

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:



ATTENTION

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



identify a hazard

- avoid a hazard
- recognize the consequence

SHOCK HAZARD

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



BURN HAZARD

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

ThinManager Security Lab

Contents

Before you begin	5
About this lab	6
Tools & prerequisites	
Additional References	
Section 1: Restore ThinManager Configuration	9
Section 2: FactoryTalk Security and Group Policy for Remote Start of Applications	10
Overview	
Add Terminal Names to FactoryTalk Directory	
Add Windows Linked User Group to FactoryTalk Directory	
Allow Remote Start of Unlisted Programs	17
Section 4: ThinManager Redundancy and Firewall Configuration	23
Overview	
Configure Automatic Synchronization	
Add Remote ThinManager Server	
Disable Automatic Synchronization	
Disable Secondary ThinManager Server	
Turn On Windows Firewall on RDS1	
Configure Windows Firewall on RDS1	
Section 5: Modules	61
Overview	
Key Block Module	
Locate Pointer Module	
MultiSession Screen Saver Module	
Section 6: Terminal Groups, Overrides, Schedules and Mouse Button Mapping	78
Overview	
Terminal Groups	
Overrides	

Schedules	
Mouse Button Mapping	
Remove Override and Mouse Button Mapping	
Section 7: Securing the ThinManager Admin Console	102
Overview	102
Create ThinManager Admin Console Display Client	
Assign Admin Console Display Client to Terminal	
ThinManager Security Groups	108
Section 8: Relevance Location Services - Geo-Fencing	113
Overview	113
Create Maintenance Access Group	114
Create Maintenance User Group	116
Create Maintenance User	
Register a Bluetooth Beacon Location Resolver	121
Register a QR Code Location Resolver	123
Create Parent (Geo-Fence) Location	126
Create Child Location	130
Reassign Display Client to Public Display Server	
Assign Default Location to Terminal	
See the Results	
Remove Default Location from Terminal	146
Section 9: Virtual Thin Clients, PXE Server and Wireshark	
Overview	
Create Virtual Thin Client	150
Modify PXE Server Mode	159
Create Terminal for Virtual Thin Client	
Re-enable Firewall Rules	
Start Wireshark Capture	
Troubleshoot the Boot Process	170
Boot Virtual Thin Client via UEFI	

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 (<u>P</u>re-Boot E<u>x</u>ecution <u>E</u>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.



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

🐸 Open			×
← → ~ ↑ 📙	≪ Local Disk (C:) → Lab Files → TMConfigs	✓ Ö Search T	MConfigs 🔎
Organize 👻 New	v folder		E 🕶 🔟 🕜
Lab Files	↑ Name	Date modified 4/28/2019 8:05 PM	Type Si ^ Data Base File
Thin02	CloudLab_05_Start	4/28/2019 8:05 PM 4/28/2019 8:05 PM	Data Base File Data Base File
Desktop	CloudLab_07_Start	4/28/2019 8:05 PM 4/28/2019 8:05 PM	Data Base File Data Base File
Documents Downloads	CloudLab_09_Start CloudLab_10_Start	4/28/2019 8:05 PM 4/28/2019 8:05 PM	Data Base File Data Base File
🍌 Music 📰 Pictures	CloudLab_11_Start	4/28/2019 8:05 PM 4/28/2019 8:05 PM	Data Base File Data Base File
📓 Videos 🏪 Local Disk (C:)	CloudLab_13_Start	4/28/2019 8:05 PM 4/28/2019 8:05 PM	Data Base File Data Base File
🧀 Network	ScloudLab_15_Start	4/28/2019 8:05 PM	Data Base File >
	File <u>n</u> ame: CloudLab_11_Start	✓ ThinMai Op	nager Configuration ~

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 <u>without</u> 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 – <u>NOT the shadowed Desktop delivered to the thin client or the thin client itself.</u>



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

Select FactoryTalk Directory		
1 ct the directory you want to use.		
Network OK Cancel Help	~	

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.

New Compute	r	×
General Polic	zy Setting	
Computer:	Versa View 5200 (1)	
Description:		
Member of:		_
	<u>A</u> dd <u>R</u> emove.	
	2	
	OK Cancel Help	

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.

New Windows-Linked User Group
General
Click the Add button to select one or more Windows user groups. When you click the Create button, a new linked user account will be created for each Windows user group you have selected.
Add Remove
OK Cancel Help

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.

Select Groups	x
Select this object type: Groups or Built-in security principals	Object Types
From this location: RDS1	Locations
Enter the object names to select (<u>examples</u>):	Check Names
Advanced OK	Cancel

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

Locations	x
Select the location you want to search.	
Location: RDS1 Entire Directory Itmlab.loc	
OK Cance	

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

Select Groups	X
Select this object type:	
Groups	Object Types
From this location:	
tmlab.loc	Locations
Enter the object names to select (<u>examples</u>):	
1 Domain Users	Check Names
0	
Advanced OK	Cancel

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

New Windows-Linked User Group	x
General	_
Click the Add button to select one or more Windows user groups. When you click the Create button, a new linked user account will be created for each Windows user group you have selected.	
TMLAB\DOMAIN USERS	
Add Remove	
OK Cancel Help	

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*.

Windows Security		
Enter your credentials		
These credentials will be used to connect to dc.tmlab.	oc.	
labuser		
•		
tmlab\labuser		
Remember me		
More choice 2		
OK Cancel		

- 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.

<u> </u>	Group	Policy Management Editor			_ 🗆 X
File Action View Help					
Come Forderer					
Game Explorer	Connections	C			
homeoroup	Allow remote start of unlisted	Setting	State	Comment	
p internet explorer	programs	E Automatic reconnection	Not configured	No	
Internet information services		E Allow users to connect remotely by using Remote Desktop S.	. Not configured	No	
Maintenance Scheduler	Edit policy setting	Deny logoff of an administrator logged in to the console ses	. Not configured	No	
Native Science	Pequirementry	Configure keep-alive connection interval	Not configured	No	
Network Accers Protection	At least Windows Server 2008	E Limit number of connections	Not configured	No	
Network Projector		Suspend user sign-in to complete app registration	Not configured	No	
	Description:	E Set rules for remote control of Remote Deskton Services use.	Not configured	No	
Oniconve	This policy setting allows you to	Select network detection on the server	Not configured	Ne	
Pactword Sunchronization	start any program on the PD	E Select RDP transport protocols	Not configured	No	
Portable Operating System	Session Host server when they	E Partrict Pamota Darkton Sanicar urar to a ringle Pamota D	Not configured	No	
Brecentation Settings	start a Remote Desktop Services	All and a state of a s	Net configured	Ne	
Presentation Sectings Presentation Sectings	session, or whether they can only	Z Allow remote start of unlisted programs	Not conligured	140	•
PD Licensing	start programs that are listed in	E Turn off Fair Share CPU Scheduling	Not configured	NO	
Remote Decising	the RemoteApp programs list.				
Remote Desktop Connection Chent	You can control which programs				
Application Compatibility	on an RD Session Host server can				
Connections	be started remotely by using the				
Device and Bernard Reditection	RemoteApp Manager on Windows				
	Server 2008 K2 and Windows				
Drinter Parlimention	Windows Server 2012 R2, you can				
Printer Redirection	configure this in the Collection				
Piones	properties sheet by using Server				
Bernete Section Environment	Manager.				
Security	By default, only programs in the				
Servion Time Limitr	RemoteApp Programs list can be				
Temporany folders	started when a user starts a				
RSS Feeds	Remote Desktop Services session.				
Security Center	Martin and the state of the section				
Security concerns	remote users can start any				
Shutdown Ontions	program on the RD Session Host				
Smatt Card	server when they start a Remote				
Sound Recorder	Desktop Services session.				
Sume your rettinge	For example, a remote user can do				
h Tablet PC	executable path at connection				
Tack Scheduler	time by using the Remote Desktop	~			
	Consideration of Considerated				
	Contended Astandard				

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.

٠	A	Illow remote start of unlisted programs
Allow remote star	t of unlisted prog	Previous Setting Next Setting
 Not Configured Enabled 	Comment:	
 Disabled 	Supported on:	At least Windows Server 2008
Options:		Help:
		This policy setting allows you to specify whether remote users can start any program on the RD Session Host server when they start a Remote Desktop Services session, or whether they can only start programs that are listed in the RemoteApp programs list. You can control which programs on an RD Session Host server can be started remotely by using the RemoteApp Manager on Windows Server 2008 R2 and Windows Server 2008. If you are using Windows Server 2012 R2, you can configure this in the Collection properties sheet by using Server Manager. By default, only programs in the RemoteApp Programs list can be started when a user starts a Remote Desktop Services session. If you enable this policy setting, remote users can start any program on the RD Session Host server when they start a Remote Desktop Services session. For example, a remote user can do this by specifying the program's executable path at connection time by using the Remote Desktop Connection client.
		OK Cancel Apply

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



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*.

Windows Security	×							
Enter your credentials								
These credentials will be used to connect to rds2.tmlab.loc.								
labuser								
•								
tmlab\labuser								
Remember me								
More choice 2								
ОК	Cancel							

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.

8.		1						
	Edit	Manage	Install	Tools	View	Remote V	2	Help
Packages	Restore	Backup	Restore E Backup E Synchror	Biometric D Biometric D Bioze	atabase atabase	PXE ThinM Server Serv	anage er List	Provide a configuration Configure Default Terminal Configure Default Terminal Configuage
Packages		(Configuratio	n				Manage

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

8	ThinManager Server List Wizard	x						
Thin I	Manager Server List Wizard Introduction	\mathfrak{l}						
The 1 netwo conne	ThinManager Server Wizard defines the ThinManager Servers on your ork. These are the servers to which the thinclients can make monitor ections.							
The 1 your o	The ThinManager Server name must be the name Windows uses to identify your computer on the network.							
lf you If you The s	are using a DNS server you will only enter the server name. are not using a DNS server you will enter a server name and IP address. erver name will be for reference only.							
<	Back Next > Finish Cancel Help							

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

8	ThinManager Server List Wizard									
Auto	o-synchronization Selection Check Automatic Synchronization to automatically synchronize the configuration of two ThinManager servers.									
Che Thin sync	Check the box if you want to use Automatic Synchronization between two ThinManager servers. Leave the box unchecked if you want to use manual synchronization.									
lf yo	ou have mirrored licenses, then you must use Automatic Synchronization.									
1 F	✓ Automatic Synchronization									
	Back Next > Finish Cancel Help									

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

🕿 T	hinManager Server List Wizard	x							
Auto-synchronizal Define the prima servers will be sy	Auto-synchronization Configuration Define the primary and secondary ThinManager servers. These servers will be synchronized.								
Primary Thin Manag	jer Server								
Name									
IP Address									
- Secondary ThinMa Name	nager ServerEdit								
IP Address									
Additional ThinMa	anager Servers								
< Back	lext > Finish Cancel	Help							

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.

8	ThinManage	r Server I	List Wizard	x						
Auto-synchroniza Define the prim servers will be s	Auto-synchronization Configuration Define the primary and secondary ThinManager servers. These servers will be synchronized.									
Primary Thin Mana	iger Server		Eda							
Name	RDS1		Edit							
IP Address	10.6.10.5	1								
- Secondary ThinM	anager Server—		Edit							
Name										
IP Address										
Additional Thin!	Manager Servers									
< Back	Next>	Finish	Cancel	Help						

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.

Enter the Secondary ThinManager Server Information						
ThinManager Server 1 RDS2 3	ОК					
ThinManager Server IP 10 . 6 . 10 . 52	Cancel					
2 Discover						

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

8	Thin	Manager Server List W	/izard ×						
A	Auto-synchronization Configuration Define the primary and secondary ThinManager servers. These servers will be synchronized.								
Γ	Primary ThinManager So	erver	Edit						
	Name	RDS1							
	IP Address	10.6.10.51							
	Secondary ThinManage	er Server	Edit						
	Name	RDS2							
	IP Address	10.6.10.52							
	Additional ThinManag	er Servers							
	< Back Next :	Finish	Cancel Help						

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**.

. R. T									
E E	dit Manage	Install	Tools	View	Remote View	Help			
	Restore Backup	Restore Bio Backup Bio Synchronize	metric D netric D)atabase Jatabase	PXE ThinManag Server Server List	🖗 DNS Config 🚔 Configure I er 🮯 Web Mana	guration Default Terminal gement	Manage Accounts	Synchronize Se Passwords
Packages	C	onfiguration				Manage		2	ctive Directory
ThinManage	er Server	_		Confi	iguration License	s Properties	Versions	Synchroniz	ation Even
🖃 🕰 Thi	inManager Servers		Γ	Attribute			Value	_	
1 🔁	RDS1			Synch	ronization Mode		Master		
_				Synch	ronization State		Synchronized		
				Synch	ronization Peers		10.6.10.52		

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**.

Edit Manage Install	Tools View	Remote View Hel	р	
ThinManager Server RDS2	🔹 🤤 Remove	DbA 🕄 🚫	😣 Delete 🛛 🔒 Lock	🔍 Find (Ctrl-F)
🚿 Add ThinManager Server	🕑 Refresh	📶 😳 Add Group	🗇 Rename 💣 Unlock	Find Next (F3)
🖋 Disconnect		Сору		
ThinManager Server		E	dit	Find
ThinManager Server	Sumn	nary		
	ThinMana	ger Server	Connection State	Version
- 🔀 RDS1	RDS1		Connected	v11.0 SP1
RDS2	RDS2		Connected	v11.0 SP1

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.

ThinManager	x
Remove ThinManager Server RDS2. Are You Sure?	
Yes No	

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.

8	ThinManager Server List Wizard	x
Thi	nManager Server List Wizard Introduction	\mathbf{R}
The netw conr	ThinManager Server Wizard defines the ThinManager Servers on your vork. These are the servers to which the thinclients can make monitor nections.	
The your	ThinManager Server name must be the name Windows uses to identify computer on the network.	
lf yo If yo The	u are using a DNS server you will only enter the server name. u are not using a DNS server you will enter a server name and IP address. server name will be for reference only.	
	K Back Next > Finish Cancel Help	

3. From the **Auto-synchronization Selection** page of the wizard, <u>un</u>check 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.**

E Computer Management							-		×
	2 🖬 🕨 🗉 🕪								
🌆 Computer Management (Local	O. Services							Actions	
✓ [™] System Tools	ThinServer	Name	Description	Status	Startup Type	Log On As	^	Service	s 🔺
> 🕑 lask Scheduler		Storage Tiers Management	Optimizes t		Manual	Local Syste		M	ore 🕨
Shared Folders	Stop the service	Superfetch	Maintains a	Running	Automatic	Local Syste			
> A Local Users and Groups	Restart the service	Sync Host_5514c	This service	Running	Automatic (D	Local Syste		ThinSe	rver 🔺
> N Performance		Sync Host_bb63f	This service	Running	Automatic (D	Local Syste		Mo	ore 🕨
🛃 Device Manager	Description:	System Event Notification S	Monitors sy	Running	Automatic	Local Syste			
🗸 🔄 Storage	ThinServer	System Events Broker	Coordinates	Running	Automatic (T	Local Syste			
> 🐞 Windows Server Backup		🆏 Task Scheduler	Enables a us	Running	Automatic	Local Syste			
📅 Disk Management		🖏 TCP/IP NetBIOS Helper	Provides su	Running	Manual (Trig	Local Service			
 Services and Applications 		🌼 Telephony	Provides Tel		Manual	Network S			
> 🖣 Internet Information Sei		🖏 Themes	Provides us	Running	Automatic	Local Syste			
Routing and Remote Ac	2	ChinServer	ThinServer	Running	Automatic	tmlab\tms			
WMI Control	_	🔍 Tile Data model server	Start	ng	Automatic	Local Syste			
wivii Control		🍓 Time Broker	Stop	ng	Manual (Trig	Local Service			
		🍓 Touch Keyboard and Han	Pause		Manual (Trig	Local Syste			
		Connect Service	Resume		Manual	Local Syste			
		TP VC Gateway Service	Pertart		Manual	Local Syste			
		Update Orchestrator Serv	Nestart		Manual	Local Syste			
		UPnP Device Host	All Tasks	>	Manual	Local Service			
		User Access Logging Serv	Refrech	ng	Automatic (D	Local Syste			
		User Data Access_5514c	Nerrestr		Manual	Local Syste	10		
		User Data Access_bb63f	Properties		Manual	Local Syste			
		User Data Storage_5514c	Help		Manual	Local Syste			
		User Data Storage_bb63f	ricip		Manual	Local Syste			
		User Experience Virtualizatio	Provides su		Disabled	Local Syste			
		🔐 User Manager	User Manag	Running	Automatic (T	Local Syste			
		User Profile Service	This service	Running	Automatic	Local Syste			
		Wirtual Disk	Provides m		Manual	Local Syste			
		WMware Alias Manager and	Alias Mana	Running	Automatic	Local Syste			
		WMware CAF AMQP Comm	VMware Co		Manual	Local Syste	¥		
< >>	Extended Standard								
Opens the properties dialog box for t	the current selection.								

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

ThinServer Properties (Local Computer)								
General Log On	Recovery Dependencies							
Service name:	ThinServer							
Display name:	ThinServer							
Description:	Thin Server							
Path to executable: "C:\Program Files (x86)\Rockwell Software\ThinManager\thinserver.exe"								
Startup type	Automatic ~							
	Automatic (Delayed Start) Automatic Manual							
Service statu.	Disabled Running	•						
<u>S</u> tart	Stop Pause Resume							
You can specify th from here.	ne start 3 neters that apply when you start the service							
Start para <u>m</u> eters:]						
	OK Cancel Apply							
7. Confirm it has stopped and click **OK**.

ThinServe	er Proper	ties (Local (Computer)		
General	Log On	Recovery	Dependencies		
Service	name:	ThinServer	r		
Display	name:	ThinServer	r		
Descrip	tion:	ThinServe	r		< >
Path to "C:\Pro	executabl gram Files	e: (x86)\Rock	well Software\T	hin Manager\thir	nserver.exe"
Startup	typ <u>e</u> :	Automatic	:		\sim
Service Service	status: Start n specify tl re.	Stopped Stop	meters that appl	ause y when you star	<u>R</u> esume t the service
Start pa	ra <u>m</u> eters:				
		[ОК	Cancel	<u>A</u> pply

- 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.

🕂 🖬 🖬 🖬 🖬 🛨 rds2.tmlab.loc 🛛 🗕 🗗 🗙	
------------------------------------	--

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.

*	New Inbound Rule Wizard	x
Protocol and Ports Specify the protocols and ports to	o which this rule applies.	
Steps: Protocol and Ports Action Profile Name	Does this rule apply to TCP or UDP? • TCP • UDP Does this rule apply to all local ports or specific local ports? • All local ports • Specific local ports: 2031 Example: 80, 443, 5000-5010	

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 <u>un</u>-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.

@	New Inbound Rule Wizard	x
Name		
Specify the name and description	ı of this rule.	
Steps:		
Rule Type		
Protocol and Ports		
Action		
Profile	Name:	
Name		
	Description (optional):	
	InnManager	
	Sack Finish Cancel	

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.

8	Edit Manad	e Install	Tools View	Pamota	View	Help						
Packages	Restore Backu	Restore Bio Backup Biol Synchronize	metric Database metric Database	PXE Thi Server S	inManager Gerver List	Reip Reip DNS Confi Configure Configure Language	guration Default Tern	ninal	Manage Sy Accounts F	ynchronize S Passwords	ettings	Manag Resolve
Tuckuges	1	configuration		Y		Young	Y	- Y		on i	210	
Terminals			Confi	guration	Modules	Schedule	Properti	les	Event Log	Shadow	Repo	nt
	erminais U VersaView520 ZenPad	10			Re	ockw	rell	4	*	2/7/20	196:2	9:0 <mark>6 /</mark>
				A-6.6				5			4	.0
						Overvie	W R	/lixe ecip	er p	eposito	or	Ove
										SII FL 19	LO 1 OUR . 7.2 kg	3

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.

🙀 Thin02 - VMware Workstation 12 Player (Non-commercial use only)	-		×
Player ▼ 📕 ▼ 🛱 🖾			*
Network boot from AMD Am79C970A Copyright (C) 2003–2014 UMware, Inc. Copyright (C) 1997–2000 Intel Corporation			
CLIENT MCC ONDE: 00 50 56 28 27 31 GUID: 564DBD4B-E2B5-5594-870A PXE-E53: No boot filename received	-9E6C1	1847D)	0C9
РХЕ-М0F: Exiting Intel РХЕ ROM. Operating System not found -			

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.

-	💡 New Inbound Rule Wizard	1	×
P	Protocol and Ports		
Sp	pecify the protocols and ports to	v which this rule applies.	
S	teps:		
۲	Rule Type	Does this rule apply to TCP or UDP?	
۲	Protocol and Ports	○ <u>I</u> CP	
۲	Action		
۲	Profile	-	
۰	Name	Does this rule apply to all local ports or specific local ports?	
		○ <u>All local ports</u>	
		Specific local ports: 2 67	
		Example: 80, 443, 5000-5010	
		3	
		< <u>B</u> ack <u>Next</u> > Cancel	

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 <u>un</u>-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.

	New Inbound Rule Wizard		×
N Sp	ame ecify the name and description (of this rule.	
St	eps:		
۲	Rule Type		
۲	Protocol and Ports		
۲	Action		
۲	Profile		
۲	Name		
		Pescription (optional): ThinManager (Second Second Secon	

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.

Protocol and Ports Specify the protocols and ports to which this rule applies. Steps: Public Type Protocol and Ports Action Profile Name Does this rule apply to TCP or UDP? Does this rule apply to all local ports or specific local ports? All local ports Specific local ports Specific	💣 New Inbound Rule Wiza	ard X
Specify the protocols and ports to which this rule applies. Steps: Does this rule apply to TCP or UDP? Protocol and Ports O TCP Action O TCP Profile Does this rule apply to all local ports or specific local ports? O All local ports: 0 Specific local ports: 0 Back Next > Cancel	Protocol and Ports	
Steps: Does this rule apply to TCP or UDP? Protocol and Ports TCP Action Image: Does this rule apply to all local ports or specific local ports? Name Does this rule apply to all local ports or specific local ports? All local ports Image: Does this rule apply to all ports or specific local ports? All local ports Image: Does this rule apply to all ports Image: Specific local ports Image: Does this rule apply to all ports Image: Specific local ports Image: Does this rule apply to all ports Image: Specific local ports Image: Does this rule apply to all ports Image: Specific local ports Image: Does this rule apply to all ports Image: Specific local ports Image: Does this rule apply to all ports Image: Specific local ports Image: Does this rule apply to all ports Image: Specific local ports Image: Does this rule apply to all ports Image: Specific local ports Image: Does this rule apply to all ports Image: Specific local ports Image: Does this rule apply to all ports Image: Specific local ports Image: Does this rule apply to all ports Image: Specific local ports Image: Does this rule apply to all ports Image: Specific local ports Image: Does this rule appl	Specify the protocols and ports	to which this rule applies.
 Rule Type Does this rule apply to TCP or UDP? Protocol and Ports Action Profile Name Does this rule apply to all local ports or specific local ports? All local ports Specific local ports: Example: 80, 443, 5000-5010 	Steps:	
 Protocol and Pots Action Profile Name Does this rule apply to all local ports or specific local ports? All local ports Specific local ports: 2 69 Example: 80, 443, 5000-5010 	Rule Type	Does this rule apply to TCP or UDP?
 Action Profile Name Does this rule apply to all local ports or specific local ports? All local ports (a) Specific local ports: (b) Specific local ports: (c) Specific local ports: (c) Specific local ports: (c) All local ports <li(c) all="" li="" local="" ports<=""> (c) All local ports</li(c)>	Protocol and Ports	О тср
 Profile Name Does this rule apply to all local ports or specific local ports? All local ports § Specific local ports: 2 69 Example: 80, 443, 5000-5010 	Action	
 Name Does this rule apply to all local ports or specific local ports? All local ports Specific local ports: 69 Example: 80, 443, 5000-5010 	Profile	
 All local ports Specific local ports: 69 Example: 80, 443, 5000-5010 	Name	Does this rule apply to all local ports or specific local ports?
(e) Specific local ports: 2 Example: 80, 443, 5000-5010		○ All local ports
Example: 80, 443, 5000-5010		Specific local ports: 2 69
Source Cancel		Example: 80, 443, 5000-5010
3 Cancel		
3 < Back Next > Cancel		
3 < Back Next > Cancel		
< Back Next > Cancel		
< Back Next > Cancel		
< Back Next > Cancel		
<pre>3 </pre> Cancel		
< Back Next > Cancel		
< Back Next > Cancel		3
		< Back Next > Cancel

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 <u>un</u>-check the **Private** and **Public** checkboxes. Click the **Next** button.



23. From the **Name** panel of the **New Inbound Rule Wizard**, enter *UDP*69 as the **Name** and *ThinManager* as the **Description**. Click the **Finish** button.

🔗 New Inbound Rule Wizard		×
Name Specify the name and description of	f this rule.	
Steps:		
Rule Type		
Protocol and Ports		
Action		
Profile		
Name		
	Description (optional):	
	2 ThinManager	
	< <u>B</u> ack <u>Finish</u> Cancel	

- 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.

😼 Thin02 - VMware Workstation 12 Player (Non-commercial use only) –	-	×
<u>P</u> layer ▼ ▼ 🖶 🖂 🔯		*
Rockwell Automation ThinManager Network Boot Loader v2.5		
Status : Loading Firmware from ThinManager Server 192.168.170.1		
Terminal IP Information IP Method PROXY Terminal IP 192.168.170.132 ThinManager Server 192.168.170.1 Router 192.168.170.2 Subnet Mask 255.255.255.0 MAC Address 00:50:56:28:27:31		

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 <u>Section 1</u>. 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:

 $\label{eq:hkey_local_MACHINE} Key_LOCAL_MACHINE \system \currentControlSet \control\TerminalServer \winStations \RDP-Tcp \PortNumber$

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

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.

· · ·	Task Mar	nager			×
File tions View					
Evit Sers Details	Services				
		30%	89%		
Name	Status	CPU	Memory		
Apps (2)					Â
Display client Runtime Framew		0%	21.4 MB		=
▷ 👔 Task Manager		0.3%	8.4 MB		- 51
Background processes (54)					
Adobe Acrobat Update Service		0%	0.7 MB		
🛃 AlmProxyCli Module (32 bit)		0%	3.3 MB		
AOA Server (32 bit)		0%	3.2 MB		
CodeMeter Runtime Server		0%	6.7 MB		
COM Surrogate		0%	2.5 MB		
Command Client Server (32 bit)		0%	4.0 MB		
CommandErrorLogSrv Module (0%	2.7 MB		
👂 🍗 Commons Daemon Service Run		0%	168.3 MB		
Data Acquisition RT Server		0%	2.9 MB		
Datalog Read Client Module (32		0%	2.8 MB		~
Fewer details				End ta	sk

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.

🕿 Terminal Configuration Wizard	×
Module Selection Select the modules that load on this terminal at boot up.	\mathfrak{C}
Installed Modules	
Module	
RDP Experience Module	
RF Ideas pcProx USB Module	
Move Up Mi	ove Down
Add Remove Ci	onfigure Help

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

Attach	Module to Terminal	x	
Module Type	All Modules Show Advanced Module	•	
eGalax Touch Screen Driver			
Hampshire TSHARL Touch Screen Driver			
	Cance		

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.

Configuration Wizard
Module Selection Select the modules that load on this terminal at boot up.
Installed Modules
Module
RDP Experience Module
RE Ideas no Prox LISB Module Key Block Module
Move Up Move Down
Add Configure Remove
< Back Next > Finish Cancel Help

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

		Module Pro	operties			x
Block Ctrl	NO		•	[~	
Block Ctrl+Alt+Del	YES		•			
Block Ctrl+Alt+Enter	YES		-			
Block Ctrl+Esc	YES		-			
Block Alt	NO		•		=	:
Block Alt+F4	NO		-	[
Block Alt+F	NO		-	[
Block Alt+Tab	NO		-	[
Block Alt+Space	NO		•			
Block Windows Key	YES		•			
Block Monu Kou	luo -				~	<u>^</u>
Set to Default						
				Done	Cancel]

20. Click the Finish button.

Sector Terminal Configuration Wizard	X
Module Selection Select the modules that load on this terminal at boot up.	times
Installed Modules	
Module	
RDP Experience Module	
RF Ideas pcProx USB Module	
Key Block Module	
Move Up	Move Down
Add Configure	Remove
< Back Next > Finish Cancel	Help

- 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.

🕿 Terminal Configuration Wizard	×
Module Selection Select the modules that load on this terminal at boot up.	$\mathfrak{>}$
Installed Modules	
Module	
RDP Experience Module	
RF Ideas pcProx USB Module	
Key Block Module	
Manulla	Maua Daum
	MOVE DOWN
Add Remove	Configure
< <u>B</u> ack <u>N</u> ext > Finish Cancel	Help

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

Attach Module to Terminal $ imes$				
Module Type	All Modules Show Advan	▼ ced Modules		
Gunze AHL Touch Sc Hampshire TSHARC Infra-T Touch Scree Key Block Module Key Block Single Key Keyboard Configura Locat Printer Module Locate Pointer Modul MicroTouch Touch Sc Monitor Configuratio Mouse Configuration MultiSession Screen	reen Driver Fouch Screen Driver In Driver Module ion Module ion Module reen-priver In Module Saver Module Saver Module			
MultiStation Configu	OK	Cancel		

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

8	Terminal Configuration Wizard X
	Module Selection Select the modules that load on this terminal at boot up.
	Installed Modules
	Module
	RDP Experience Module
	RF Ideas pcProx USB Module
	Kev Block Module
	Add Remove Configure
	Conguents < Back Next > Finish Cancel Help

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

Locate Pointer Hotkey		F5	•
Locate Pointer Hotkey Modifier	2	NONE	-
Home Pointer Hotkey	3	F6	•
Home Pointer Hotkey Modifier	4	NONE	-
Locator Inactivity Time (seconds)	5	5	
Home Pointer Inactivity Time (see	6	10	
Locator Display Time (seconds)	7	3	

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

🕿 Terminal Configuration Wizard	×
Module Selection Select the modules that load on this terminal at boot up.	\mathfrak{S}
Installed Modules	
Module	
RDP Experience Module	
RF Ideas pcProx USB Module	
Key Block Module	
Locate Pointer Module	
Move Up	Move Down
Add Remove	Configure
< <u>B</u> ack <u>N</u> ext > Finish Cancel	Help

- 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 <u>Section 7</u>, **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.
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.

🕿 Terminal Configuration Wizard		×
Display Client Selection Select the Display Clients to use or	n this terminal	$temp{}$
Available Display Clients EXC_OEECalc FTV_Cookie Demo FTV_Instant Fizz FTV_Studio Camera IPC_Video IPC_Video IPC_Video IPC_Video IPC_Video IPC_Video IPC_Video	Selected Display Clients	
FTV_SuperJuice	•	_
Edit Display Clients	Overrid	e
< <u>B</u> ack	<u>N</u> ext > Finish C	Cancel Help

- 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.

🕿 Terminal Configuration Wizard	×
Module Selection Select the modules that load on this terminal at boot up.	$temp{}$
Installed Modules	
Module	
RDP Experience Module	
RF Ideas pcProx USB Module	
Key Block Module	
Locate Pointer Module	
2	Move Up Move Down
Add Remove	Configure
< <u>B</u> ack <u>N</u> ext > Fi	inish Cancel Help

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

🕿 Terminal Configuration Wizard	×
Module Selection Select the modules that load on this terminal at boot up.	$\mathfrak{>}$
Installed Modules	
Module	
RDP Experience Module	
RF Ideas pcProx USB Module	
Key Block Module	
, Move IIn	Move Down
Move op	MOVEDOWN
Add Remove	Configure
< Back Next > Finish Cancel	Help

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.

🕿 Terminal Configuration Wizard	×
Module Selection Select the modules that load on this terminal at boot up.	\varkappa
Installed Modules	
Module	
RDP Experience Module	
RF Ideas pcProx USB Module	
Key Block Module	
USB Touch Screen Driver	
Redundant Ethemet Module	
MultiSession Screen Saver Module	
Move Up Move Dov	wn
Add Remove Configure	
< <u>B</u> ack <u>N</u> ext > Finish Cancel He	elp

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.

Module Propert	ties
Mode Start Delay Time in secs Switch Interval in secs (Cycle 3) 10	
Set to Default	Cancel

16. Click the Finish button.

🕿 Terminal Configuration Wizard	×
Module Selection Select the modules that load on this terminal at boot up.	times
Installed Modules	
Module	
RDP Experience Module	
RF Ideas pcProx USB Module	
Key Block Module	
MultiSession Screen Saver Module	
	Move Up Move Down
Add Remove	Configure
< Back Next >	Finish Cancel Help

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

S Terminal Configuration Wizard	x
Terminal Group Name Enter the name for the terminal group	\sim
Group Name	
Mixer This must be a unique name using letters, numbers, hyphens (·), and underscores (_) only.	
Description	
Teminal Group Change Group	
Permissions	
< Back Next > [Finish] Cancel Help	

4. Double click the VersaView5200 terminal.



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

🕿 Terminal Configuration Wizard	×			
Terminal Name Enter the name for this terminal, select the terminal group to which this terminal belongs, or choose to copy the configuration from another terminal.				
Terminal Name VersaView5200 This must be a unique name using letters, numbers, hyphens (-), and underscores (_) only.	Description			
- Terminal Group	Change Group			
Copy Settings	Copy From			
Permissions				
< <u>B</u> ack <u>N</u> ext > Finish	Cancel Help			

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

	Select Terminal Group	2 ×
Terminals Mixer		OK Cancel

- 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.
- 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.

8	Terminal Configuration Wizard
	Terminal Group Options Select the options for terminals in this group.
	Terminal Options Group Setting ✓ Allow replacement at terminal if off line Put Terminal in Admin Mode at Startup Enforce Boot Priority
	Terminal Schedule Group Setting Group Settin
	Show terminal status messages Shadowing Allow terminal to be shadowed YES Allow Interactive Shadow
	< Back Finish Cancel Help

- 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 <u>ThinManager Client</u>. 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.

8 T	erminal Configuration Wizard	X		
Module Selection for this Group Select the modules that load on Terminals in this group at boot up.				
Installed Modules				
Module	Pa	ckages		
	Move Up	Move Down		
Add	Configure	Remove		
< Back	Next > Finish Cano	cel Help		

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



22. Click the **Finish** button.

8	Terminal Configuration Wizard			×	
	Module Selection for this Group Select the modules that load on Terminals in this group at boot up.				
	Installed Modules				
	Module		Packages		
	Key Block Module		5.8.1.8.2		
	Add Demove		Move Up	Move Down	
	Add Hemove	Next >	Finish C	Contigure	

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.

🕿 Terminal Configuration Wizard	×
Module Selection Select the modules that load on this terminal at boot up.	\cong
Installed Modules	
Module Rey Block Module RDP Experience Module RF Ideas pcProx USB Module Key Block Module MultiSession Screen Saver Module	
Add Remove	Move Up Move Down Configure
< <u>B</u> ack <u>N</u> ext >	Finish Cancel Help

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

🕿 Terminal Configuration Wizard	×
Module Selection Select the modules that load on this terminal at boot up.	times
Installed Modules	
Module	
Even Block Module	
RDP Experience Module	
RF Ideas pcProx USB Module	
MultiSession Screen Saver Module	
2	Move Up Move Down
Add Remove	Configure
< <u>B</u> ack <u>N</u> ext > F	inish Cancel Help

- 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**.

🙀 Thin02 - VMwar	e Work	station 12 Player (Non-cor
<u>P</u> layer •	æ	u d
📮 CookieDer	mo1	280 - FactoryTalk \
	0	ckwel
Auto	Dr	nation

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.

🕿 Terminal Configuration Wizard		×
Display Client Selection Select the Display Clients to use on this termina	1	$temp{}$
Available Display Clients Image: Splay Clients Image: Splay Clients Image: Splay Clients Image: Splay Clients Image: Splay Clients	Selected Display Clients FTV_CookieDemo FTV_InstantFizz FTV_SuperJuice IPC_Video Override	•
< <u>B</u> ack <u>N</u> ext >	Finish Cancel	Help

 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.

Display Name				
Display Name			Override	6
Windows Login Settings —			Override	
Username 2	labuser@tmlab.	loc	Sear	rch
Password 3	**		Password O	ptions
				_
-			- Override	
Domain			4	
			Verify	User
AppLink Command Line				
Command Line Options			Override	Γ
]				
Video Settings			Override	Г
Resolut	tion	Color Depth		
240x320	Ψ.	256 Colors		
		01		

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.

🕿 Terminal Configuration Wizard	×
Display Client Selection Select the Display Clients to use on this terminal	$temp{}$
Available Display Clients	▲ ▼
Edit Display Clients	
< Back Next > Finish Can	cel Help

- 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.

Q ⁻				- 🗆 X
Edit Manage Install Tools	View Remote View Help			
Packages Configuration	Database PAE ThinManager Configure Database Patabase Server Server List Galaxyage 2	Active Directory	Manage Access Settings Resolvers Groups Relevance	
Terminals	Configuration Properties Schedule Users Session	ns Processes Graph	Event Log Connect Report	-
Truminals	User Session thous RDP-Top#42 labuser RDP-Top#43	Section ID 4 6	State Initial Program Active C: Program Fi Active C: Program Fi	Logon Time 2019-04-02 11:28:02 2019-04-02 18:25:14
🕿 📃 📗 📜 ಿ 🎱 🤔 ະ				

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.

Contraction Wizard	x
System Schedule Edit the system schedule	\aleph
System Schedule	
< Back Next > Finish Cancel	Help

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

	Ev	ent Schedule		x
Select Event Categor	y 1 system		•	
Event Type	Time			
2				
(Add)	Edit	Delete		ОК

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.

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.

Schedule
Event Type
1 Backup Configuration Database 🔹
Backup File Auto Generate Filename Browse Repeat Interval C Once Only C Time Interval
Weekly / Daily Monthly C Yearly
Weekly Schedule Monday Tuesday Wednesday Thursday Friday
🗖 Saturday
Sunday
Time 3 3:38 PM 4 ÷ Cancel OK

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

	Event Schedule		X
Select Event Category	ystem	•	
Event Type	Time		
Backup Configuration Database	every Thursday at 03:38 PM		
Add	Edit Delete		

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.

📙 🛛 🛃 🖬 🖛 🛛 ThinM	lanager			- 🗆	×
File Home Sh	are View				~ ?
← → * 11 «	Program Files (x86) > Rockwell Software > ThinManager	>	✓ Ö Search Thi	nManager	م
📰 Pictures 🛛 🖈	^ Name	Date modified	Туре	Size	^
Advanced	PocoFoundation.dll	12/13/2018 11:51	Application extens	1,196 KB	
Installs	PocoNet.dll	12/13/2018 11:49	Application extens	730 KB	
Lab Files	🚳 termcap	4/1/2019 5:59 PM	Data Base File	4,612 KB	
TMConfigs	👔 ThinManager	12/14/2018 1:09 PM	Compiled HTML	44,723 KB	
- Twiconings	ThinManager	4/2/2019 11:12 AM	Data Base File	536 KB	
💻 This PC	ThinManager.db.shutdown.bak	4/2/2019 11:12 AM	BAK File	536 KB	
📃 Desktop	ThinManager.db.startup.bak	4/2/2019 11:12 AM	BAK File	536 KB	- 6
🛱 Documents 💊	🔀 ThinManager	2/11/2019 12:08 PM	Application	11,538 KB	
Downloads	ThinManagerConfigBackup_2019_04_02_18_36	4/2/2019 6:36 PM	Data Base File	536 KB	
Muric	ThinServer	2/11/2019 12:07 PM	Application	6,775 KB	
	thinservercl.dll	12/20/2018 3:41 PM	Application extens	13 KB	
Pictures	ThinServerSubscriptionCom.dll	12/20/2018 3:39 PM	Application extens	41 KB	
Videos	ThinServerSubscriptionCom.tlb	12/20/2018 10:13	TLB File	4 KB	
🏪 Local Disk (C:)	🗋 tmboot32.bin	8/13/2018 1:52 PM	BIN File	461 KB	
🛖 Shared Folders (tmboot64.bin	8/13/2018 1:52 PM	BIN File	631 KB	
a	TMHistory	4/2/2019 11:12 AM	Data Base File	28 KB	
Vetwork	TMMaster	4/1/2019 6:36 PM	LIC File	2 KB	
34 items 1 item select	ted 536 KB	10/00/0010 10.14	A	1 704 MD	

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.

🕿 Terminal Configu	ration Wizard
Hotkey Configuration Configure the hotkeys to apply to this termin	nal 😤
Teminal Hotkeys	
Enable Instant Failover Hotkey	Change Hotkey
✓ Enable Display Client Hotkeys	Change Hotkeys
✓ Enable Tiling Hotkey	Change Hotkey
Enable Swap Hotkey	Change Hotkey
Enable Fullscreen Hotkey	Change Hotkey
🔽 Enable Main Menu Hotkey	Change Hotkey
< Back Next >	Mouse Button Mapping
< Back Next > F	inish Cancel Help

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.

N	louse Button Mapping		×
	Mouse Button Action		
	Button 1 (Left Mouse)	Go to next display client	^
	Button 2 (Middle Mouse)	Default 💌	
	Button 3 (Right Mouse)	Tile	
	Button 4 (Scroll Wheel Up)	Default 💌	
	Button 5 (Scroll Wheel Down)	Default 🔹	
	Button 6	Default 💌	
	Button 7	Default 💌	
	Button 8	Default 💌	
	Button 9	Default	~
		OK Can	el

- 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.

🕿 Terminal Configuration Wizard	×
Display Client Selection Select the Display Clients to use on this terminal	\aleph
Available Display Clients	•
Edit Display Clients Override	
< Back Next > Finish Cancel	Help

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

Override Settings for 'FTV	_CookieDemo' D	isplay Client		×
Display Name Display Name			Override	
Windows Login Settings		1	Override	
Username	labuser@tmlab.	loc	Searc	
Password			Password Opt	tions
Domain			Override	Г
			Verify U	ser
AppLink Command Line -				
Command Line Options			Override	
Video Settings			Override	
Reso	lution	Color Depth	ovende	
J240X320	<u> </u>	230 COIOTS		
		OK	Car	ncel

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.

🞇 Terminal Configuration Wizard	×
Display Client Selection Select the Display Clients to use on this terminal	\approx
Available Display Clients Remote Desktop Services Camera Terminal Shadow Workstation VNC Virtual Screen	Selected Display Clients
Edit Display Clients	Ovemde
< Back Next >	Finish Cancel Help

- 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.

X	Terminal Configu	uration Wizard	x
Hotkey Con Configure	figuration the hotkeys to apply to this termi	nal	\varkappa
_ Teminal Ho	tkeys		
🗔 Enab	le Instant Failover Hotkey	Change Hotkey	
🔽 Enab	le Display Client Hotkeys	Change Hotkeys	
🔽 Enab	le Tiling Hotkey	Change Hotkey	
🗆 Enab	le Swap Hotkey	Change Hotkey	
🗌 Enab	le Fullscreen Hotkey	Change Hotkey	
🔽 Enab	le Main Menu Hotkey	Change Hotkey	
		Mouse Button N	lapping
< E	Back Next > F	Finish Cancel	Help

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

Mouse Button Mapping		×
Mouse Button Action		
Button 1 (Left Mouse)	1 Default	• ^
Button 2 (Middle Mouse)	Default	•
Button 3 (Right Mouse)	Tile	•
Button 4 (Scroll Wheel Up)	Default	•
Button 5 (Scroll Wheel Down)	Default	•
Button 6	Default	•
Button 7	Default	•
Button 8	Default	•
Button 9	Default	•
1	2	
	OK	Cancel

- 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). <u>Clear the **Command Line Options** text box</u>. Click the **Finish** button.

Program Path and Filename:

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

🕿 Display Client Wizard	×
App Link Enter the linked application path.	times
AppLink Path	
Program Path and Filename	
rogram Files (x86)\Rockwell Software\ThinManager\Th	nin Manager.exe
-	Browse
Command Line Options	
2	
	Browse
Start in the following folder	
	Browse
0	
3	
< <u>Back</u> <u>N</u> ext> FinishCa	ncel Help

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, <u>remove</u> the existing **Display Clients** from the **Selected Display Clients** list box, and <u>add</u> 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.
- 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.

🕿 Terminal Configura	ation Wizard	×	
Log In Information Enter the log in information to log in automatically. Leave the log in information blank or fill only some of the fields to force manual log in.			
Windows Log In Inf	omation		
Usemame	thin01@tmlab.loc Search		
Password	** Password Options		
Domain	Verify		
	(Back Next) Finish Concel	Help	
	Cancel	neip	

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.


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.



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.

🕿 ThinManager Server Configuration \	Vizard	×
ThinManager Security Groups Assign access to ThinManager func	tions for Windows User Groups.	\preccurlyeq
Windows User Group	Delete Group	
Administrators		
Administrators	Add Group	
V Thin Manager Administrators		
A Thin Manager Power Users	5	
ThinManager Shadow Users		
	Reset Sessions	
	Kill Processes	
	Reboot Terminal Servers	
	Logoff Term.Secure Users	
	Administer Thin Manager Servers 🗸	
< >	>	
	Current Permissions	
< Back Next > Fir	nish Cancel Help	

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.

ThinManager Server Configuration Wizard X
ThinManager Security Groups Assign access to ThinManager functions for Windows User Groups.
Windows User Group Thin Manager Users
Vindows User Group Permissions Available Allowed
Shadow Interactive Shadow Reset Sessions Kill Processes Reboot Terminal Servers Connect Restart Terminals Connect to Terminal Servers Connect to Terminals Connect to Terminals Connect Terminals Connect Terminals Connect Terminals Connect Terminals
Current Permissions
A section of the s

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 <u>Section 10</u>, 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 <u>Section 10</u>. 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.

Acce	ss Groups
Unrestricted All Users All Terminals All Locations Engineer	<u></u> OK
	Edit
	Add
	Delete
	Calc Permissions

3. Click the Select Windows Security Group button.

	Access Group	x
Enter Group Name	Select Windows Security Group	OK Cancel
		Edit Members

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.

Select Security Group to	Add 🛛 🗙	:
Domain Users Engineer Enterprise Admins Enterprise Read-only Domain Controllers Group Policy Creator Owners HelpLibraryUpdaters Haintenance Operator	<u>^</u>	
Protected Users Arrow Controllers Schema Admins Supervisor WinRMRemoteWMIUsers		
	OK Cancel	

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

	Access Group	X
Enter Group Name	Maintenance	ОК
	Select Windows Security Group	Cancel
		Edit Members

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

Access Groups	x
Unrestricted All Users All Terminals All Locations Engineer Maintenance	
	Add
	Delete
	Calc Permissions
3	

Create Maintenance User Group

1. Click the **Users** icon ¹ 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.

🕿 Relevance User Configuration Wizard
Relevance User Group Information Enter the Relevance User Group name.
AD Synchronization Group Group Name User Name Password Verify Password Customize
Password Options PIN Options Group Setting
Group Change Group
Permissions 2 < Back

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.

🙄 Relevance User Configuration Wizard	×
Relevance User Information Enter Relevance username, password and permission information.	\aleph
Customize	
Group Change Group	
Copy Settings from another User Copy From	
Permissions	
< Back Next > Finish Cancel	lelp

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

	Search for AD User	×
Filter	Recurse Security Groups	Locations
Name	User Principal Name	
	ОК	Cancel

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

		Locations
Filter Contai	Recurse IV	Search
Name	User Principal Name	
loc01	loc01@tmlab.loc	
loc02	loc02@tmlab.loc	
loc03	loc03@tmlab.loc	
loc04	loc04@tmlab.loc	
loc05	loc05@tmlab.loc	=
Mike 1	mike@tmlab.loc	
oscar	oscar@tmlab.loc	
sid	sid@tmlab.loc	
tab01	tab01@tmlab.loc	
tab02	tab02@tmlab.loc	
tab03	tab03@tmlab.loc.	
tah04	tab04@tmlab.loc	

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

Active Directory U	lser omation	
AD User Name	Mike	
	Customize Password Options PIN Options	
Group	Change Group	
Copy Settings	ettings from another User Copy From	
	Permissions	

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.

Relevance Settings			×
Location Transfer Timeout	15	seconds	
Location Transfer Extension Time	15	seconds	
Bluetooth Device Name Filter Prefix	ACP-		
Beacon GUIDs			
			Add
			Delete
			Edit
Enable iPhone Beacons			
Allow New Resolvers to be registered	$\overline{\mathbf{v}}$		
		OK	Cancel

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.

		1												
	Edit Ma	nage	Install	Tools	View	Rem	ote View	Help				2		
Packages	Restore Ba	ckup	Restore Bi Backup Bi Synchroni	iometric Da iometric Da ize	atabase Itabase	PXE Server	ThinManage Server List	Register DNS Configuration Register Default Terminal Configure Default Terminal	Manage Account	Synchroniz Passwords	e Settings	Manage Resolver	Access Groups	<u>Settings</u>
Packages		Co	onfiguration	n				Manage	J 4	ctive Directo	ory		Relevance	e

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

Res	olver Management		×	
	lame	Type QR Code	Add Delete Edit Search	
1				

 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.

Add New Reso	lver X
Name	1 Бт
Description	
Туре	2 Bluetooth
Data	3 2F234454-CF6D-4A0F-ADF2-F4911BA9FFA6.1.1
	OK Cancel

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.

			💲 🗔 🖬 12:35 PM
Settings			
RELEVANCE RESOLVERS			
Register QR Code			
Register Bluetooth Beacon			
Register WiFi Access Point			
CAMERA			
Set Camera Location			
DEBUGGING			
Debug Logging: Disabled			
	Ĵ	D	

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

1 = 1			🗱 🖨 ‹፡›؛ 🛢 7:41
Settings			
RELEVANCE RESOLVERS			
Register QR Code			
Register GPS Location			
Register Bluetooth Beacon			
Register WiFi Access Point			
CAMERA			
Set Camera Location			
DEBUGGING			
Debug Logging: Disabled			
	\triangleleft	0	

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.

⊡∓⊡⊘	0,						*	🔜 🔜 2:15 PM
aTMC		ENTER ID	ENTIFIER N	AME				
		Data: LGX_	CookieDemo					
		Enter Name:	<u>MixerHMI</u>					
			CANCEL US	E DATA AS NA				
MixerHMI	MissoURI	ModerN	MiddlETOn	MiserY	MuseuMS	MuseuM	MisogYNY	Mod 🔽
1	[!] 2 [@]	3 #	4 ^{\$} 5	5 6	5 [^] 7 ⁸	8	9 (0)
^I p	w 1	e r	t	у	u	i	o p	×
а	S	d	f g	h	· j ;	k		Done
Ŷ	z	x c	v	b ⁻	n	m ′	!?	Ŷ
\$	1@#	2		<u> </u>			, .	:-)
			\bigtriangledown	$\overline{\Box}$	[T		iii

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

□ ± □ ⊘ 0,		\$ ⊑	2:15 PM
aTMC	ENTER IDENTIFIER NAME		
i i i	Data: LGX_CookieDemo		
	Enter Name: MixerHMI		
8	SUCCESS		
MixerHMI MissoU	Resolver Successfully Registered	sogYNY	Moci 🔽
1 2		9 ()
q [w]	ок	р ⁺	
a s	d f g h j k	1	Done
ी ट	x c v b n m ¹ !	?	Û
‡ 1@#	y ,	•	:-)

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.

8	Location Configuration Wizard
Lo	c ation Name Enter Name for this location
1	Mixer_Fence
	This must be a unique name using letters, numbers, hyphens (-), and underscores (_) only.
	Description
	Change Group
	opy Settings
	Permissions 2 C Back Next > Finish Cancel Help

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		Location Configuration Wizard	x				
'	Relevance Resolver Selection Assign Relevance Resolvers to this location						
1	Relevance Resolvers						
	Name	Type Action					
	<	m					
	Add	Delete Edit					
	< Back	Next> Finish Cancel H	elp				

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

Choose a Relevance Res	olver	×
		Only Show Unassigned Resolvers
Resolver Name	1 ра	•
Resolver Description	-	
Resolver Type	Bluetooth	
Choose Action	2 Clone	•
	-	3 Settings
		Permissions
		OK Cancel

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.

Bluetooth Resolver Sett	ings X
RSSI to Log In	-64
RSSI to Log Out	-74
ОК	Cancel

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

•			
Choose a Relevance Resolver			×
		Only Show Unassigne	d Resolvers 🔎
Resolver Name	btb		•
Resolver Description			
Resolver Type	Bluetooth		
Choose Action	Clone		•
			Settings
			Permissions
		OK	Cancel

11. Click the **Finish** button.

Location Config	guration Wizard				>
Relevance Re Assign Relev	solver Selection rance Resolvers to thi	s location			
Relevance Resol	vers				
Name	Type		Action		
btb	Bluetooth		Clone		
Add	Delete	Edit]		
	< <u>B</u> ack	<u>N</u> ext >	Finish	Cance	el Help

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.

8	Location Configuration Wizard
Lo	cation Name Enter Name for this location
ć	ocation Name
	This must be a unique name using letters, numbers, hyphens (-), and underscores (_) only.
	Description
	Change Group
C	Copy Settings from another Location
	Permissions 2 3 3 3 4 3 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5

- 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.

🕿 Location Configuration Wizard		×
Display Client Selection Select the display clients to use at this loca	ation	
Available Display Clients	Selected Display Clients	
FTV_LookeDemo FTV_InstantFizz FTV_Studio GX_CookieDemo SmartSession GT_Comera Terminal Shadow		•
Edit Display Clients	Override	
< Back New	xt > Finish Cancel Hel	p

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.

8	Location Configuration Wizard
Windows Log Enter Windo	In information ws usemame and password information.
- Windows Log I	n Information
Username Password	1 loc02@tmlab.loc Search 2
Domain	Venfy Password Options
	4
< Bac	k Next > Finish Cancel Help

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

8		Location Cor	nfiguration	Wizard		x
'	Relevance Resolver Selection Assign Relevance Resolvers to this location					
1	Relevance Resolvers					
	Name	Туре		Action		
	<				>	
	Add	Delete	Edit			
	< Back	Next >	Finish	Cancel	Help	

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

Choose a	Relevance Resolver
	Only Show Unassigned Resolvers
Resolver Name	lixerHMI 🗨
Resolver Description	
Resolver Type QF	R Code
Choose Action	orce Transfer
	Settings
	3 [Permissions]
	OK Cancel

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

Permissions			
TermSec	cure Access Groups		
Available All Terminals All Users Maintenance Unrestricted	Member Of Engineer		
		2	

9. Click the **OK** button.

Choos	e a Relevance Resolver	x
	Only Show Unassigne	ed Resolvers 🕅
Resolver Name	MixerHMI	-
Resolver Description		
Resolver Type	QR Code	
Choose Action	Force Transfer	-
		Settings
		Permissions
	ОК	Cancel

10. Click the Add button.

8	Location Configu	ration Wizard	x		
Relevance Re Assign Rele	Relevance Resolver Selection Assign Relevance Resolvers to this location				
Relevance Reso	lvers				
Name	Туре	Action			
MixerHMI	QR Code	Force Transfer			
<		>			
Add	Delete Edi	2			
< Bac	k Next> Fir	nish Cancel H	lelp		

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

Choose	e a Releva	ance Resolver
		Only Show Unassigned Resolvers 🔲
Resolver Name	MixerHMI	•
Resolver Description		
Resolver Type	QR Code	
Choose Action	Shadow	•
-		Settings
		3 Permissions
		OK Cancel

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

Permissions			
TermSe	cure Access Groups		
Available All Terminals All Users Engineer Unrestricted	Member Of Maintenance		
	2		

13. Click the **OK** button.

Choos	e a Relevance Resolv	er 🛛 🗙
	Only Show Ur	assigned Resolvers 🔲
Resolver Name	MixerHMI	•
Resolver Description		
Resolver Type	QR Code	
Choose Action	Shadow	•
		Settings
		Permissions
	ОК	Cancel

14. Click the **Finish** button.

Relevance Resolve	Type		Action	
MixerHMI MixerHMI	QR Code QR Code		Force Transfer Shadow	
			-1	
Add	Delete	Edit		

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 **International** 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.

🞇 Display Client Wizard	×
Display Client Members Select the Remote Desktop Servers for this Display Client.	$temp{}$
Available Remote Desktop Servers Selected Remote Desktop Serve	ers
RDS1 (10.6.1.51) RDS2 (10.6.1.52)	
	•
Edit Server List	
2	
<pre> < Back Next > Cancel</pre>	Help

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.

8	Terminal Configuration Wizard	x	
Terminal Mode Selection Select the operating modes for this terminal			
Tem	ninal Mode		
	I ✓ Enable Relevance User Services		
1	✓ Enable Relevance Location Services		
	Enable MultiMonitor		
	Enable MultiStation		
	2		
	< Back Next > Finish Cancel	Help	

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

🕿 Terminal Configuration Wizard	×
Display Client Selection Select the Display Clients to use on this terminal	times
Available Display Clients	Selected Display Clients
Edit Display Clients	Override

- 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.

8	Terminal Configuration Wizard	x
	Relevance Options Select the types of Relevance Resolvers to use on this client. Optionally choose an assigned location for this client	\prec
	Assigned Location	
	Options Enabled Resolver Types Finable QR Code Location Ids Enable Bluetooth Locations Enable GPS Locations Enable Wi-Fi Locations	
	Use Force Transfer to restore Assigned Location Allow selection of Location manually Enforce fencing on manual Location selection Confirm before entering a location Resolver Update Interval 3000 ms	
	< Back Next > Finish Cancel Help	

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



11. Click the Finish button.

Sector Terminal Configuration Wizard	X
Relevance Options Select the types of Relevance Resolvers to use on this client. Op choose an assigned location for this client	otionally
Assigned Location Mixer_Fence\Mixer_HMI	Change Clear
Options Enabled Resolver Types Carbon Code Location Ids Enable Bluetooth Locations Enable GPS Locations Enable Wi-Fi Locations	
Use Force Transfer to restore Assigned Location Allow selection of Location manually Enforce fencing on manual Location selection Confirm before entering a location Resolver Update Interval	
< Back Next > Finish Cance	el Help

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.

🖻 🛨 🦷 📾				*	3:53	3 PM
aTMC						
	Select Terminal Create new T	to Replace: erminal	CAI	NCEL		
	Ð	<u>ن</u>	D			

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.

🕿 Terminal Configuration Wizard	×
Display Client Selection Select the Display Clients to use on this terminal	\cong
Available Display Clients Remote Desktop Services Desktop EXC_OEECalc FTV_CookieDemo FTV_InstantFizz FTV_Studio LGX_CookieDemo GSmartSession TM_AdminConsole Camera	Selected Display Clients
Edit Display Clients 2 < Back Next >	Override Finish Cancel Help

8. From the **Terminal Interface Options** page of the wizard, check the **Enable Tiling** checkbox.

🕿 Terminal Configuration Wizard	×
Terminal Interface Options Select the display client selector and main menu options that	will be available on the terminal.
Display Client Selection Options	
Show Selector on Terminal	Selector Options
1 🔽 Enable Tiling	Tiling Options
Screen Edge Display Client Selection	
Allow Display Clients to move to/from screen	
Main Menu Options	
	Main Menu Options
- PIN Pad Uptions	PIN Pad Options
2	,
< Back Next > Fin	ish Cancel Help

9. From the **Relevance Options** page of the wizard, click the **Clear** button followed by the **Finish** button.

🕿 Terminal Configuration Wizard	×
Relevance Options Select the types of Relevance Resolvers to use on this client. Optionally choose an assigned location for this client	\aleph
Assigned Location	
Mixer_Fence\Mixer_HMI Change	
Options Enabled Resolver Types Enable QR Code Location Ids Enable Bluetooth Locations Enable GPS Locations	
Linable WiFri Locations Use Force Transfer to restore Assigned Location Allow selection of Location manually Enforce fencing on manual Location selection Confirm before entering a location Resolver Update Interval 3000 ms	
A Back Next > Finish Cancel	Help

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 <u>not</u> 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. <u>P</u>reboot e<u>X</u>ecution <u>E</u>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.

🚭 VMware Workstation 12 Player (Non-commercial use	only)	– 🗆 X
<u>P</u> layer ▼ ▶ ▼ 🖶 🛱 🔯		
Home	Welco Work	ome to VMware station 12 Player
Thin01	+	Create a <u>New Virtual Machine</u> Create a new virtual machine, which will then be added to the top of your library.
		Open a Virtual Machine Open an existing virtual machine, which will then be added to the top of your library.
		Upgrade to VMware Workstation Pro Get advanced features such as snapshots, virtual network management, and more.
	?	H <u>e</u> lp View online help.
		This product is not licensed and is authorized for non- commercial use only. For commercial use, purchase a license. <u>Buy now.</u>

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

New Virtual Machine Wizard	\times			
Welcome to the New Virtual Machine Wizard A virtual machine is like a physical computer; it needs an operating system. How will you install the guest operating system?				
Install from:				
◯ Installer <u>d</u> isc:				
No drives available \sim				
O Installer disc image file (iso):	_			
✓ Browse				
1				
 I will install the operating system later. 				
The virtual machine will be created with a blank hard disk.				
2				
Help < Back Next > Cance	9			

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.

New Virtual Machine Wizard			×
Select a Guest Operating Sys Which operating system will	stem be installed on	this virtual machine	=?
Guest operating system			
Version Other		0	~
Help	< Back	Next >	Cancel

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.

New Virtual Machine Wizard	×
Name the Virtual Machine What name would you like to use for this virtual machine?	
Virtual machine name: Thin03	
C: \Users\labuser.TMLAB\Documents\Virtual Machines\Thin03	Browse
2	
< <u>B</u> ack <u>N</u> ext >	Cancel

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

New Virtual Machine Wizard X
Specify Disk Capacity How large do you want this disk to be?
The virtual machine's hard disk is stored as one or more files on the host computer's physical disk. These file(s) start small and become larger as you add applications, files, and data to your virtual machine. Maximum disk <u>size</u> (GB):
 Store virtual disk as a single file Split virtual disk into <u>multiple</u> files Splitting the disk makes it easier to move the virtual machine to another computer but may reduce performance with very large disks.
Help < <u>B</u> ack <u>N</u> ext > Cancel

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

New Virtual Machine	Wizard	×	
Ready to Create Virtual Machine Click Finish to create the virtual machine. Then you can install Other.			
The virtual machine v	vill be created with the following settings:		
Name:	Thin03	^	
Location: C:\Users\abuser.TMLAB\Documents\Virtual Machines			
Version: Workstation 12.0			
Operating System:	Other		
Hard Disk:	8 GB, Split		
Memory:	256 MB		
Network Adapter:	NAT		
Other Devices:	CD/DVD, Sound Card	×	
<u>C</u> ustomize Hardwa	are		
	< <u>B</u> ack Finish Cance	1	

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

dware		
Device Memory Processors New CD/DVD (Summary 256 MB 1 Auto detect	Device status Connected Connect at power on
Network Adapter	NAT	Network connection
🐠 Sound Card 💻 Display	Auto detect Auto detect	O Bridged: Connected directly to the physical network Replicate physical network connection state
		Configure Adapters
		○ NAT: Used to share the host's IP address
		O Host-only: A private network shared with the host
		○ Custom: Specific virtual network
		VMnet0 (Bridged)
		OLAN segment:
		LAN <u>S</u> egments Ad <u>v</u> anced
	Add <u>R</u> emove	3
		Close Help

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.

Name: Thin03 Location: C:\Users\Jabuser.TMI	
Location: C:\Users\labuser.TML	
er josere jababer i me	AB\Documents\Virtual Machines
Version: Workstation 12.0	
Operating System: Other	
Hard Disk: 8 GB, Split	
Memory: 256 MB	
Network Adapter: Bridged (Automatic)	
Other Devices: CD/DVD, Sound Card	

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**.



-	-				
🔜 🗹 🔜 🖛 Thin03				- 0	×
File Home Share	View				~ 🕐
← → ∽ ↑ 📘 > Tł	nis PC > Documents > Virtual Machines >	Thin03	✓ Ö Search Thi	n03	Q
^	Name	Date modified	Туре	Size	
📌 Quick access		A/22/2010 0:13 DM	NVRAM File	0 KB	
📃 Desktop 🛛 🖈	A Thin03	4/22/2019 5:13 PM	VMware virtual dis	1 KB	
🕂 Downloads 🖈	Thin03 ymsd	4/22/2019 9:12 PM	VMSD File	0 KB	
🔮 Documents 🖈	Thin03	4/22/2010 0.14 PM	VMware virtual m	3 KB	
Pictures 🖈	Thin03 ymyf	4/22/2019 9:12 PM	VMXE File	1 KB	
Lab Files	A Thin03-s001	4/22/2019 9:12 PM	VMware virtual dis	512 KB	
This 01	A Thin03-s002	4/22/2019 9:12 PM	VMware virtual dis	512 KB	
	A Thin03-s003	4/22/2019 9:12 PM	VMware virtual dis	64 KB	
Thin02	ymware	4/22/2019 9:13 PM	Text Document	185 KB	
TMConfigs	ymware-0	4/22/2019 9:12 PM	Text Document	29 KB	
💻 This PC		1/ 22/ 2013 512 1111		20110	
Desktop					
Documents					
Downloads					
b Music					
Pictures					
🐺 Videos					
Local Disk (C)					
10 items					

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

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

🔜 🗹 🔜 🖛 Thin03	1		– 🗆 🗙
File Home Share	View		-m 🕐
Navigation Details pane	Extra large icons Large icons Medium icons Small icons List Endotes	Sort by ✓ Hidden items	lected Options
Panes	Layout	Current view Show/hide	1 // D
👆 Downloads 🖈	Thin02.umad	4/22/2019 9:12 PM VIVIWare VIItual dis	IND
🛱 Documents 🖈	Thin02.vmv	4/22/2019 9:12 PM VM3D File	2 1/2
Pictures 🖈	Thin03.vmvf	4/22/2019 5:14 PM VMWare Vitual III	1 KB
Lab Filer	Thin03-s001 ymdk	4/22/2019 9:12 PM VMware virtual dis	512 KB
Thi=01	Thin03-s002.vmdk	4/22/2019 9:12 PM VMware virtual dis	512 KB
	A Thin03-s003.vmdk	4/22/2019 9:12 PM VMware virtual dis	64 KB
I hin02	vmware.log	4/22/2019 9:13 PM Text Document	185 KB
TMConfigs	vmware-0.log	4/22/2019 9:12 PM Text Document	29 KB
💻 This PC			
E Desktop			
🖆 Documents			
👆 Downloads			
b Music			
Pictures			
Videos			
10 items			

- 🔜 | 🕑 🔜 🗢 | Thin03 \times _ File Home Share View \sim 2 ← → ~ ↑ → This PC → Documents → Virtual Machines → Thin03 5 V Search Thin03 Q ^ Name Date modified Туре Size 📌 Quick access Thin03.nvram 4/22/2019 9:13 PM NVRAM File 9 KB 📃 Desktop å Thin03.vmdk 4/22/2019 9:12 PM VMware virtual dis... 1 KB 🕹 Downloads * Thin03.vmsd 4/22/2019 9:12 PM VMSD File 0 KB 🗄 Documents 🖈 🗗 Thin03.vmx 4/22/2019 9:14 PM VMware virtual m... 3 KB Pictures 📄 Thin03.vmxf KF File 1 KB -Open with VMware Player 📥 Thin03-s001.vmdk Lab Files 🖶 Scan with Windows Defender... vare virtual dis.. 512 KB 🐣 Thin03-s002.vmdk Thin01 Open with Notepad 🐣 Thin03-s003.vmdk hin02 📆 VMware Player Share with vmware.log TMConfigs Restore previous versions Search the Store vmware-0.log Choose another app > 💻 This PC Send to 📃 Desktop Cut 🗄 Documents Сору 🕹 Downloads Create shortcut Music Delete Pictures Rename 📲 Videos Properties Local Dick (Ci) 10 items | 1 item selected 2.05 KB
- 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.
- 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.

🕿 PXE Server Wizard	×
Network Interface Configuration Select the settings for each network interface	\aleph
Select Interface to Configure	
AWS PV Network Device #0	•
Interface Primary IP Address 10.6.1.51	
PXE Server Mode C Using standard DHCP server Using standard DHCP server on this machine Using standard DHCP server with Boot Options (PXE Disabled) Not using standard DHCP server	
□ IP Address Conflict Detection	_
C None	
Allow New PXE clients	
< Back Next > Finish Cancel	Help

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

🕿 PXE Server Wizard		×
IP Address Range Configu Configure each range of IF	ration Addresses	\aleph
Beginning IP Address	Ending IP Address	1
Add	Delete	Edit
< <u>B</u> ack <u>N</u> ext >	Finish Cance	Help

- 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

IP Address Range	Х
Starting IP Address 10 10 . 6 . 10 . 100	
Ending IP Address 2 10 . 6 . 10 . 110	
Subnet Mask 3 255 . 255 . 255 . 0	-
Router IP Address 4 10 . 6 . 10 . 1	
Exclusions Reservations Advanced	1
Clear IP Assignments 5	
(OK) Cancel	

6. Back at the **IP Address Range Configuration** page of the wizard, click the **Finish** button.

Configure each range of	IP Addresses	
Beginning IP Address	Ending IP Address	
10.6.1.100	10.6.1.110	
Add	Delete	Edit

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.

🕿 Terminal Configuration Wizard		×
Display Client Selection Select the Display Clients to use on this tem	ninal	$temp{}$
Available Display Clients Remote Desktop Services Content Desktop Conte	Selected Display Clients	•
Edit Display Clients	✓ Override	
<u>Z</u>	t> Finish Cancel H	Help

- 11. Click the Next button on the Terminal Interface Options page of the wizard.
- 12. Click the Next button on the Relevance Options page of the wizard.
- 13. Click the Next button on the Hotkey Configuration page of the wizard.
- 14. On the Log In Information page of the wizard, enter *thin02@tmlab.loc* as the Username and *rw* as the Password. Click the Verify button which should confirm that the credentials entered are valid. Click the Next button.

🕿 Terminal Configu	ration Wizard			×
Log In Informatic Enter the log in some of the fiel	n information to log in automatic ds to force manual log in.	ally. Leave the log in inf	ormation blank or fill only	\aleph
Windows Log In I	nformation			
Usemame	1 thin02@tmlab.loc		Search	
Password	2 -		Password Options	
Domain			3 Verify	
	•			
	< <u>B</u> ack Next >	Finish	Cancel	Help

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

🕿 Terminal Configura	ation Wizard				×
Video Resolution Select the video	resolution for this	teminal.			st
Select Video Resolu	ution				
These are	the resolutions su	pported by the Thin (Client model yo	ou selected.	
Resolu	tion	Color Dept 64K Colors	h •	Refresh Rate	_
			0		
	< <u>B</u> ack	<u>N</u> ext >	Finish	Cancel	Help

Re-enable Firewall Rules

In <u>Section 11</u>, 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.

🔗 Windows Firewall				-	×
← → → ↑ 🔗 > Control Pan	el > System and Security > Windows Firewall		ٽ ~	Search Control Panel	9
Control Panel Home	Help protect your PC with Windows Fire	ewall			
Allow an app or feature through Windows Firewall	Windows Firewall can help prevent hackers or malic Internet or a network. 	ious software from gaining access to your PC through the			
Change notification settings	Do <u>m</u> ain networks	Connected 🔗			
Turn Windows Firewall on or off	Networks at a workplace that are attached to a don	nain			
Restore defaults	Windows Firewall state:	On			
Advanced settings Troubleshoot my network	Incoming connections:	Block all connections to apps that are not on the list of allowed apps			
	Active domain networks:	tmlab.loc			
	Notification state:	Do not notify me when Windows Firewall blocks a new app			
	P <u>r</u> ivate networks	Not connected \odot			
	Guest or <u>p</u> ublic networks	Not connected 📎			
See alco					
Security and Maintenance					
Network and Sharing Center					

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 <u>Section 11</u>. Right click it and select **Disable Rule**.



 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.

📕 The Wiresh	ark Network Analyzer		-	
<u>F</u> ile <u>E</u> dit <u>V</u> i	ew <u>G</u> o <u>C</u> apture <u>A</u> nalyze <u>S</u> tatistics Telephon <u>y W</u> ireles	s <u>T</u> ools <u>H</u> elp		
🧉 🔳 🙆 🔘	📙 🛅 🕱 🛅 9. 🗇 🗢 🕾 🗿 🕹 📃 📃 9. 9.	€,⊞		
Apply a displa	y filter <ctrl-></ctrl->			Expression +
A				
1	Welcome to Wireshark			
	Capture			
•	using this filter: 📙 Enter a capture filter	*	All interfaces shown $ imes$	
	Ethernet0 M			
	Learn			
	User's Guide · Wiki · Questions and Answers · Mailing	Lists		
	You are running Wireshark 3.0.0 (v3.0.0-0-g937e33de). You receive a	utomatic updates.		
Ready to I	pad or capture	No Packets		Profile: Default

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.

💋 Capturing from Ethernet0							- 0	×
File Edit View Go Capture	Analyze Statistics	s Telephony Wireless	Tools Help					
	९ 👄 🔿 🕾 👔		1					
heath	•••=•		•				Evoracci	on ±
рооф							- Cxpress	JII T
No. Time Source	e	Destination	Port Src Port De	s Protocol	Length Into			^
981 1 67994 Vmwa	re_10:25:ce	Broadcast		ARP	60 Who has 10.6	5.10.254? Tell 10.6.10.50		
982 16.7 424 10.6	.10.50	10.6.10.51	4241 50012	TCP	439 4241 → 50012	2 [PSH, ACK] Seq=5/76 Ack=1381 Win=20	49 Len=385	
983 16.728 9 10.6	.10.51	10.6.10.50	50012 4241	TCP	146 50012 → 4241	L [PSH, ACK] Seq=1381 Ack=6161 Win=20	51 Len=92	
964 16.758051 10.6	10.50	10.0.10.51	4241 50012	NDCC	60 4241 → 50012	2 [ACK] Sed=0101 ACK=1475 W1N=2049 Le	n=ø	
965 16 838789 10.6	10.51	10.0.10.52	49764 445	NDSS	55 NBSS Continu	acton Hessage		
900 10.030700 10.0	10.51	10.0.10.52	49705 445	NRSS	55 NBSS Continu	lation Message		
988 16 839858 10 6	10.52	10.6.10.52	45/00 445	TCP	66 445 - 49784	[ACK] Seg-1 Ack-2 Win-2048 Len-0 SLE	-1 SPE-2	
989 16 839858 10 6	10.52	10.6.10.51	445 49785	TCP	66 445 - 49785	[ACK] Seg=1 Ack=2 Win=2050 Len=0 SLE	=1 SPE=2	
990 16.830858 10.6	.10.52	10.6.10.51	445 49786	TCP	66 445 → 49786	[ACK] Seg=1 Ack=2 Win=2050 Len=0 SLE	=1 SRE=2	
								¥
> Transmission Control Pro	tocol, Src Port:	49746, Dst Port: 133	2, Seq: 1, Ack	: 1, Len:	0			
0010 00 28 0b 8d 00 00 80	06 06 d2 0a 06	0a 34 0a 06 · (····						
0020 0a 32 c2 52 05 34 10	56 al 51 81 9e	cd a9 50 10 · 2·R·4	·V ·Q····P·					
0030 08 04 b6 e8 00 00 00	00 00 00 00 00							
😑 🍸 "bootp" is deprecated or ma	ay have unexpected res	ults. See the User's Guide.			F	Packets: 990 · Displayed: 990 (100.0%)	Profile: [Default 🔡

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.

VirtualTC - VMware Workstation 15 Player $\qquad \qquad \qquad$						
?	Cannot connect the virtual device ide1:0 because no corresponding device is available on the host.					
	Do you want to try to connect this virtual device every time you power on the virtual machine?					
	<u>Y</u> es <u>N</u> o					

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**.

	(*E	therr	net													_		×
Fil	e	Edit	View	Go	Capture	Analyze	Statistic	Telephony	Wireless	Tools I	Help							
		1			NO.	9 00 0	. 😎 🕢		ΘΘ	0.11								
				i lovel	And the	• •	- = 0			-							Typroscion	- L - L - L
	DOC	ψ	-		-													T
No		1000	lime	24.0	Source			Destination		Port Src	Port Des	Protocol	Length Info	- C1	T 11	70 0 0 0 05		
F	4	7990	45.316	216	0.0.0	.0		255.255.25	5.255	6	s 5	7 DHCP	590 DHCP	Discover	- Transaction	ID 0x2ac0a25e		
		2352	45.510	103	0.0.0			255 255 255	5 255	6	8 6		590 DHCP	Discover	- Transaction	TD 0x2ac0a25e		
		2353	46 028	407	0.0.0			255 255 25	5 255	6	8 6		590 DHCP	Discover	- Transaction	TD 0x2bc0a25e		
	8	3687	47.401	297	0.0.0	.0		255.255.25	5.255	6	в 6	7 DHCP	590 DHCP	Discover	- Transaction	ID 0x2cc0a25c		
	8	3688	47.401	303	0.0.0	.0		255.255.25	5.255	6	8 6	7 DHCP	590 DHCP	Discover	- Transaction	ID 0x2cc0a25e		
L	9	9851	51.267	418	0.0.0	.0		255.255.255	5.255	6	8 6	7 DHCP	590 DHCP	Discover	- Transaction	ID 0x2dc0a25e		
<																		>
>	Fn	ame	7990: 5	590 b	ytes on 1	wire (47	20 bits)	, 590 bytes	capture	d (4720 b	its) on	interfac	e 0					
>	Et	hern	et II,	Src:		c0:a2:5e	(00:0c:	29:c0:a2:5e	e), Dst:	Broadcast	: (ff:ff:	ff:ff:ff	f:ff)					
>	In	tern	et Prot	tocol	Version	4, Src:	0.0.0.0	, Dst: 255.	255.255.	255								
>	Us	er D	atagrar	n Pro	tocol, S	rc Port:	68, Dst	Port: 67										
>	Dy	nami	c Host	Conf	iguratio	n Protoc	ol (Disc	over)										
00	00	ff	ff ff	ff fi	f ff 00 0	Эс 29 с	0 a2 5e	08 00 45 00)	· E ·							^
00	10	02	40 00	00 00	0 00 14 1	l1 a4 a	e 00 00	00 00 ff ff	· @ · · ·									
00	20	ff	ff 00	44 00	ə 43 02 2	2c 4b f	d 01 01	06 00 2a c0	· · · D ·	с., к	.*.							
00	30	a2	5e 00	04 80	00 00 0	00 00 0	0 00 00	00 00 00 00										
00	40	00	00 00	00 00	00 00 0	1C 29 C	0 az se	00 00 00 00 00)								
00	60	00	00 00	00 00	3 00 00 0	30 00 0 30 00 0	0 00 00	00 00 00 00 00 00 00 00										
00	70	00	00 00	00 00	00 00 0	00 00 0	0 00 00	00 00 00 00 00										
00	80	00	00 00	00 00	00 00 0	0 00 00	0 00 00	00 00 00 00										
00	90	00	00 00	00 00	a oo oo e	90 00 O	0 00 00	00 00 00 00										
00	a0	00	00 00	00 00	a oo oo e	00 00 06	0 00 00	00 00 00 00		• • • • • • • • •								
00	b0	00	00 00	00 00	00 00 0	0 00 0	0 00 00	00 00 00 00										~
0)	/ v	vireshark_	Ethern	net_2019042	23125534_	a03648.pca	png					Pa	kets: 1094429	9 • Displayed: 7 (0.0	1%)	Profile: De	fault

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.

1	🗃 T🊹 - VMware Workstation 12 Player (Non-commercial use only) — 🛛 🛛 🛛 🛛 🗖								
<u>P</u> lay	rer 🕶 📔 💌 🖧 💢				۲	(📰			
	<u>F</u> ile	>							
2	Power	> >	<u>P</u> ower On						
\odot	<u>R</u> emovable Devices	>	Shut D <u>o</u> wn Guest						
÷	Send <u>C</u> trl+Alt+Del	Ш	Suspend Guest	2A-5440-1F45-4EDD-279	IF49CØA	125E			
*	<u>M</u> anage	>(3	<u>R</u> estart Guest	ed.					
j (ji)	Full Screen Ctrl+Alt+Enter								
	<u>U</u> nity								
i i	Help	>							
	E <u>x</u> it								

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**.

🚭 Thin03 - VMware Workstation 12 Player (Non-commercial use only)	- 🗆 X	(
<u>P</u> layer ▼ ▼ ⊕ ⊐ ∑	« 📱	
Network boot from AMD Am79C970A Copyright (C) 2003-20 Copyright (C) 1997-20 Receives IP address		
CLIENT MAC ADDR: 00 0C 23 C0 A2 5E GUID: 564D342 CLIENT IP: 10.6.1.100 MASK: 255.255.255.0 DHCP GATEWAY IP: 10.6.1.1 PXE-E32: TFTP open timeout TFTP	2A-5440-1F45-4EDD-279F49C0A25E IP: 10.6.1.51 m ThinManager.	
PXE-E32: TFTP open timeout		

 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.

	(*Eth	ernet						-	- 🗆 🗙
Fil	e E	dit View Go	Capture Analyze	Statistics Telephony Wireless	Tools Help				
1		0 0 0	🕅 🖸 🔍 ⇔ ⇒	🕾 T 🕹 其 📃 Q, Q,	Q. 🎹				
	bootp)							Expression +
No.		Time	Source	Destination	Port Src Pr	ort Des Protocol	Length Info		^
Ι.	378	64 174.083146	10.6.10.51	255.255.255.255	67	68 DHCP	377 DHCP Offer	- Transaction ID 0x2deeb	cc4
	378	65 174.083151	10.6.10.51	255.255.255.255	67	68 DHCP	377 DHCP Offer	- Transaction ID 0x2deeb	cc4
	429	86 190.165497	0.0.0.0	255.255.255.255	68	67 DHCP	590 DHCP Request	- Transaction ID 0x2deeb	cc4
	429	87 190.165502	0.0.0	255.255.255.255	68	67 DHCP	590 DHCP Request	- Transaction ID 0x2deeb	cc4
	429	88 190.166079	10.6.10.51	255.255.255.255	67	68 DHCP	377 DHCP ACK	- Transaction ID 0x2deeb	cc4
L	429	89 190.166082	10.6.10.51	255.255.255.255	67	68 DHCP	377 DHCP ACK	- Transaction ID 0x2deeb	cc4
<									>
	R	elay agent IF	address: 0.0.0.0						^
	c	lient MAC add	ress: Vmware_ee:bc	::c4 (00:0c:29:ee:bc:c4)					
	C	lient hardwar	e address padding:	00000000000000000000					
	S	erver host na	me: RDS1						
	B	oot file name	: acpboot.bin						
	M	lagic cookie:	DHCP						
	> 0	ption: (67) E	ootfile name						
	> 0	ption: (43) \	endor-Specific Inf	ormation (PXEClient)					
	> 0	otion: (53) [HCP Message Type (Offer)					*
00	fØ	00 00 00 00 0	0 00 00 00 00 00	00 00 00 00 00 00	• • • • • • • • • • • •				^
01	10	00 00 00 00 00 0	0 00 00 00 00 00 00			1			
01	20	6f 6f 74 2e 6	2 69 6e 00 2b 0d	45 6C 61 65 76 62	in +····				
01	30	00 01 0a 06 0	a 33 ff 35 01 02	01 04 ff ff ff 00	3-5				
01	40	03 <mark>04</mark> 0a 06 0	a 01 42 0a 31 30	2e 36 2e 31 30 2e 📑	·B· 10.6.10.				
01	50	35 31 82 07 4	1 43 50 5f 50 58	45 3c 09 50 58 45 51 · A	CP_ PXE< PXE				
01	50	60 43 6c 69 65 6e 74 36 04 0a 06 0a 33 33 04 00 05 Client633							
101	10	/ +0 00 04 0	a 00 0a 51 TT	~@···	· · T ·	1			~
C	🔵 🍸 Relay agent IP address (dhcp.ip.relay), 4 bytes 🛛 Profile: Default 🗋								

 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.

1	🖼 T🊹 - VMware Workstation 12 Player (Non-commercial use only) - 🛛 🗙								
<u>P</u> lay	rer 🕶 📘 💌 🕂 🖳 💐							«	
	<u>F</u> ile	>	2						
2	Power	>	►	<u>P</u> ower On					
\odot	<u>R</u> emovable Devices	>		Shut D <u>o</u> wn Guest					
ц.	Send <u>C</u> trl+Alt+Del		Ц	Suspend Guest	2A-5440-1F45-4EDD-279F49	9C0A25E			
х,	<u>M</u> anage		3	<u>R</u> estart Guest	ed.				
j (jic)	Full Screen Ctrl+Alt+Ente	r							
	<u>U</u> nity								
i i	Help	>							
	E <u>x</u> it								

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.

🚭 Thin03 - VMware Workstation 12 Player (Non-commercial use only)	-		×
Player 🕶 📕 🕶 🛱 🖾		«	-
Rockwell Automation ThinManager Network Boot Loader v2.5			
Status : Loading Firmware from ThinManager Server 10.6.10.51			
Terminal IP Information IP Method PXE Terminal IP 10.6.10.100 ThinManager Server 10.6.10.51 Router 10.6.10.1 Subnet Mask 255.255.255.0 MAC Address 00.0c:29:ee:bc:c4			

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.

🔗 Windows Firewall with Advanced	🔐 Windows Firewall with Advanced Security						
File Action View Help							
🗢 🄿 🙋 📰 🗟 🔽 🗊							
 Windows Firewall with Advance Inbound Rules Outbound Rules Connection Security Rules Monitoring 	Inbound Rules Name RSAlarmFileReader.exe RSAlarmFileReader.exe RSLinx.exe ESLinx.exe	Group					
	 RSLinx.exe RSLinx.exe RSLinx.exe RsvcHost.exe RsvcHost.exe RsvcHost.exe RsvcHost.exe Studio 5000 Logix Designer v30.01.00 (CP Studio 5000 Logix Designer v30.01.00 (CP 						
	TCP2031 V UDP67 V UDP69 V Mware Authd Service V Ware Authd Service (pr V Studio.exe V Studio.exe	Enable Rule Cut Copy Delete Properties Help					

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.

🖷 Thin03 - VMware Workstation 12 Player (Non-commercial use only) - 🛛							
<u>P</u> layer ▼	• 🕂	H A		*			
		This Terminal is Undefined on Server RDS1 Choose the Terminal to Replace or Action		.]			
Status :	Name	Туре					
	Create	new Terminal					
	Mixer	Group					
		Ter minur					

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).

∠ *Ethernet0		– 🗆 X
<u>File Edit View Go Capture Analyze Statistics</u>	Telephon <u>y W</u> ireless <u>T</u> ools <u>H</u> elp	
	J 🗐 🗏 @ Q @ 🎹	
tfp		Expression +
No. Time Source De	Pestination Port Src Port	t Des Protocol Length Info
2361 3217.531203 10.6.10.51 10	0.6.10.101 56777 52	146 TFTP 1205 Data Packet, Block: 14 (last)
2361 3217.531207 10.6.10.51 10	0.6.10.101 56777 52	146 TFTP 1205 Data Packet, Block: 14 (last)
2361 3217.531579 10.6.10.101 10	0.6.10.51 52146 56	777 TFTP 46 Acknowledgement, Block: 14
2361 3217.531580 10.6.10.101 10	0.6.10.51 52146 56	777 TFTP 46 Acknowledgement, Block: 14
2361 3218.048308 10.6.10.101 10	0.6.10.51 36445 69	TFTP 96 Read Request, File: 8.2\\module_usbtouch.mod, Transfer type: oc
2361 3218.048312 10.6.10.101 10	0.6.10.51 36445 69	TFTP 96 Read Request, File: 8.2\\module_usbtouch.mod, Transfer type: oc
2361 3218.058899 10.6.10.51 10	0.6.10.101 567/8 364	445 IFIP 69 Option Acknowledgement, tsize=29250, blksize=1432
2361 3218.058903 10.6.10.51 10	0.6.10.101 567/8 364	445 IFIP 69 Option Acknowledgement, tsize=29250, biksize=1432
2501	0.0.10.51 50445 50	776 TFTP 46 Acknowledgement, block: 0
2362 3218 050722 10 6 10 51 10	0.0.10.51 50445 50 0.6.10.101 56778 36	1/6 IFIP 46 Acknowledgement, block: 6
> Frame 28358: 103 bytes on wire (824 bits).	103 bytes cantured (824 bits)	on interface 0
Ethernet II, Src: Vmware 27:4c:72 (00:50:56	6:27:4c:72). Dst: Vmware 9c:d4:	:c7 (00:0c:29:9c:d4:c7)
> Internet Protocol Version 4, Src: 10.6.10.4	49, Dst: 10.6.10.101	
> Internet Control Message Protocol	-	
0000 00 0c 29 9c d4 c7 00 50 56 27 4c 72 08	8 00 45 00 ···)····P V'Lr··E·	
0010 00 59 08 42 00 00 80 01 09 c1 0a 06 0a	a 31 0a 06 · Y·B·····1··	
0020 0a 65 03 03 25 09 00 00 00 00 45 00 00 0030 00 00 14 11 7e 04 0a 05 0a 65 0a 06 0a	a 31 08 1f	
0040 00 45 00 29 ee 39 00 01 61 63 70 62 6f	f 6f 74 2e ·E·)·9·· acpboot.	
0050 62 69 6e 00 6f 63 74 65 74 00 62 6c 6b	o 73 69 7a bin octe t blksiz	
0060 65 00 31 34 35 36 00	e∙1456∙	
Wireshark_Ethernet0_20190409102822_a04936.pcapr	ng	Packets: 272337 · Displayed: 41790 (15.3%) Profile: Default

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.

	Programs and Features	
	Power Options	
	Event Viewer	
	System	
	Device Manager	
	Network Connections	
	Disk Management	
	Computer Management	
	Command Prompt	
	Command Prompt (Admin)	
	Task Manager	
	Control Panel	
	2 File Explorer	
	Search	
	Run	
	Shut down or sign out	
1	Desktop	
	· · · · · · · · · · · · · · · · · · ·	4

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

	= Th	iin03	3						—	o ×
File Hom	ne	Sh	are	View						~ 🕐
\leftrightarrow \rightarrow \cdot \cdot	$\leftarrow \rightarrow \sim \uparrow 1$ This PC > Documents > Virtual Machines > Thin03 $\sim \eth$ Search Thin03						م			
📌 Quick ac	cess		^	Name		Date modified 4/23/2019 4:22 PM	Type NVRA	/I File	Size 73 KB	
Deskto	р	*		📇 Thin03.vmdk		4/23/2019 12:40 PI	M VMwa	re virtual dis	1 KB	
🕂 Downlo	oads	*		Thin03.vmsd		4/23/2019 12:40 PI	M VMSD	File	0 KB	
🛱 Docum	ients	*	2	Thin03.vmx		A/32/2010 A.22 DK/		re virtual m	3 KB	
Picture	s	*	г	Thin03.vmxf	Open wit	th VMware Player	F	File	1 KB	
📙 Lab File	25			Thin03-s001.vmdk	Scan with	Windows Defender		re virtual dis	512 KB	
Thin01				Thin03-s002.vmdk	Open wit	n	4	Notepad		
📑 Thin02				Thin03-s003.vmdk	Share wit	h	>	C VMware P	layer	
TMCon	nfigs			vmware.log	Restore p	revious versions		Search the	Store	
💻 This PC				Thware-0.log	Send to		>	Choose an	other app	
📃 Desktoj	р				Cut					
🔮 Docum	ents				Сору					
🕹 Downlo	oads				Create sh	ortcut				
👌 Music					Delete					
Nicture	s				Rename					
📑 Videos					Propertie	s				
10 items 1 item selected 2.06 KB										

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"

Thin03.vmx - Notepad × File Edit Format View Help numa.autosize.cookie = "10001" ۸ uuid.bios = "56 4d 34 2a 54 40 1f 45-4e dd 27 9f 49 c0 a2 5e" uuid.location = "56 4d 34 2a 54 40 1f 45-4e dd 27 9f 49 c0 a2 5e" migrate.hostlog = ".\Thin03-8d6ed9e3.hlog"
ide0:0.redo = "" pciBridge0.pciSlotNumber = "17" pciBridge4.pciSlotNumber = "21" pciBridge5.pciSlotNumber = "22" pciBridge6.pciSlotNumber = "23" pciBridge7.pciSlotNumber = "24" scsi0.pciSlotNumber = "16" ethernet0.pciSlotNumber = "32" sound.pciSlotNumber = "33" vmci0.pciSlotNumber = "34" ethernet0.generatedAddress = "00:0c:29:c0:a2:5e" ethernet0.generatedAddressOffset = "0" vmci0.id = "1237361246" monitor.phys_bits_used = "42" vmotion.checkpointFBSize = "33554432" vmotion.checkpointSVGAPrimarySize = "33554432" cleanShutdown = "TRUE" softPowerOff = "FALSE" ide1.0 startConnected = "FALSE" 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 **VirtuaITC** 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.

Æ *Ethernet			- L ;	×				
File Edit View Go Capture Analyze Statis	tics Telephony Wireless	Tools Help						
	🗿 J. 🚍 📃 Q. Q. (ə, 🎹						
		•						
bootp			Expression	+				
No. Time Source	Destination	Port Src Port Des Protocol	Length Info	^				
2705 749.665139 0.0.0.0	255.255.255.255	68 67 DHCP	389 DHCP Discover - Transaction ID 0xf1eb431c					
2705 749.675610 10.6.10.51	255.255.255.255	67 68 DHCP	363 DHCP Offer - Transaction ID 0xfleb431c					
2705 749.675615 10.6.10.51	255.255.255.255	67 68 DHCP	363 DHCP Offer - Transaction ID 0xf1eb431c					
2715 753.616990 0.0.0.0	255.255.255.255	68 67 DHCP	401 DHCP Request - Transaction ID 0xfleb431c					
2/15 753.616994 0.0.0.0	255.255.255.255	68 67 DHCP	401 DHCP request - Transaction ID 0xfleb431c					
2715 752 617467 10.6.10.51	200.200.200.200	67 68 DHCP	363 DHULACK - Transaction ID 0x11eb431c					
2715 753 626415 10 6 10 100	10 6 10 51	4011 4011 DHCP	389 n pxyDHCP Request - Transaction ID 0x1eb451c					
2715	10.6.10.51	4011 4011 DHCP	389 coxyDHCP Request - Transaction TD 0x3acacb3d					
2717 754.622061 10.6.10.100	10.6.10.51	4011 4011 DHCP	38 proxyDHCP Request - Transaction ID 0x3acacb3d					
4				• *				
Hops: 0				1				
Seconds elansed: 0								
> Bootn flags: 0x8000 Broadcast flag	Seconds elapsed: 0							
Client IP address: 0.0.0.0	(b) budduse)							
Your (client) IP address: 10.6.10.10	0							
Next server IP address: 10.6.10.51								
Relay agent IP address: 0.0.0.0				~				
00-0 00 00 00 00 00 00 00 00 00 00 00 00	a aa aa aa aa							
00d0 00 00 00 00 00 00 00 00 00 00 00 00	0 00 00 00 00							
00e0 00 00 00 00 00 00 00 00 00 00 00	0 00 00 00 00							
00f0 00 00 00 00 00 00 00 00 00 00 00 00	0 00 00 00 00							
	0 00 00 00 00	a. SaC taba						
0120 6f 74 33 32 2e 65 66 69 99 35 91 9	2 01 04 ff ff 0t32.e	fi .5						
0130 ff 00 03 04 0a 06 0a 01 42 0a 31 3	0 2e 36 2e 31	·· B·10.6.1						
0140 30 2e 35 31 82 07 41 43 50 5f 50 5	8 45 3c 09 50 0.51··	AC P_PXE<·P						
0150 58 45 43 6c 69 65 6e 74 36 04 0a 0	6 0a 33 33 04 XEClie	nt 633.						
0160 00 05 /e 40 06 04 0a 06 0a 31 ff	· · ~@ · ·			~				
🔵 🌋 Relay agent IP address (dhcp.ip.relay), 4 bytes			Packets: 291112 · Displayed: 69 (0.0%) Profile: Default	t				

- 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.

@	New Inbound Rule Wizard				
Rule Type Select the type of firewall rule to c	areate.				
Steps: Protocol and Ports Action Profile Name	What type of rule would you like to create? Program Rule that controls connections for a program. Predefined: BranchCache - Content Retrieval (Uses HTTP) Rule that controls connections for a Windows experience. Custom Custom rule. Cancel				

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 <u>un</u>-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.

🔐 New Inbound Rule Wizard X								
N Sp	Name Specify the name and description of this rule.							
S	leps:							
۲	Rule Type							
۲	Protocol and Ports							
۲	Action							
۲	Profile	9	Name:					
۲	Name	•	00F4011					
			Description (optional):					
		2	ThinManager					
			9					
			O					
			< Back Finish Cance	el				

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

www.rockwellautomation.com

Power. Control and Information Solutions Headquarters

Publication XXXX-XX###X-EN-P — Month Year Supersedes Publication XXXX-XX###X-EN-P — Month Year

Copyright© 2019 Rockwell Automation, Inc. All rights reserved.