Rockwell Automation

ThinManager™ Security 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.

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

Throughout this manual we use the following notes to make you aware of safety considerations:

WARNING

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

IMPORTANT

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

ATTENTION

Identifies information about practices or circumstances that can lead to personal injury or death, property damage, or economic loss. Attentions help you:

- identify a hazard
- avoid a hazard
- recognize the consequence

SHOCK HAZARD

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

BURN HAZARD

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

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.

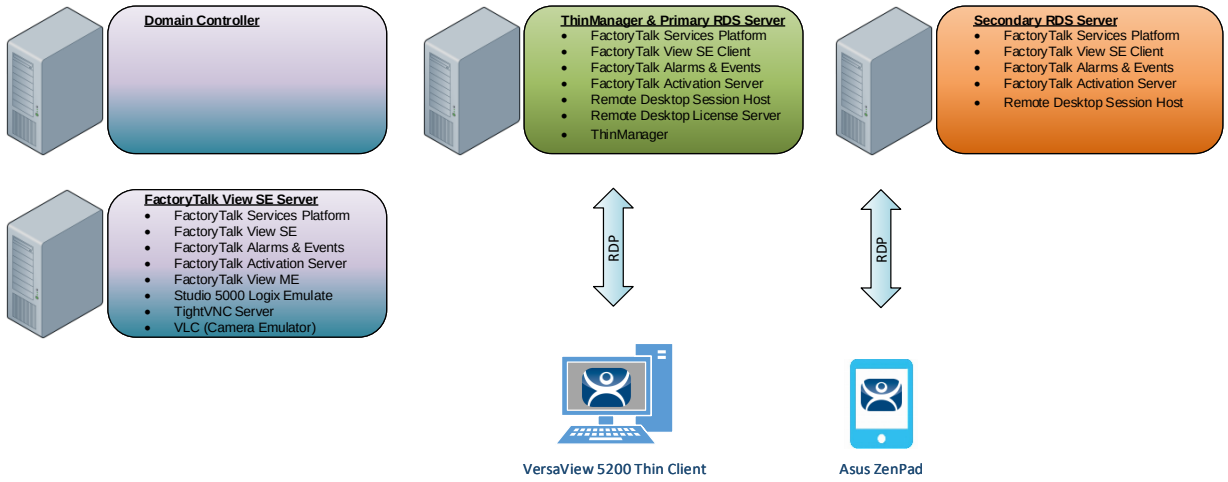
his lab is broken up into smaller segments and should be performed sequentially to start. Start by completing Sections 1 – 14 **in order**. Once Section 14 is completed you may proceed to complete **any** subsequent Section (15 – 18) in **any** order. To set expectations properly, it will most likely 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 9 separate sections. In this lab, you will specifically gain experience with the following topics:

- Section 1: Restore ThinManager Database
- Section 2: FactoryTalk Security and Group Policy for Remote Start of Applications
- Section 3: ThinManager Redundancy and Firewall Configuration
- Section 5: Modules
- Section 6: Terminal Groups, Overrides, Schedules and Mouse Button Mapping
- Section 7: Securing the ThinManager Admin Console
- Section 8: Relevance Location Services - Geo-Fencing
- Section 9: Virtual Thin Clients, PXE Server and Wireshark

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

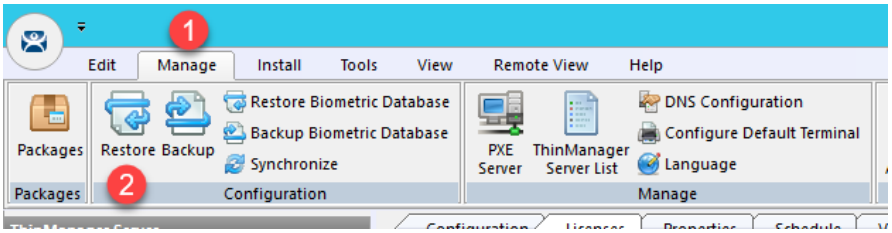
Section 1: Restore ThinManager Configuration

Within ThinManager, it is very easy to backup and restore your configuration. It is even possible to setup a simple schedule to automatically backup the ThinManager Configuration.

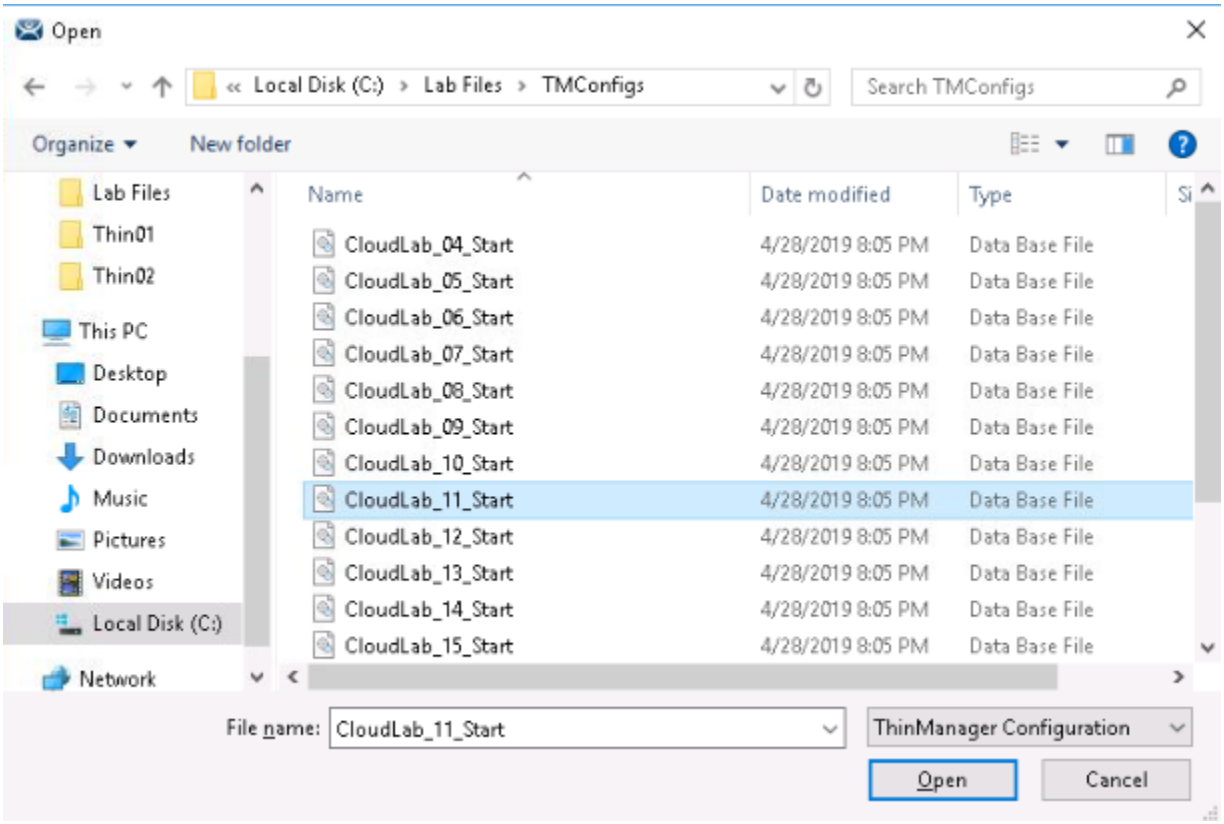
Here you will restore a backup of the ThinManager configuration database to get you started in this section.

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

2. From ThinManager, click the **Manage** ribbon, followed by the **Restore** icon.



3. From the **Open** dialog, navigate to the **C:\Lab Files\TMConfigs** folder and select the **CloudLab_11_Start** file, followed by the **Open** button.



Section 2: FactoryTalk Security and Group Policy for Remote Start of Applications

Overview

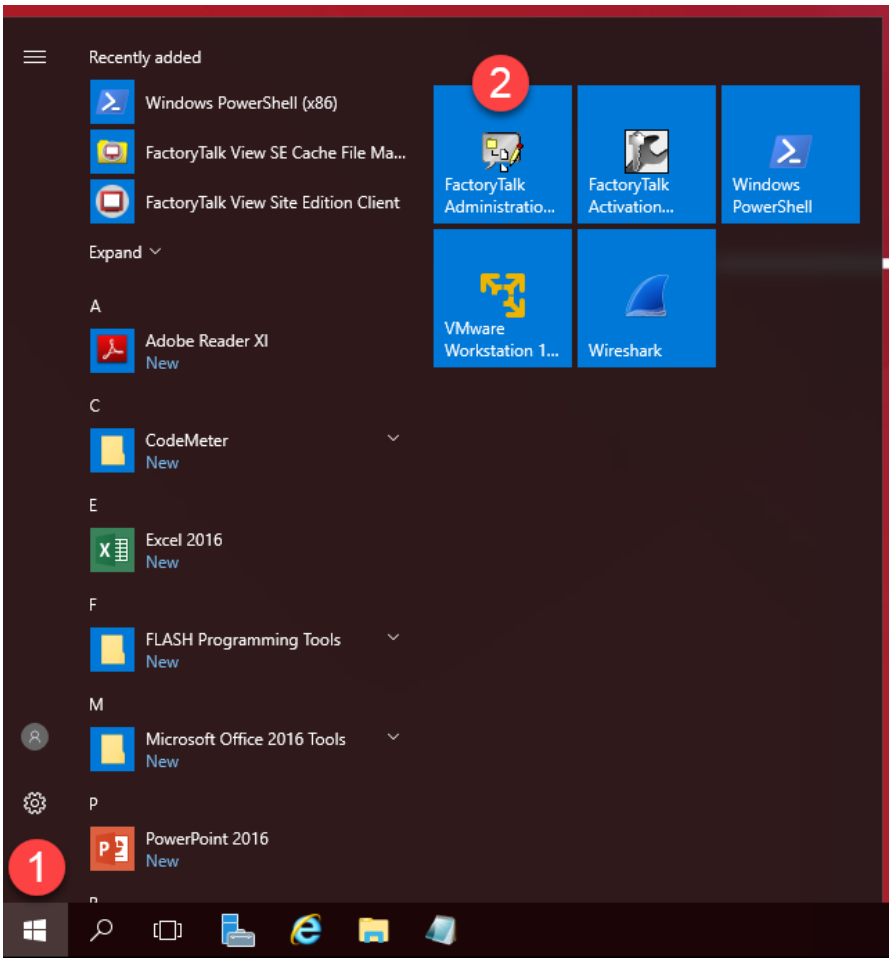
This section will use ThinManager Application Link to deliver the base setup for delivering secure sessions to the virtual thin client **without** a desktop. To do this, you will be performing the following tasks:

1. Add Terminal Names to FactoryTalk Directory
2. Add Windows Linked User Group to FactoryTalk Directory
3. Allow Remote Start of Unlisted Programs

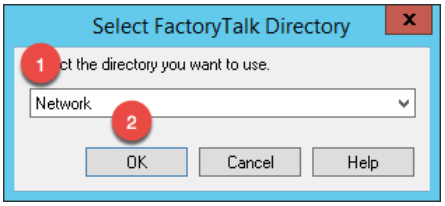
Add Terminal Names to FactoryTalk Directory

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.

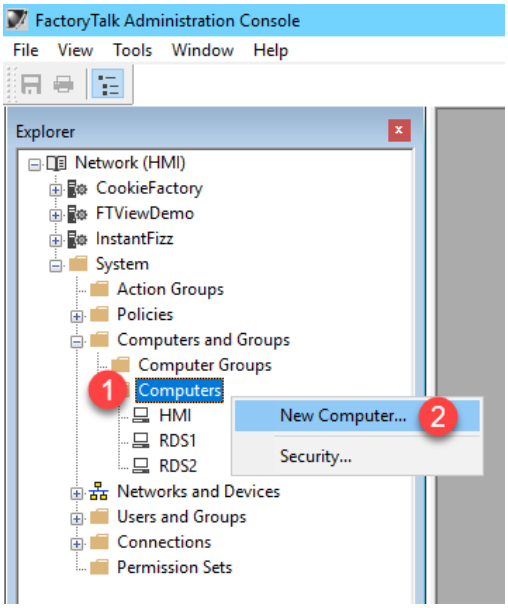
1. Click the **Windows Start** button from the **RDS1** host image – **NOT** the shadowed Desktop delivered to the thin client or the thin client itself.



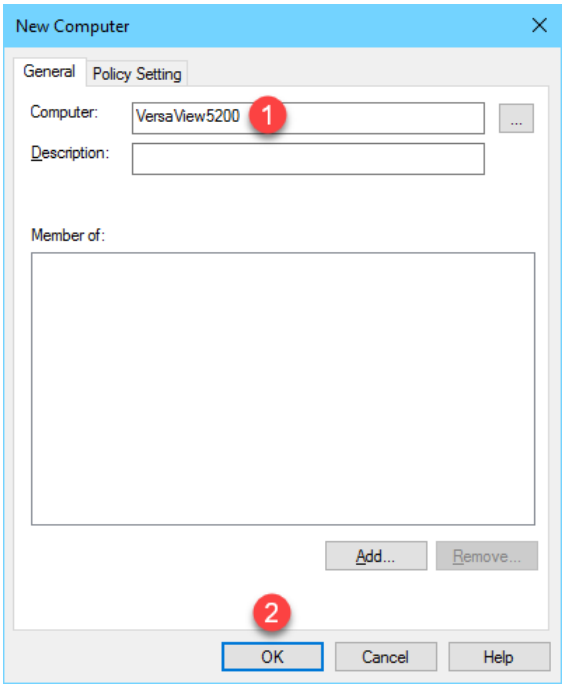
2. On the **Select FactoryTalk Directory** dialog, make sure **Network** is selected and click the **OK** button.



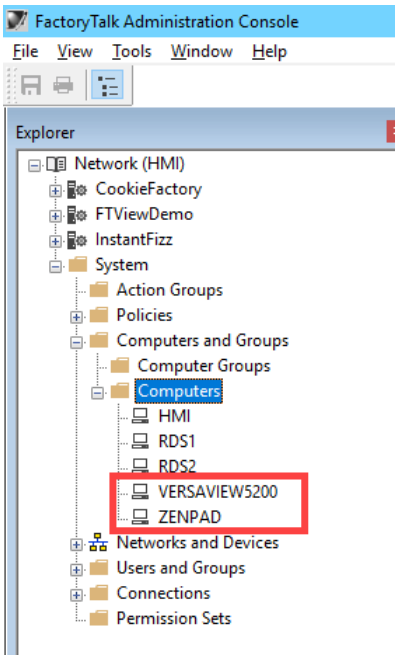
3. In the **Explorer** view, browse to **Network (THIS COMPUTER) →System→Computers and Groups→Computers**, right click **Computers** and select **New Computer…** from the menu.



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.

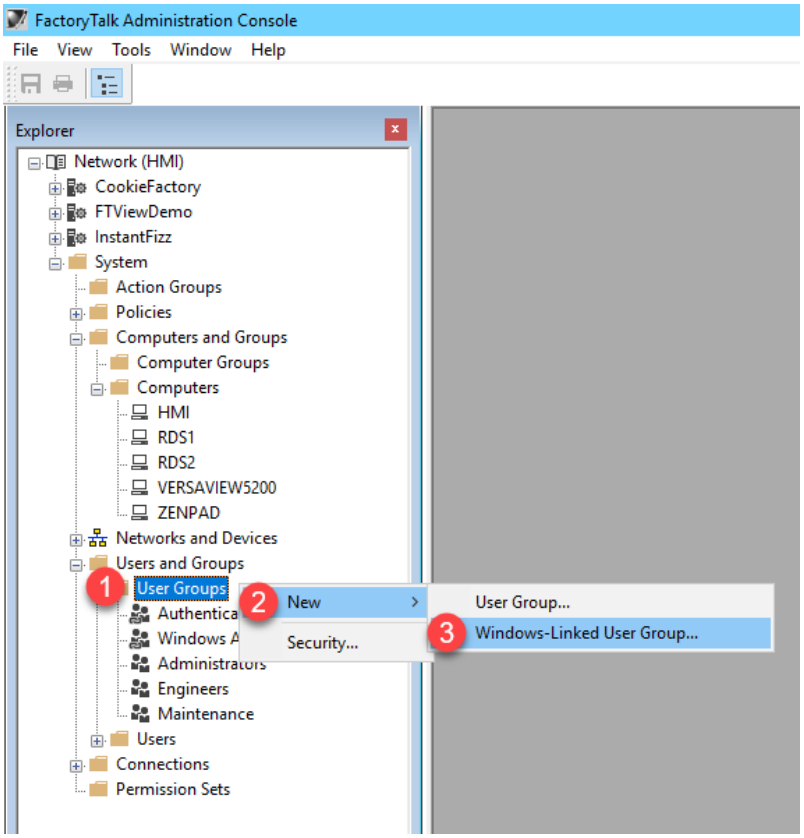


6. Keep the **FactoryTalk Administration Console** open for the next section.

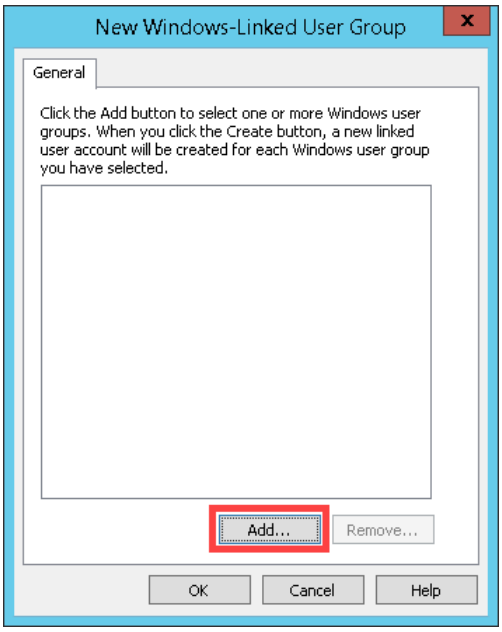
Add Windows Linked User Group to FactoryTalk Directory

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.

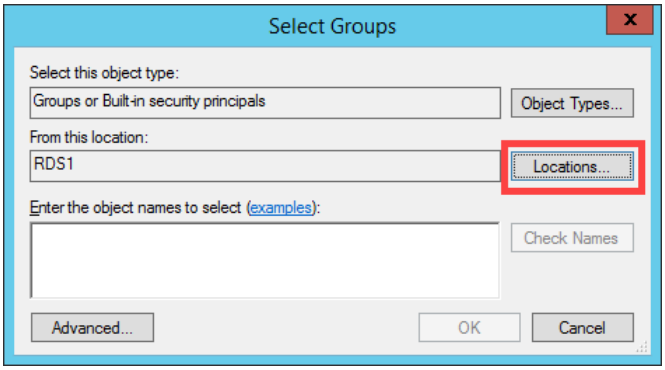
1. In the **Explorer** view, browse to **Network (THIS COMPUTER) →System→Users and Groups→User Groups**, right click **User Groups** and select **New | Windows-Linked User Group…** from the menu.



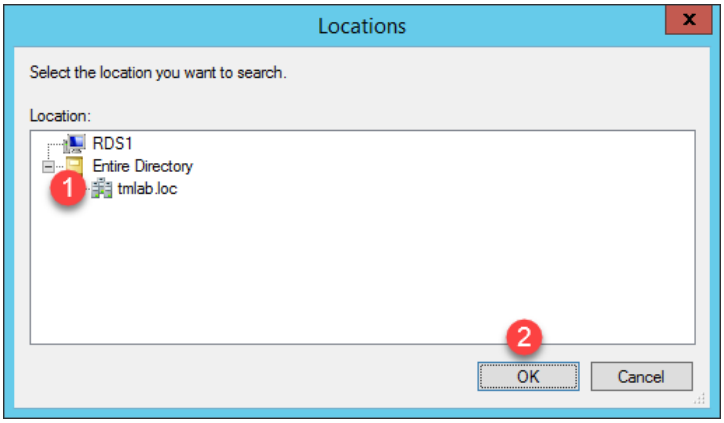
2. From the **New Windows-Linked User Group** popup, click the **Add** button.



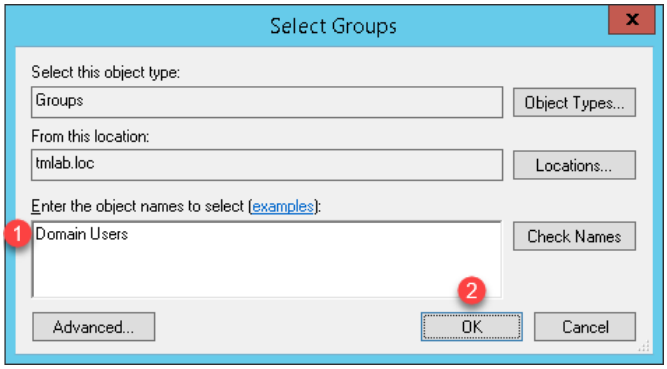
3. By default, this dialog box will show the local computer's user and groups, but we want to browse the **TMLAB** domain. From the **Select Groups** window, click the **Locations…** button.



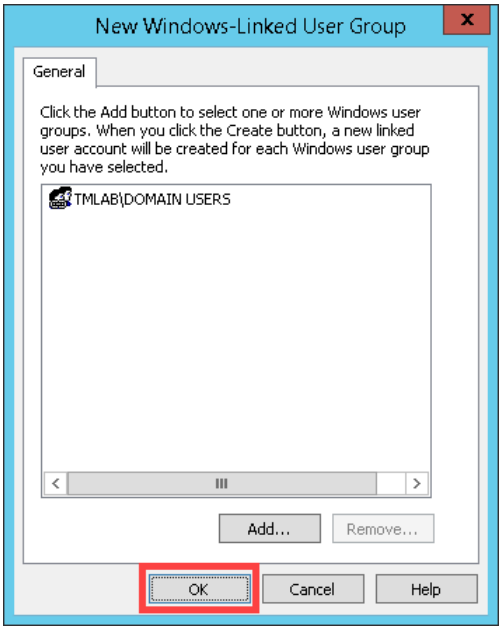
4. From the **Locations** selection box, expand the **Entire Directory** item and select the **tmlab.loc** item. Click the **OK** button.



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**.

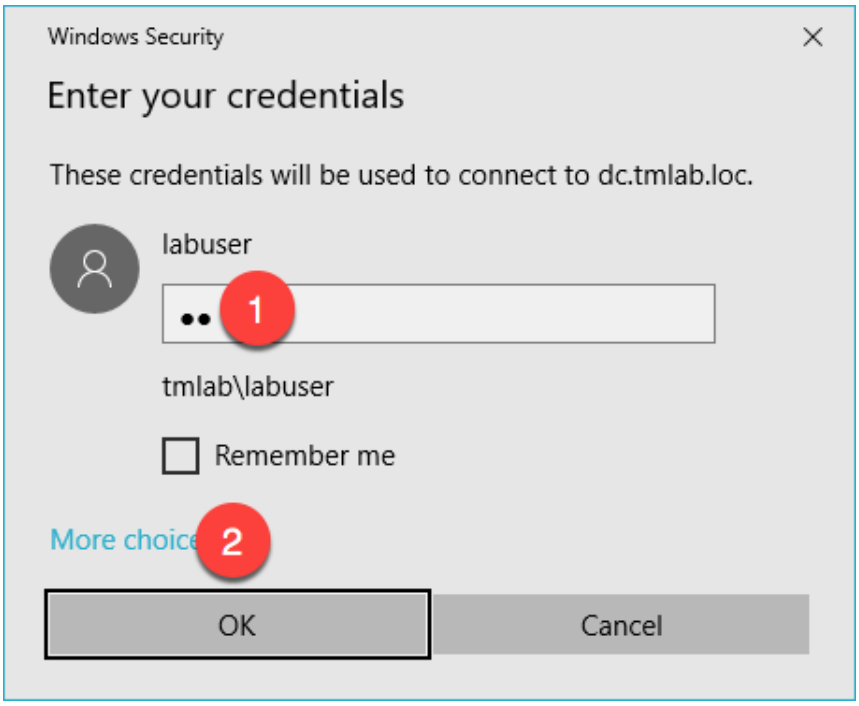
> In your deployments, you will most likely want to be more selective with which Windows user groups to link and to which FactoryTalk group to assign them. This section utilized the entire Domain Users group to simplify the lab going forward.

Allow Remote Start of Unlisted Programs

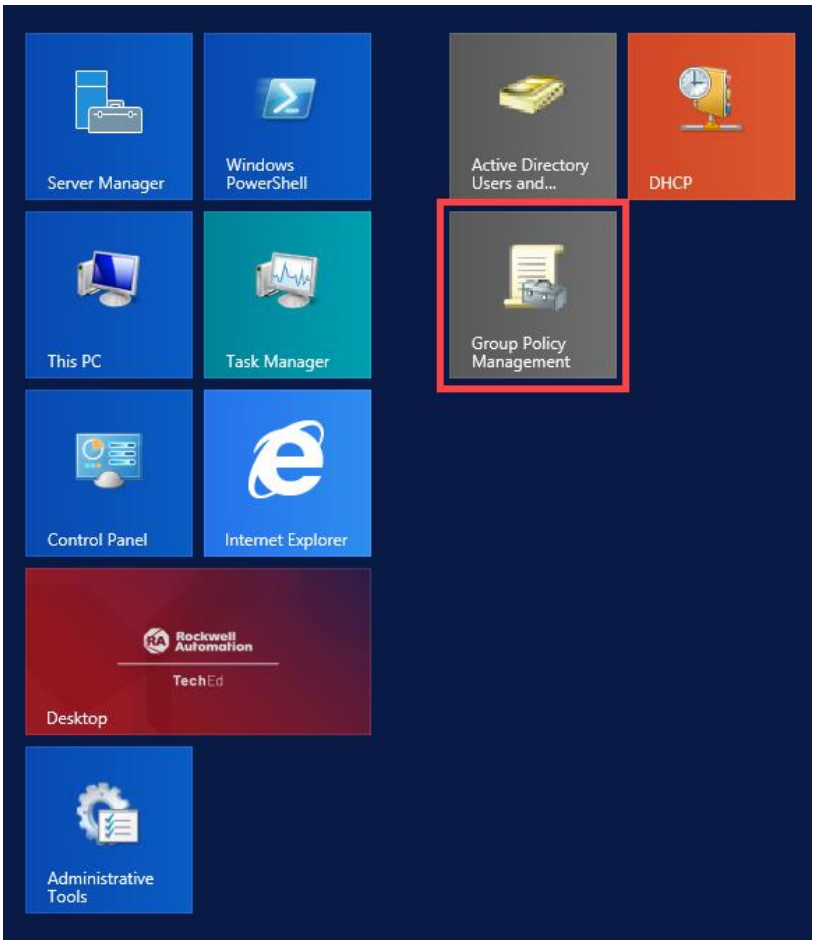
As described previously, Remote Desktop Services considers any program configured to run initially - like the ones used with ThinManager **ApplicationLink** - an "Initial Program." By default, Windows Server 2008R2 and later Remote Desktop Services requires that each Initial Program be added to the published **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.

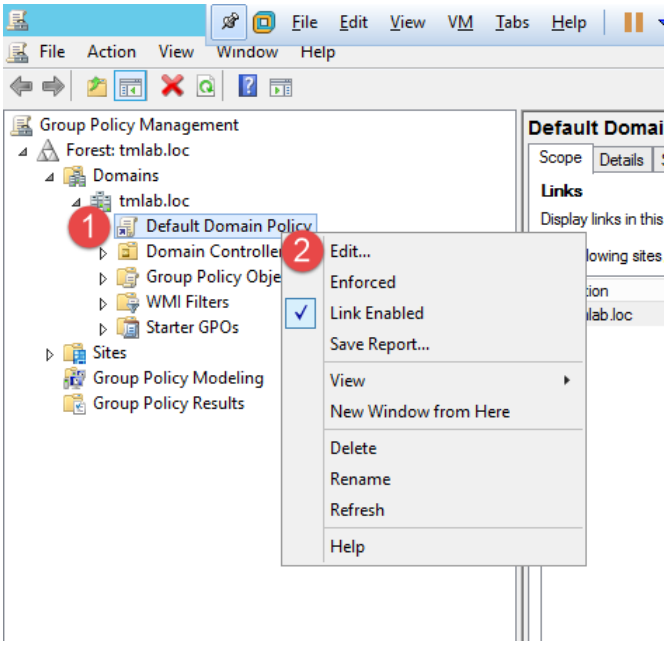
2. If you are prompted to enter login credentials, make sure the username is *tmlab\labuser* and enter a password of *rw*.



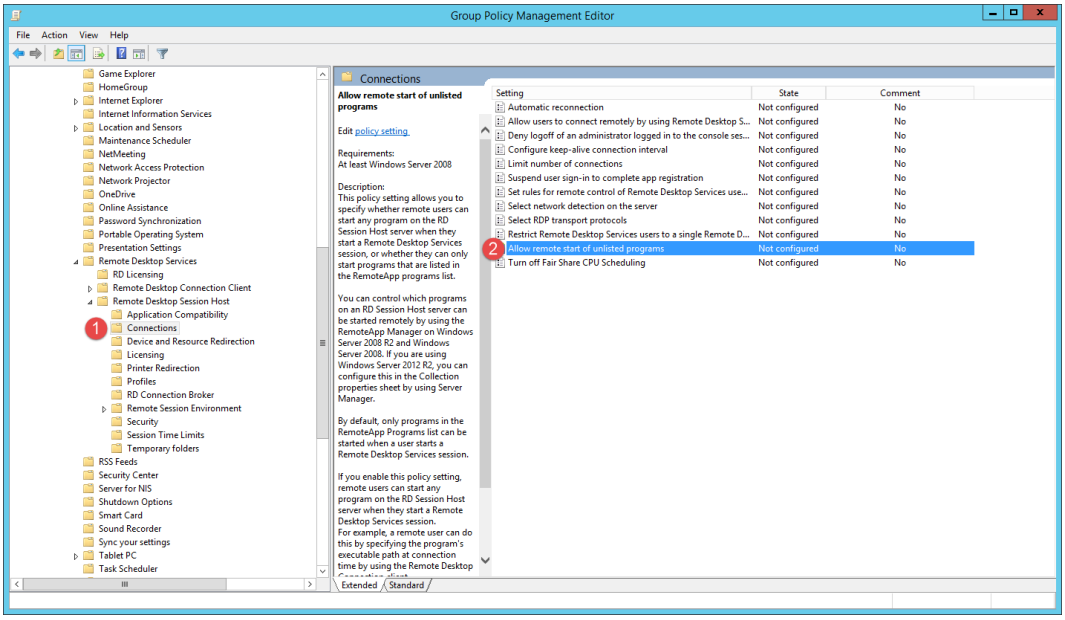
3. Click the **Windows Start** button.
4. From the **Windows Start Menu**, click the **Group Policy Management** icon.



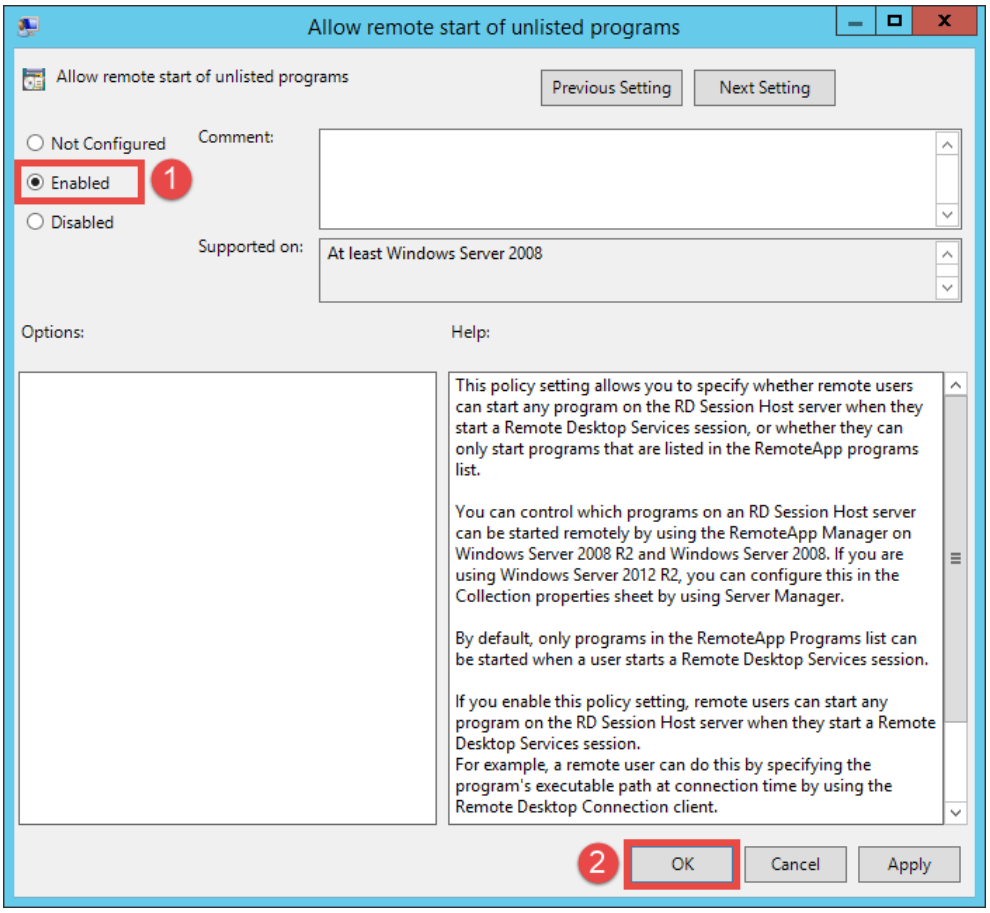
5. From the **Group Policy Editor**, right click the **Default Domain Policy** item and click **Edit…**



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.

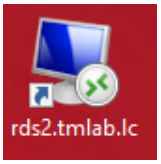


7. From the ensuing policy setting dialog box, click the **Enabled** option button followed by the **OK** button. Close the **Group Policy Management Editor** and the **Group Policy Management** window.

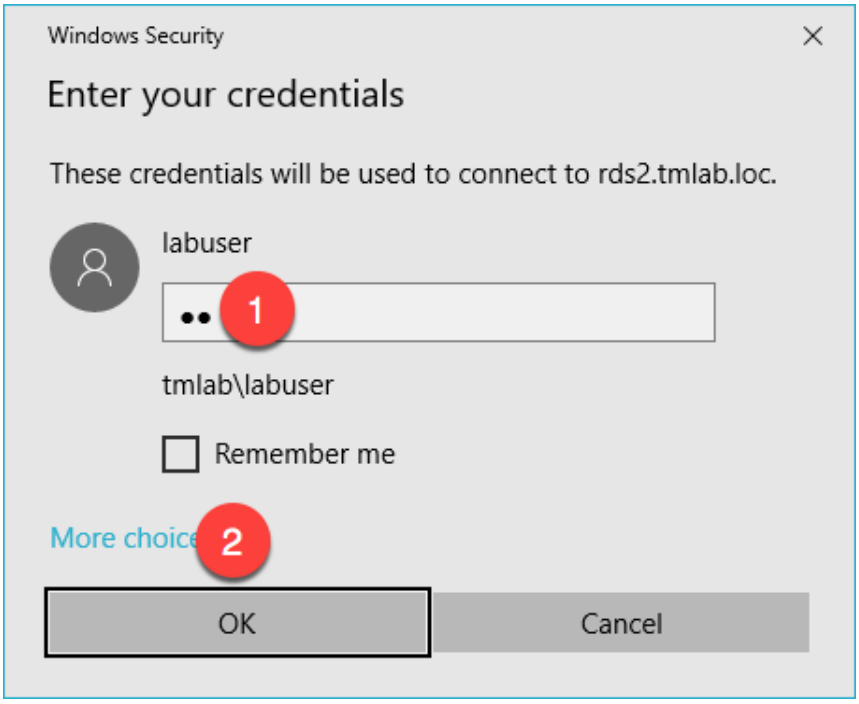


8. Close the remote desktop session on **dc.tmlab.loc**. Click **OK** to the confirmation dialog box.

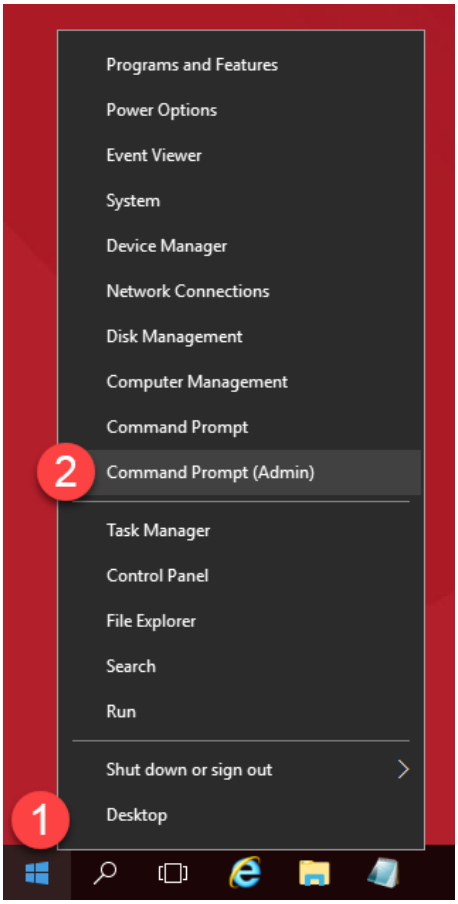
9. The **Group Policy** does not take effect immediately on the member **Remote Desktop Servers**. The final steps of this section will force the update to occur. To apply the change to **RDS2**, double click the **rds2.tmlab.loc** shortcut on the **RDS1** desktop.



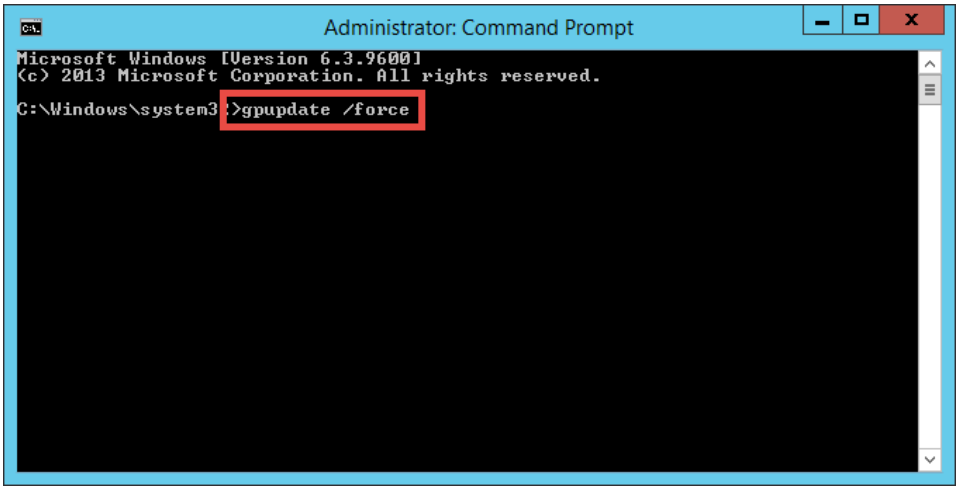
10. If you are presented with a login dialog box, make sure the username is *tmlab\labuser* and enter a password of *rw*.



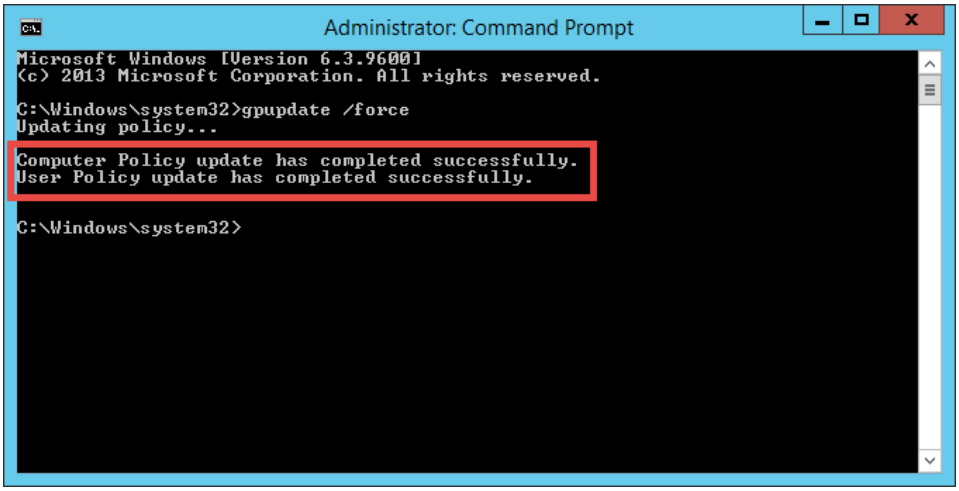
11. From **RDS2**, right click the **Windows Start Button** and click **Command Prompt** (**Admin**).



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



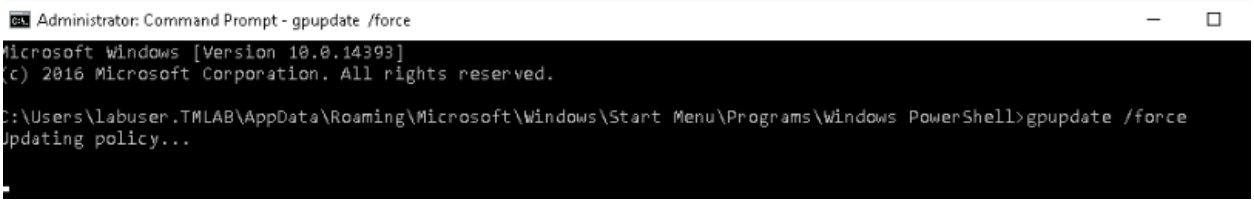
13. Once the updated policy has been applied, close the **Administrator: Command Prompt window**.



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

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

Note: On RDS1, the default path will be different than C:\Windows\system32 as it was on RDS2. The gpupdate /force command can be run from any directory.



Section 4: 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.

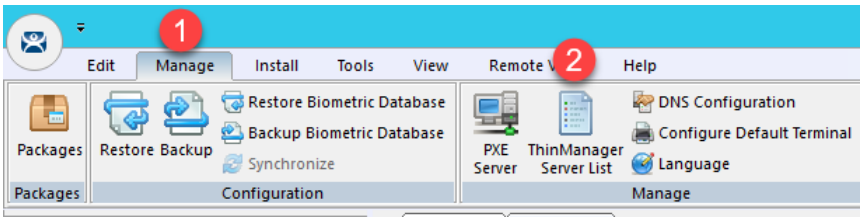
In this section, you will be performing the following tasks:

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

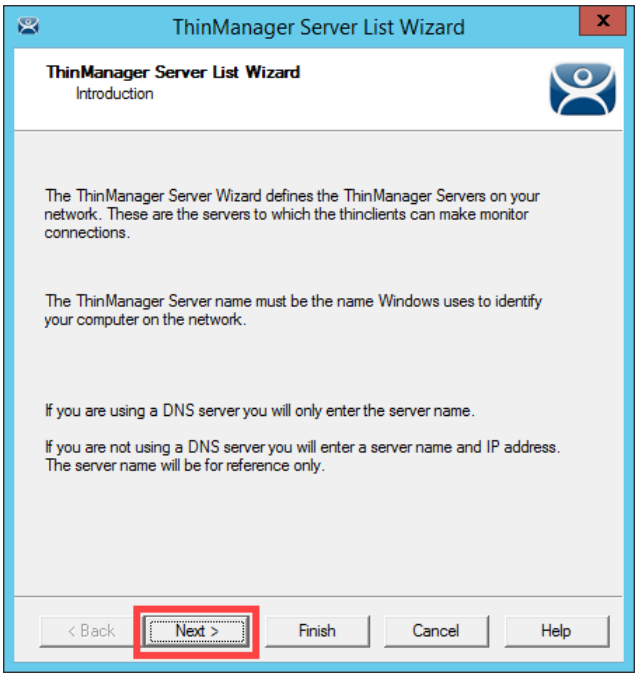
Configure Automatic Synchronization

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.

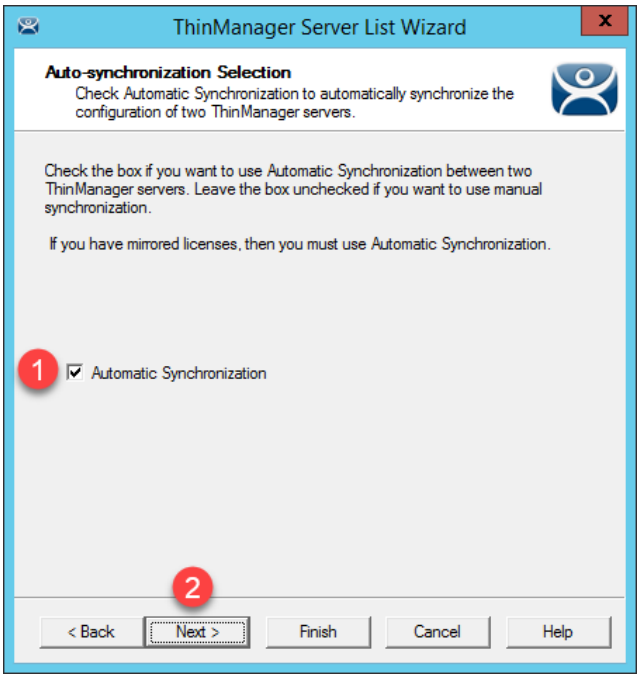
1. From ThinManager, click the **Manage** ribbon followed by the **ThinManager Server List** icon.



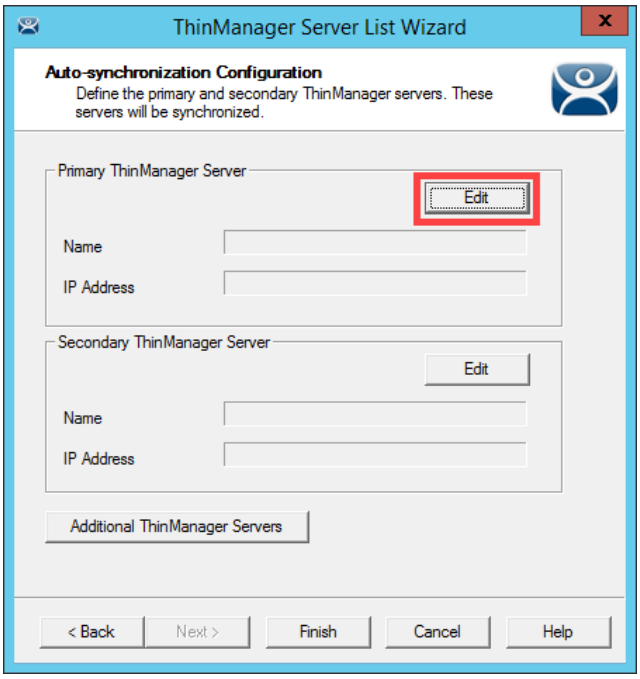
2. The **ThinManager Server List Wizard** will launch. Click the **Next** button from the **Introduction** page of the wizard.



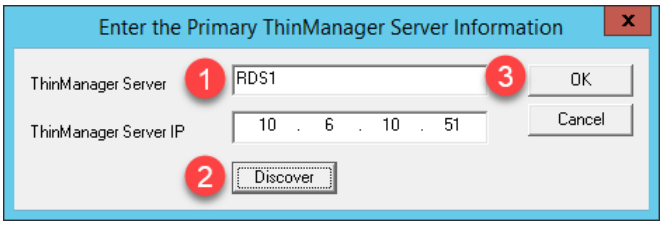
3. From the **Auto-synchronization Selection** page of the wizard, check the **Automatic Synchronization** checkbox and click the **Next** button.



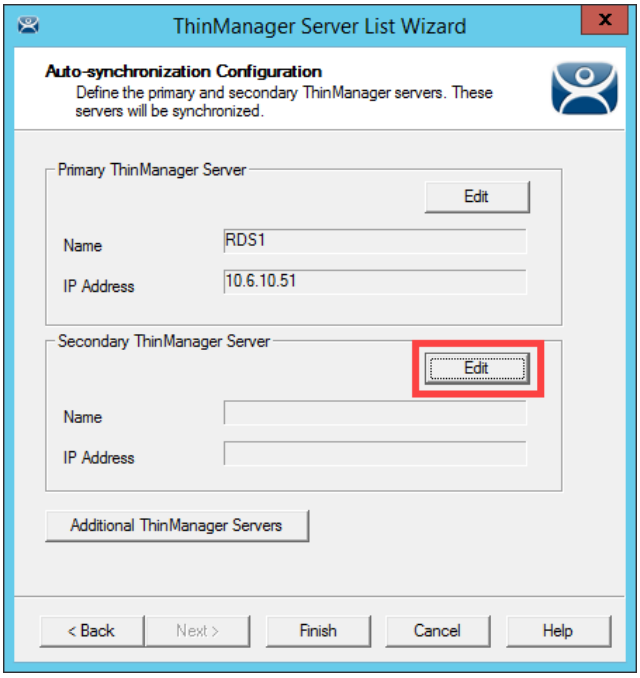
4. From the **Auto-synchronization Configuration** page of the wizard, click the **Edit** button in the **Primary ThinManager Server** frame.



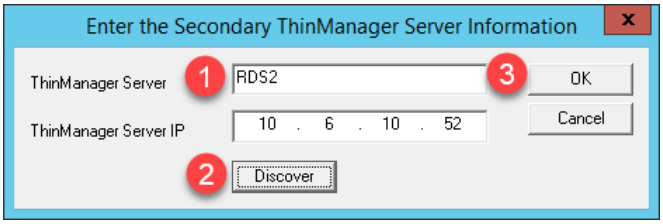
5. Enter *RDS1* in the **ThinManager Server** field, followed by the **Discover** button, which should auto-fill the **IP Address** of **RDS1** in the **ThinManager Server IP** Field. Click the **OK** button.



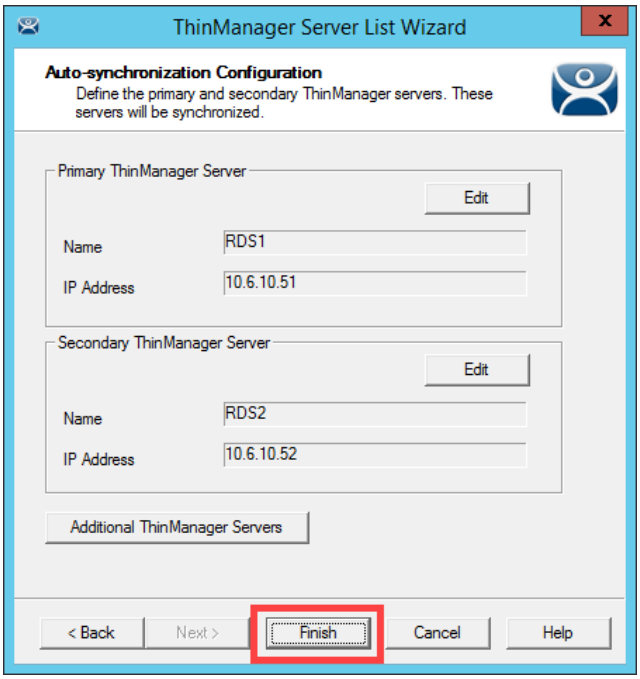
6. Back on the **Auto-synchronization Configuration** page of the wizard, click the **Edit** button from the **Secondary ThinManager Server** frame of the wizard.



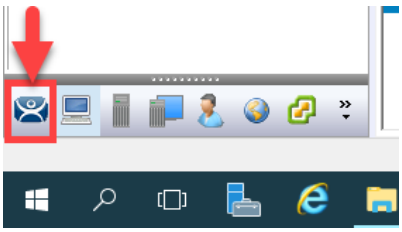
7. Enter *RDS2* in the **ThinManager Server** field, followed by the **Discover** button, which should auto-fill the **IP Address** of **RDS2** in the **ThinManager Server IP** Field. Click the **OK** button.



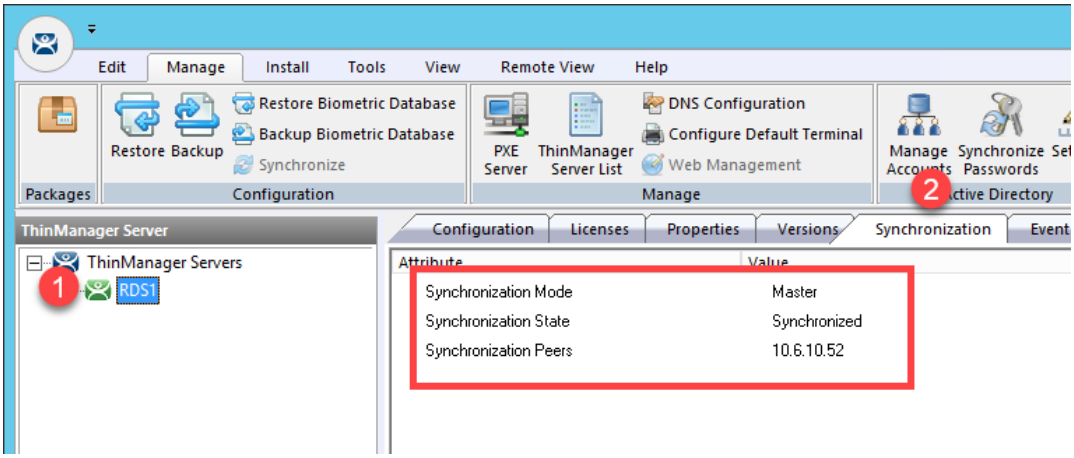
8. Back on the **Auto-synchronization Configuration** page of the wizard, click the **Finish** button.



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



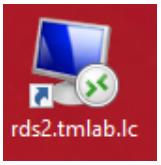
10. From the **ThinManager Server** tree, select **RDS1**, followed by the **Synchronization** tab. You should see a **Synchronization State** of **Synchronized**.



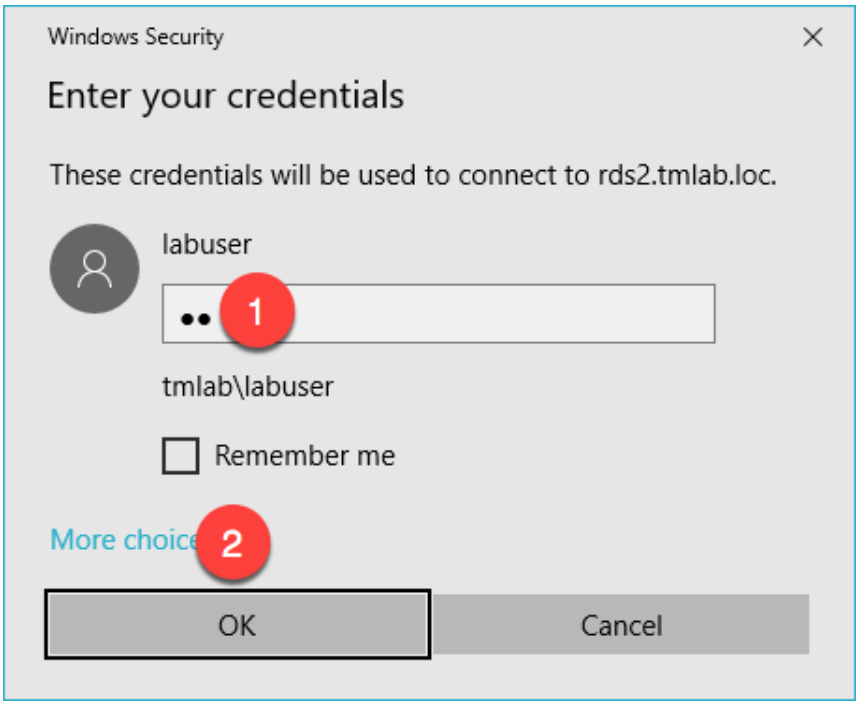
If the Synchronization State does not immediately show Synchronized, simply click on another tab, and return to the Synchronization tab to refresh its state.

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.

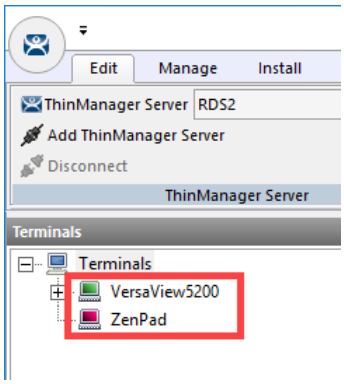


12. If you are presented with a login dialog box, make sure the username is *tmlab\labuser* and enter a password of *rw*. Click the **OK** button.



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**.

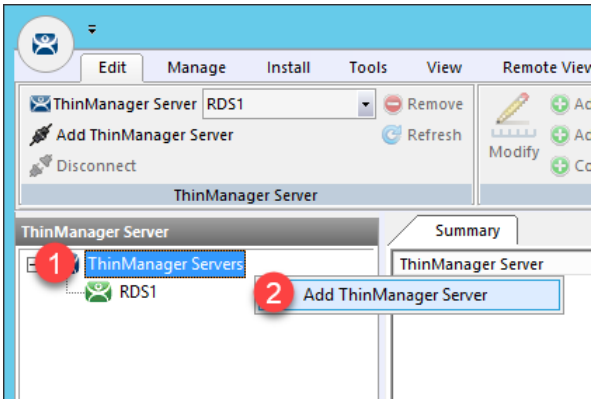


15. Close the remote desktop session on **RDS2**. Click the **OK** button if you are presented with a confirmation dialog box.

Add Remote ThinManager Server

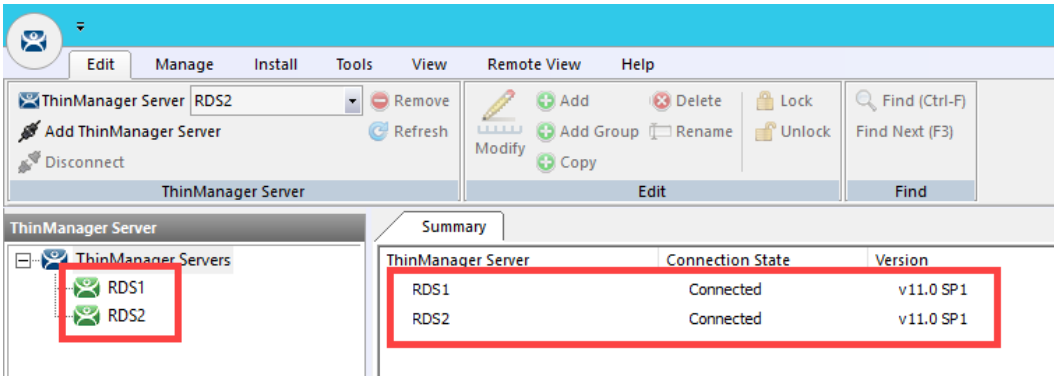
The ThinManager **Administrative Console** can manage not only the **ThinServer** installed on its machine, but also remote **ThinServers** installed on remote machines. Keep in mind that the **Administrative Console** does not have to be installed on the same machine as the **ThinServer** service, although 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**.

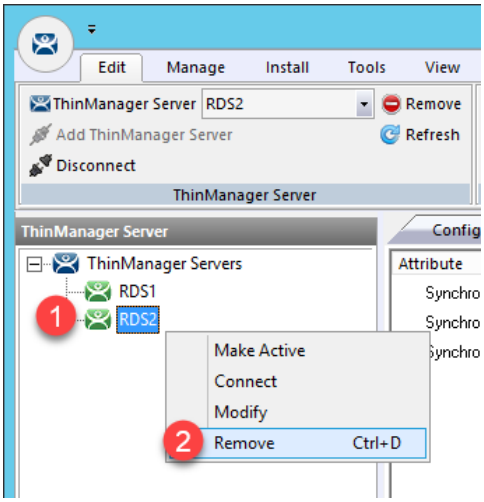


2. From the **ThinManager** popup window, enter *RDS2* in the **Enter ThinManager Server** field and click the **OK** button.

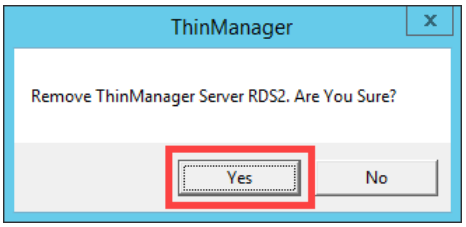
3. Notice that **RDS2** has now been added to the **ThinManager Admin Console**. You could now manage the ThinManager configuration of **RDS2** remotely from **RDS1**.



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**.



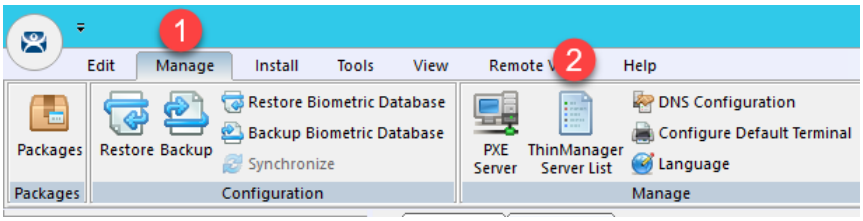
5. From the ensuing confirmation dialog box, click the **Yes** button.



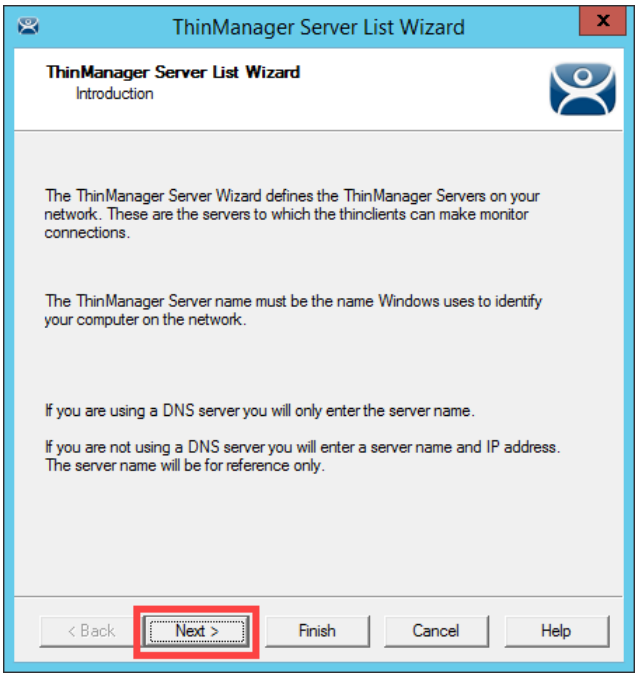
Disable Automatic Synchronization

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

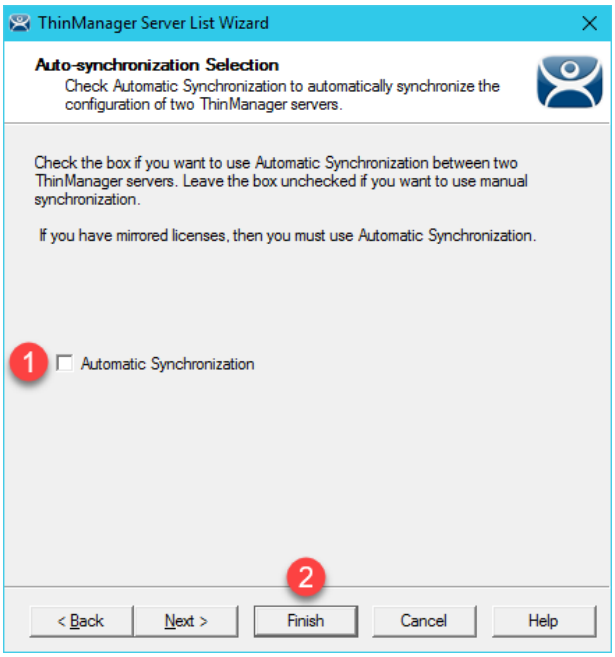
1. From ThinManager, click the **Manage** ribbon followed by the **ThinManager Server List** icon.



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



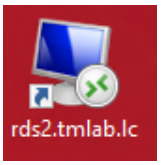
3. From the **Auto-synchronization Selection** page of the wizard, uncheck the **Automatic Synchronization** checkbox and click the **Finish** button.



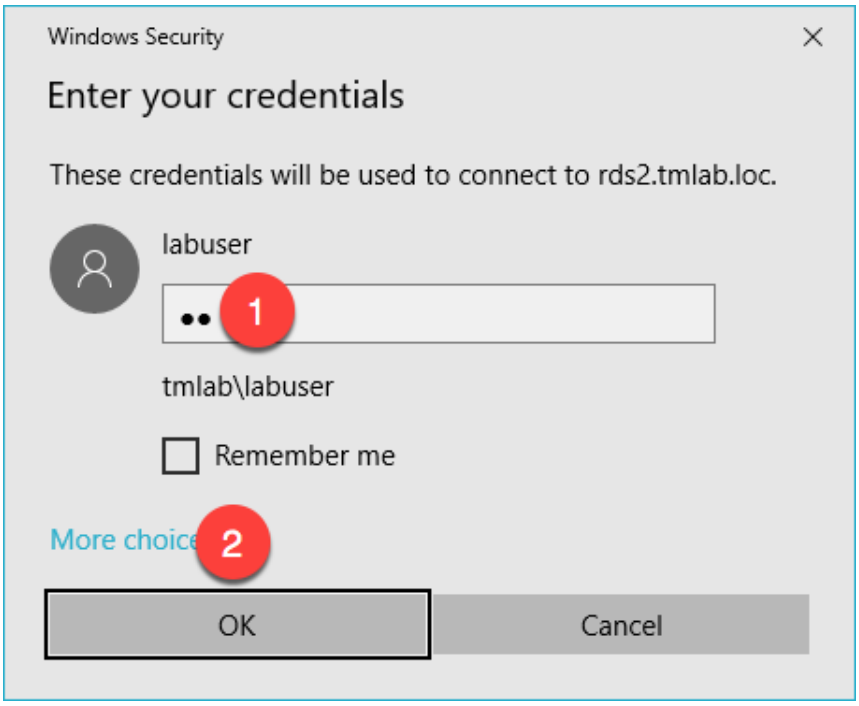
Disable Secondary ThinManager Server

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

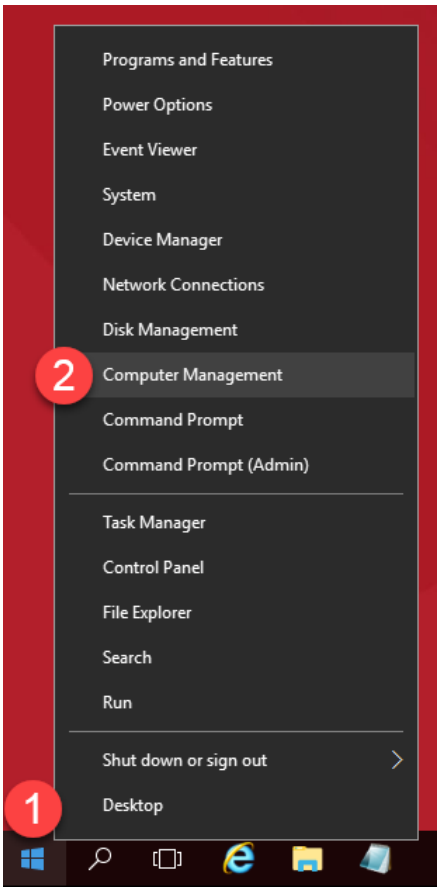
1. Double click the **rds2.tmlab.loc** shortcut on the **RDS1** desktop.



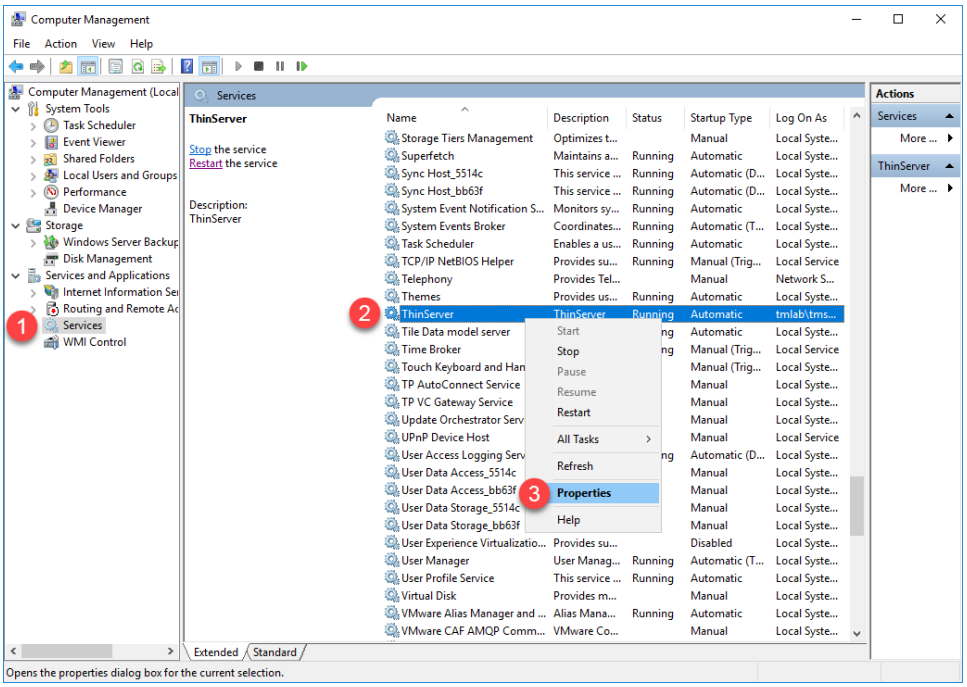
2. If you are presented with a login dialog box, make sure the username is *tmlab\labuser* and enter a password of *rw*. Click the **OK** button.



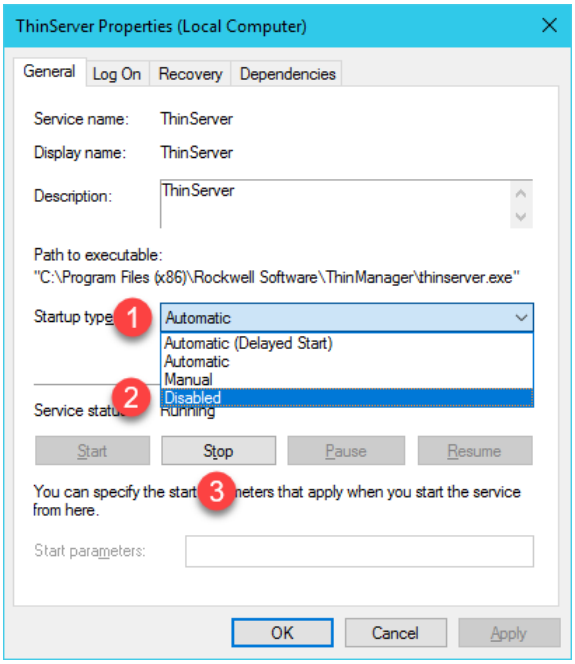
3. Close the **ThinManager Admin Console** if it is open.
4. Right-click the **Windows Start** button and select **Computer Management**.



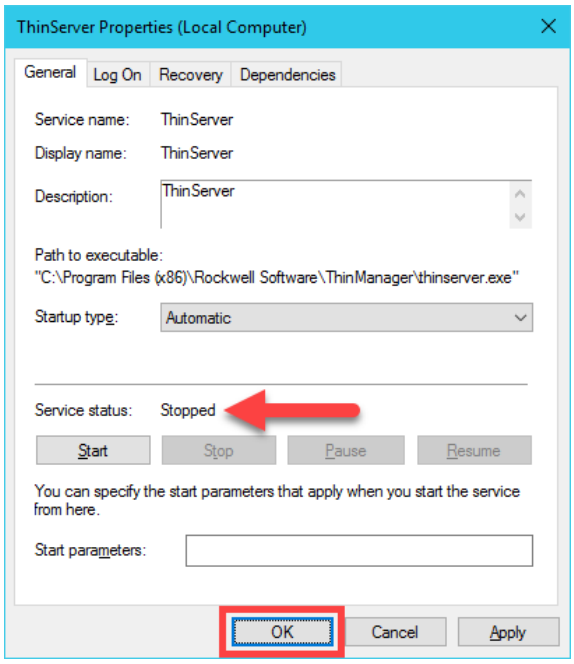
5. Expand the **Services and Applications** node and select the **Services** management console. Scroll down to find the **ThinServer** service, right-click and select **Properties.**



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.**

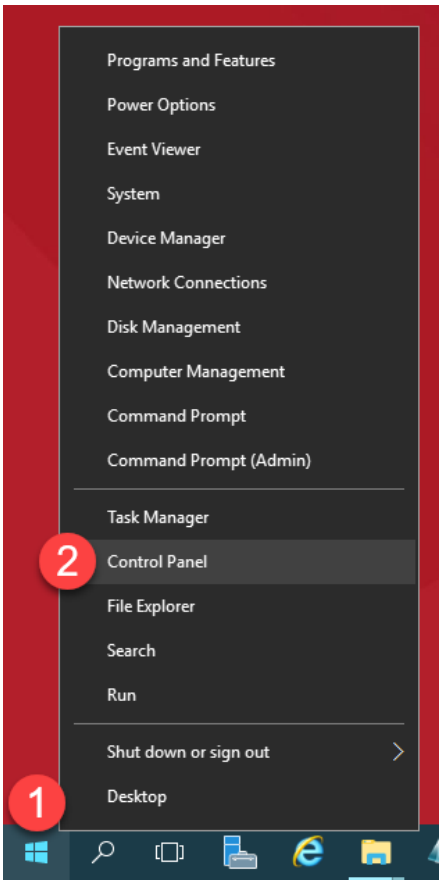


8. You have successfully disabled the **Secondary ThinManager Server**. The remaining lab sections can be completed with a single **ThinManager Server**. Close out of the **Computer Management** console on **RDS2**.

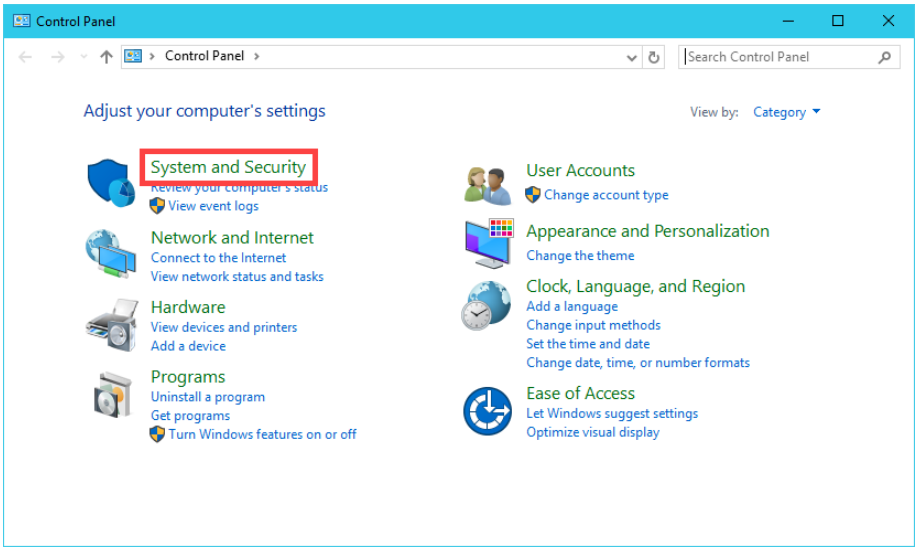
9. Close the remote desktop session on **rds2.tmlab.loc** to return to **RDS1**. Click the **OK** button if presented with a confirmation dialog box.

Turn On Windows Firewall on RDS1

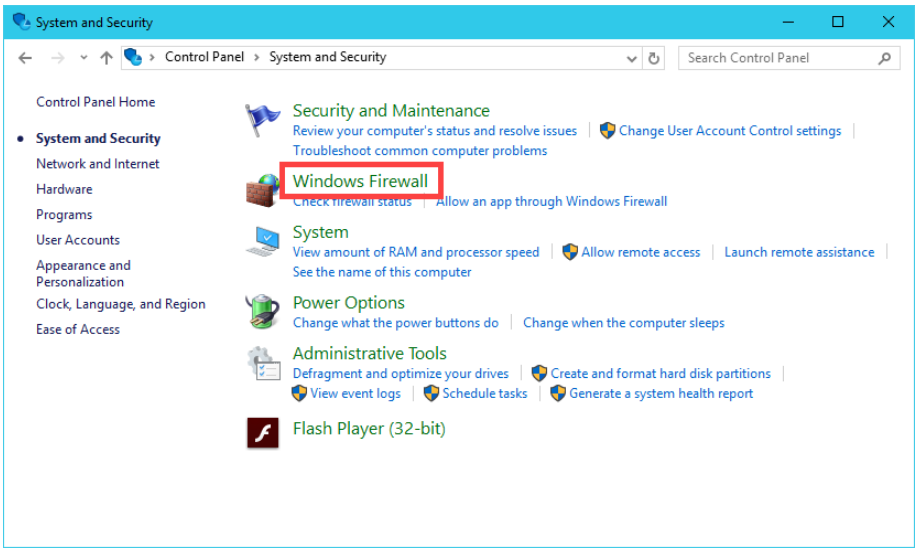
1. With the **VersaView5200** virtual thin client still powered on, right click the **Windows Start Button** on **RDS1** and select **Control Panel**.



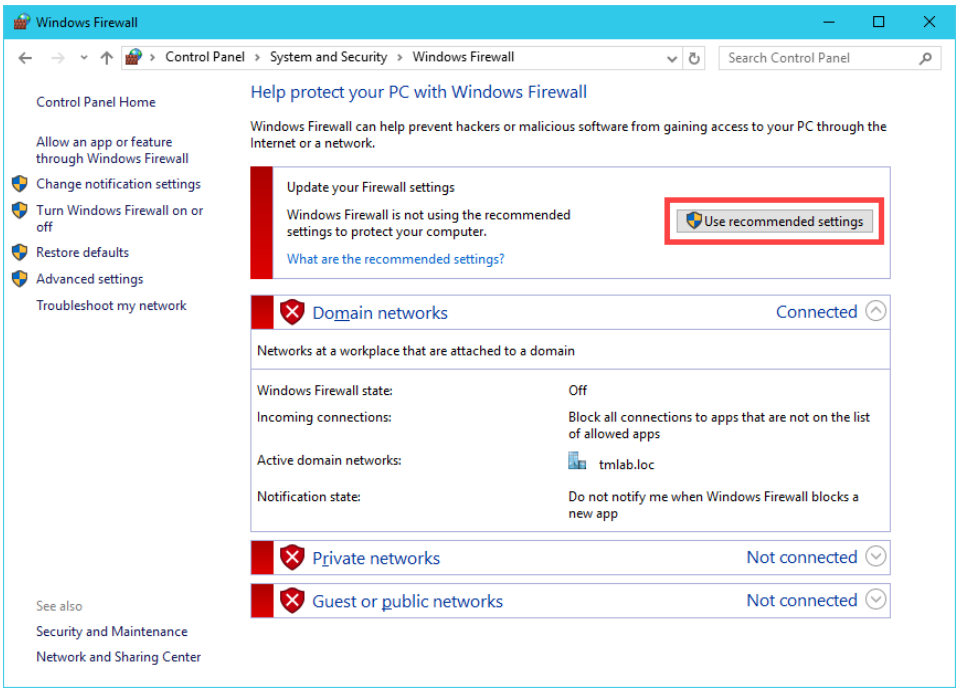
2. From the **Control Panel**, click the **System and Security** link.



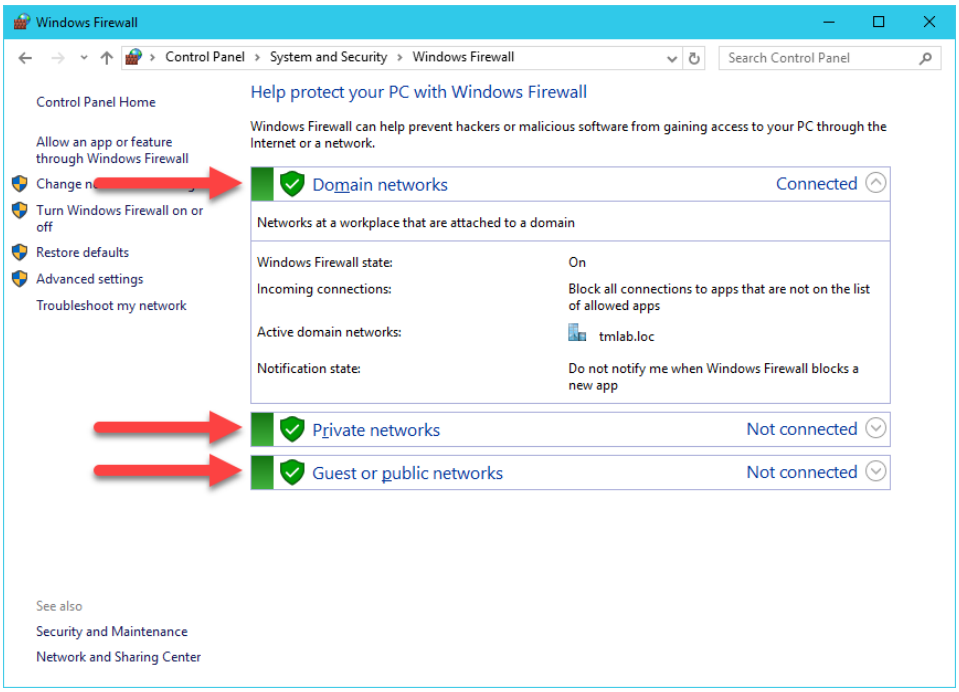
3. From the **System and Security** page of the **Control Panel**, click the **Windows Firewall** link.



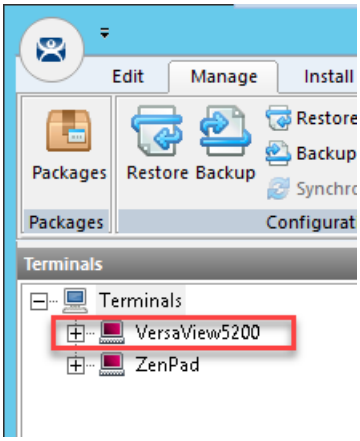
4. From the **Windows Firewall** page of the **Control Panel**, click the **Use recommended settings** button.



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**.

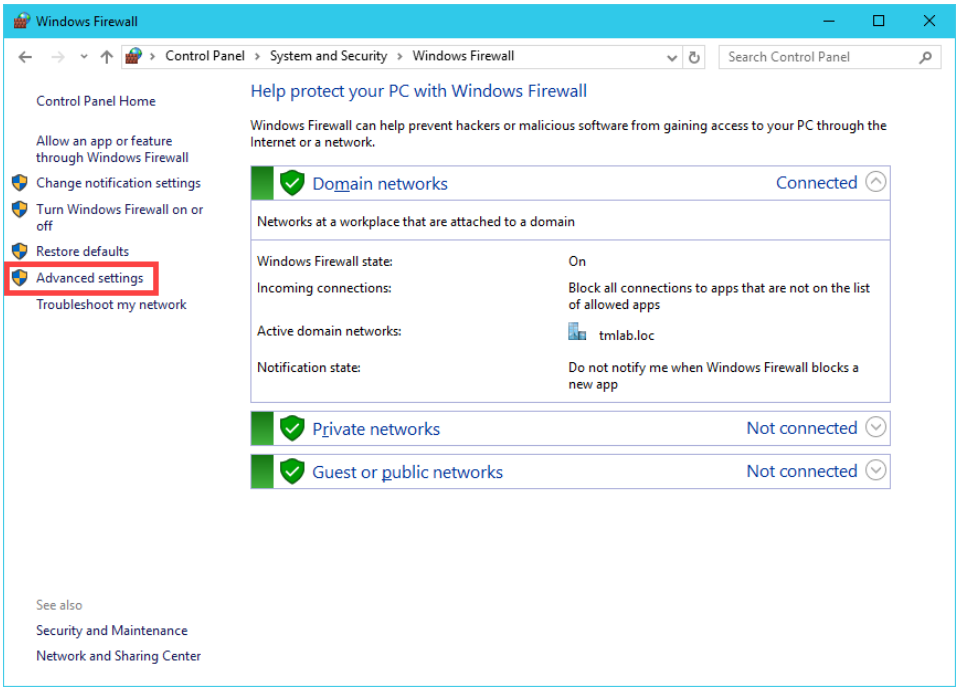


If you had a physical thin client and attempted to reboot it at this point, it would still be able to boot but not from the ThinManager installed on **RDS1**, instead **RDS2** would respond to the PXE request and boot the terminal. Unfortunately, we are unable to demonstrate this in the Cloud as the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

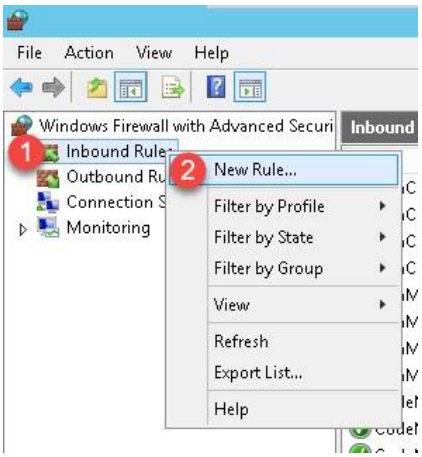
Configure Windows Firewall on RDS1

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.

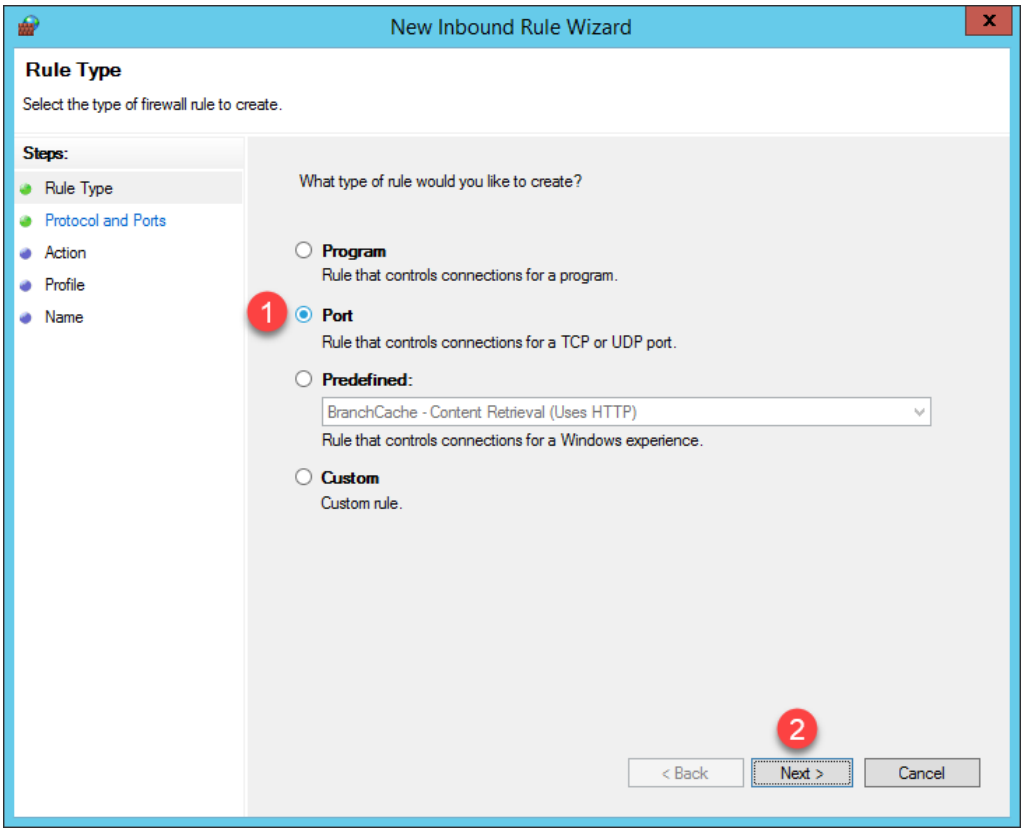
1. Return to the **Windows Firewall** page of the **Control Panel** on **RDS1** and click the **Advanced Settings** link.



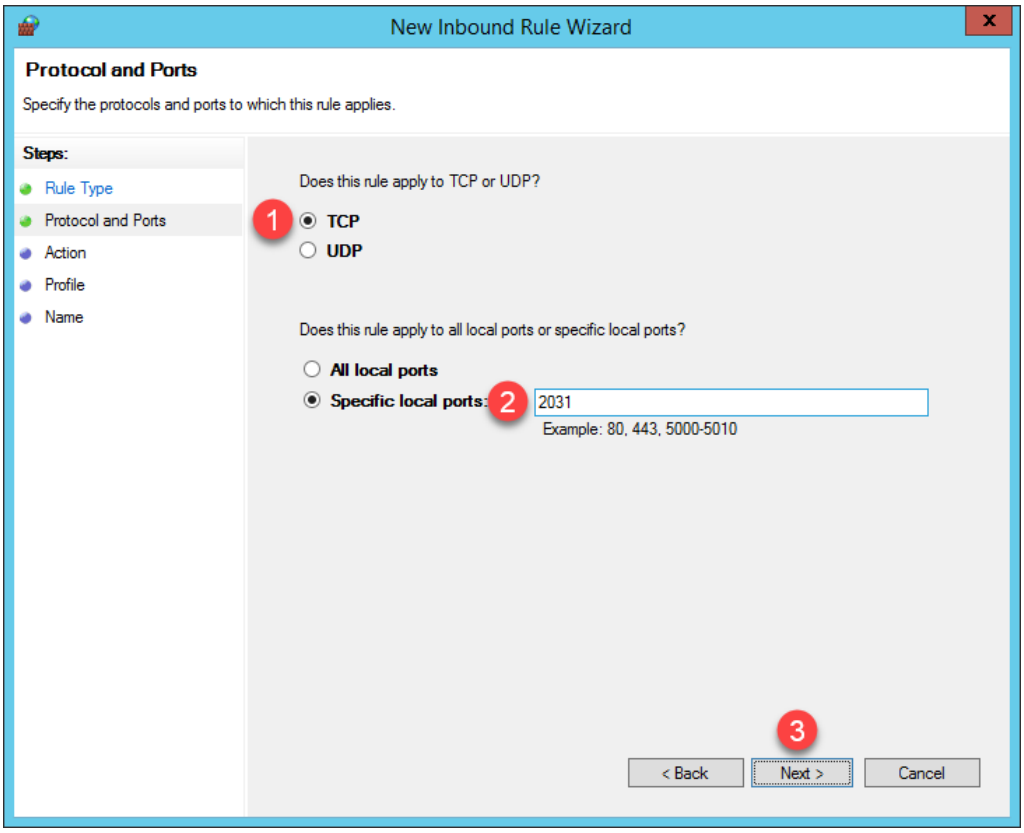
2. From the **Windows Firewall and Advanced Security** window, right click the **Inbound Rules** tree item and select **New Rule..**



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

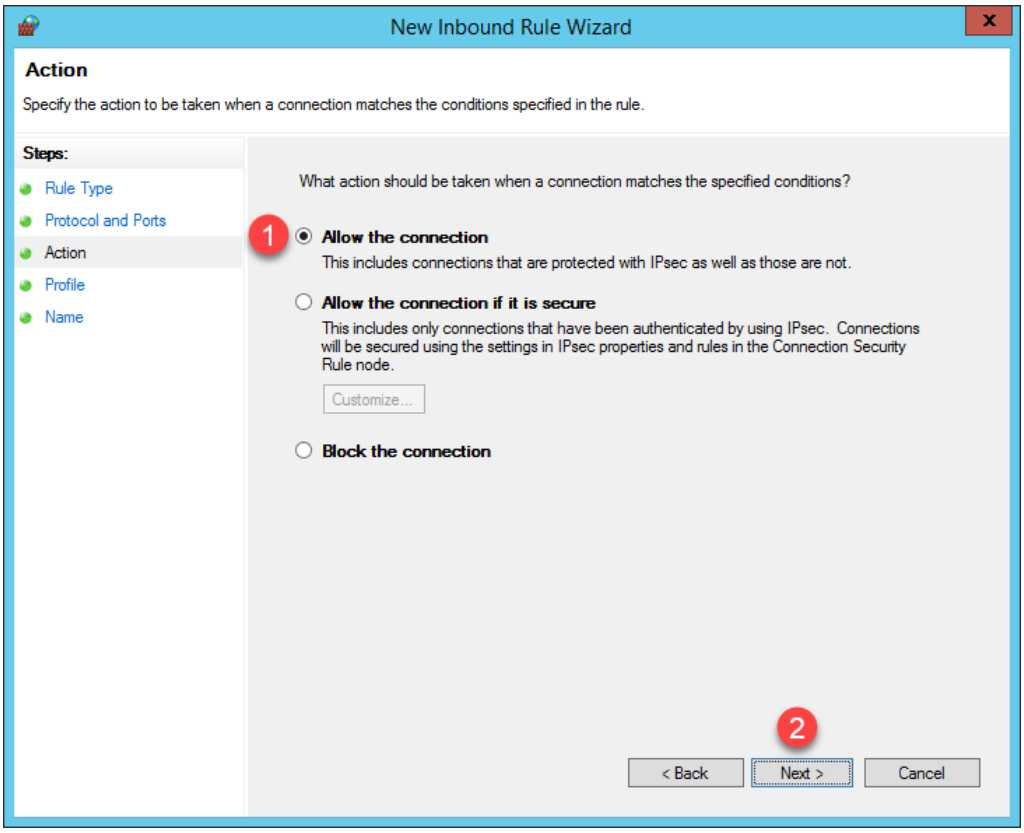


4. From the **Protocol and Ports** panel of the **New Inbound Rule Wizard**, select the **TCP** radio button and enter *2031* in the **Specified local ports** field. Click the **Next** button.

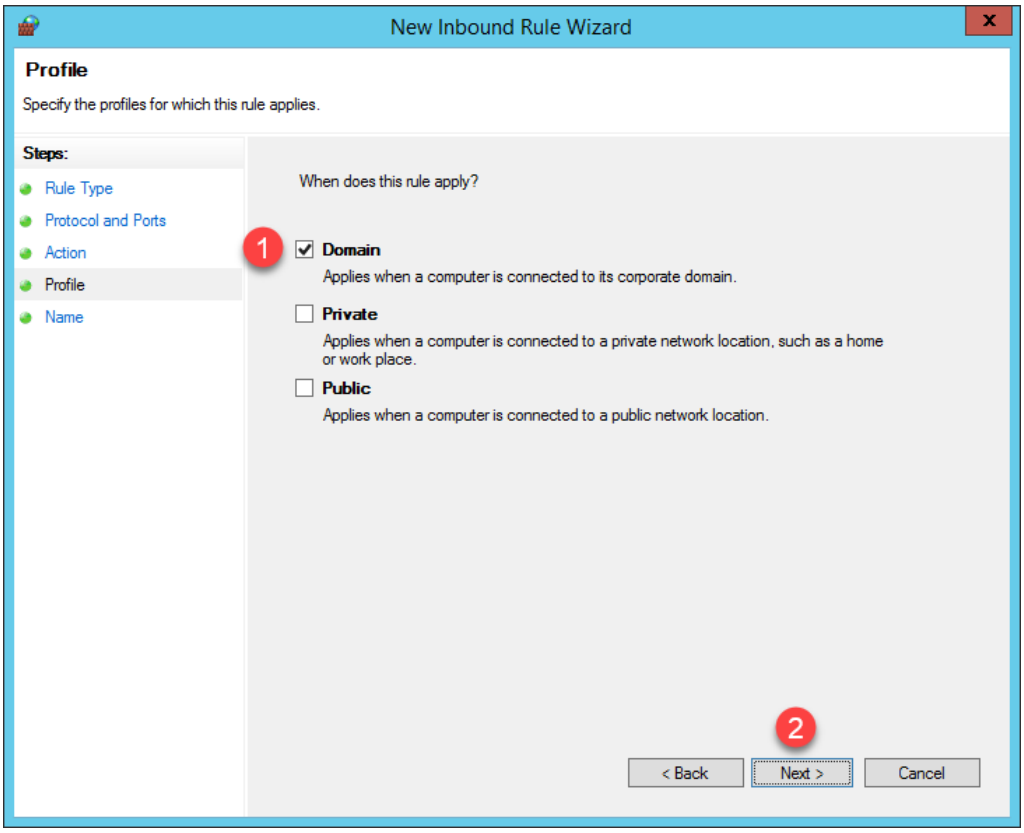


TCP Port 2031 is required by ThinManager for the Terminal Monitor Connection as well as for the delivery of the Terminal Profile to the terminal when it is booting up.

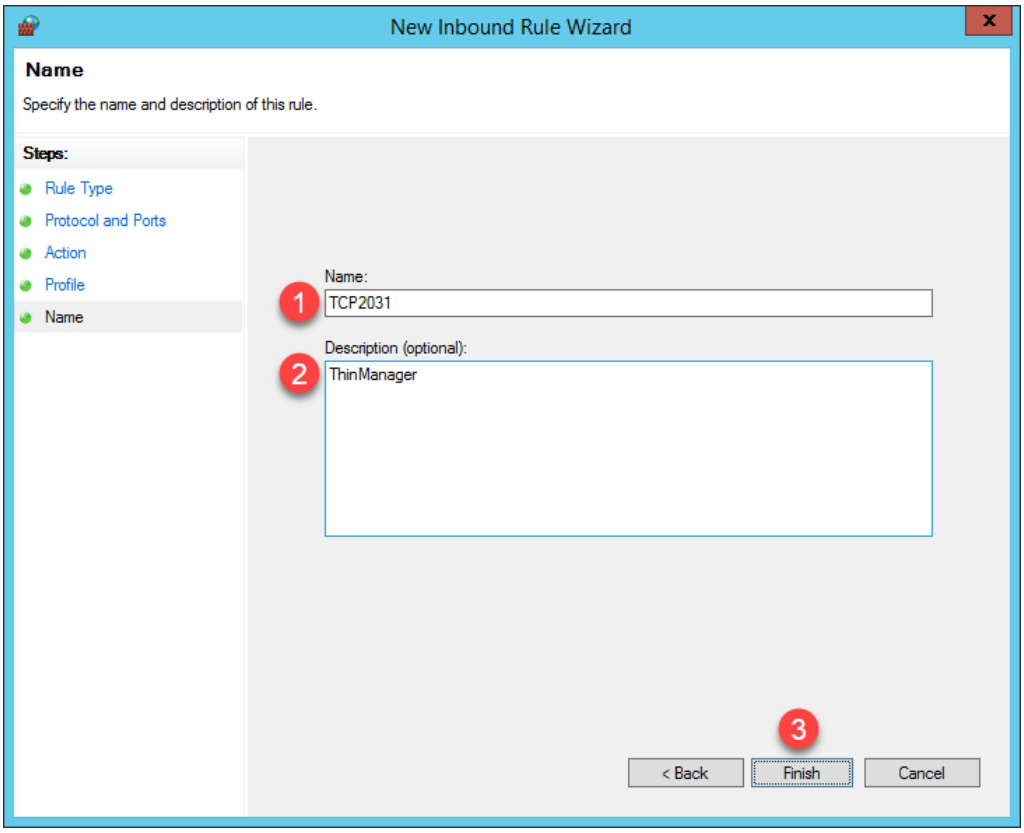
5. From the **Action** panel of the **New Inbound Rule Wizard**, select the **Allow the connection** radio button and click the **Next** button.



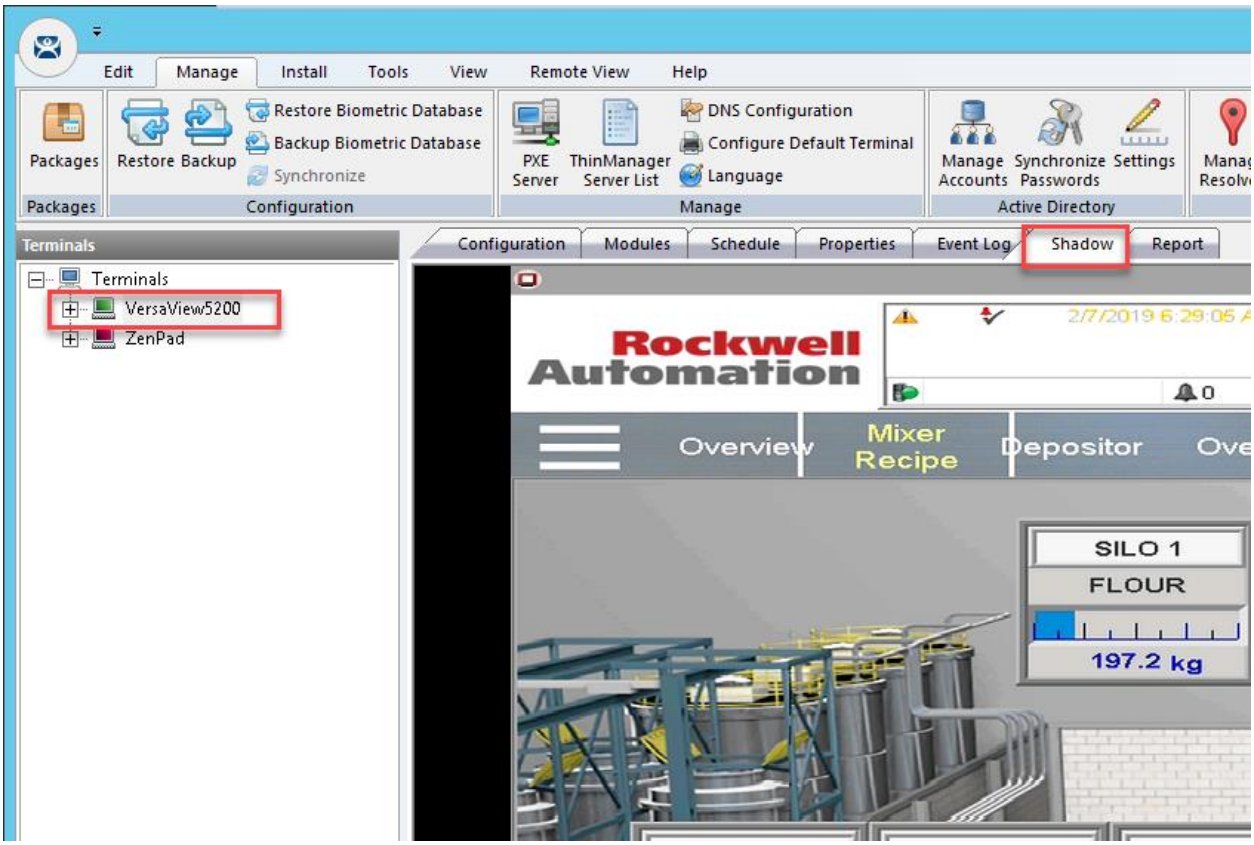
6. From the **Profile** panel of the **New Inbound Rule Wizard**, check the **Domain** checkbox and **un**-check the **Private** and **Public** checkboxes. Click the **Next** button.



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.

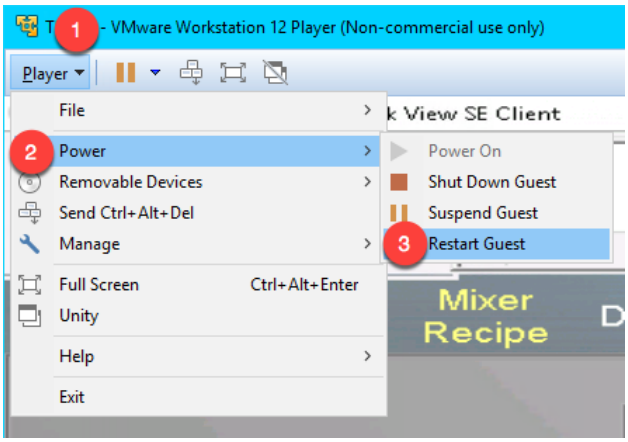


8. If you return to ThinManager, you should see the **Terminal Monitor Connection** is restored for **VersaView5200** since its icon has returned to **Green**. Terminal shadowing should be restored as well.

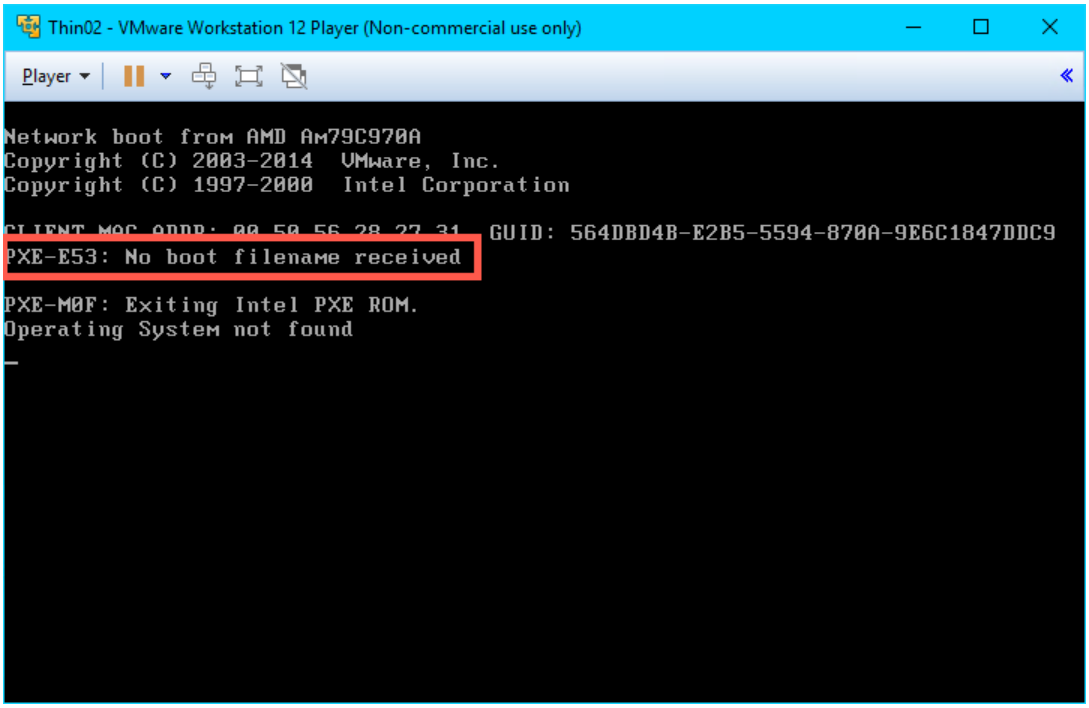


Terminal **shadowing** actually uses **TCP5900** for communication. This **outbound port** on **RDS1** was already enabled, but the **Terminal Monitor Connection** is first required before being able to establish a **shadow**.

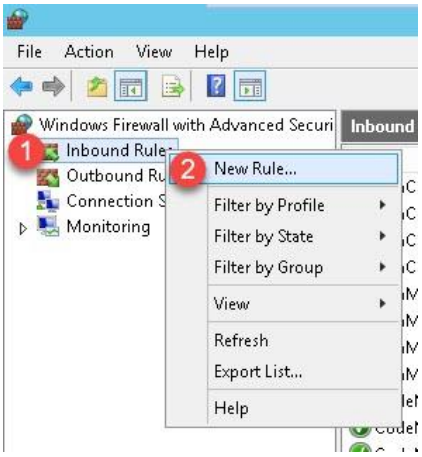
9. Switch to the virtual thin client so we can restart it and watch the boot process. Click the **Player** drop down, followed by the **Power** menu item then the **Restart Guest** item. Click the **Yes** button to the confirmation dialog box.



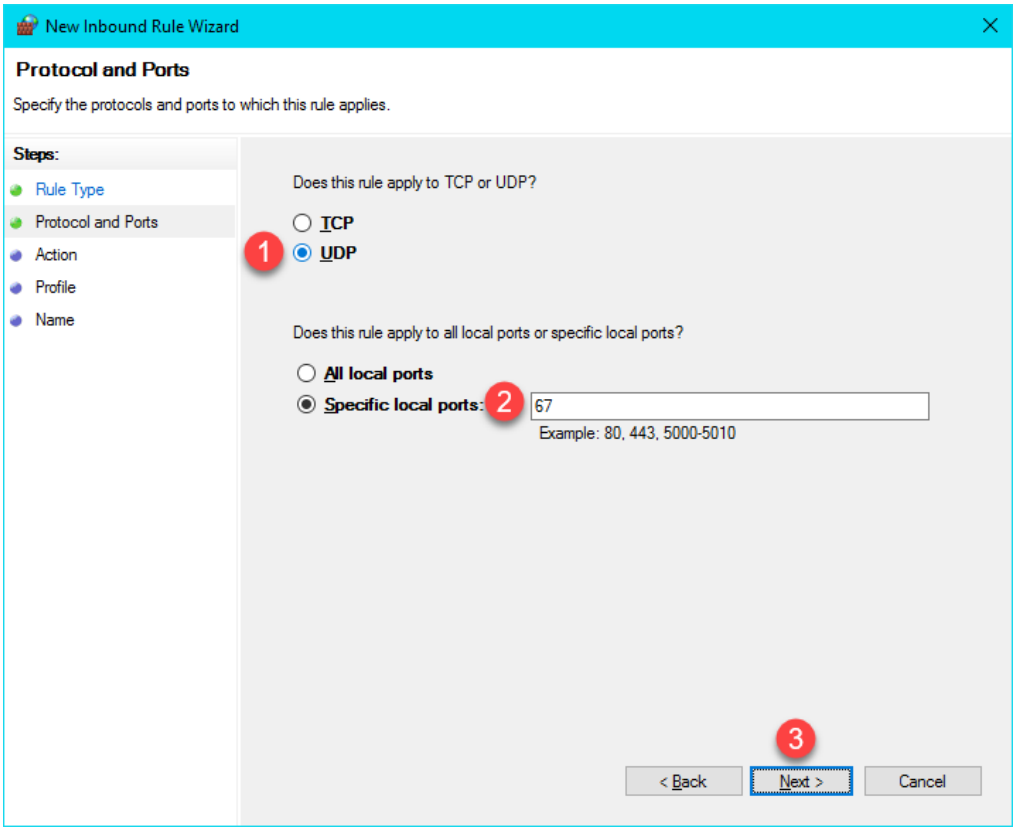
10. After a few seconds of attempting to acquire a **DHCP** address, the **PXE** boot process will timeout. Recall we configured **ThinManager** to use a Standard DHCP Server. Since **VMWare Player** is configured for **NAT**, it will issue the IP address. The error indicates that it probably received 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.



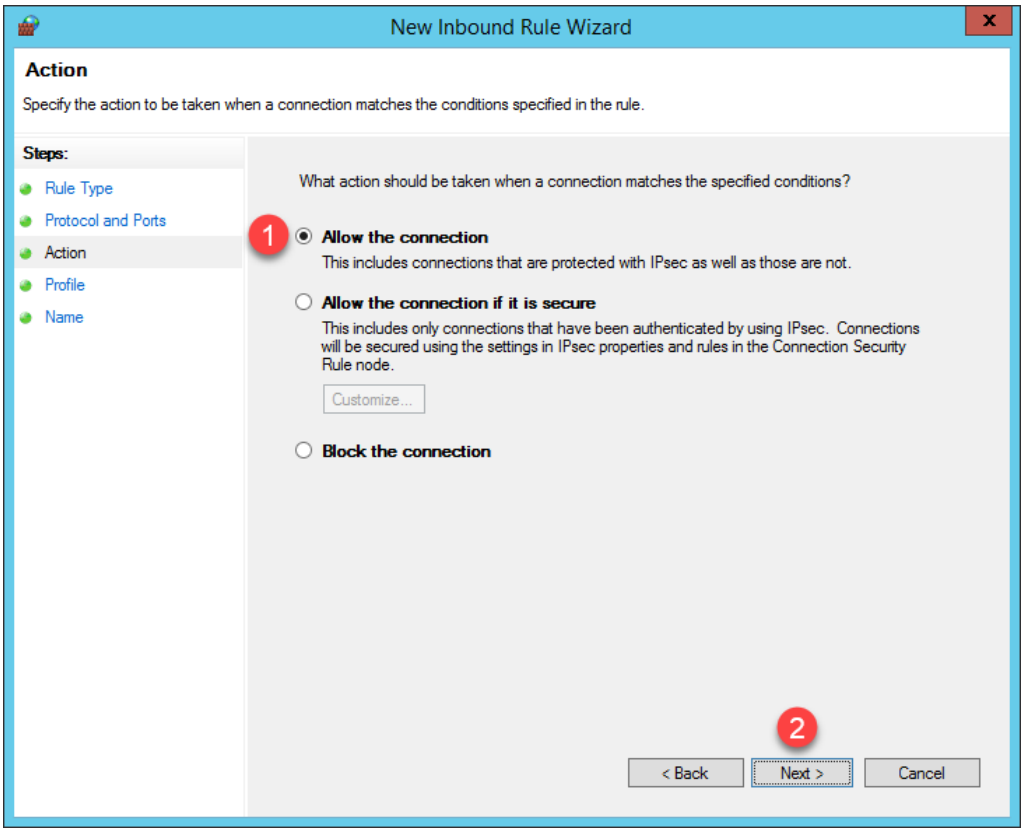
11. While we have addressed the **Terminal Monitor Connection** issue, the virtual thin client will still be unable to boot from **RDS1** with the current **Firewall** configuration. To address this, return to the **Windows Firewall and Advanced Security** window, right click the **Inbound Rules** tree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



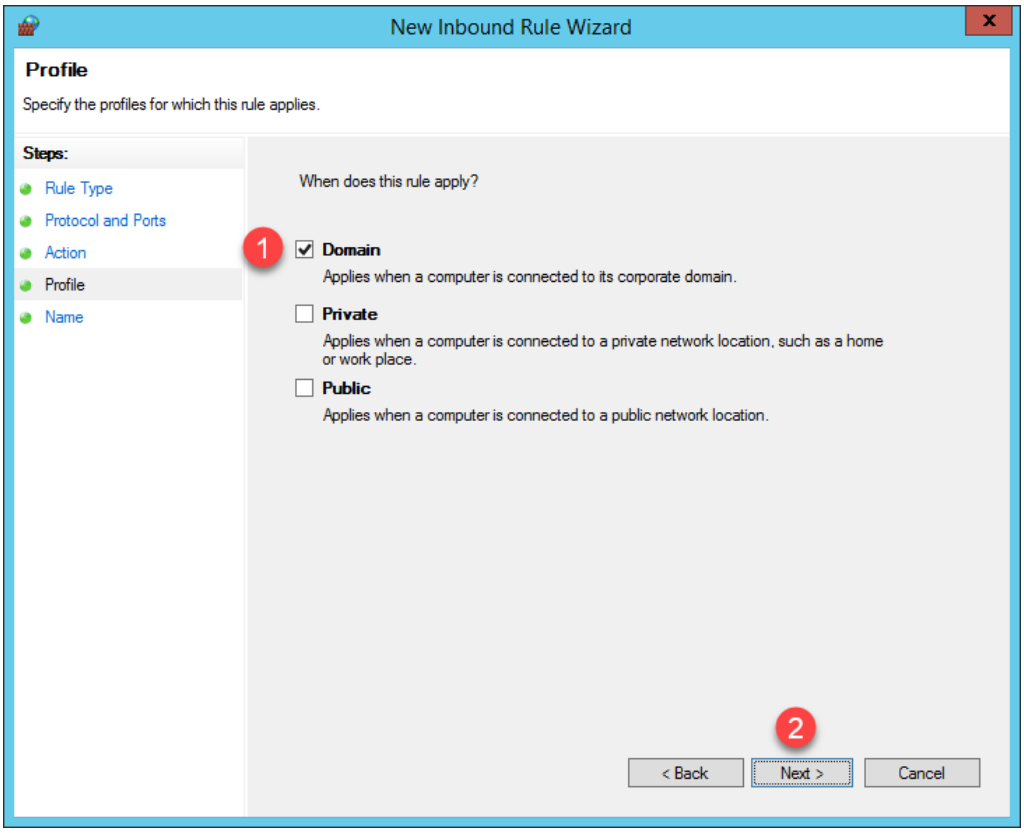
12. From the **Protocol and Ports** panel of the **New Inbound Rule Wizard**, select the **UDP** radio button and enter *67* in the **Specified local ports** field. Click the **Next** button.



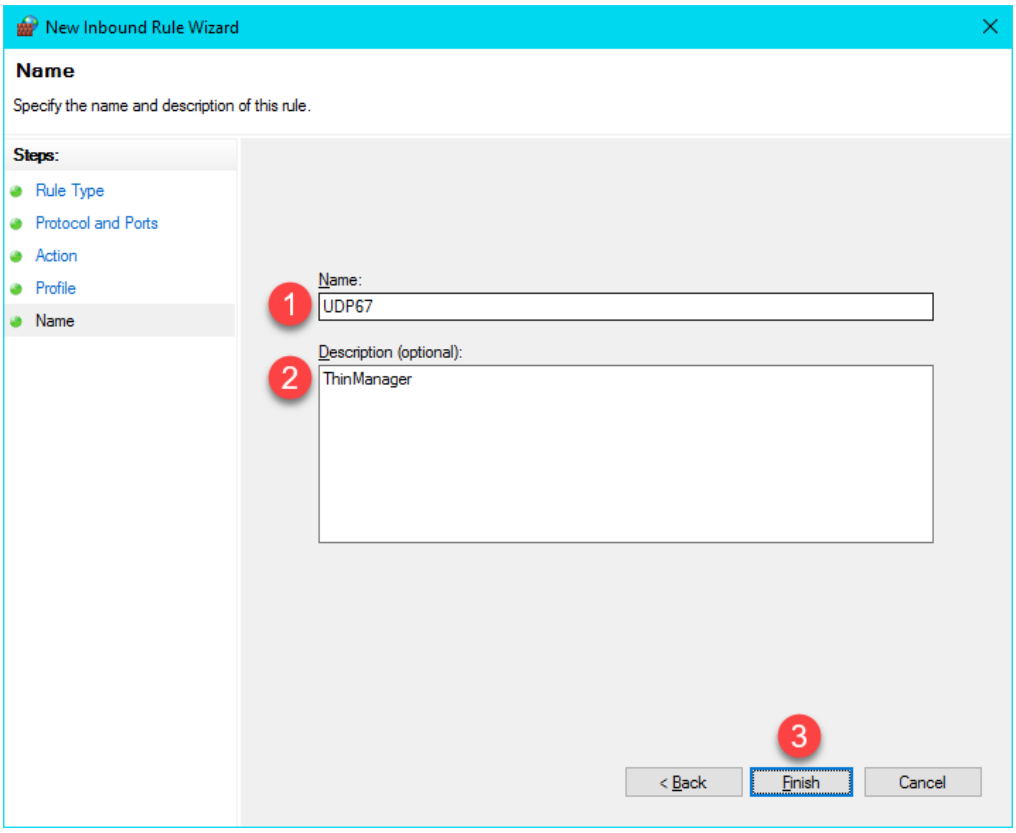
13. From the **Action** panel of the **New Inbound Rule Wizard**, select the **Allow the connection** radio button and click the **Next** button.



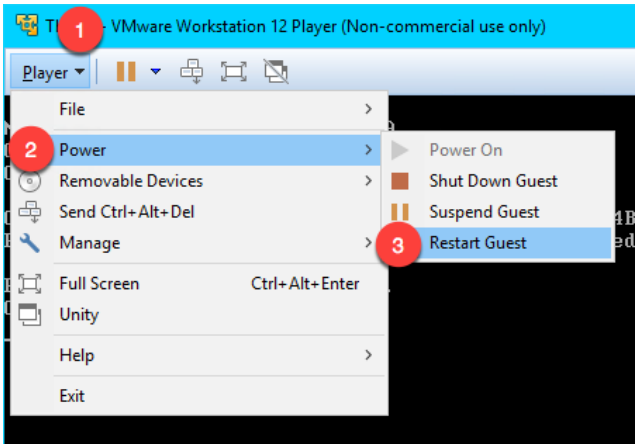
14. From the **Profile** panel of the **New Inbound Rule Wizard**, check the **Domain** checkbox and **un**-check the **Private** and **Public** checkboxes. Click the **Next** button.



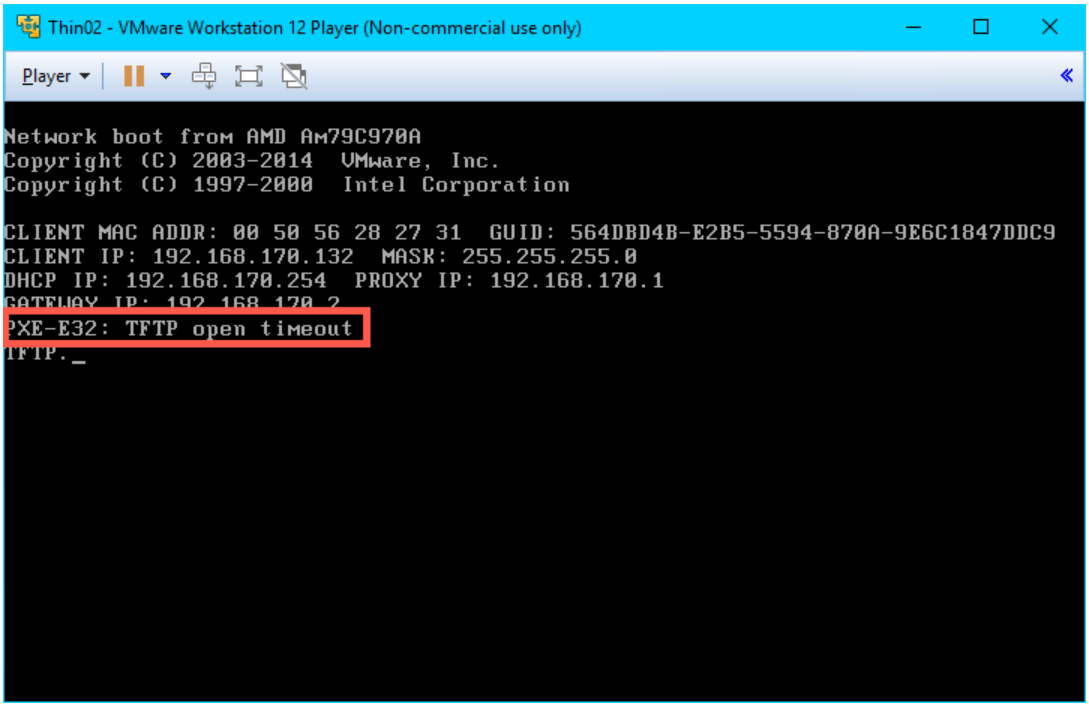
15. From the **Name** panel of the **New Inbound Rule Wizard**, enter *UDP67* as the **Name** and *ThinManager* as the **Description**. Click the **Finish** button. Leave the **Windows Firewall with Advanced Security** window open.



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.

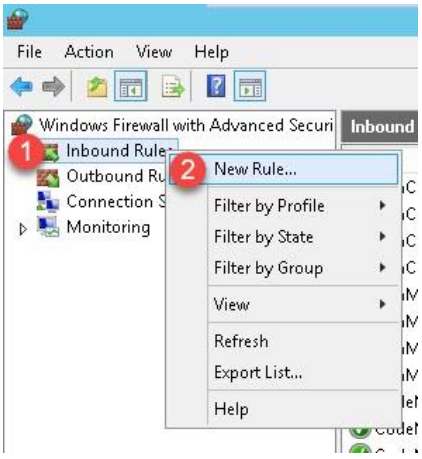


17. This time, the virtual thin client receives an IP address, but now it appears to timeout during the **TFTP** stage of the boot process. Once again, this is due to our firewall blocking this traffic.

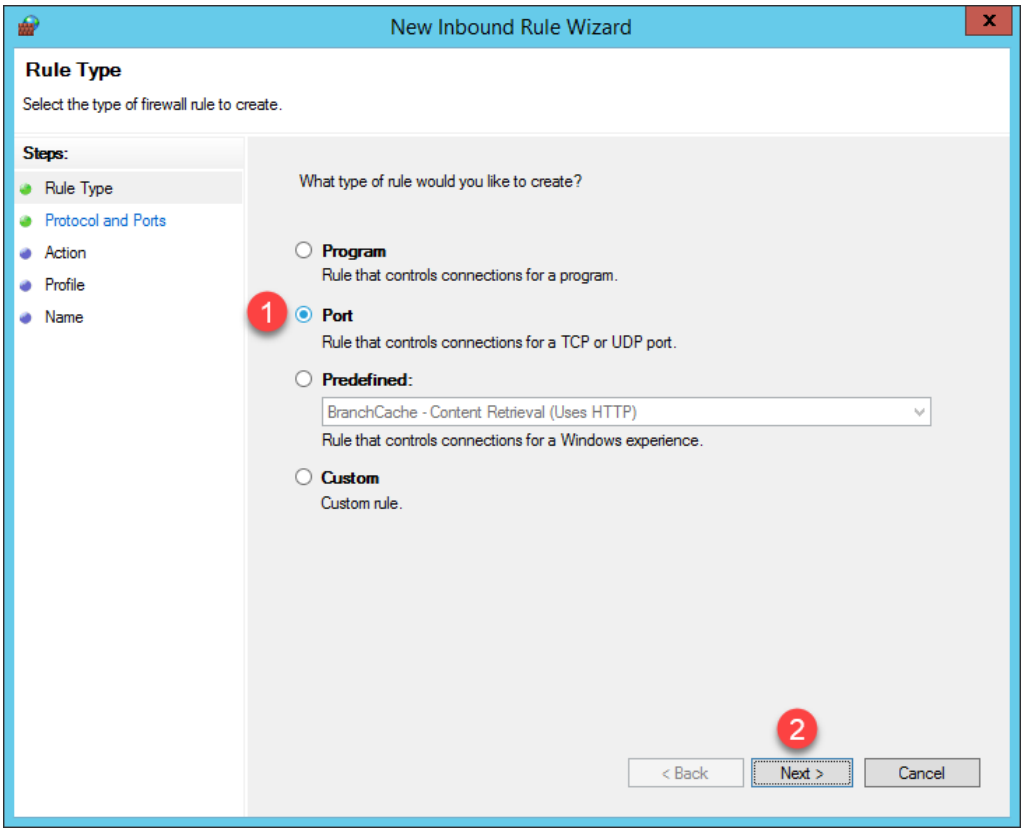


> Your IP addresses will most likely be different. The 192.168.x.y subnet is being issued by **VMWare Player** since the virtual thin client is configured for **NAT**.

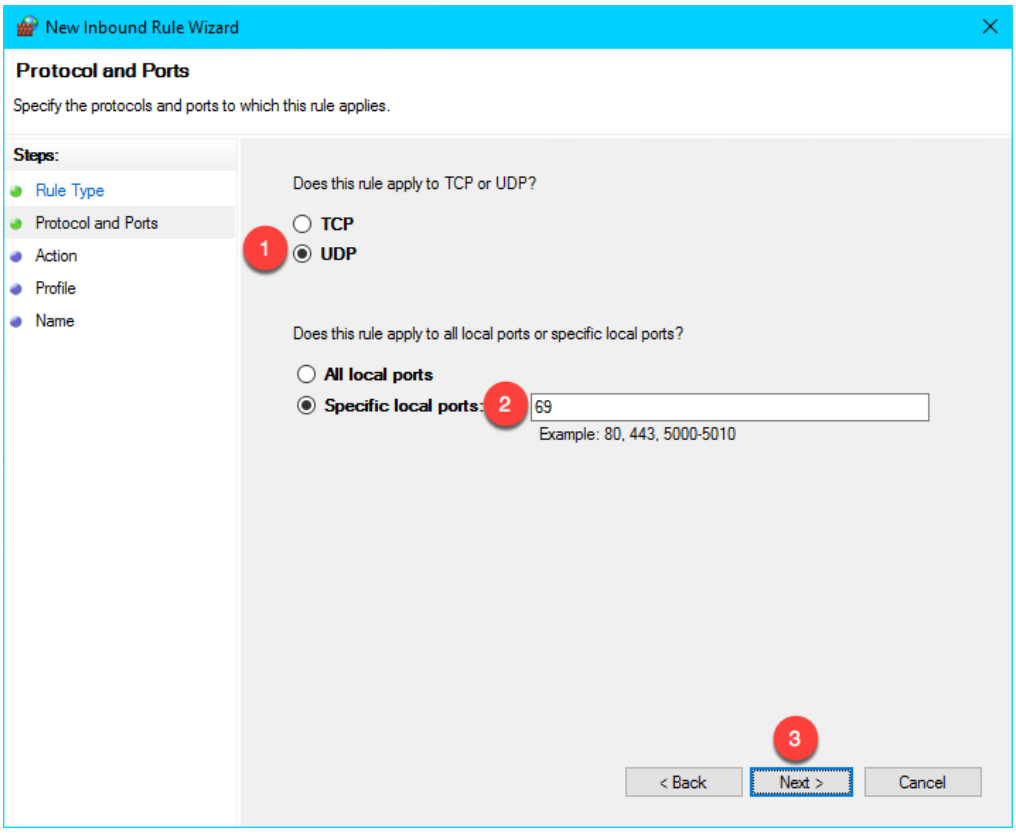
18. To address this, return to the **Windows Firewall and Advanced Security** window, right click the **Inbound Rules** tree item and select **New Rule..**



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

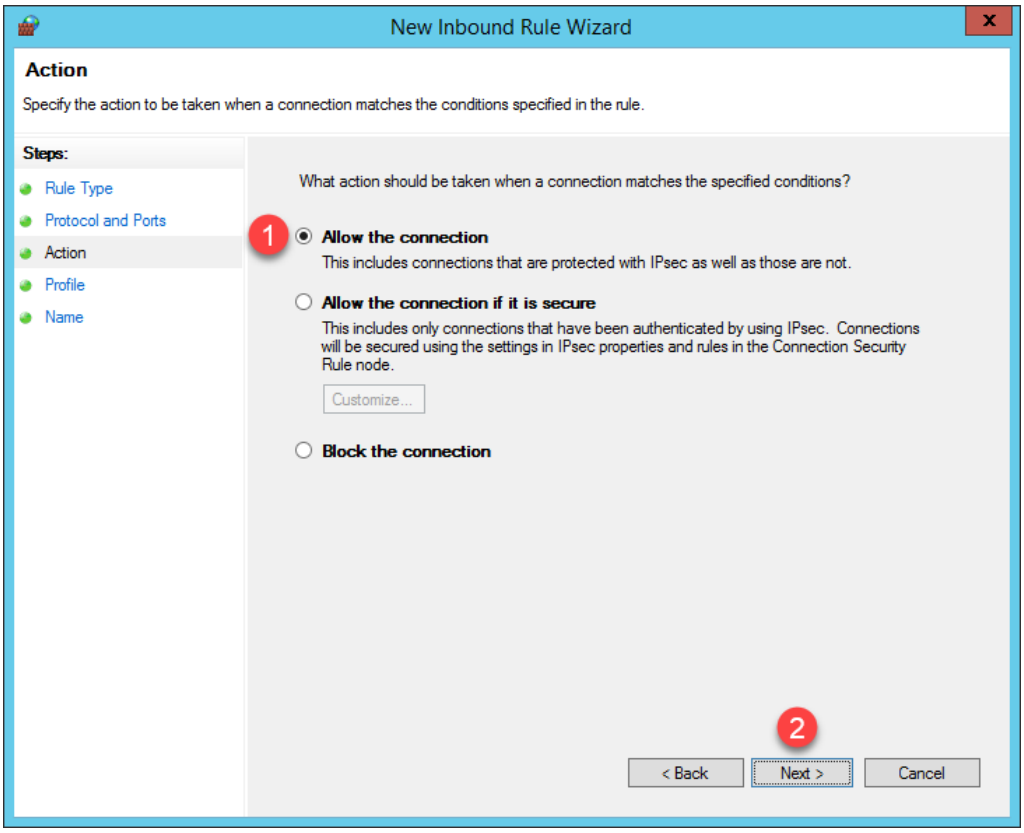


20. From the **Protocol and Ports** panel of the **New Inbound Rule Wizard**, select the **UDP** radio button and enter *69* in the **Specified local ports** field. Click the **Next** button.

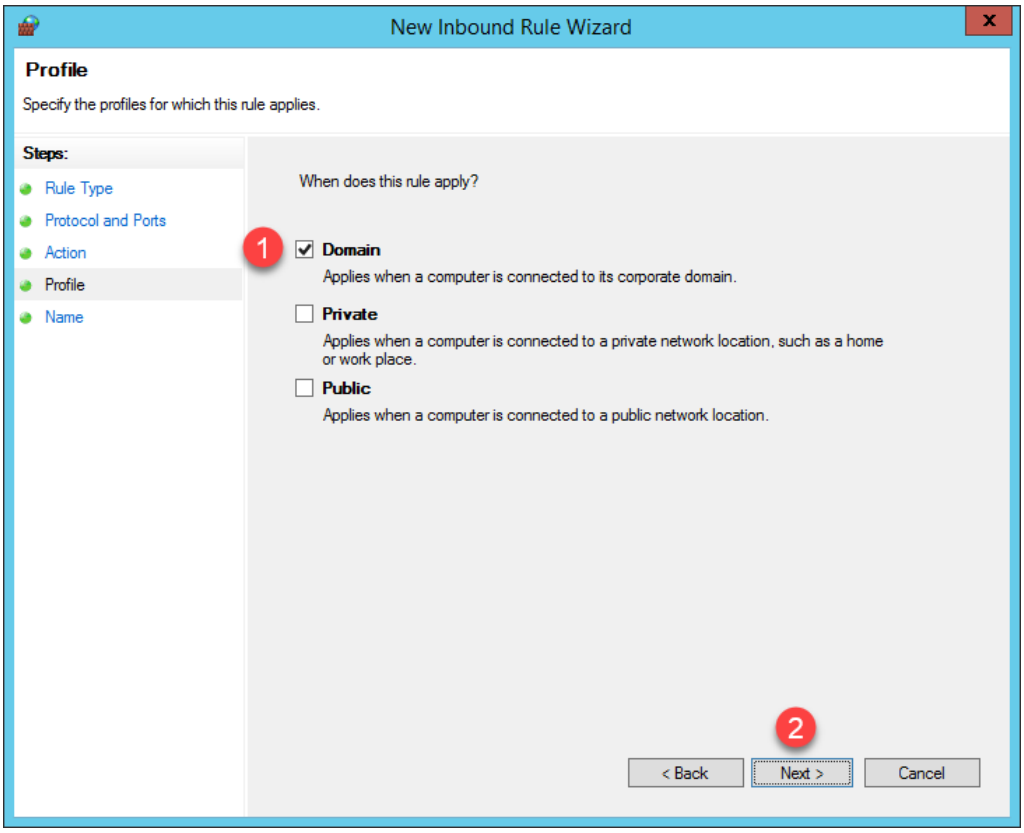


UDP Port 69 is required by ThinManager to transfer the **firmware** to **ThinManager Compatible** terminals (PXE), like the virtual thin client(s) in this Cloud lab. This transfer is accomplished using **Trivial File Transfer Protocol** (**TFTP**). **ThinManager Readey** terminals, which have the **ThinManager 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**.

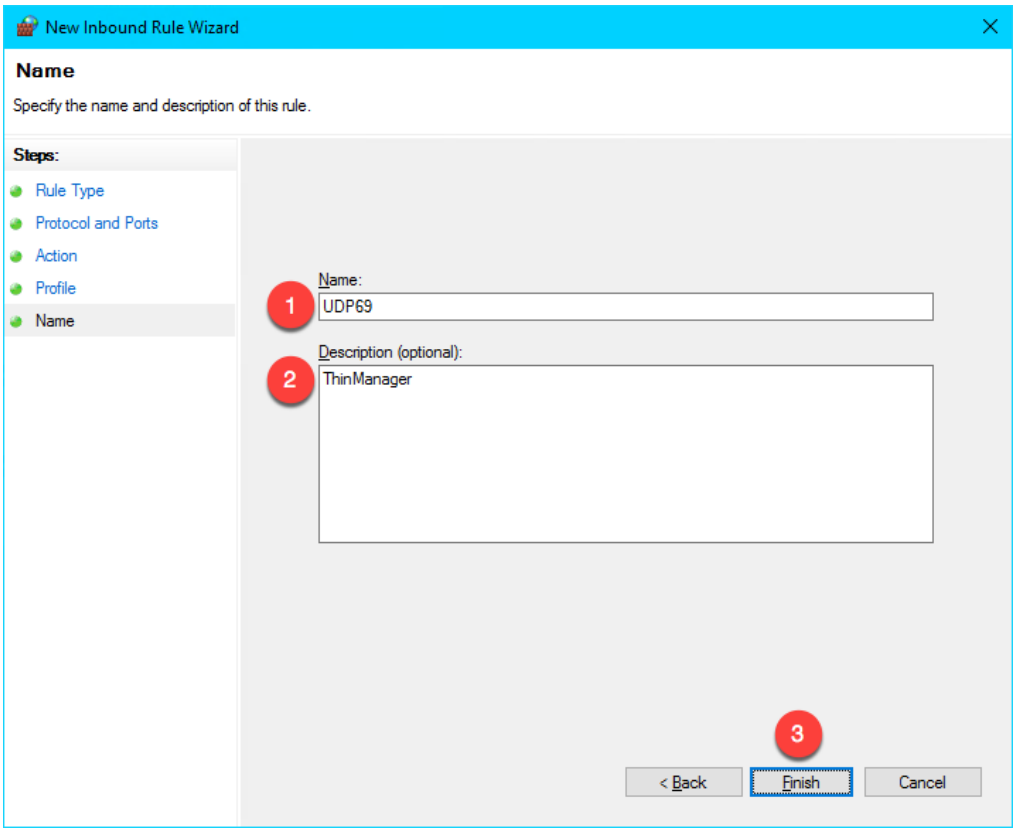
21. From the **Action** panel of the **New Inbound Rule Wizard**, select the **Allow the connection** radio button and click the **Next** button.



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.

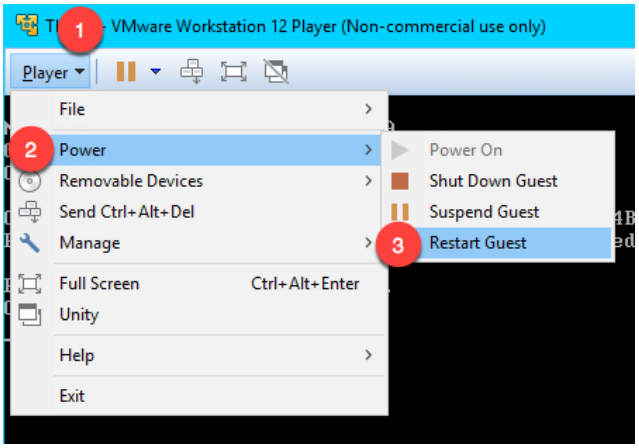


23. From the **Name** panel of the **New Inbound Rule Wizard**, enter *UDP69* as the **Name** and *ThinManager* as the **Description**. Click the **Finish** button.

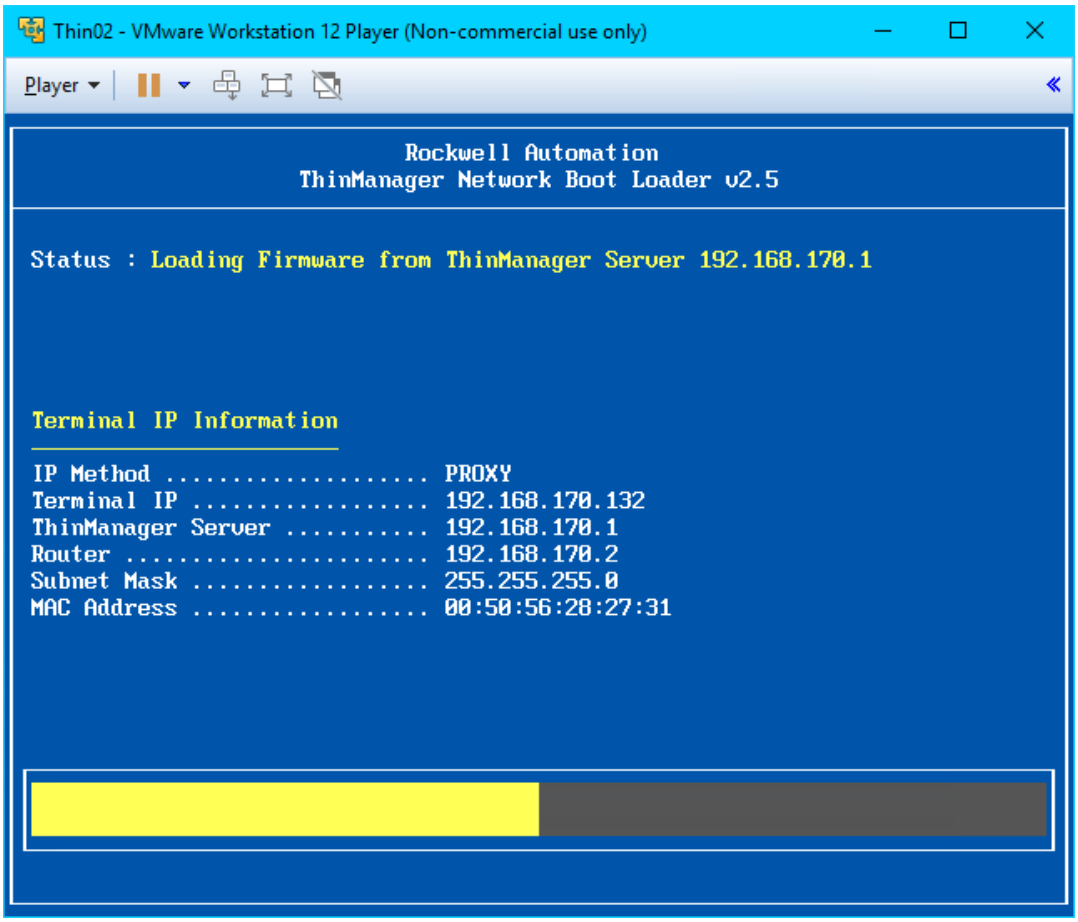


24. Close the **Windows Firewall with Advanced Security** window and the **Control Panel**.

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.

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

Section 5: 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.

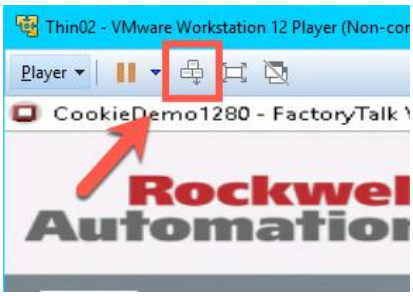
In this section, you will be performing the following tasks:

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

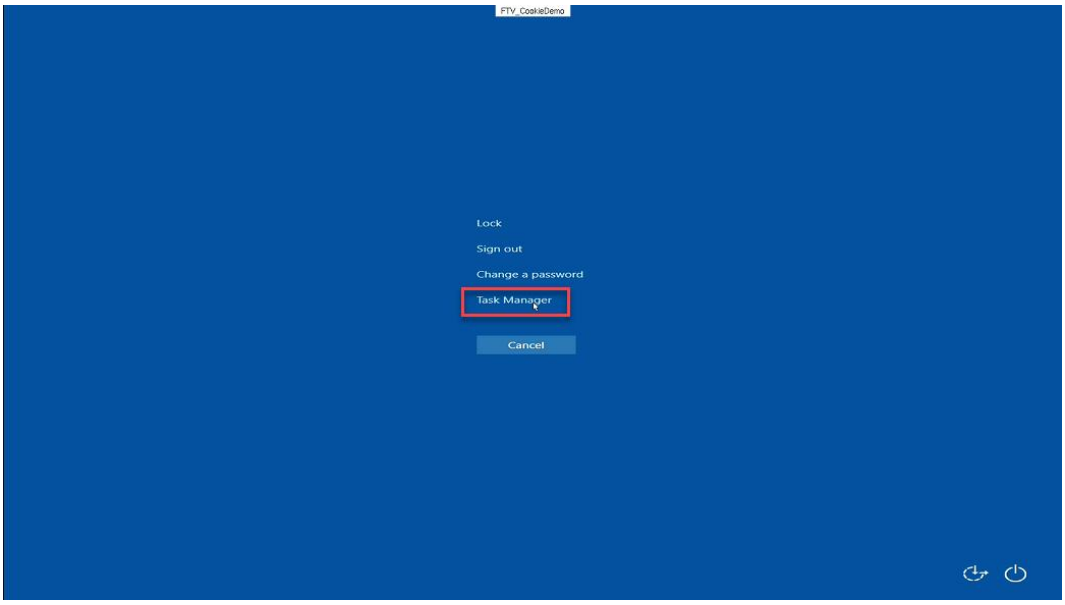
Key Block Module

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

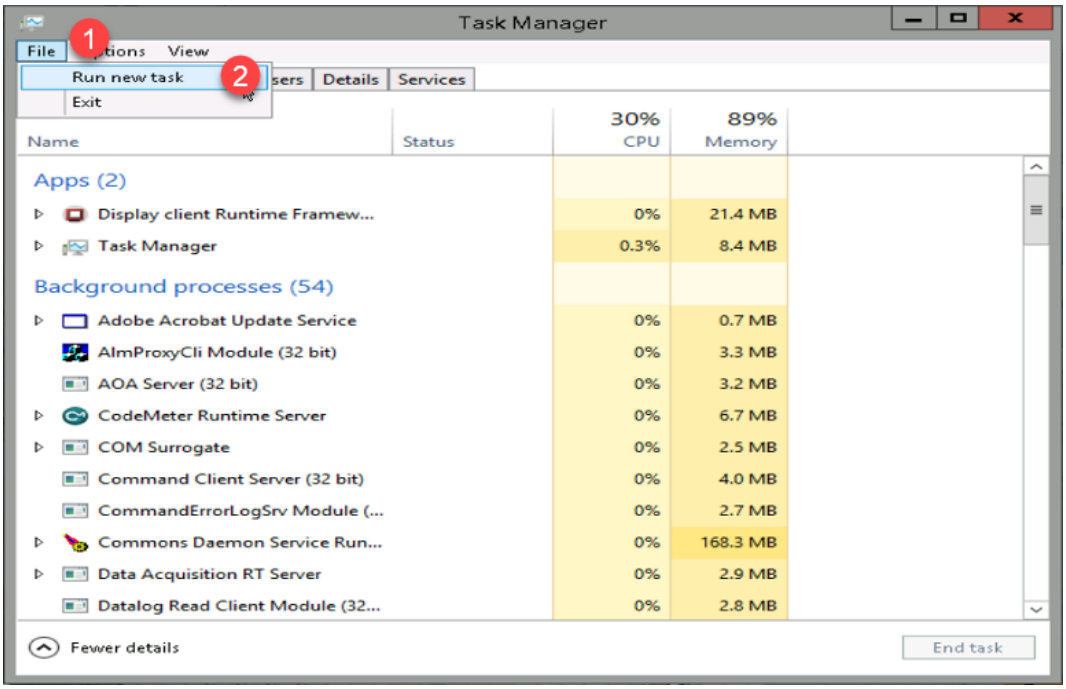
1. From the virtual thin client hit the **CTRL-ALT-DEL** icon in the toolbar to send that key sequence to the virtual thin client.



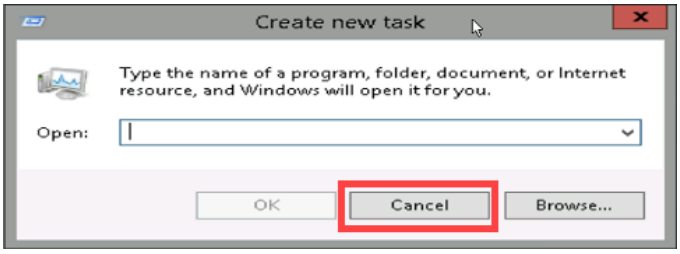
2. Notice this results in the ability to **Lock**, **Sign out**, **Change a password** or even access **Task Manager**! Click the **Task Manager** link.



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.

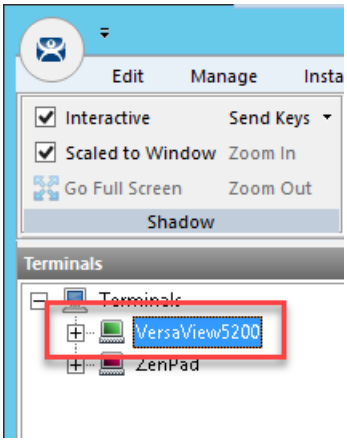


4. At this point, we have effectively defeated the intent of using **Application Link** (eliminating access to other elements within the **Windows Desktop**) in ThinManager, as the user could launch any application they wish – on the **Remote Desktop Server** no less! Click the **Cancel** button and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



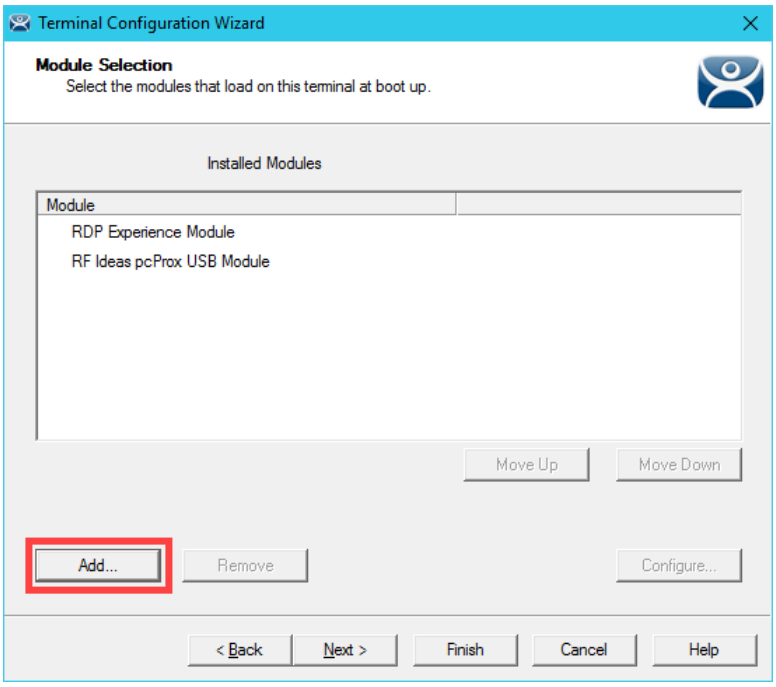
5. Return to the **ThinManager Admin Console**. Click the **Terminals** tree selector icon.

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

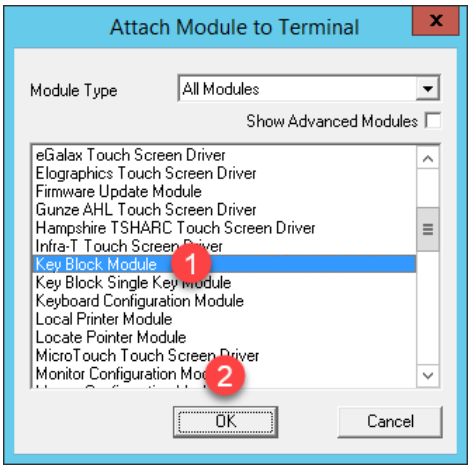


7. Click the **Next** button on the **Terminal Name** page of the wizard.
8. Click the **Next** button on the **Terminal Hardware** page of the wizard.
9. Click the **Next** button on the **Terminal Options** page of the wizard.
10. Click the **Next** button on the **Terminal Mode Selection** page of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

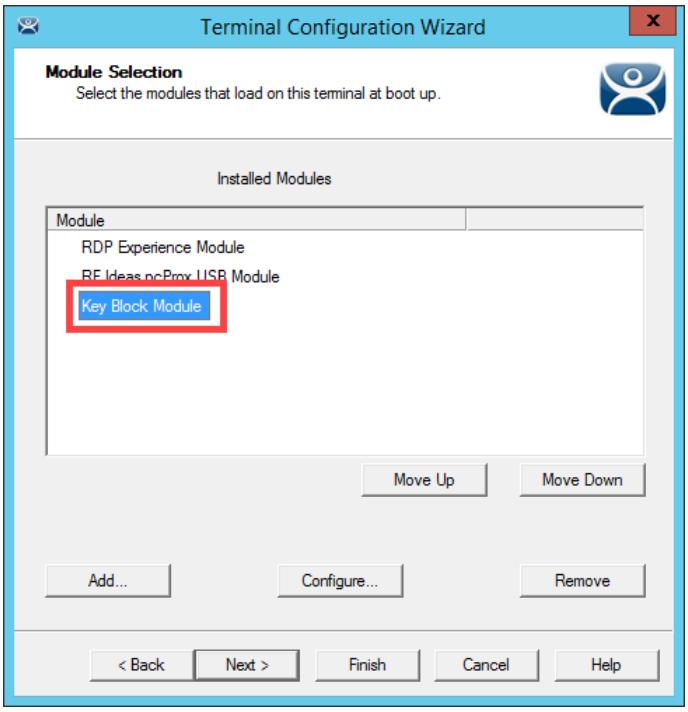


17. Scroll down and select the **Key Block Module**. Click the **OK** button.

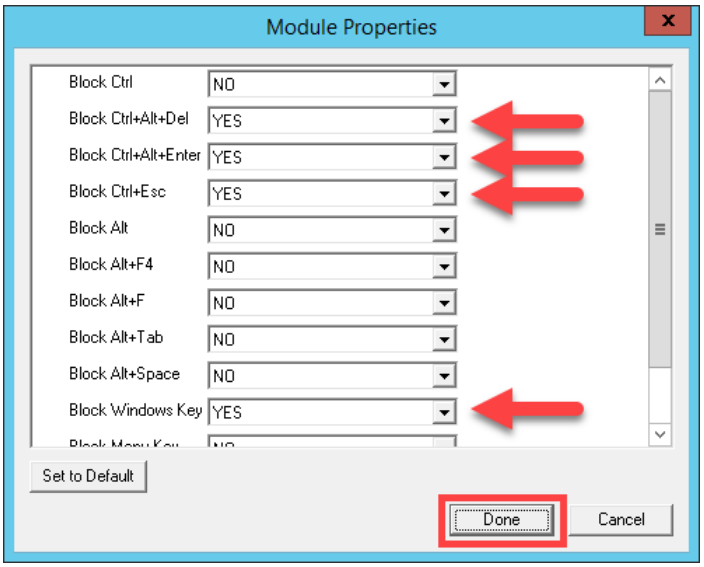


You may notice the **Key Block Single Key Module** and the **Keyboard Configuration Module** as well. The **Key Block Single Key Module** allows you to block specific keys, like CTRL-B, or any other combination, like ALT-S. The **Keyboard Configuration Module** provides the ability to set the initial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

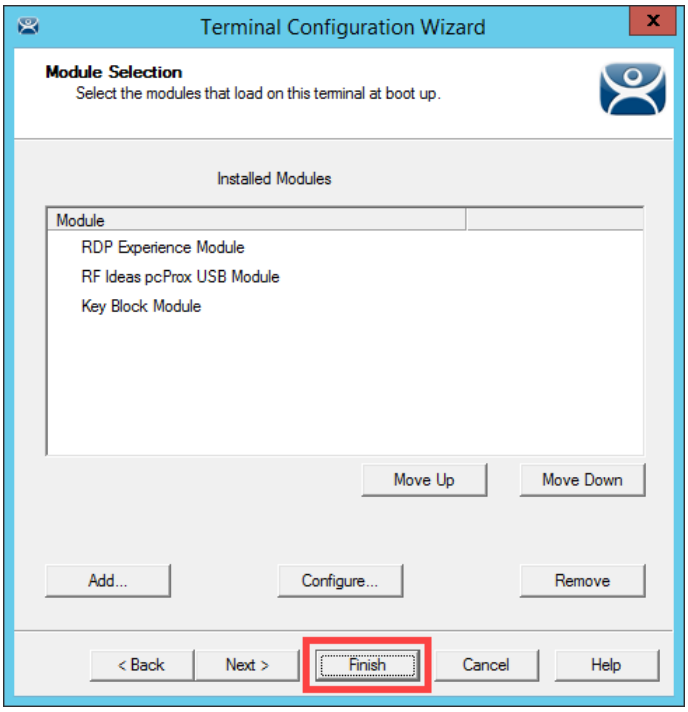
18. Double click the **Key Block Module** item in the **Installed Modules** list to configure it.



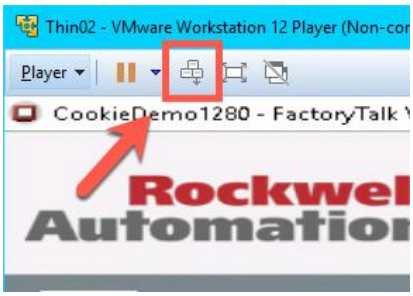
19. Notice the default **Block** settings. Accept the defaults and click the **Done** button.



20. Click the **Finish** button.



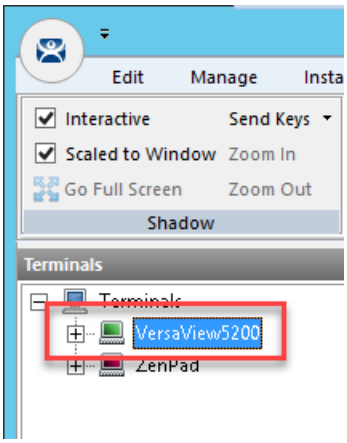
21. Right click the **VersaView5200** terminal and select the **Restart Terminal** item. Click the **Yes** button to confirm.
22. Return to the virtual thin client and click the **CTRL-ALT-DEL** icon from the toolbar again to verify it is now blocked.



Locate Pointer Module

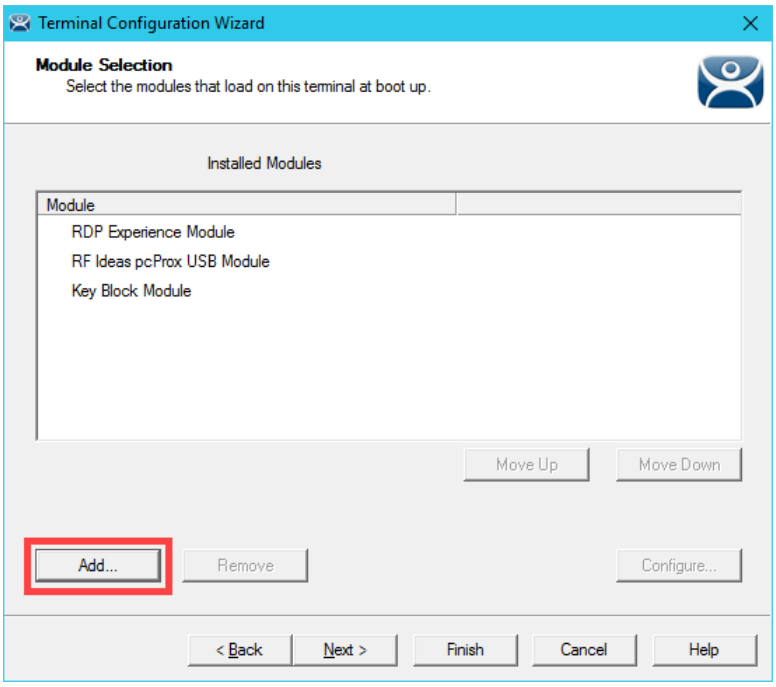
The Locate Pointer Module is very useful on high resolution screens and/or with MultiMonitor deployments.

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

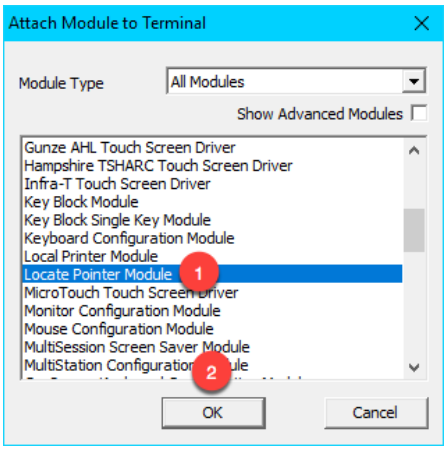


2. Click the **Next** button on the **Terminal Name** page of the wizard.
3. Click the **Next** button on the **Terminal Hardware** page of the wizard.
4. Click the **Next** button on the **Terminal Options** page of the wizard.
5. Click the **Next** button on the **Terminal Mode Selection** page of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

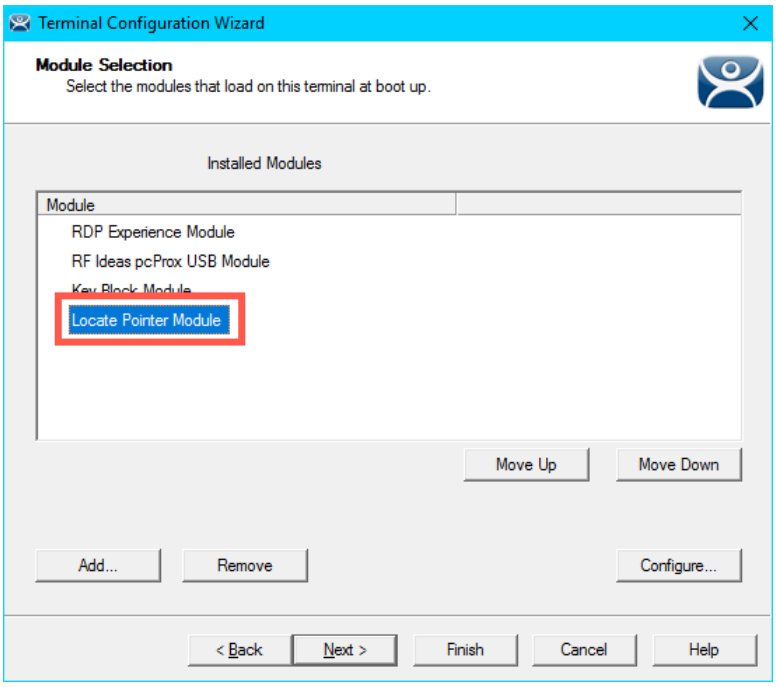
11. Click the **Add…** button on the **Module Selection** page of the wizard.



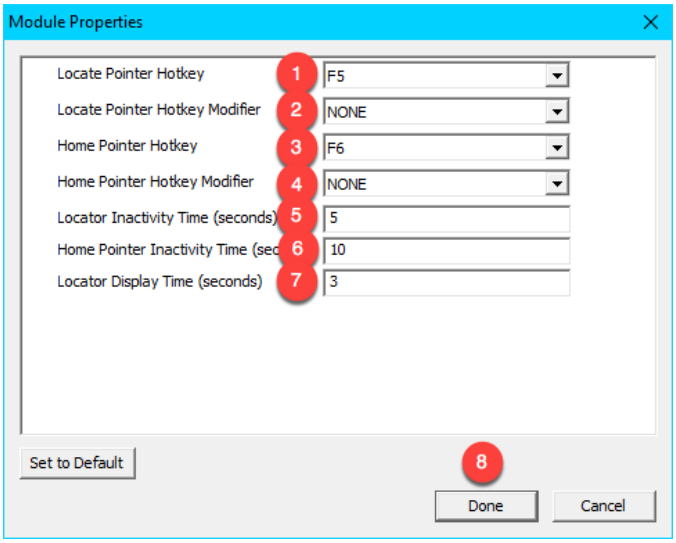
12. Scroll down and select the **Locate Pointer Module**. Click the **OK** button.



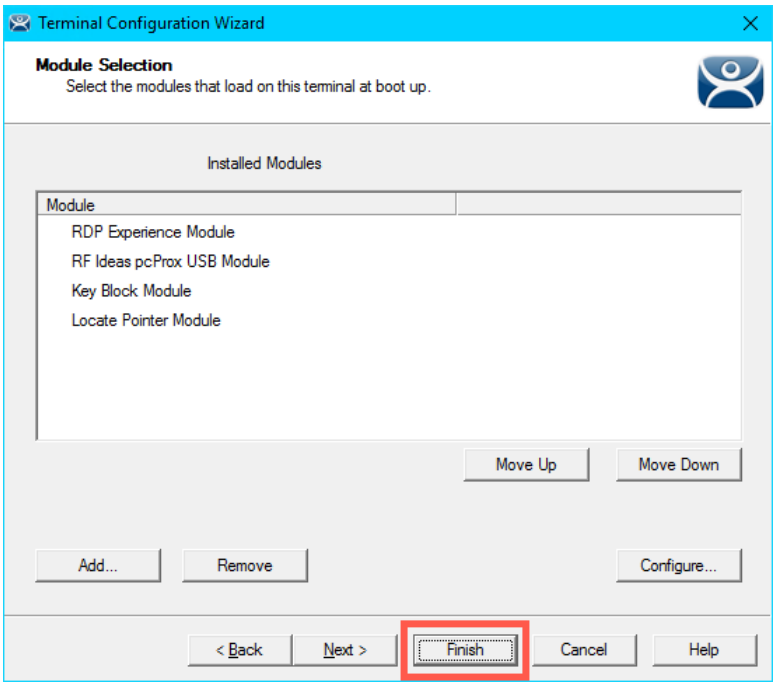
13. Back at the **Module Selection** page of the wizard, double click the **Locate Pointer Module**.



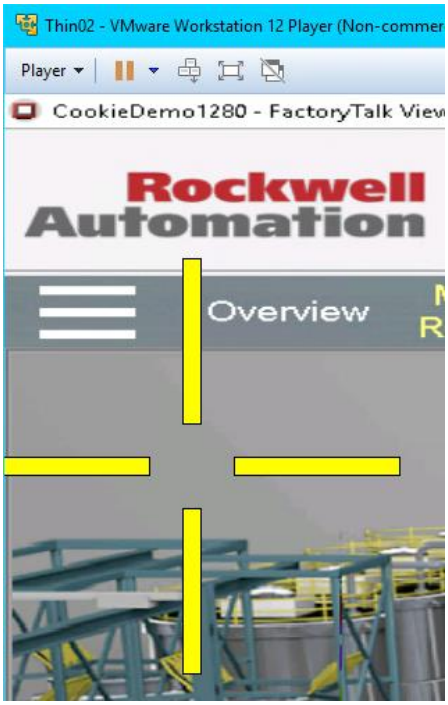
14. From the **Module Properties** page of the wizard, match the settings in the screen shot below and click the **Done** button.



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



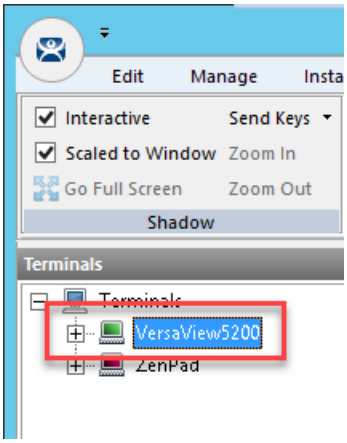
16. Right click the **VersaView5200** terminal and select the **Restart Terminal** item. Click the **Yes** button to confirm.
17. Return to the virtual thin client, click in an open area of the screen to ensure the focus is there, then hit the *F5* key on your keyboard. You should see a large crosshair 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

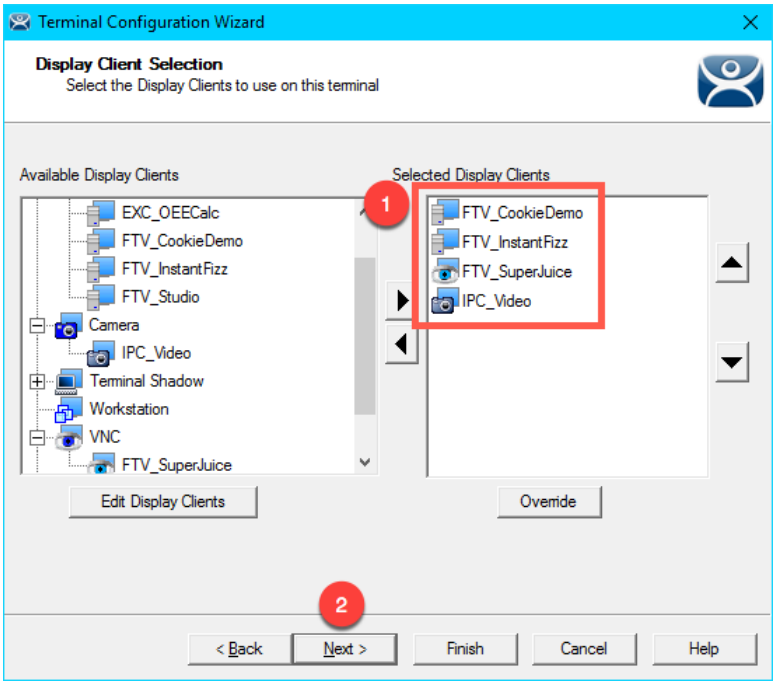
If you recall from Section 7 , **MultiSession** is the term used to define when we deliver more than one **Display Client** to a **Terminal**. We used **Tiling Mode** and **Virtual Screens** to demonstrate the **Visualization** options for **MultiSession**. The **MultiSession Screen Saver Module** operates 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.



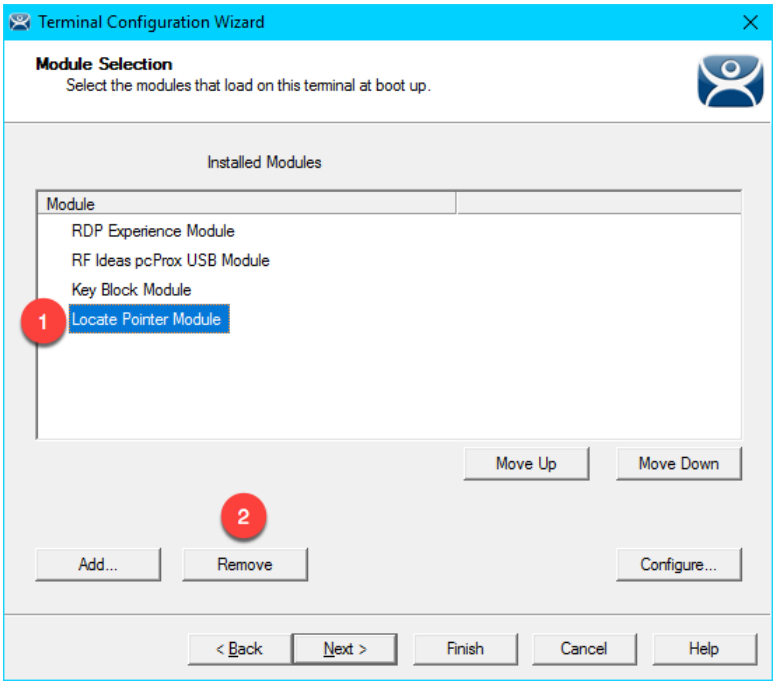
2. Click the **Next** button on the **Terminal Name** page of the wizard.
3. Click the **Next** button on the **Terminal Hardware** page of the wizard.
4. Click the **Next** button on the **Terminal Options** page of the wizard.
5. Click the **Next** button on the **Terminal Mode Selection** page of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

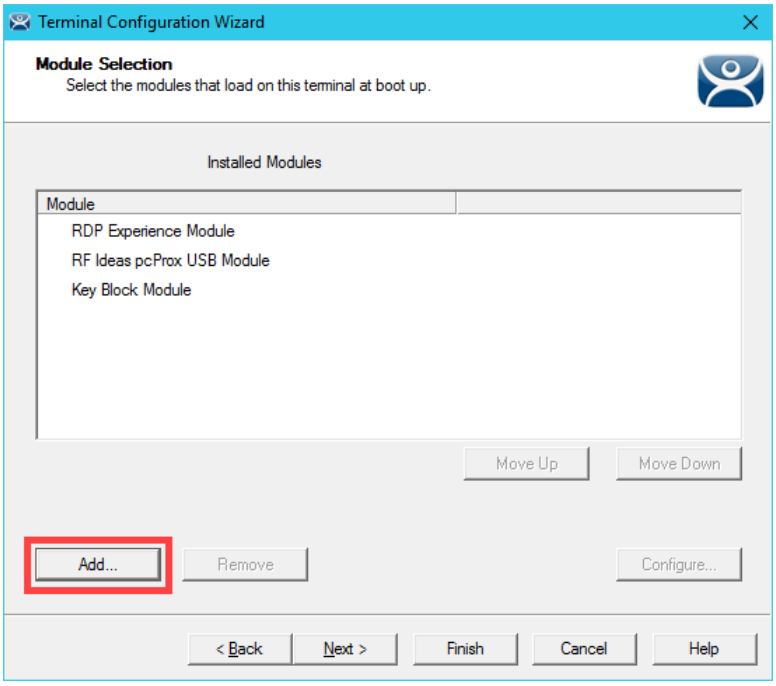


7. Click the **Next** button on the **Terminal Interface Options** page of the wizard.
8. Click the **Next** button on the **Hotkey Configuration** page of the wizard.
9. Click the **Next** button on the **Log In Information** page of the wizard.
10. Click the **Next** button on the **Video Resolution**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

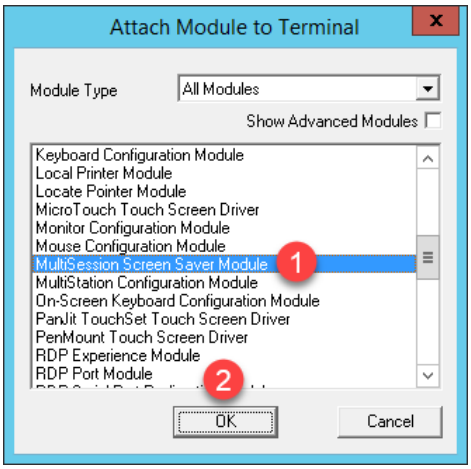
11. Let's remove the **Locate Pointer Module** by selecting it and then clicking the **Remove** button.



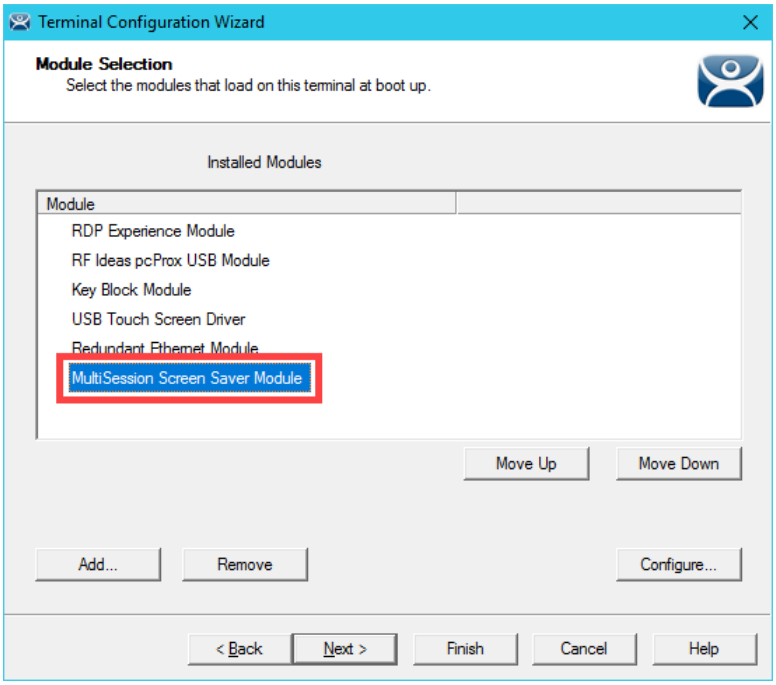
12. Click the **Add…** button on the **Module Selection** page of the wizard.



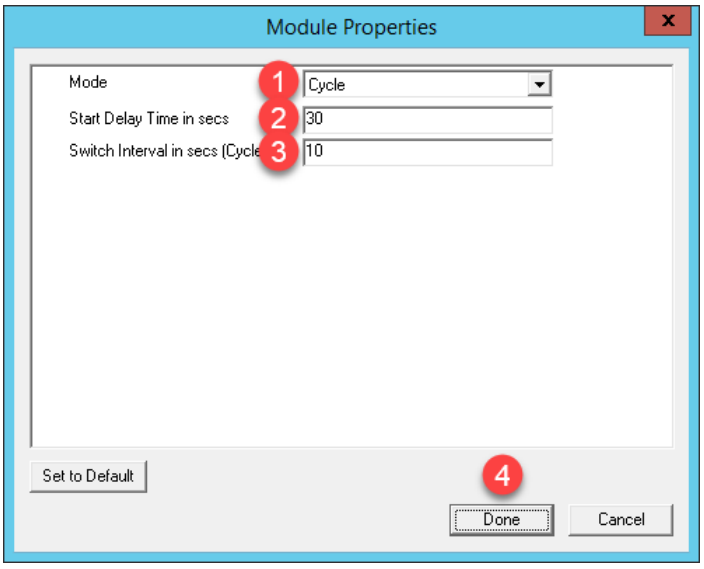
13. From the **Attach Module to Terminal** window, select the **MultiSession Screen Saver Module** and click the **OK** button.



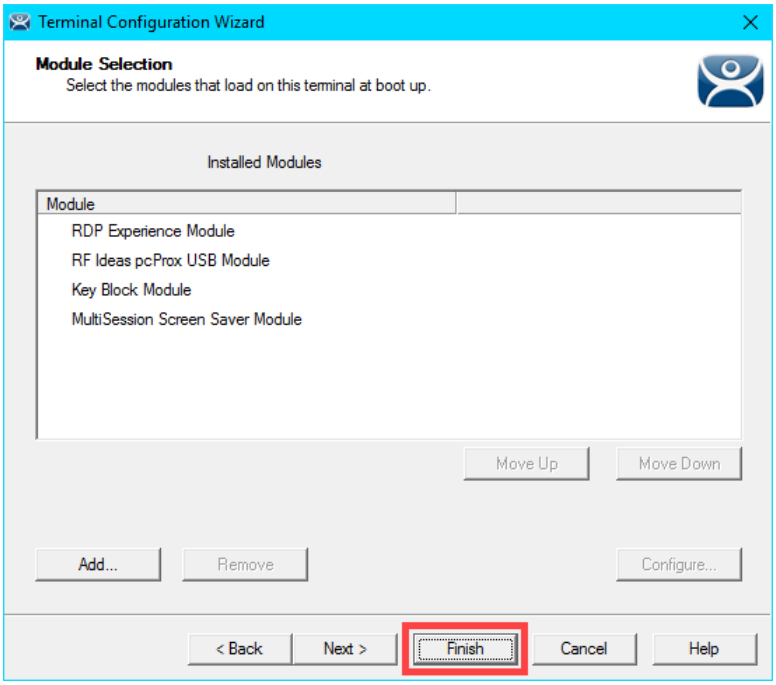
14. Double click the **MultiSession Screen Saver Module** from the **Installed Modules** list.



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.

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 6: 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:

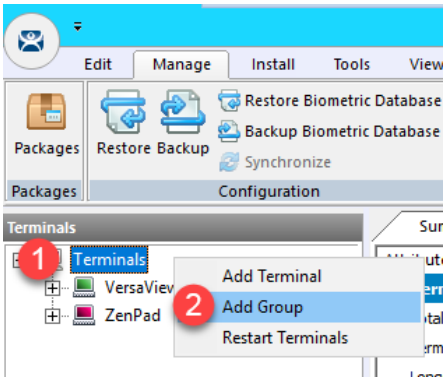
1. Terminal Groups
2. Overrides
3. Schedules
4. Mouse Button Mapping
5. Remove Override and Mouse Button Mapping

Terminal Groups

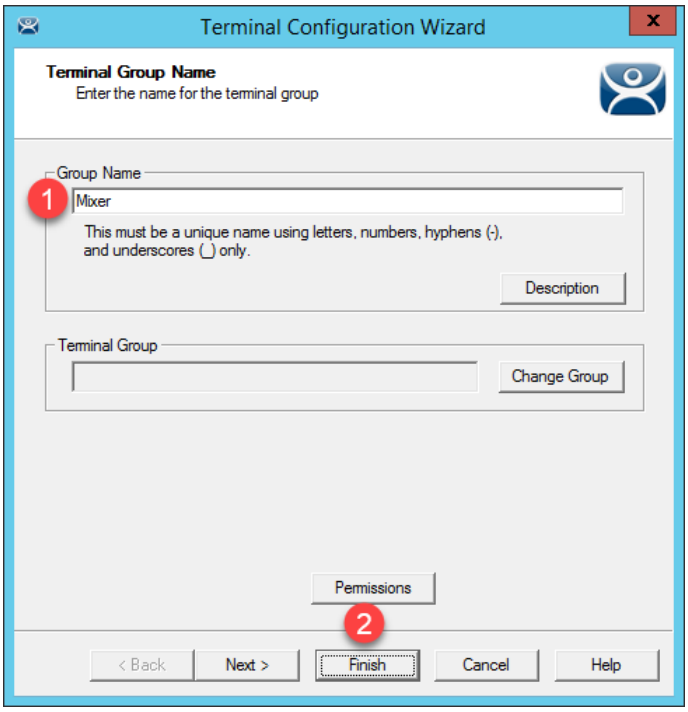
Terminal Groups provide 2 key capabilities: (1) terminal organization and (2) settings inheritance. With terminal organization, you can create **Terminal Groups** much like folders in Windows Explorer, and then add **Terminals** to the **Terminal Group**. The other key benefit of **Terminal Groups**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

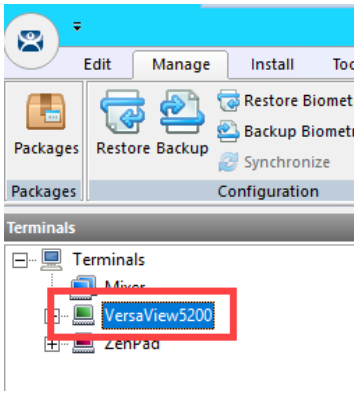
2. Right click the **Terminals** root item in the **Terminals tree** and select **Add Group**.



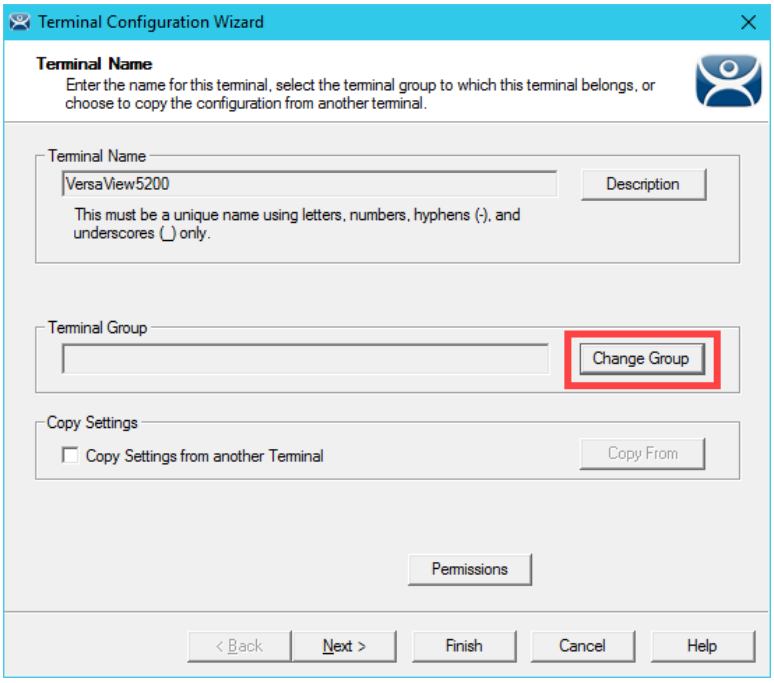
3. From the **Terminal Group Name** of the **Terminal Configuration Wizard**, enter *Mixer* as the **Group Name**. Click the **Finish** button.



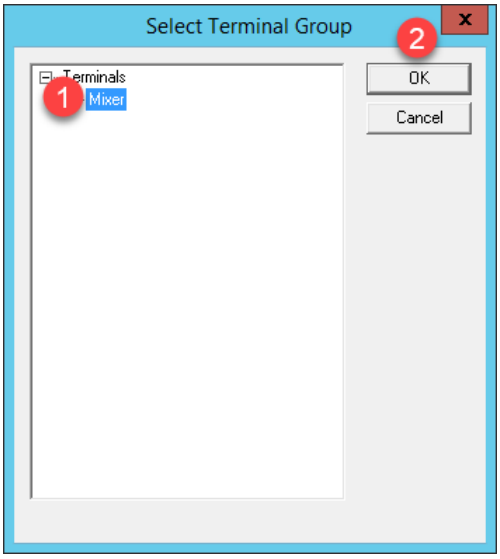
4. Double click the **VersaView5200** terminal.



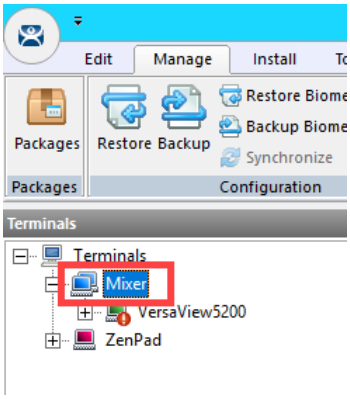
5. From the **Terminal Name** page of the **Terminal Configuration Wizard**, click the **Change Group** button.



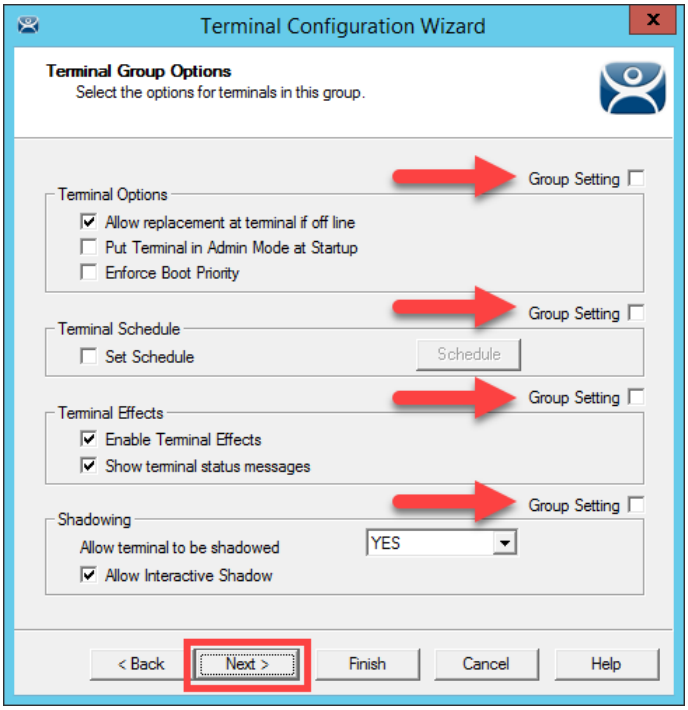
6. From the **Select Terminal Group** window, select **Mixer** and click the **OK** button.



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**.



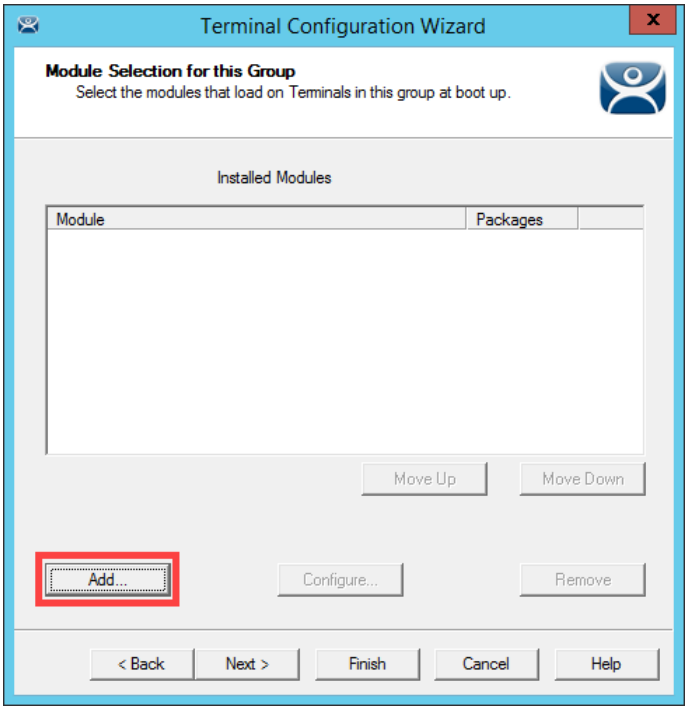
9. Click the **Next** button from the **Terminal Group Name** of the **Terminal Configuration Wizard**.
10. From the **Terminal Group Options** page of the wizard, notice the **Group Setting** checkboxes. Checking any of those checkboxes will result in that setting or group of settings to be inherited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



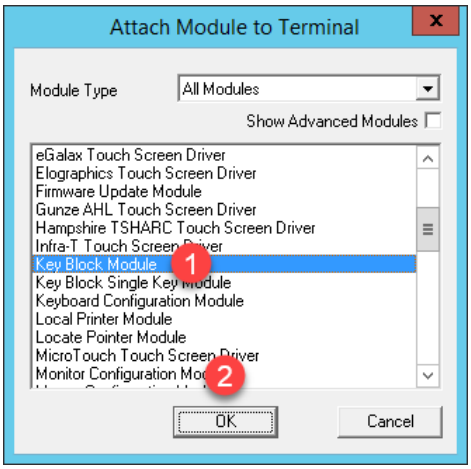
11. Click the **Next** button on the **Terminal Mode Selection** page of the wizard.
12. Click the **Next** button from the **Terminal Mode Selection** page of the wizard.
13. Click the **Next** button on the **Display Client Selection** page of the wizard.
14. Click the **Next** button on the **Terminal 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.

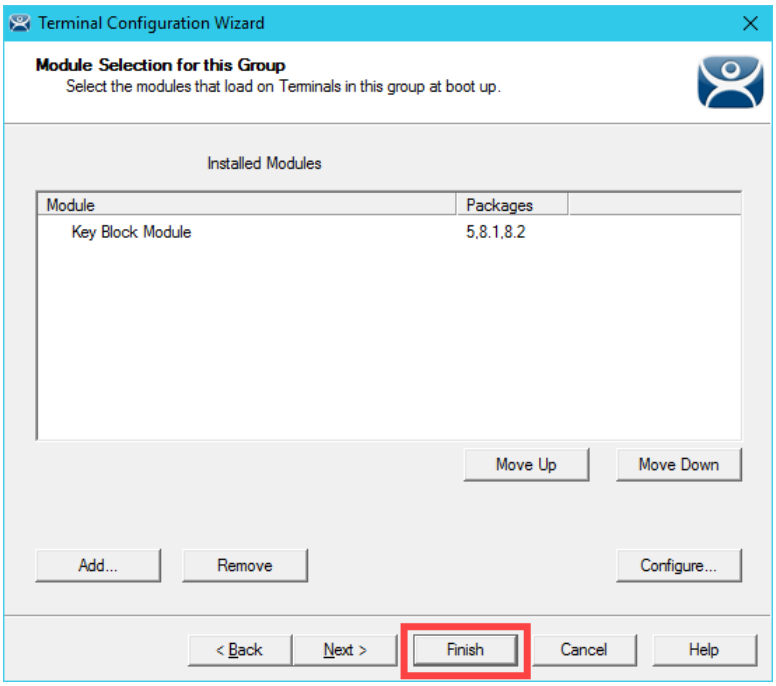
19. Click the **Next** button from the **Mobile Device Group Options** page of the wizard.
20. Click the **Add…** button from the **Module Selection for this Group** page of the wizard.



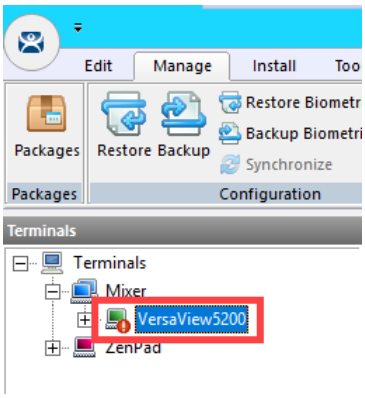
21. Scroll down and select the **Key Block Module**. Click the **OK** button.



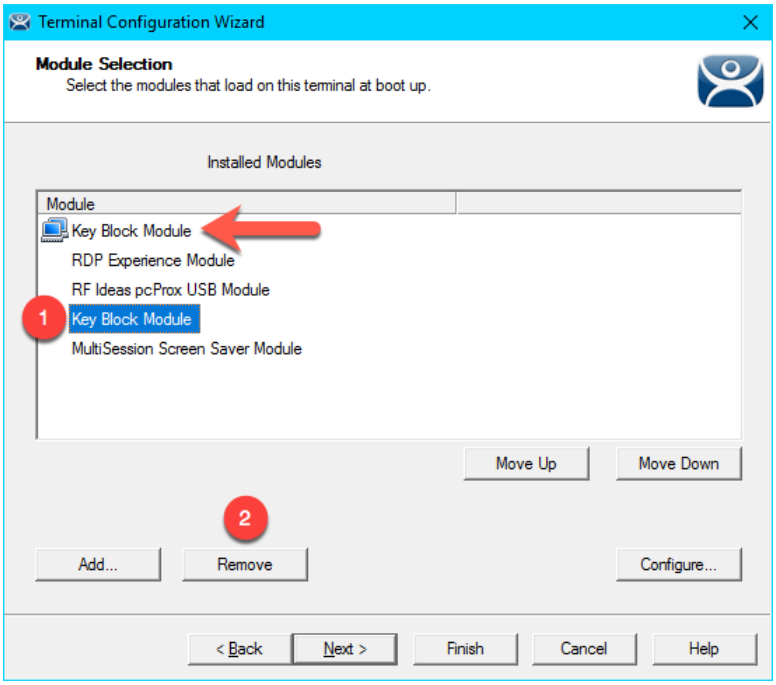
22. Click the **Finish** button.



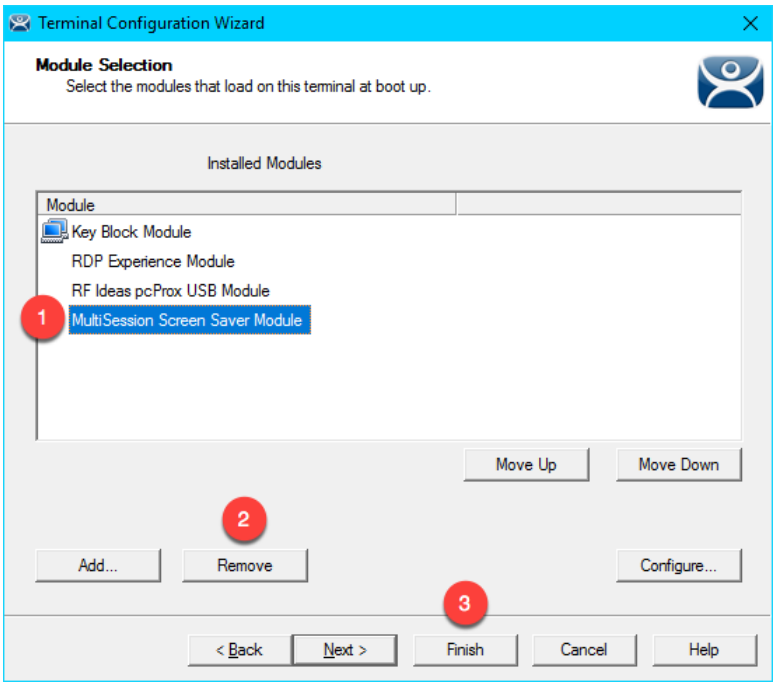
23. Double click on the **VersaView5200** terminal.



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.

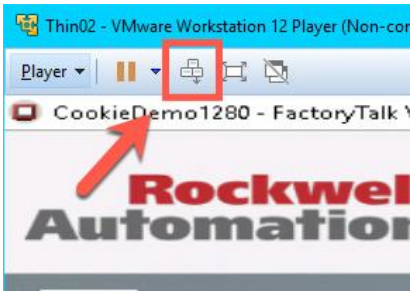


34. While still on the **Module Selection** page of the wizard, remove the **MultiSession Screen Saver Module** followed by the **Finish** button.



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

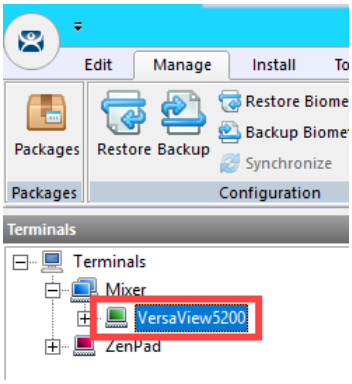
36. Confirm that **CTRL-ALT-DEL** is still blocked, and therefore proving that the **Key Block Module** is successfully inherited from the **Mixer Terminal Group**.



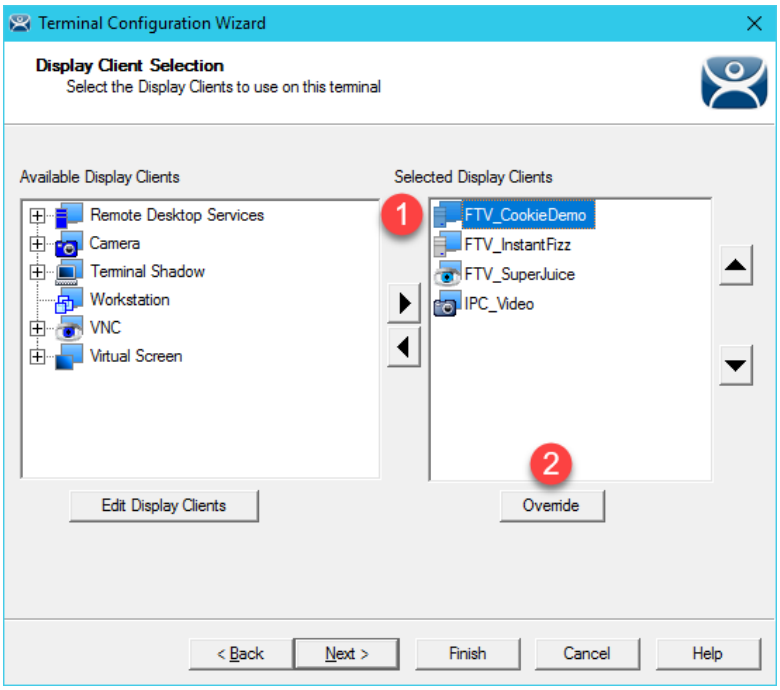
Overrides

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.

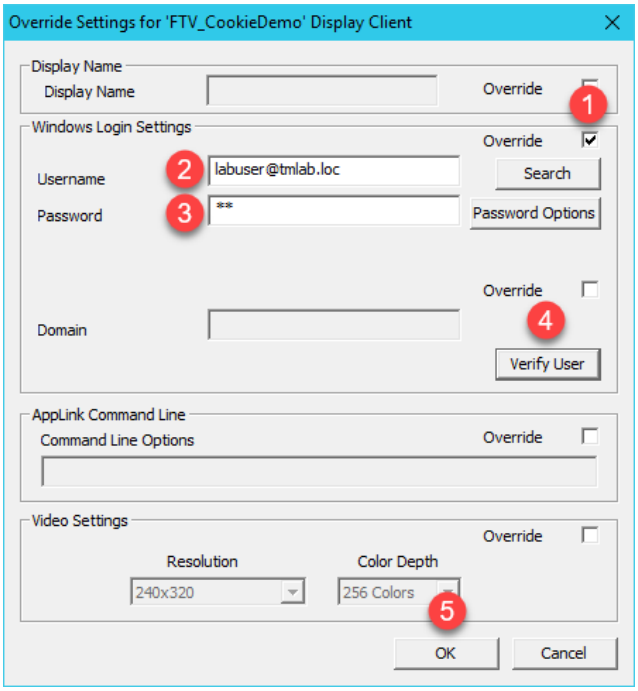
1. Double click the **VersaView5200** terminal.



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.

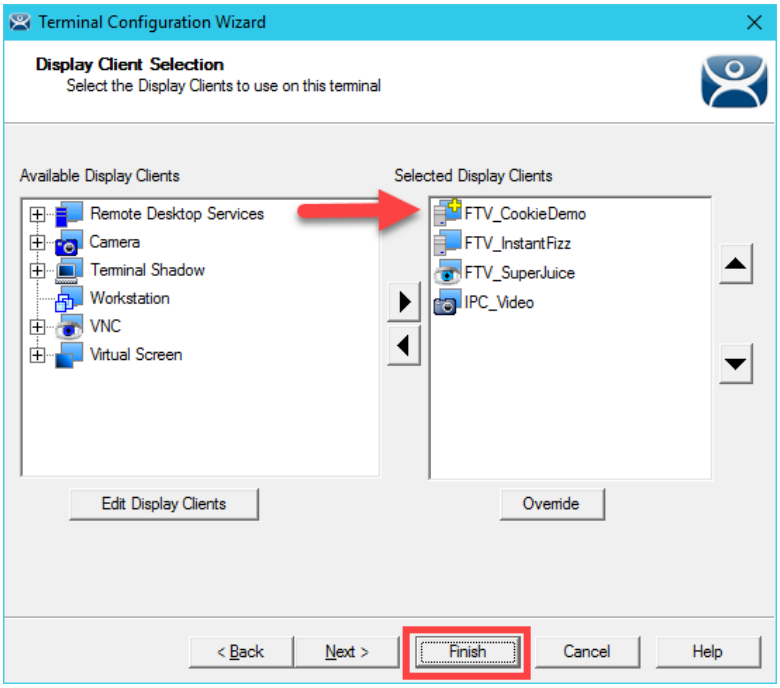


7. From the **Override Settings** window, check the **Override** checkbox on the **Windows Login Settings** frame, enter *labuser@tmlab.loc* as the **Username**, enter *rw* as the **Password**. Click the **Verify User** button to confirm the credentials entered. Click the **OK** button twice.



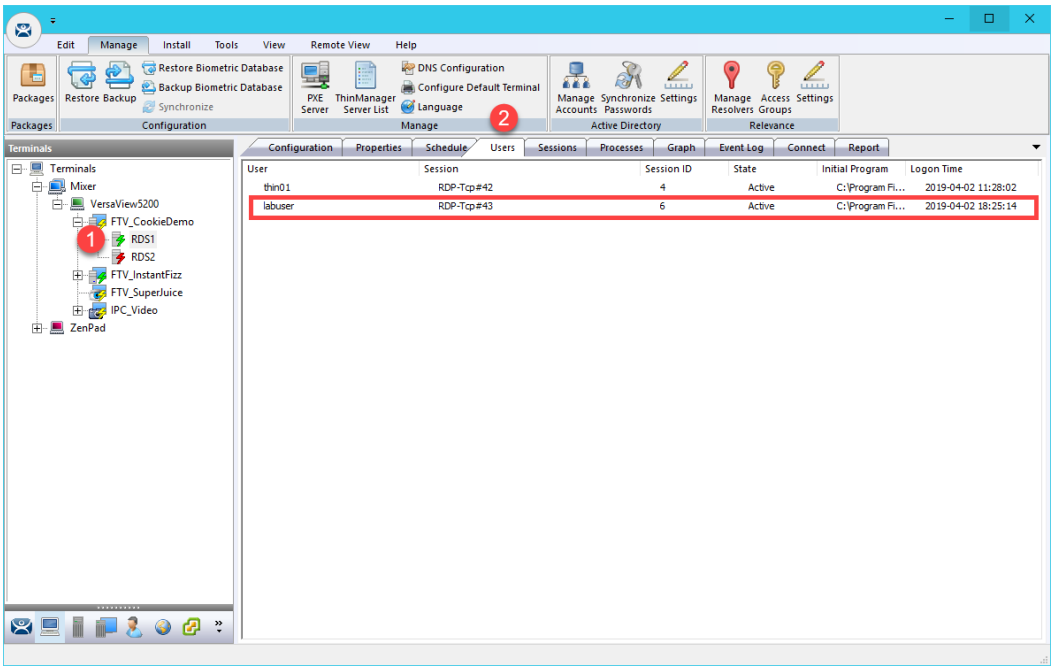
> In addition to user credentials, the **Domain** can be overridden, along with the **AppLink Command Line** and **Video Settings**.

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.

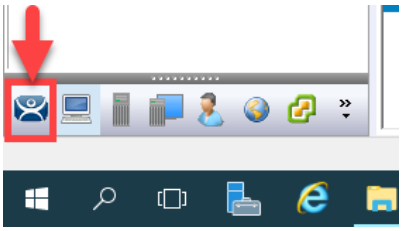
10. At the virtual thin client, you should see a new instance of the **FTV_CookieDemo** launching. Instead of launching as the user assigned to the **VersaView5200 Terminal Profile** (thin01@tmlab.loc), it is now launched as labuser@tmlab.loc. Navigate to **Terminals->Mixer->VersaView5200->FTV_CookieDemo** 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.



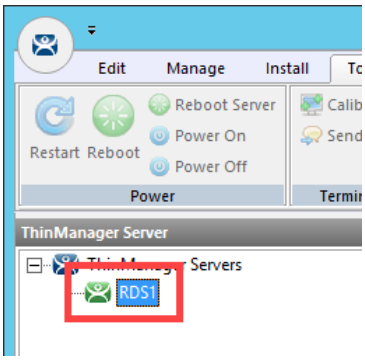
Schedules

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.

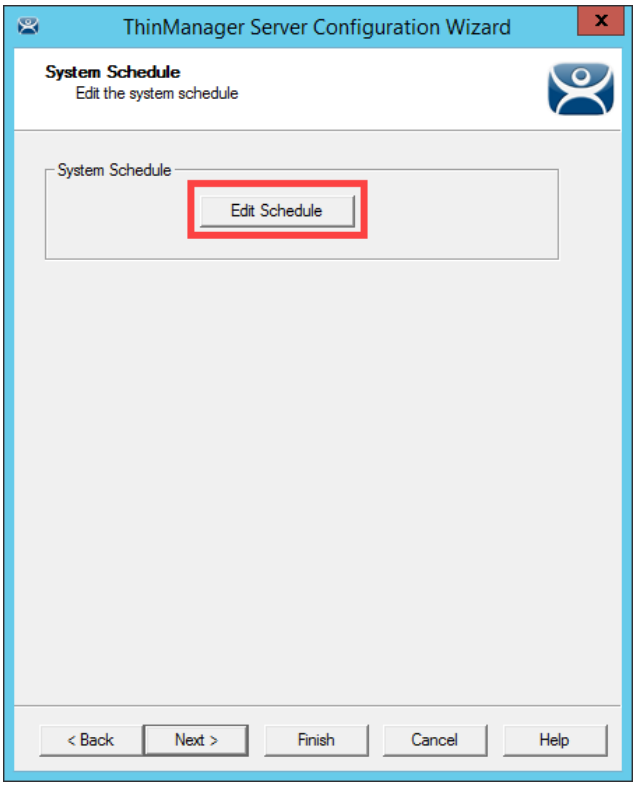


2. Double click the **RDS1** item in the **ThinManager Servers** tree.

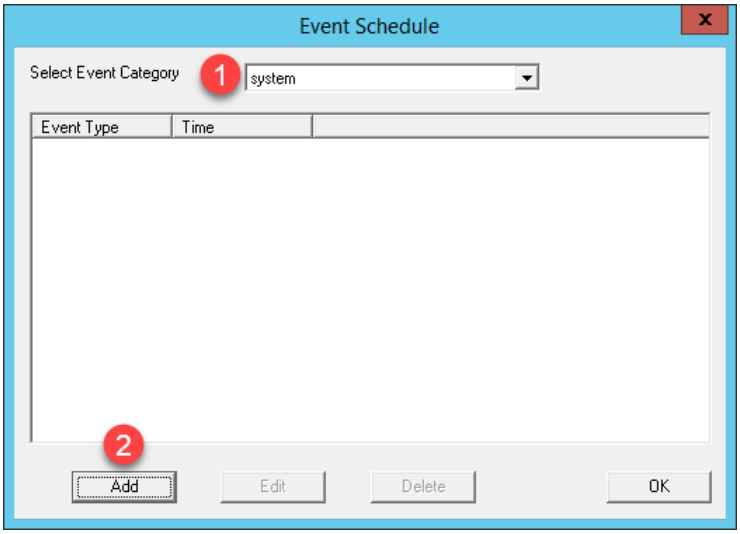


3. Click the **Next** button on the **Introduction** page of the **ThinManager Server Configuration Wizard**.
4. Click the **Next** button on the **Unknown Terminals** page of the wizard.
5. Click the **Next** button on the **Terminal Replacement** page of the wizard.
6. Click the **Next** button on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

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

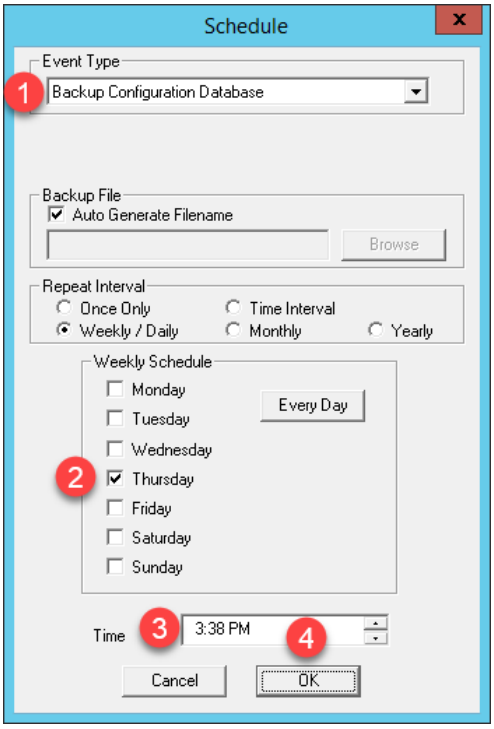


8. From the **Event Schedule** window, select **system** from the **Select Event Category** drop down list and click the **Add** button.

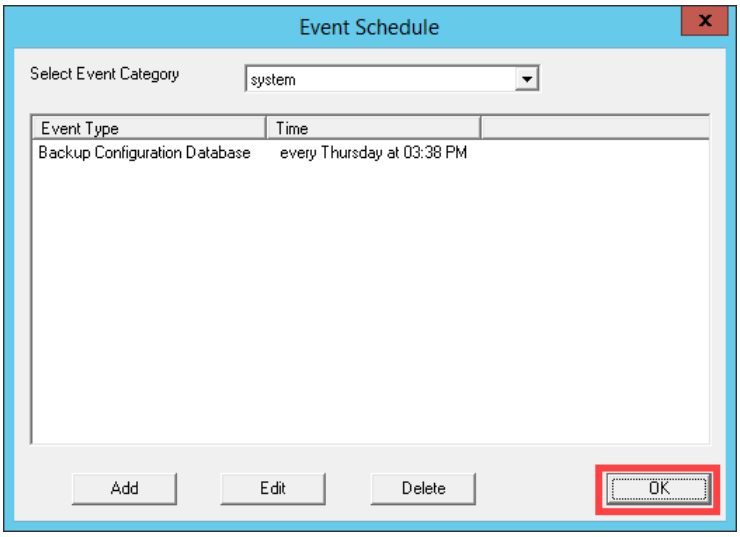


You may notice that is you select **terminal**, **terminalserver** or **user** from the drop down list, the **Add** button will become disabled. That is because **schedules** for these items are created on their respective objects. For example, to set a **terminal schedule** you would do that using the **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.

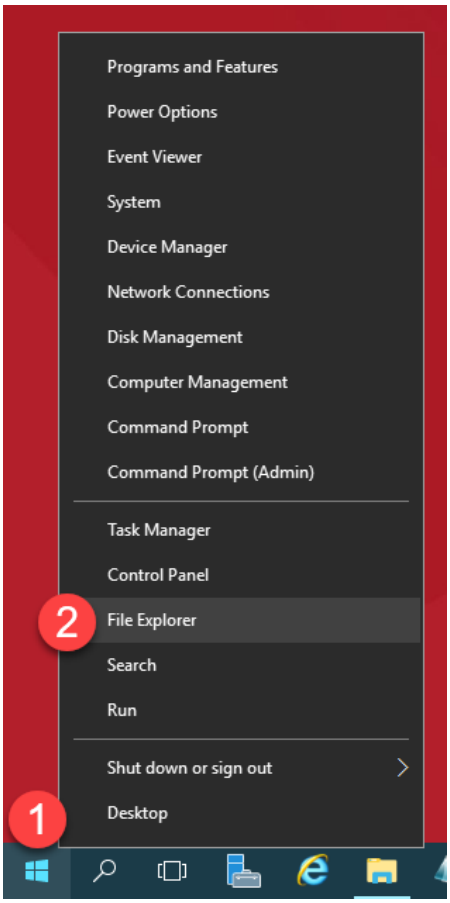
9. Select **Backup Configuration Database** from the **Event Type** drop down list. Leave **Auto Generate Filename** checked. Leave the **Weekly / Daily** radio button selected. Check today's day (**Thursday** in the screen shot) checkbox in the **Weekly Schedule** frame and set the time to 2 minutes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



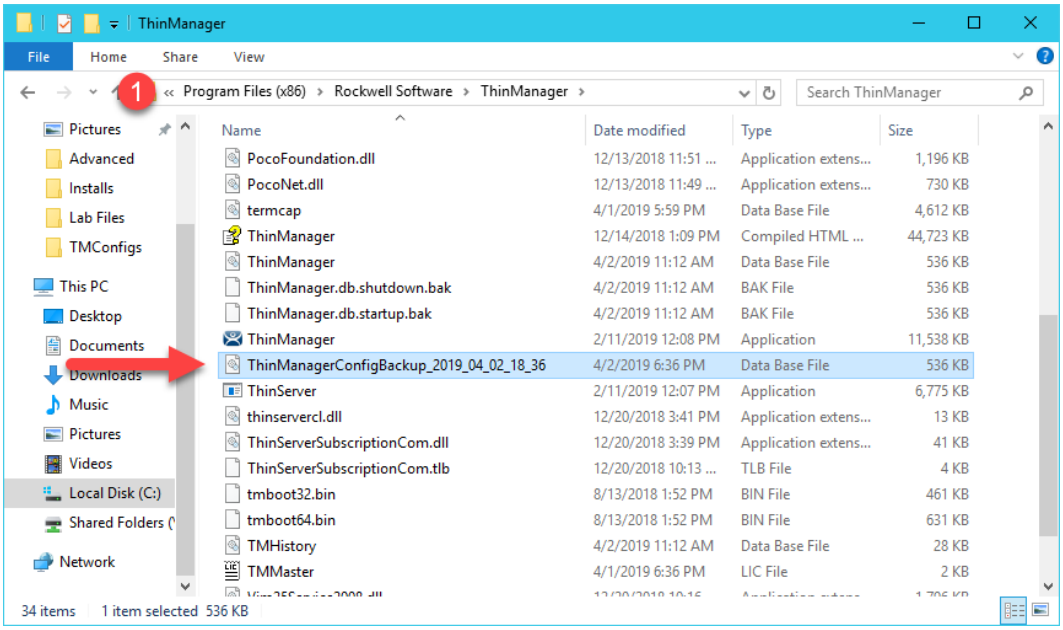
10. Click the **OK** button followed by the **Finish** button.



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

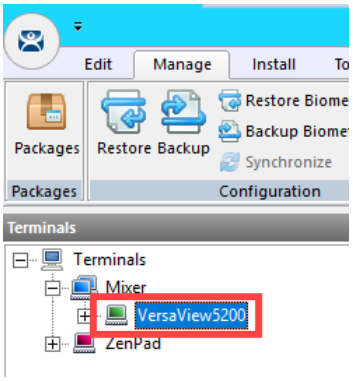
Enhanced **mouse button mapping** was added with the release of ThinManager 9.0. You can assign and perform the following ThinManager-related actions to any mouse button.

- 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**.

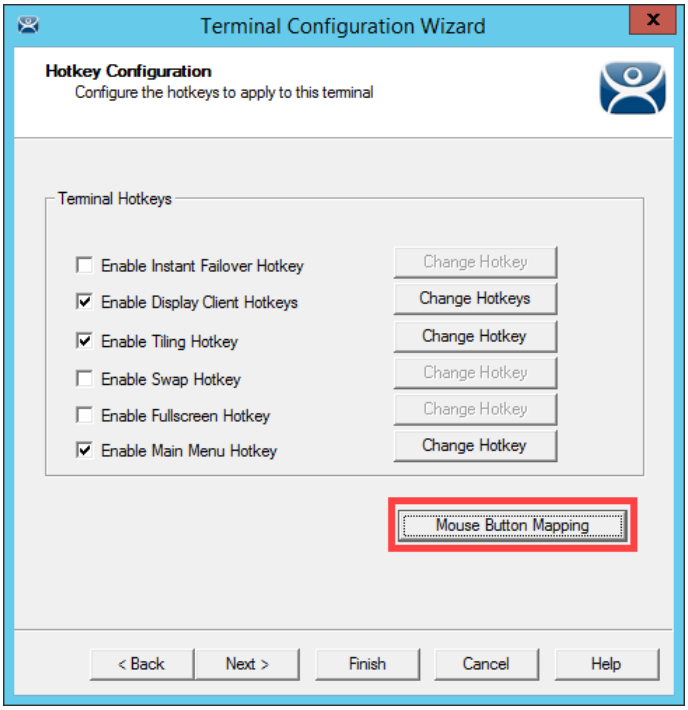
1. Click the **Terminals** icon from the button bar.

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

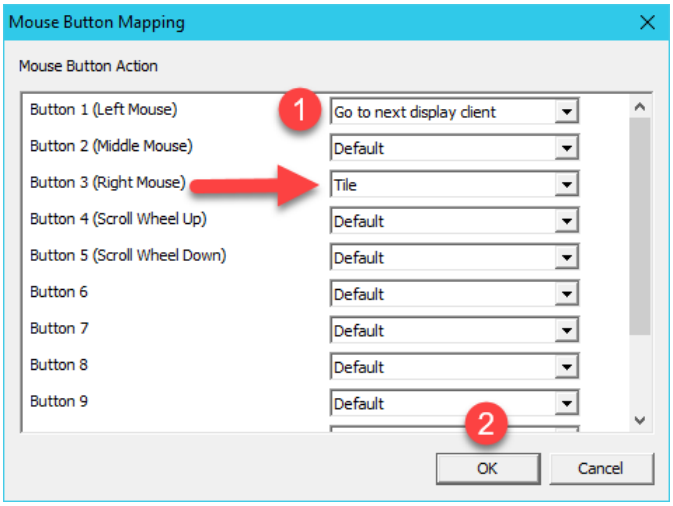


3. Click the **Next** button on the **Terminal Name** page of the wizard.
4. Click the **Next** button on the **Terminal Hardware** page of the wizard.
5. Click the **Next** button on the **Terminal Options** page of the wizard.
6. Click the **Next** button on the **Terminal Mode Selection** page of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

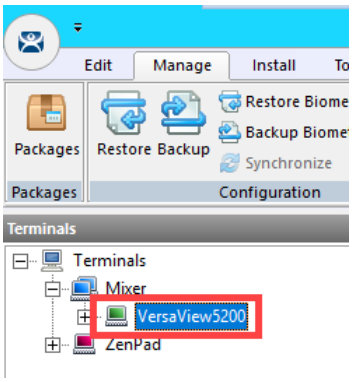


11. Click the **Finish** button.
12. Right click the **VersaView5200** terminal and select the **Restart Terminal** item. Click the **Yes** button to confirm.
13. At the virtual thin client, verify that a **Left Click** (or touch) switches to the next **Display Client**.

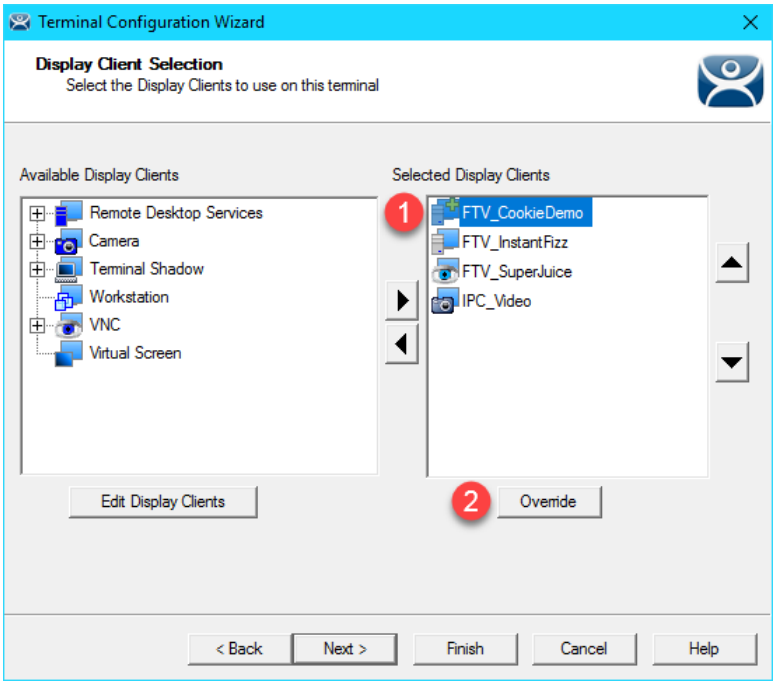
Remove Override and Mouse Button Mapping

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

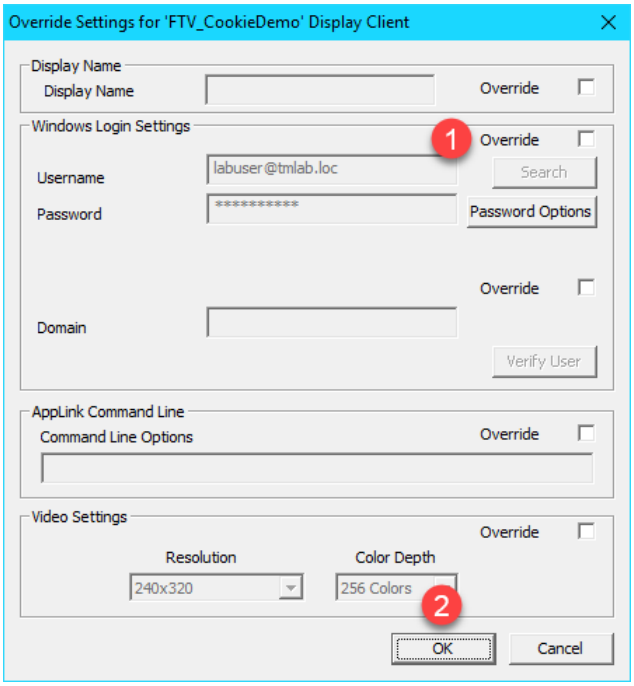
1. Double click the **VersaView5200** terminal.



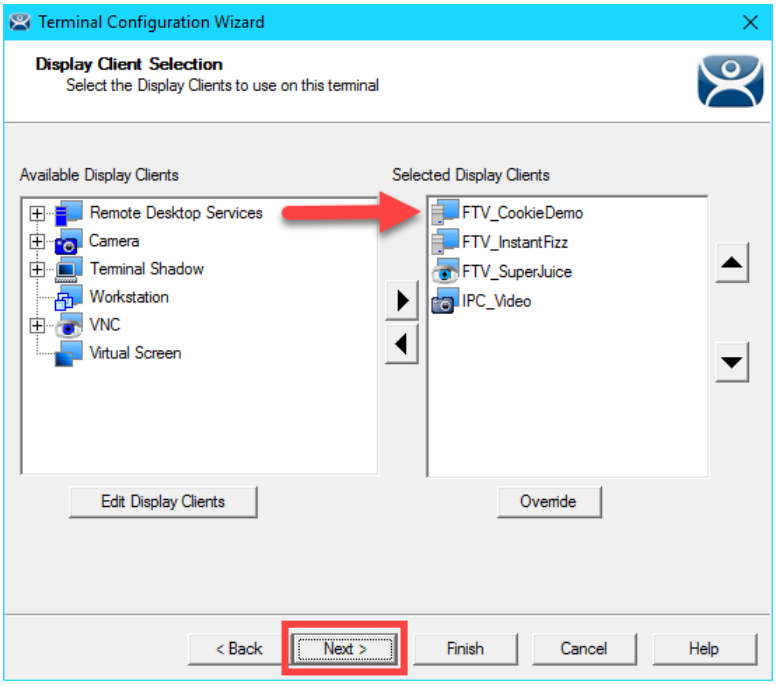
2. Click the **Next** button on the **Terminal Name** page of the wizard.
3. Click the **Next** button on the **Terminal Hardware** page of the wizard.
4. Click the **Next** button on the **Terminal Options** page of the wizard.
5. Click the **Next** button on the **Terminal Mode Selection** page of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



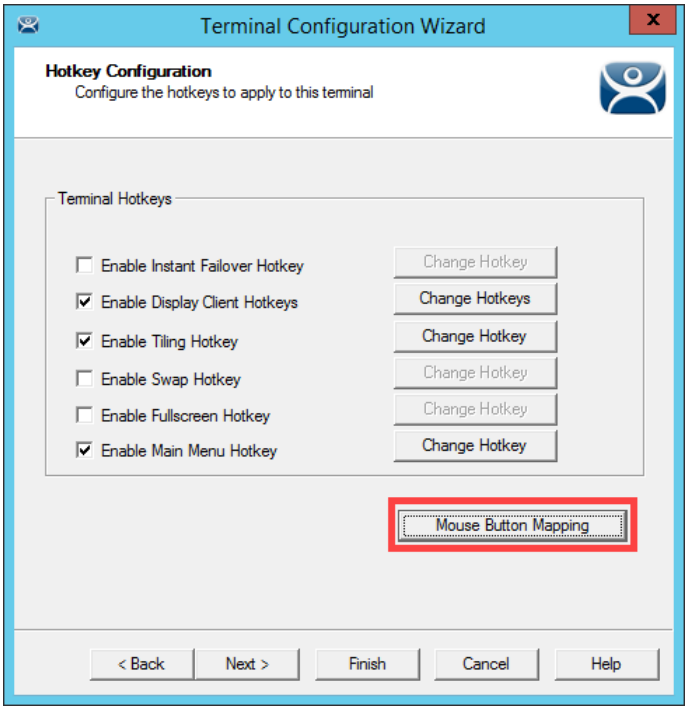
7. From the **Override Settings** window, un-check the **Override** checkbox and click the **OK** button.



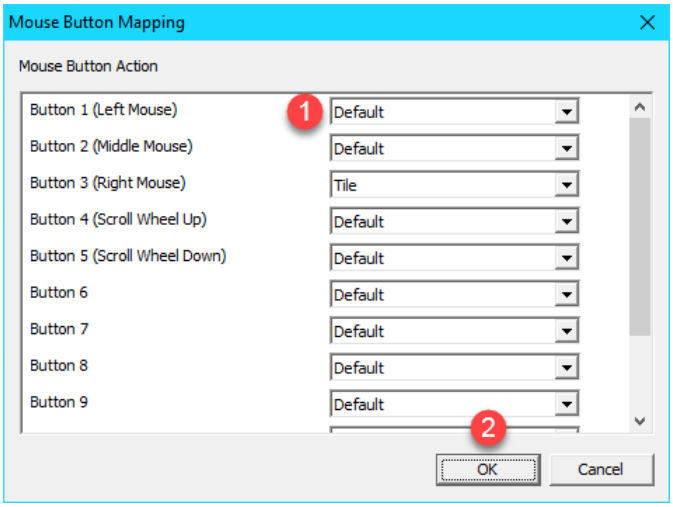
8. From the **Display Client Selection** page of the wizard, notice the **FTV_CookieDemo Display Client** no longer has the **Override** icon assigned to it. Click the **Next** button.



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.

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 7: Securing the ThinManager Admin Console

Overview

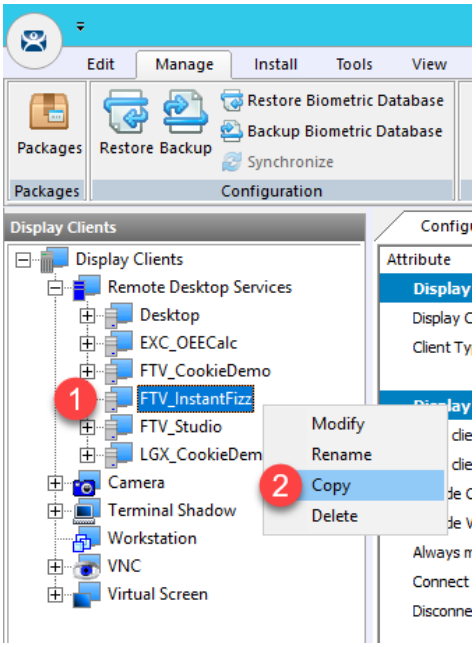
By default, only local administrator user accounts can access the **ThinManager Admin Console**. For ThinManager systems on an **Active Directory** (AD) domain, AD users who will administer the ThinManager system must initially be added to the local Administrators group on the ThinManager server. To 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

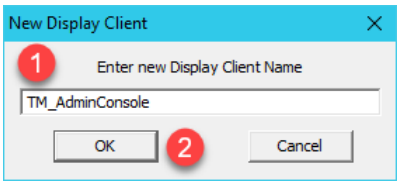
Create ThinManager Admin Console Display Client

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

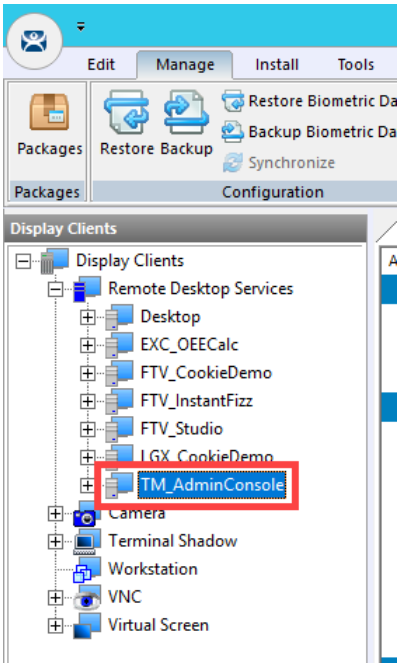
2. Expand the **Remote Desktop Services** tree item, right click the **FTV_InstantFizz Display Client** and select **Copy**.



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



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



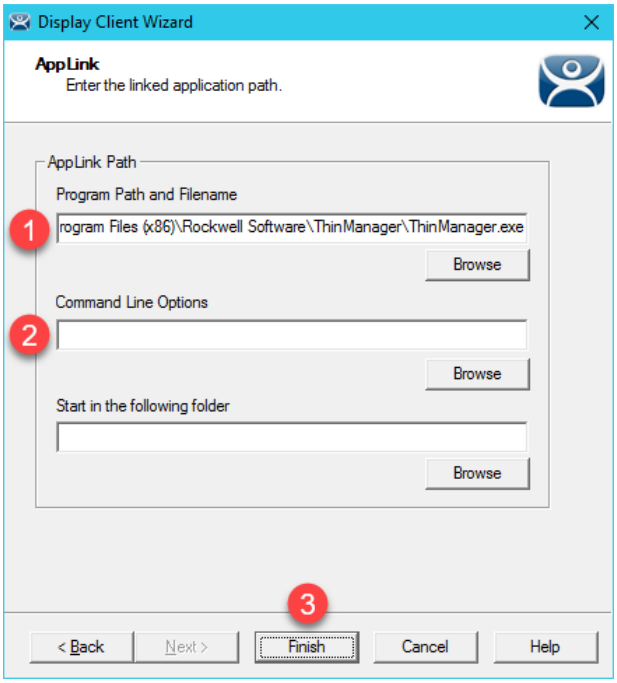
5. From the **Client Name** page of the wizard, click the **Next** button.
6. From the **Display Client Options** page of the wizard, click the **Next** button.
7. From the **Remote Desktop Services and Workstation Options** page of the wizard, click the **Next** button.
8. From the **Screen Resolution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

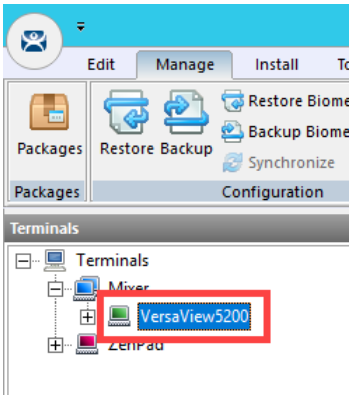
    Command Line Options:



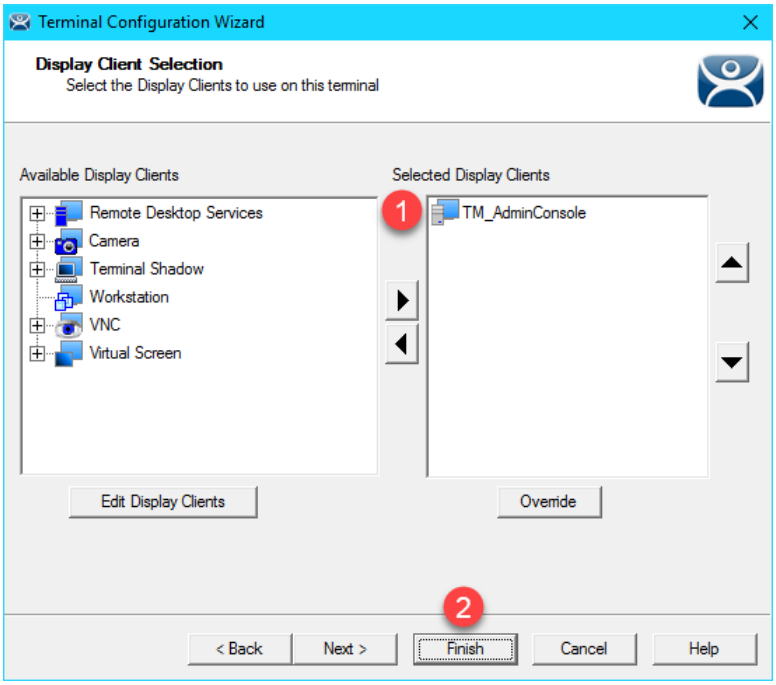
Assign Admin Console Display Client to Terminal

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

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

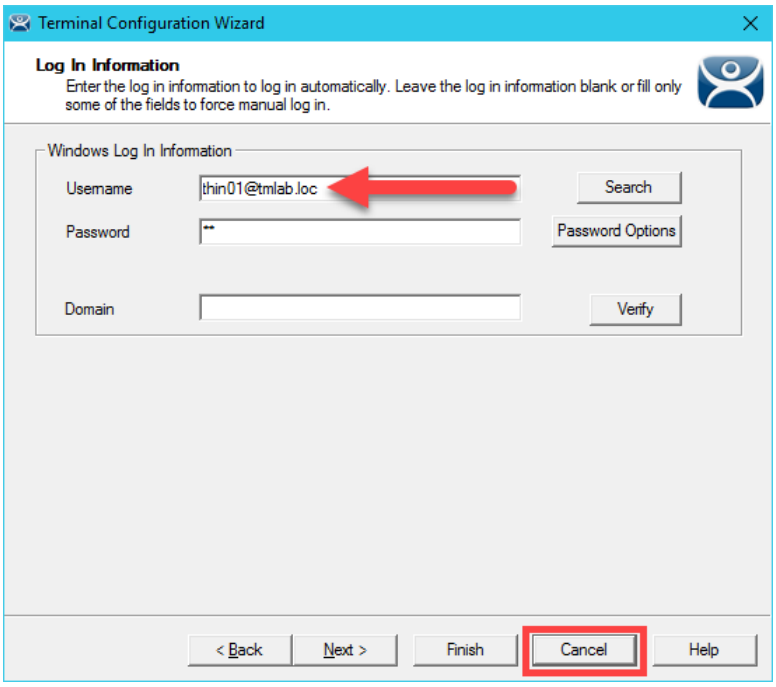


3. Click the **Next** button from the **Terminal Name** page of the wizard.
4. Click the **Next** button from the **Terminal Hardware** page of the wizard.
5. Click the **Next** button from the **Terminal Options** page of the wizard.
6. Click the **Next** button from the **Terminal Mode Selection**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

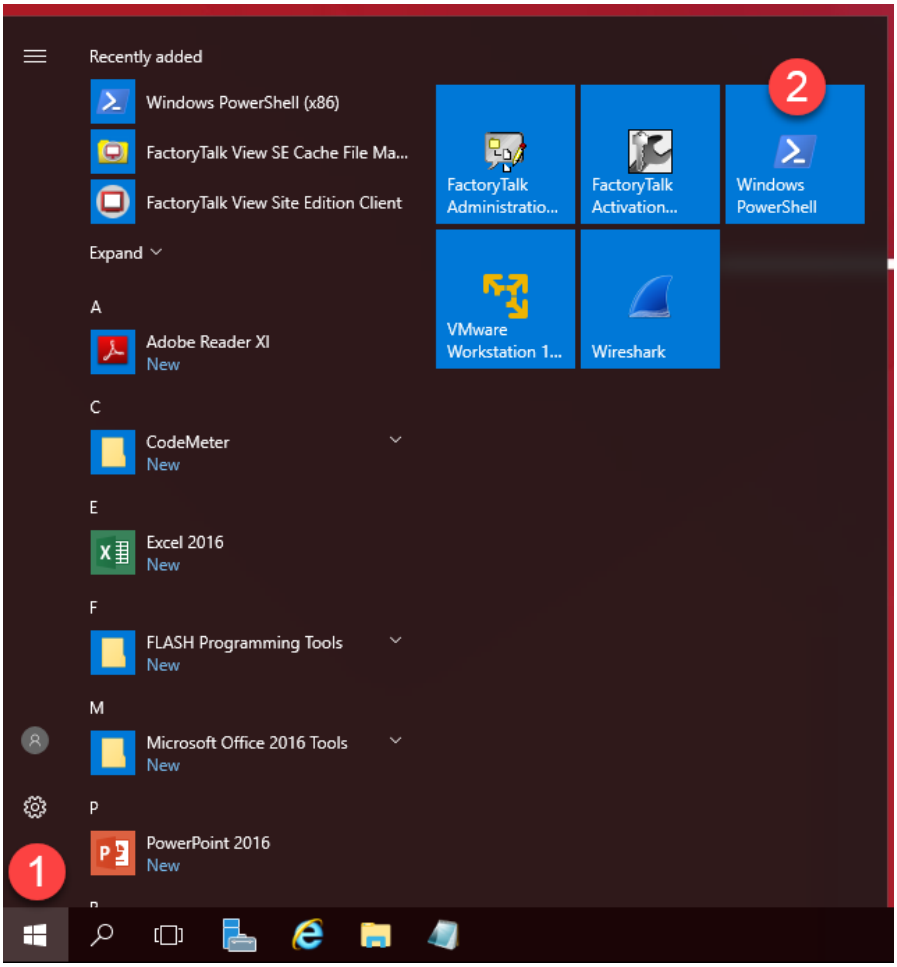
10. Recall that the user account assigned to the **VersaView5200** terminal is **thin01@tmlab.loc**. You can verify this by double clicking the **VersaView5200** terminal profile and advancing through the **Terminal Configuration Wizard** until you reach the **Log In Information** page. Since the **thin01@tmlab.loc** 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

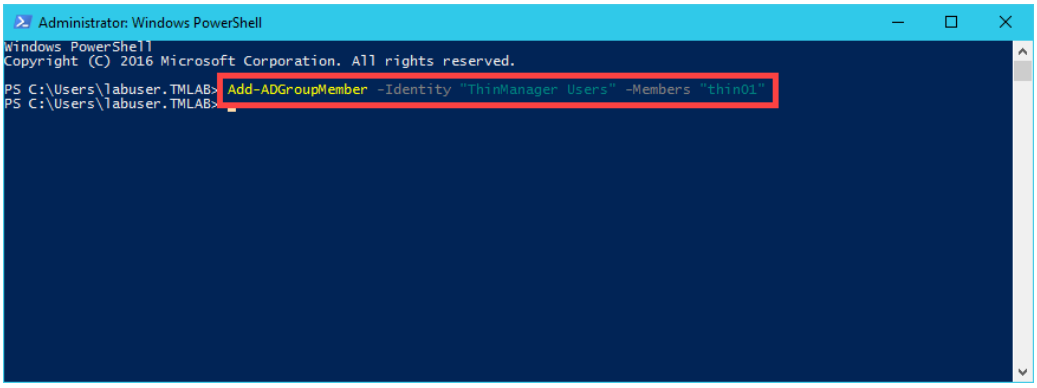
The Windows Security Groups utilized in this section of the lab have been pre-created within Active Directory. If you do not have a domain, these Security Groups could also be Local Security Groups.

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**.



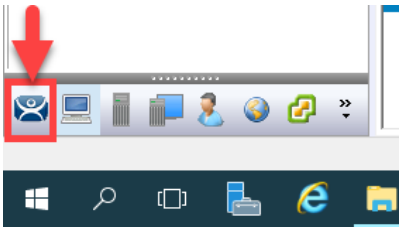
2. In the **PowerShell** window, enter the following command (you can also copy this from the **LabPaths.txt** file) and hit ENTER. This will add the **thin01** user to the **ThinManager Shadow Users ActiveDirectory Security Group**. Once completed, close the **PowerShell** window.

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

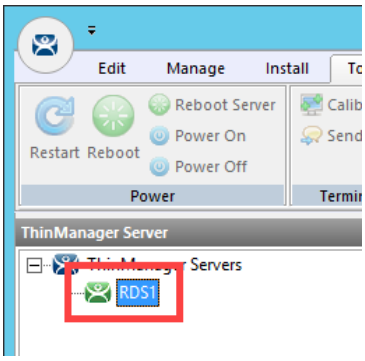


The **ServerManager PowerShell** module was preinstalled on **RDS1** as well as the **ActiveDirectory PowerShell** feature.

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

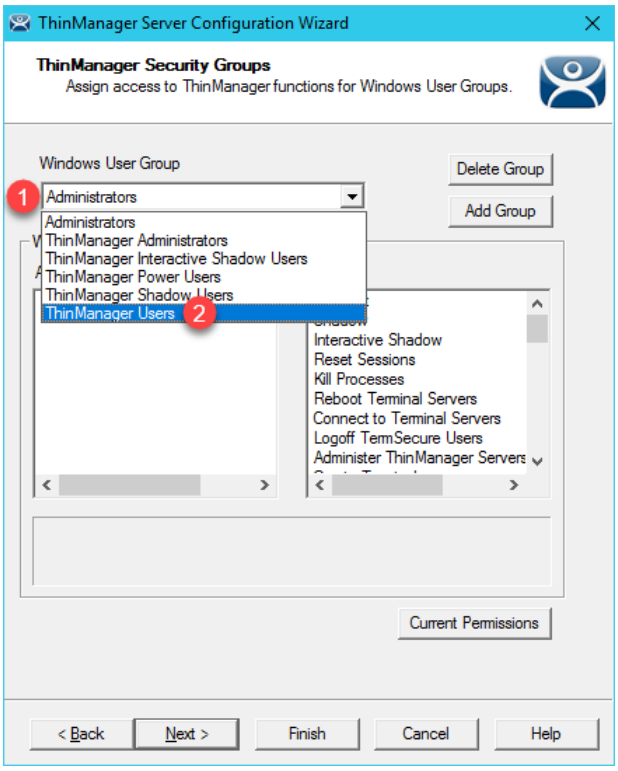


4. Double click the **RDS1** item in the **ThinManager Servers** tree.

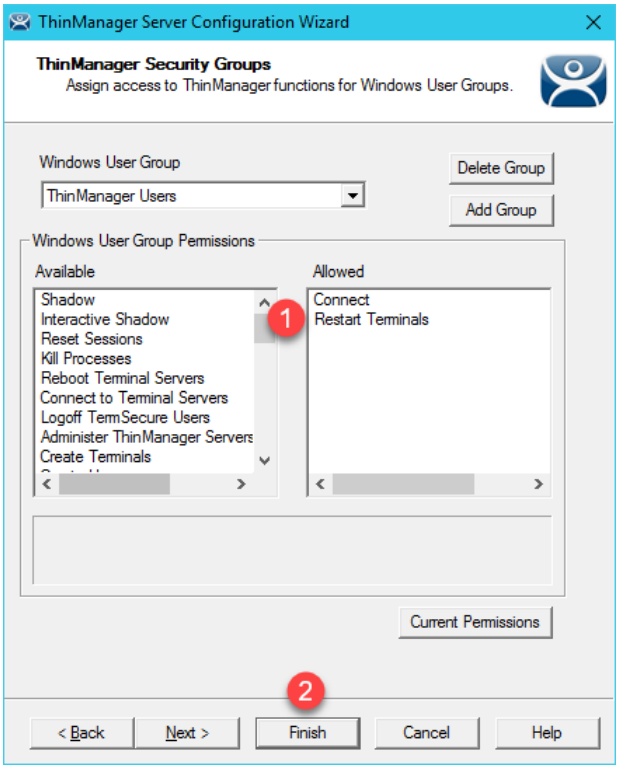


5. Click the **Next** button on the **Introduction** page of the **ThinManager Server Configuration Wizard**.
6. Click the **Next** button on the **Unknown Terminals** page of the wizard.
7. Click the **Next** button on the **Terminal Replacement** page of the wizard.
8. Click the **Next** button on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

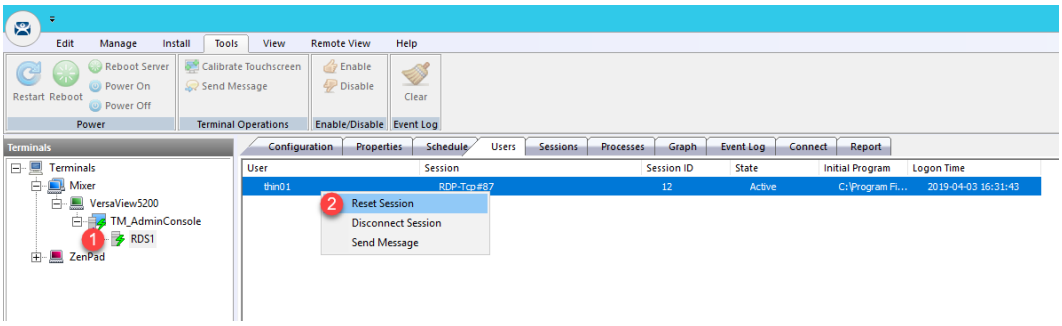
10. From the **ThinManager Security Groups** page of the wizard, notice that the pre-selected **Administrators** group has every **Available** list box **permission** in the **Allowed** list box. This indicates that, by default, members of the local **Administrators** group where **ThinManager** is installed 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.



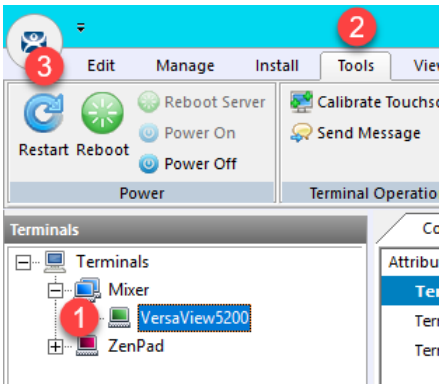
11. The **ThinManager Users** group is permitted to **Connect** only by default and can essentially do nothing else within the **Admin Console**. Scroll to the **Restart Terminals** permission and double click it to add it to the **Allowed** list. Click the **Finish** button.



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 8: 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.

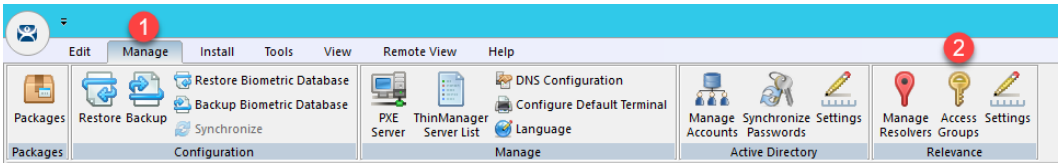
In this section, you will be performing the following tasks:

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

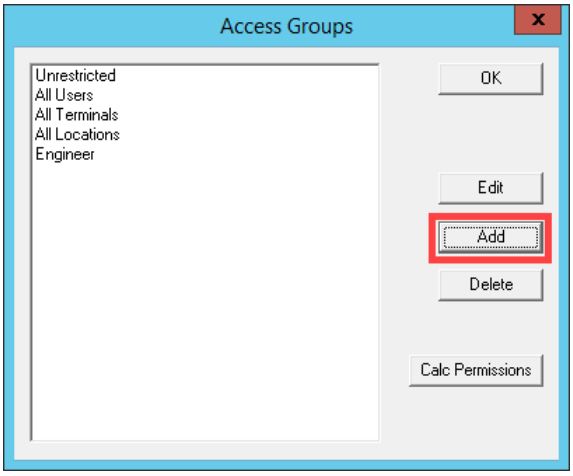
Create Maintenance Access Group

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.

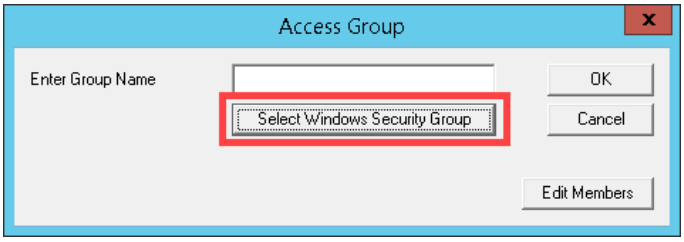
1. Click the **Manage** ribbon, followed by the **Access Groups** icon.



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

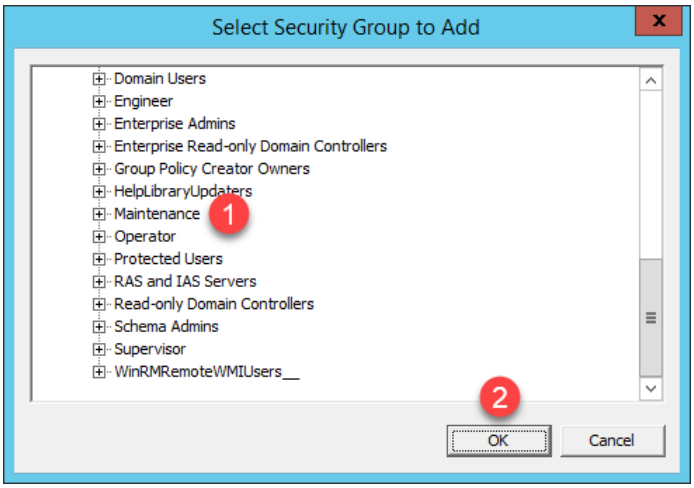


3. Click the **Select Windows Security Group** button.

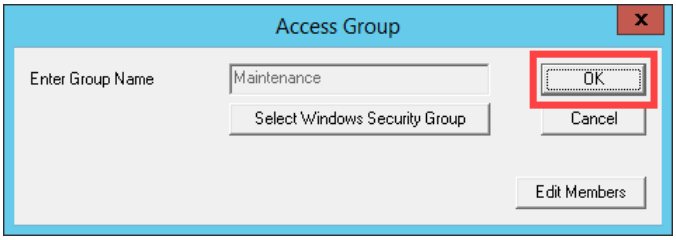


The Select Windows Security Group provides the ability to link an **Access Group** to a **Widows Security Group**. Therefore, you could manage access to ThinManager resources (**Terminals**, **Display Clients**, etc.) through **Windows Security Groups** as well. You could also use the **TermMon ActiveX**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

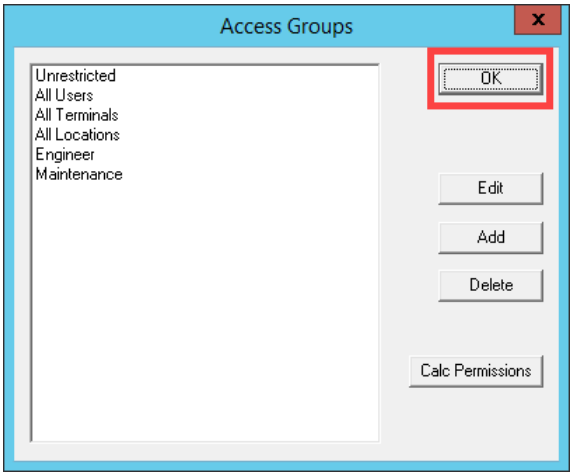
4. From the **Select Security Group to Add** window, expand the **Users** item and select the **Maintenance** group, followed by the **OK** button.



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

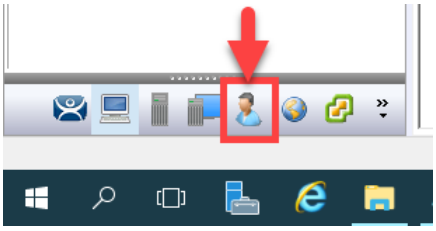


6. From the **Access Groups** window, click the **OK** button.

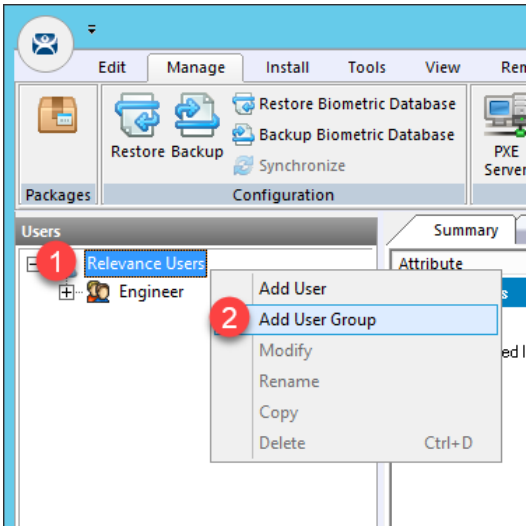


Create Maintenance User Group

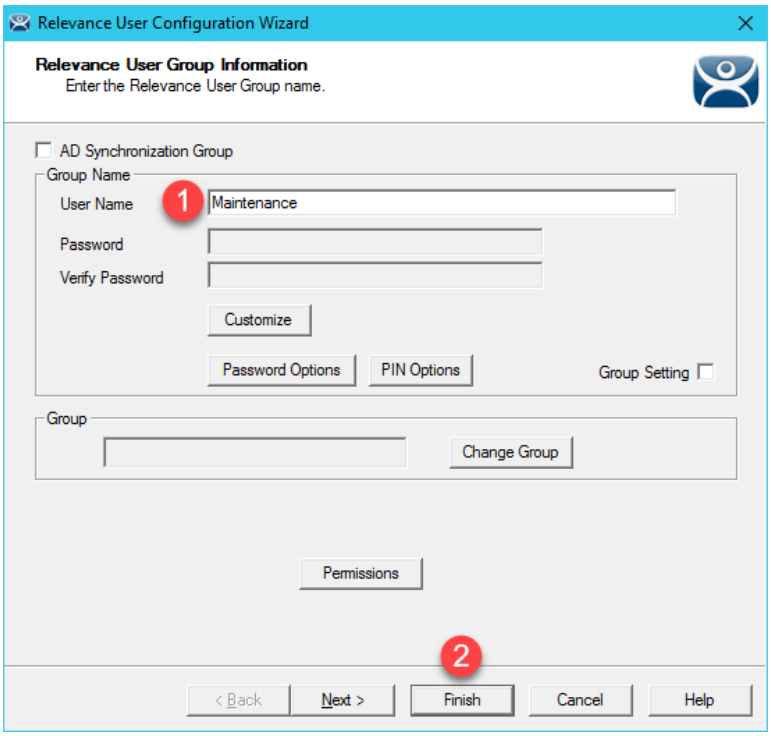
1. Click the **Users** icon  in the ThinManager tree selector.



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**.

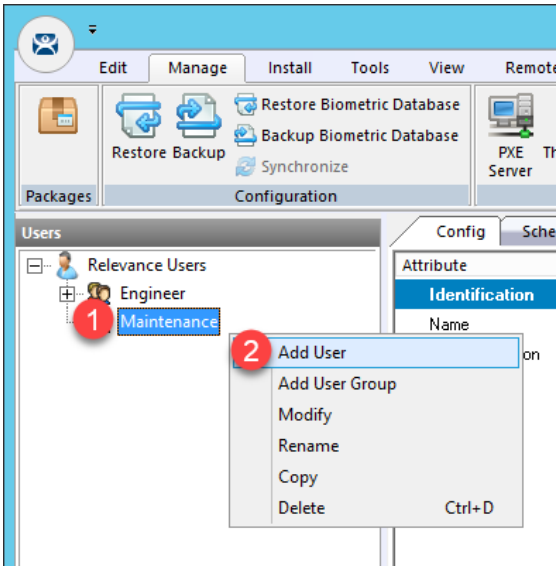


3. From the **Relevance User Group Information** page of the wizard, enter *Maintenance* as the **User Name** in the **Group Name** frame. Click the **Finish** button.

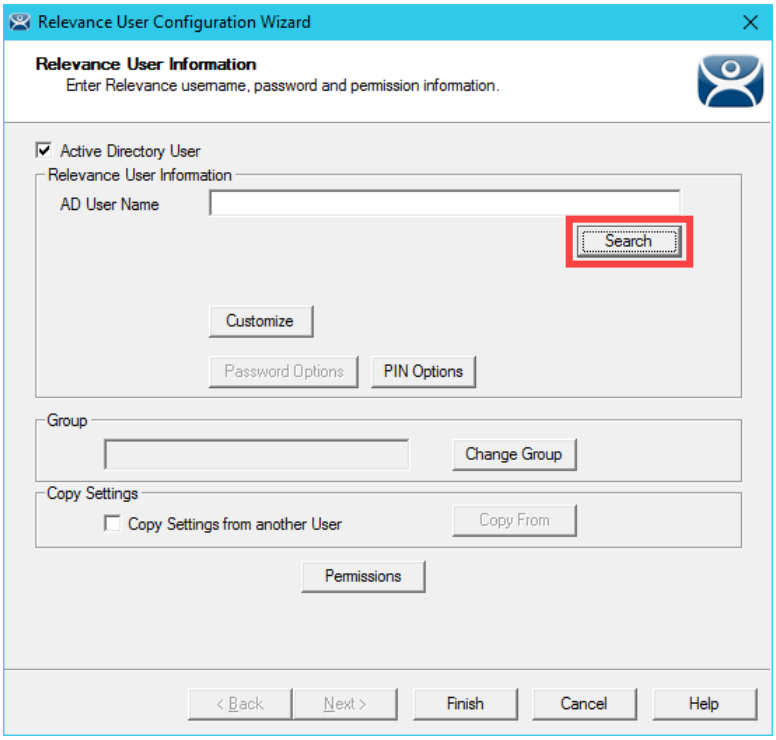


Create Maintenance User

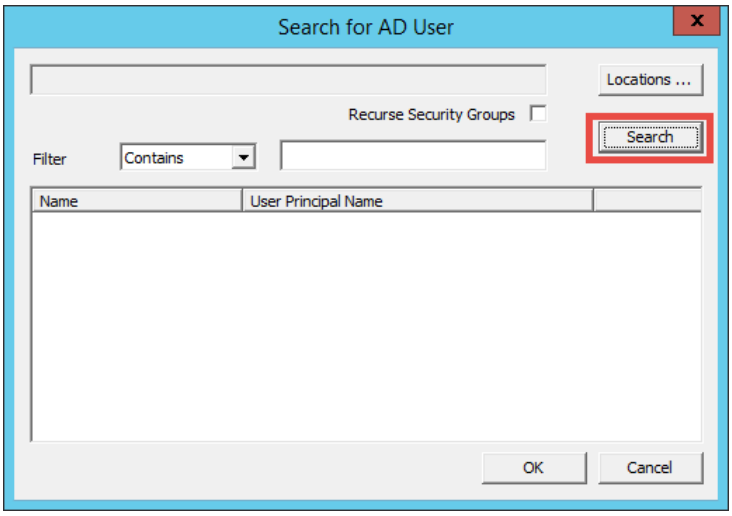
1. Expand the **Relevance Users** node.
2. Right click the newly created **Maintenance User Group** and select **Add User**. This will launch the **Relevance User Configuration** wizard.



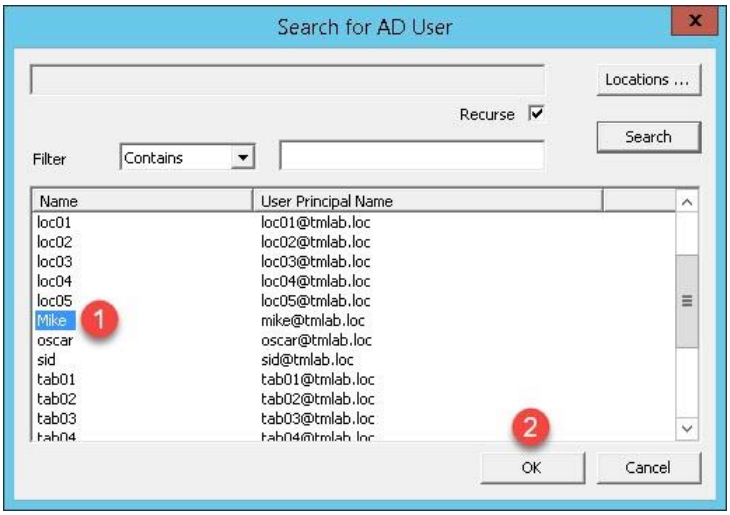
3. From the **Relevance User Information** page of the wizard, check the **Active Directory User** checkbox if it is not already checked. Click the **Search** button.



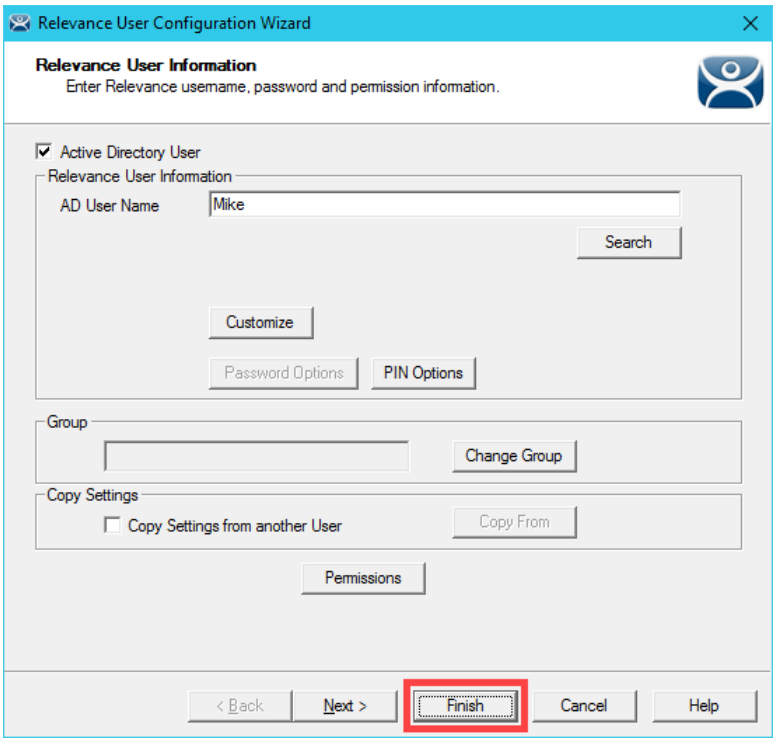
4. From the **Search for AD User** dialog box, click the **Search** button.



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.

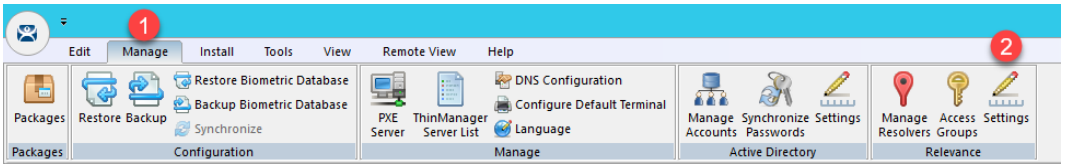


Register a Bluetooth Beacon Location Resolver

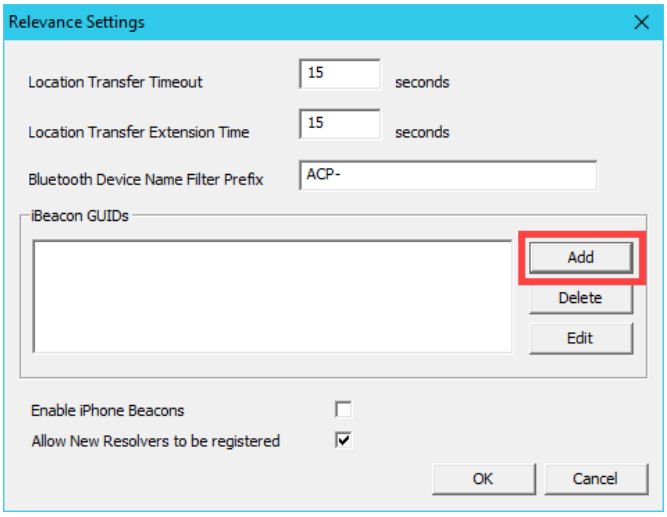
A **Bluetooth Beacon** uses **Bluetooth Low Energy** (**BTLE**) to transmit a signal continuously, hence the name beacon. This signal includes a **Received Signal Strength Indicator** (**RSSI**). Version 4.0 of the Bluetooth Standard, which a majority of today's mobile devices support, included support 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**.

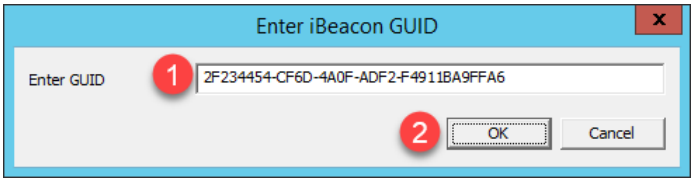
1. From ThinManager, click the **Manage** ribbon followed by the **Settings** icon within the **Relevance** group.



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

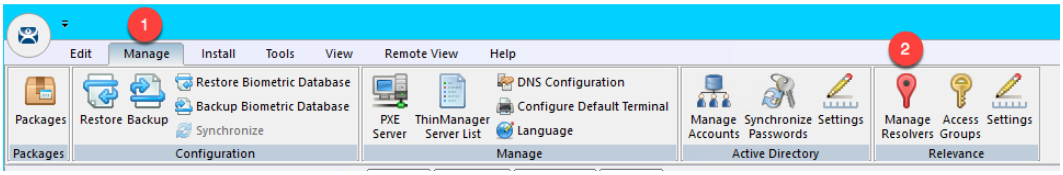


3. Enter the following in the **GUID** field *2F234454-CF6D-4A0F-ADF2-F4911BA9FFA6* (you can also copy and paste this path from the **LabPaths.txt** file by right clicking the **Notepad** icon pinned to the start bar and selecting **LabPaths.txt**). Click the **OK** button.

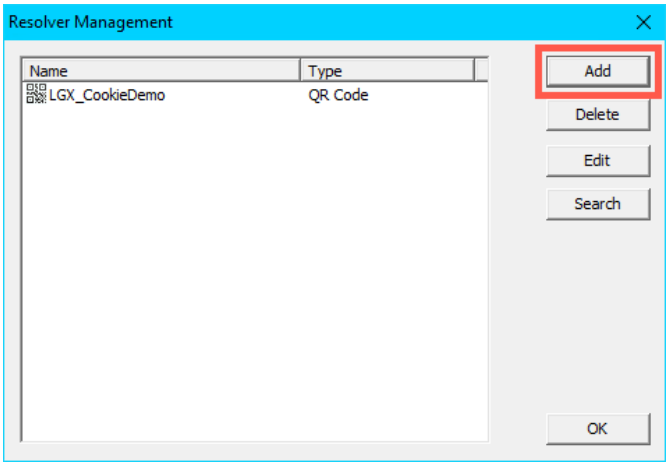


4. Click the **OK** button.

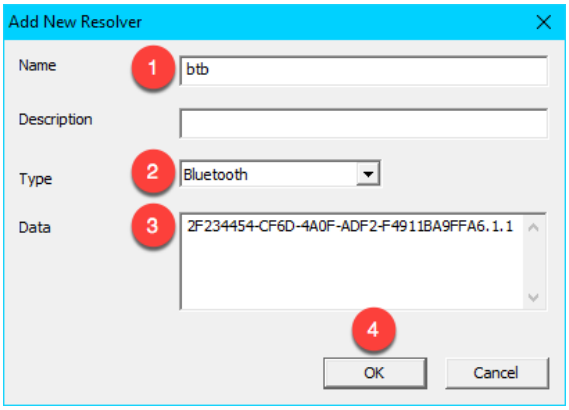
5. Click the **Manage** ribbon followed by the **Manage Resolvers** icon.



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

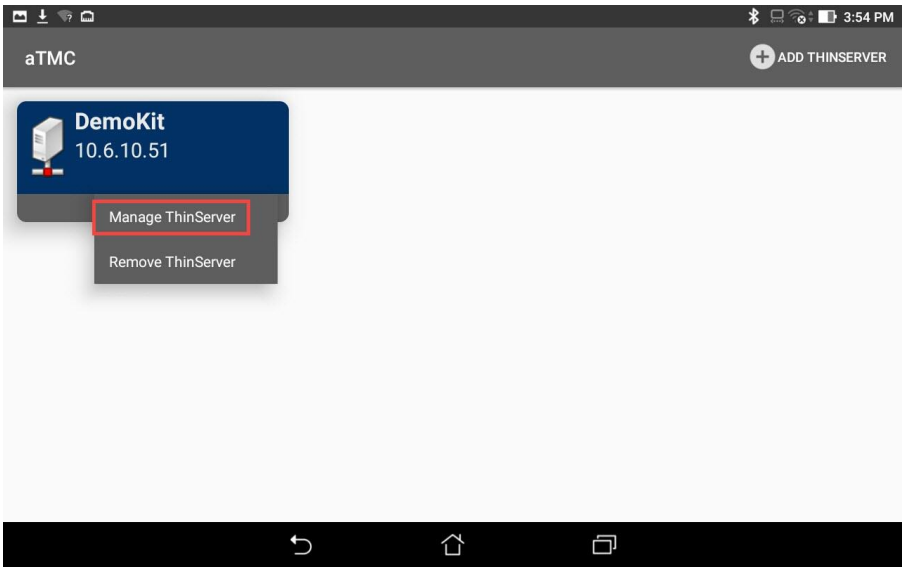


8. From the **Add New Resolver** window, enter *btb* as the **Name**, select **Bluetooth** as the **Type** and enter or copy/paste *2F234454-CF6D-4A0F-ADF2-F4911BA9FFA6.1.1* into the **Data** field. Click the **OK** button followed by the **OK** button again.

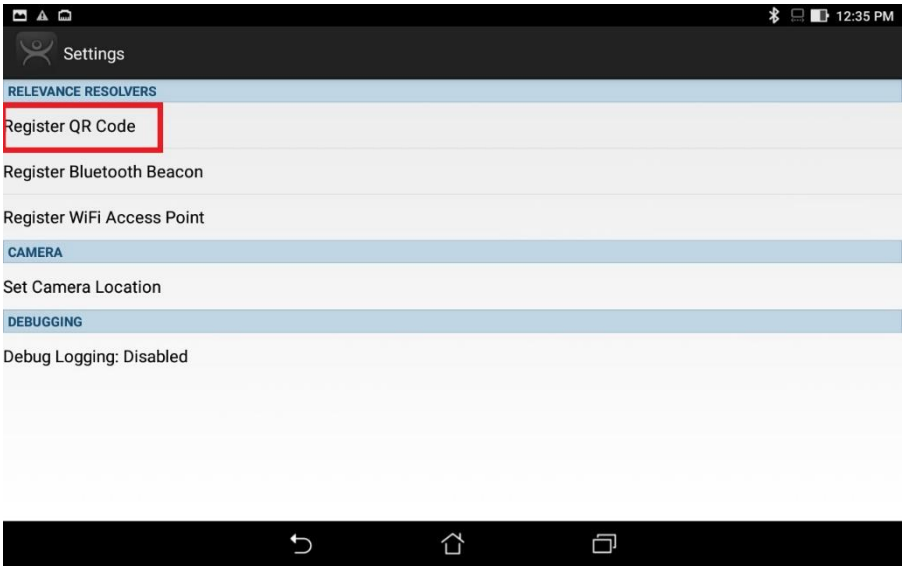


Register a QR Code Location Resolver

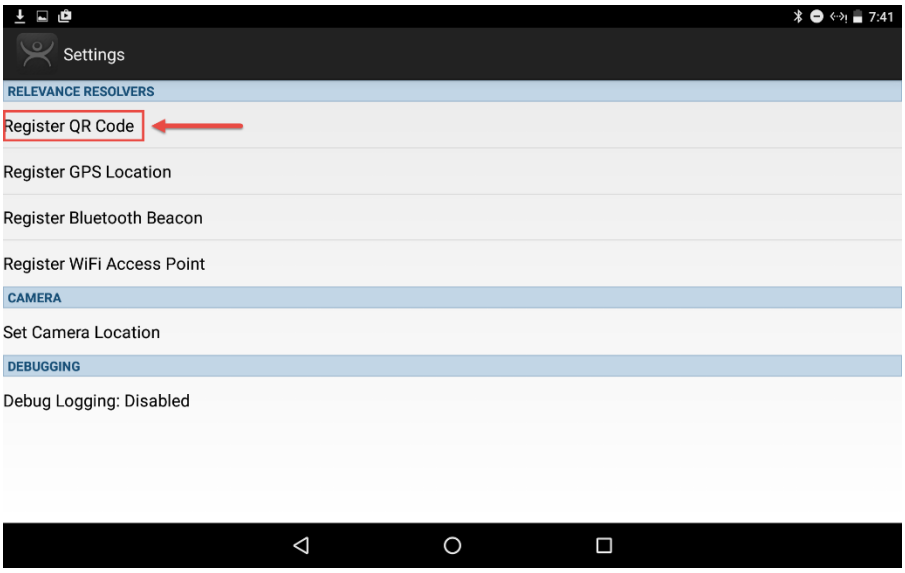
1. From the aTMC **Main Menu**, touch the **Settings** button (3 vertical dots below the **DemoKit** button), followed by the **Manage ThinServer** button.



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

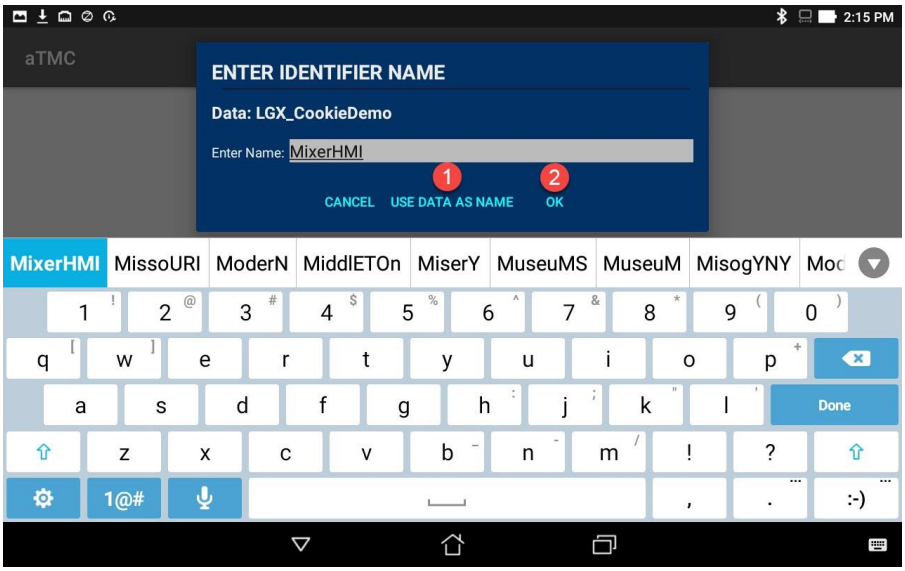


3. Back at the **aTMC Settings** window, touch the **Register QR Code** button.

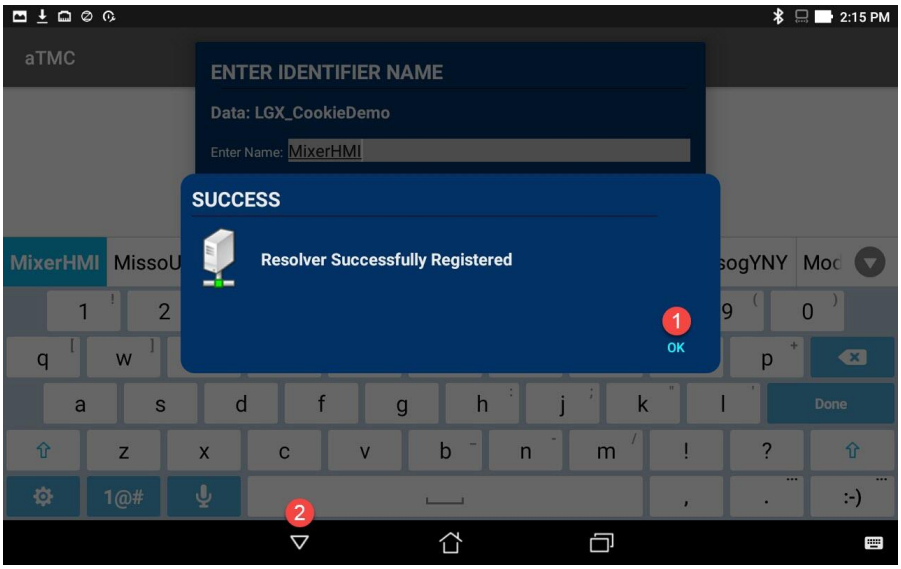


4. A camera window will appear. Point the Tablet camera at the **QR Code** below.

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.



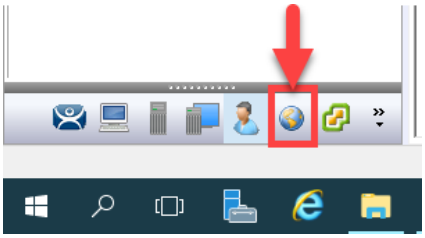
6. You should receive a successful confirmation dialog. Touch the **OK** button, followed by the **Back** button to return to the **Main Menu.**



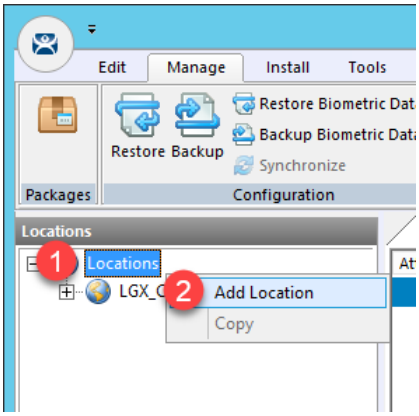
Create Parent (Geo-Fence) Location

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**.

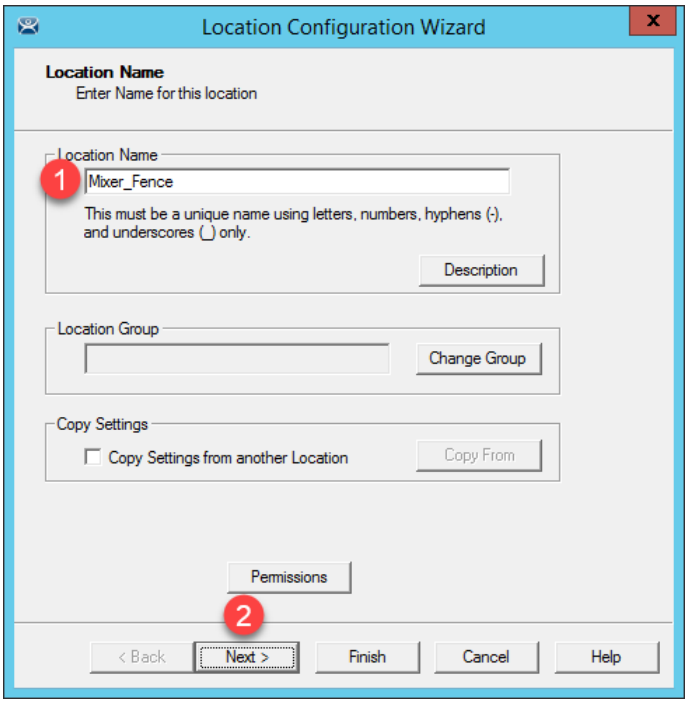
1. Click the **Locations** icon  in the tree selector. This icon will only be present if you have a **Relevance** license activated.



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.

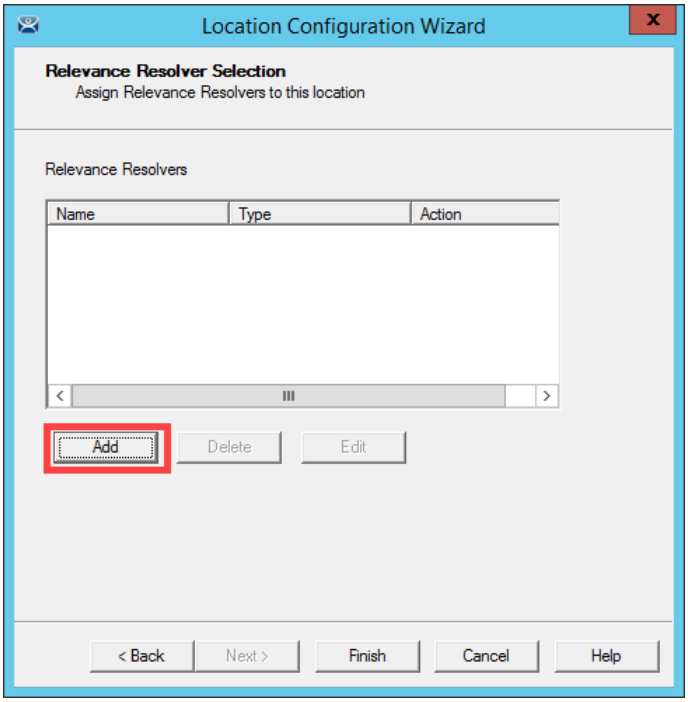
5. Click the **Next** button on the **Display Client Selection** page of the wizard.

> 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.

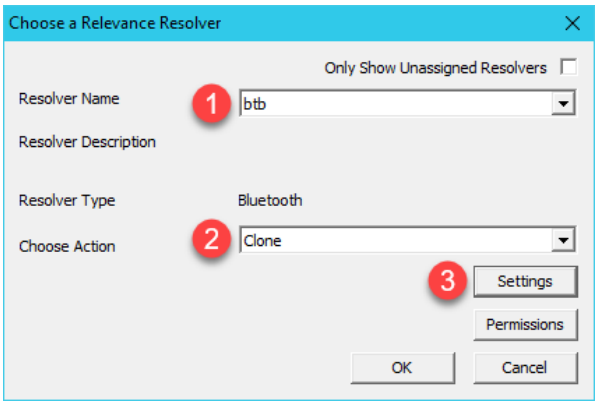
6. Click the **Next** button on the **Windows Log In Information** page of the wizard.

> Since we have not assigned a Display Client to this Location, we don't need to provide Login Credentials.

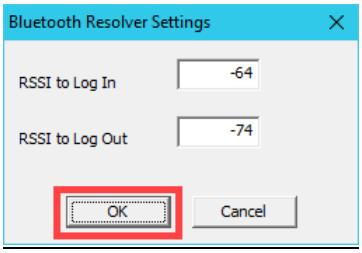
7. Click the **Add** button from the **Relevance Resolver Selection** page of the wizard.



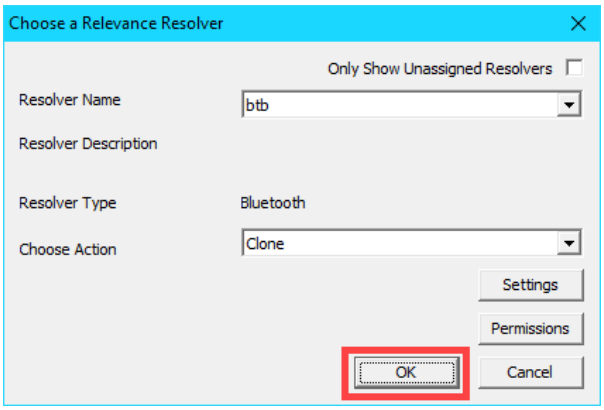
8. Select **btb** from the **Resolver Name** drop down list and **Clone** from the **Choose Action** page of the wizard. Click the **Settings** button.



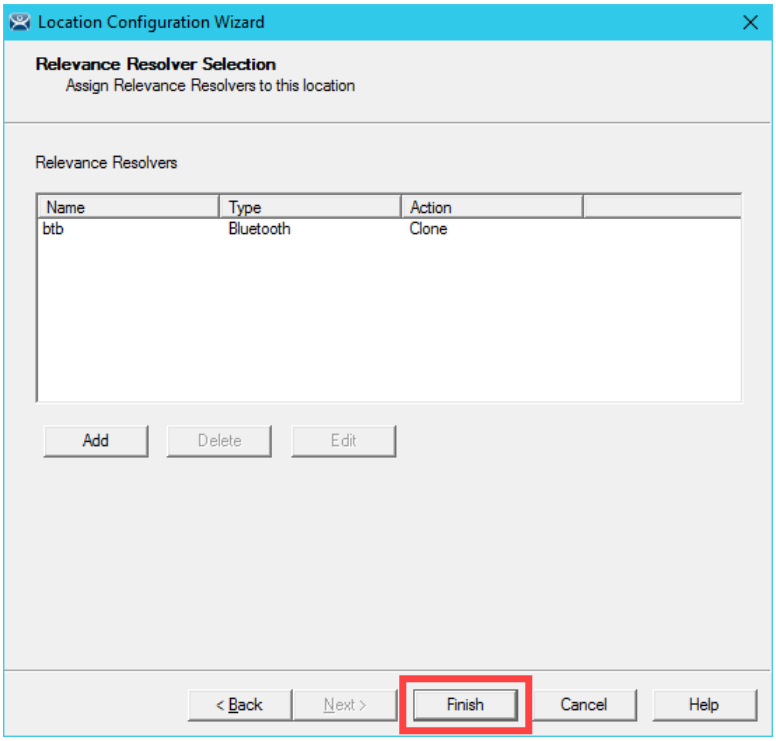
9. The **RSSI to Log In** value is the one captured when you registered the Beacon. The **RSSI to Log Out** is just 10 less than the **RSSI to Log In.** For the purposes of this lab, do not change the values. Click the **OK** button.



10. Click the **OK** button again.



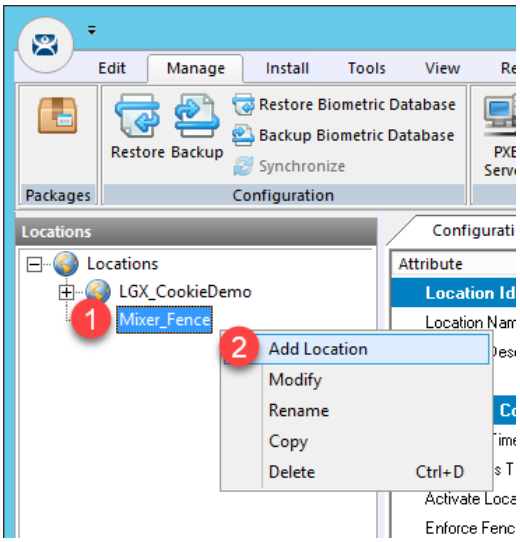
11. Click the **Finish** button.



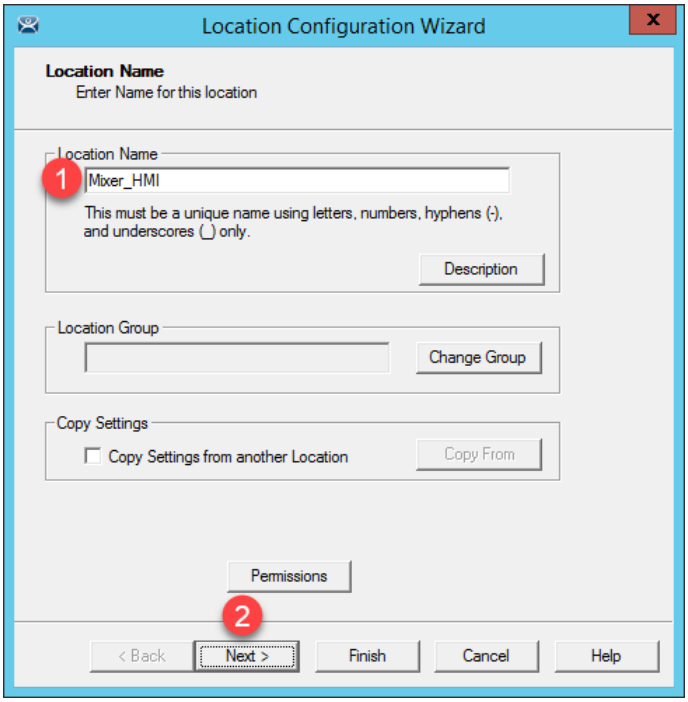
Create Child Location

We will assign the **CookieDemo Display Client** to the **Child Location** and the **QR Code Location Resolver** we just registered.

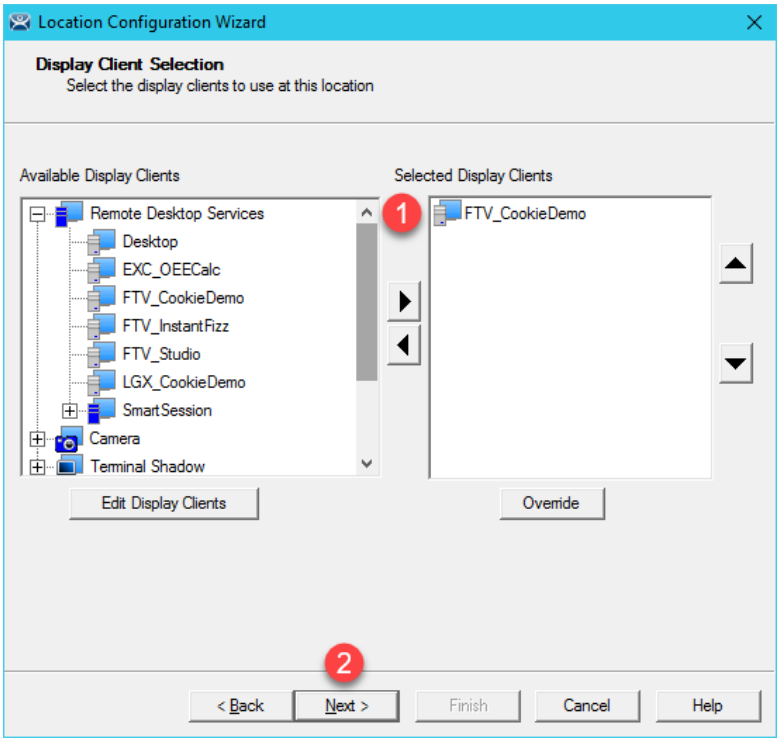
1. Right click the **Mixer_Fence** location and select the **Add Location** item.



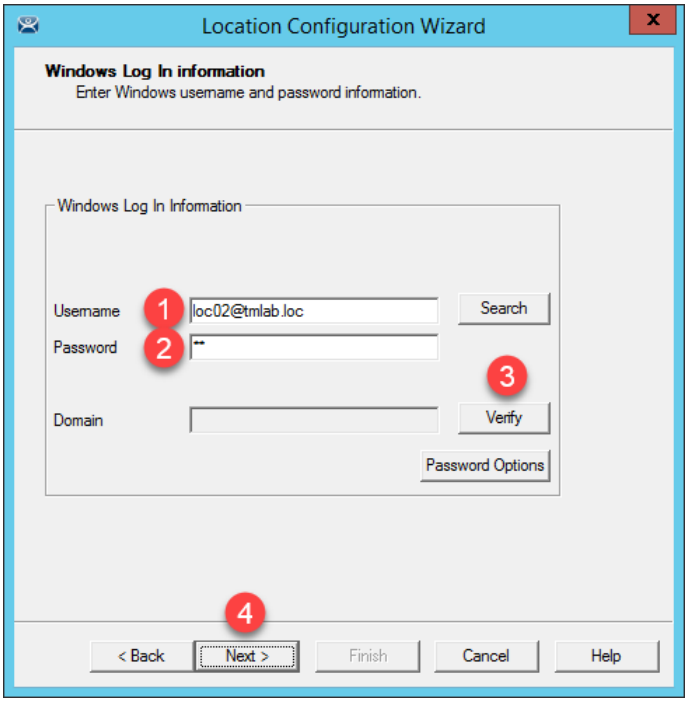
2. From the **Location Name** page of the **Location Configuration Wizard**, enter *Mixer_HMI* as the **Location Name**. Click the **Next** button.



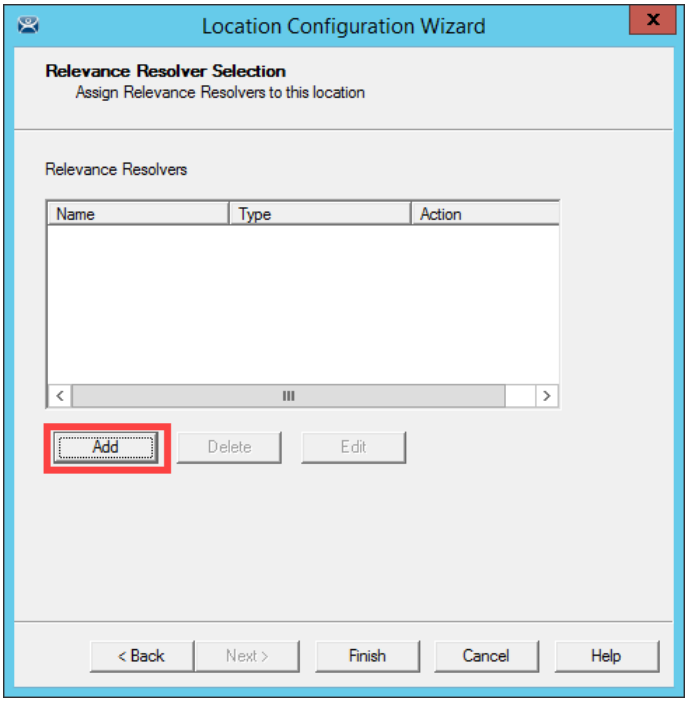
3. Click the **Next** button on the **Location Options** page of the wizard.
4. From the **Display Client Selection** page of the wizard, remove all existing **Display Clients** and move the **FTV_CookieDemo Display Client** to the **Selected Display Clients** list. Click the **Next** button.



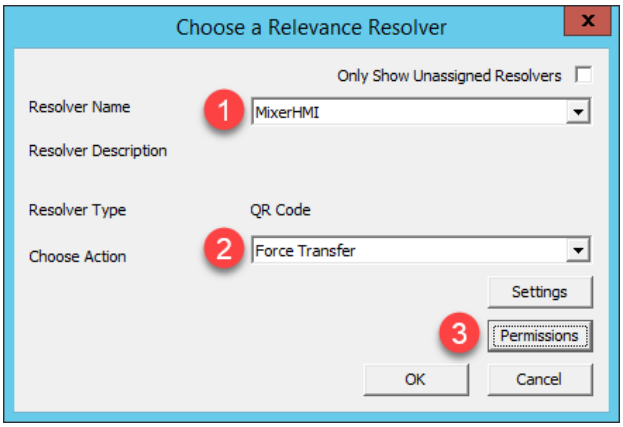
5. From the **Windows Log In Information** page of the wizard, enter *loc02@tmlab.loc* as the **Username** and *rw* as the **Password**. Click the **Verify** button to validate the credentials entered. Click the **Next** button.



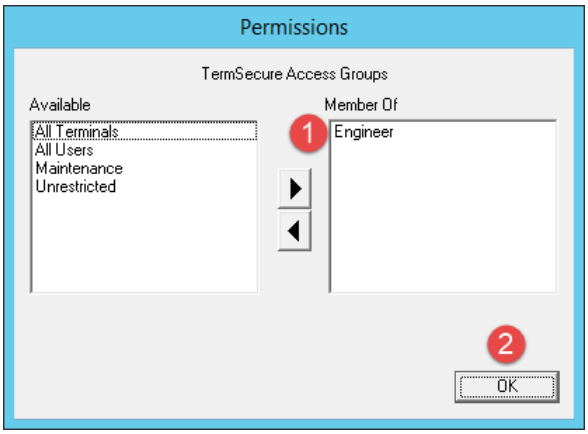
6. From the **Relevance Resolver Selection** page of the wizard, click the **Add** button.



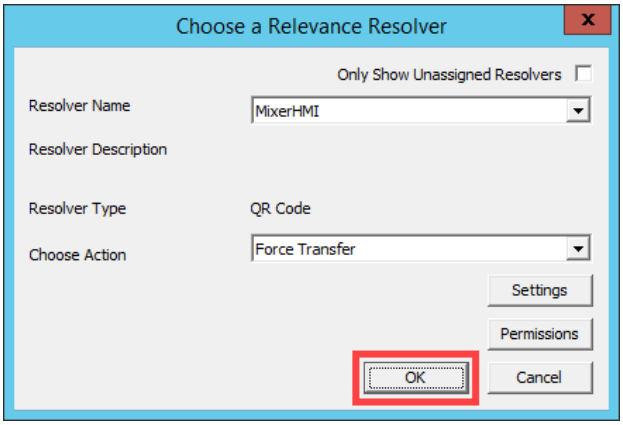
7. Select **MixerHMI** as the **Resolver Name** and **Force Transfer** as the **Choose Action**. Click the **Permissions** button.



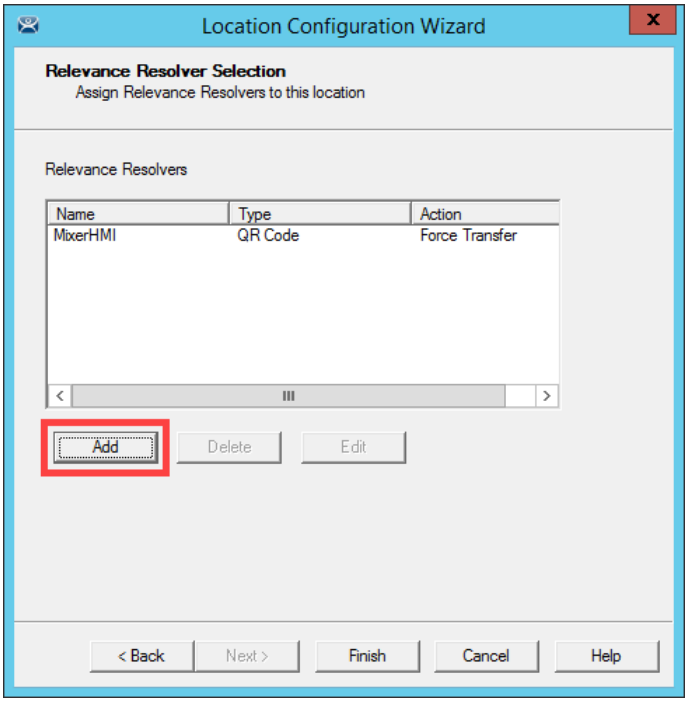
8. From the **Permissions** window, remove **Unrestricted** from the **Member Of** list and add **Engineer**. Click the **OK** button.



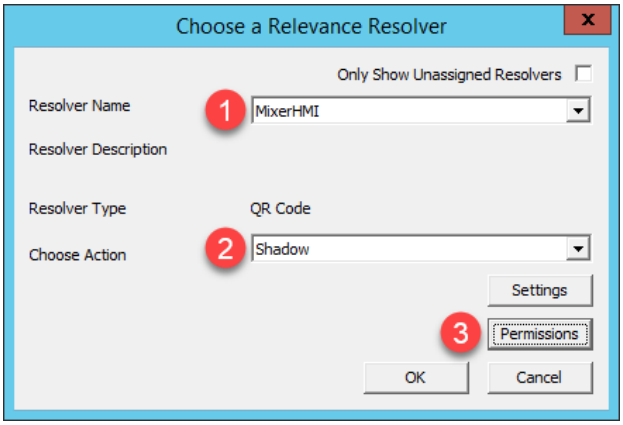
9. Click the **OK** button.



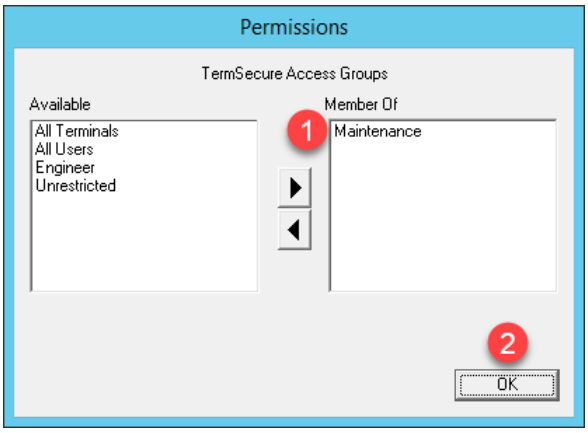
10. Click the **Add** button.



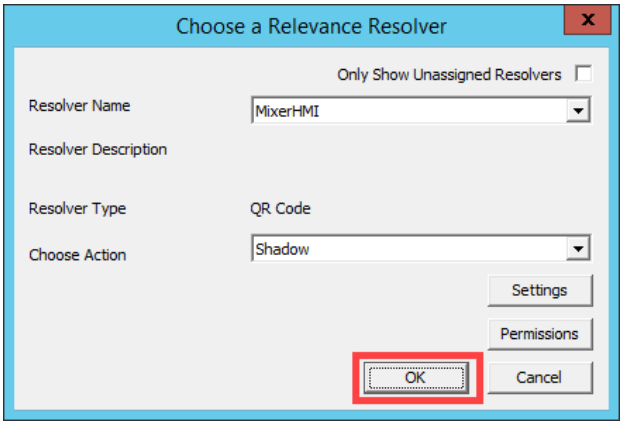
11. Select **MixerHMI** as the **Resolver Name** and **Shadow** as the **Choose Action**. Click the **Permissions** button.



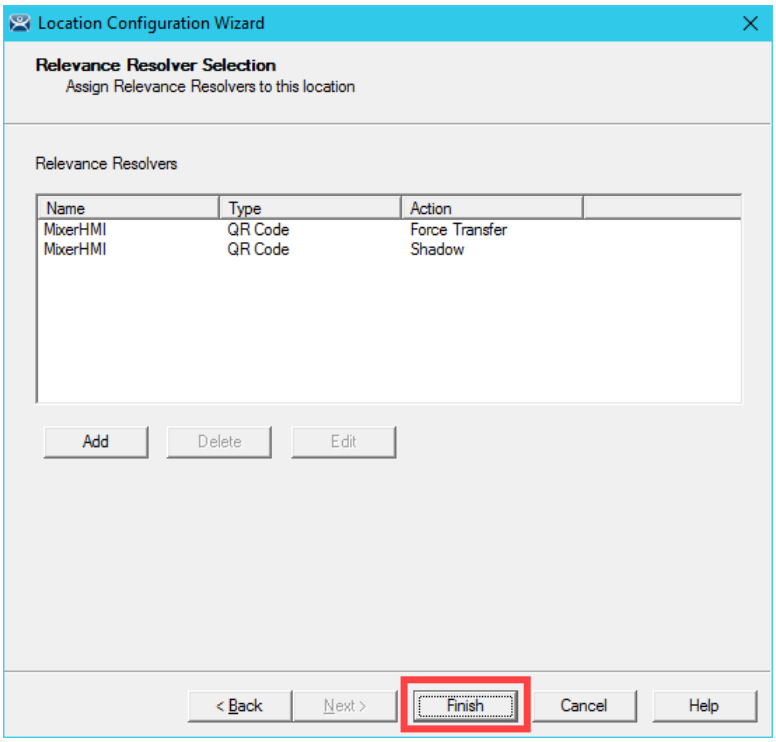
12. From the **Permissions** window, remove **Unrestricted** from the **Member Of** list and add **Maintenance**. Click the **OK** button.



13. Click the **OK** button.



14. Click the **Finish** button.



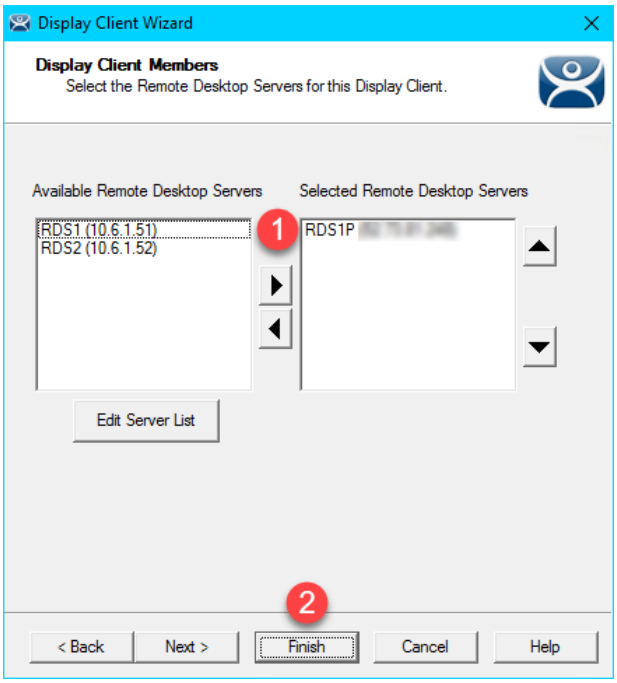
Reassign Display Client to Public Display Server

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.

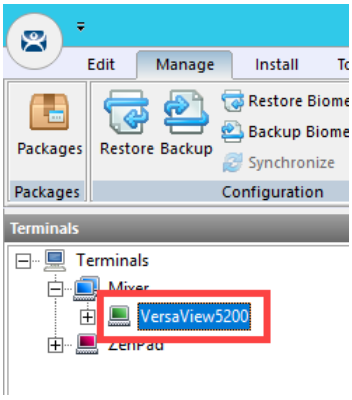
7. From the **Display Client Members** page of the wizard, remote **RDS2** from the **Selected Remote Desktop Servers** list box and add **RDS1P** instead. Click the **Finish** button.



Assign Default Location to Terminal

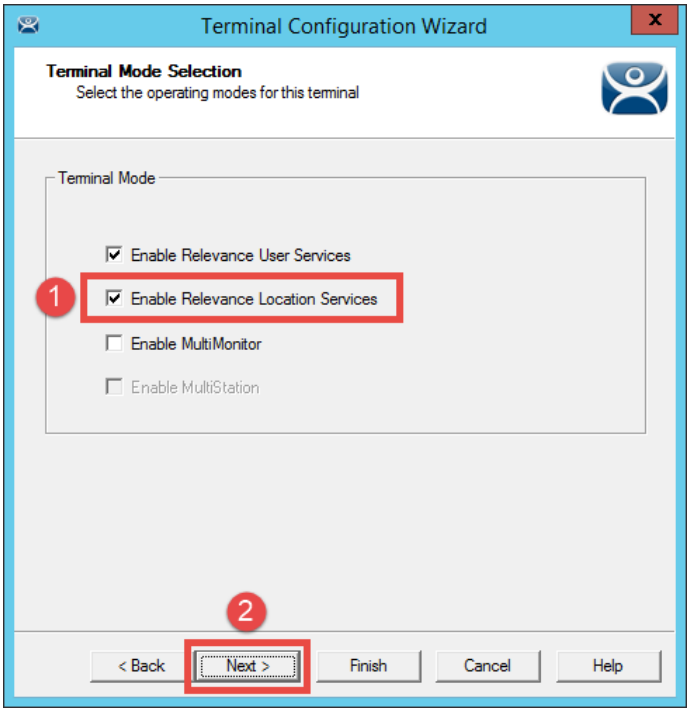
1. Click the **Terminals** tree selector icon.

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

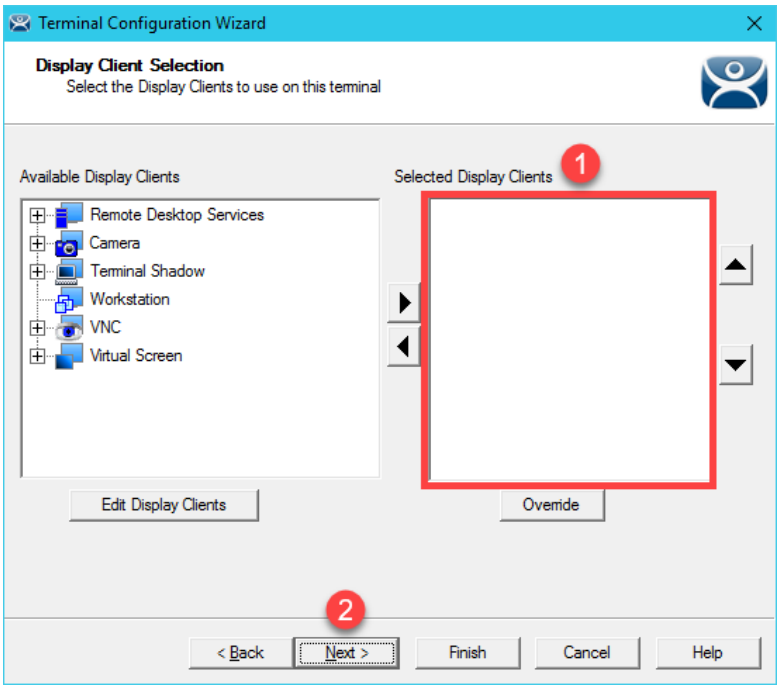


3. Click the **Next** button on the **Terminal Name** page of the wizard.
4. Click the **Next** button on the **Terminal Hardware** page of the wizard.
5. Click the **Next** button on the **Terminal Options** page of the wizard.

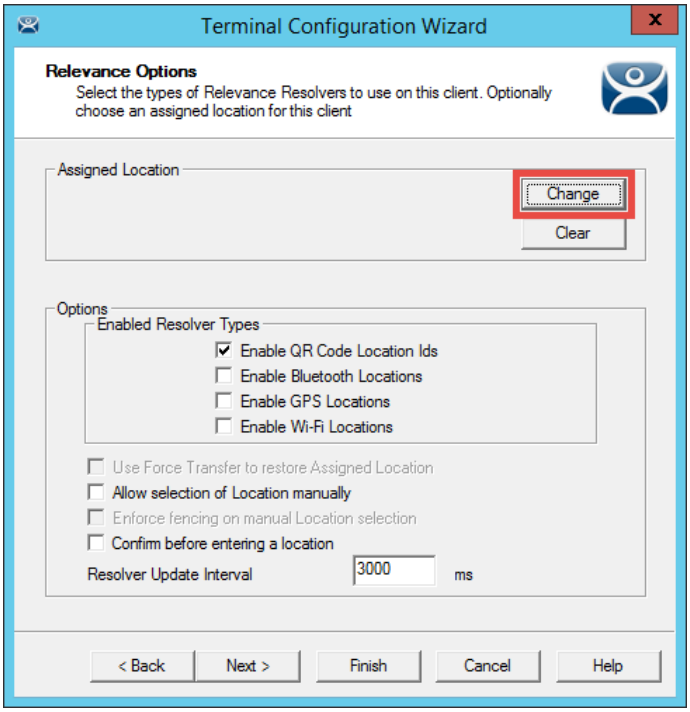
6. From the **Terminal Mode Selection** page of the wizard, make sure **Enable Relevance User Services** is checked. Also check the **Enable Relevance Location Services**. This is required to use this **Terminal** with **Relevance**. Click the **Next** button.



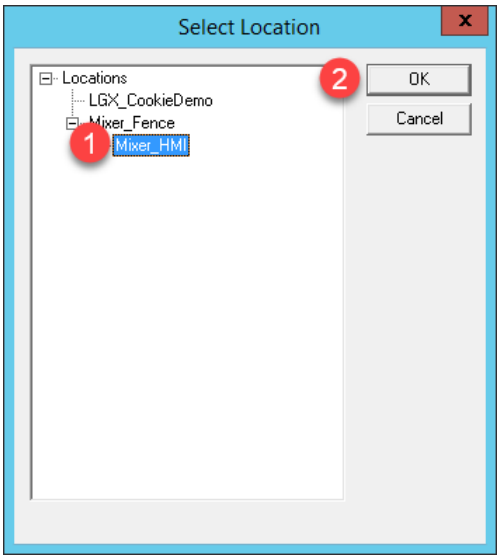
7. Ensure all **Display Clients** are removed from the **Selected Display Clients** list. Click the **Next** button.



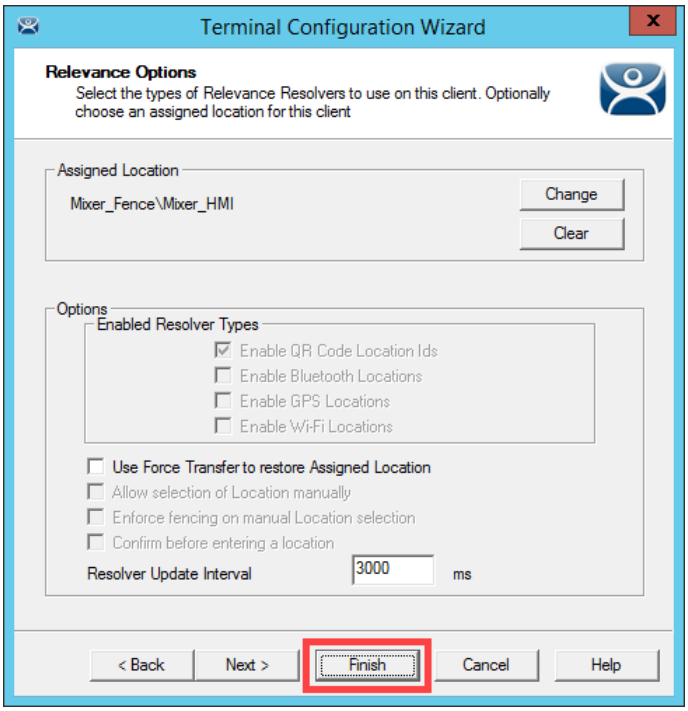
8. From the **Terminal Interface Options** page of the wizard, click the **Next** button.
9. From the **Relevance Options** page of the wizard, click the **Change** button.



10. From the **Select Location** popup, select **Mixer_HMI**. Click the **OK** button.



11. Click the **Finish** button.



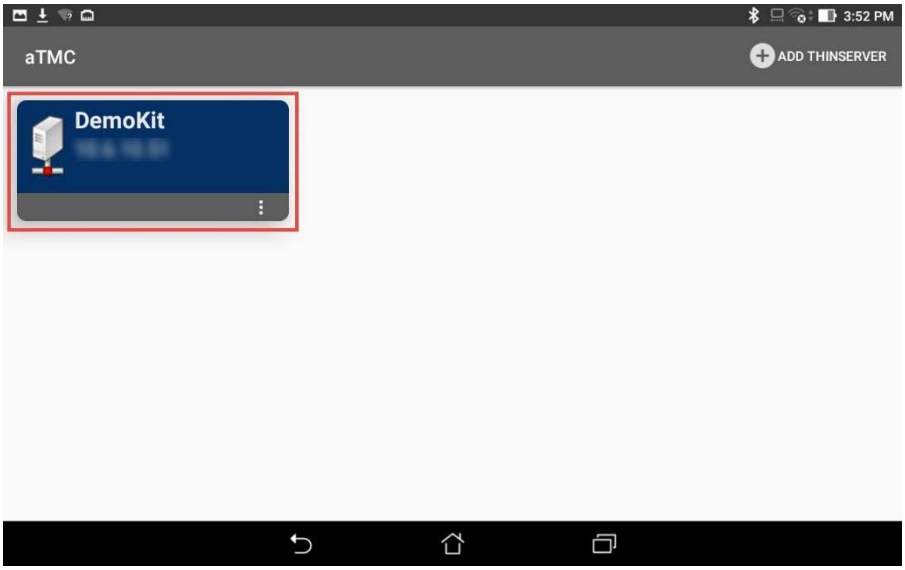
Notice the **Allow selection of Location manually** checkbox. With this checked, the **Terminal** to which this profile is assigned will be able to manually login to **Locations** that permit this action. In this scenario, if the **Enforce fencing on manual Location selection** is not checked, then the **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.

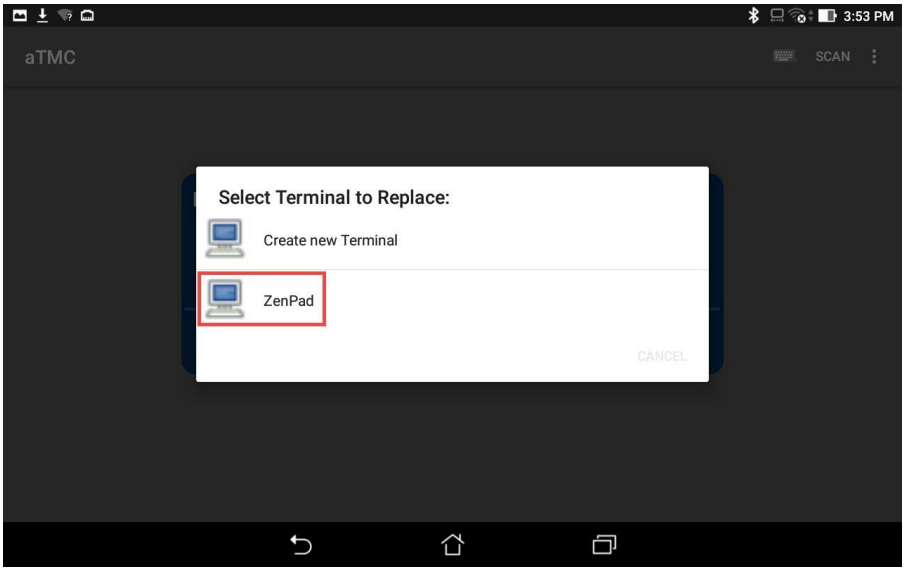
After restarting the **Terminal**, you will notice that the **FTV_CookieDemo** application is still delivered to the virtual thin client. This is because we assigned the **FTV_CookieDemo Display Client** to the **Mixer_HMI Location** and then assigned this **Location** to the **VersaView5200 Terminal**. 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

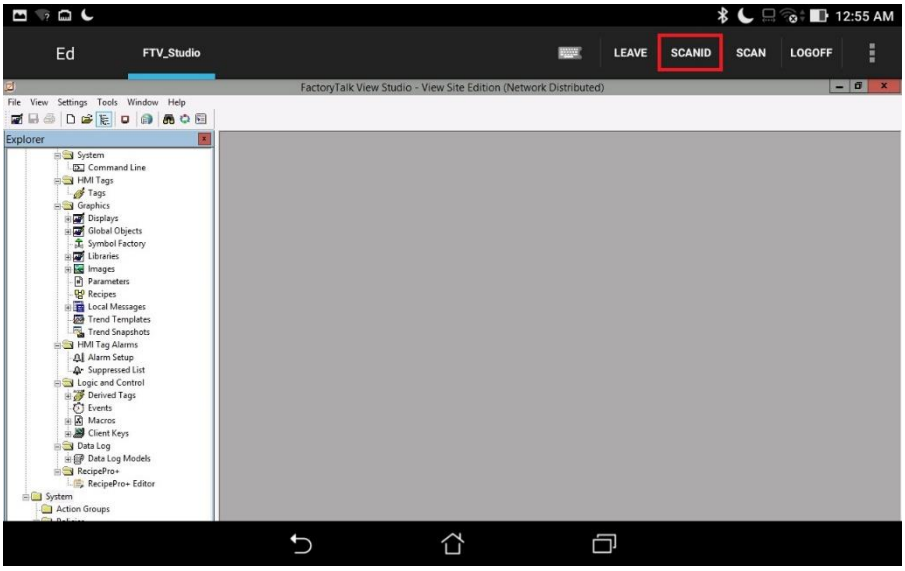
1. Return to **aTMC** on your mobile device. If so, you may also have to reconnect **aTMC** to the **DemoKit** server listed.



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).

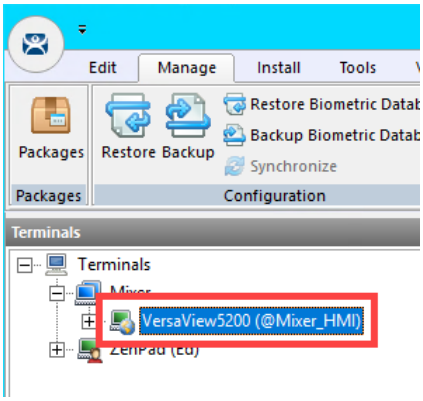
5. Since you are logged in as a member of the **Engineer** group, you should see the **CookieDemo Display Client** transferred from the virtual thin client and delivered to the tablet. However, you should only be able to keep this **Display Client** while within the **geo-fence** established by the **Bluetooth 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

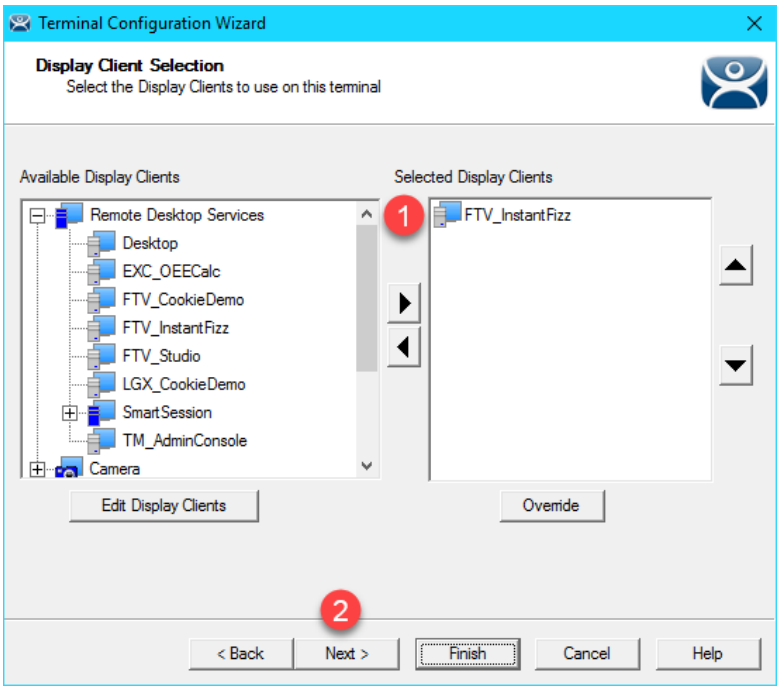
1. Click the **Terminals** tree selector icon.

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

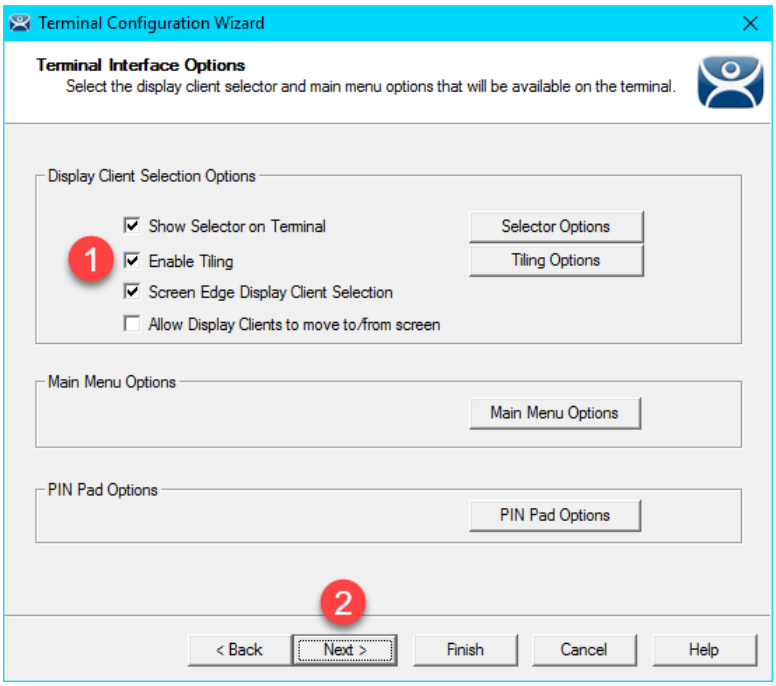


3. Click the **Next** button on the **Terminal Name** page of the wizard.
4. Click the **Next** button on the **Terminal Hardware** page of the wizard.
5. Click the **Next** button on the **Terminal Options** page of the wizard.
6. Click the **Next** button on the **Terminal Mode Selection** page of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

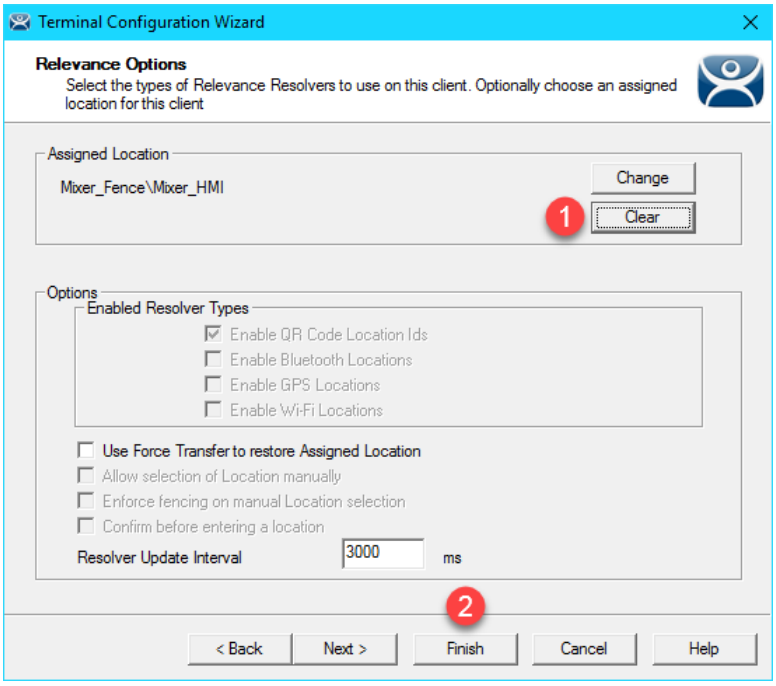
7. Assign **FTV_InstantFizz** to the **Select Display Clients** listbox. Click the **Next** button.



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 9: 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.

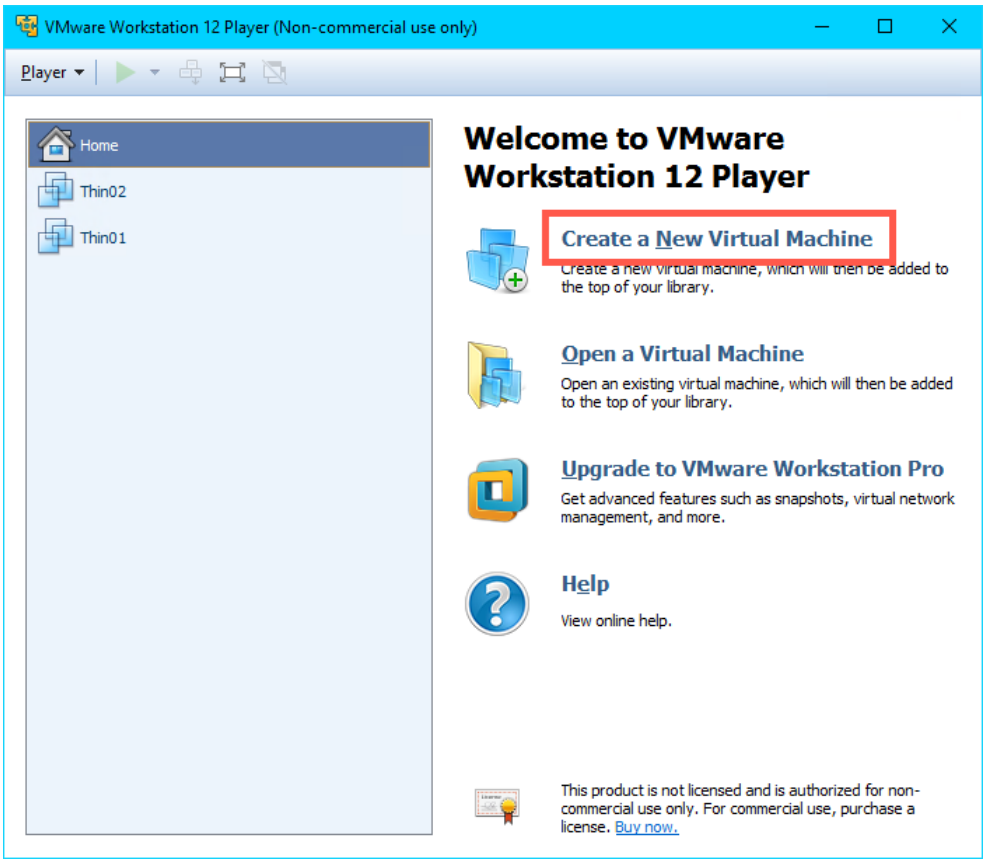
1. Create Virtual Thin Client
2. Modify PXE Server Mode
3. Create Terminal for Virtual Thin Client
4. Re-Enable Firewall Rules
5. Start Wireshark Capture
6. Troubleshoot the Boot Process
7. Boot Virtual Thin Client via UEFI

Create Virtual Thin Client

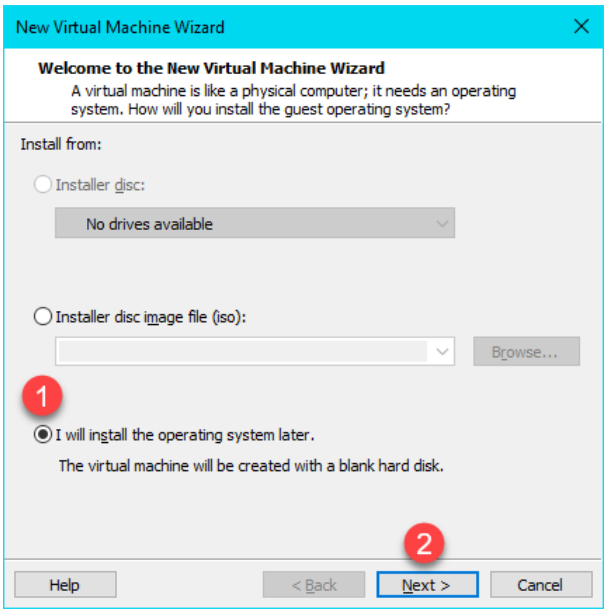
As demonstrated through this Cloud lab, a virtual thin client is fairly simple to create and can be a great tool for troubleshooting, testing and education. In this section, we will use VMWare's free Workstation Player to create a new virtual machine without an Operating System, which we will subsequently boot via ThinManager's PXE Server.

1. Double click the **VMWare Player** shortcut on the **RDS1** desktop.

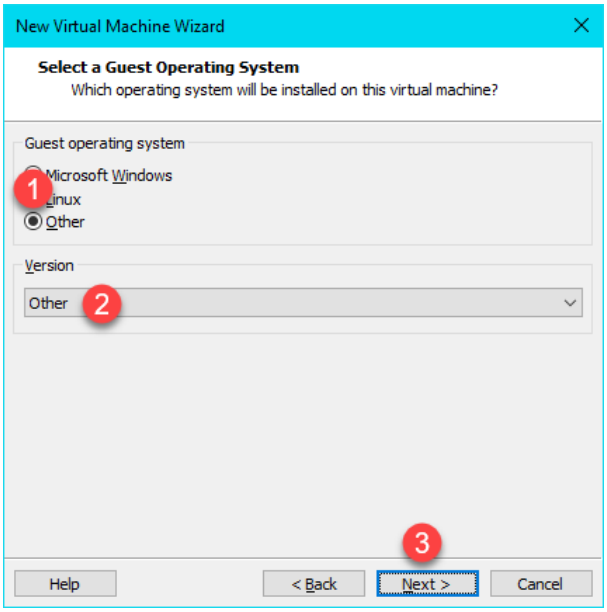
2. From **VMWare Workstation Player** click the **Create a New Virtual Machine** link.



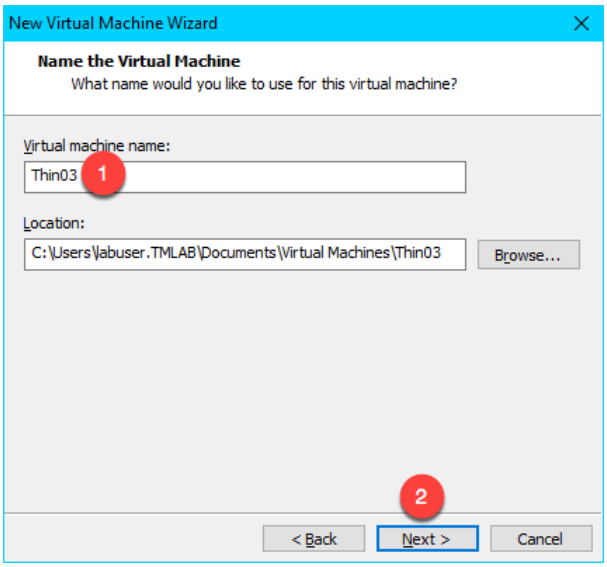
3. From the **New Virtual Machine Wizard**, select the **I will install the operating system later** radio button. Click the **Next** button.



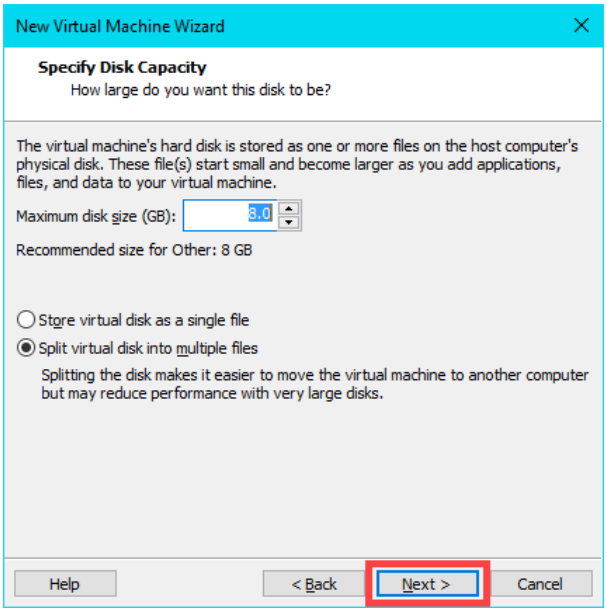
4. From the **Select a Guest Operating System** page of the wizard, select the **Other** radio button, **Other** from the **Version** drop down list and click the **Next** button.



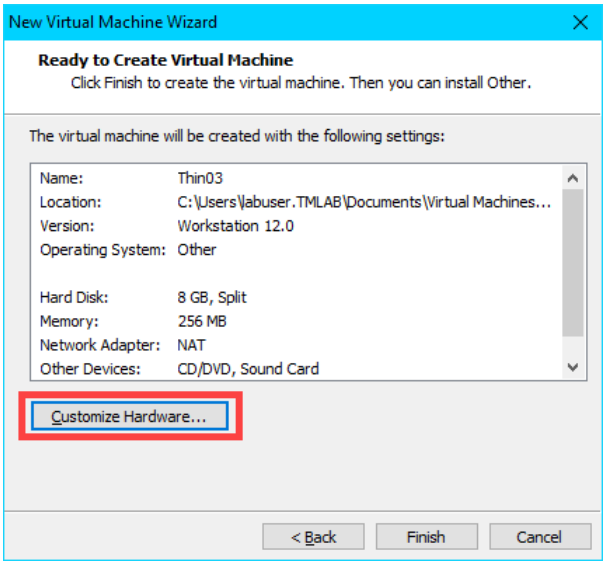
5. From the **Name the Virtual Machine** page of the wizard, enter *Thin03* as the **Virtual machine name**. You can leave the default **Location**. Click the **Next** button.



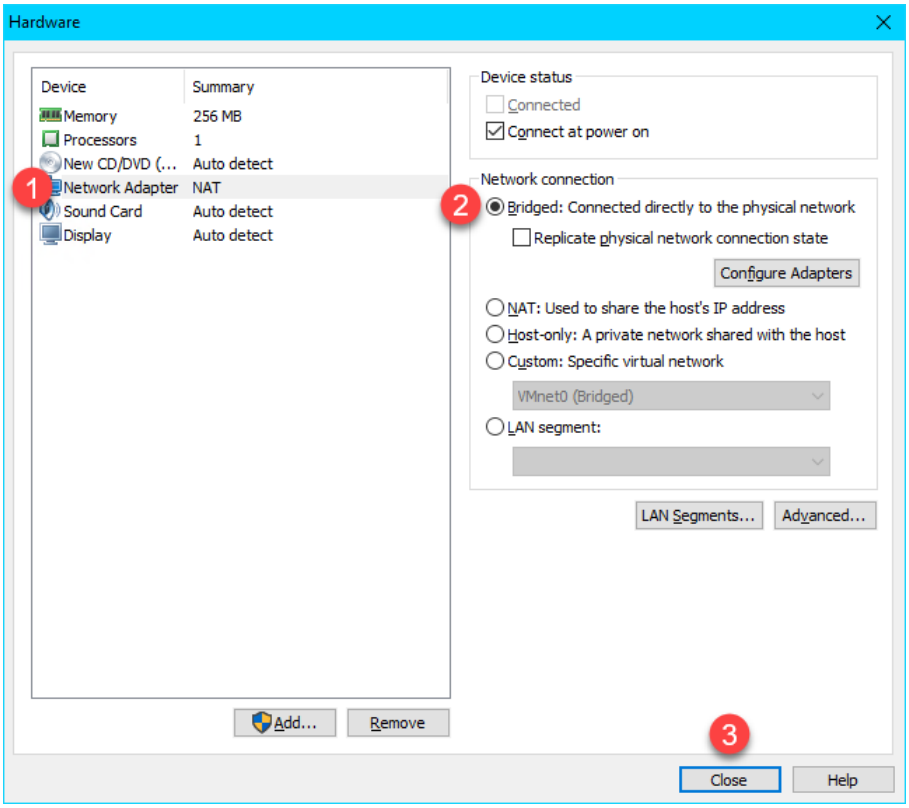
6. Click the **Next** button on the **Specify Disk Capacity** page of the wizard, keeping the defaults.



7. Click the **Customize Hardware** button on the **Ready to Create Virtual Machine** page of the wizard.

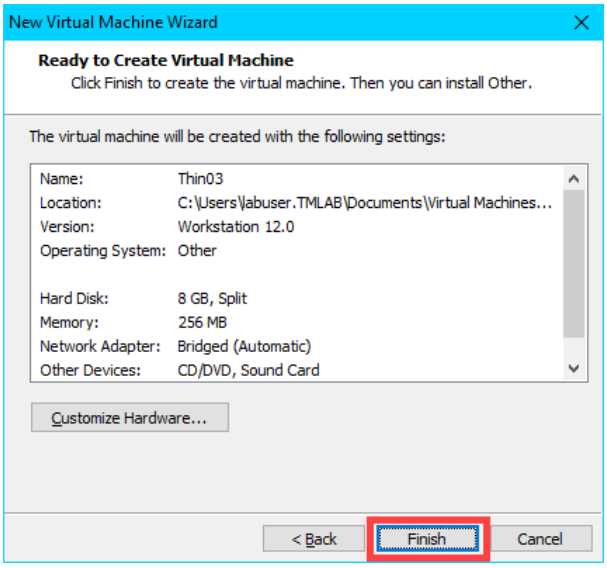


8. From the **Hardware** window, select the **Network Adapter** device and click the **Bridged** radio button. Click the **Close** button.



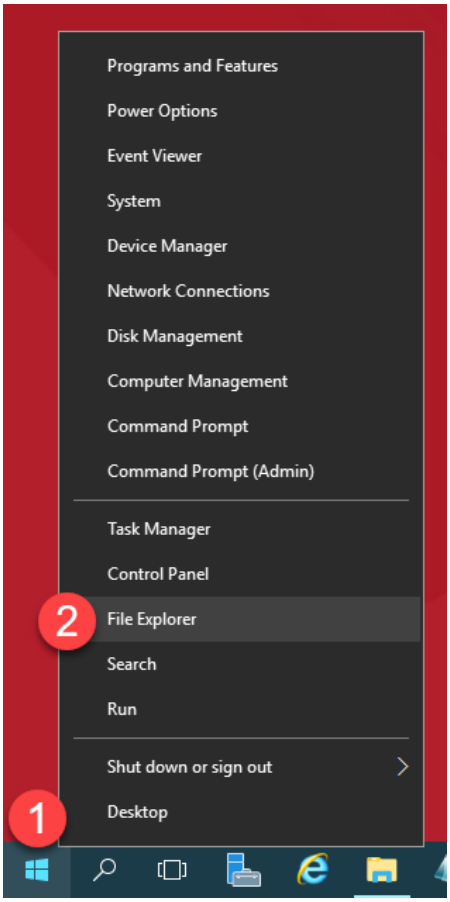
We have been using NAT for our virtual thin clients to this point in the lab. We will switch to Bridged in this section so we can see the desired network traffic in Wireshark. With that said, we will need to modify our PXE Server settings so that ThinManager will issue IP addresses for PXE requests.

9. Back at the **Ready to Create Virtual Machine** page of the wizard, click the **Finish** button.

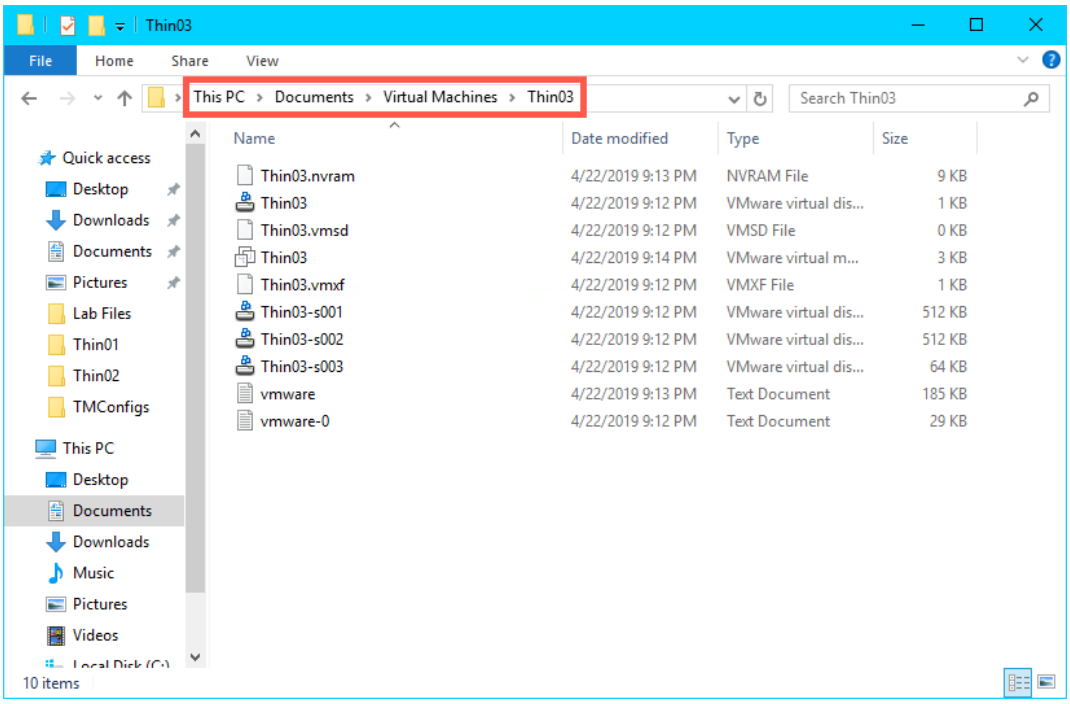


The default 8GB of hard disk space and 256MB RAM is plenty for our virtual thin client.

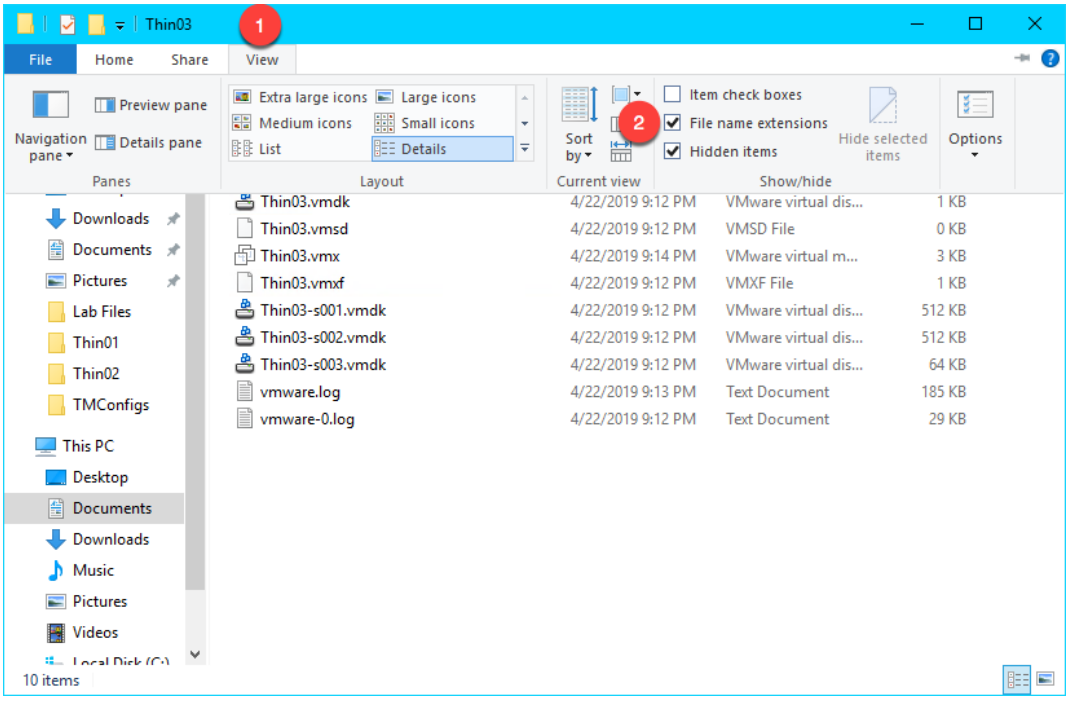
10. Because this virtual thin client is running on a virtual machine (**RDS1**), which is referred to as **nesting**, we need to add a special setting to the virtual machine configuration file for **Thin03**. Right click the **Windows Start Button** and select **File Explorer**.



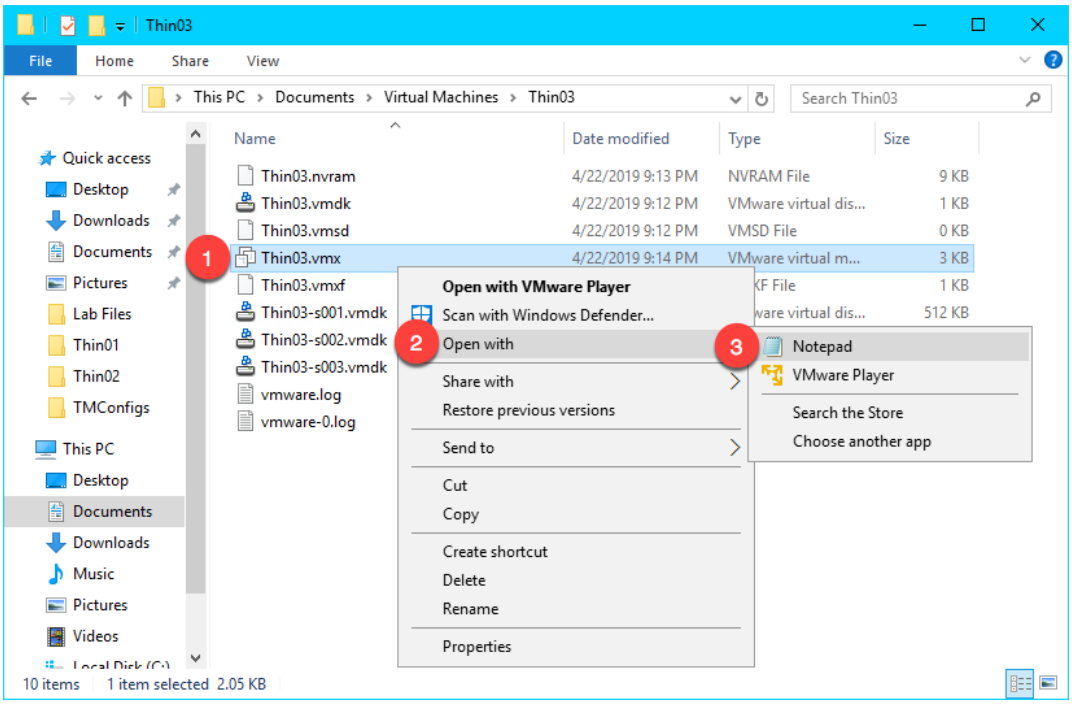
11. Within **File Explorer**, navigate to **Documents->Virtual Machines->Thin03.**



12. Click the **View** menu item and check the **File name extensions** checkbox.

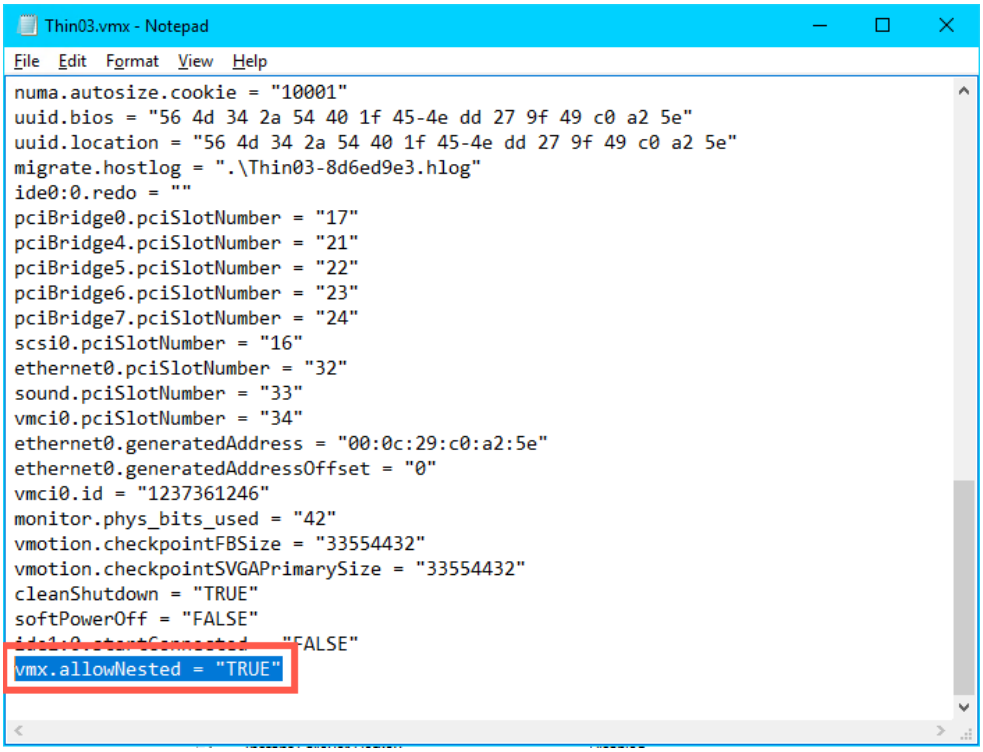


13. Right click **Thin03.vmx** and select **Open with…**



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**.

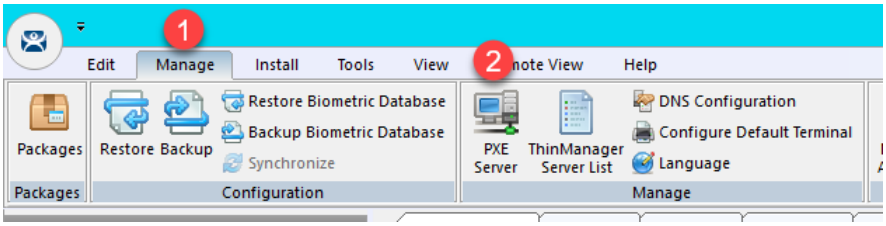
```
vmx.allowNested = "TRUE"
```



Again, the **vmx.allowNested = "TRUE"** setting is only required if you are running your virtual thin client on a virtual host.

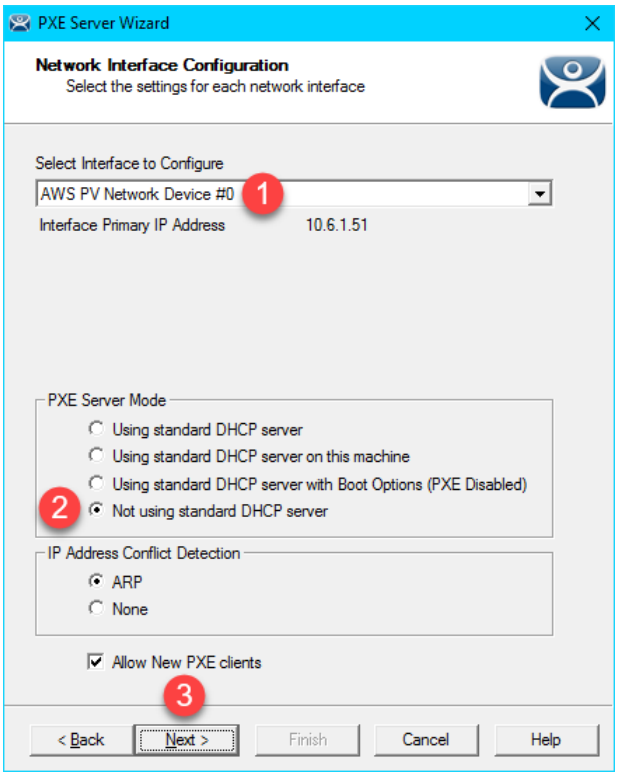
Modify PXE Server Mode

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

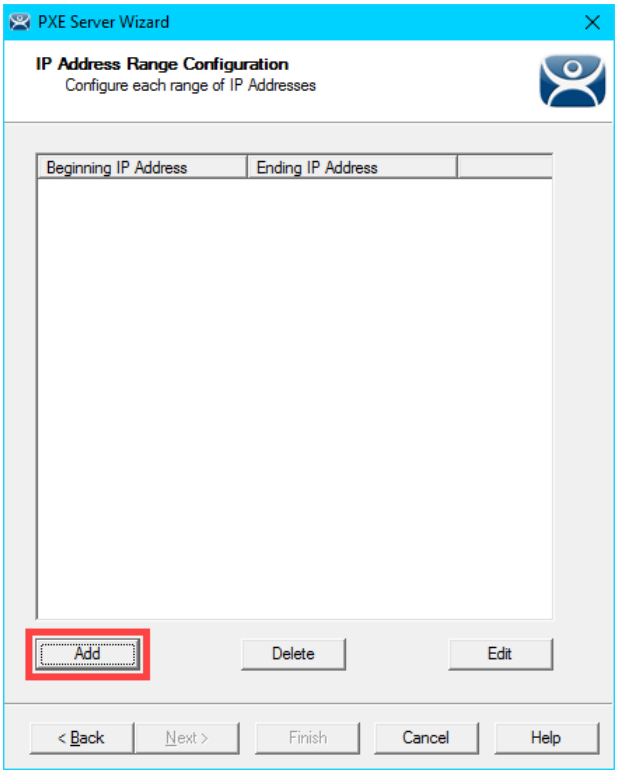


2. Click the **Next** button from the **PXE Server Configuration** page of the wizard.

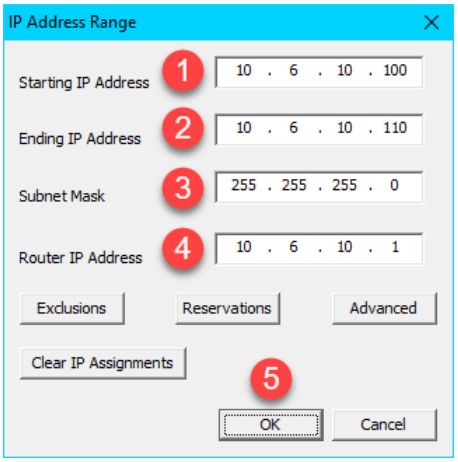
3. From the **Network Interface Configuration** page of the wizard, select **AWS PV Network Device #0** from the **Select Interface to Configure** drop down list, and select the **Not using standard DHCP server** option button. Click the **Next** button.



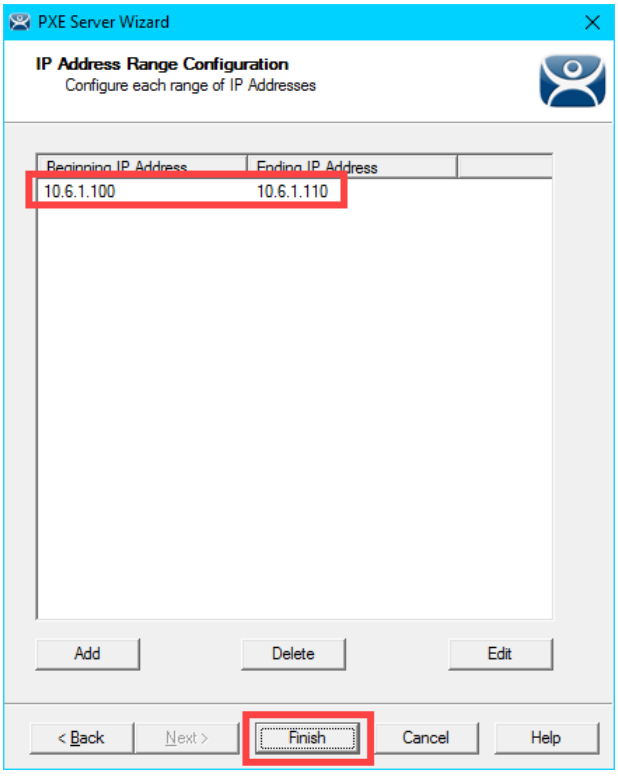
4. From the **IP Address Range Configuration** page of the wizard, click the **Add** button.



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.

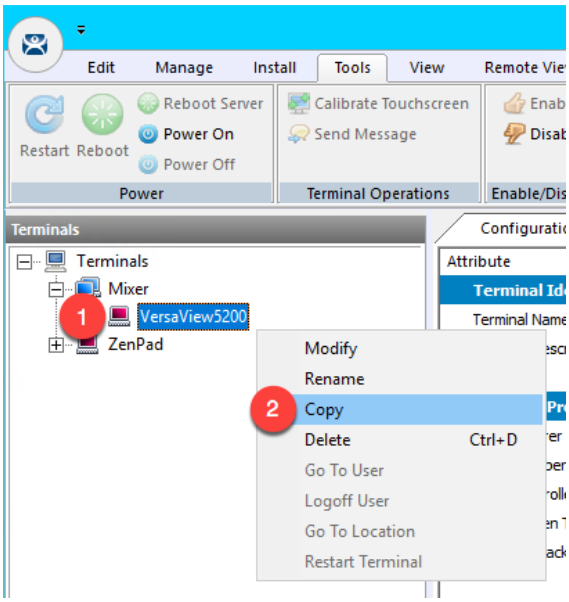


Create Terminal for Virtual Thin Client

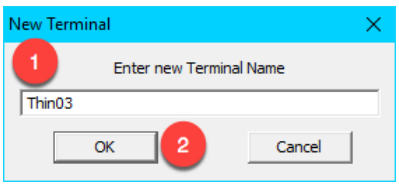
We will create a new **ThinManager Terminal Profile** to assign to our **Virtual Thin Client**.

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

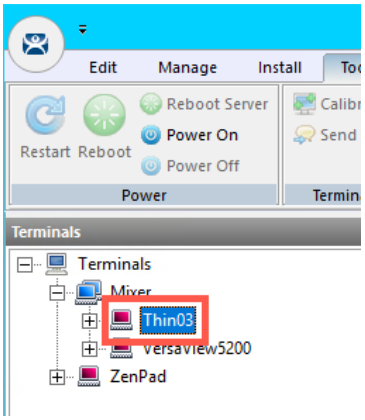
3. From the **Terminals** tree, right click the **VersaView5200** terminal and select **Copy** terminal and select **Copy**.



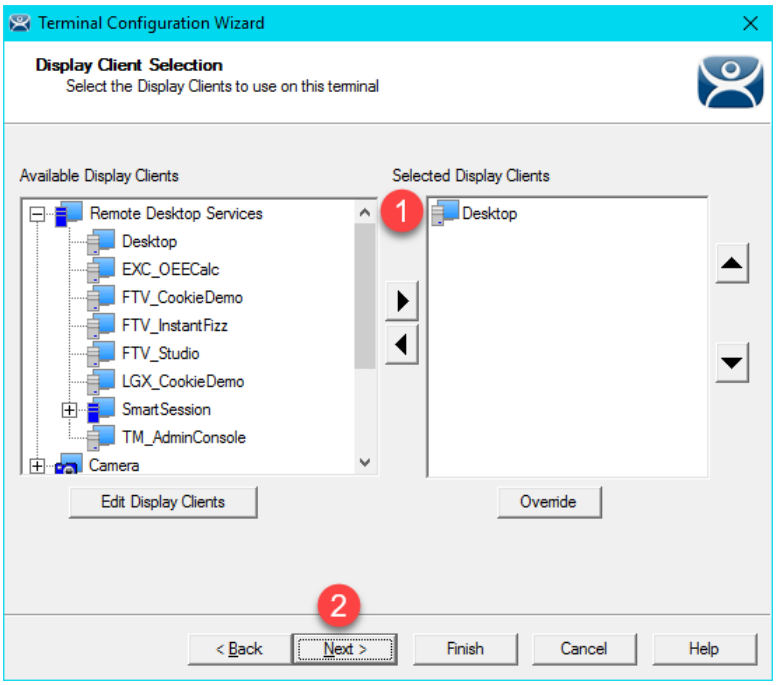
4. Enter *Thin03* as the new **Terminal Name** and click the **OK** button.



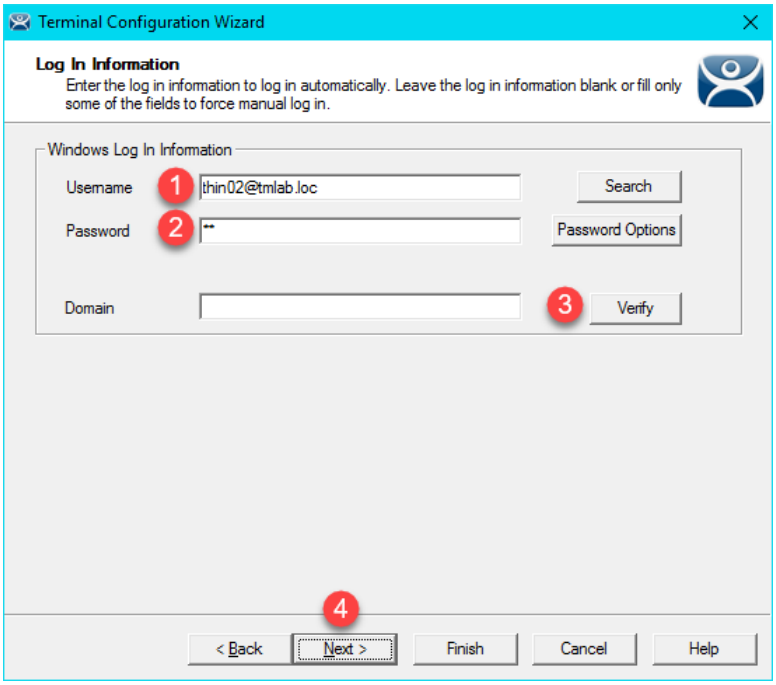
5. With the new terminal created, double click the **Thin03** terminal to launch the **Terminal Configuration Wizard**.



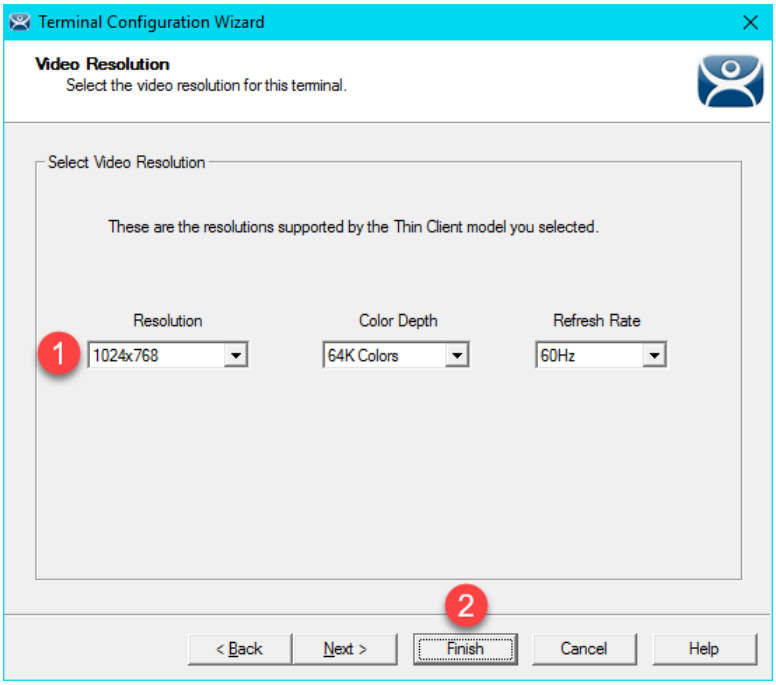
6. Click the **Next** button on the **Terminal Name** page of the wizard.
7. Click the **Next** button on the **Terminal Hardware** page of the wizard
8. Click the **Next** button on the **Terminal Options** page of the wizard.
9. Click the **Next** button on the **Terminal Mode Selection** page of the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



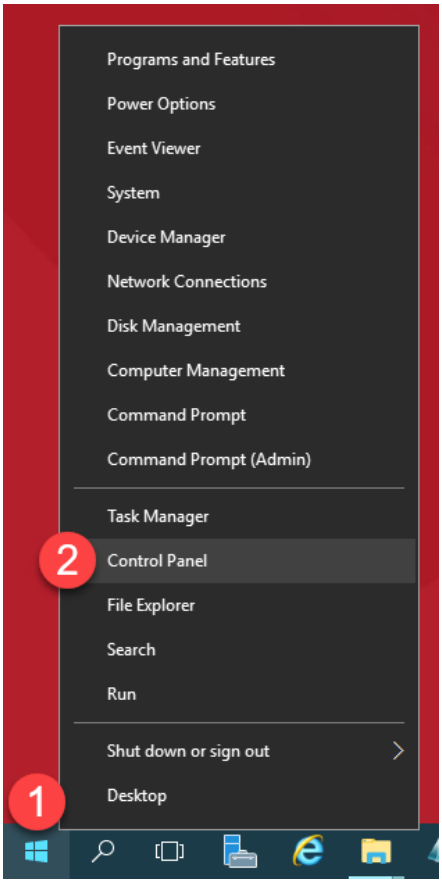
7. From the **Video Resolution** page of the wizard, select **1024x768** from the **Resolution** drop down list. Click the **Finish** button.



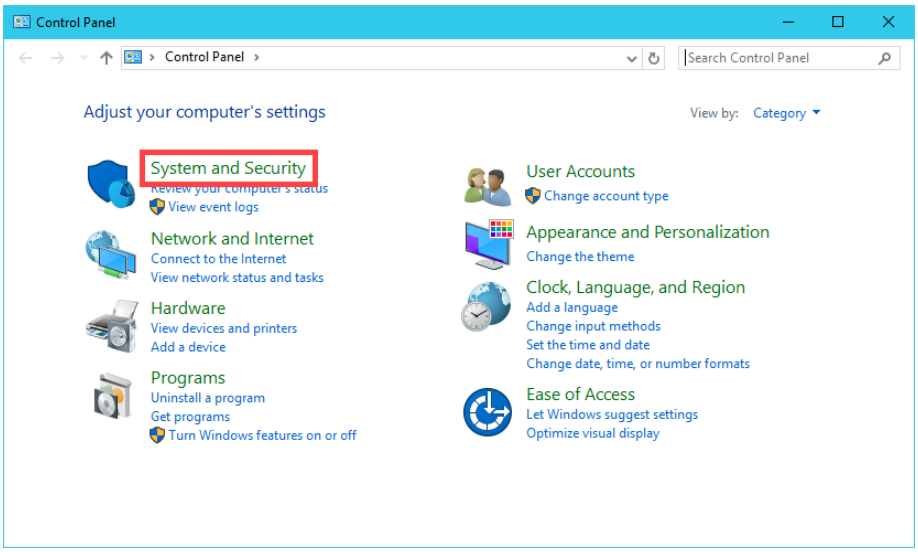
Re-enable Firewall Rules

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.

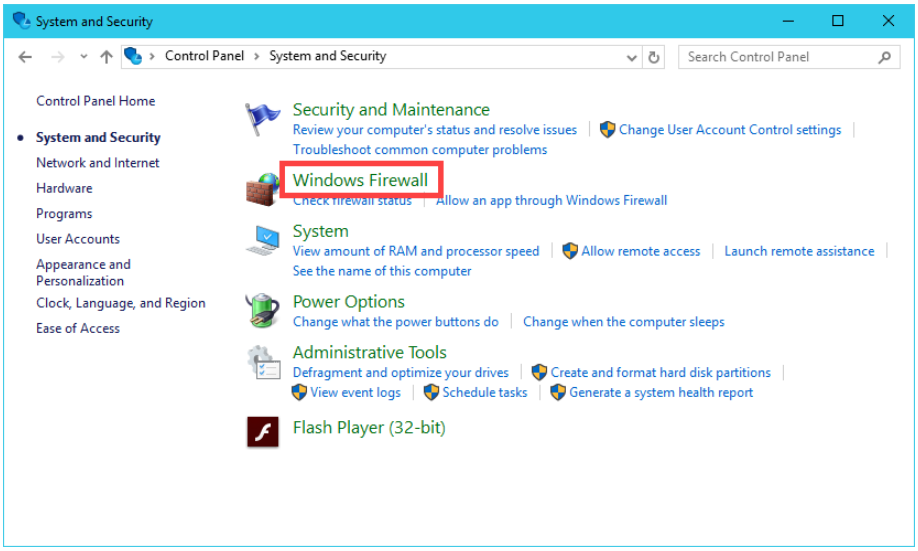
1. While still on **RDS1**, right click the **Windows Start Button** and select **Control Panel**.



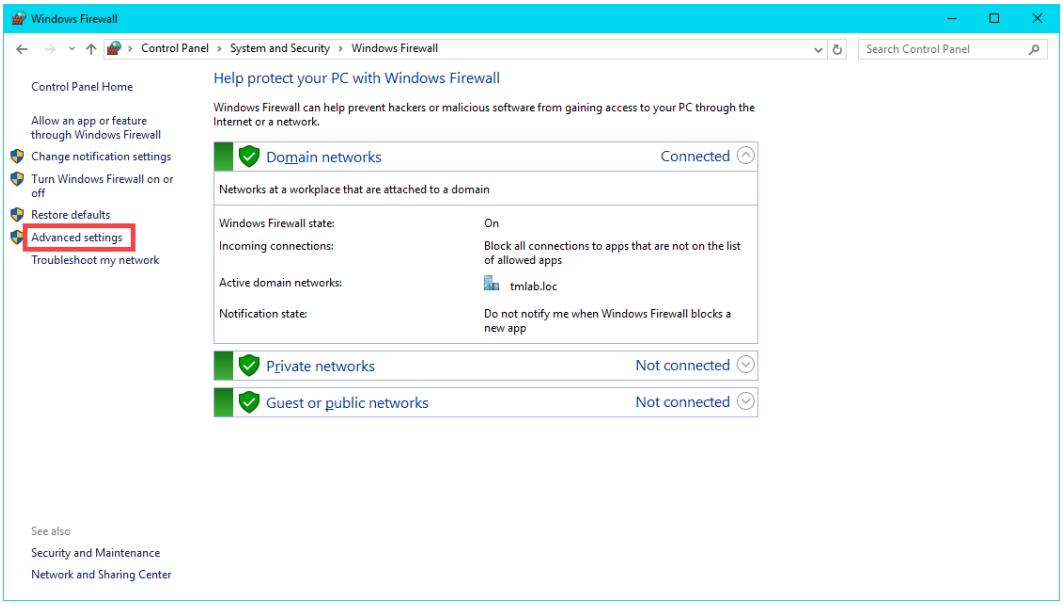
2. From the **Control Panel**, click the **System and Security** link.



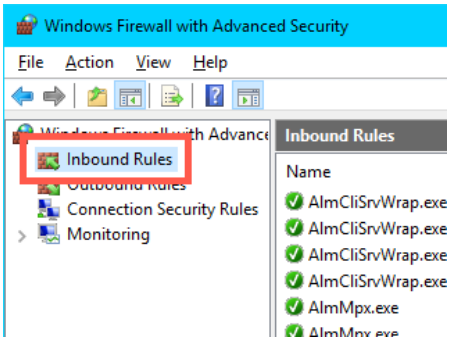
3. From the **System and Security** page of the **Control Panel**, click the **Windows Firewall** link.



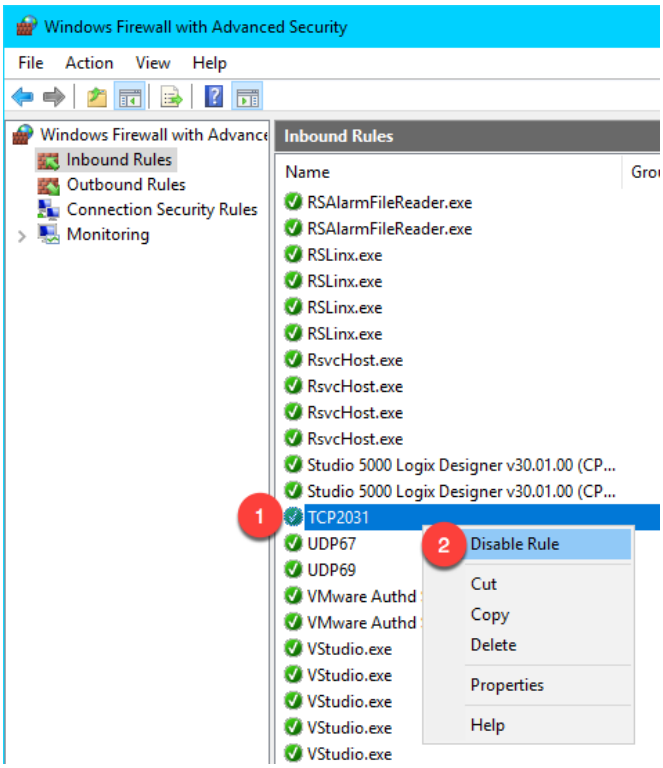
4. From the **Windows Firewall Control Panel**, click the **Advanced settings** link on the left hand side.



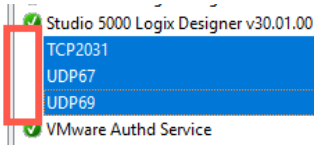
5. From the **Windows Firewall and Advanced Security** window, click the **Inbound Rules** item.



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.

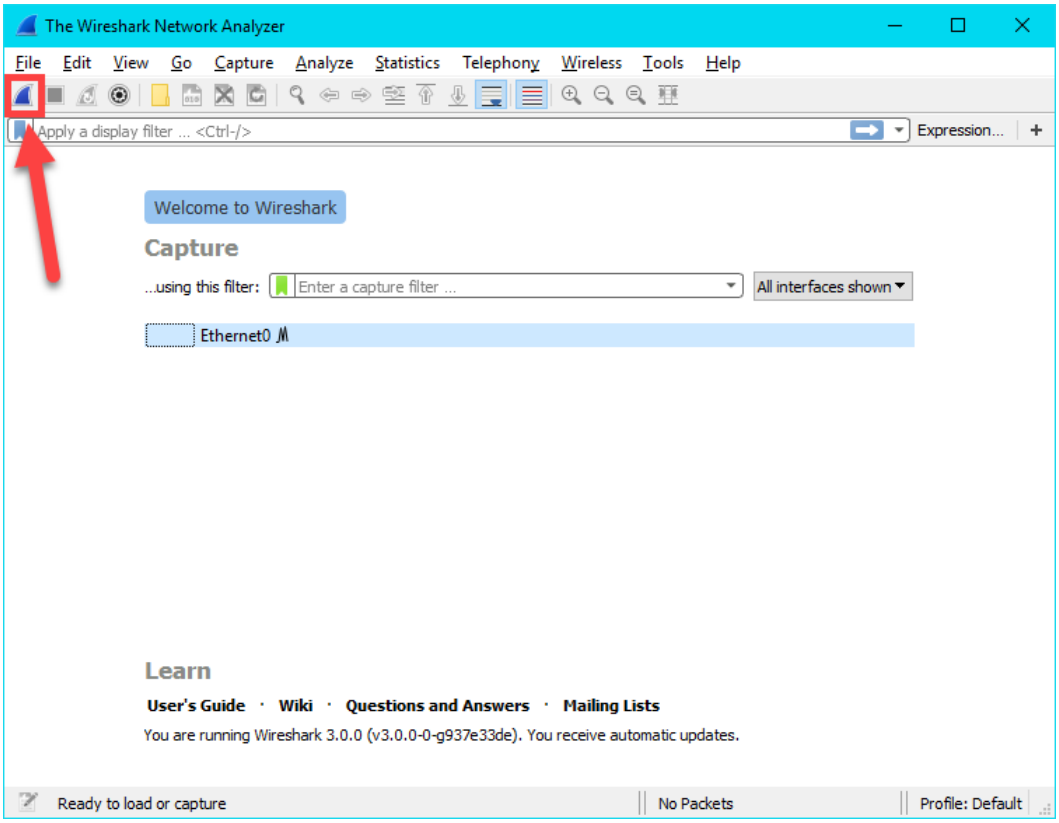


Start Wireshark Capture

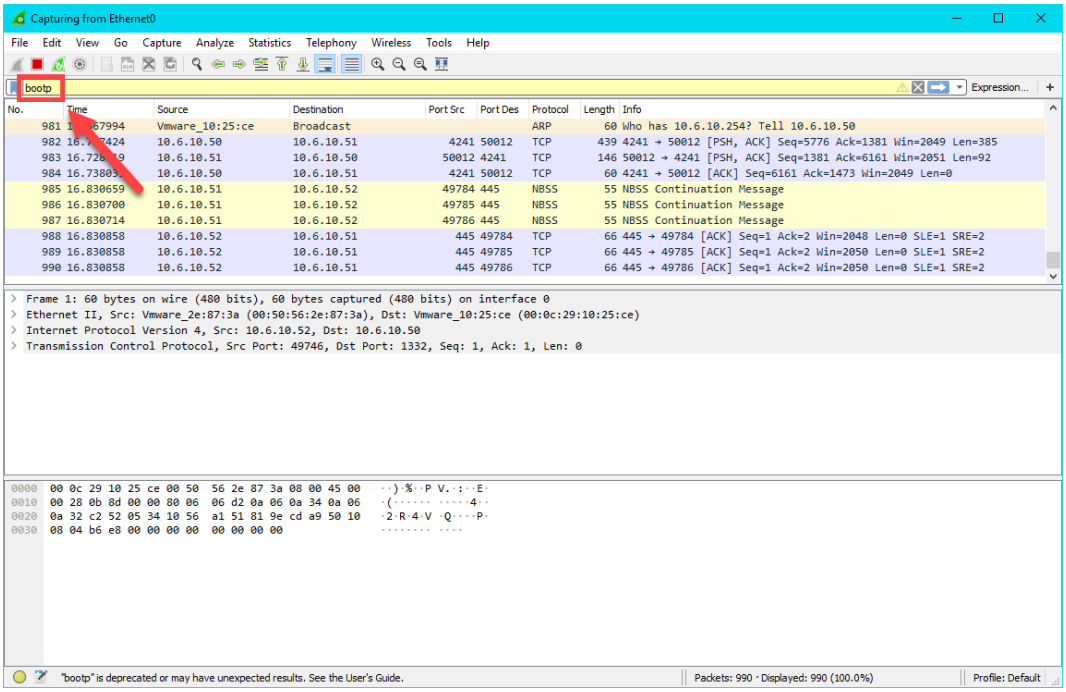
Wireshark is a free and open source packet analyzer. It is often used for network troubleshooting and is a tremendous help when diagnosing thin client boot issues. The ThinManager support team can generally pinpoint network issues by analyzing a Wireshark capture file.

1. Double click the **Wireshark** shortcut on the **RDS1** desktop.

2. Click the **Start Capturing Packets** icon in the **Wireshark** toolbar.

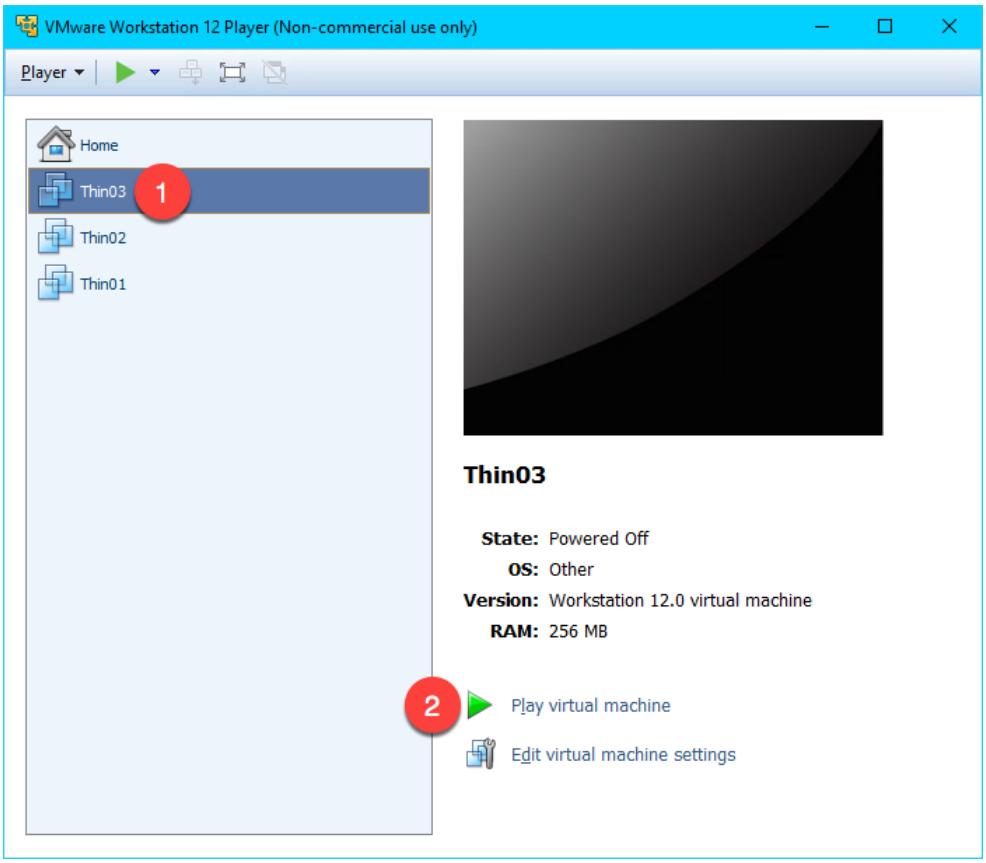


3. When the network capturing begins, you will see a consistent stream of network packets in the capture pane. We want to filter the packets initially to only look at bootp packets, so enter *bootp* followed by the ENTER key in the filter field. This should result in clearing the capture pane, since we have not attempted to boot a client yet.

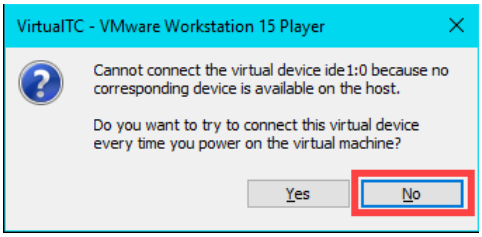


Troubleshoot the Boot Process

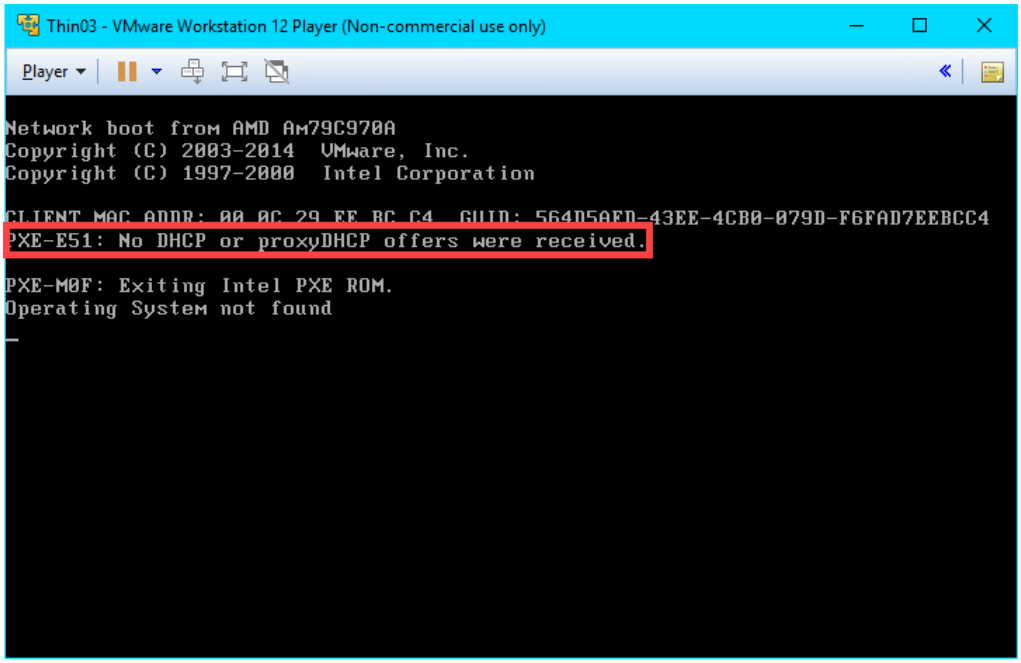
1. Return to **VMWare Player**. If it is closed, you can re-launch it by double clicking its shortcut on the desktop. Select the **Thin03** virtual image we created earlier and click the **Play virtual machine** link.



2. Click the **No** button to the connect virtual device message box.

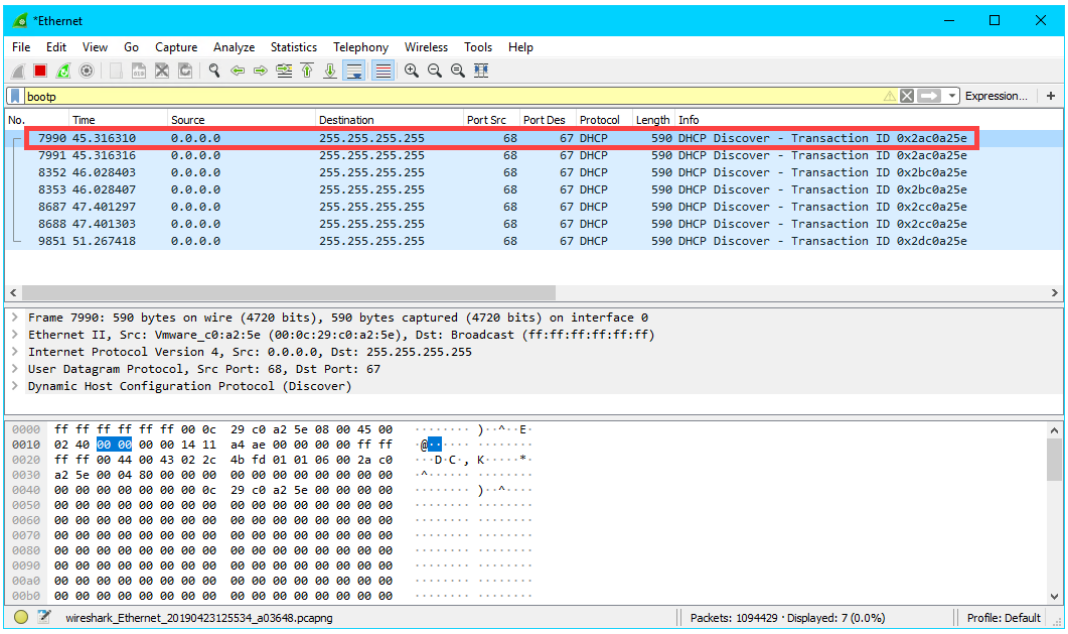


3. Since we have not installed an **Operating System** in our virtual machine, it will attempt to **PXE boot**. After a few seconds, we receive a **PXE-E53** error indicating **No boot filename received**. Recall that **PXE** is inherently dependent on **DHCP**. As part of this dependence, any **PXE** 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.

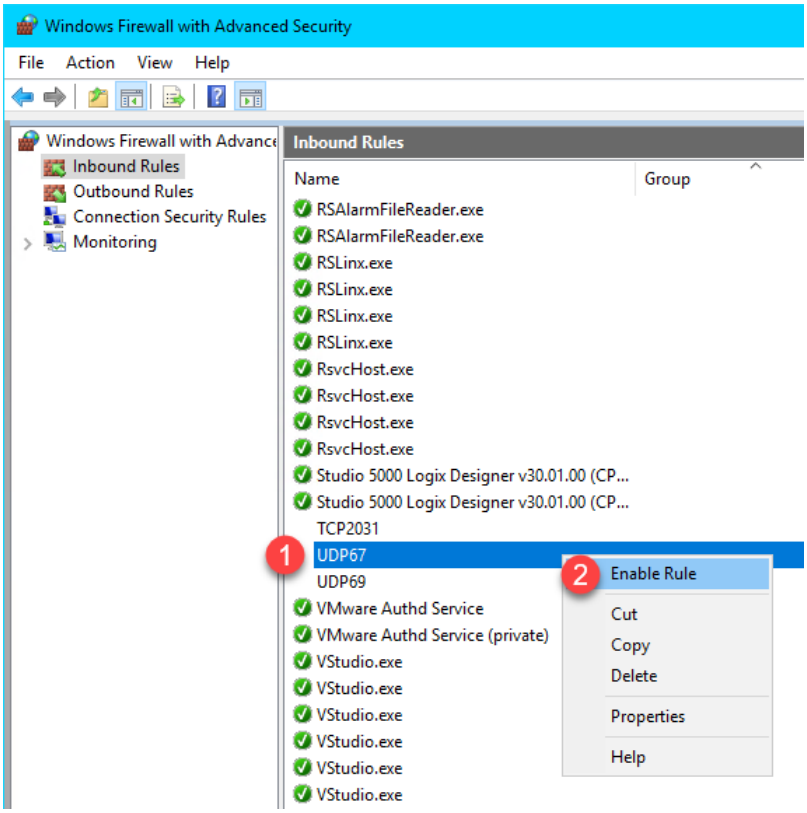


TFTP, **Trivial File Transfer Protocol**, is used by all ThinManager managed thin clients to deliver the boot file, the firmware, as well as the terminal configuration.

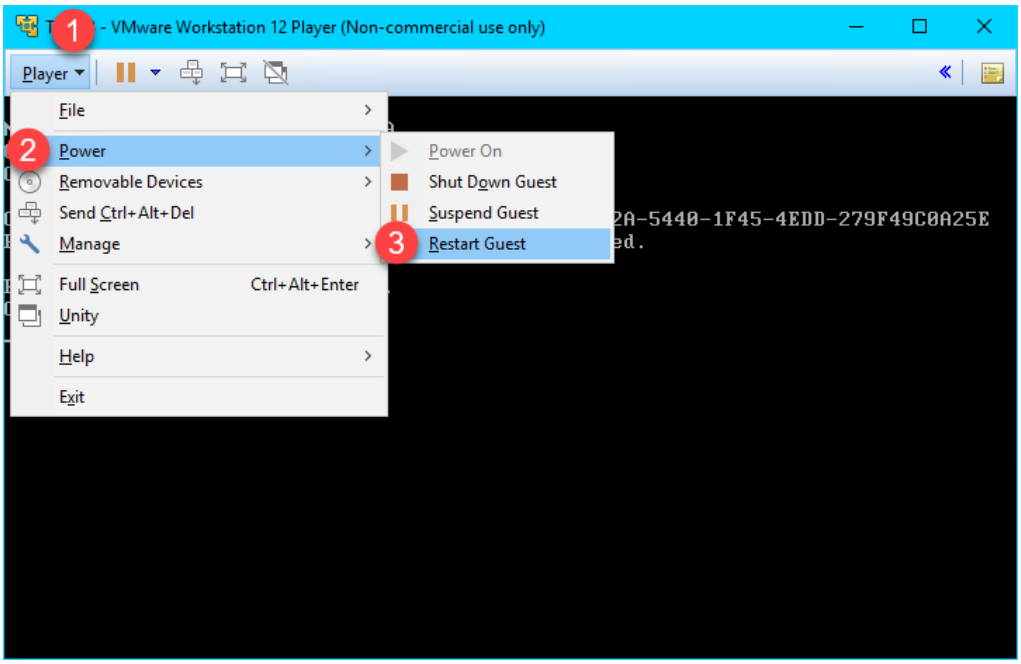
4. Return to **Wireshark** so we can investigate what might be the problem. As we can see from the capture log, a **DHCP Discover** packet was sent to a **Port Destination of 67**, but no **DHCP Offers** were made from **ThinManager**.



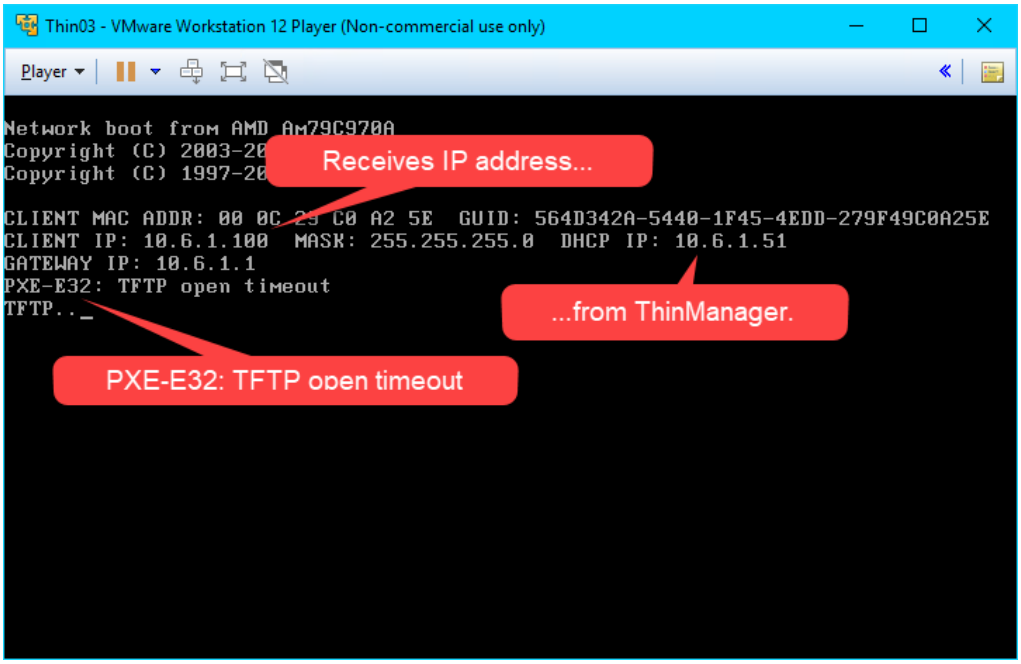
5. Return to the **Windows Firewall with Advanced Security** window. Right click the **UDP67** firewall rule and select **Enable Rule**. This is the rule that permits UDP67 traffic through the firewall, which enables **DHCP** traffic.



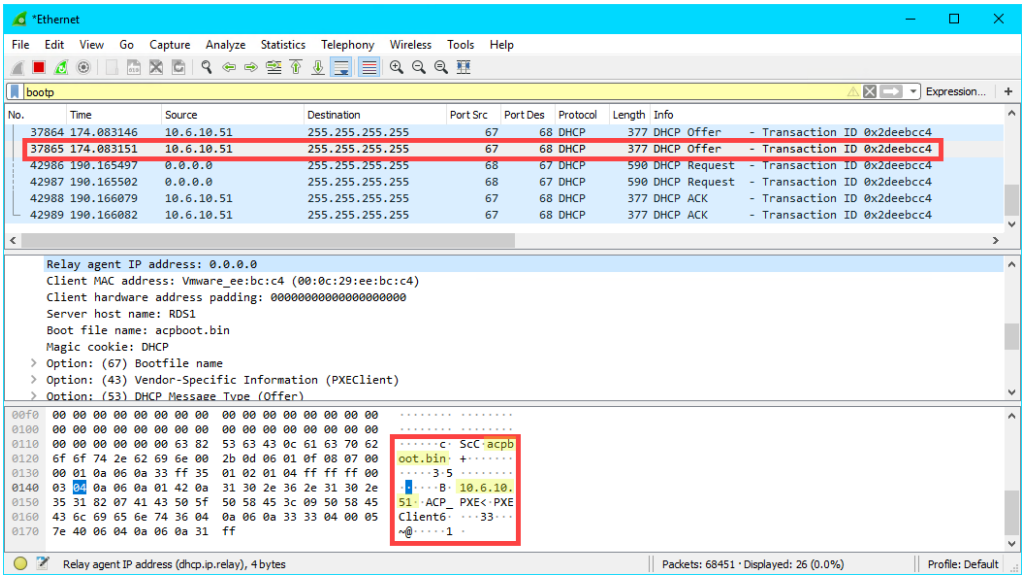
6. Return to **VMWare Player**. Select the **Player** drop down menu, followed by the **Power** item then the **Restart Guest** item. Click **Yes** to the confirmation dialog.



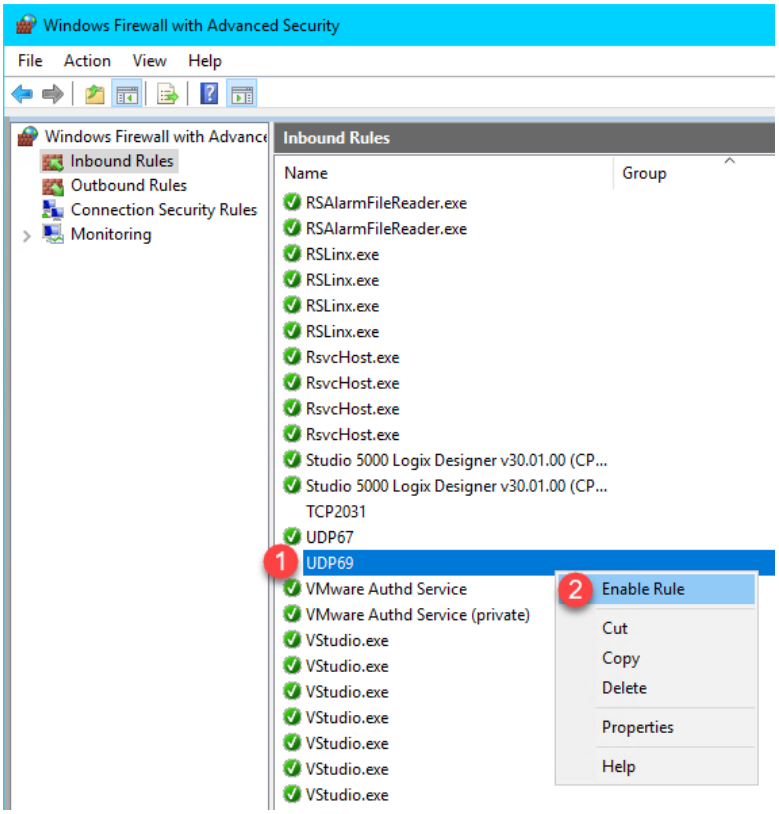
7. After restarting the virtual thin client, we receive a **TFTP** timeout. It looks like we might be getting a little closer. This time we receive the necessary IP information from ThinManager. This indicates that **ThinManager** responded to the **DHCP Request** with a **DHCP Offer**. Let's confirm this with **Wireshark**.



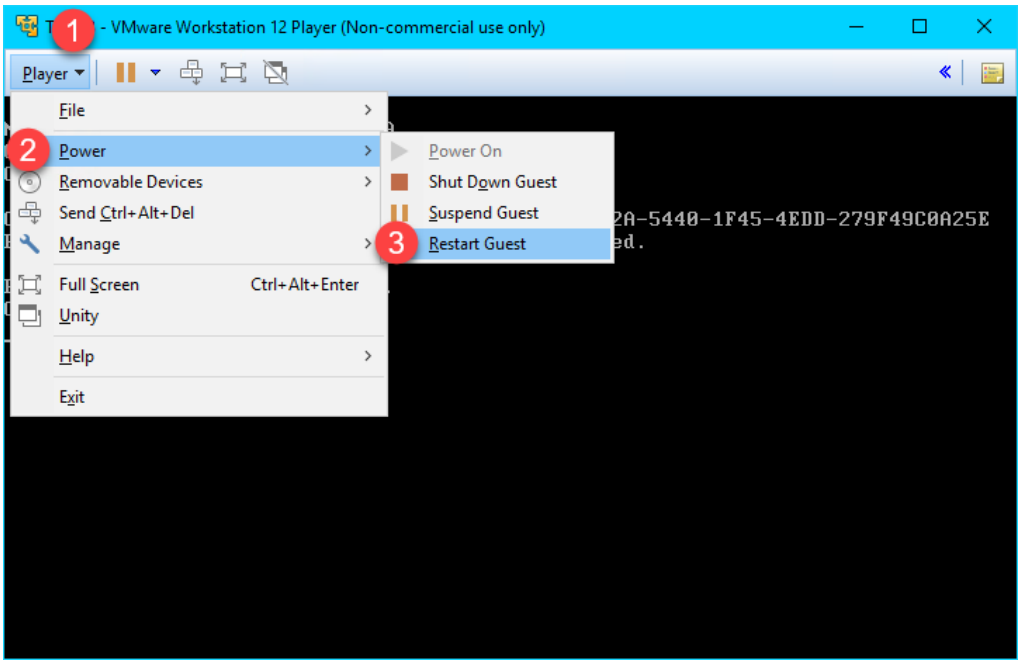
8. Sure enough, we see that this time we received a **DHCP Offer** from 10.6.10.51 which includes the **boot server** (10.6.1.51) and the **boot filename** (acpboot.bin). So our virtual thin client should have all it needs to boot, but we are still receiving a **TFTP** timeout.



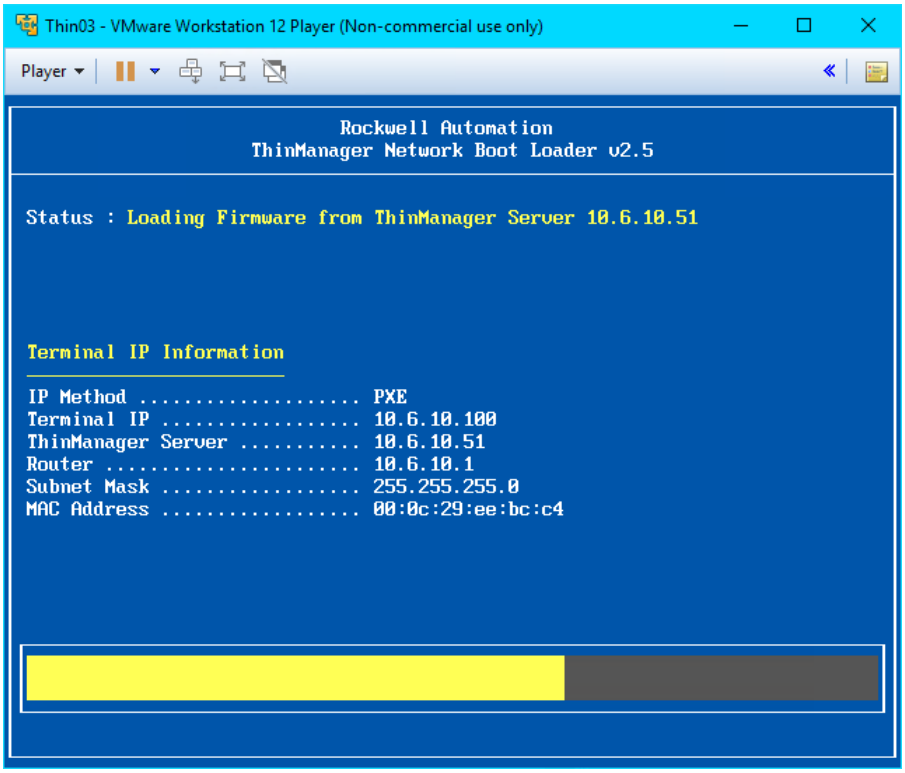
9. Return to the **Windows Firewall with Advanced Security** window. Right click the **UDP69** firewall rule and select **Enable Rule**. This is the rule that permits UDP69 traffic through the firewall, which is required for **TFTP** communication for **PXE** clients.



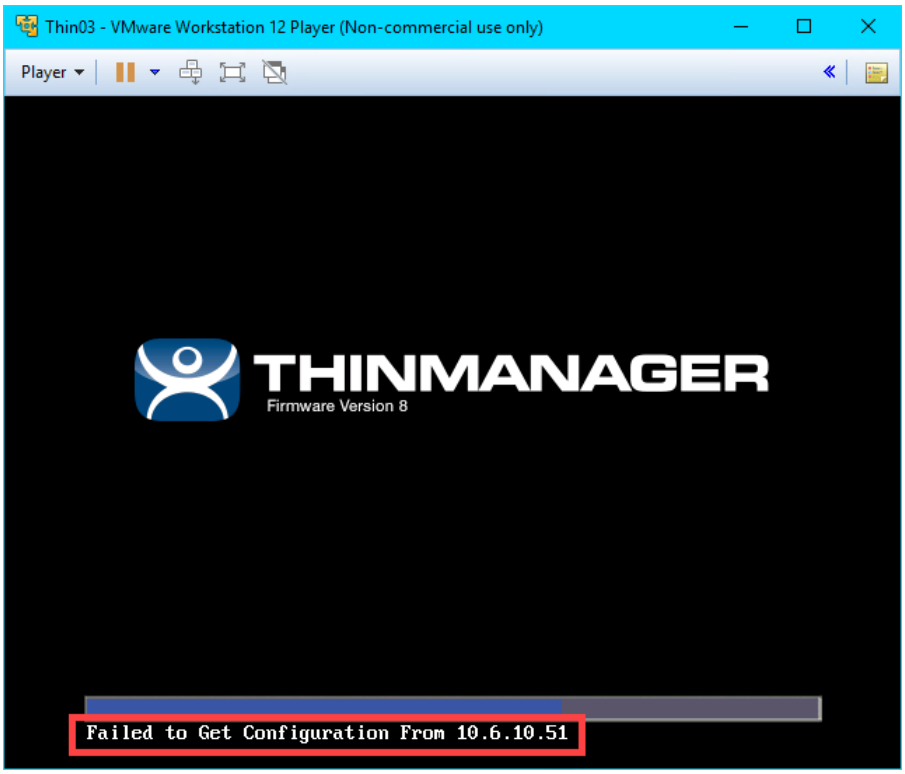
10. Return to **VMWare Player**. Select the **Player** drop down menu, followed by the **Power** item then the **Restart Guest** item. Click **Yes** to the confirmation dialog.



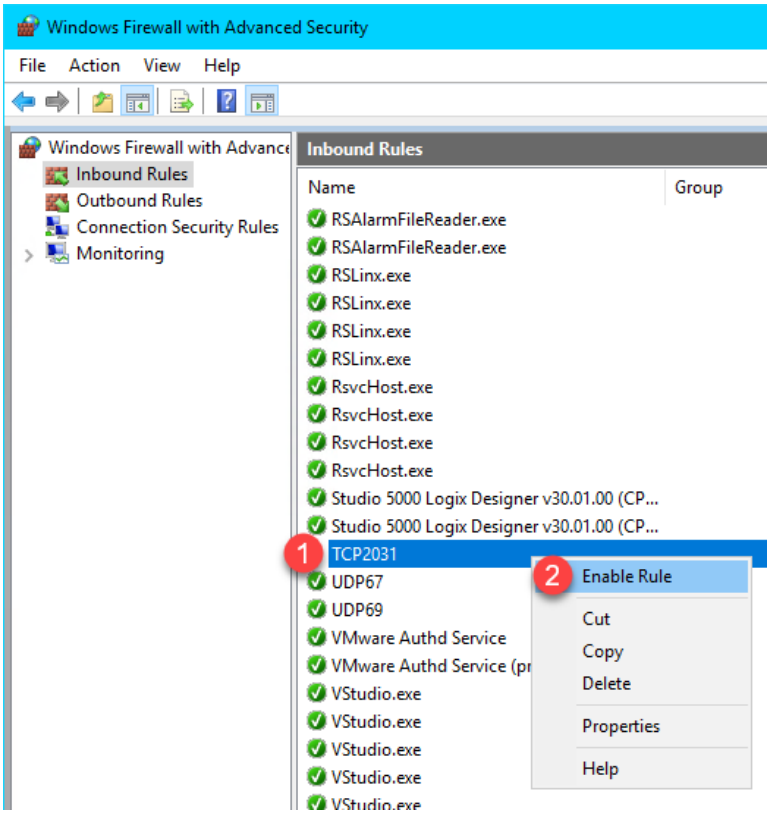
11. This time, the **Virtual Thin Client** should begin to boot. It will first receive the boot loader (**acpboot.bin** for **Legacy PXE** clients like this one), and then the firmware. Notice that the **IP Method** is listed as **PXE**, which indicates that **ThinManager** acted as a **DHCP Server** to deliver the IP address for the terminal, the IP address of the ThinManager Server and the boot filename.



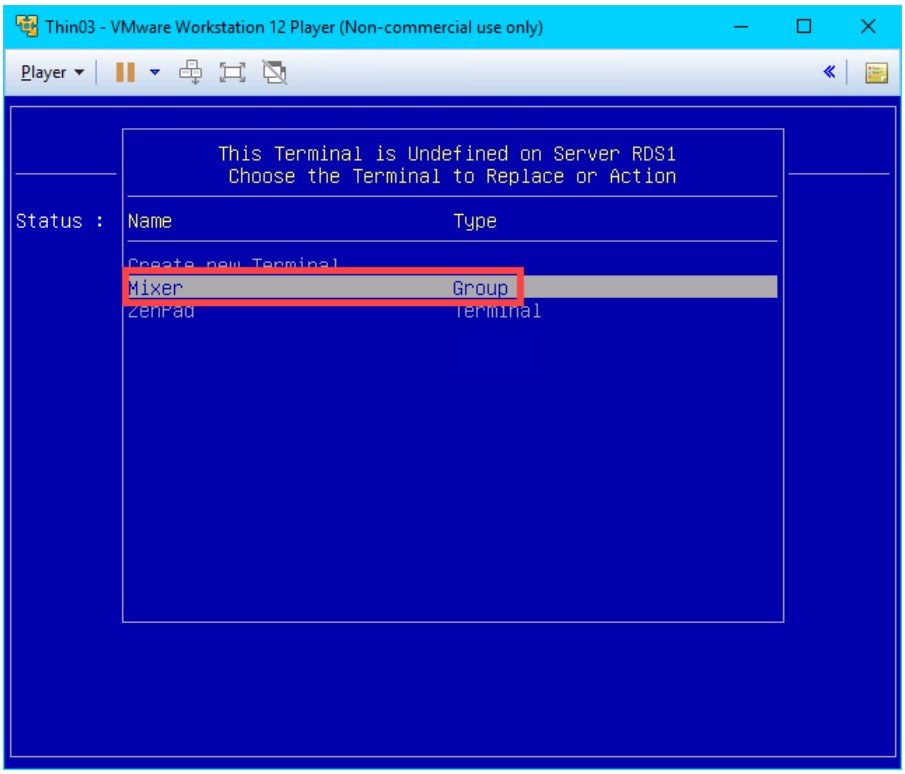
12. We will now see the final hurdle to clear, which is the delivery of the terminal profile, which requires **TCP2031**. Since this port is not currently open, we are receiving a **Failed to Get Configuration From 10.6.10.51** error message.



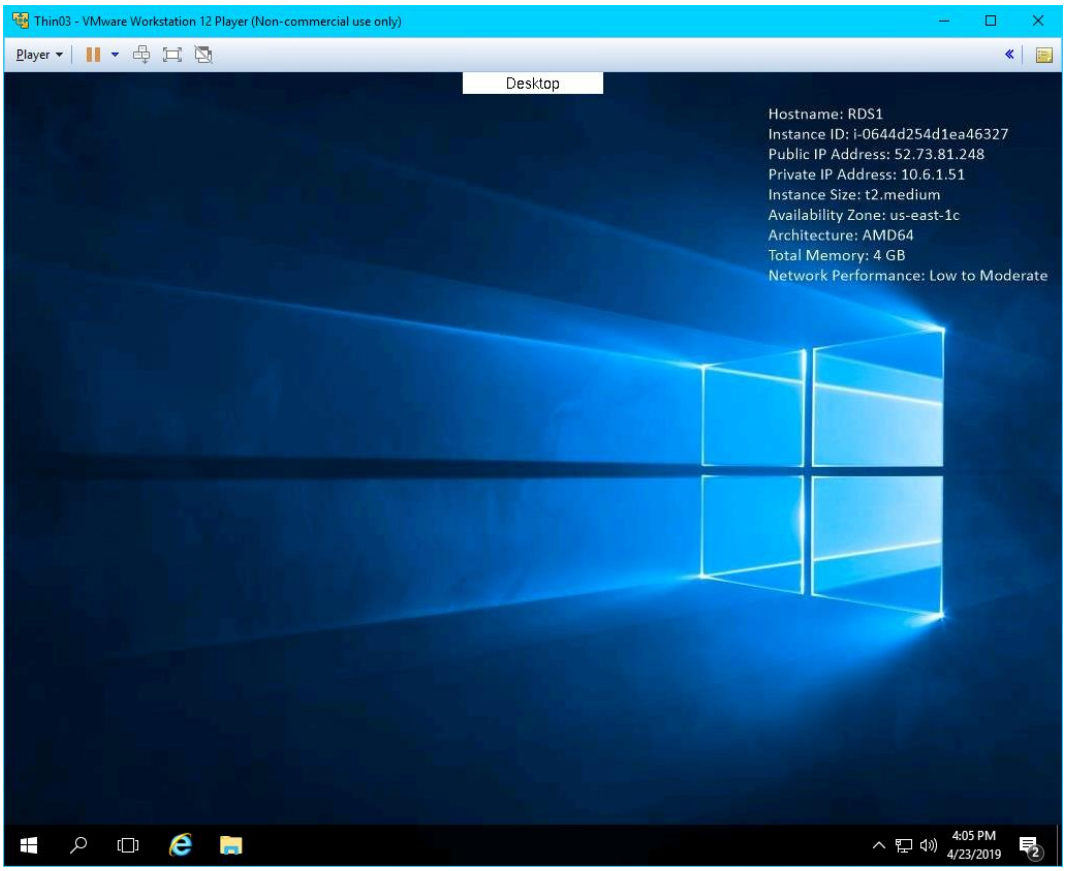
13. Return to the **Windows Firewall with Advanced Security** window. Right click the **TCP2031** firewall rule and select **Enable Rule**. This is the rule that permits **TCP2031** traffic through the firewall, which is required for the delivery of the terminal profile and for communication between **ThinServer** and the terminal.



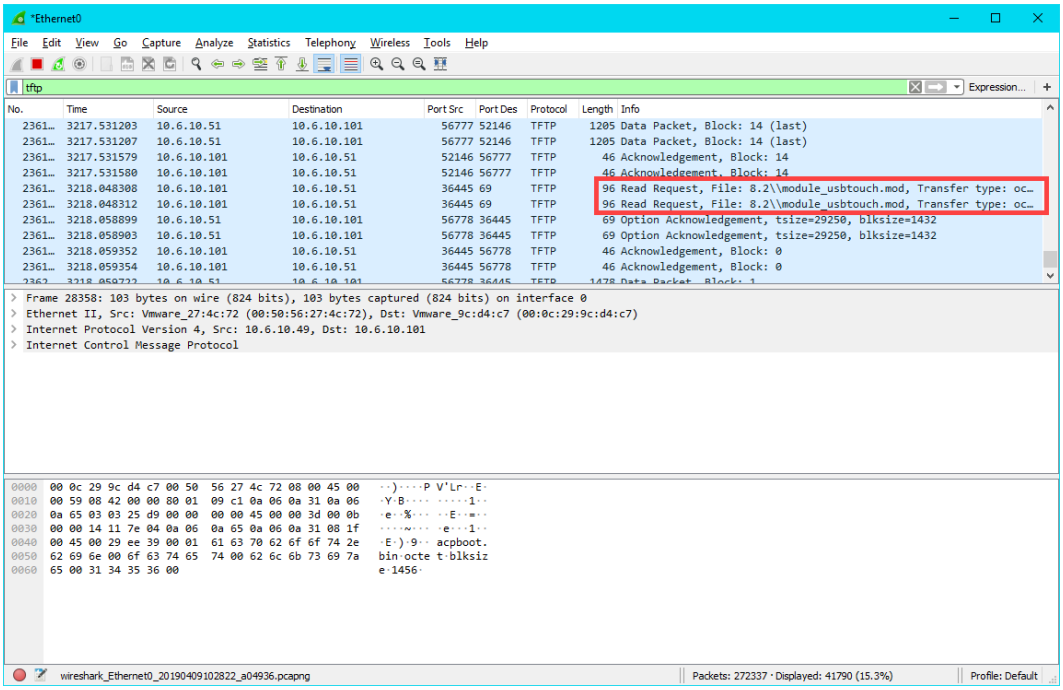
14. Return to the virtual thin client once more and we should now see the terminal profile assignment screen. Arrow down to select the **Mixer Terminal Group** followed by the **Thin03** terminal profile.



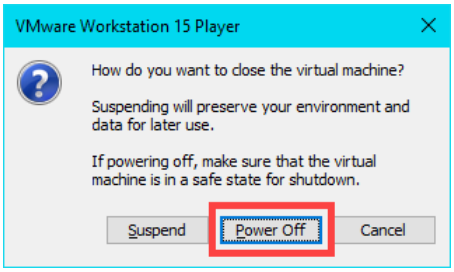
15. The boot process should continue now delivering the terminal's profile, with the ultimate result being the delivery of the **Desktop Display Client** that we assigned to the **Thin03** terminal profile in the **ThinManager**.



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).



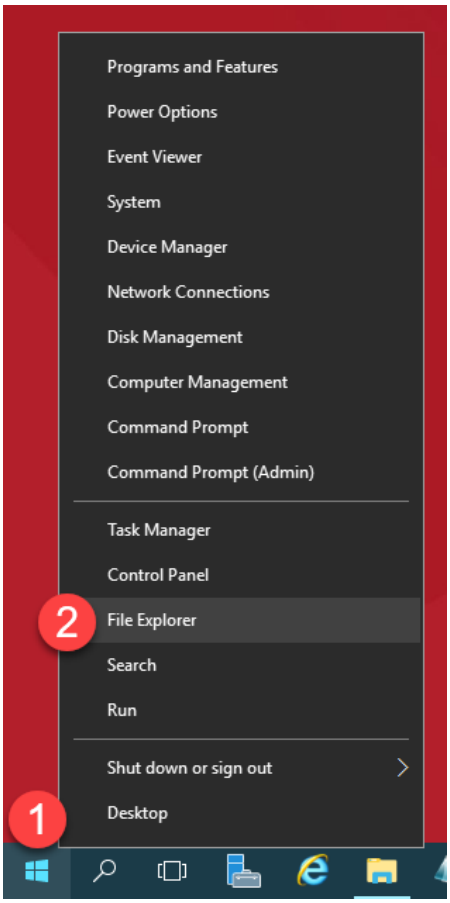
17. Return to **VMWare Player** and close it. Click the **Power Off** button.



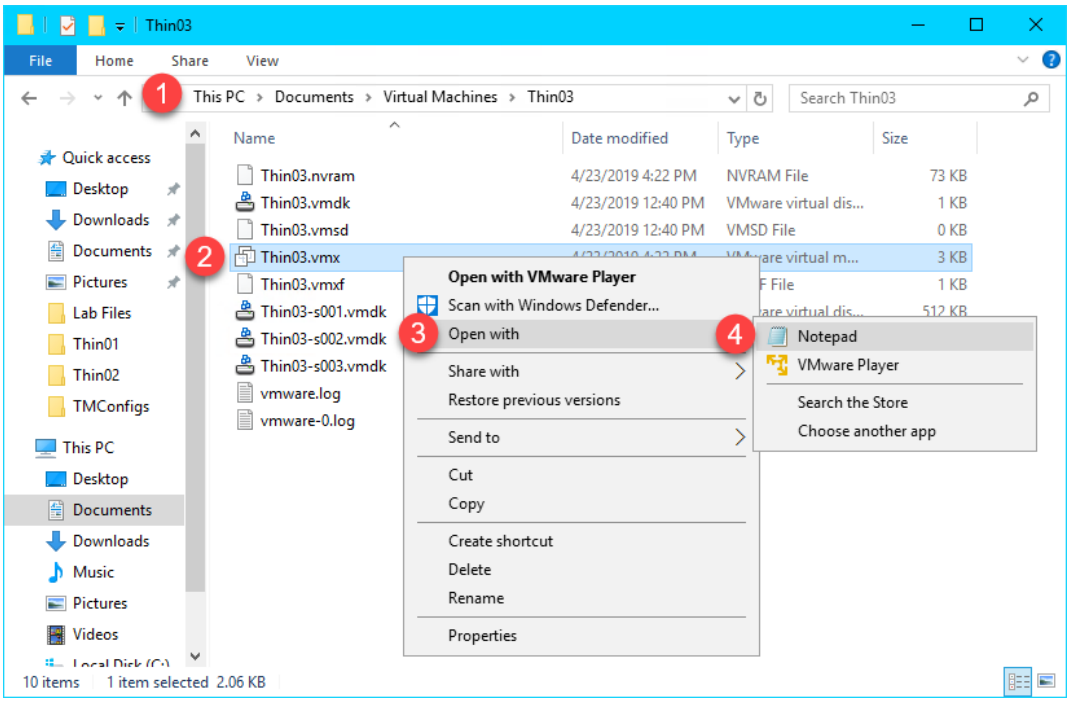
Boot Virtual Thin Client via UEFI

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**.

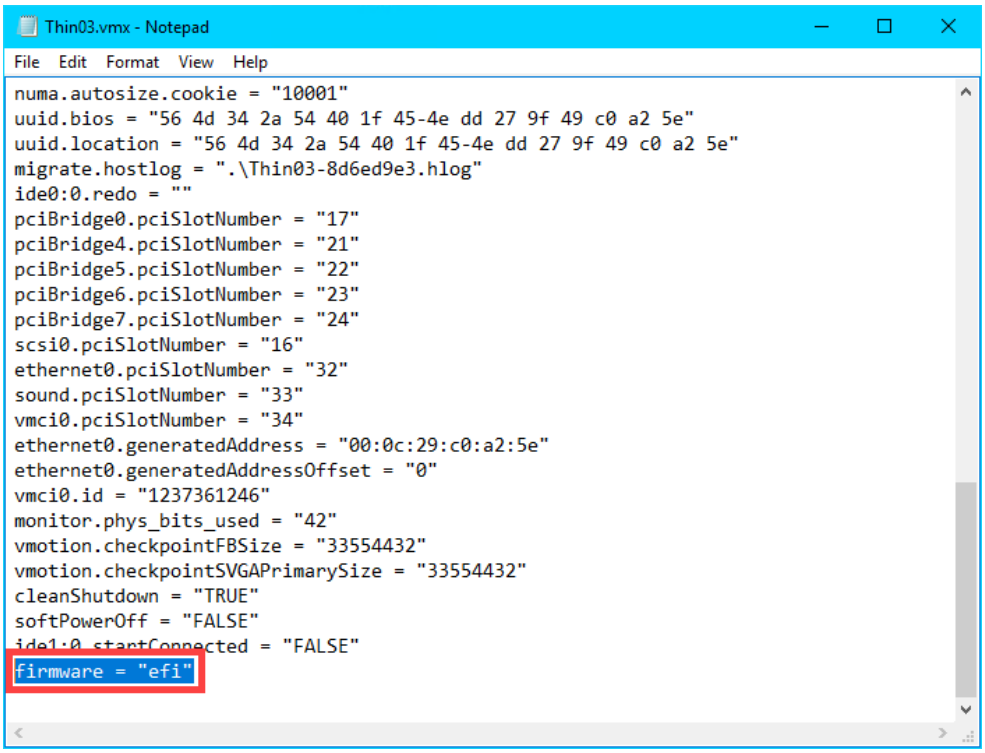


15. Within **File Explorer**, navigate to **Documents->Virtual Machines->Thin03**, right click **Thin03.vmx** and select **Open With…** followed by **Notepad**.



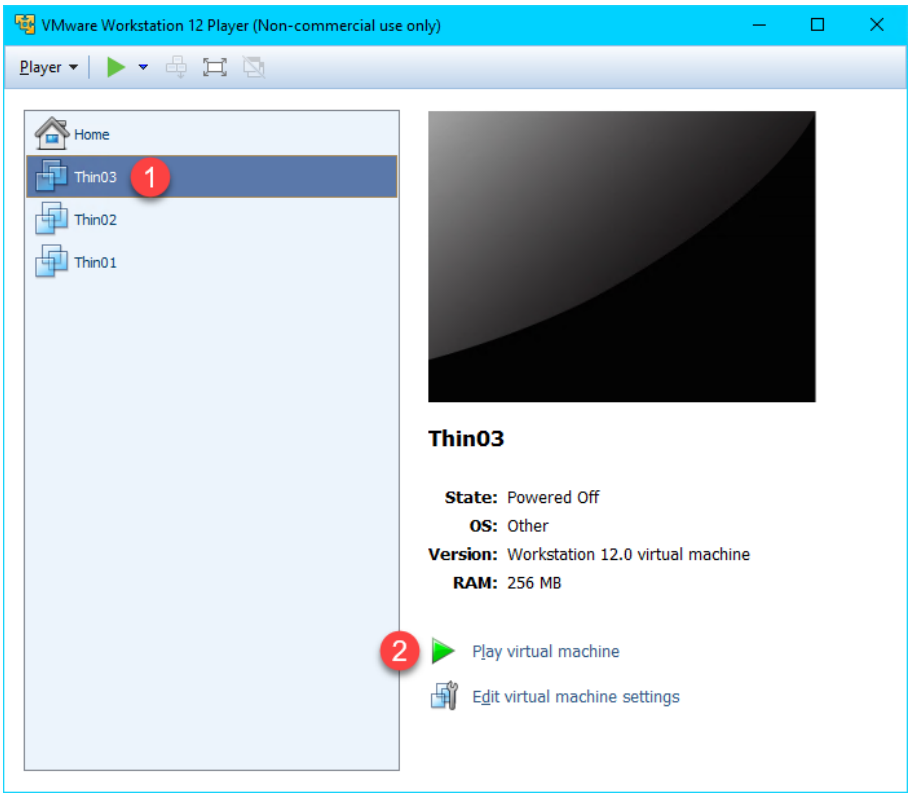
16. Scroll to the bottom of the text file and enter the following on a new line (this can also be copied and pasted from the **LabPaths.txt** file from the **RDS1 Desktop**). **Save** the file and close **Notepad**.

```
firmware = "efi"
```

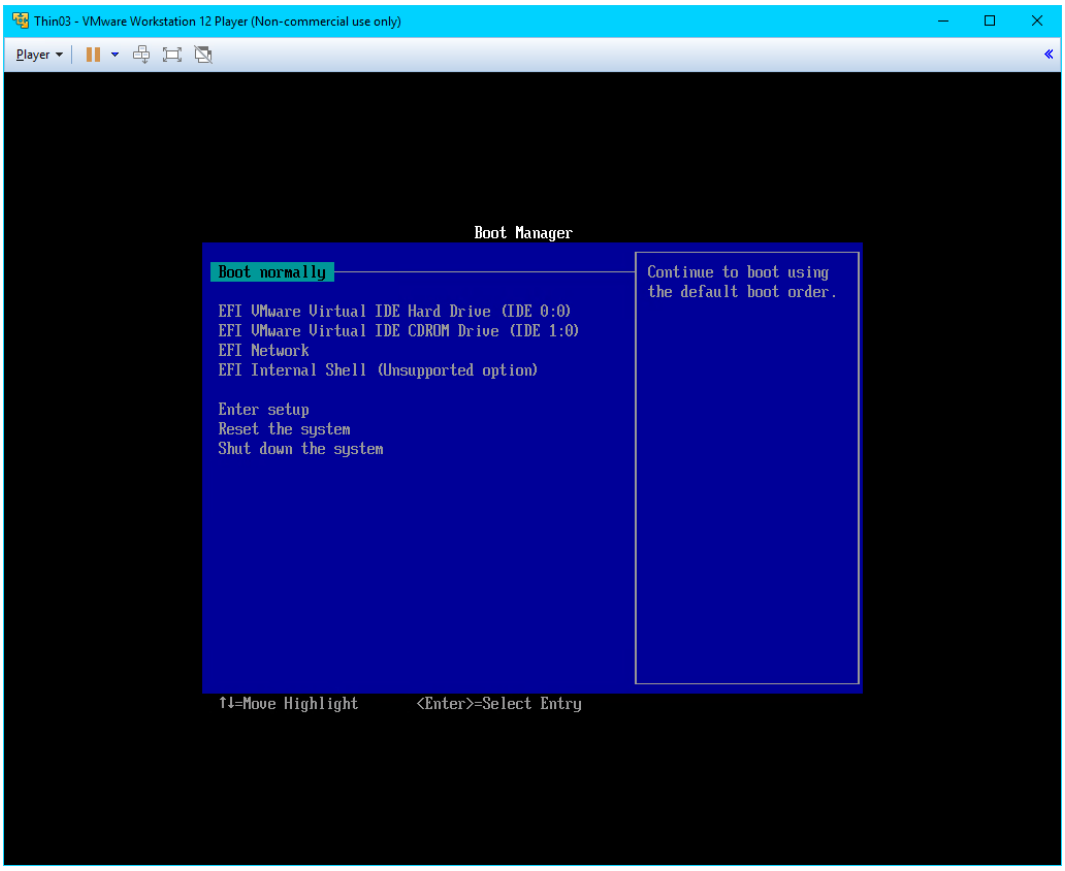


17. Double click the **VMWare Player** shortcut on the **RDS1** desktop.

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.



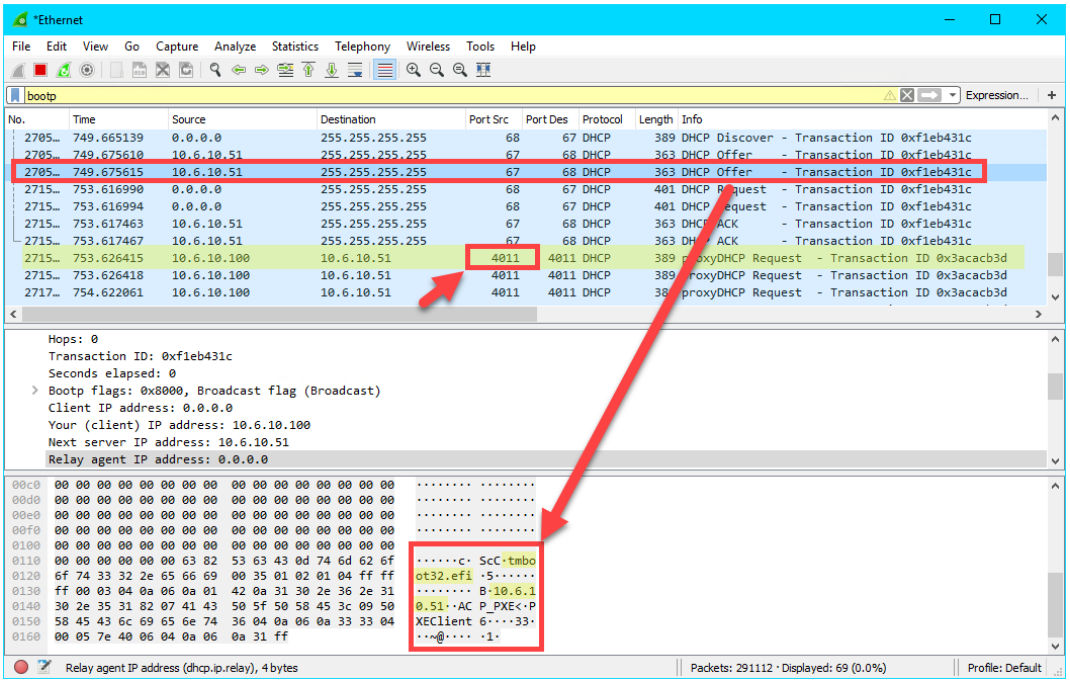
19. The **VirtualTC** image should now attempt to **PXE** boot via **UEFI** as opposed to **BIOS**. You should see the following screen indicating that it was unable to boot.



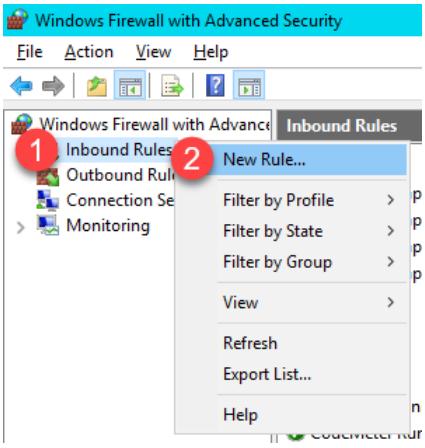
20. Let's return to **Wireshark** and examine the capture. Enter *bootp* as the capture filter again and scroll towards the bottom of the capture window.

    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**.

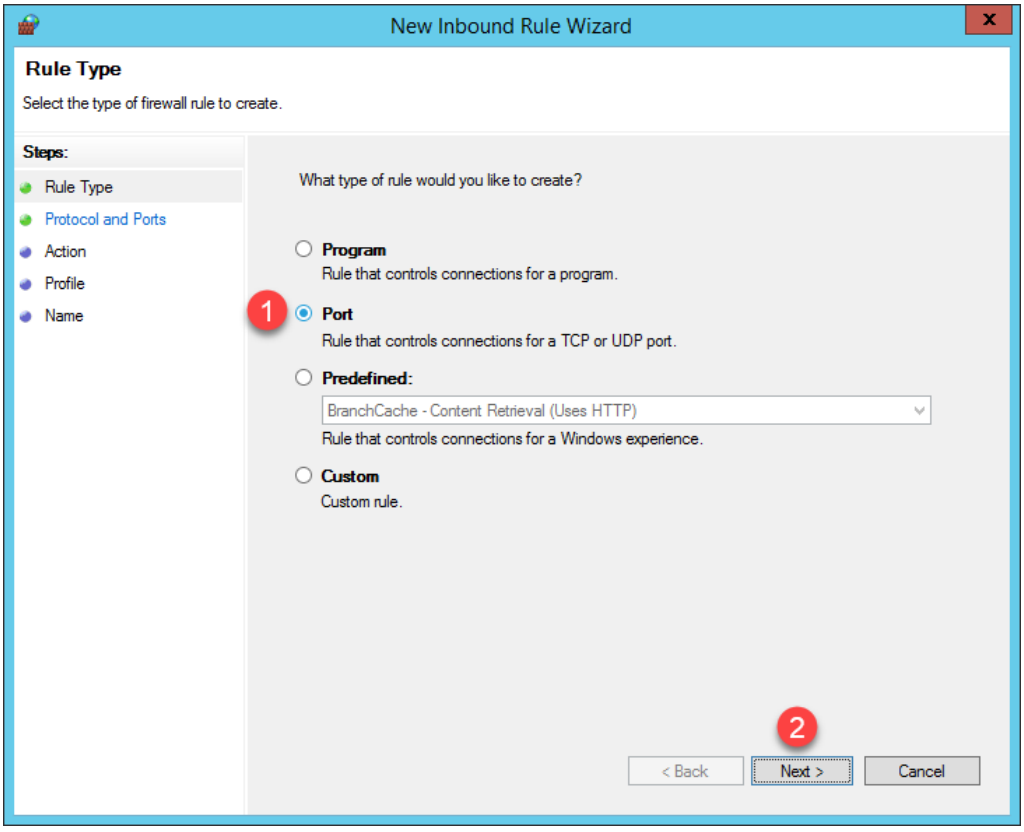
    The 2nd thing to notice is the **proxyDHCP Request**(s) on port **4011**. **UEFI** requires that we also open **UDP Port 4011**.



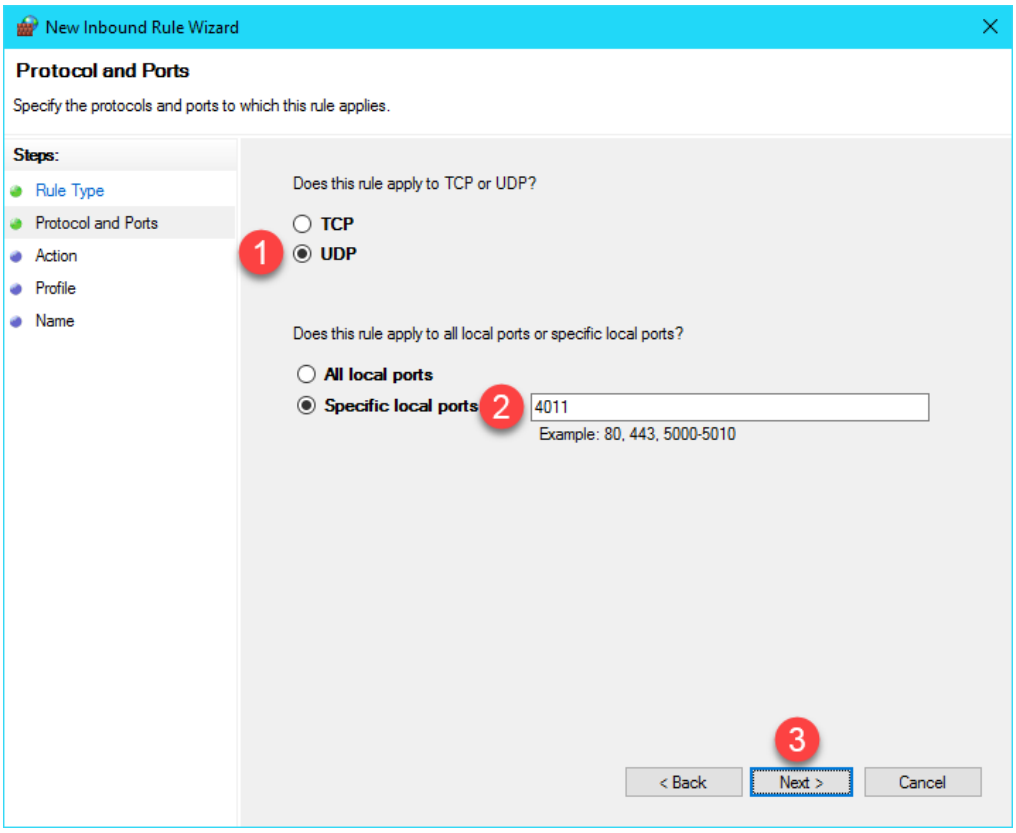
21. Return to the **Windows Firewall and Advanced Security** window.
22. Let's add a new **Inbound Rule** to permit the **UDP4011** port. Right click the **Inbound Rules** item and select the **New Rule…** item.



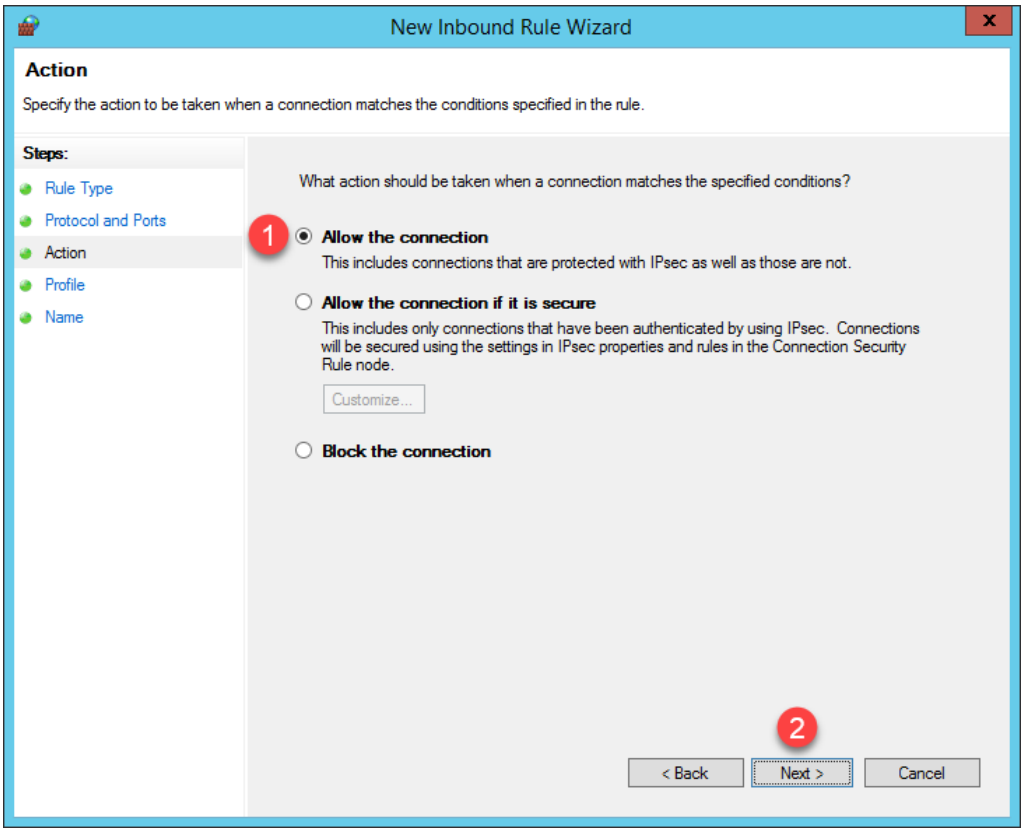
23. From the **Rule Type** panel of the **New Inbound Rule Wizard**, select the **Port** radio button, followed by the **Next** button.



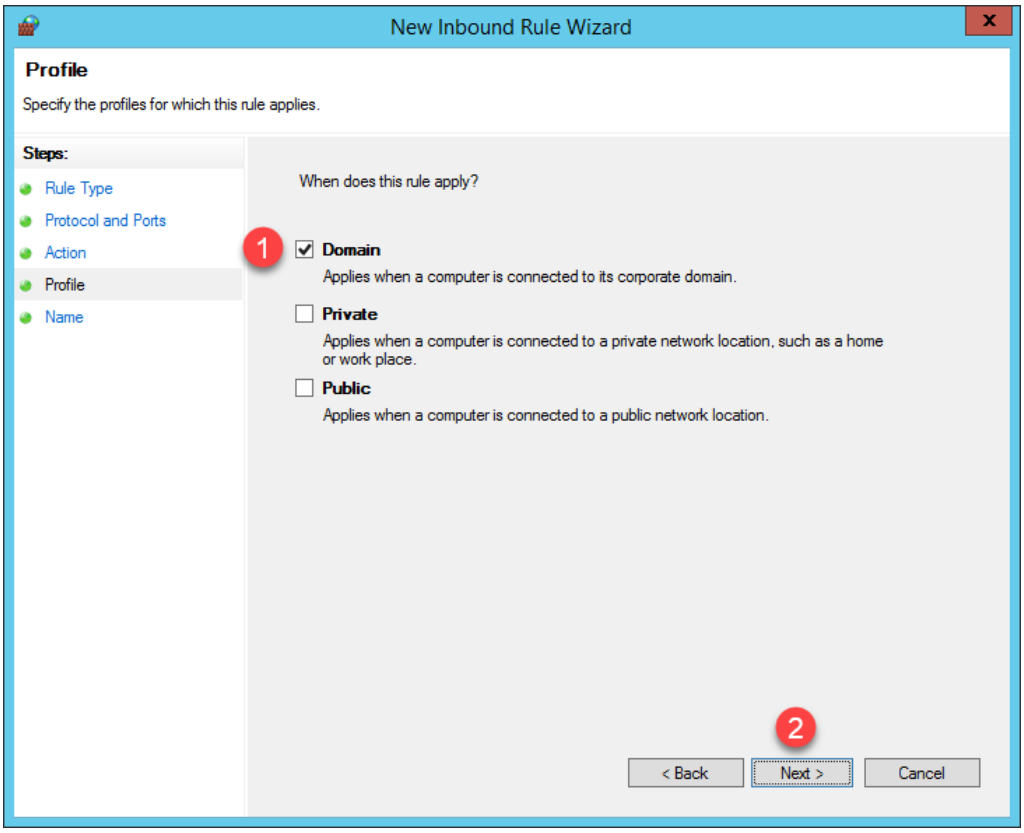
24. From the **Protocol and Ports** panel of the **New Inbound Rule Wizard**, select the **UDP** radio button and enter *4011* in the **Specified local ports** field. Click the **Next** button.



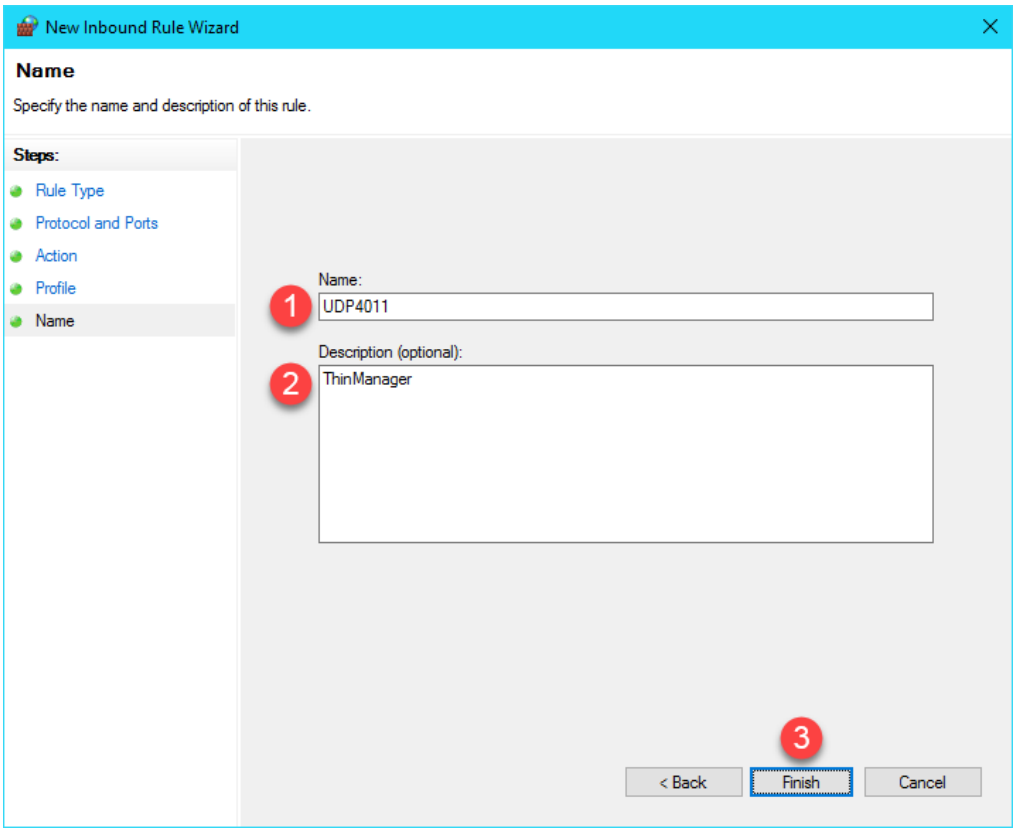
25. From the **Action** panel of the **New Inbound Rule Wizard**, select the **Allow the connection** radio button and click the **Next** button.



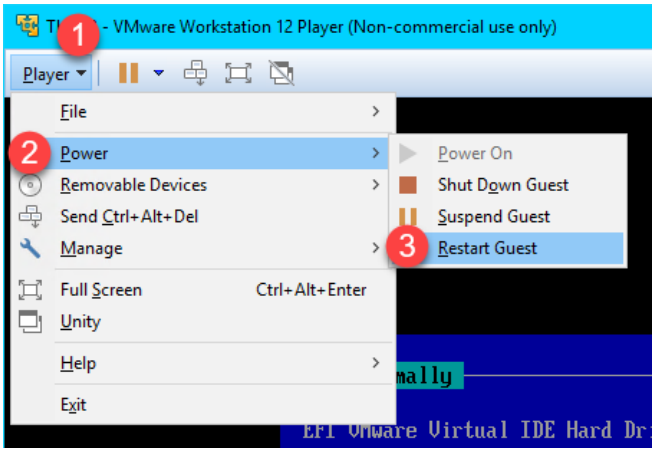
26. From the **Profile** panel of the **New Inbound Rule Wizard**, check the **Domain** checkbox and **un**-check the **Private** and **Public** checkboxes. Click the **Next** button.



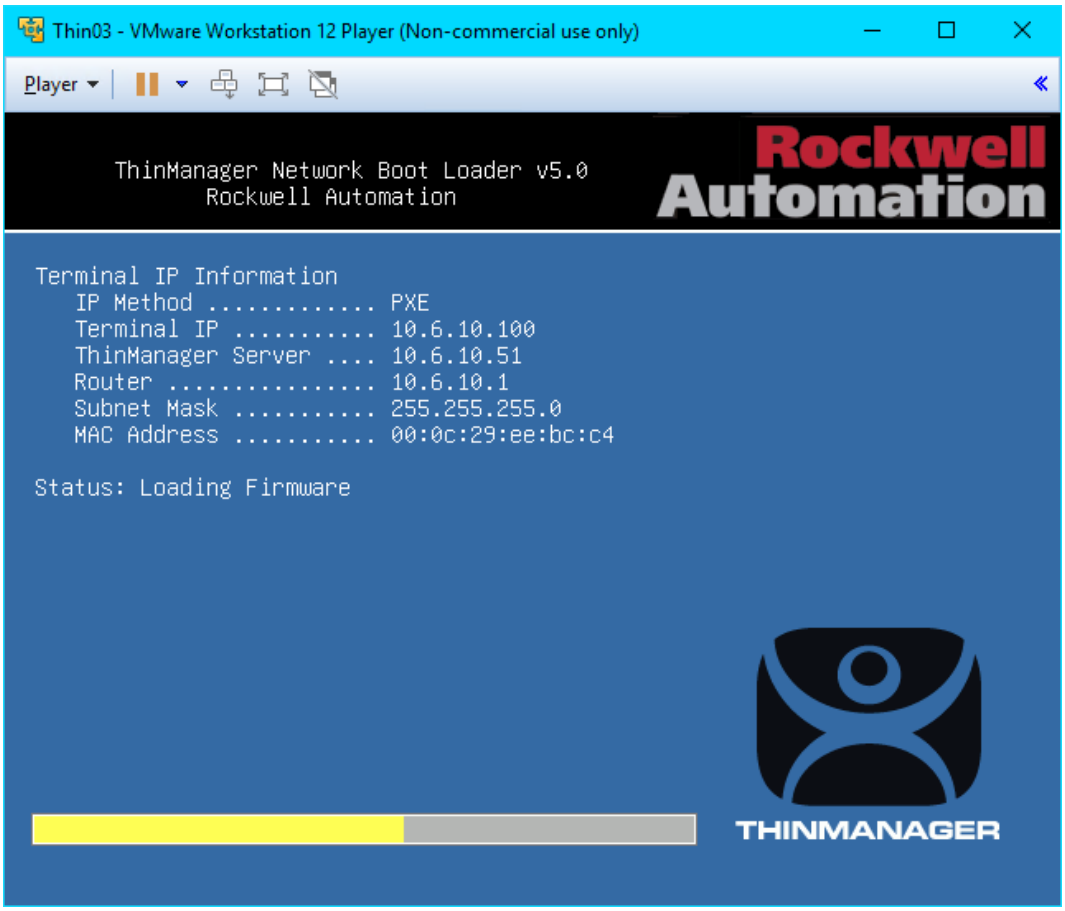
27. From the **Name** panel of the **New Inbound Rule Wizard**, enter *UDP4011* as the **Name** and *ThinManager* as the **Description**. Click the **Finish** button. Leave the **Windows Firewall with Advanced Security** window open.



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!

Notes