manually login to **Locations** that permit this action. In this scenario, if the **Enforce fencing on manual Location selection** is not checked, then the **Terminal** to which this profile is assigned will be able to login to any geo-fenced **Location** even when not within the geo-fence.

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

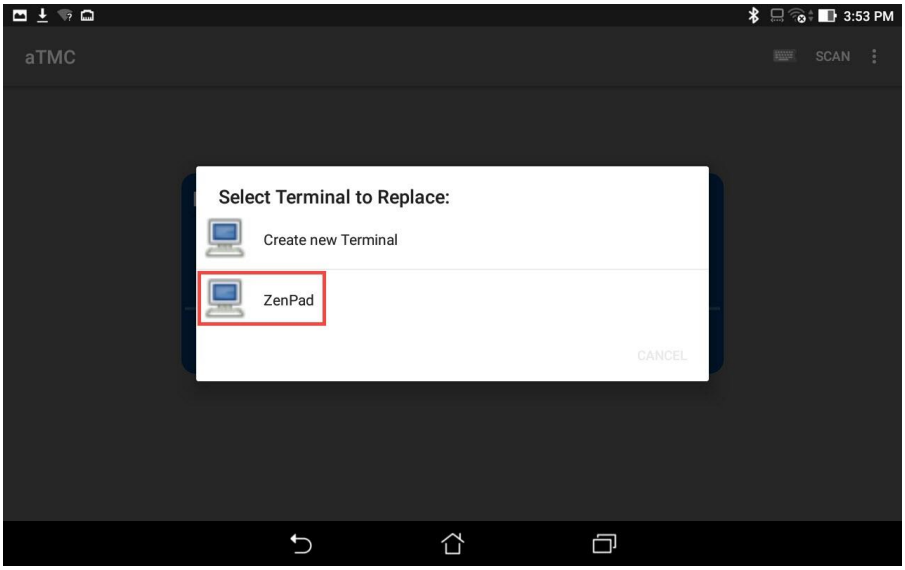
After restarting the **Terminal**, you will notice that the **FTV_CookieDemo** application is still delivered to the virtual thin client. This is because we assigned the **FTV_CookieDemo Display Client** to the **Mixer_HMI Location** and then assigned this **Location** to the **VersaView5200 Terminal**. The more interesting part of the configuration is how the **Mixer_Fence** and **Mixer_HMI Locations** were configured. Using a mobile device, the **MixerHMI QR Code** can be scanned if and only if the mobile device is within the defined range of the btb **Bluetooth Beacon** AND the user logged in is a member of either the Engineer or Maintenance **Access Groups**. If the user is a member of the Engineer group, the **FTV_CookieDemo Display Client** would be transferred from **VersaView5200** and redirected to the mobile device. If the user is a member of the Maintenance **Access Group**, **VersaView5200** would be shadowed from the mobile device. In both cases, the **Display Client** would remain on the mobile device as long as it stays within the range of the **Bluetooth Beacon**, which is acting as a **geo-fence**. The user can also choose to manually **Leave** the **Location** from the mobile device. Experiment with the results in the last section!

See the Results

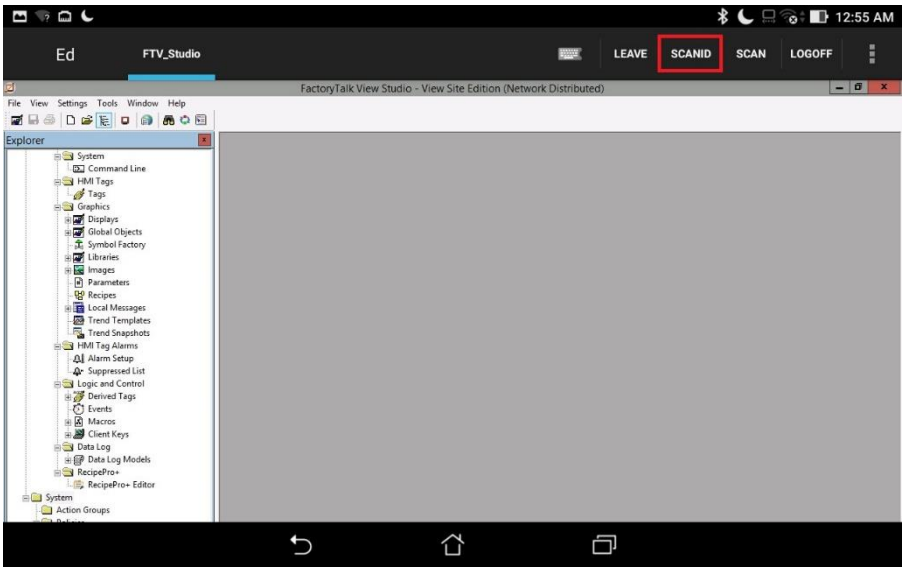
1. Return to **aTMC** on your mobile device. If so, you may also have to reconnect **aTMC** to the **DemoKit** server listed.



2. Select the **ZenPad** terminal profile if prompted.



3. If not already logged in as **Ed**, touch the **LOGIN** button and enter a **username** of *ed* and a PIN of *1234*. You should have received the **FactoryTalk View Studio Display Client** because this is assigned to the **Engineer User Group**, of which Ed is a member. 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.

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

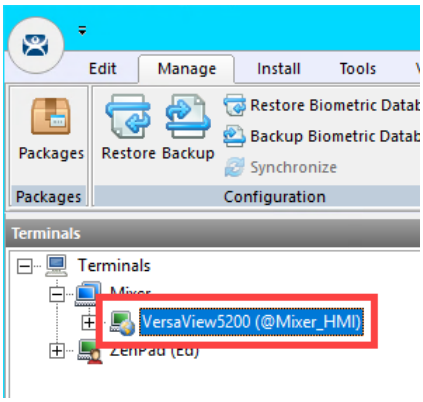
5. Since you are logged in as a member of the **Engineer** group, you should see the **CookieDemo Display Client** transferred from the virtual thin client and delivered to the tablet. However, you should only be able to keep this **Display Client** while within the **geo-fence** established by the **Bluetooth Beacon**. Since we do not have a beacon for the Cloud lab, you can simulate this behavior by touching the **Leave** button. This should result in the **CookieDemo Display Client** returning to the virtual thin client.

> To see the signal strength of your beacon(s) at any time, touch the **More Options** (3 vertical dots) button in the top right corner followed by the **Beacons** item.

Remove Default Location from Terminal

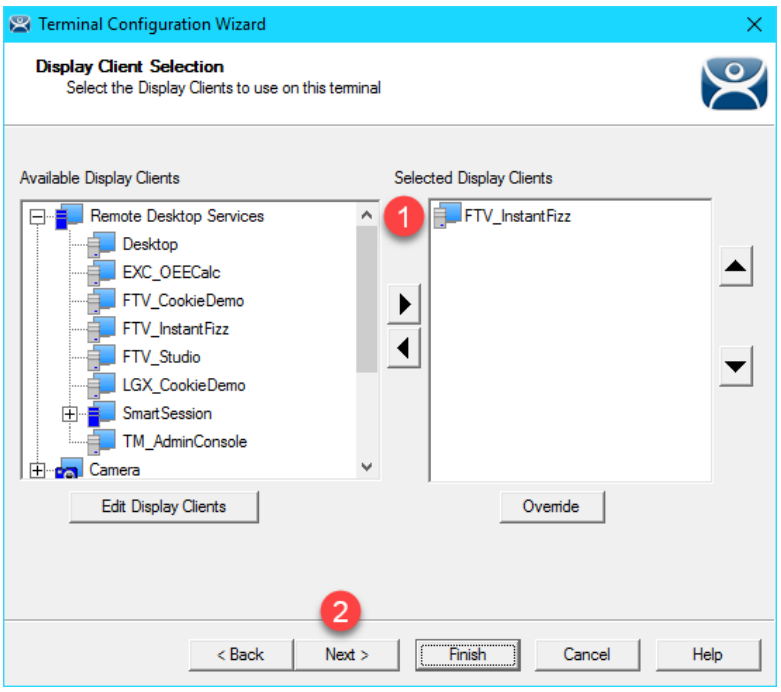
1. Click the **Terminals** tree selector icon.

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

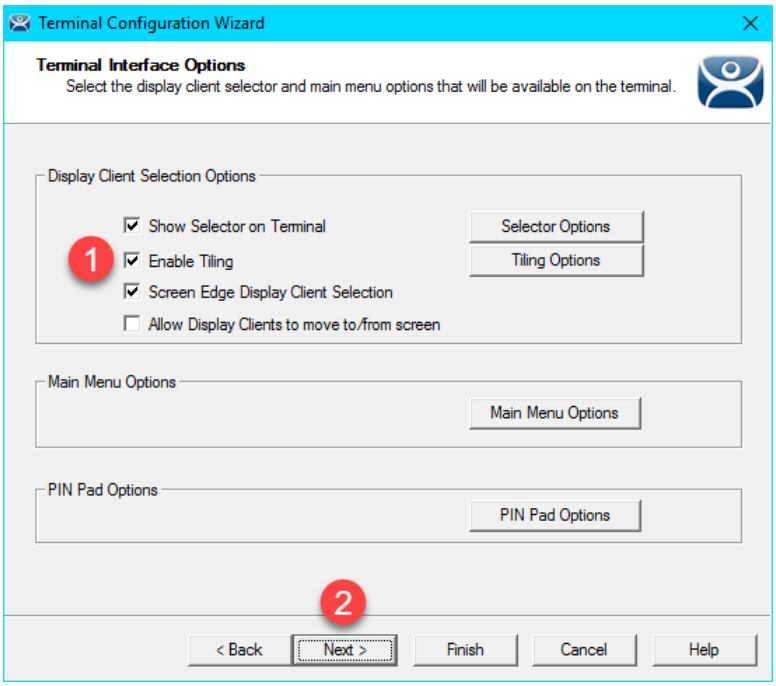


3. Click the **Next** button on the **Terminal Name** page of the wizard.
4. Click the **Next** button on the **Terminal Hardware** page of the wizard.
5. Click the **Next** button on the **Terminal Options** page of the wizard.
6. Click the **Next** button on the **Terminal Mode Selection** page of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

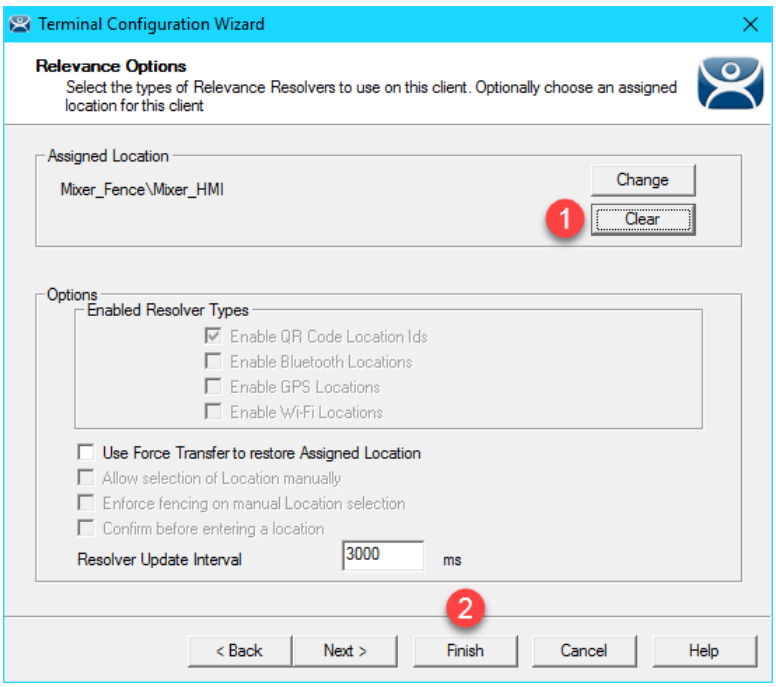
7. Assign **FTV_InstantFizz** to the **Select Display Clients** listbox. Click the **Next** button.



8. From the **Terminal Interface Options** page of the wizard, check the **Enable Tiling** checkbox.



9. From the **Relevance Options** page of the wizard, click the **Clear** button followed by the **Finish** button.



10. 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 **Relevance and Geo-Fencing**. Please continue on to the **TermMon ActiveX** section of the lab.

Section 18: ThinManager TermMon ActiveX

Overview

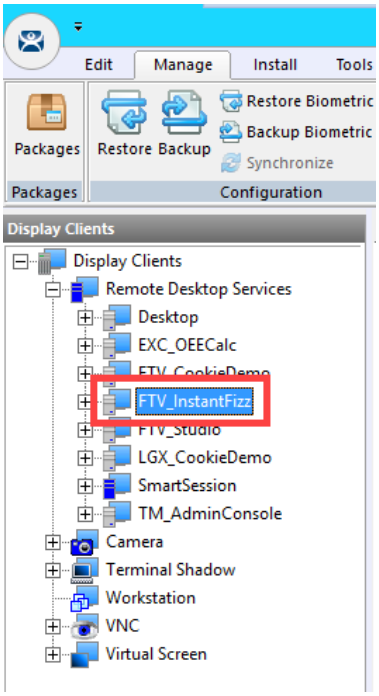
The **ThinManager TermMon ActiveX** enables programmatic control of many aspects related to ThinManager from an **ActiveX Container**. For example, from an **ActiveX Container** like **FactoryTalk View SE**, you can programmatically access ThinManager managed terminal properties like the IP address, MAC address, currently logged in user, connection state, **Relevance Location**, etc. You can also launch the touchscreen calibration utility, manipulate **IP camera overlays**, etc. In this section we will embed the ActiveX in the **FactoryTalk View SE** InstantFizz application to allow an operator to control the visibility of an IP camera overlay.

1. Create Camera Overlay
2. Registering and Updating the TermMon ActiveX Control
3. Add TermMon ActiveX to HMI Application
4. Test Camera Overlay Visibility
5. Explore TermMon Test Display

Create Camera Overlay

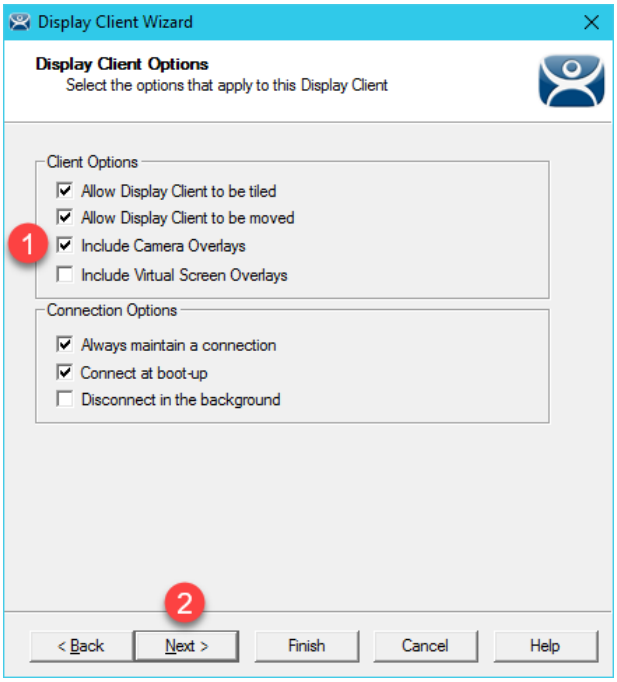
1. From ThinManager, click the **Display Clients** tree selector.

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

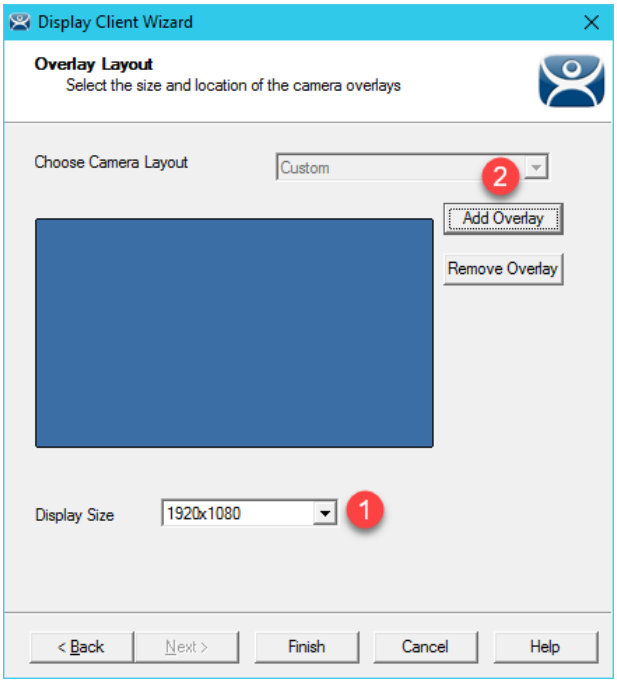


3. From the **Client Name** page of the wizard, click the **Next** button.

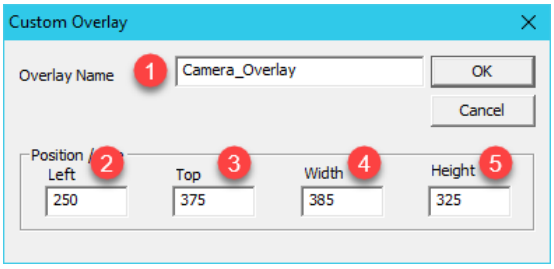
4. From the **Display Client Options** page of the wizard, check the **Include Camera Overlays** checkbox. Click the **Next** button.



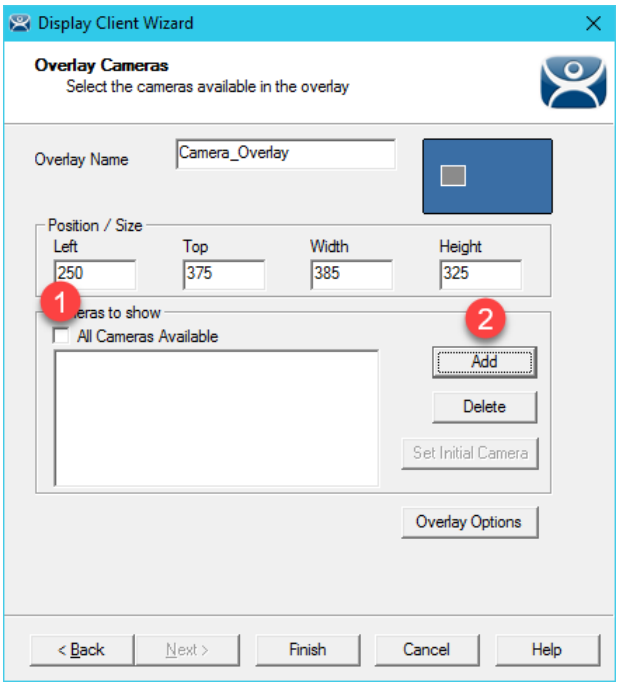
5. From the **Remote Desktop Services and Workstation Options** page of the wizard, click the **Next** button.
6. From the **Screen Resolution / Scaling Options** page of the wizard, click the **Next** button.
7. From the **Display Client Members** page of the wizard, click the **Next** button.
8. From the **AppLink** page of the wizard, click the **Next** button.
9. On the **Overlay Layout** page, setup the **Display Size** to **1920x1080,** click the **Add Overlay** button.



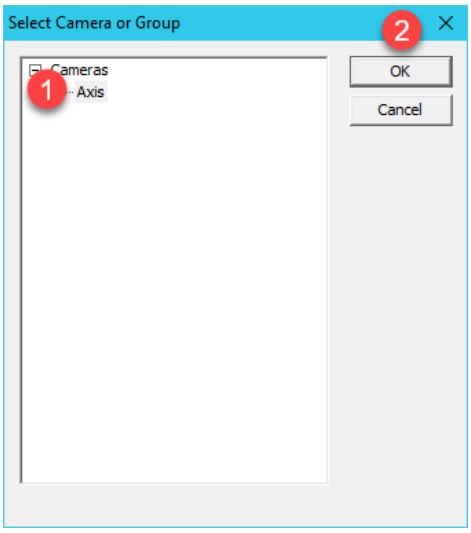
10. In the **Overlay Name** field enter *Camera_Overlay*. Enter *250* in the **Left** position field, *375* in the **Top** position field, *385* in the **Width** size field, and *325* in the **Height** size field. Click the **OK** button, followed by the **Next** button.



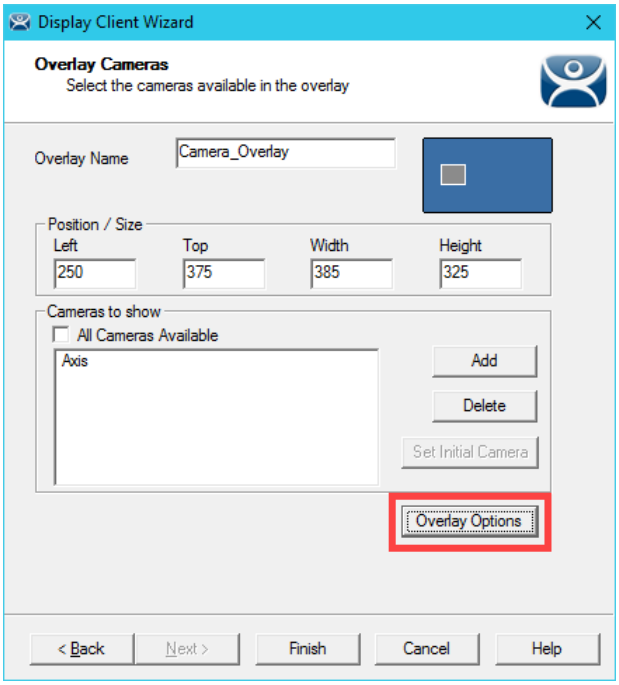
11. From the **Overlay Cameras** page of the wizard, uncheck the **All Cameras Available** checkbox in the **Cameras to show** frame and click the **Add** button.



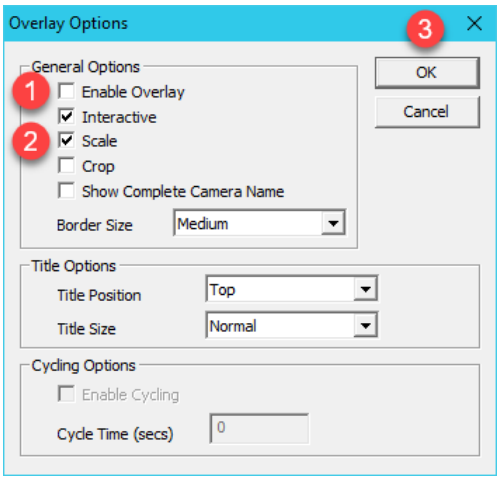
12. Select the **Axis** camera and click the **OK** button.



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

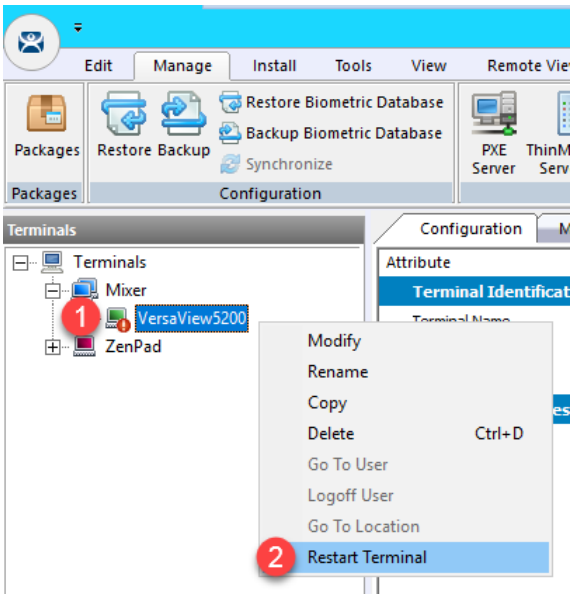


14. From the **Overlay Options** window, un-check the **Enable Overlay** checkbox and check the **Scale** checkbox. Click the **OK** button, followed by the **Finish** button.



Unchecking the **Enable Overlay** button will disable the camera by default when the terminal starts up. We will use the **ActiveX Control** to programmatically enable and disable it, so the operator has control of the camera visibility with a button.

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



Registering and Updating the TermMon ActiveX Control

Starting with **FactoryTalk View SE version 10.0**, the **TermMon.ocx** ActiveX Control is automatically installed on **FactoryTalk View SE Server** and **FactoryTalk View SE Client** installations. Therefore, no steps are required here for the lab since we are running **FactoryTalk View SE 11.0**.

If you need to update the version of **TermMon.ocx** for these installations, you will need to replace the **TermMon.ocx** file located in the **FactoryTalk View SE** installation folder, and then re-register the control. This task would need to be completed on **FactoryTalk View SE Server** as well as **FactoryTalk View SE Client** installations.

You can find the latest version of the **TermMon.ocx** from the ThinManager Downloads Webpage.

To register TermMon.ocx, execute the following command from an Administrative Command Prompt:

32-bit operating systems:

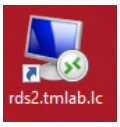
```
regsvr32 c:\path\to\termmon.ocx
```

64-bit operating systems:

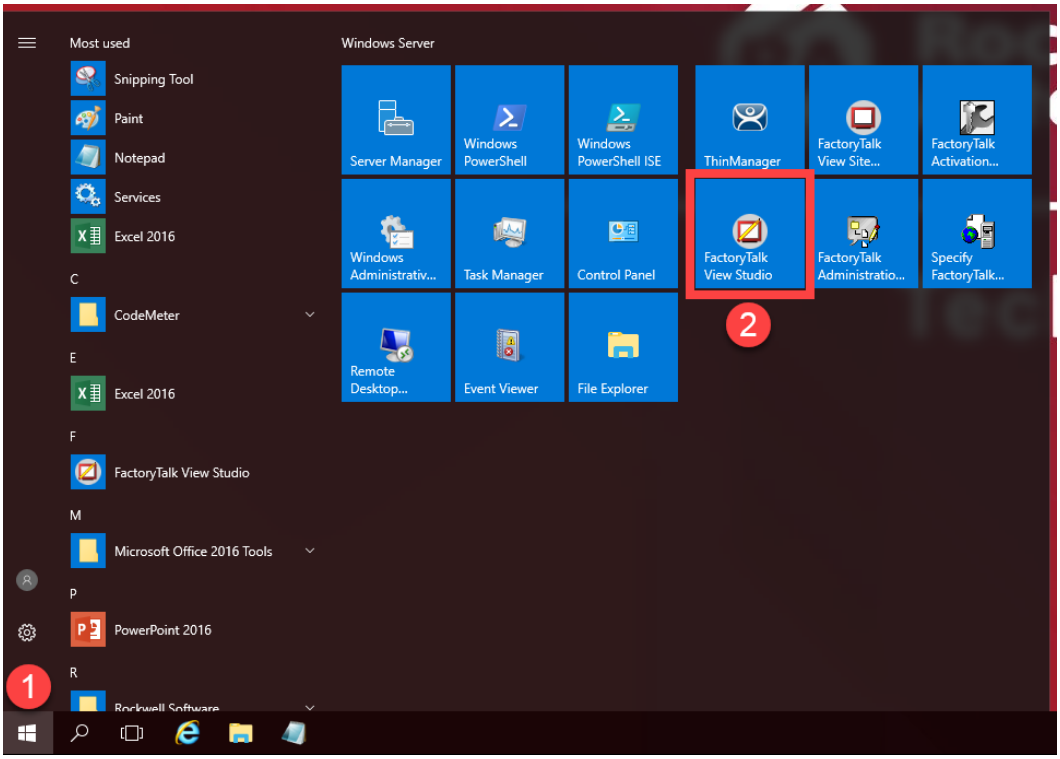
```
C:\windows\syswow64\regsvr32 c:\path\to\termmon.ocx
```

Add TermMon ActiveX to HMI Application

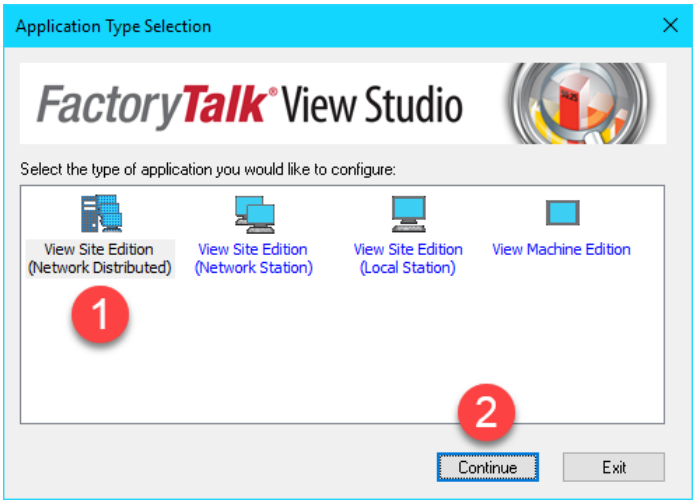
1. To begin this section, launch a remote desktop session on **RDS2** if you don't already have one open.



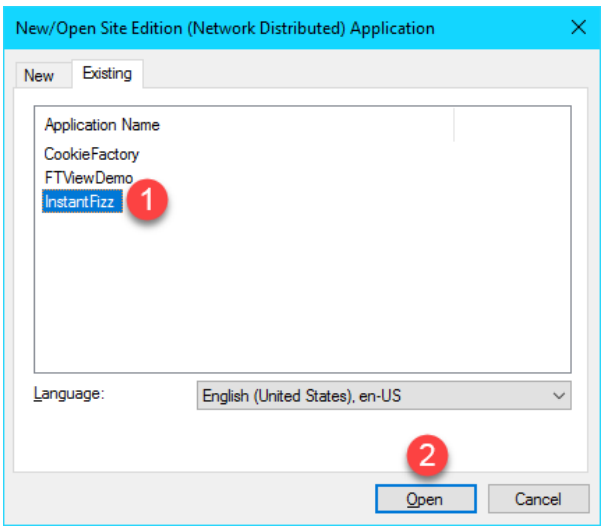
2. While still on **RDS2**, open **FactoryTalk View Studio** from the **Windows Start Menu**.



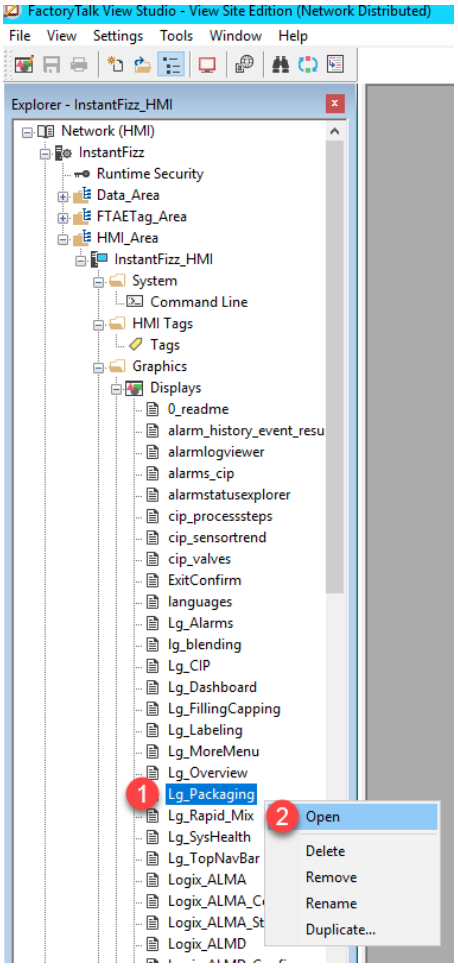
3. Select **View Site Edition (Network Distributed)**, click **Continue**



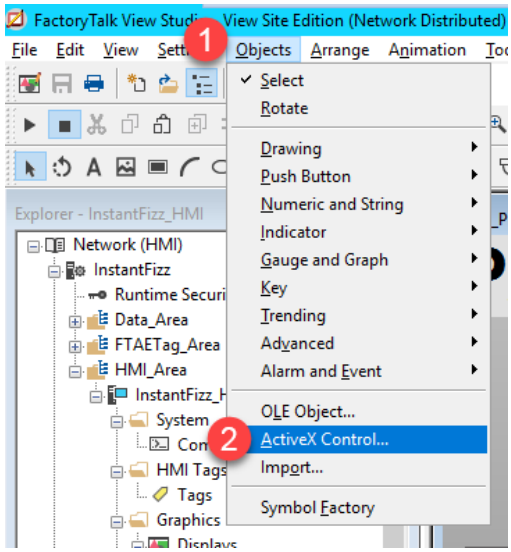
4. Select the **InstantFizz** application and click the **Open** button.



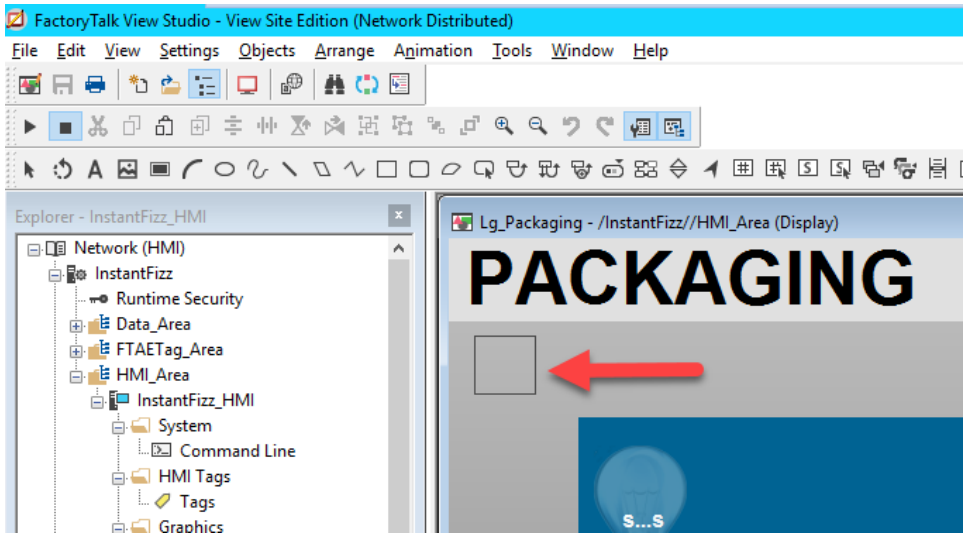
5. Browse to the **HMI_Area > InstantFizz_HMI > Graphics > Displays > Lg_Packaging** display object in the Explorer Window, right click and select **Open**.



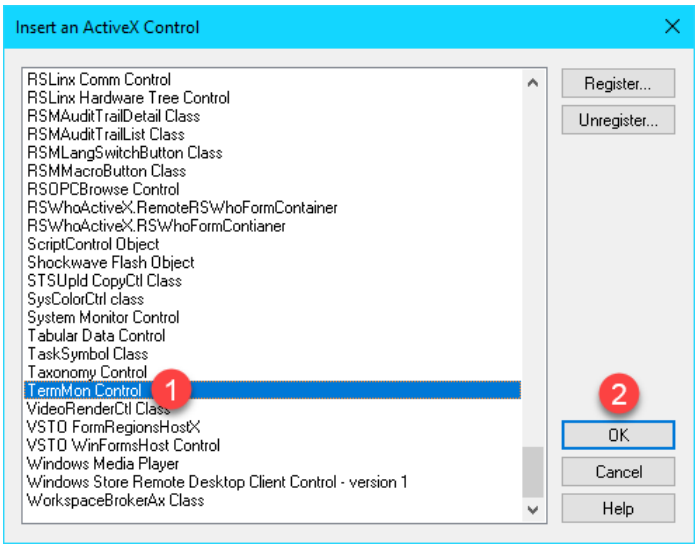
6. Click the **Objects** drop down menu, and select **ActiveX Control**



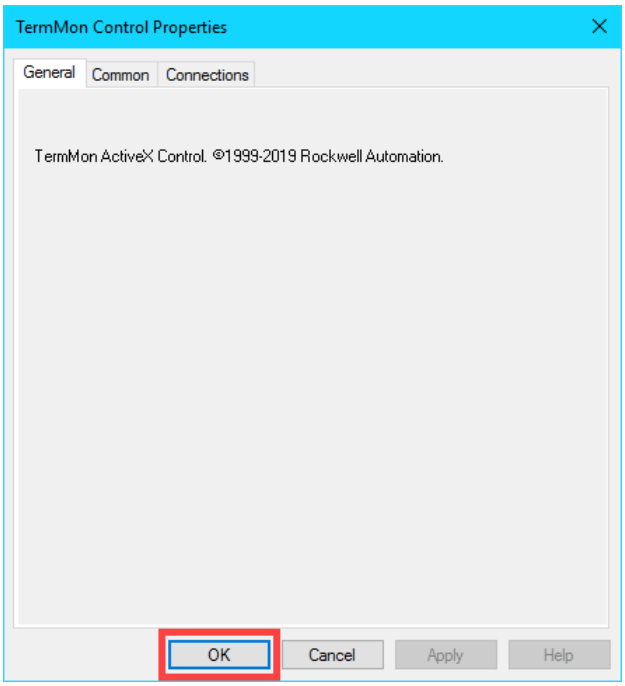
7. Click and drag within the **Lg_Packaging** display window to draw the ActiveX object into the display. The object will be invisible once it is drawn, this is ok.



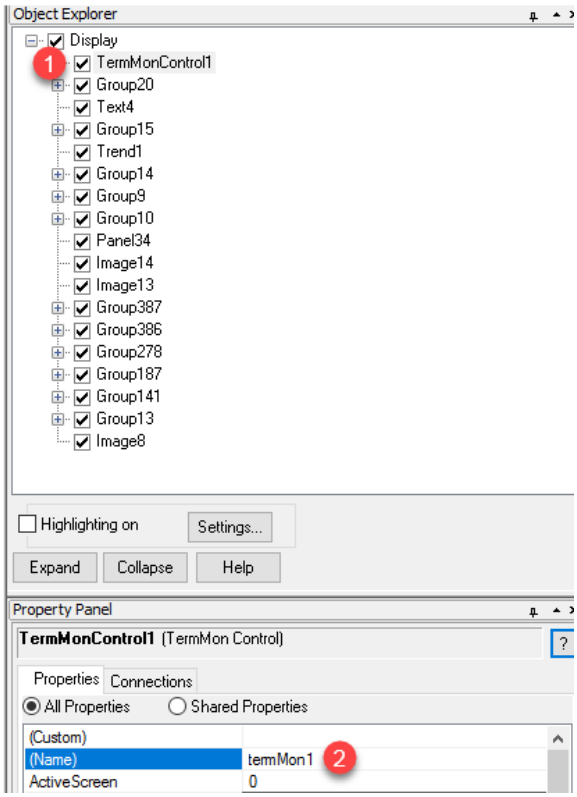
8. The **Insert an ActiveX Control** menu will display. Scroll down near the bottom and locate the **TermMon Control**. Select it and click the **OK** button.



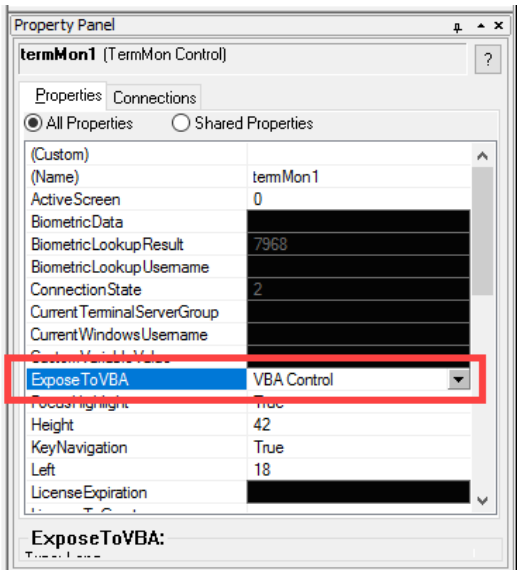
9. It may take a few seconds for the **TermMon Control Properties** configuration window to open. Once it does, click the **OK** button.



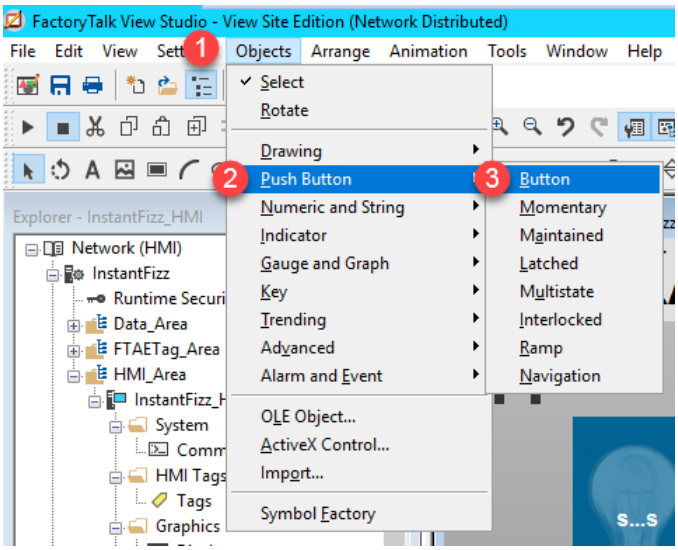
10. In the right-hand pane of **View Studio**, within the **Object Explorer** menu, click on the **TermMonControl1** object. The **Property Panel** below will show the **Properties** and **Connections** tabs of the object. You may have to temporarily expand the size of the right-hand pane menus to read the properties. Make sure the **Properties** tab is selected and click inside the **(Name)** property field to rename the object to *termMon1*.



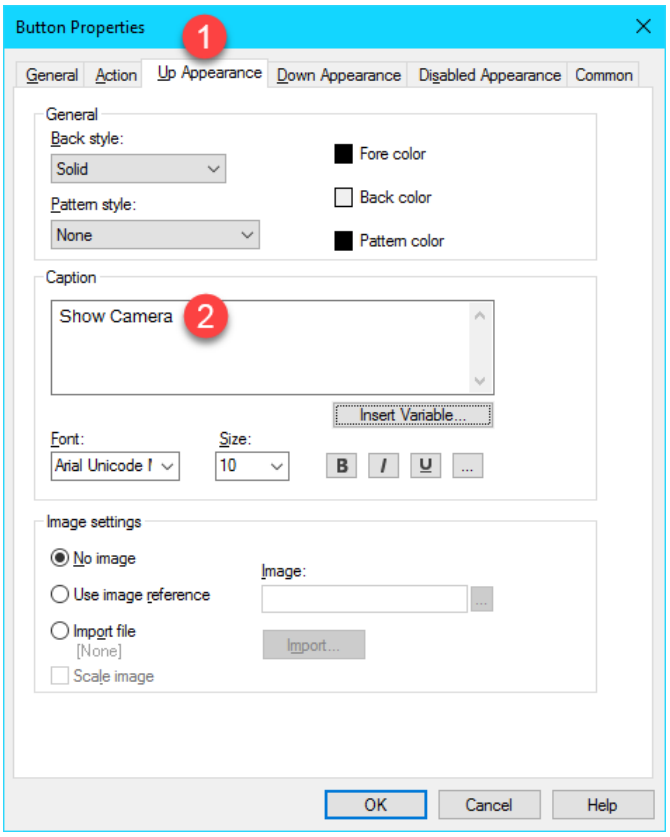
11. Locate the **ExposeToVBA** property in the same **Properties** panel and set it to **VBA Control**.



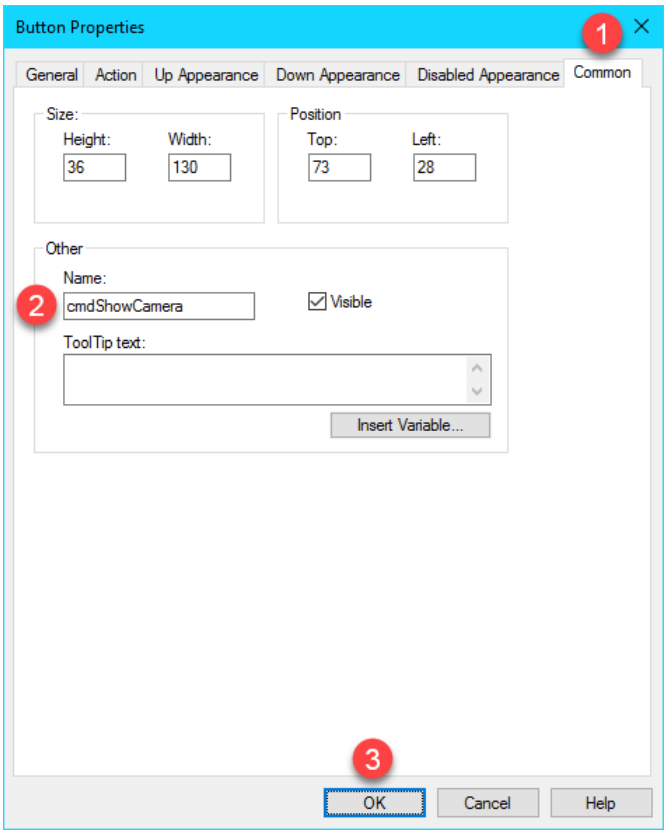
12. Add a **button** object to the display by clicking on the **Objects** menu item and select **Push Button > Button**. Draw the button on to the display by clicking and dragging.



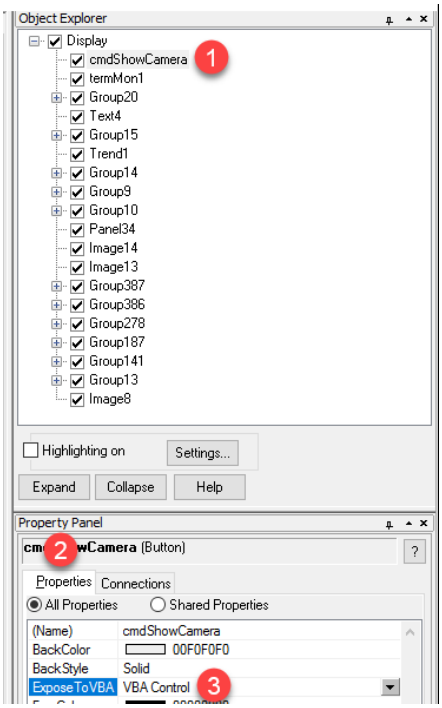
13. The **Button Properties** configuration will popup, click on the **Up Appearance** tab and input *Show Camera* into the **Caption** field.



14. Still on the **Button Properties** window, click the **Common** tab, and enter *cmdShowCamera* in the **Name** property. Click the **OK** button.

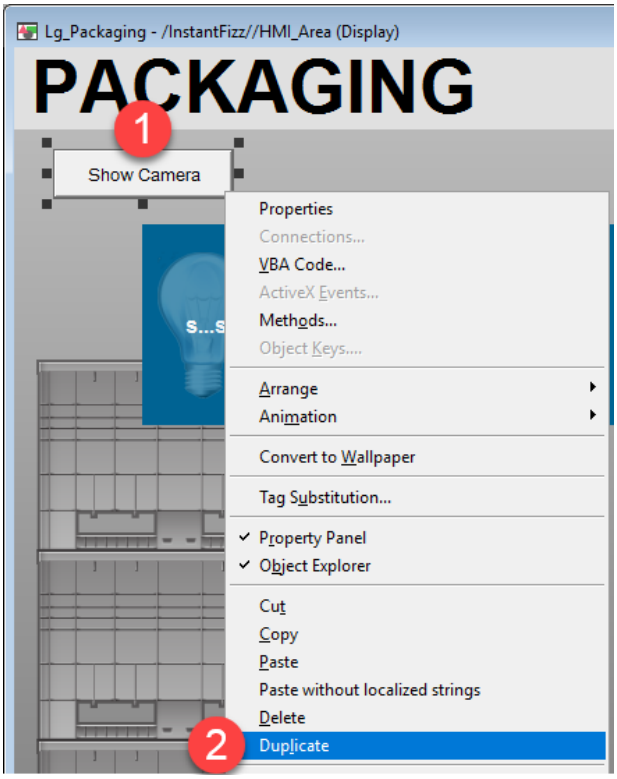


15. Return to the **Object Explorer** pane on the right-hand side of **View Studio**, select the newly created **cmdShowCamera** object. From the Property Panel set the **ExposeToVBA** property to **VBA Control**.

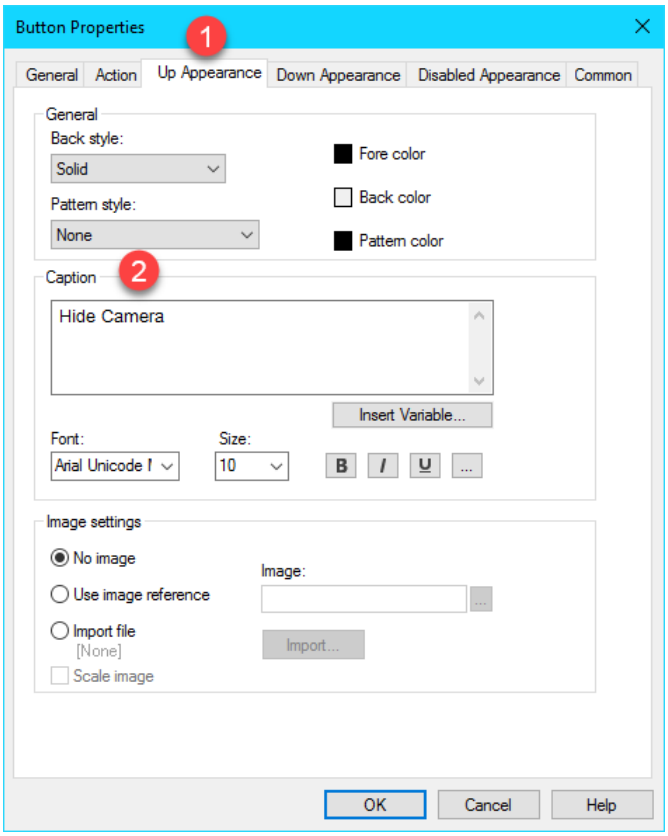


16. Add another push button to the **Lg_Packaging** display next to the **Show Camera** button just created. To do this, right click the **Show Camera** button and select **Duplicate.** Move the duplicated button along-side the initial **Show Camera**

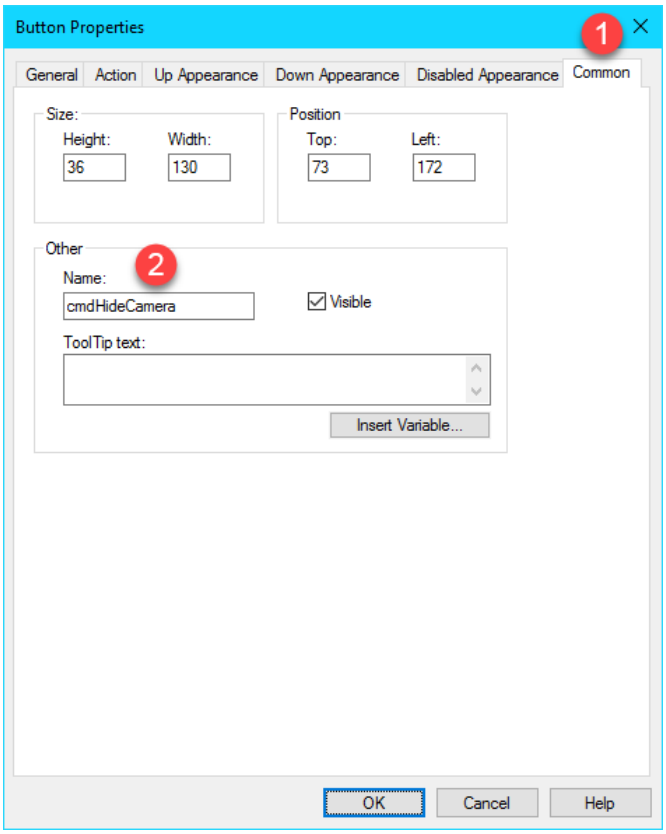
button. Double click the new button to open the **Button Properties** window.



17. The **Button Properties** configuration will popup, click on the **Up Appearance** tab and input *Hide Camera* into the **Caption** field.

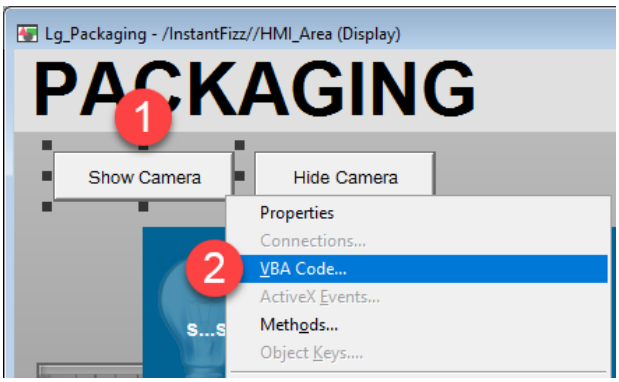


18. Still on the **Button Properties** window, click the **Common** tab, and enter *cmdHideCamera* in the **Name** property. Click the **OK** button.

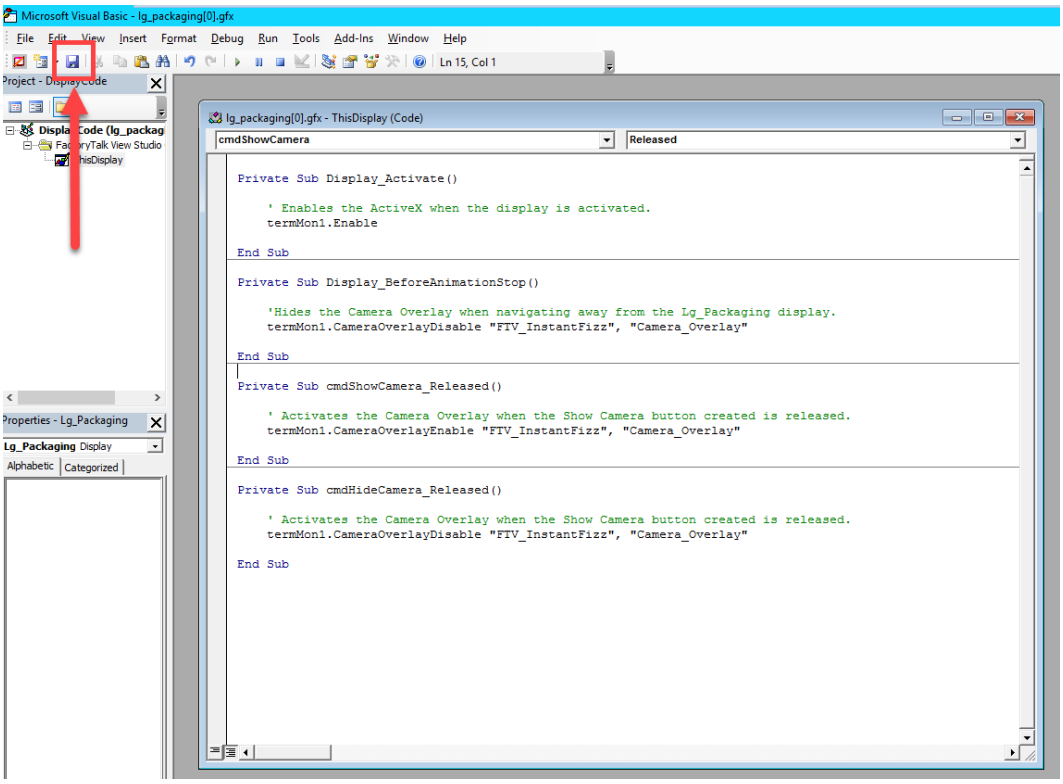


> Since we duplicated the **Show Camera** button, the **ExposeToVBA** property will already be properly set to **VBA Control** for the **Hide Camera** button.

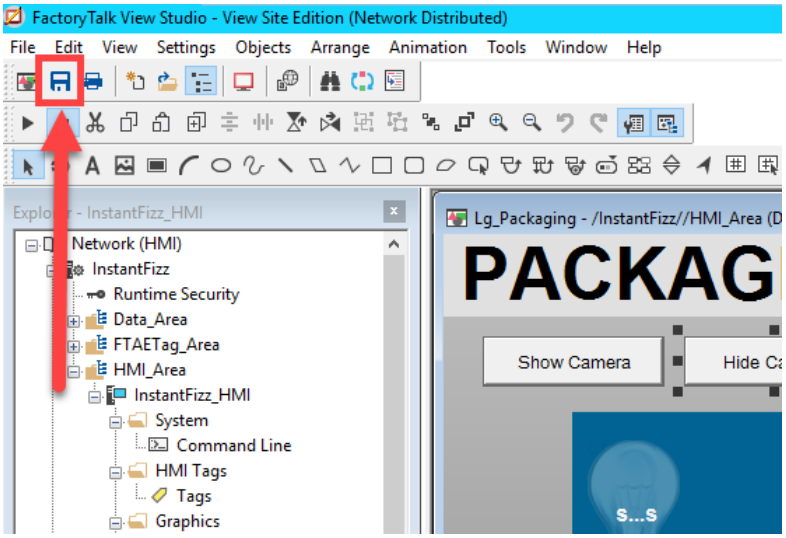
19. Inside the **Lg_Packaging** display, right click on the **Show Camera** button and select **VBA Code…**



20. The **Microsoft Visual Basic Editor** will open (you may have to select it in the **Windows Taskbar** ) with the **DisplayCode** for the **Lg_Packaging** display. First, select all of the text in the code window and **Delete** it. Then copy all of the text from the **C:\Lab Files\ActiveX VBA Code.txt** file and **Paste** it into the **DisplayCode** window. Please find comments in the text file to explain the functions used in this example. Click the **Save** icon and close the **Visual Basic Editor**.



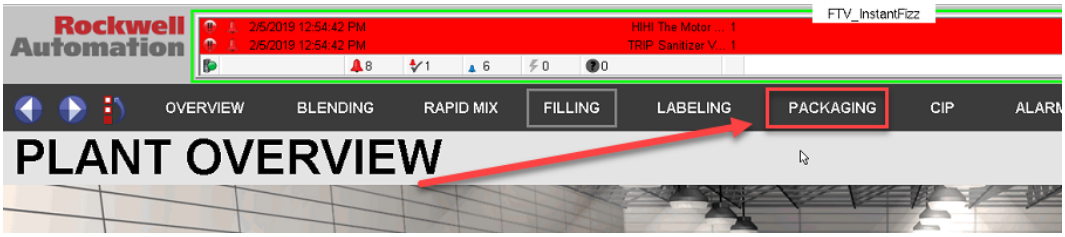
21. Save the changes to the **Lg_Packaging** display from the main menu.



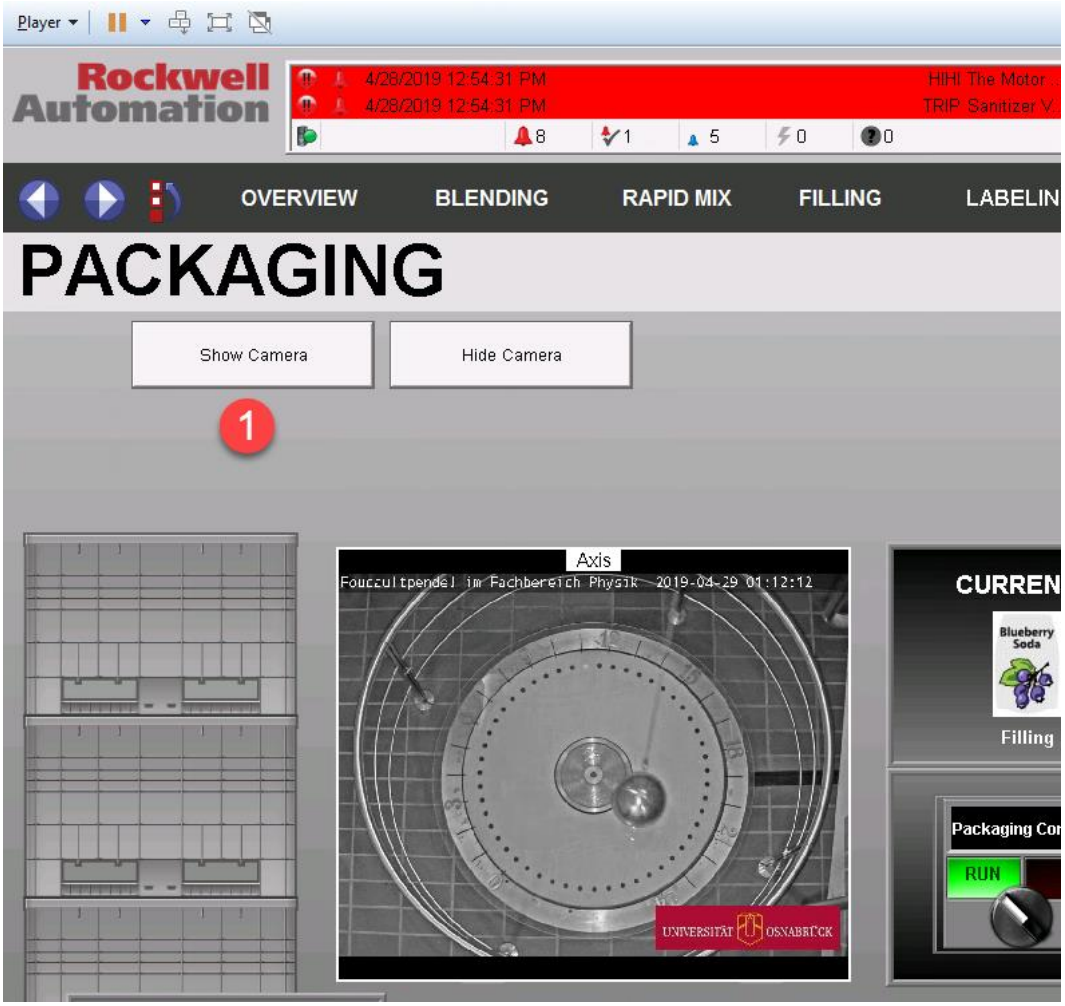
Test Camera Overlay Visibility

1. Close the remote desktop session on **rds2.tmlab.loc** to return to **RDS1**. Click the **OK** button on the confirmation dialog box.

2. From the virtual thin client, click on the **PACKAGING** button on the main overview screen from the navigation bar. It may take a few seconds for the **Lg_Packaging** screen to load.



3. Click the **Show Camera** button. The **CameraOverlayEnable** method of the **TermMon ActiveX** control will be called and the camera will display.



4. Click the **Hide Camera** button to hide the camera. This calls the **CameraOverlayDisable** method.
5. The disable method is also called when navigating away from the **Lg_Packaging** screen. Test this by enabling the camera and then navigating back to the overview screen without clicking the disable button.

As demonstrated in the previous steps, the **TermMon.ocx** is embedded within an ActiveX container – FactoryTalk View SE in the example provided. Then an instance of the FactoryTalk View SE application is running within a Remote Desktop Server session and is delivered to the virtual thin client. When the Lg_Packaging display is launched in View SE, the Display_Activate event fires and the termMon1.Enable method is called. This method establishes a connection between the **ActiveX** control and the terminal on which it is running.

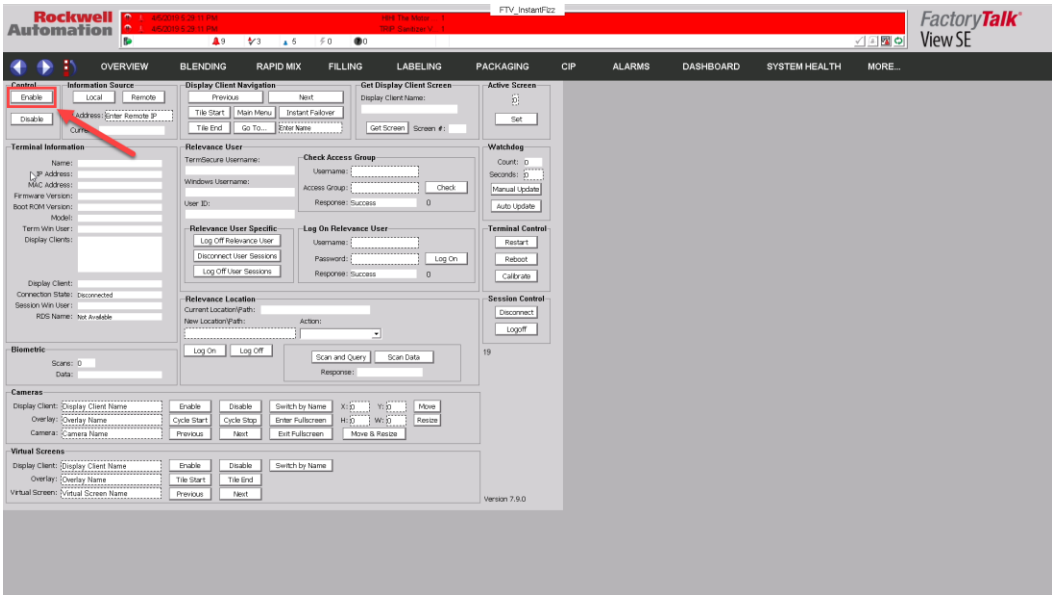
There also exists the **TermMon ActiveX Configuration Module**, which can be applied to a specific terminal from the **ThinManager Admin Console**. This module allows you to specify whether the terminal will permit **ActiveX** connections, and if so, if they can be established from local or remote sessions. If remote sessions are permitted, this would enable **TermMon** to control other terminals remotely. Version 7.9.0 of **TermMon** also permits the ability to enable/disable **Relevance User Changed Events**, which essentially allows you to enable/disable **Authentication Pass Through** for FactoryTalk View SE.

Earlier versions of **TermMon.ocx** (versions prior to 7.8.0) only supported a single event called **OnEvent**. It included an **EventCode** parameter that would indicate which event had been raised (i.e.: EventCode = 17 would indicate the terminal's **Relevance Location** had changed). With 7.8.0 and newer, there are now separate events. So to respond to a **Relevance Location** change event, you can use the **OnRelevanceLocationName** event, which includes the current **RelevanceLocationName** as a parameter).

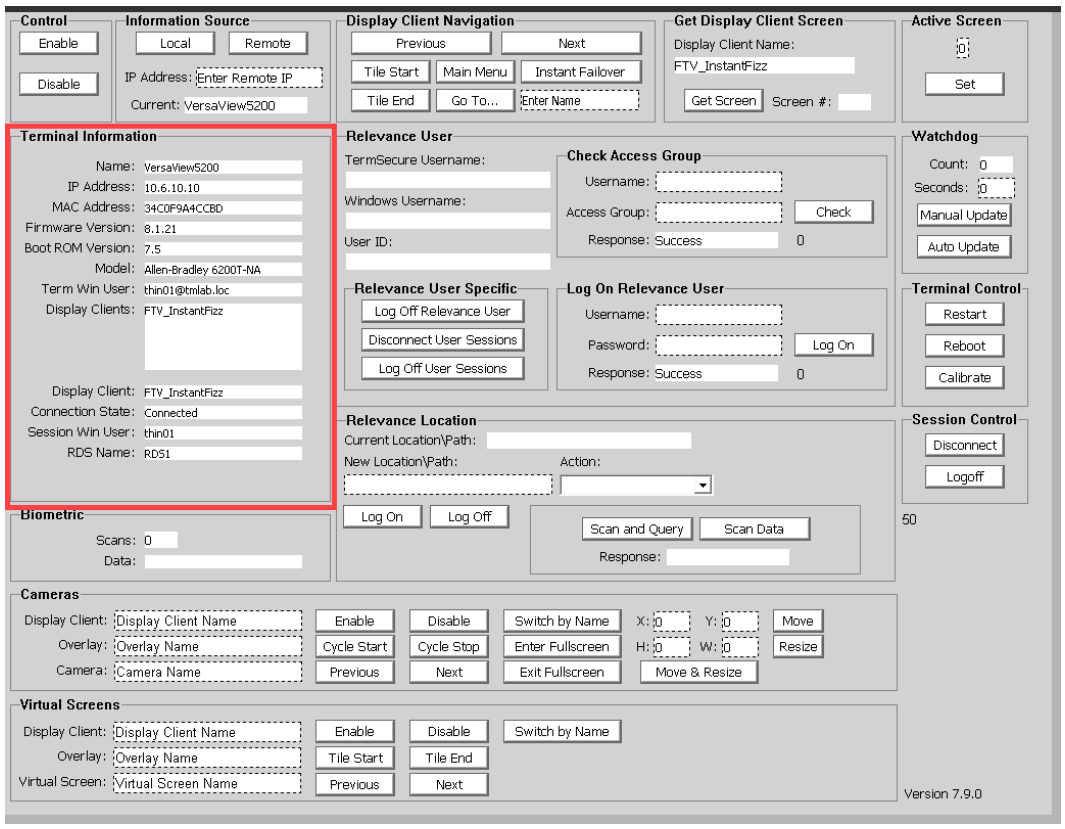
Explore TermMon Test Display

1. From the **PACKAGING** display, click the **MORE…** navigation button followed by the **TERMMON** menu item.

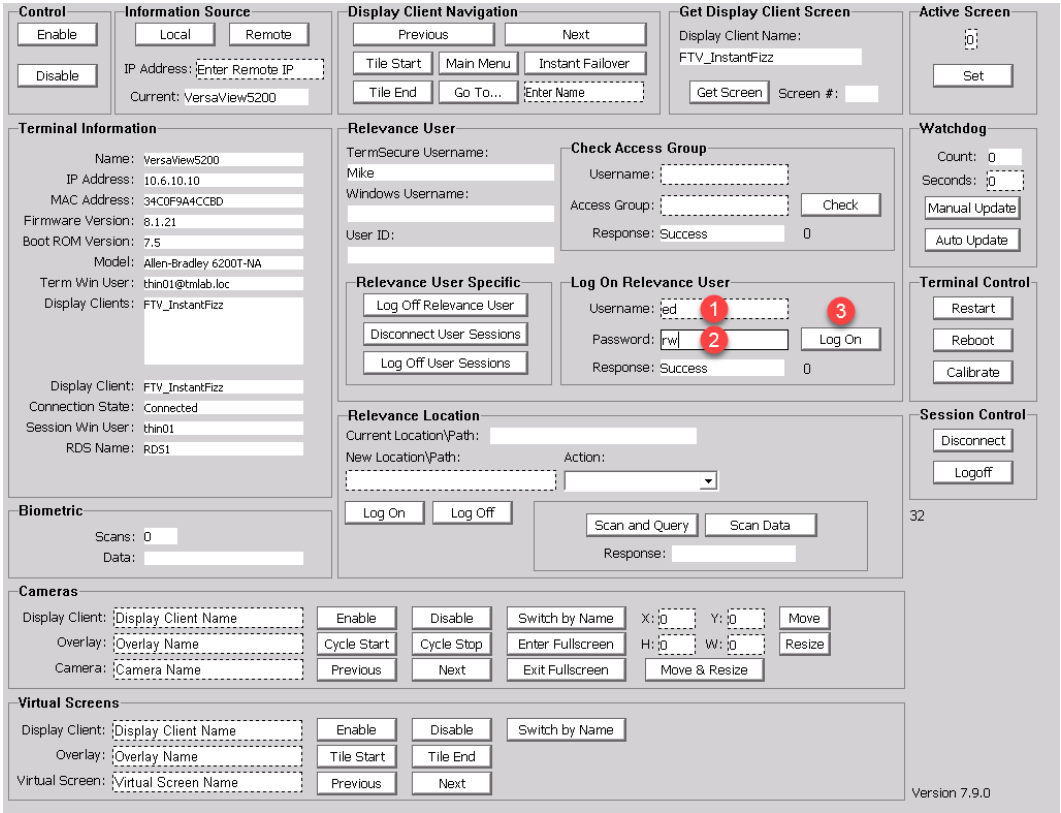
2. The **TERMMON** display demonstrates a majority of the **TermMon.ocx Object Model**. To start exploring, first click the **Enable** button in the top left corner of the display. This calls the **Enable** method of the **ActiveX** control and initiates a connection between the **InstantFizz Display Client** and the terminal to which it is being delivered.



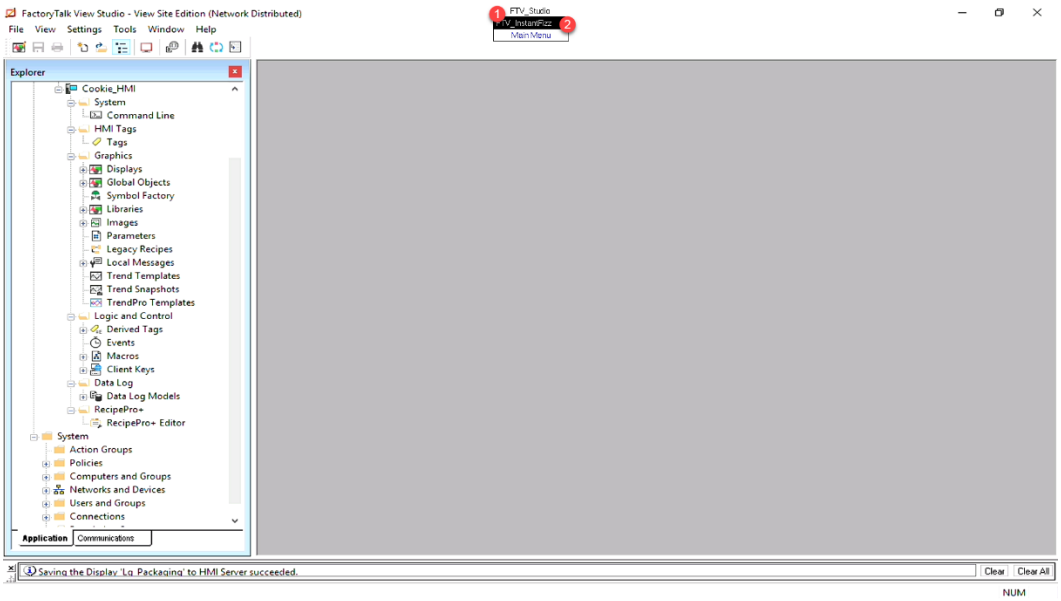
3. Upon clicking the **Enable** button, the **Terminal Information** frame should fill in the **Properties** listed.



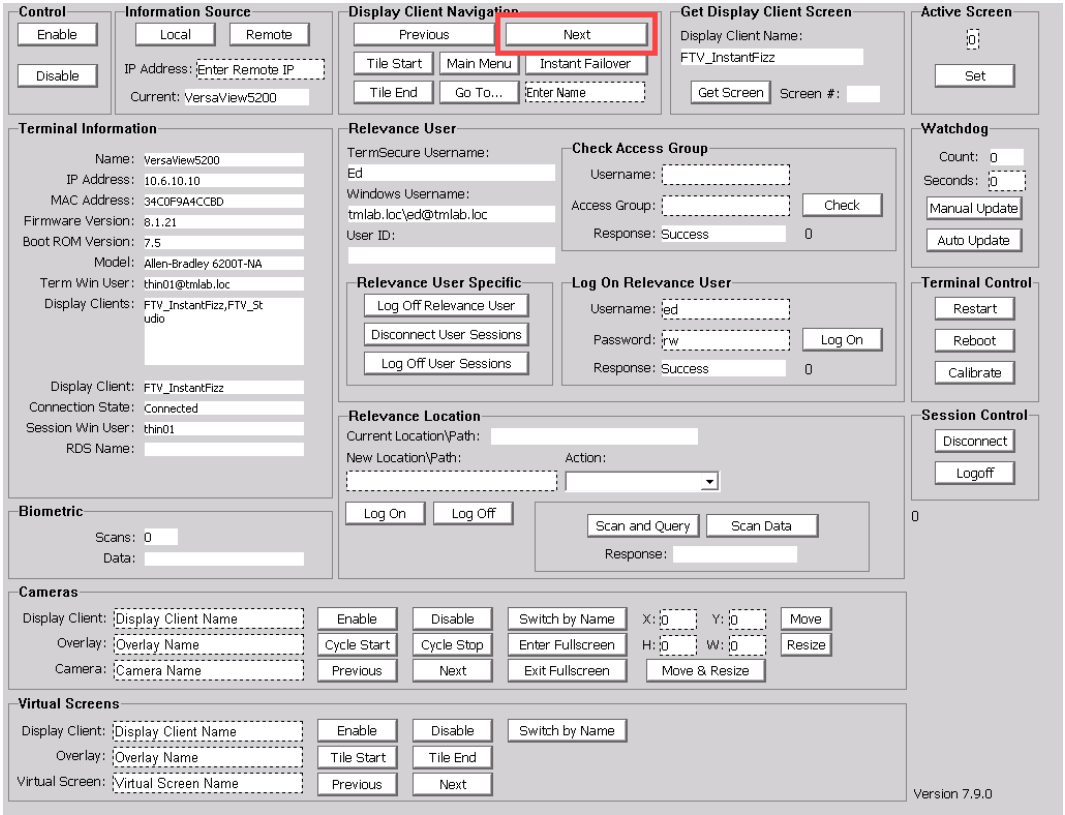
4. In the **Log On Relevance User** frame, enter *ed* in the **Username** input box and *rw* in the **Password** input box. Click the **Log On** button. You should be presented with a PIN dialog – enter *1234*. This will programmatically login Ed as a Relevance User and deliver the **FTV_Studio Display Client** (since this **Display Client** was assigned to the **Engineer Relevance User Group** in the Section 9).



5. Click and hold the **Display Click Selector**, hover over the **FTV_InstantFizz Display Client** release to return to the **FTV_InstantFizz Display Client**.

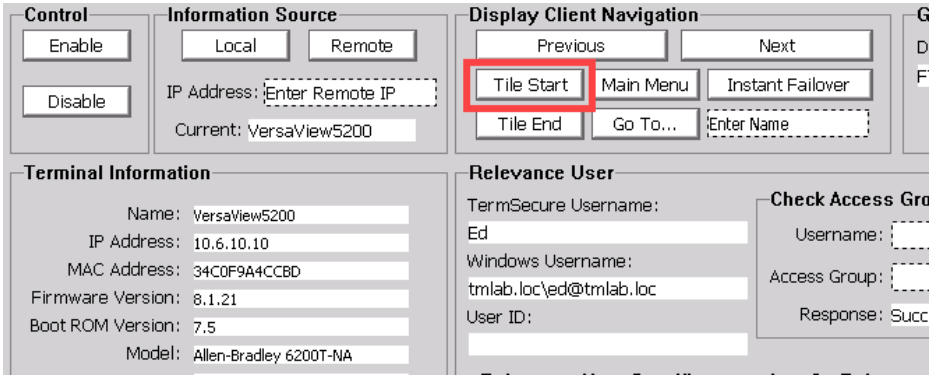


6. From the **Display Client Navigation** frame, click the **Next** button.



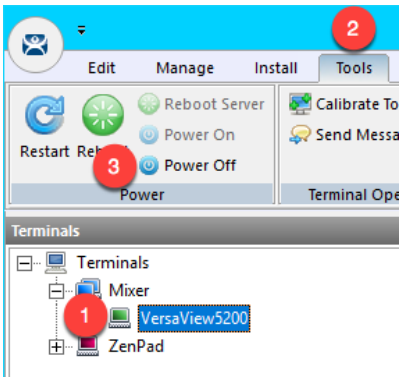
7. Click and hold the **Display Click Selector**, hover over the **FTV_InstantFizz Display Client** release to return to the **FTV_InstantFizz Display Client**.

8. From the **Display Client Navigation** frame, click the **Tile Start** button. This should trigger Tile Mode to start.



9. Feel free to explore some more with **TermMon** test display. You can return to **RDS2** and open the **termmon** display from **View Studio** to inspect some of the associated **VBA code**. To find out more about the **TermMon ActiveX** control, please refer to this [ThinManager Knowledgebase Article].

10. When finished power off the **VersaView5200** terminal.



This completes the section **Programmatic Terminal Monitoring and Control with ThinManager TermMon ActiveX** of the lab. Please continue on to the **Virtual Thin Clients, PXE Server and Wireshark** section of the lab.

Section 19: Virtual Thin Clients, PXE Server and Wireshark

Overview

To review from Section 4, 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. The **VersaView 5200** (Catalog #: **6200T-NA**) box thin client used in this lab is an example of a **ThinManager Ready** terminal.

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**X**ecution **E**nvironment (PXE) is an Intel standard whereby an operating system can be delivered over the network.

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

In this section we will create a virtual thin client and configure **ThinManager** as a **PXE Server** in order to deliver the **ThinManager** firmware to it. We will also introduce **Wireshark** to examine how **ThinManager** managed thin clients actually boot from a network perspective, and how this process differs slightly for **ThinManager Ready** and **ThinManager Compatible** terminals.

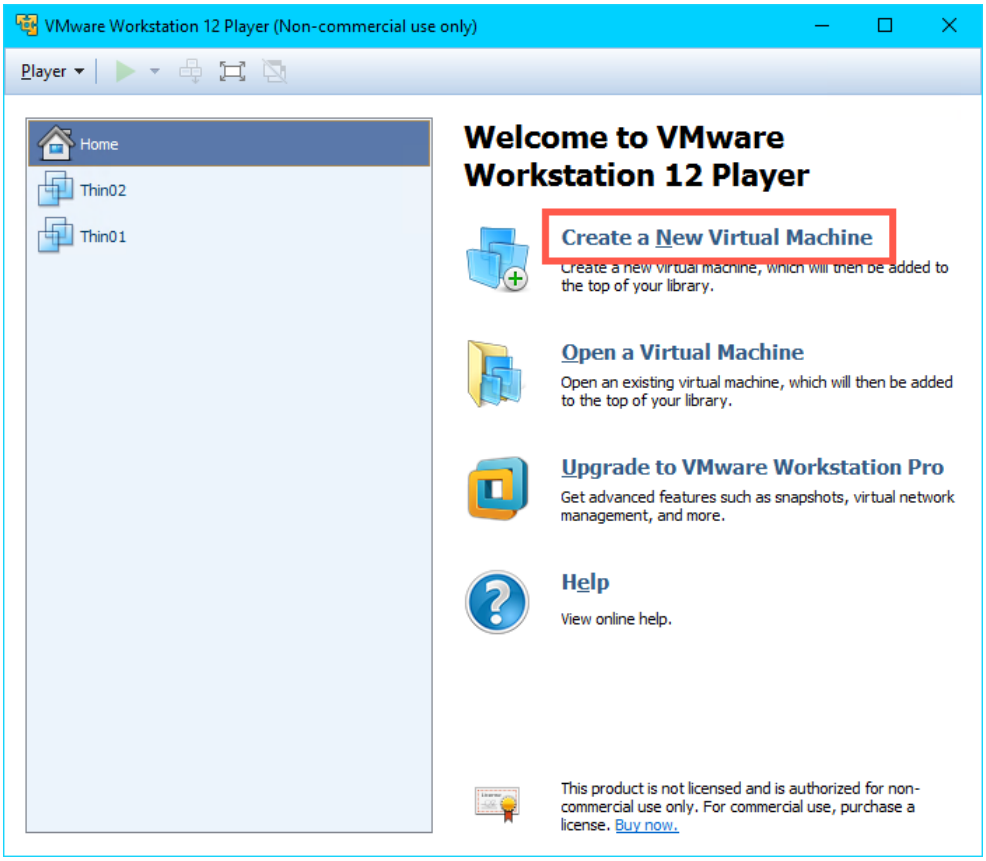
1. Create Virtual Thin Client
2. Modify PXE Server Mode
3. Create Terminal for Virtual Thin Client
4. Re-Enable Firewall Rules
5. Start Wireshark Capture
6. Troubleshoot the Boot Process
7. Boot Virtual Thin Client via UEFI

Create Virtual Thin Client

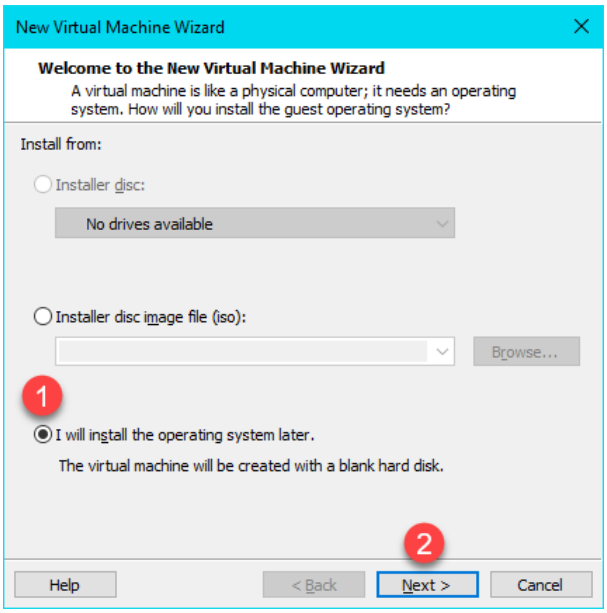
As demonstrated through this Cloud lab, a virtual thin client is fairly simple to create and can be a great tool for troubleshooting, testing and education. In this section, we will use VMWare's free Workstation Player to create a new virtual machine without an Operating System, which we will subsequently boot via ThinManager's PXE Server.

1. Double click the **VMWare Player** shortcut on the **RDS1** desktop.

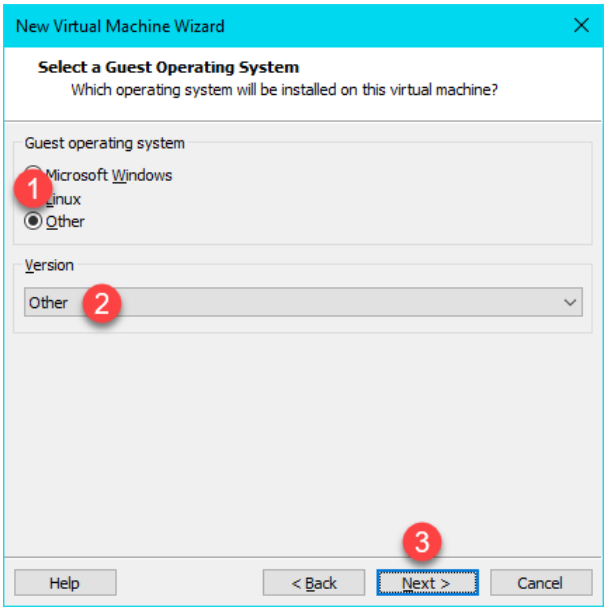
2. From **VMWare Workstation Player** click the **Create a New Virtual Machine** link.



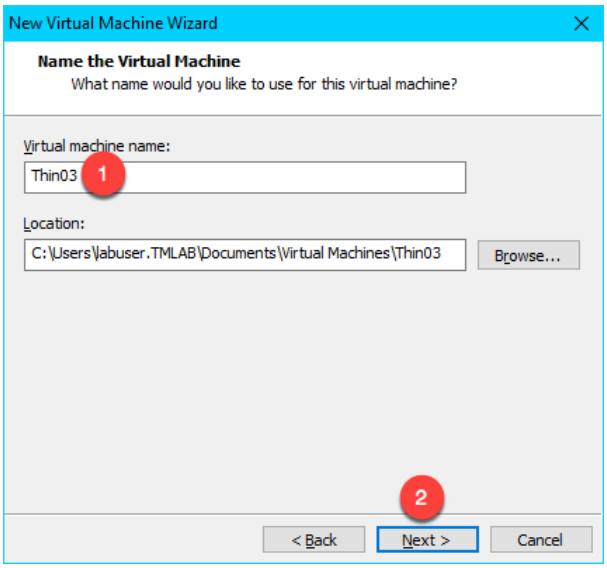
3. From the **New Virtual Machine Wizard**, select the **I will install the operating system later** radio button. Click the **Next** button.



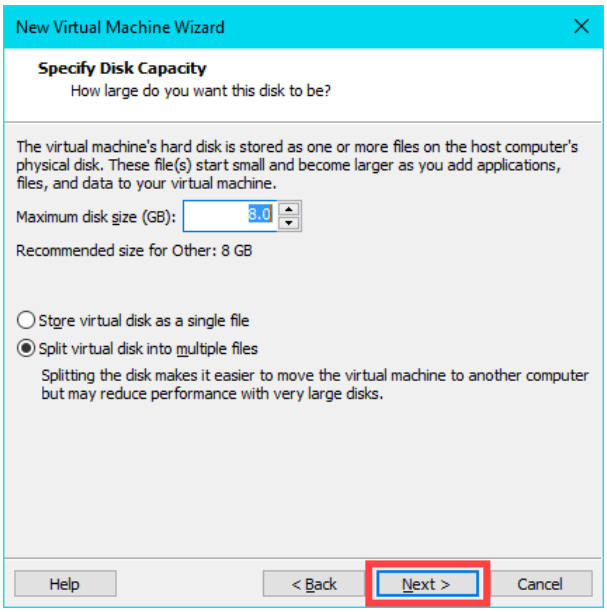
4. From the **Select a Guest Operating System** page of the wizard, select the **Other** radio button, **Other** from the **Version** drop down list and click the **Next** button.



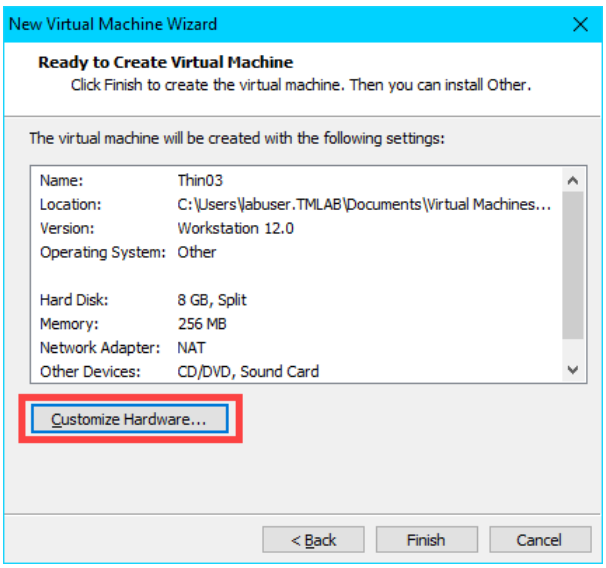
5. From the **Name the Virtual Machine** page of the wizard, enter *Thin03* as the **Virtual machine name**. You can leave the default **Location**. Click the **Next** button.



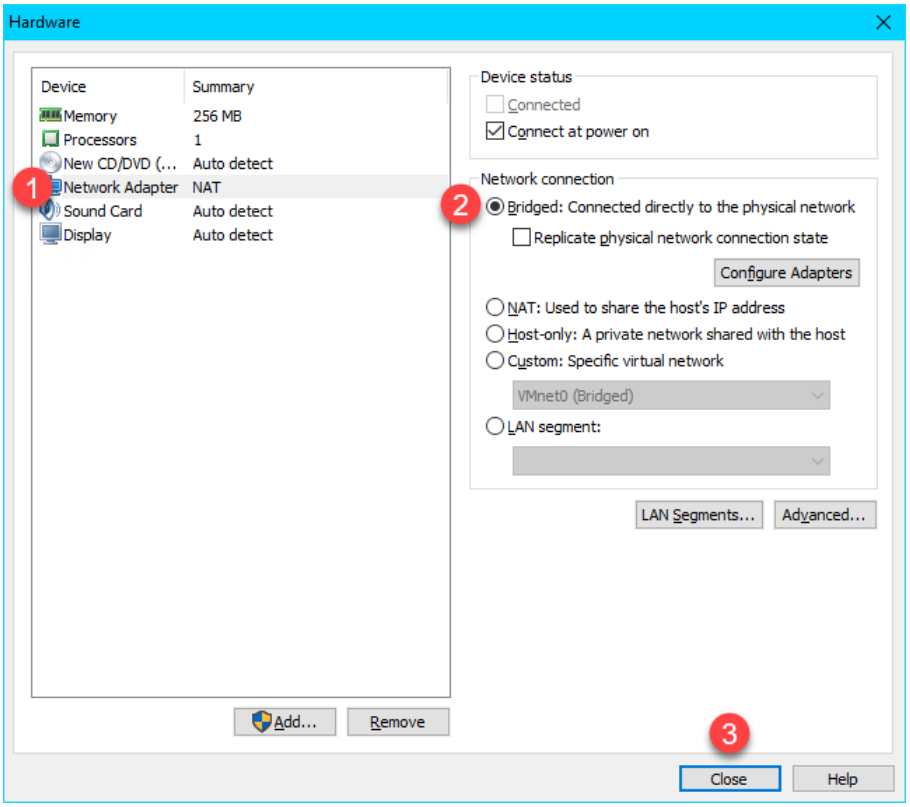
6. Click the **Next** button on the **Specify Disk Capacity** page of the wizard, keeping the defaults.



7. Click the **Customize Hardware** button on the **Ready to Create Virtual Machine** page of the wizard.

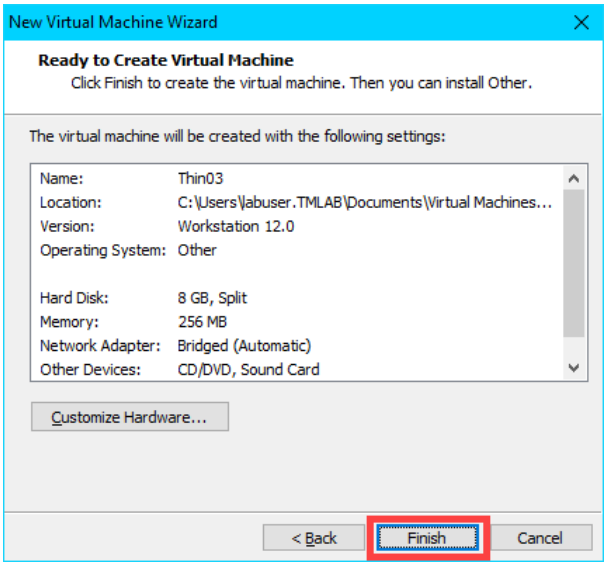


8. From the **Hardware** window, select the **Network Adapter** device and click the **Bridged** radio button. Click the **Close** button.



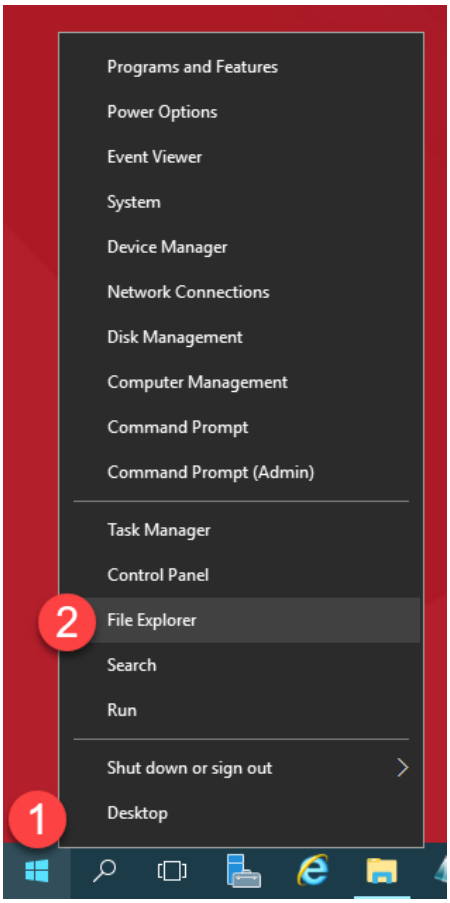
We have been using NAT for our virtual thin clients to this point in the lab. We will switch to Bridged in this section so we can see the desired network traffic in Wireshark. With that said, we will need to modify our PXE Server settings so that ThinManager will issue IP addresses for PXE requests.

9. Back at the **Ready to Create Virtual Machine** page of the wizard, click the **Finish** button.

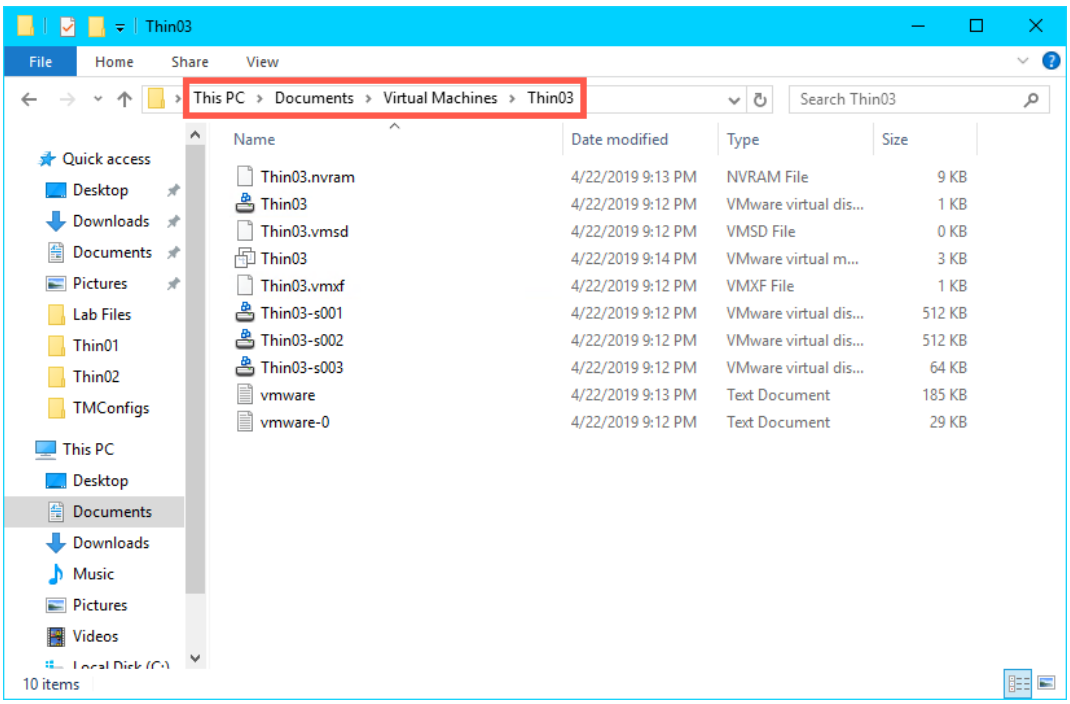


The default 8GB of hard disk space and 256MB RAM is plenty for our virtual thin client.

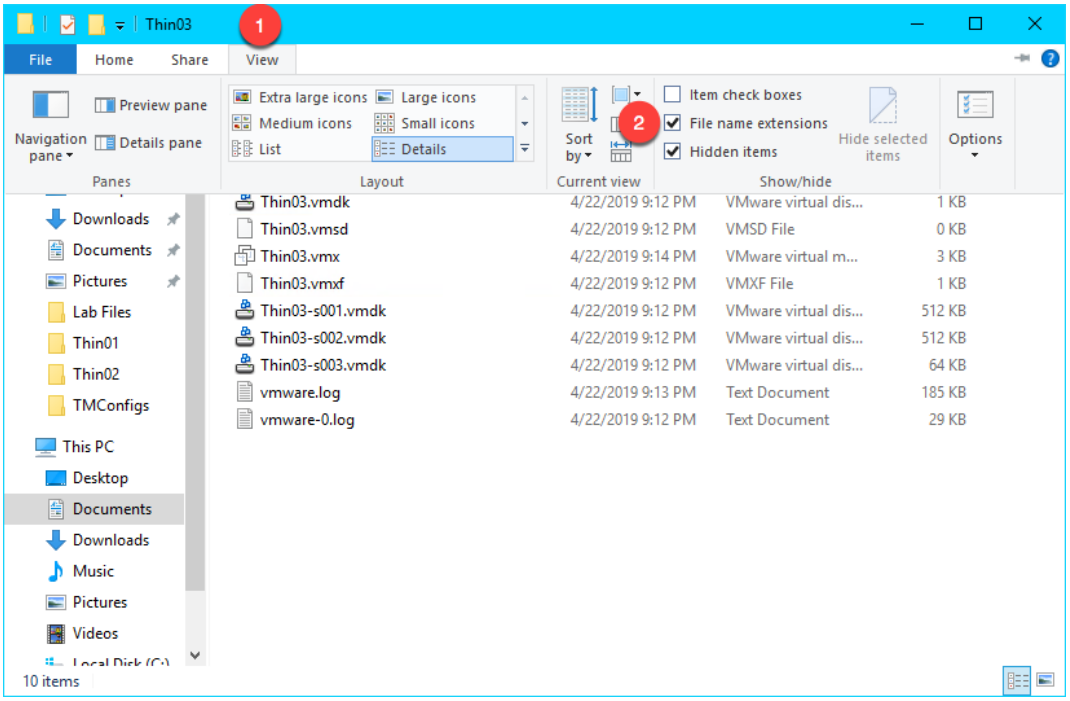
10. Because this virtual thin client is running on a virtual machine (**RDS1**), which is referred to as **nesting**, we need to add a special setting to the virtual machine configuration file for **Thin03**. Right click the **Windows Start Button** and select **File Explorer**.



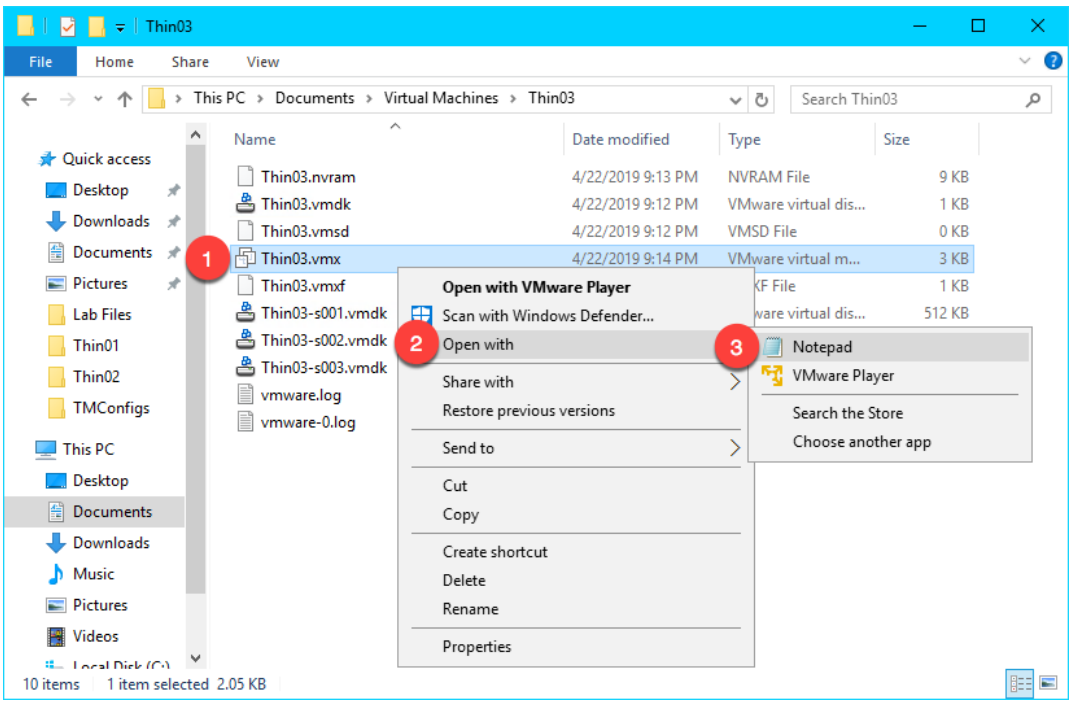
11. Within **File Explorer**, navigate to **Documents->Virtual Machines->Thin03.**



12. Click the **View** menu item and check the **File name extensions** checkbox.

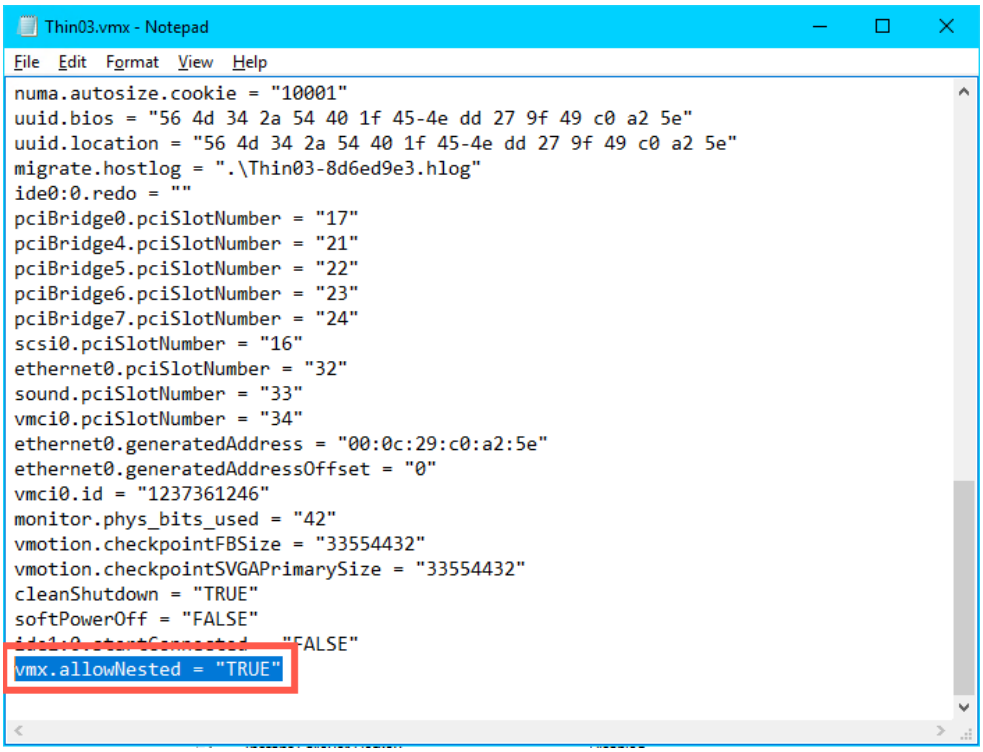


13. Right click **Thin03.vmx** and select **Open with…**



14. Scroll to the bottom of the text file and enter the following on a new line (you can also copy and paste this text from the **LabPaths** file accessible from the RDS1 desktop). **Save** the file and close **Notepad**.

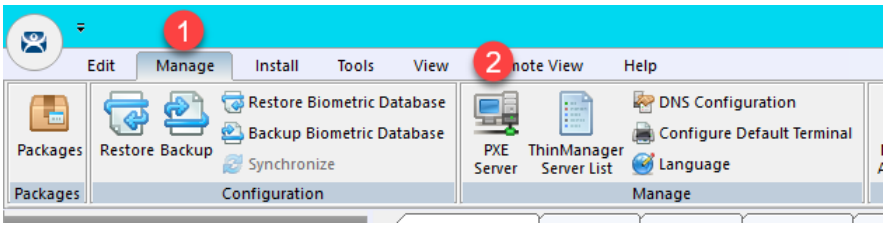
```
vmx.allowNested = "TRUE"
```



Again, the **vmx.allowNested = "TRUE"** setting is only required if you are running your virtual thin client on a virtual host.

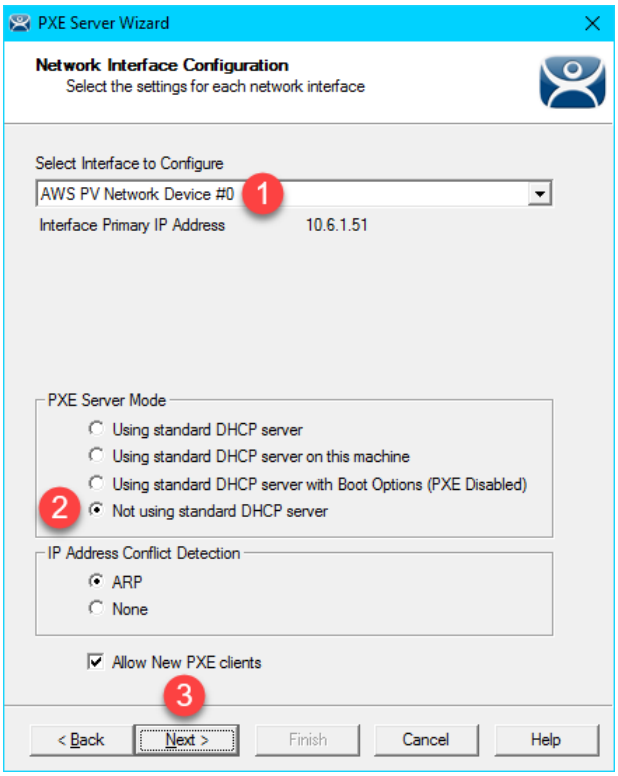
Modify PXE Server Mode

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

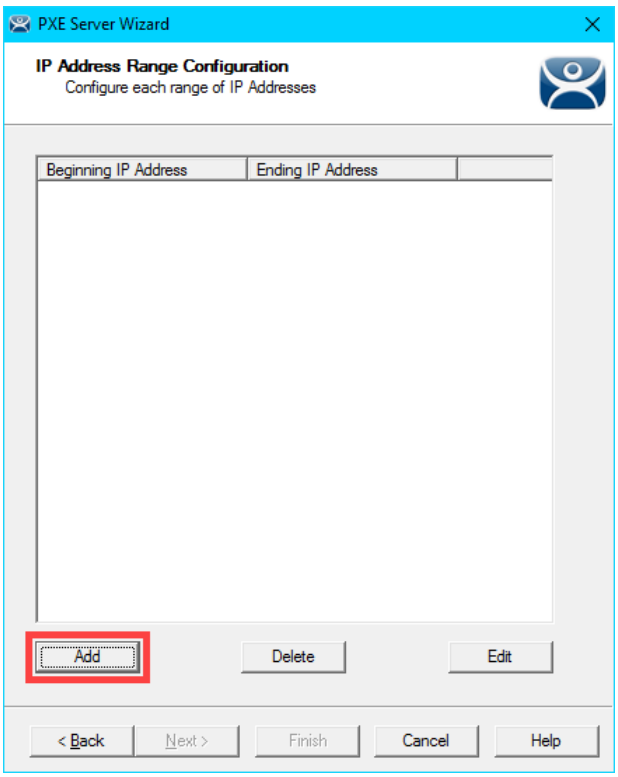


2. Click the **Next** button from the **PXE Server Configuration** page of the wizard.

3. From the **Network Interface Configuration** page of the wizard, select **AWS PV Network Device #0** from the **Select Interface to Configure** drop down list, and select the **Not using standard DHCP server** option button. Click the **Next** button.

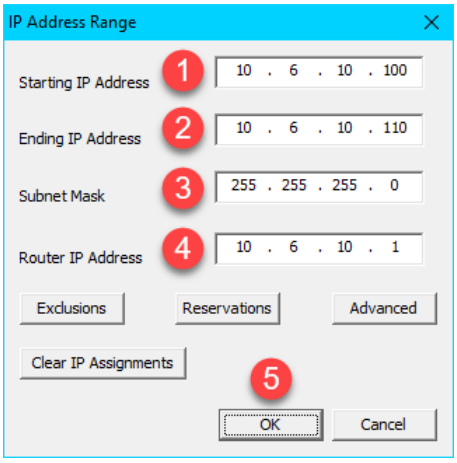


4. From the **IP Address Range Configuration** page of the wizard, click the **Add** button.

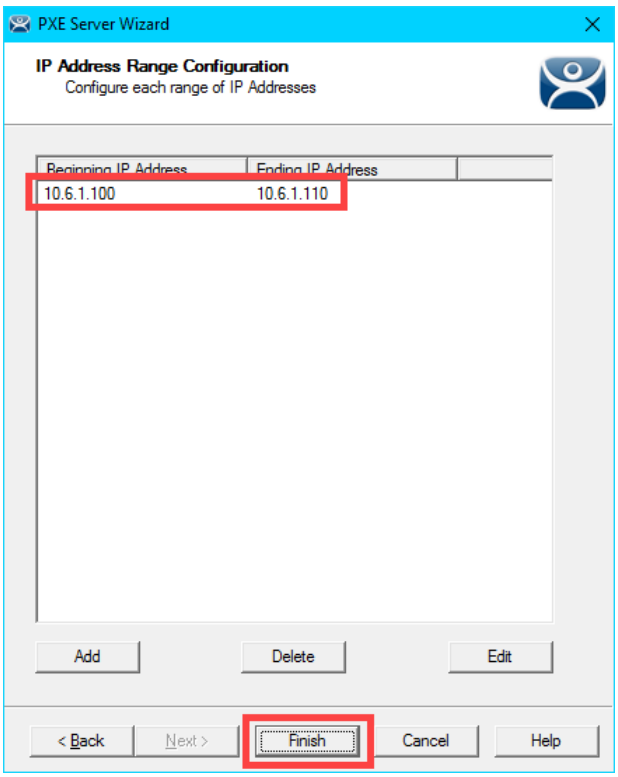


5. From the **IP Address Range** window, enter the following and click the **OK** button.

- **Starting IP Address** = *10.6.10.100*
- **Ending IP Address** = *10.6.10.110*
- **Subnet Mask** = *255.255.255.0*
- **Router IP Address** = *10.6.10.1*



6. Back at the **IP Address Range Configuration** page of the wizard, click the **Finish** button.

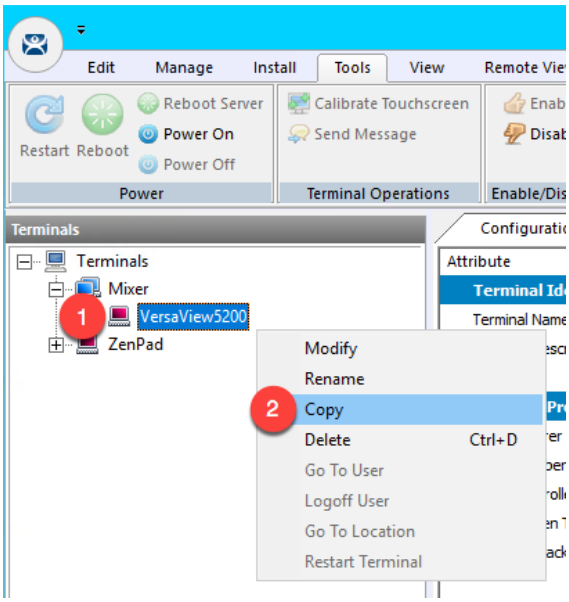


Create Terminal for Virtual Thin Client

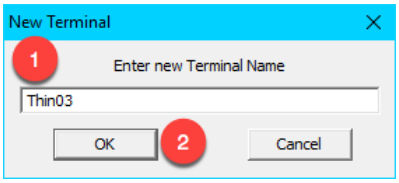
We will create a new **ThinManager Terminal Profile** to assign to our **Virtual Thin Client**.

1. Return to the **ThinManager Admin Console**.
2. Click the **Terminals** tree selector icon.

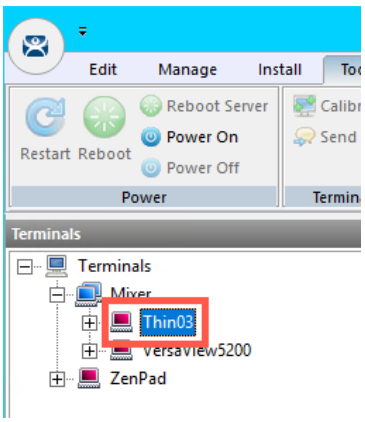
3. From the **Terminals** tree, right click the **VersaView5200** terminal and select **Copy** terminal and select **Copy**.



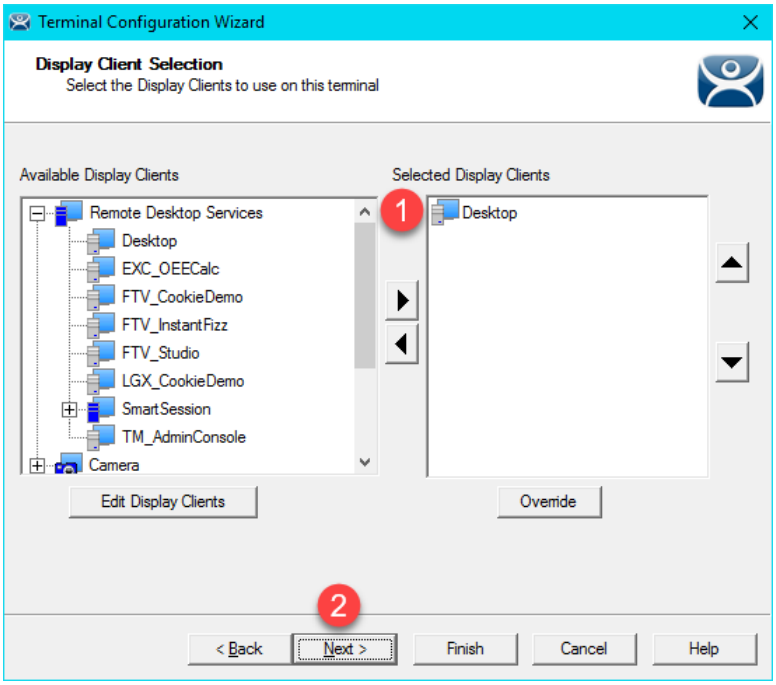
4. Enter *Thin03* as the new **Terminal Name** and click the **OK** button.



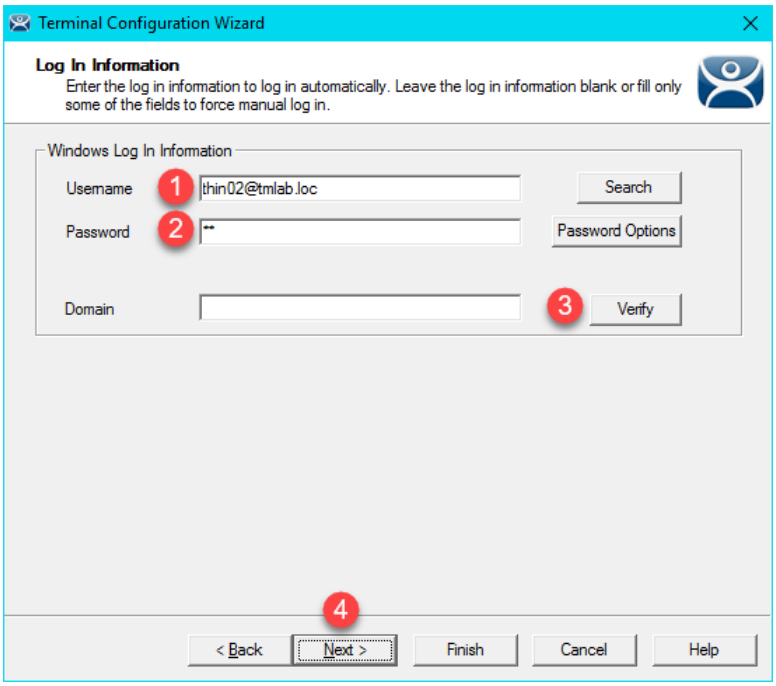
5. With the new terminal created, double click the **Thin03** terminal to launch the **Terminal Configuration Wizard**.



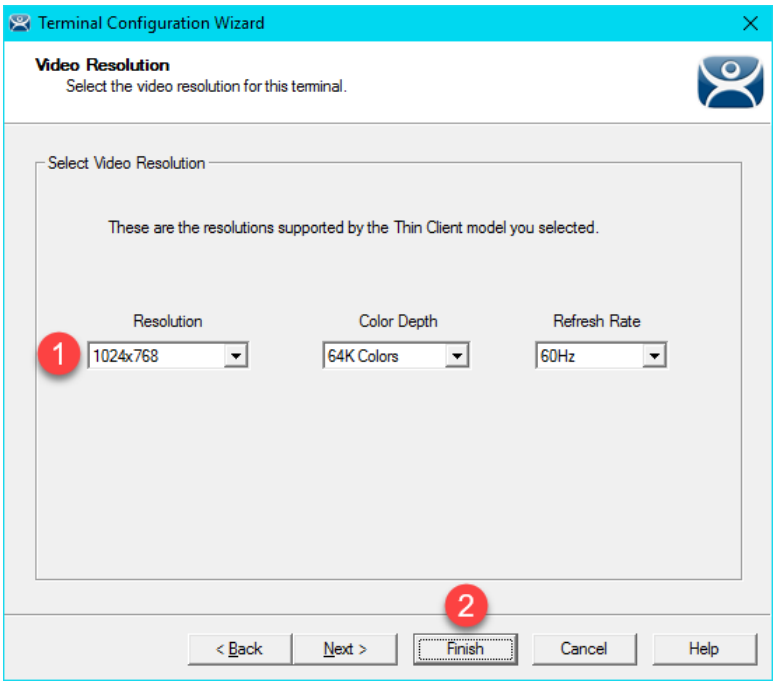
6. Click the **Next** button on the **Terminal Name** page of the wizard.
7. Click the **Next** button on the **Terminal Hardware** page of the wizard
8. Click the **Next** button on the **Terminal Options** page of the wizard.
9. Click the **Next** button on the **Terminal Mode Selection** page of the wizard.
10. From the **Display Client Selection** page of the wizard, remove any existing **Display Clients** from the **Selected Display Clients** list box. Move the **Desktop Display Client** to the **Selected Display Clients** list. Click the **Next** button.



11. Click the **Next** button on the **Terminal Interface Options** page of the wizard.
12. Click the **Next** button on the **Relevance Options** page of the wizard.
13. Click the **Next** button on the **Hotkey Configuration** page of the wizard.
14. On the **Log In Information** page of the wizard, enter *thin02@tmlab.loc* as the **Username** and *rw* as the **Password**. Click the **Verify** button which should confirm that the credentials entered are valid. Click the **Next** button.



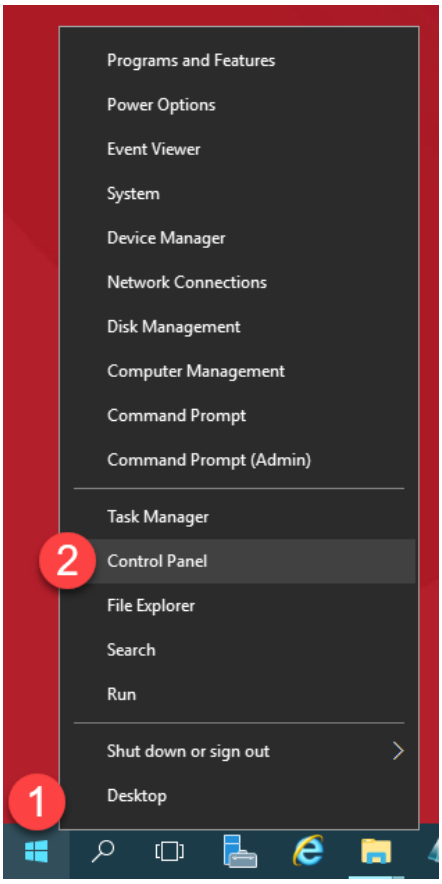
7. From the **Video Resolution** page of the wizard, select **1024x768** from the **Resolution** drop down list. Click the **Finish** button.



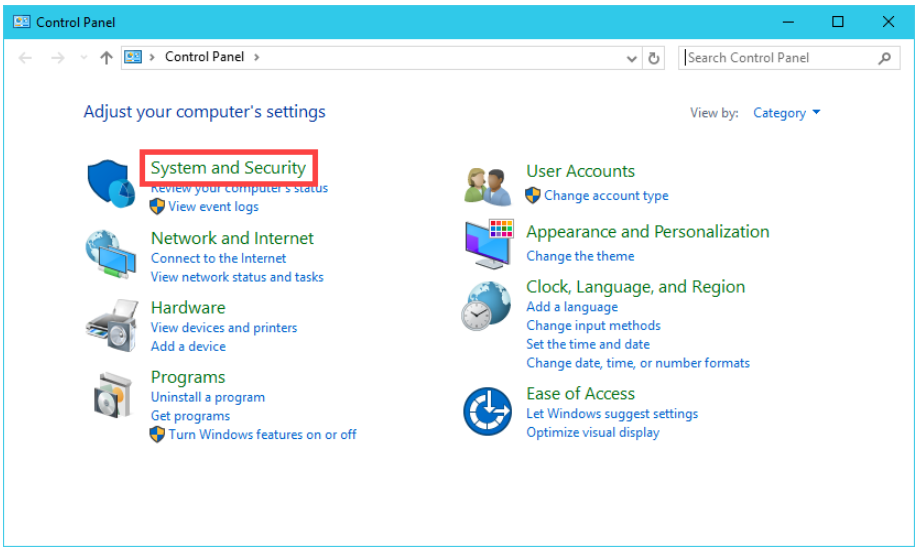
Re-enable Firewall Rules

In Section 11, we turned on the Windows Firewall and created specific Firewall Rules to permit our virtual thin clients to boot. In this section, we are going to disable each of those rules, and use Wireshark to troubleshoot the boot process step by step.

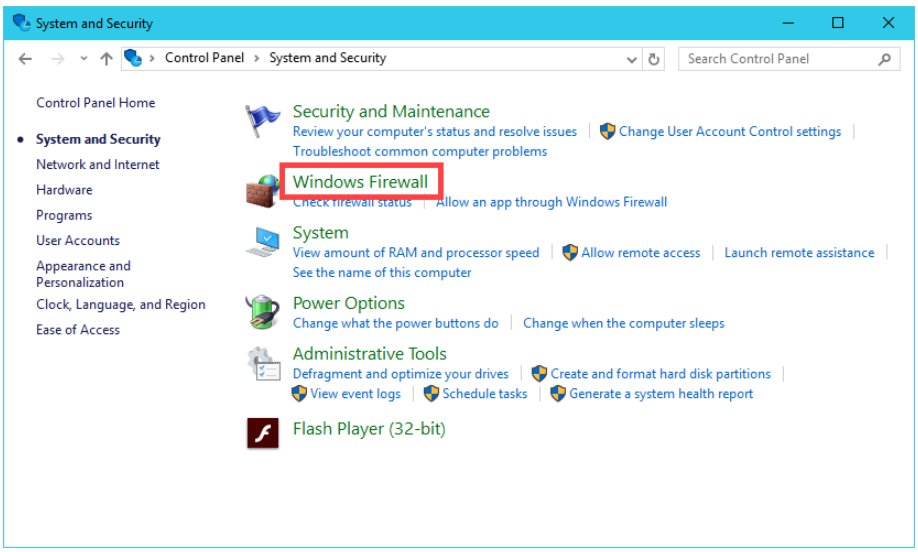
1. While still on **RDS1**, right click the **Windows Start Button** and select **Control Panel**.



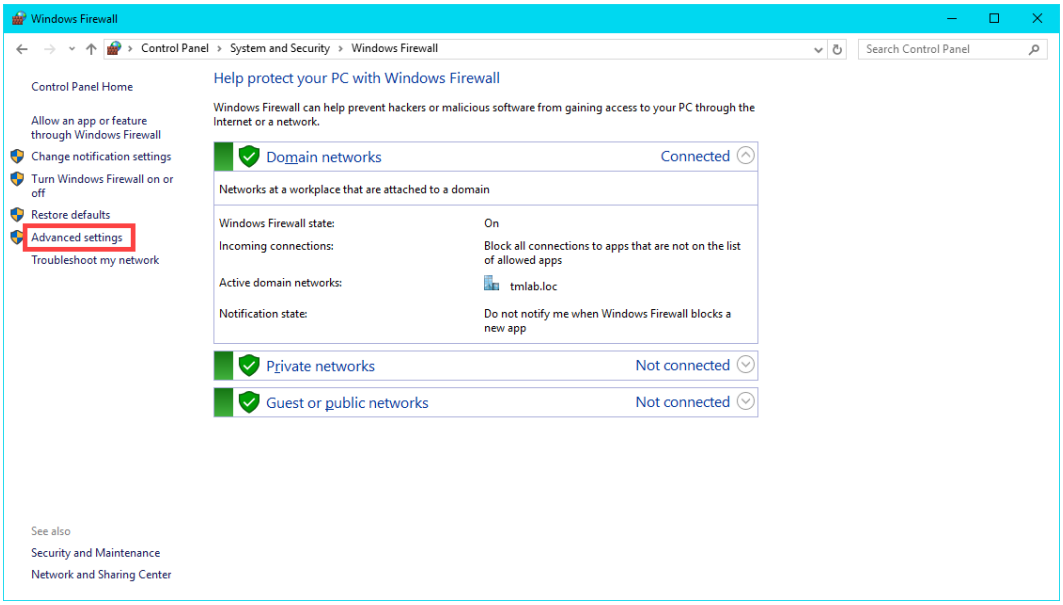
2. From the **Control Panel**, click the **System and Security** link.



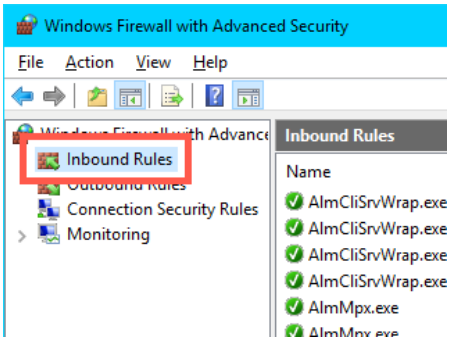
3. From the **System and Security** page of the **Control Panel**, click the **Windows Firewall** link.



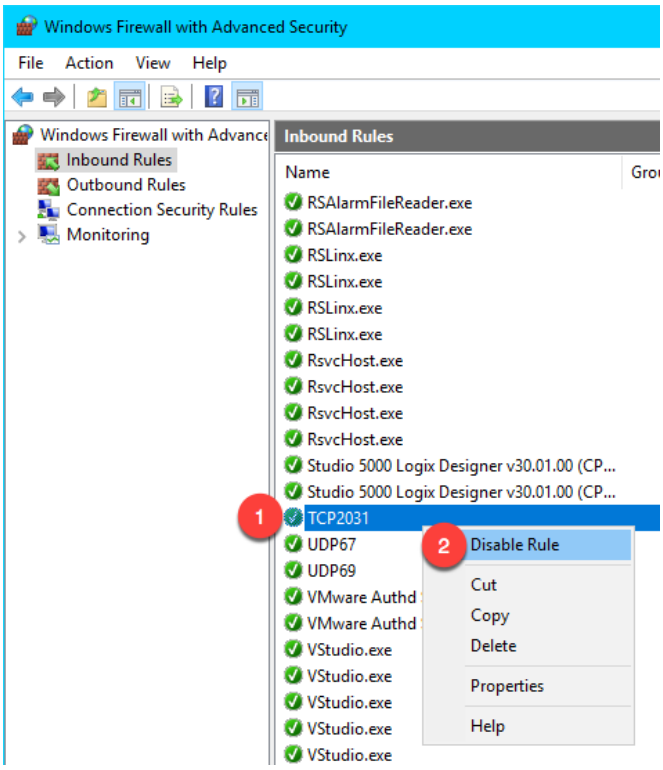
4. From the **Windows Firewall Control Panel**, click the **Advanced settings** link on the left hand side.



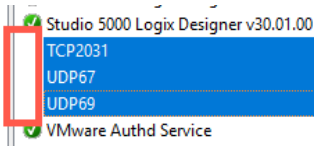
5. From the **Windows Firewall and Advanced Security** window, click the **Inbound Rules** item.



6. Scroll down through the **Inbound Rules** until you find the **TCP2031** rule we added in Section 11. Right click it and select **Disable Rule**.



7. Repeat the previous step for the **UDP67** and **UDP69** rules, so that all 3 rules are disabled. Verify that these 3 rules do not have green check marks beside them. When finished, leave the **Windows Firewall with Advanced Security** window open.

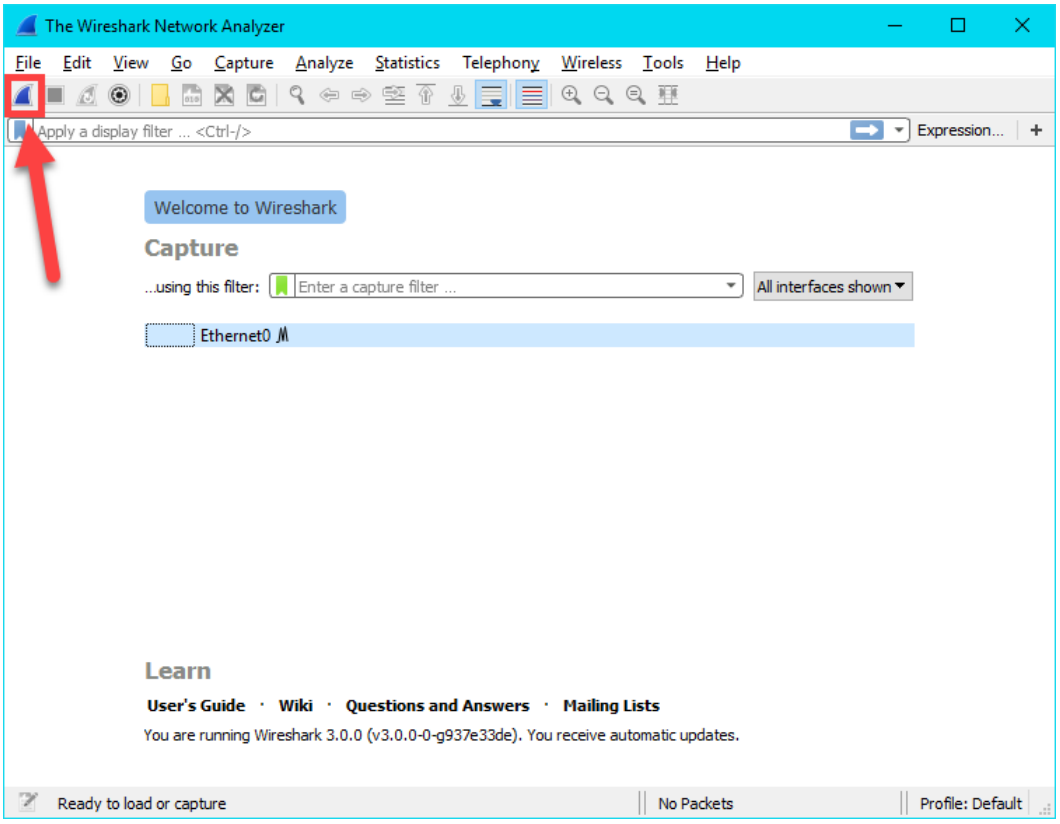


Start Wireshark Capture

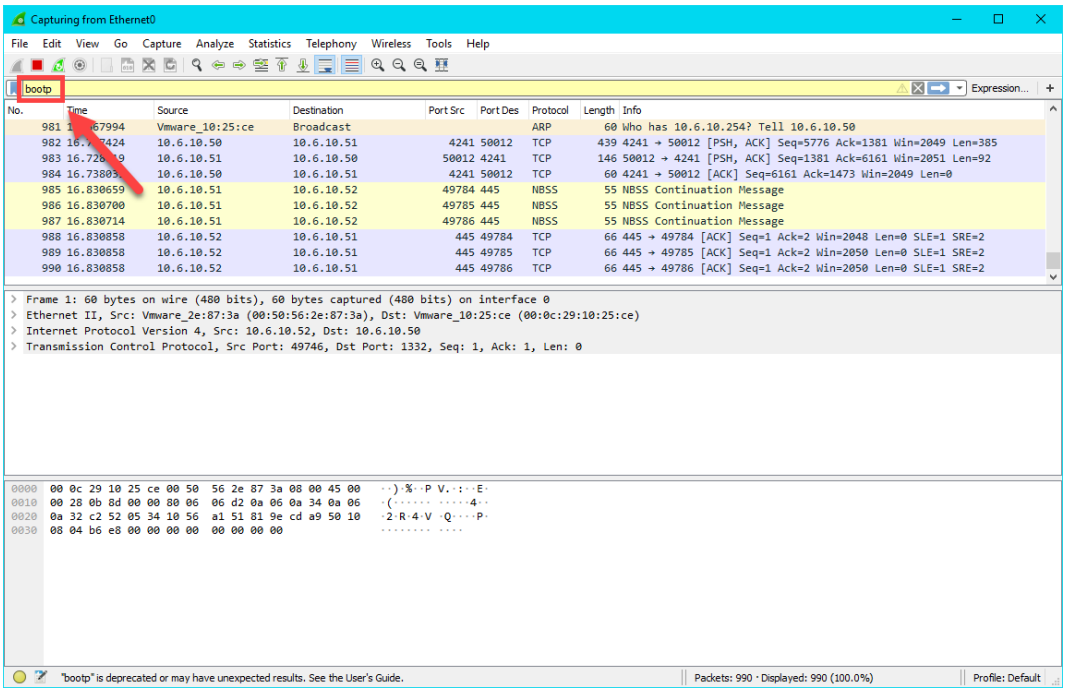
Wireshark is a free and open source packet analyzer. It is often used for network troubleshooting and is a tremendous help when diagnosing thin client boot issues. The ThinManager support team can generally pinpoint network issues by analyzing a Wireshark capture file.

1. Double click the **Wireshark** shortcut on the **RDS1** desktop.

2. Click the **Start Capturing Packets** icon in the **Wireshark** toolbar.

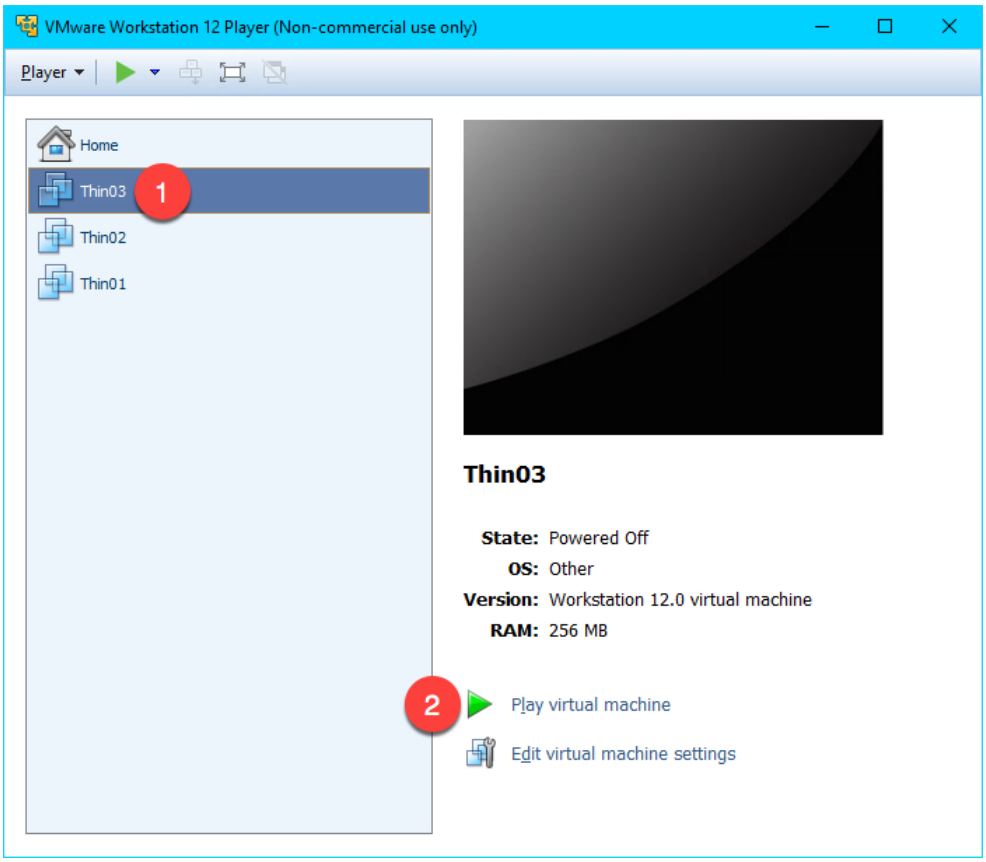


3. When the network capturing begins, you will see a consistent stream of network packets in the capture pane. We want to filter the packets initially to only look at bootp packets, so enter *bootp* followed by the ENTER key in the filter field. This should result in clearing the capture pane, since we have not attempted to boot a client yet.

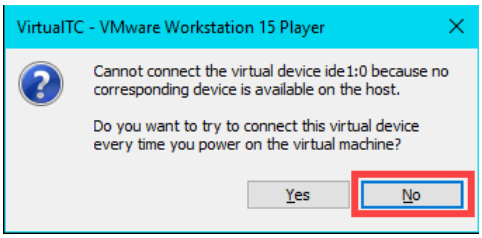


Troubleshoot the Boot Process

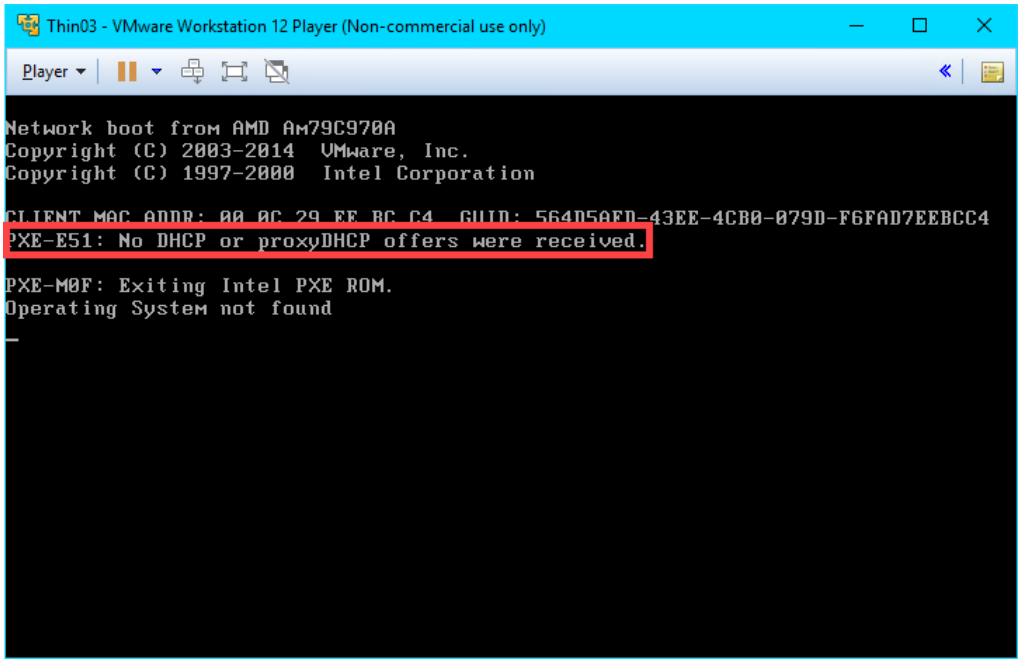
1. Return to **VMWare Player**. If it is closed, you can re-launch it by double clicking its shortcut on the desktop. Select the **Thin03** virtual image we created earlier and click the **Play virtual machine** link.



2. Click the **No** button to the connect virtual device message box.

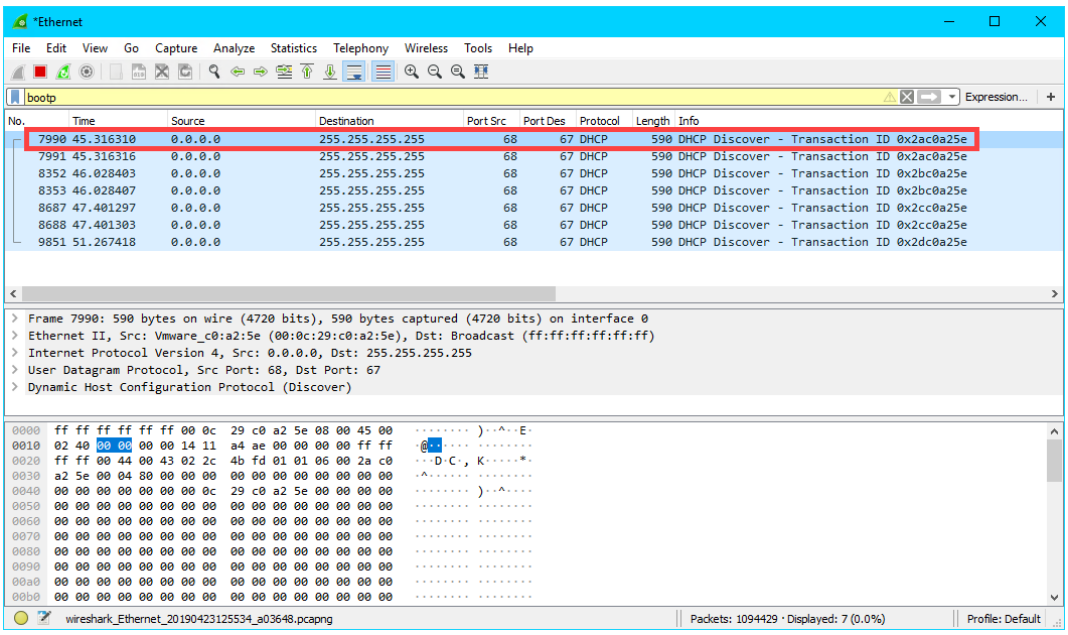


3. Since we have not installed an **Operating System** in our virtual machine, it will attempt to **PXE boot**. After a few seconds, we receive a **PXE-E53** error indicating **No boot filename received**. Recall that **PXE** is inherently dependent on **DHCP**. As part of this dependence, any **PXE** client needs 3 things to boot – (1) an IP address, (2) a boot server IP address and (3) a boot file name. We have the virtual thin client configured for **NAT**, so **VMWare Player** will provide a NAT'd IP address, but we need ThinManager to provide the boot server IP address(es) as well as the boot file name. We configured ThinManager's **PXE Server Mode** accordingly to be **Using standard DHCP server**. We know that we just disabled some important **Firewall Rules** that we created in Section 11, but let's imagine that we didn't know this.

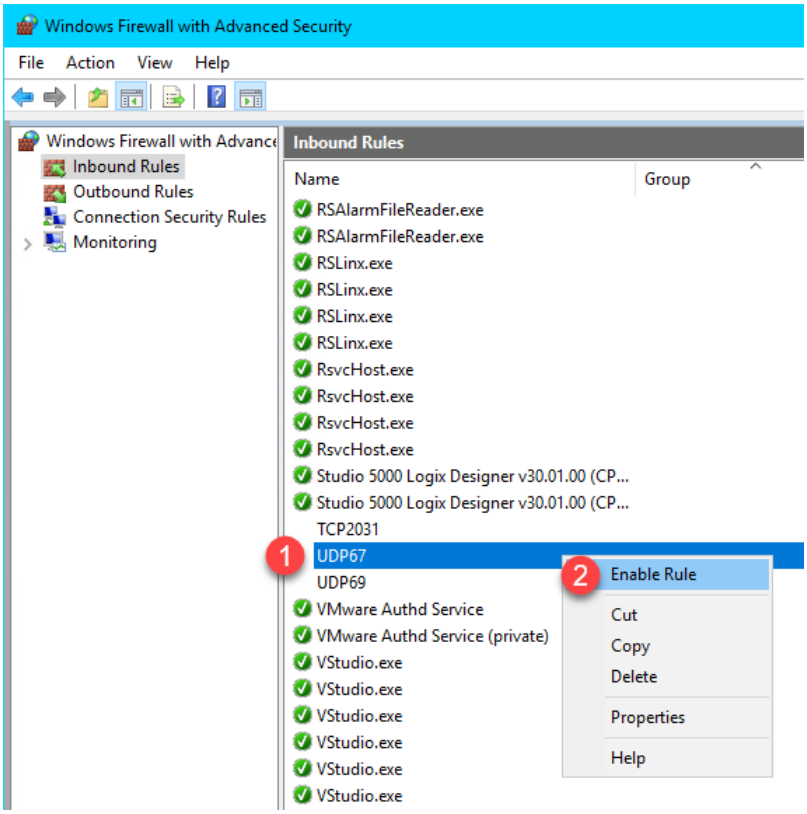


TFTP, **Trivial File Transfer Protocol**, is used by all ThinManager managed thin clients to deliver the boot file, the firmware, as well as the terminal configuration.

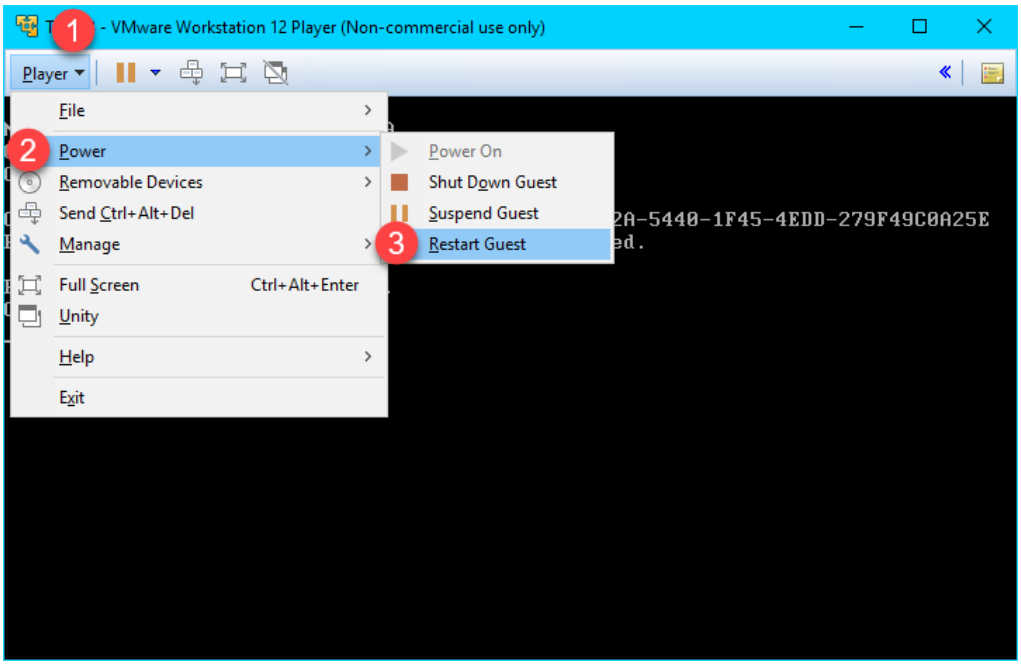
4. Return to **Wireshark** so we can investigate what might be the problem. As we can see from the capture log, a **DHCP Discover** packet was sent to a **Port Destination of 67**, but no **DHCP Offers** were made from **ThinManager**.



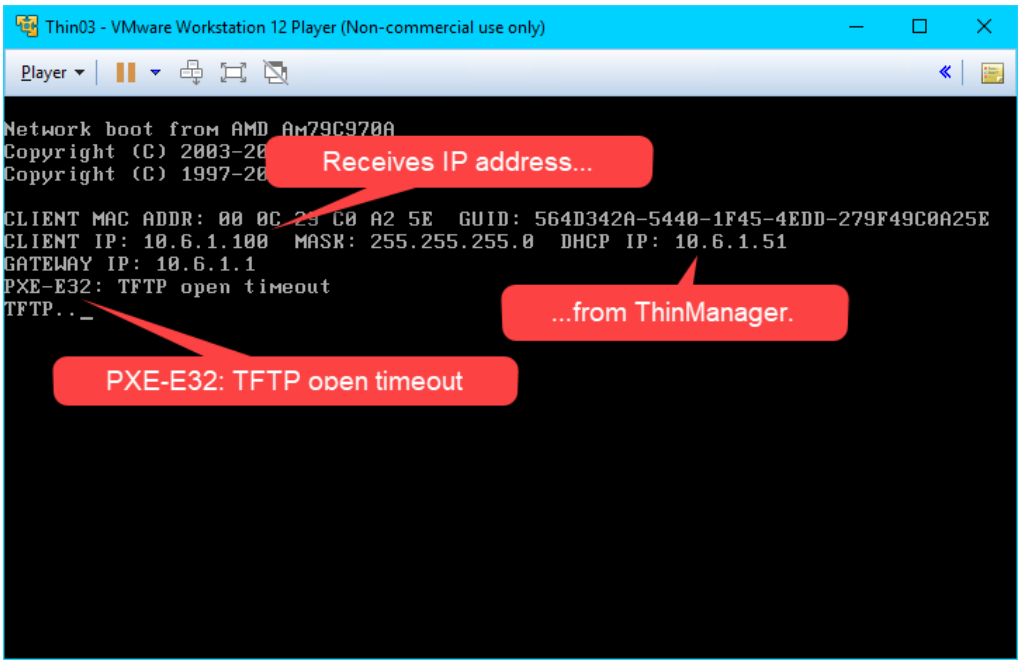
5. Return to the **Windows Firewall with Advanced Security** window. Right click the **UDP67** firewall rule and select **Enable Rule**. This is the rule that permits UDP67 traffic through the firewall, which enables **DHCP** traffic.



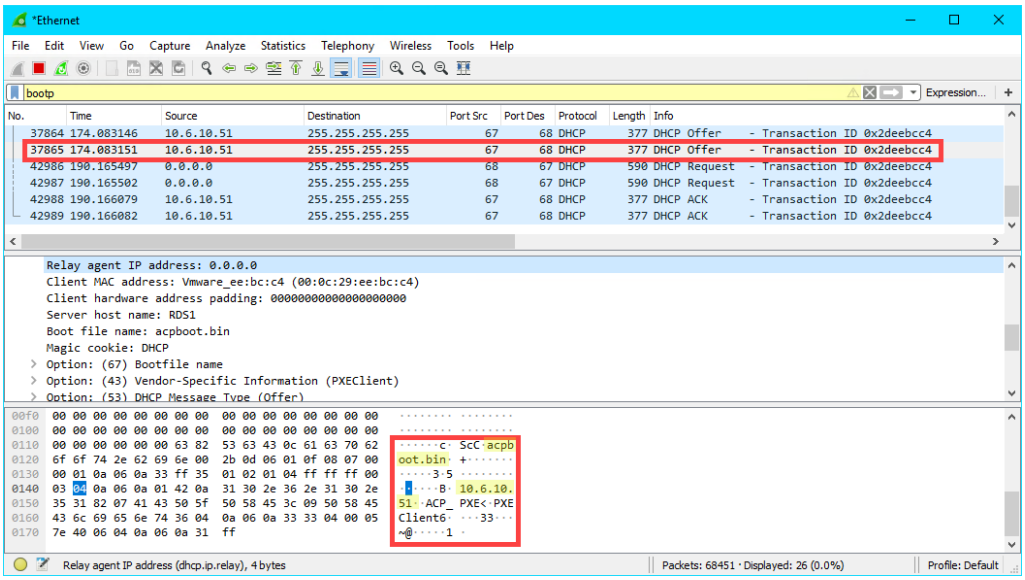
6. Return to **VMWare Player**. Select the **Player** drop down menu, followed by the **Power** item then the **Restart Guest** item. Click **Yes** to the confirmation dialog.



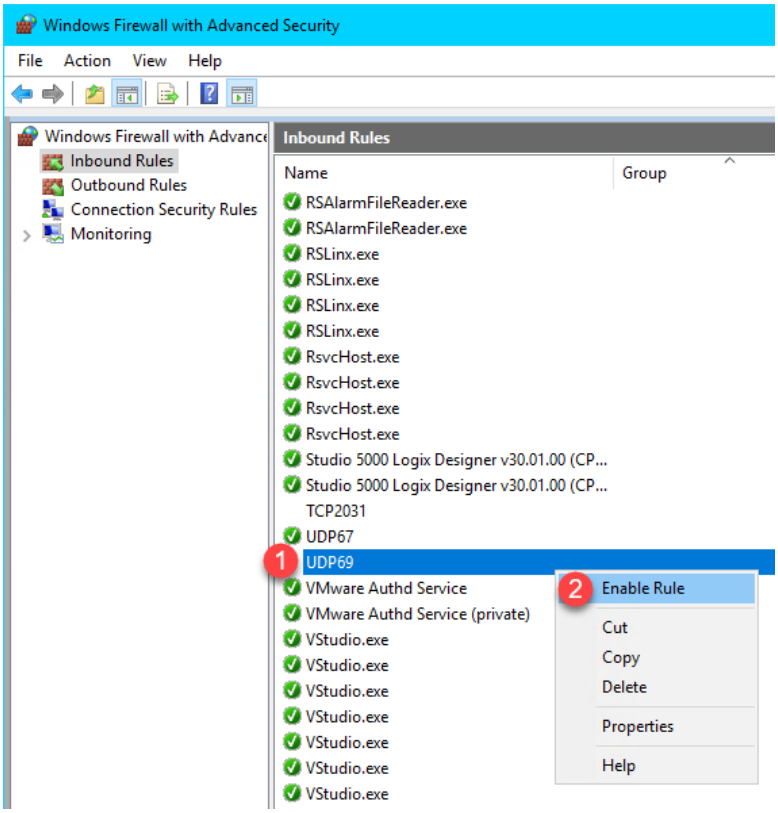
7. After restarting the virtual thin client, we receive a **TFTP** timeout. It looks like we might be getting a little closer. This time we receive the necessary IP information from ThinManager. This indicates that **ThinManager** responded to the **DHCP Request** with a **DHCP Offer**. Let's confirm this with **Wireshark**.



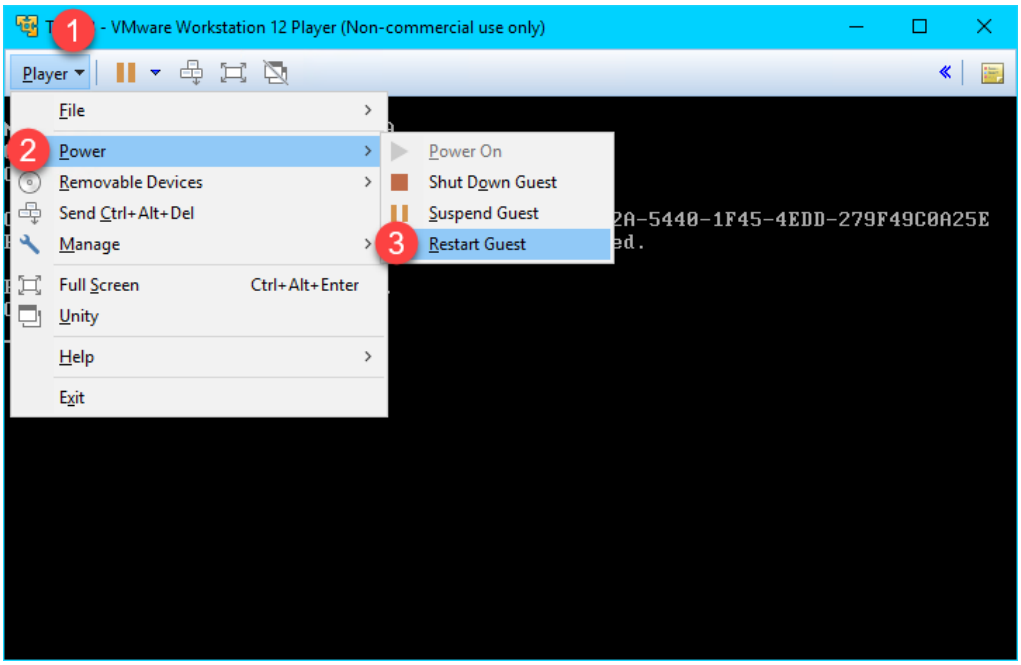
8. Sure enough, we see that this time we received a **DHCP Offer** from 10.6.10.51 which includes the **boot server** (10.6.1.51) and the **boot filename** (acpboot.bin). So our virtual thin client should have all it needs to boot, but we are still receiving a **TFTP** timeout.



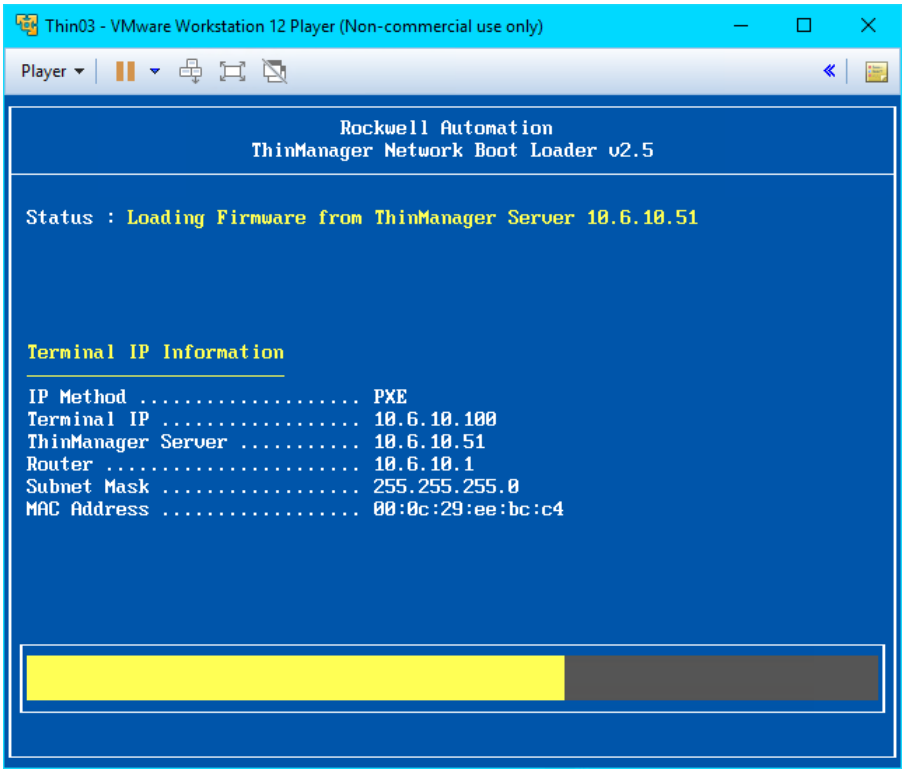
9. Return to the **Windows Firewall with Advanced Security** window. Right click the **UDP69** firewall rule and select **Enable Rule**. This is the rule that permits UDP69 traffic through the firewall, which is required for **TFTP** communication for **PXE** clients.



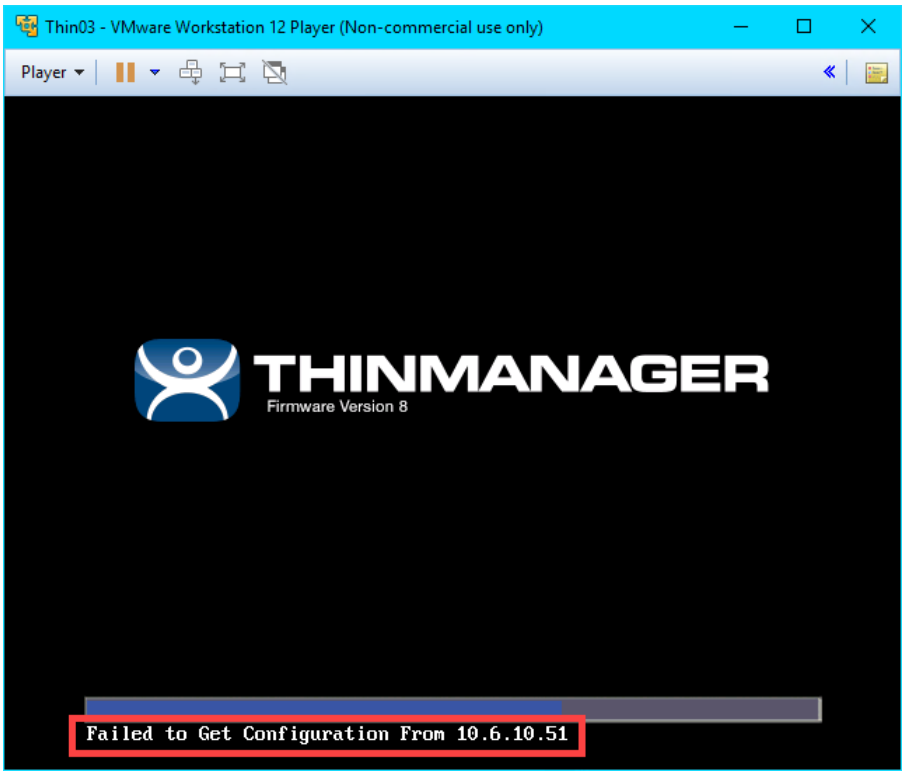
10. Return to **VMWare Player**. Select the **Player** drop down menu, followed by the **Power** item then the **Restart Guest** item. Click **Yes** to the confirmation dialog.



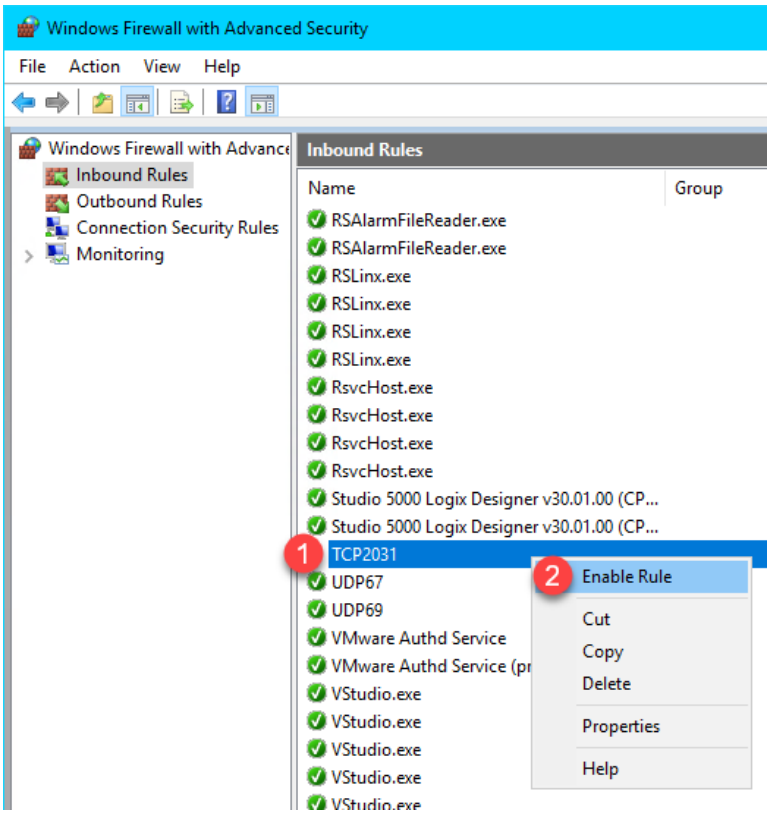
11. This time, the **Virtual Thin Client** should begin to boot. It will first receive the boot loader (**acpboot.bin** for **Legacy PXE** clients like this one), and then the firmware. Notice that the **IP Method** is listed as **PXE**, which indicates that **ThinManager** acted as a **DHCP Server** to deliver the IP address for the terminal, the IP address of the ThinManager Server and the boot filename.



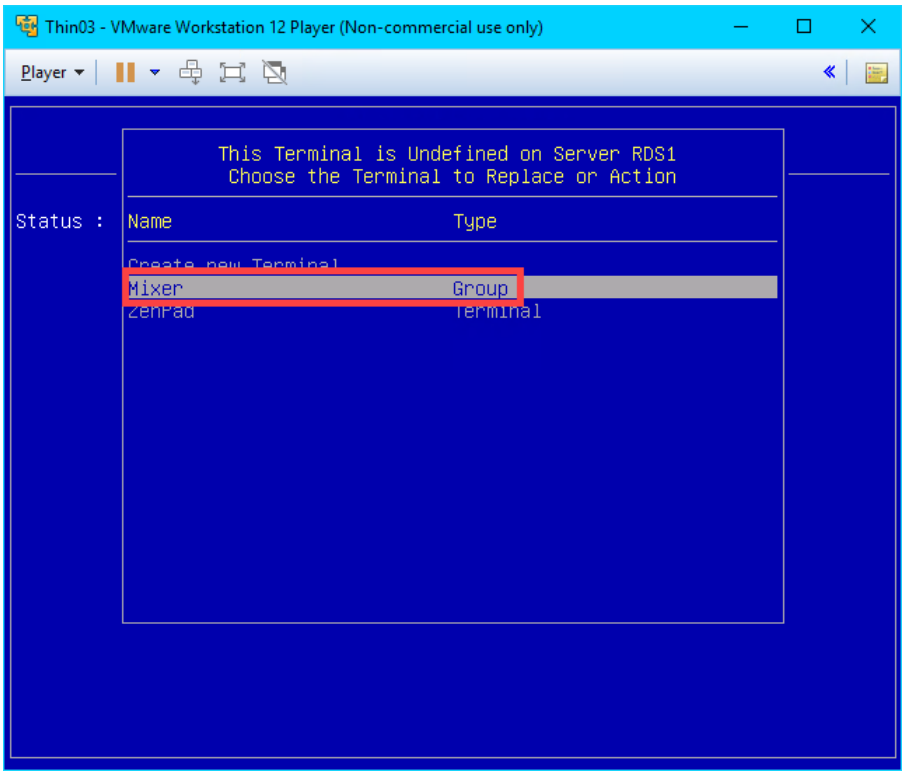
12. We will now see the final hurdle to clear, which is the delivery of the terminal profile, which requires **TCP2031**. Since this port is not currently open, we are receiving a **Failed to Get Configuration From 10.6.10.51** error message.



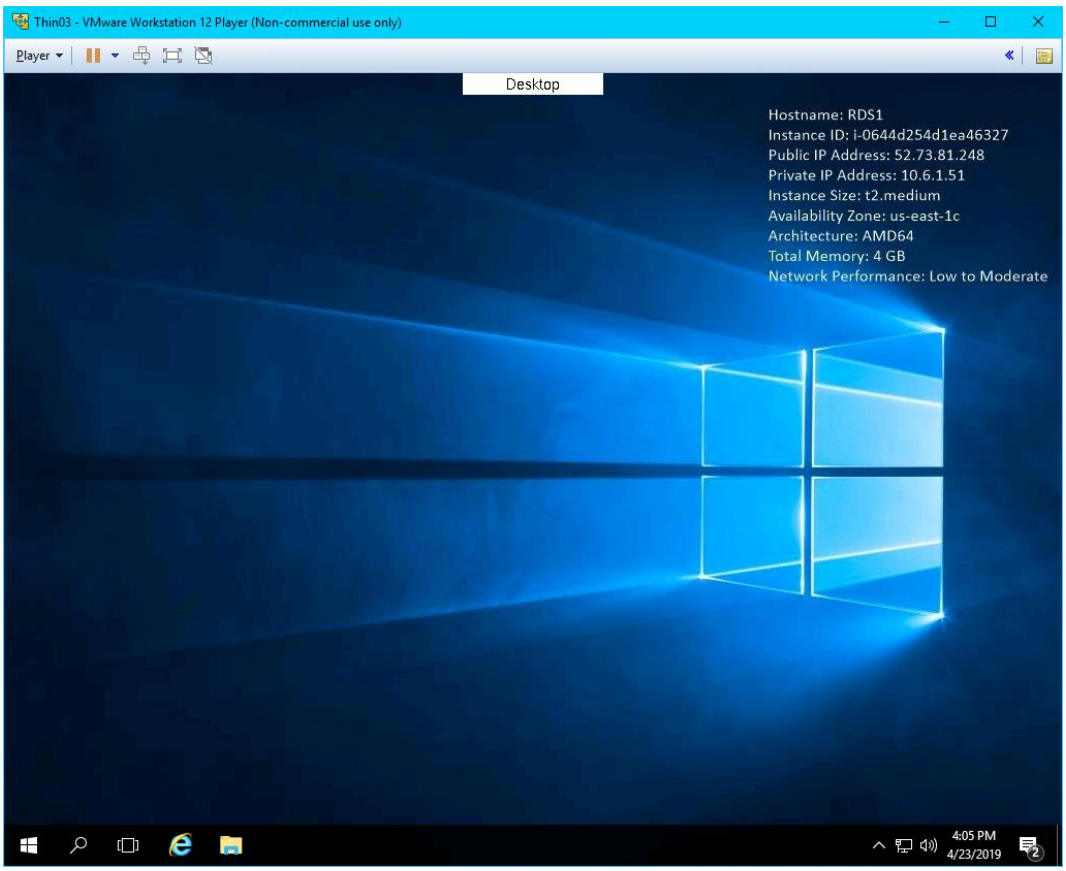
13. Return to the **Windows Firewall with Advanced Security** window. Right click the **TCP2031** firewall rule and select **Enable Rule**. This is the rule that permits **TCP2031** traffic through the firewall, which is required for the delivery of the terminal profile and for communication between **ThinServer** and the terminal.



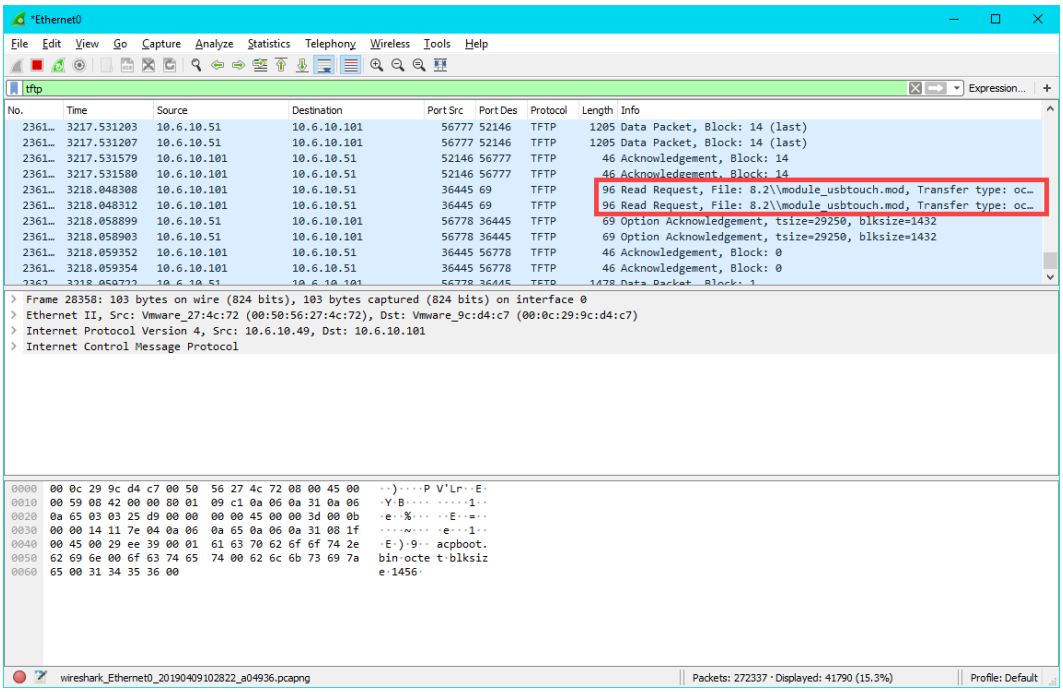
14. Return to the virtual thin client once more and we should now see the terminal profile assignment screen. Arrow down to select the **Mixer Terminal Group** followed by the **Thin03** terminal profile.



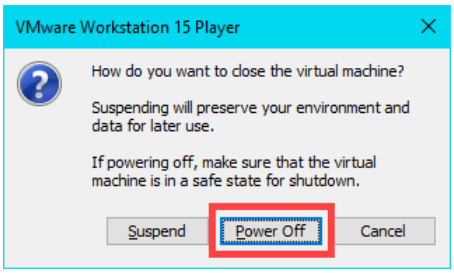
15. The boot process should continue now delivering the terminal's profile, with the ultimate result being the delivery of the **Desktop Display Client** that we assigned to the **Thin03** terminal profile in the **ThinManager**.



16. Return to **Wireshark** and replace the **bootp** capture filter with *tftp*. Now you can see the delivery of the boot loader, the firmware and the terminal profile (including the associated modules).



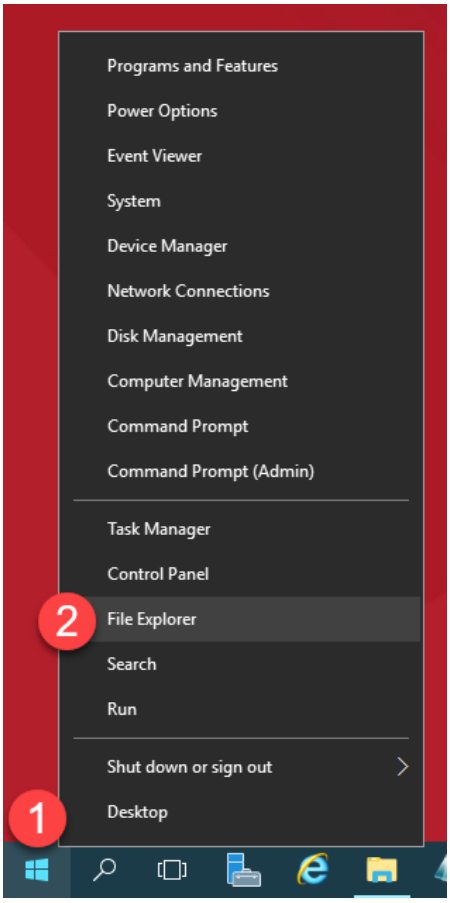
17. Return to **VMWare Player** and close it. Click the **Power Off** button.



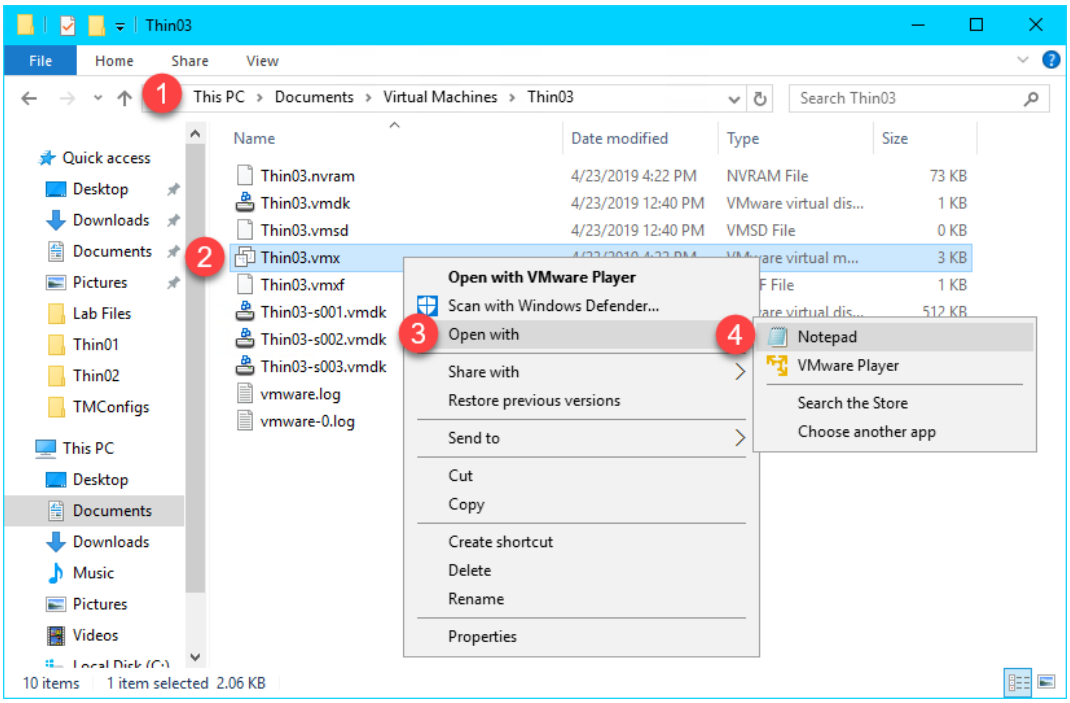
Boot Virtual Thin Client via UEFI

ThinManager v11 introduces support for **UEFI** (**Unified Extensible Firmware Interface**). Also referred to as EFI, UEFI is a new generation of system firmware and is stored in ROM or Flash ROM. Essentially, UEFI provides the first instructions used by the CPU to initialize hardware and subsequently pass control to an operating system or bootloader. UEFI is intended to replace traditional BIOS and is also capable of running on platforms other than PCs. Adding support for UEFI enables ThinManager to continue to support a very broad range of thin client offerings.

1. We need to configure our **Virtual Thin Client** to use **UEFI** instead of **traditional BIOS**. To do so, right click the **Windows Start** button on **RDS1** and select **File Explorer**.

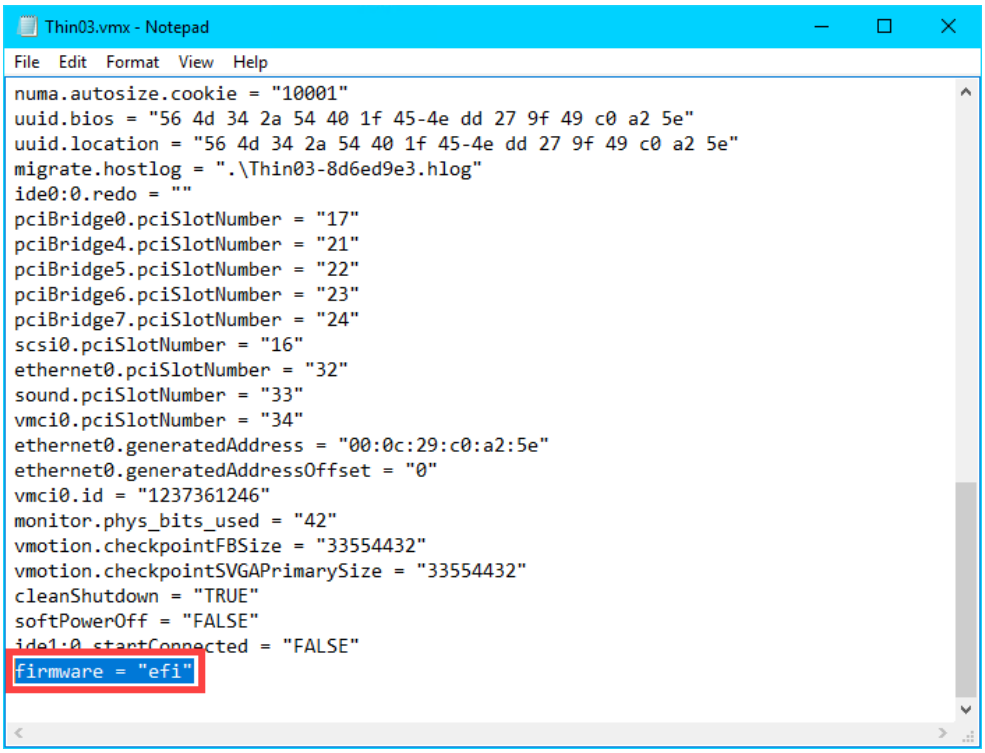


15. Within **File Explorer**, navigate to **Documents->Virtual Machines->Thin03**, right click **Thin03.vmx** and select **Open With…** followed by **Notepad**.



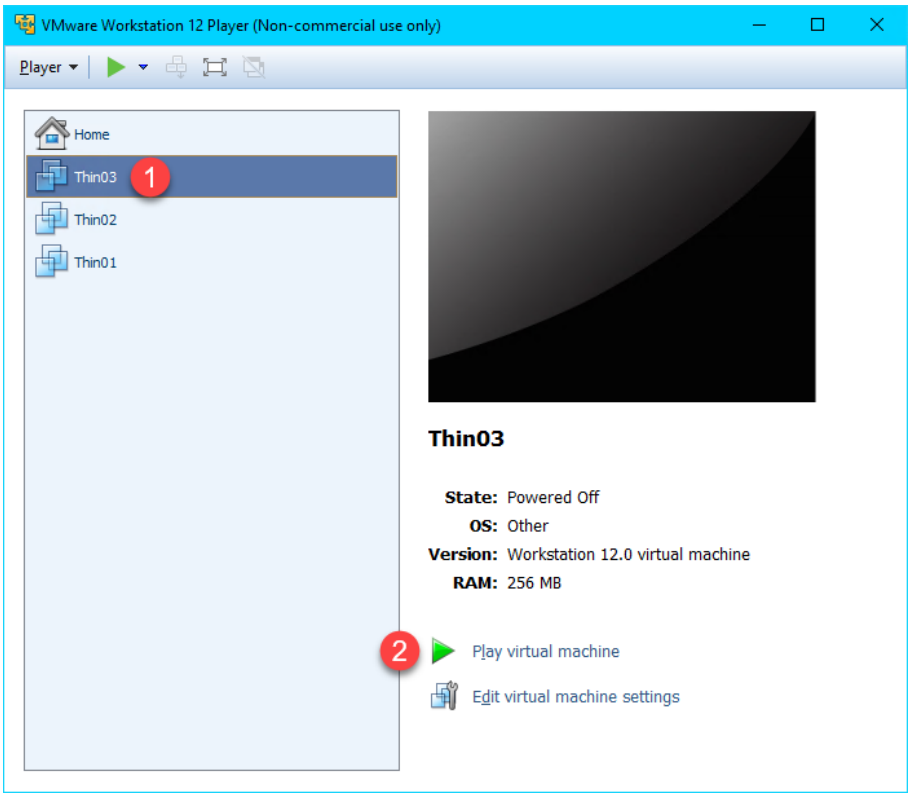
16. Scroll to the bottom of the text file and enter the following on a new line (this can also be copied and pasted from the **LabPaths.txt** file from the **RDS1 Desktop**). **Save** the file and close **Notepad**.

```
firmware = "efi"
```

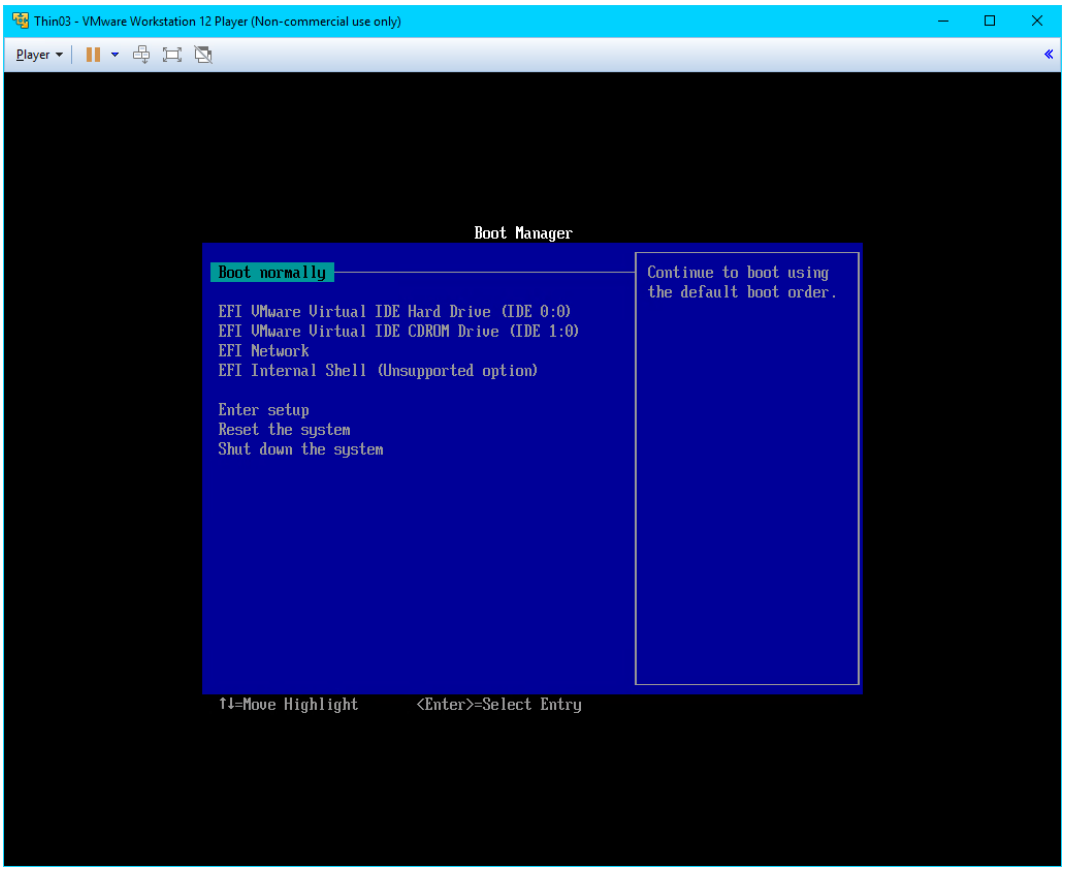


17. Double click the **VMWare Player** shortcut on the **RDS1** desktop.

18. Return to **VMWare Player** by double clicking its shortcut on the desktop. Select the **Thin03** virtual image we created earlier and click the **Play virtual machine** link.



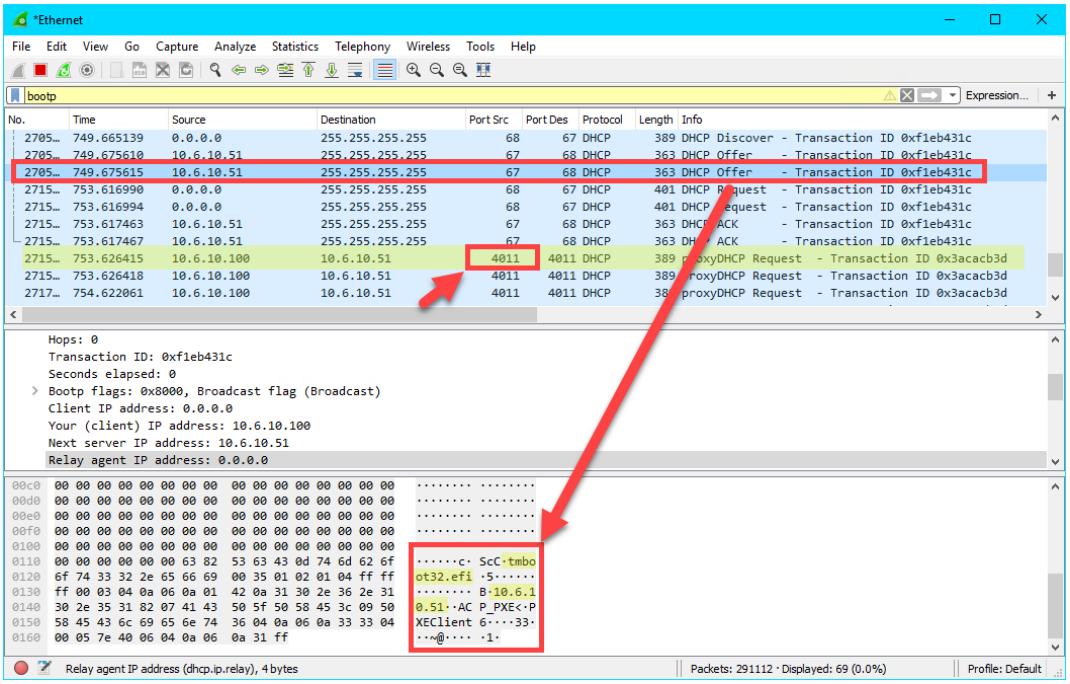
19. The **VirtualTC** image should now attempt to **PXE** boot via **UEFI** as opposed to **BIOS**. You should see the following screen indicating that it was unable to boot.



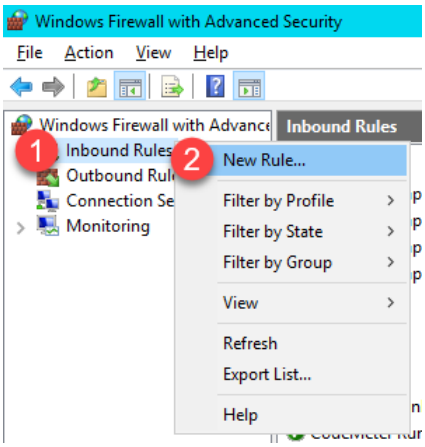
20. Let's return to **Wireshark** and examine the capture. Enter *bootp* as the capture filter again and scroll towards the bottom of the capture window.

    The 1st thing to notice is the **DHCP Offer** from **10.6.10.51** which is our **RDS1** virtual image where we have **ThinManager** installed. This capture item is selected in order to see the data included in the packet. As you can see from the screen shot below, the response from **10.6.10.51** includes the **boot server – 10.6.10.51**, as well as the boot filename – **tmboot32.efi**.

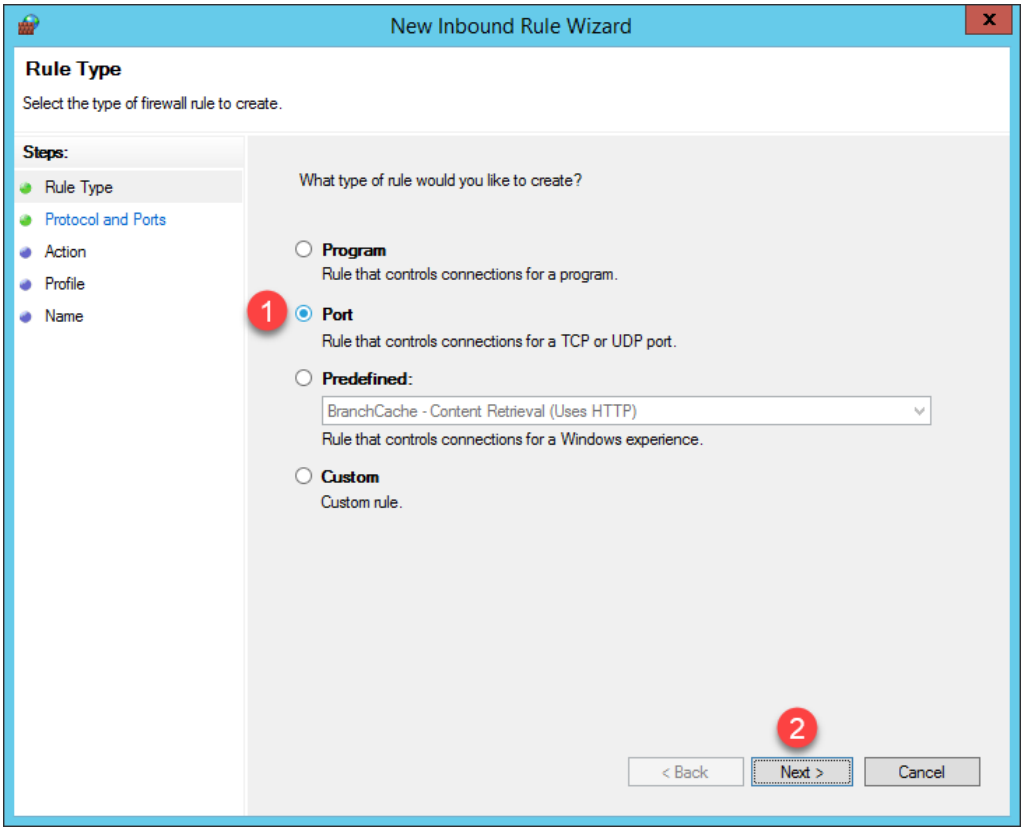
    The 2nd thing to notice is the **proxyDHCP Request**(s) on port **4011**. **UEFI** requires that we also open **UDP Port 4011**.



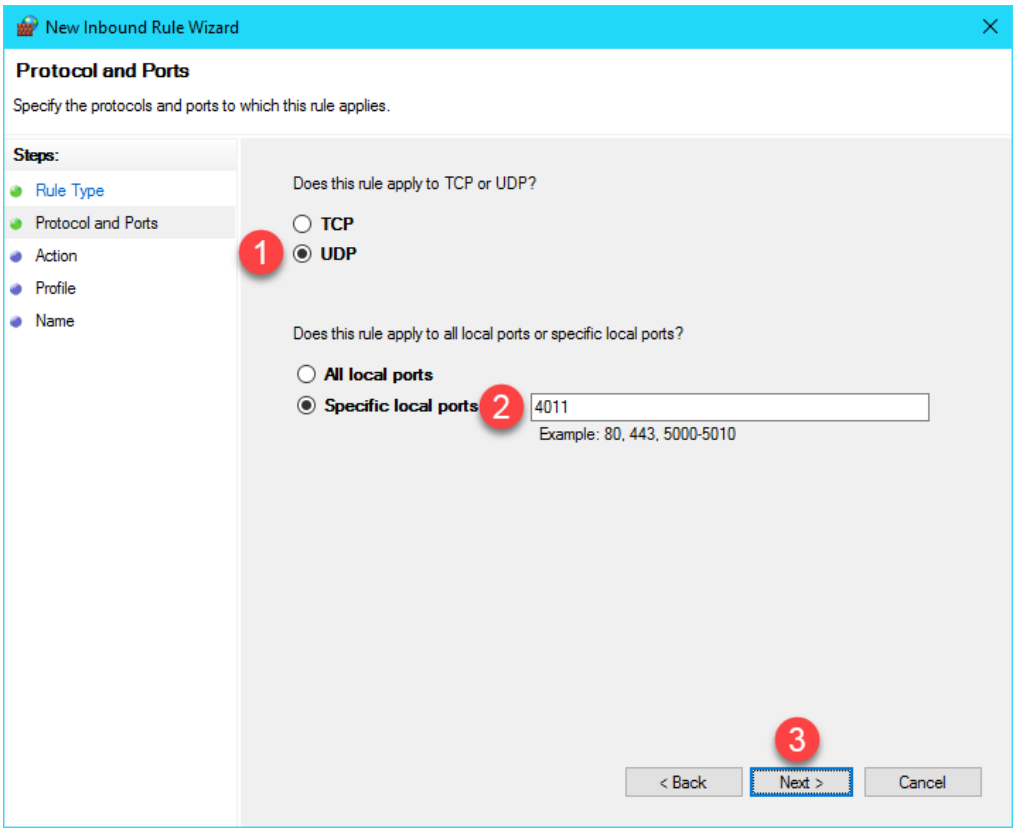
21. Return to the **Windows Firewall and Advanced Security** window.
22. Let's add a new **Inbound Rule** to permit the **UDP4011** port. Right click the **Inbound Rules** item and select the **New Rule…** item.



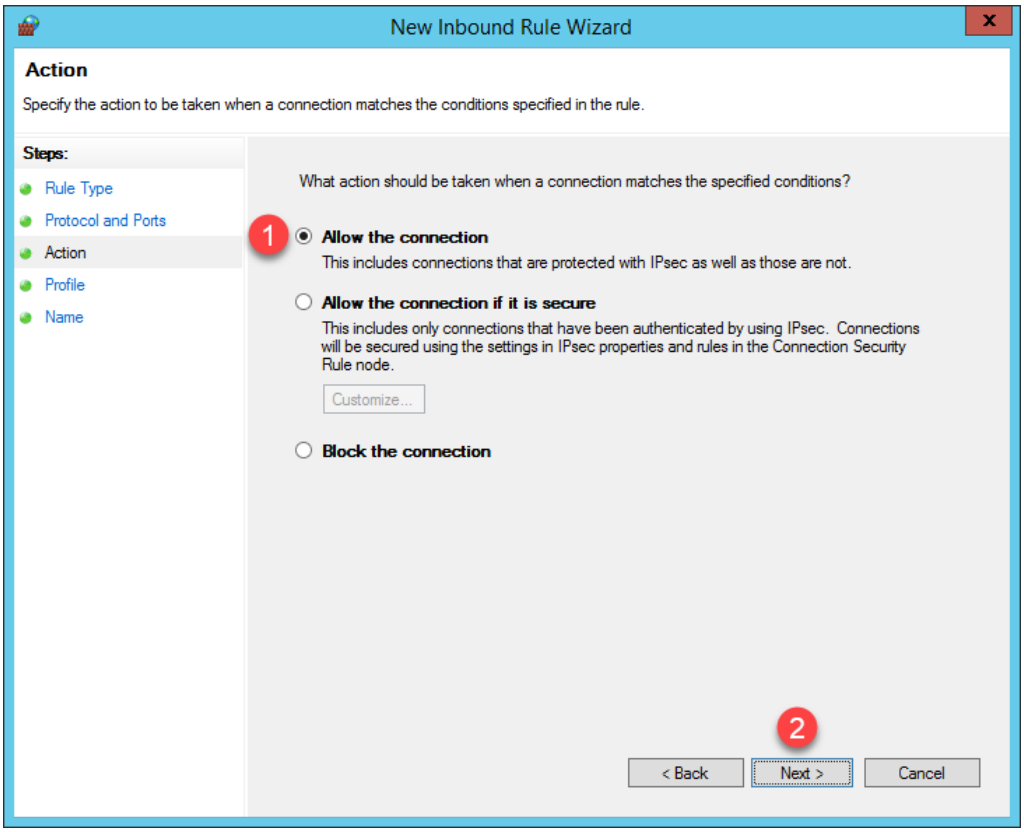
23. From the **Rule Type** panel of the **New Inbound Rule Wizard**, select the **Port** radio button, followed by the **Next** button.



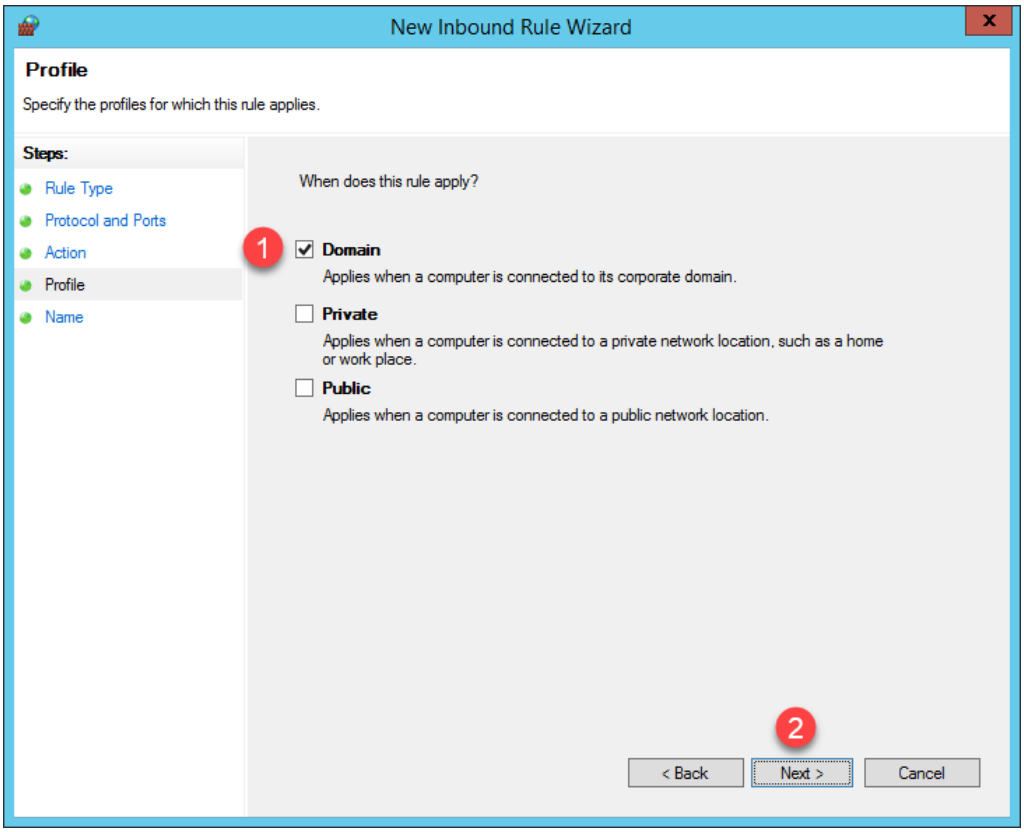
24. From the **Protocol and Ports** panel of the **New Inbound Rule Wizard**, select the **UDP** radio button and enter *4011* in the **Specified local ports** field. Click the **Next** button.



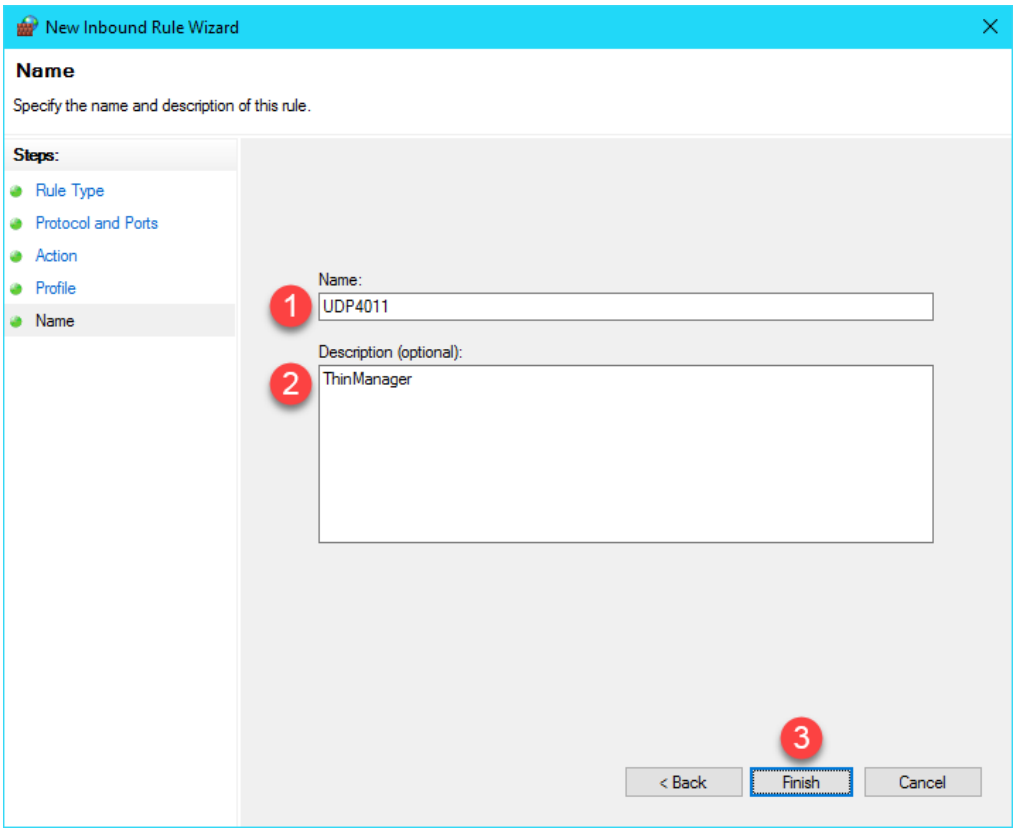
25. From the **Action** panel of the **New Inbound Rule Wizard**, select the **Allow the connection** radio button and click the **Next** button.



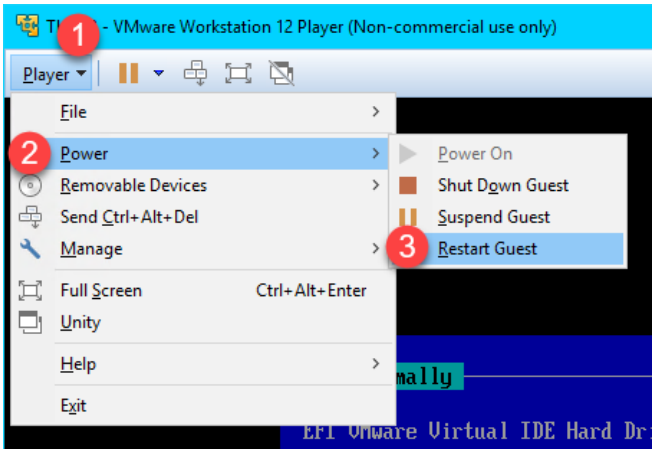
26. From the **Profile** panel of the **New Inbound Rule Wizard**, check the **Domain** checkbox and **un**-check the **Private** and **Public** checkboxes. Click the **Next** button.



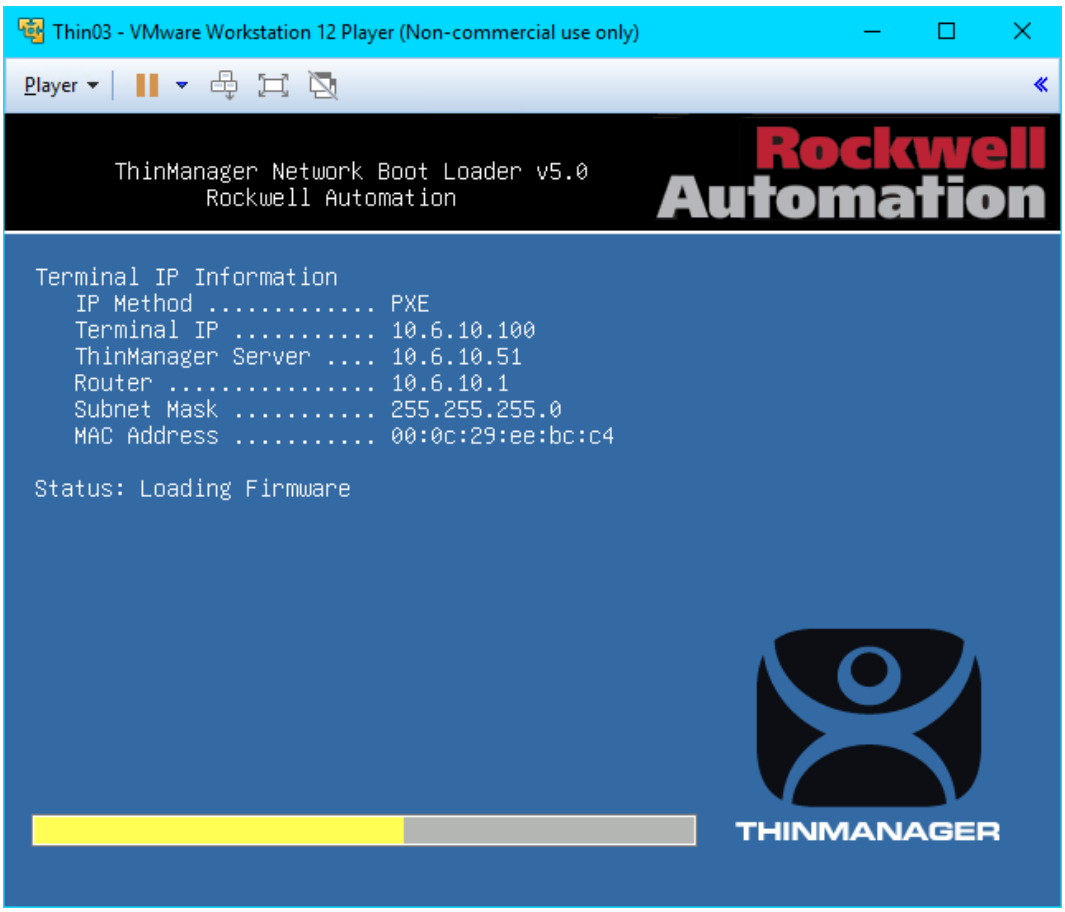
27. From the **Name** panel of the **New Inbound Rule Wizard**, enter *UDP4011* as the **Name** and *ThinManager* as the **Description**. Click the **Finish** button. Leave the **Windows Firewall with Advanced Security** window open.



28. Return to **VMWare Player**. Select the **Player** drop down menu, followed by the **Power** item then the **Restart Guest** item. Click **Yes** to the confirmation dialog.



29. This time, the **Thin03** image should successfully boot via **UEFI PXE**.



A couple of final words on **ThinManager Compatible Terminals** (**PXE**). In general, you will want to make sure that you have only one **PXE Server** on a single network segment/VLAN, otherwise it becomes very difficult with managing which **PXE Server** responds to **PXE** requests. Furthermore, since **PXE** inherently depends on **DHCP**, it is important to note that you will need to set up a **DHCP Relay** on a managed switch if you need to boot **PXE** terminals that are on a different network segment than ThinManager.

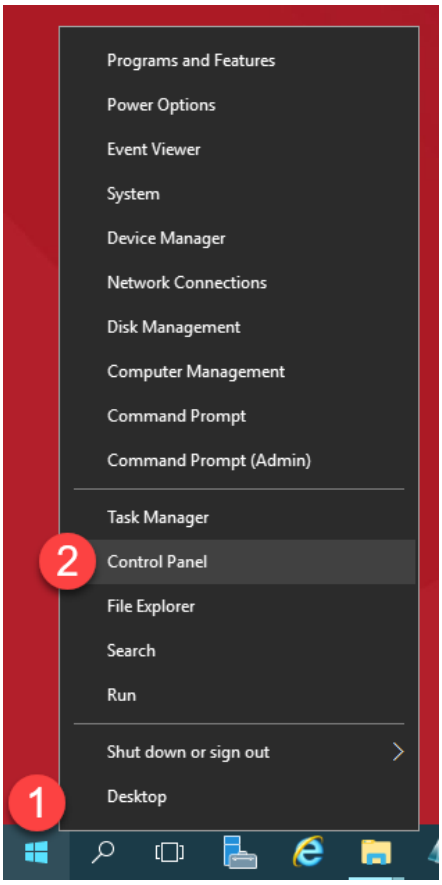
This completes the hands on lab. Thank you for your time, attention and interest in ThinManager. The ThinManager team truly appreciates it!

Install FactoryTalk View Site Edition Client in RD-Install Mode

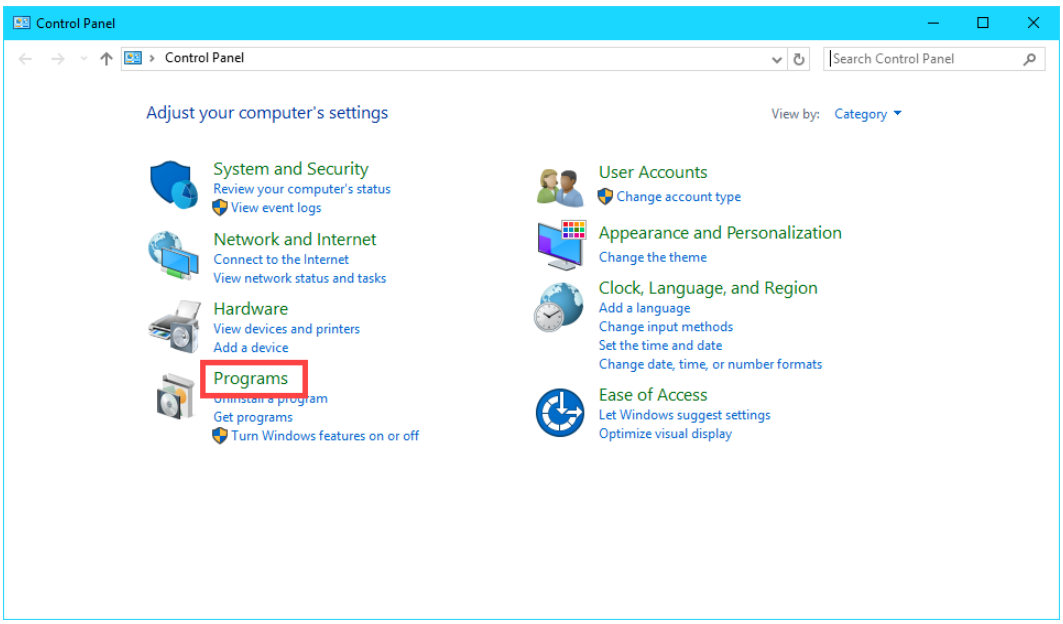
These steps are for reference only. Do not complete during the lab session, as these steps have already been completed.

Installation of applications for use in a Remote Desktop Session Host environment should be installed through RD-Install mode. In addition, they should always be installed **AFTER** the Remote Desktop Services role services have been installed and configured. This allows the server to capture and preserve per-user installation data to be applied across all sessions. This section walks you through the installation of the FactoryTalk View Site Edition Client in RD-Install mode.

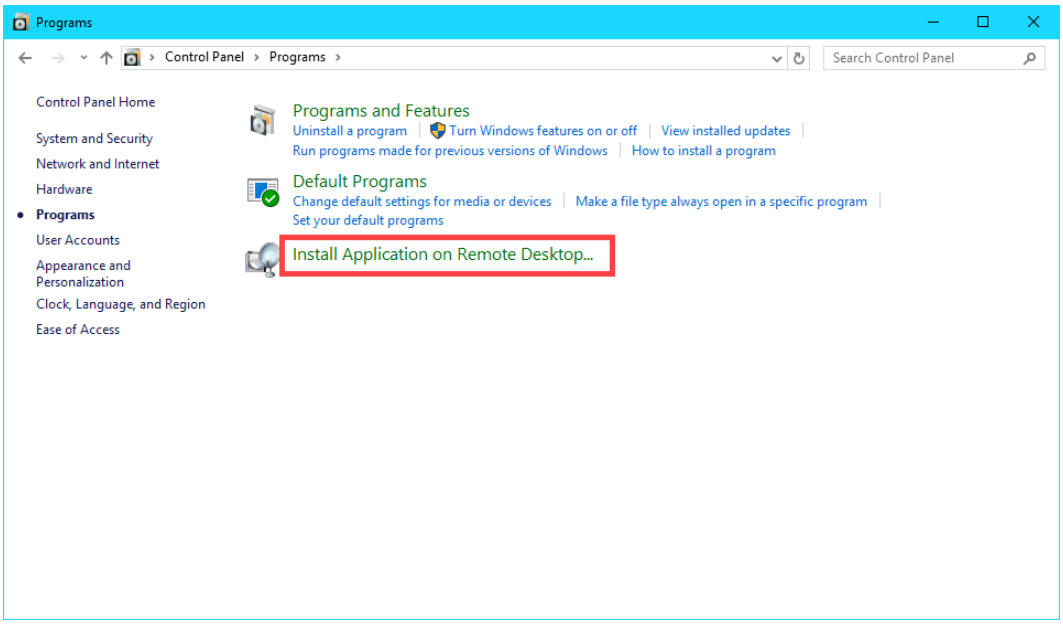
1. Right click the **Windows Start** button and click the **Control Panel** item.



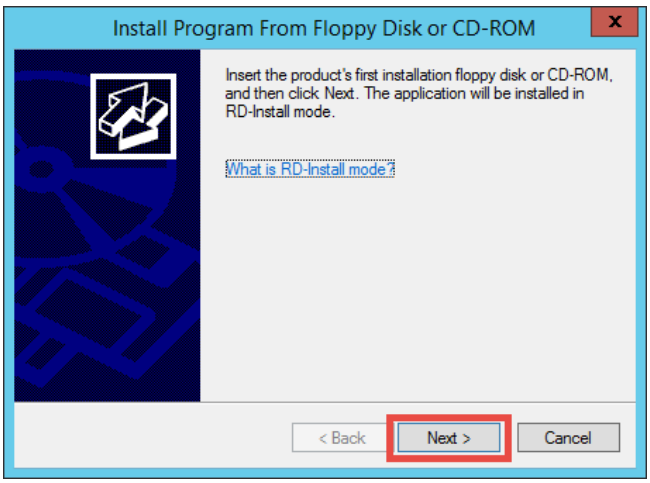
2. From the **Control** Panel, click the **Programs** link.



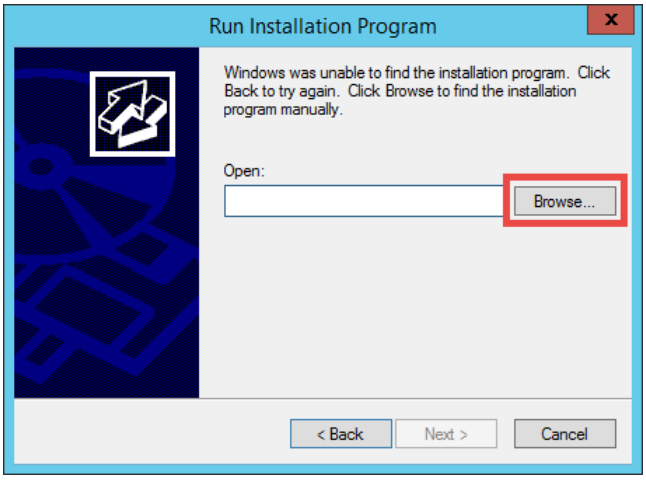
3. From the **Programs** page of the **Control Panel**, click the **Install Application on Remote Desktop…** link.



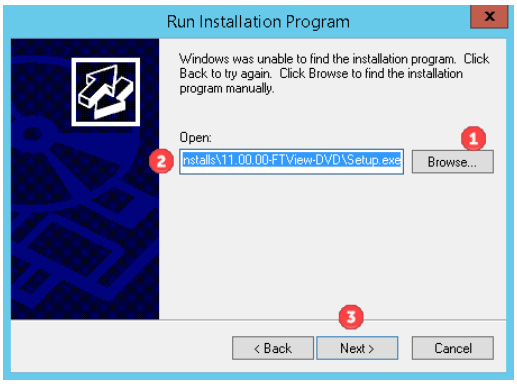
4. Click the **Next** button of the **Install Program From Floppy Disk or CD-ROM** wizard.



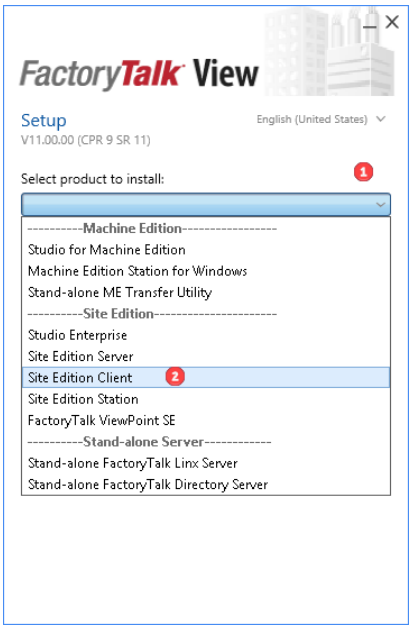
5. Click the **Browse…** button from the **Run Installation Program** page of the wizard.



6. In the **Browse** dialog, browse to the folder **C:\Tools\Installs\11.00.00-FTView-DVD**, select **Setup** and click **Open**.
7. Click **Next>** to launch the FactoryTalk View Site Edition installation program.



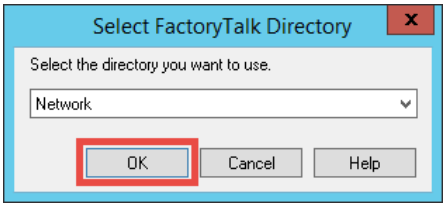
8. From the **FactoryTalk View Setup 11.00.00 (CPR 9 SR 11)** common installer, select **Site Edition Client** in the **Select product to install** dropdown box. Click **Install now>**.



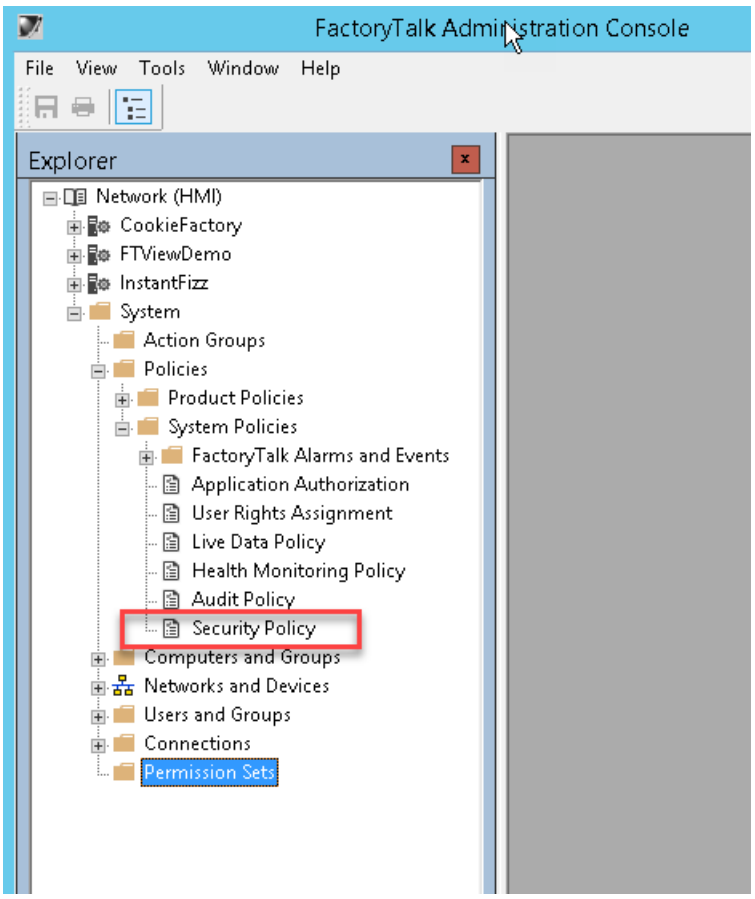
9. From the **End User License Agreements** page, click the **Accept all** button.

It may take 5 to 10 minutes to complete the install. In the meantime, we can review some other relevant FactoryTalk settings on **RDS2**, where we have pre—installed the FactoryTalk View SE Client for you, while the install completes. There are other FactoryTalk policy settings that have specific impacts to a Remote Desktop Services environment. One of which was taken care of in Section 5, and will not be repeated here. Namely, creating a **Computer Account** in the **FactoryTalk Directory** for each **Terminal Name** created in ThinManager. **VersaView5200** and **ZENPAD** have already been added for you in this lab.

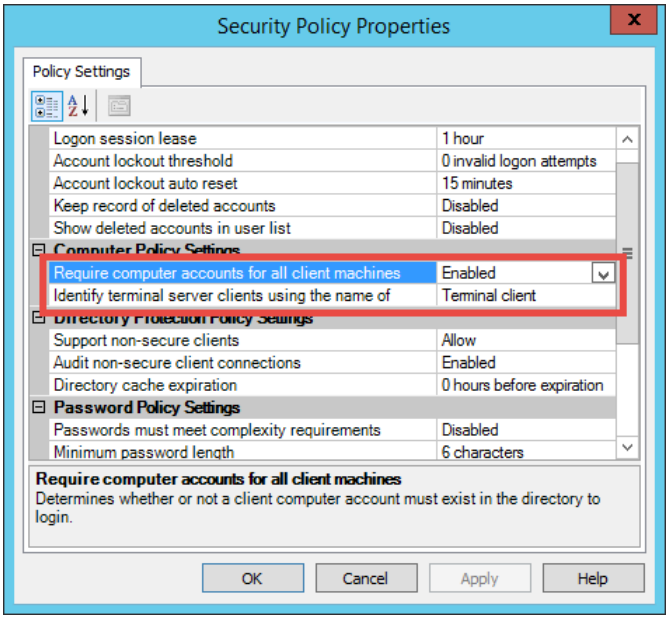
10. Switch to the **RDS2** image.
11. On **RDS2**, start the **FactoryTalk Administration Console** by clicking the **Windows Start** button, followed by the **Down Arrow** at the bottom left corner of the Start Menu screen.
12. From the **Apps Start Menu** screen, find and select the shortcut for the **FactoryTalk Administration Console**.
13. On the **Select FactoryTalk Directory** dialog, make sure **Network** is selected and click the **OK** button.



14. In the **Explorer** view, browse to **Network (HMI) →System→Policies→System Policies→Security Policy** and double click on **Security Policy** or right click on **Security Policy** and select **Properties…** from the menu.



15. Scroll down to the **Computer Policy Settings** section. The **Require computer accounts for all client machines** policy is by default set to *Enabled* and the **Identify terminal server clients using the name of** policy setting is set to *Terminal client*. Click **Cancel** to close the dialog. Close the **FactoryTalk Administration Console**.



These two policies significantly effect security, activity logging, and auditing. They should not be changed from default values without fully understanding the consequences.

Require computer accounts for all client machines

Determines whether **client** computers can access the FactoryTalk Network Directory without having a computer account in the Directory.

Enabled allows users to log on to FactoryTalk only if they are logging on from a client computer that has an account in the FactoryTalk Directory. Even if set to Enabled, Terminal Services clients can still log on to FactoryTalk Directory without computer accounts if the **Identify terminal server clients using the name of** policy is set to **Server Computer**. See below.

- Advantage – tighter security…only authorized clients can access the system
- Disadvantage – you must add the name of every authorized computer to the FTD

Disabled allows users to log on to FactoryTalk from any *client* computer, even if that computer has no computer account in the FactoryTalk Network Directory.

- Advantage - when you have many client computers that will be connected/disconnected and you will not have control over when new clients will be connected to the system, or don't want to manage all of the clients.
- Disadvantage - allows ANY computer to connect as a client, even if not part of the directory.

Important! Even when this setting is disabled, you must still create computer accounts for any computers hosting **servers** — for example, Terminal Servers, Rockwell Automation Device Servers (RSLinx Enterprise), OPC data servers, Tag Alarm and Event Servers, or HMI servers. Without the server computer accounts, you will not be able to configure the servers from client computers on the network because the FactoryTalk Network Directory Server cannot locate these servers on the network without their computer accounts.

Identify terminal server clients using the name of

Determines what computer name identifies clients connecting to the FactoryTalk Directory through Terminal Services. This policy also affects whether client computers connecting through Terminal Services require computer accounts in the FactoryTalk Directory.

Server Computer allows client computers to connect through Terminal Services without requiring accounts in the FactoryTalk Directory, even if the **Require computer accounts for all client machines** policy is **Enabled**. This is possible because Remote Desktop clients are identified by the Remote Desktop Server name, and the Remote Desktop Server must always have an account configured in the FactoryTalk Directory.

- Advantage: There is no need to add the name of each RDP client to the FactoryTalk Directory.
- Disadvantage: Any computer can use an RDP client to remote into the system. Remote Desktop clients are identified by the Remote Desktop Server name, thus actions are logged using the server name instead of the client name, so troubleshooting and auditing actions may be more difficult.

Results of combining the two policies

If set to **Terminal Client** and the **Require computer accounts for all client machines** policy is **Enabled**, client computers must have computer accounts in the FactoryTalk Directory to access FactoryTalk applications.

- Advantage: tighter security…only authorized clients can access the system, even using RDP. All activity is logged using the client name.
- Disadvantage: you must add the name of every authorized computer to the FTD, including RDP clients.

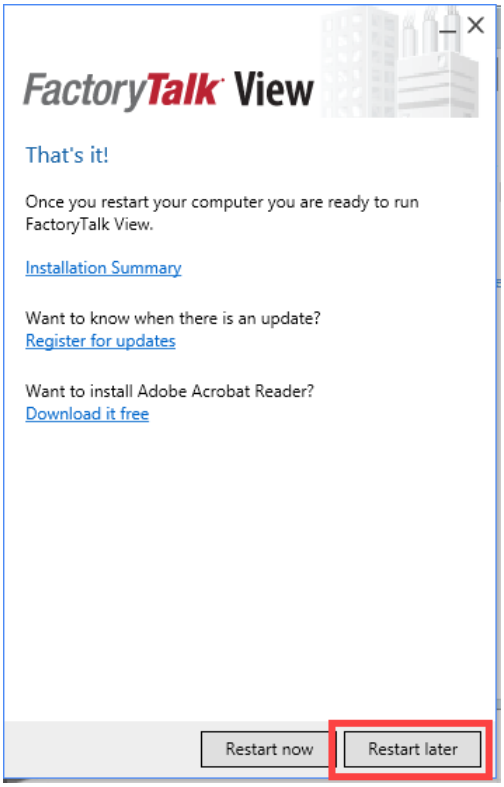
If set to **Terminal Client** and the **Require computer accounts for all client machines** policy is **Disabled**, client computers do not require computer accounts in the FactoryTalk Directory to access FactoryTalk applications. This combination of settings is useful for diagnostic logging because the name of the client computer where actions originate can be logged.

- Advantage: There is no need to add the name of each RDP client to the FactoryTalk Directory. The client name is used for logging.
- Disadvantage: Any computer can connect a client to the system. This include thick client as well as RDP clients.

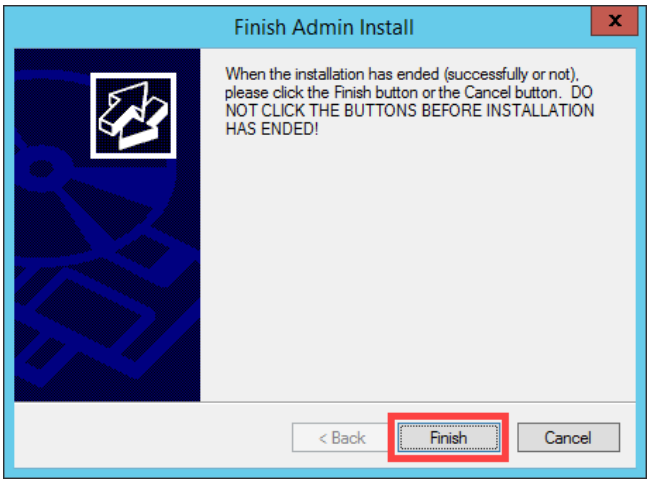
Please consult the FactoryTalk Security online help for a detailed explanation of behaviors by clicking the **Help** button in the **Security Policy Properties** dialog.

16. Return to the **RDS1** virtual machine by clicking the **RDS1** tab at the top of your screen to check the status of the install process.

17. After the installation completes, on the **Installation Summary** page, click the **Restart later** button.



18. After the dialog box is closed, you will be returned to the **Install Application on Remote Desktop Session Host** tool on the **Finish Admin Install** page. Click the **Finish** button.



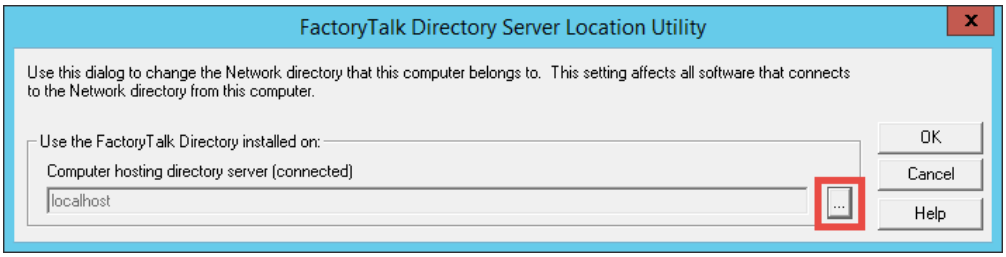
19. **Continue to the next section**. Do not restart yet, you will be asked to restart after configuring the network directory.

Configure the FactoryTalk Directory to Point to a Network Directory

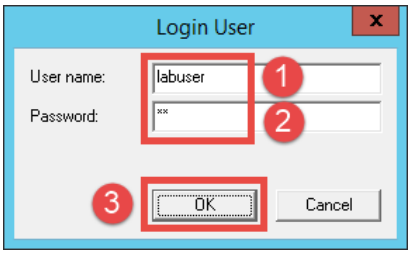
These steps are for reference only. <u>Do not complete</u> during the lab session, as these steps have already been completed.

Once the FactoryTalk View Site Edition client installation has completed, the machine needs to be configured to log on to the Network FactoryTalk Directory hosting the application. The network directory is located on the server **HMI** which has already been configured for you.

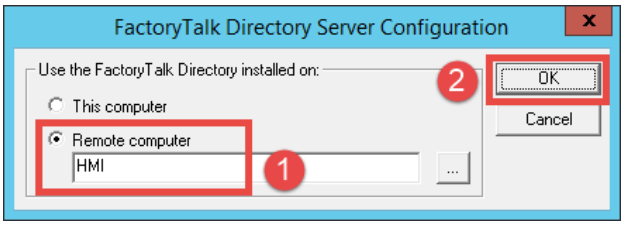
1. Launch the **FactoryTalk Directory Server Location Utility** by clicking the **Windows Start** button, followed by the **Down Arrow** icon in the bottom left corner of the **Windows Start** screen.
2. From the **Apps Start Menu** screen, scroll to the right and click the **Specify FactoryTalk Directory Location** shortcut.
3. From the **FactoryTalk Directory Server Location Utility**, click the **Browse** button.



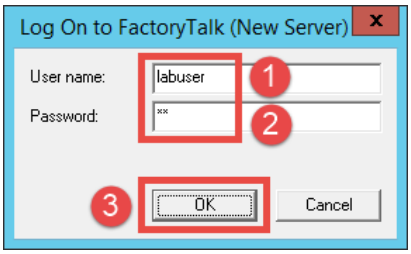
4. You will be prompted to log on to the local directory. Use *labuser* as the username and *rw* as the password and click **OK**.



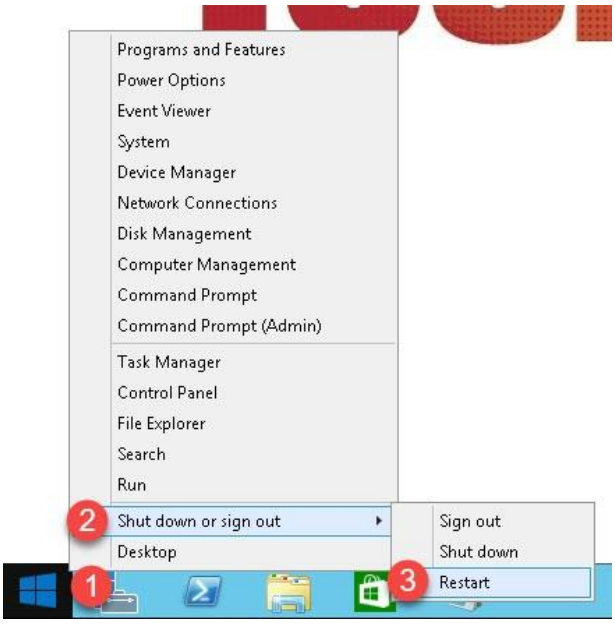
5. On the **FactoryTalk Directory Server Configuration** dialog, select the **Remote computer** option, type in *HMI* and click **OK**.



6. In the **FactoryTalk Directory Server Location Utility**, click the **OK** button to continue.
7. Click **OK** on the dialog notifying you that a restart of the computer is required.
8. You will then be prompted to log on to the new server. Use *labuser* as the username and *rw* as the password and click **OK**.



9. Now you can restart the computer by right clicking the **Windows Start** button and selecting **Shut down or sign out →Restart**. If prompted about other users being connected to the Server, click the **Restart Anyway** link.



This completes the section **Installation and Configuration of FactoryTalk View Site Edition Client on Remote Desktop Server**. Continue to the next section to install and activate **ThinManager**.

Notes

www.rockwellautomation.com

Power, Control and Information Solutions Headquarters

Publication XXXX-XX###X-EN-P — Month Year

Supersedes Publication XXXX-XX###X-EN-P — Month Year

www.rockwellautomation.com

Publication XXXX-XX###X-EN-P — Month Year
Supersedes Publication XXXX-XX###X-EN-P — Month Year

Europe/Middle East/Africa: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgium, Tel: (32) 2 663 0600, Fax: (32) 2 663 0640
Asia Pacific: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel: (852) 2887 4788, Fax: (852) 2508 1846