

Application Technique

Original Instructions

ThinManager and FactoryTalk View SE Deployment Guide



Contents

Background	4
Goal of Configuration Guide	4
Terminology and Abbreviations.....	4
Versions.....	5
Failover versus Redundancy	6
Workgroup versus Domain Deployments.....	6
Server Preparation	7
Configure Windows Firewall	7
User Account Control (UAC).....	11
Data Execution Prevention (DEP).....	13
Remote Desktop Services Role Installation and Configuration	14
Domain Environment Setup.....	14
Remote Desktop Services Licensing Role Installation.....	21
Remote Desktop Services Licensing Role Configuration.....	24
Workgroup Deployments.....	28
Install Remote Desktop Services RD Host and Licensing Server	28
Configure Remote Desktop Licensing	33
Configure Local Group Policy	34
Create Local Users.....	39
Install FTVSE	41
Publish Remote Applications (Domain Environment Only)	45
Create a RemoteApp for FactoryTalk View SE	50
FactoryTalk View SE Client Configuration	53
FactoryTalk Security	53
ThinManager Installation.....	62
System Preparation.....	62
Software Installation.....	67
FactoryTalk Activation.....	72
FactoryTalk View SE Client Licenses.....	76
Redundancy	76
Synchronization.....	76
ThinManager Configuration.....	80

Display Servers	80
Display Clients	82
Smart Session	83
Session Scaling	84
Failover.....	85
Terminal Configuration	88
ThinManager Ready Terminals - VersaView 5200	93
ThinManager Compatible Terminals (PXE/UEFI)	98
ThinManager Clients (iTMC, aTMC, WinTMC)	100
MultiMonitor and MultiSession.....	103
FactoryTalk View SE MultiMonitor Option with ThinManager.....	106
ThinManager Security	111
Active Directory Integration and Relevance Users	111
Authentication Pass-Through	116

Background

FactoryTalk View® Site Edition (SE) is a supervisory human machine interface (HMI) software package for enterprise solutions. It can be purchased as a stand-alone HMI (SE Station), or as a distributed and scalable HMI (SE Server) that supports distributed-server/multi-user applications, giving maximum control over information where you want it. ThinManager can be deployed with either SE Station and/or SE Server. This guide will focus on deploying ThinManager with SE Server, as this is the most common architecture.

View SE is composed of the following primary components:

- FactoryTalk View Studio: Configuration software for developing and testing HMI applications.
- FactoryTalk View SE Server: HMI Server that stores HMI project components and serves these components to clients.
- FactoryTalk View SE Client: HMI Client for viewing and interacting with supervisory-level applications developed with FactoryTalk View Studio.

These components can be installed on a single server, or distributed across multiple servers. For smaller, less critical applications, these components can be located on a single server.

Goal of Configuration Guide

The goal of this Configuration Guide is to provide specific guidance on how to deploy View SE using ThinManager. It is not intended to replace the various FactoryTalk View SE nor ThinManager documentation, but to instead highlight the specific elements that require attention when deploying View SE in a Remote Desktop Server environment, managed by ThinManager. As such, every feature and option of ThinManager will not be described or demonstrated.

Terminology and Abbreviations

Microsoft renamed the Terminal Services components to Remote Desktop Services for the Windows Server 2008 R2 release. Terminal Services and Remote Desktop Services are often used interchangeably, but since this document will focus on View SE 11.0 in a Windows Server 2012 R2 architecture, the Remote Desktop Services terminology will be used.

DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Server
HMI	Human Machine Interface
FTV	FactoryTalk View SE
FTD	FactoryTalk Directory
FTA	FactoryTalk Activation
NLA	Network Level Authentication
PXE	Pre-boot Execution Environment
RDSCAL	Remote Desktop Services Client Access License
SE	Site Edition
TSCAL	Terminal Services Client Access License

Versions

This document will focus on the deployment of FactoryTalk View SE version 11.0 within a ThinManager version 11.0 environment.

View SE version 11.0 supports the following server class operating systems:

- Windows Server 2016 Standard Edition – 64 Bit Only
- Windows Server 2012 R2 Standard Edition – 64 Bit Only
- Windows Server 2012 R2 Datacenter Edition – 64 Bit Only
- Windows Server 2012 Standard Edition – 64 Bit Only
- Windows Server 2012 Datacenter Edition – 64 Bit Only
- Windows Server 2008 R2 Standard Edition (with and without Service Pack 1) – 64 Bit Only
- Windows Server 2008 R2 Enterprise Edition with Service Pack 1 – 64 Bit Only
- Windows Server 2008 Standard Edition with Service Pack 2 – 32 Bit or 64 Bit

ThinManager 11.0 supports the following server class operating systems:

- Windows Server 2019 Standard Edition – 64 Bit Only
- Windows Server 2016 Standard Edition – 64 Bit Only
- Windows Server 2012 R2 Standard Edition – 64 Bit Only
- Windows Server 2012 R2 Datacenter Edition – 64 Bit Only
- Windows Server 2012 Standard Edition – 64 Bit Only
- Windows Server 2012 Datacenter Edition – 64 Bit Only
- Windows Server 2008 R2 Standard Edition – 64 Bit Only
- Windows Server 2008 R2 Enterprise Edition – 64 Bit Only
- Windows Server 2008 Standard Edition – 32 Bit or 64 Bit

Therefore, ThinManager is supported in all of the server class operating systems that View SE 11.0 supports.

This configuration guide will utilize Windows Server 2012 R2 Standard Edition – 64 Bit Only.

ThinManager can also be installed on workstation operating systems like Windows Vista, Windows 7, Windows 8 or Windows 10. For the purposes of this configuration guide, the server class operating systems will be the focus, since they alone offer the Remote Desktop Services role, which will enable multiple remote desktop connections to a single server OS; whereas the workstation class OS only provides a single remote desktop connection.

In this configuration guide, two new images will be created - a primary Remote Desktop Server named RDS1, and a secondary Remote Desktop Server named RDS2. Each server will be configured with the Remote Desktop Services role. It is important that this role be added to the Remote Desktop Server first, before any applications are installed. Once installed, the View SE client software as well as ThinManager will be installed on both servers (although ThinManager is not required on each RDS Server, it is in this configuration guide to demonstrate ThinManager Redundancy). They will then be joined to an existing FactoryTalk Directory that exists on a third server named FTHMI, which will also be

the FactoryTalk Activation Server. These FactoryTalk roles can be broken out into separate servers per recommendations from Rockwell Automation, but they are being consolidated for simplification purposes. For the purposes of this configuration guide, the HMI server will be the only FactoryTalk View SE HMI Server, but redundant View SE architectures are also suitable. The Cookie Demo sample application will be utilized.

Failover versus Redundancy

It is important to understand the difference between Failover and Redundancy with regard to ThinManager, as they are often considered the same thing, but they are in fact very different. Failover is included in all ThinManager licensing and is the ability for a ThinManager terminal to automatically failover between Remote Desktop Servers to receive its content. Redundancy, on the other hand, is having two ThinManager installs whose configurations are automatically synchronized. With Redundant ThinManager installations, terminals would be able to receive their firmware and terminal configurations from either one. This guide will demonstrate how to configure both Failover and Redundancy.

Workgroup versus Domain Deployments

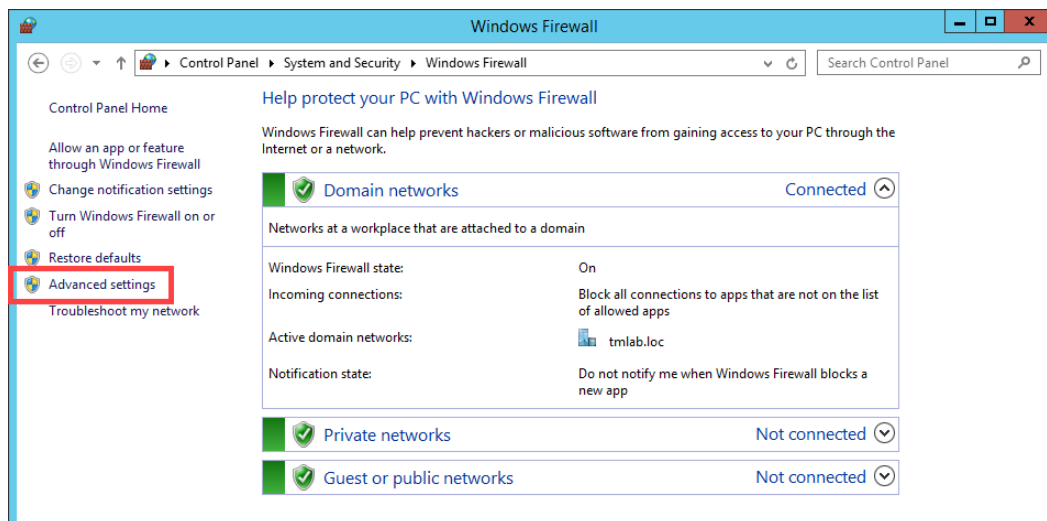
Both ThinManager and FactoryTalk View SE can be deployed in either Workgroup or Domain environments. The process required to configure the Microsoft Remote Desktop Services role differs on Windows Server 2012 depending on whether a Workgroup or Domain is being utilized. This guide will serve as a document to deploy ThinManager in either type of environment, however it is recommended that a Domain environment be used. It is outside of the scope of this document to cover setting up a Domain Controller. For more information on setting up a domain controller, the PlantPAx documentation can be used.

Server Preparation

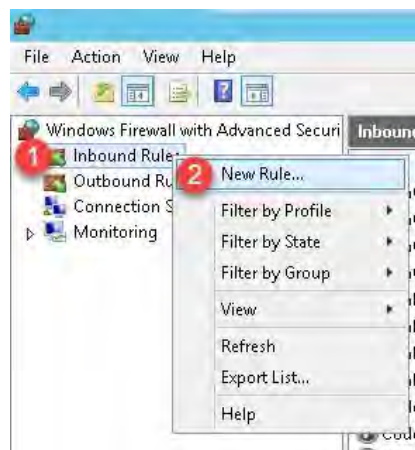
This section will cover the required configuration that should be made to the Windows Server in preparation for deploying ThinManager in a Remote Desktop Services environment. The windows firewall can be disabled or configured to allow ThinManager to communicate to its terminals and to synchronize with a Redundant ThinManager server. We will show how to configure the windows firewall, which is the recommended setting.

Configure Windows Firewall

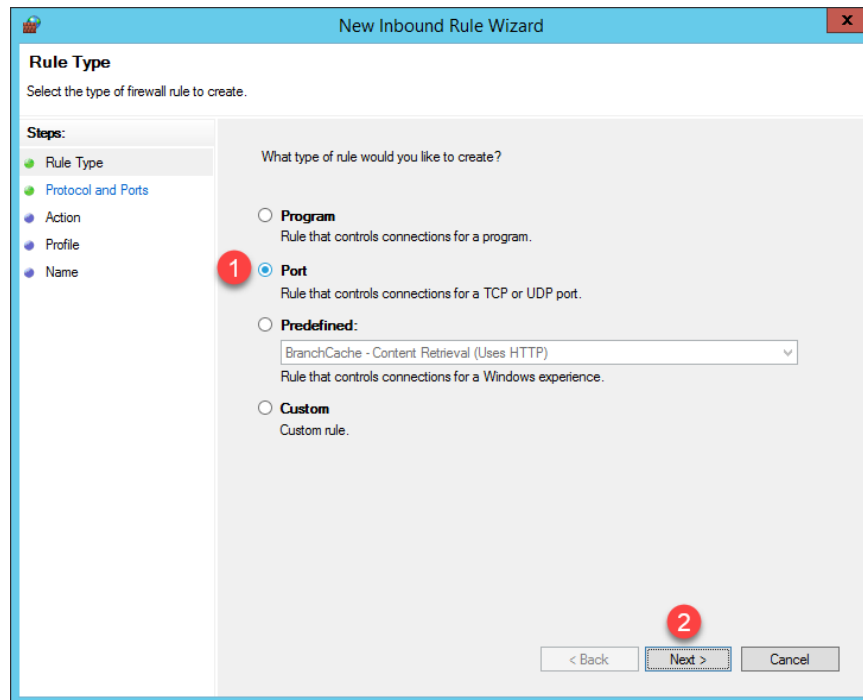
1. Return to the **Windows Firewall** page of the **Control Panel** on **RDS1** and click the *Advanced Settings* link.



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



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



New Inbound Rule Wizard

Rule Type
Select the type of firewall rule to create.

Steps:

- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

What type of rule would you like to create?

☐ **Program**
Rule that controls connections for a program.

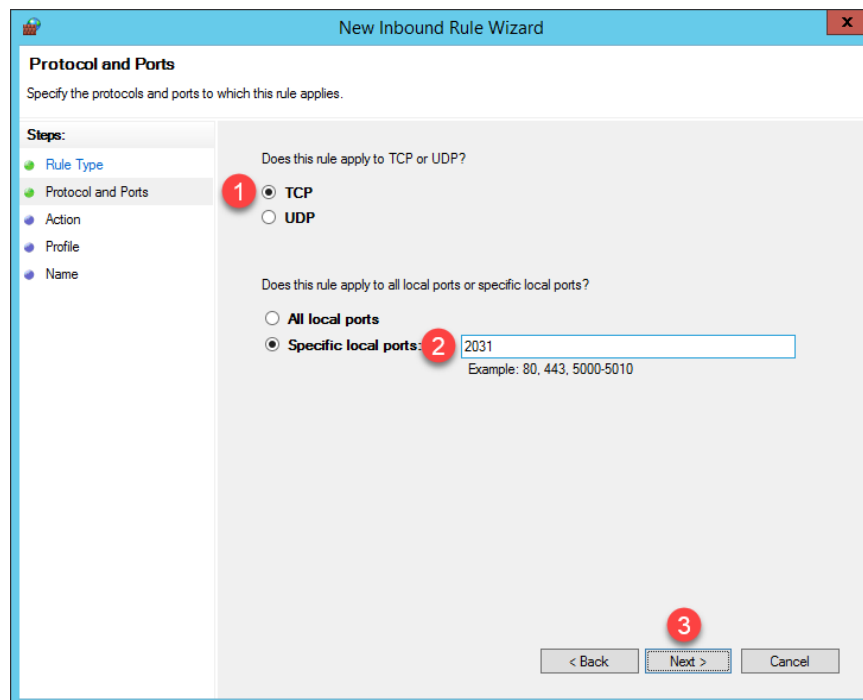
☒ **Port**
Rule that controls connections for a TCP or UDP port.

☐ **Predefined:**
BranchCache - Content Retrieval (Uses HTTP)
Rule that controls connections for a Windows experience.

☐ **Custom**
Custom rule.

< Back **Next >** Cancel

- 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

Protocol and Ports
Specify the protocols and ports to which this rule applies.

Steps:

- Rule Type
- 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?

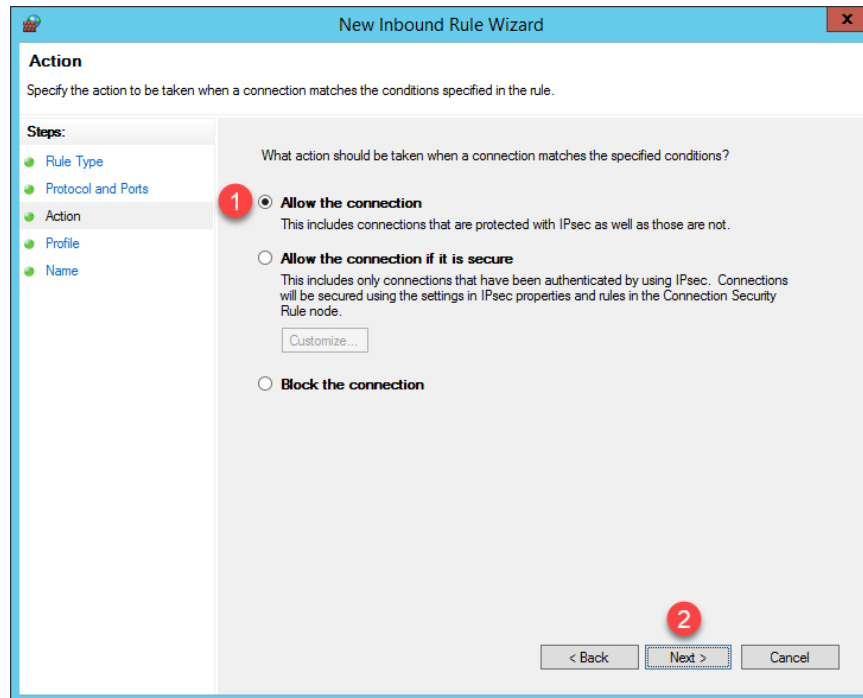
☐ **All local ports**

☒ **Specific local ports:** 2031
Example: 80, 443, 5000-5010

< Back **Next >** Cancel

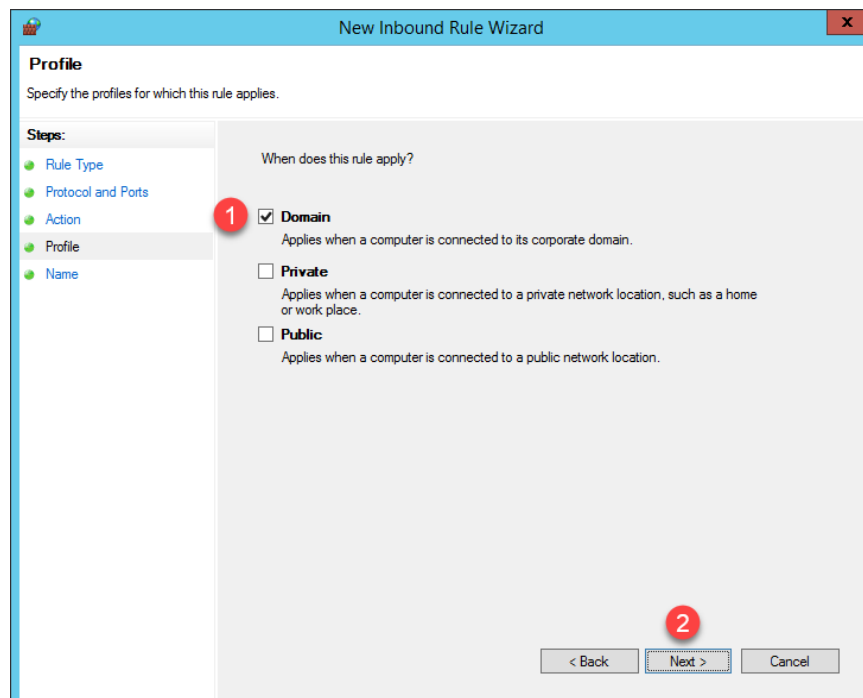
TCP Port 2031 is required by ThinManager for the Terminal Monitor Connection as well as for the delivery of the Terminal Profile to the terminal when it is booting up.

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



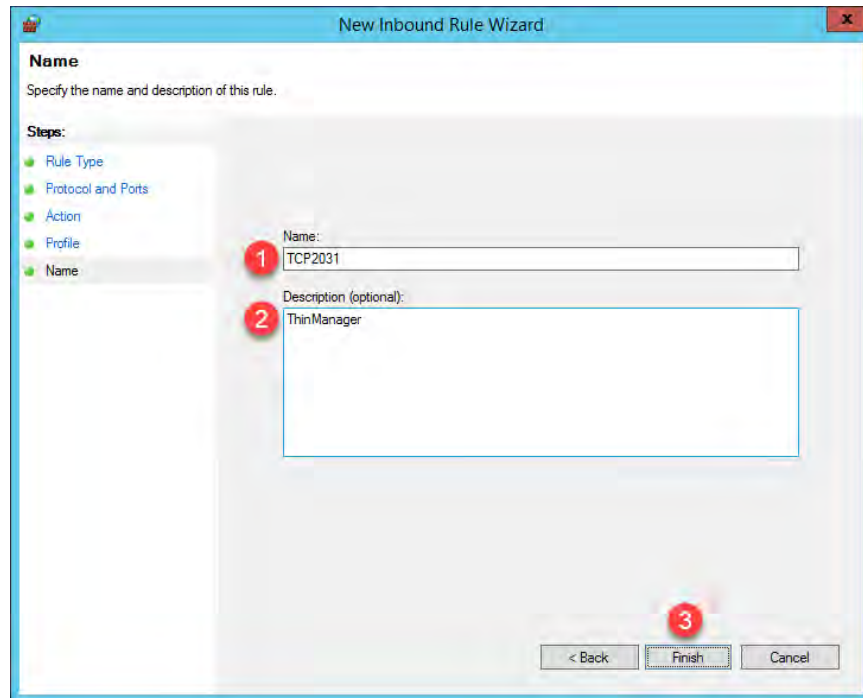
The screenshot shows the 'New Inbound Rule Wizard' window with the 'Action' panel selected. The 'Steps' list on the left includes Rule Type, Protocol and Ports, Action, Profile, and Name. The main area asks 'What action should be taken when a connection matches the specified conditions?'. Three radio buttons are present: 'Allow the connection' (selected and marked with a red '1'), 'Allow the connection if it is secure', and 'Block the connection'. The 'Next >' button is highlighted with a red '2'.

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



The screenshot shows the 'New Inbound Rule Wizard' window with the 'Profile' panel selected. The 'Steps' list on the left includes Rule Type, Protocol and Ports, Action, Profile, and Name. The main area asks 'When does this rule apply?'. Three checkboxes are present: 'Domain' (checked and marked with a red '1'), 'Private', and 'Public'. The 'Next >' button is highlighted with a red '2'.

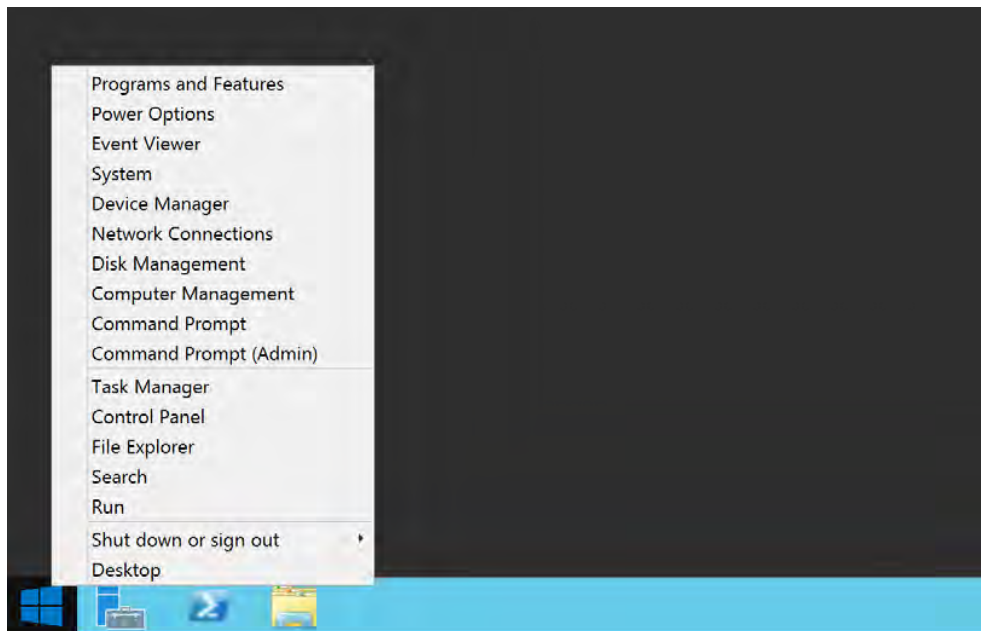
7. From the **Name** panel of the **New Inbound Rule Wizard**, enter *TCP2031* as the **Name** and ThinManager as the **Description**. Click the *Finish* button.



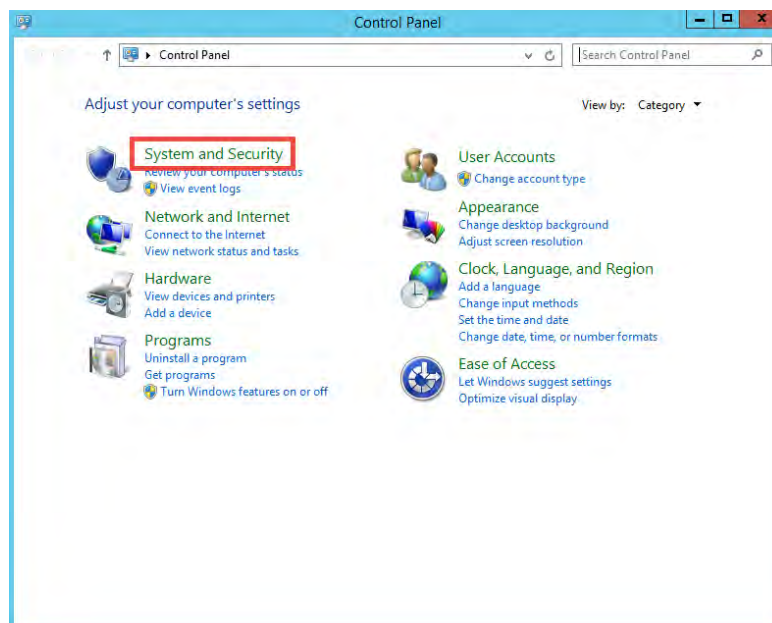
The image shows the 'New Inbound Rule Wizard' window, specifically the 'Name' panel. The window title is 'New Inbound Rule Wizard'. The panel is titled 'Name' and contains the instruction 'Specify the name and description of this rule.' On the left, a 'Steps' list shows five steps: 'Rule Type', 'Protocol and Ports', 'Action', 'Profile', and 'Name'. The 'Name' step is currently selected and highlighted. The main area contains two input fields: 'Name:' with the value 'TCP2031' and 'Description (optional):' with the value 'ThinManager'. Red circular callouts with numbers 1 and 2 point to these fields respectively. At the bottom right, there are three buttons: '< Back', 'Finish', and 'Cancel'. A red circular callout with the number 3 points to the 'Finish' button.

User Account Control (UAC)

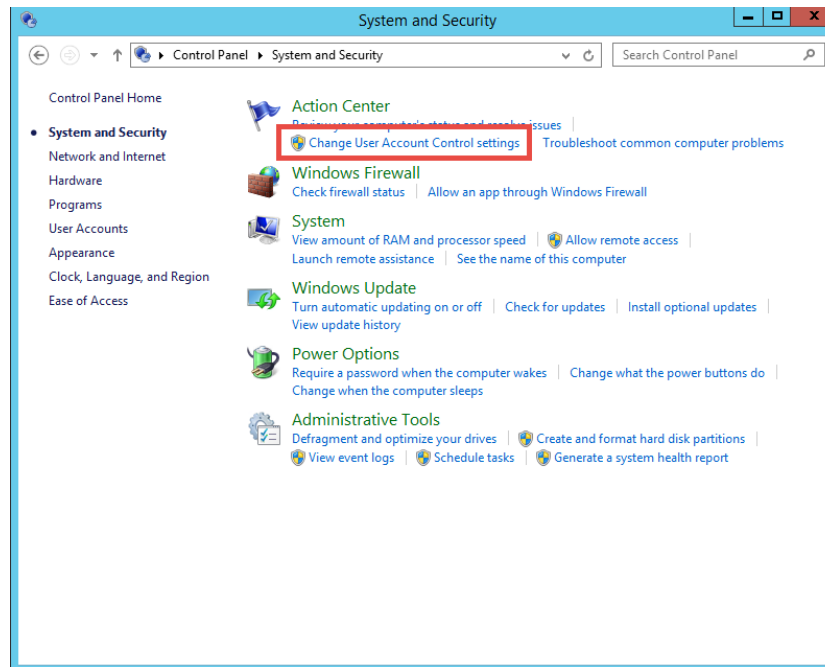
1. In addition, the User Account Control (UAC) will be set to Never notify.
 - Again, this is to simplify the deployment guide. If you are unable to change this setting in your environment, just ensure that each setup.exe process in the steps that follow is “Run as Administrator” by right clicking it and selecting Run as Administrator.
2. Right click the *Windows Start* button and select the *Control Panel* menu item.



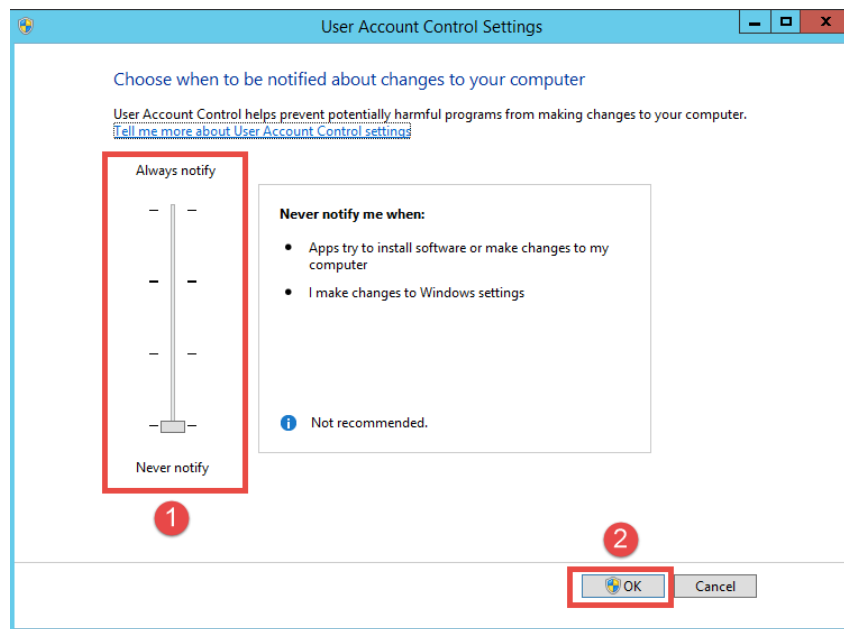
3. From the **Control Panel**, click the *System and Security* link.



4. From the **System and Security** window, click the *Change User Account Control settings* link.

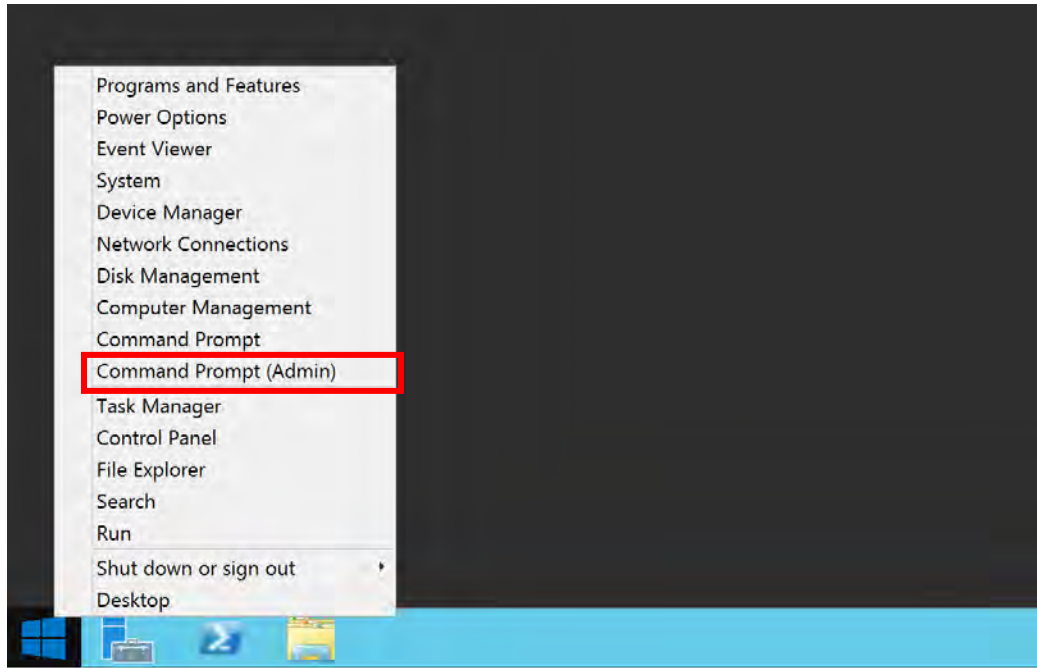


5. From the **User Account Control Settings** window, drag the vertical slider down to *Never notify*. Click the *OK* button.

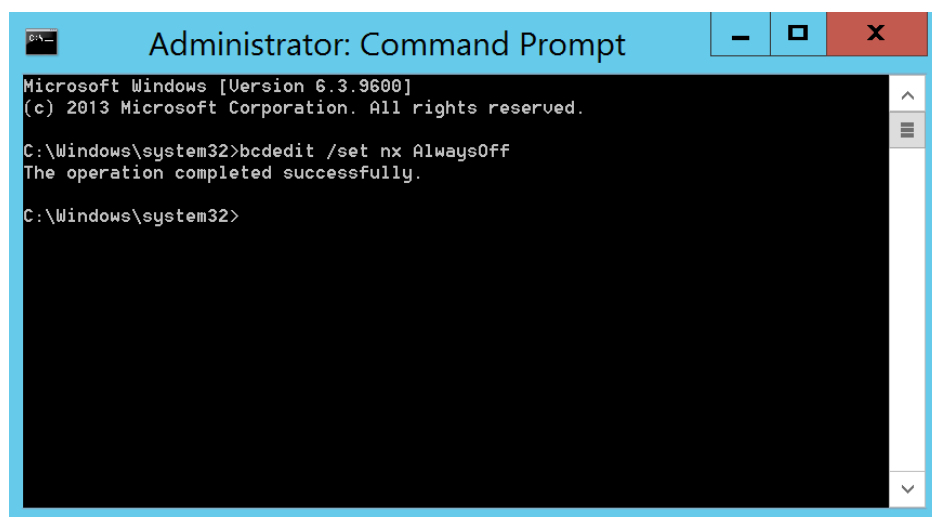


Data Execution Prevention (DEP)

1. Now we will disable Data Execution Prevention (DEP). Right click the *Windows Start* button and select *Command Prompt (Admin)*.



2. From the ensuing command prompt, enter (Followed by the ENTER key):
`bcdedit /set nx AlwaysOff`
3. This command will turn off the Data Execution Prevention (DEP) of Windows.
 - o Additional information on DEP can be found at <http://support.microsoft.com/kb/875352>.
4. Restart the server.



Remote Desktop Services Role Installation and Configuration

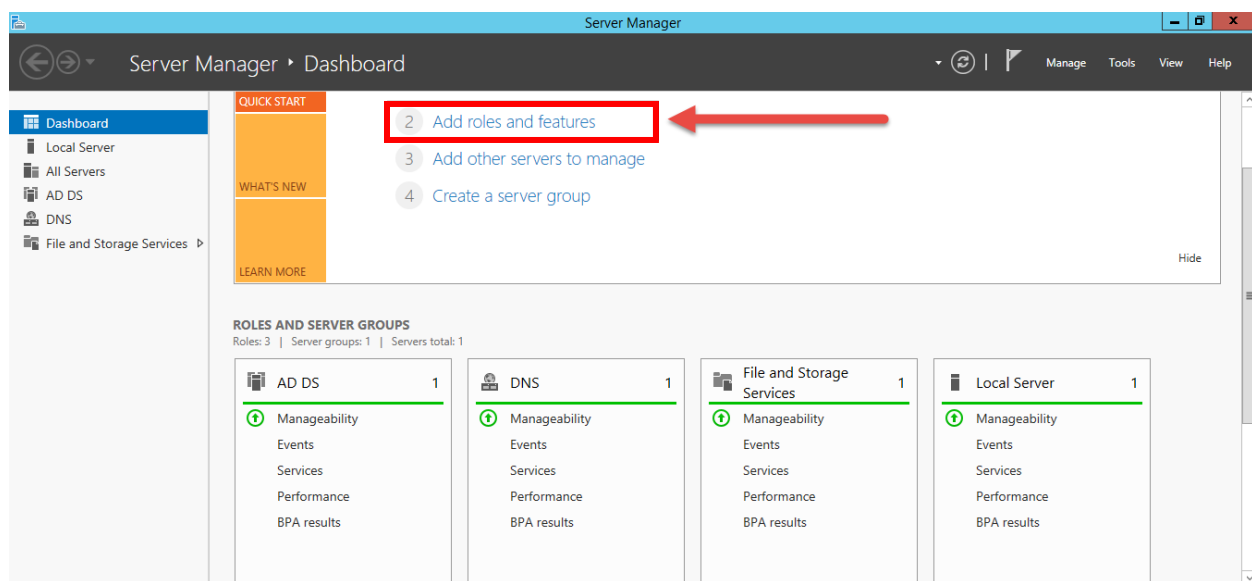
Starting with Windows Server 2012, it is highly advised that the server be part of a domain as the Remote Desktop Services graphical configuration is only available to Domain Admins. This document will assume that your new Remote Desktop Services Server is already part of a domain and you have credentials for a Domain Admin user account. By default, the Domain\Domain Users Group will be added to the deployment as the users with access to the remote applications that will be published later in this document. Any domain group of users can be granted access to the deployment.

It is possible for you to setup Active Directory for a stand-alone server, and make that server also a Domain Controller. That setup is outside the scope of this document.

Important: Installing the Remote Desktop Services role on Windows Server 2012 or Windows Server 2012 R2 in a workgroup is not recommended. The Remote Desktop Services configuration tool is not accessible without being logged in as a domain user resulting in all configuration needing to be performed through the local group policy editor or PowerShell.

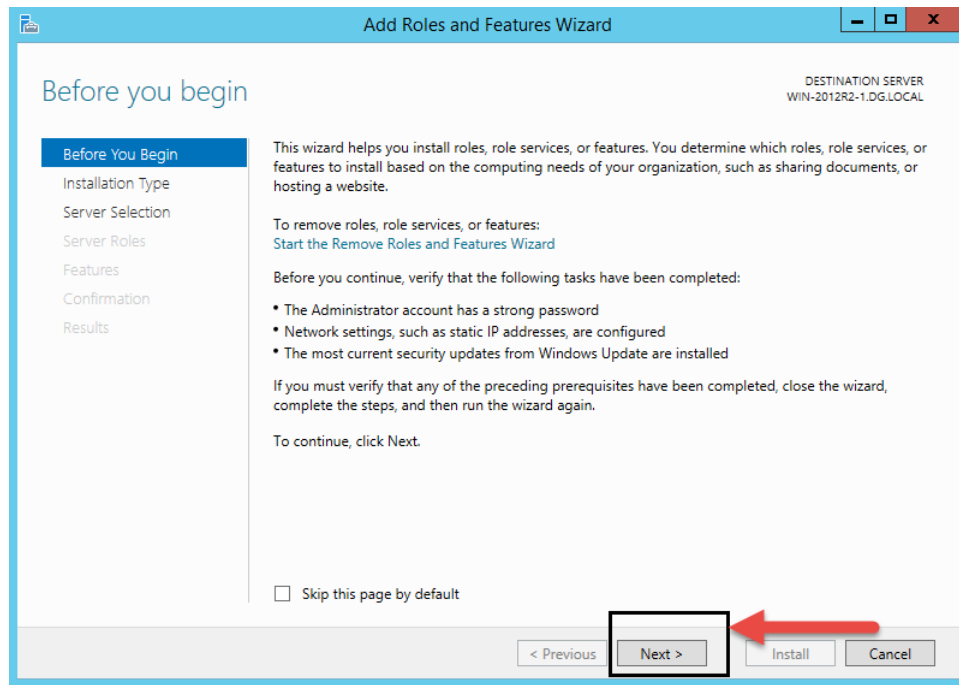
Domain Environment Setup

1. Log into the Server with a Domain Admin account (or a local admin that is also a domain user).
2. Run **Server Manager**.

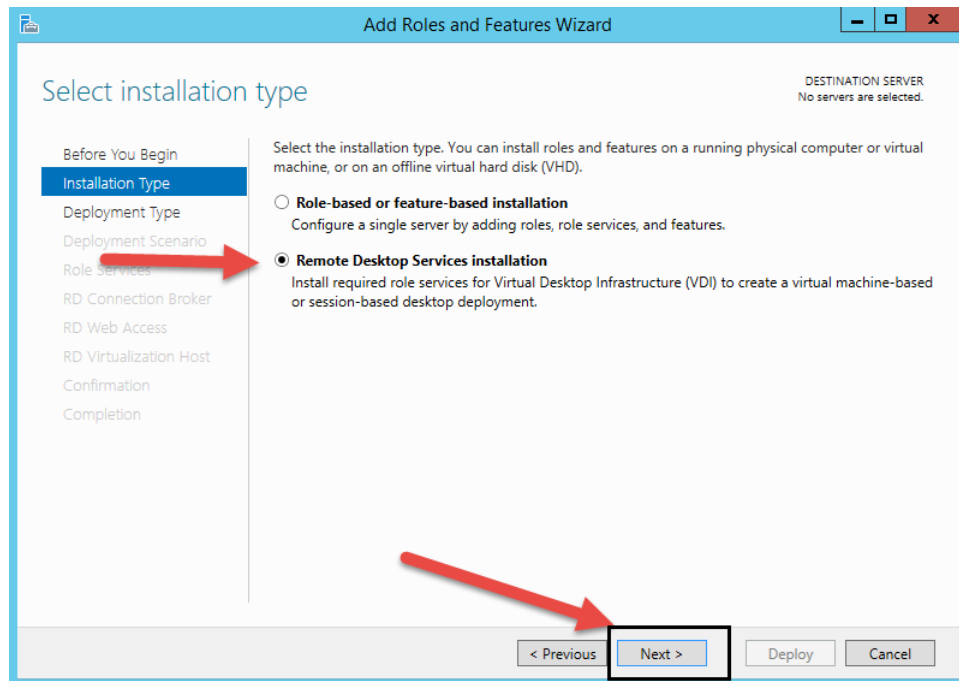


3. Click on *Add Roles and Features*.

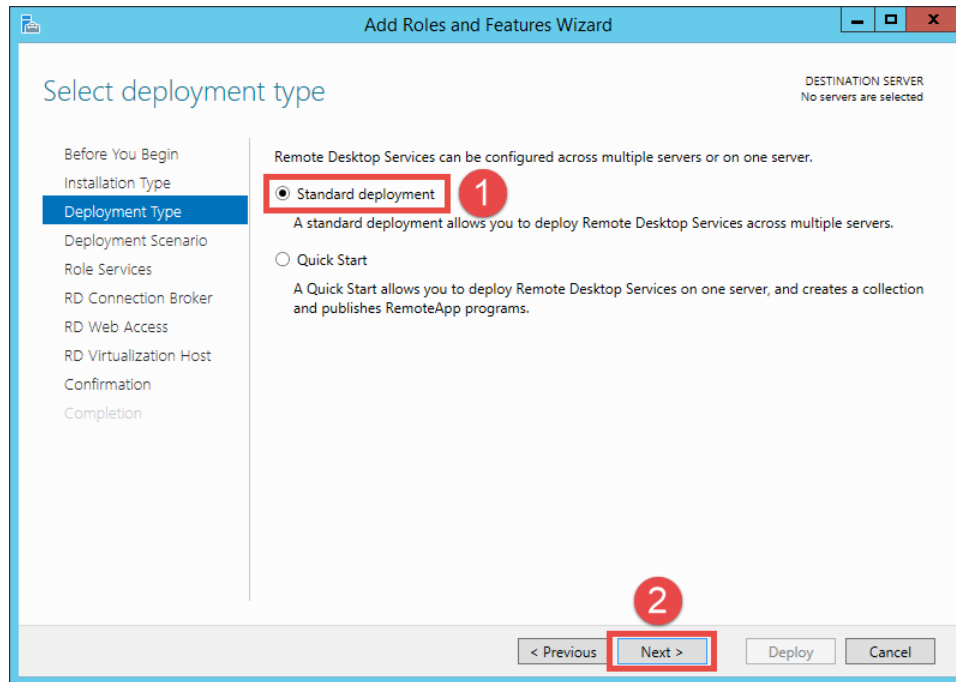
- Click *Next*.



- Select *Remote Desktop Services* installation, and then press *Next*.



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

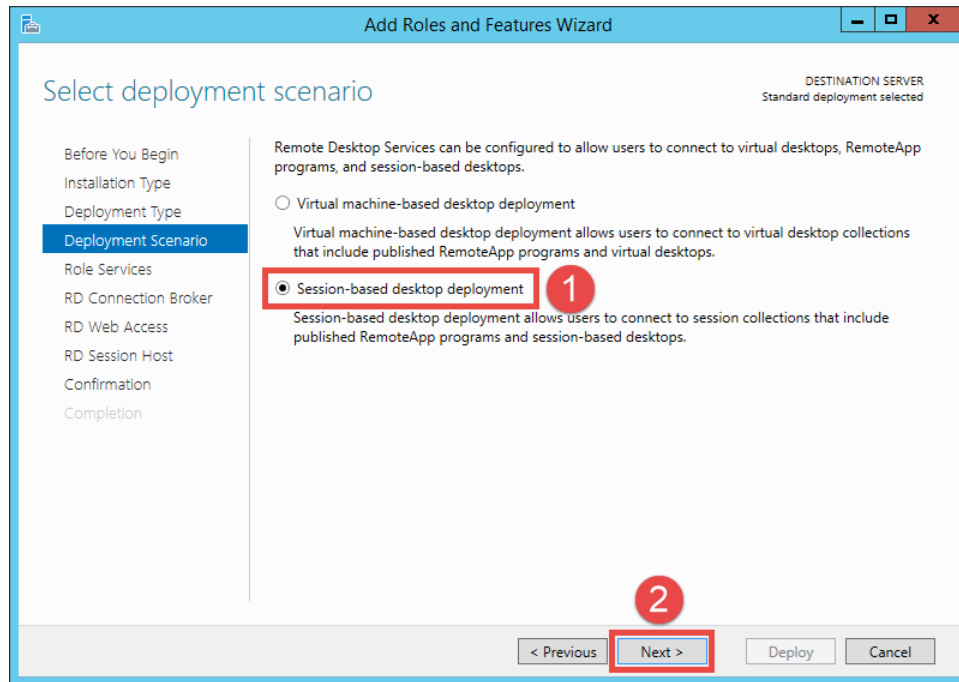


The Quick Start option is only suitable when deploying a single Remote Desktop Server. Since this lab is only using a single Remote Desktop Server, this option could have been used as well.

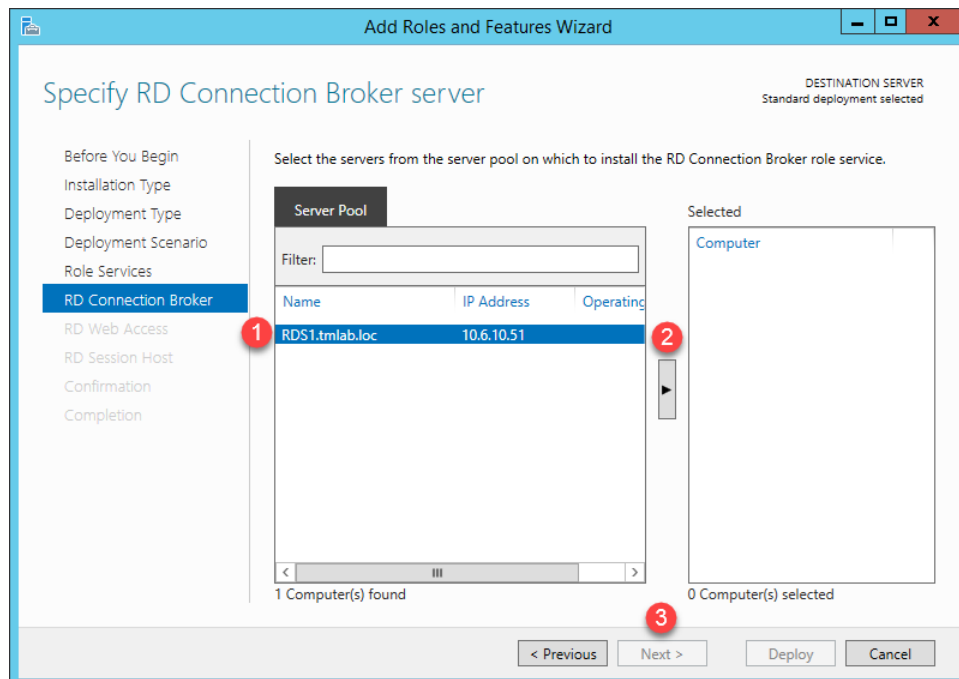
For deployments with more than one Remote Desktop Server, it is best to create a Server Group within Server Manager and add the Remote Desktop Servers to that group. Server groups allow you to view and manage a smaller subset of your server pool as a logical unit. To create a Server Group, click the Manage menu button within Server Manager, followed by the Create Server Group item. You can then add the desired servers to the new group.

It is also a recommendation to create a separate Organizational Unit (OU) within the Active Directory domain for the Remote Desktop Servers. You will then be able to manage the Group Policies for all of your Remote Desktop Servers through a single OU.

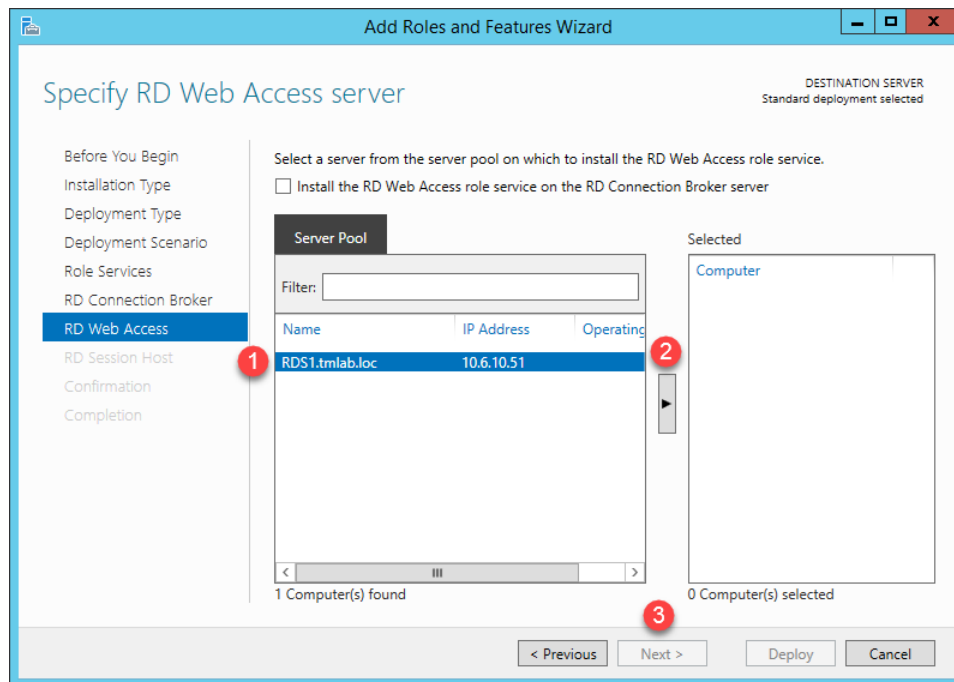
- On the **Deployment Scenario** page of the **Add Roles and Features Wizard**, select *Session-based desktop deployment* and click *Next>*.



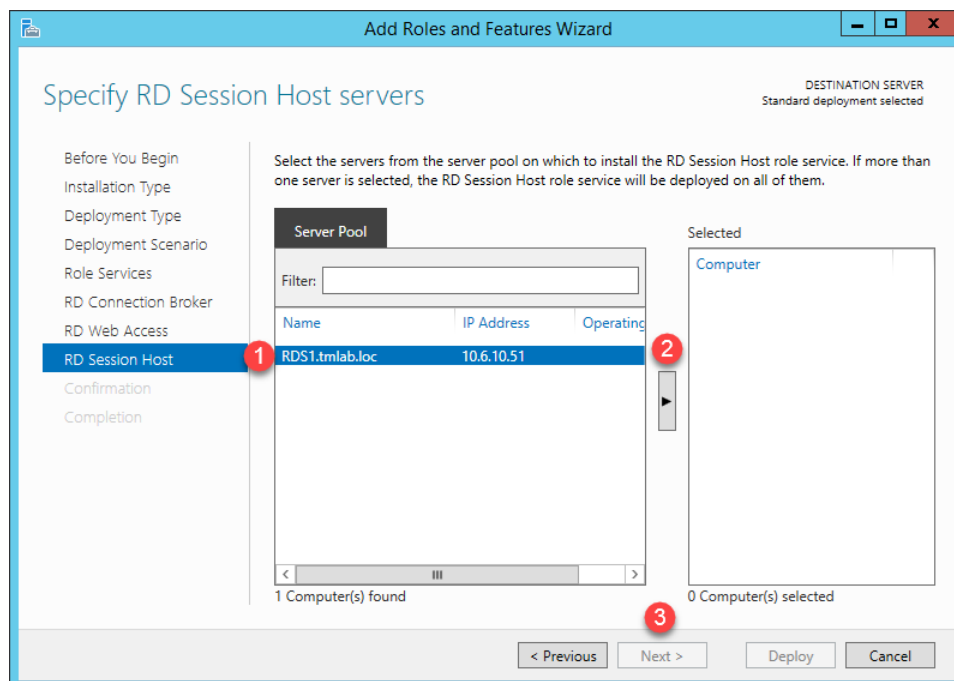
- Click the *Next>* button on the **Role Services** page of the **Add Roles and Features Wizard**.
- From the **RD Connection Broker** page of the **Add Roles and Features Wizard**, click the *Right Arrow* button to add the **RDS1.tmlab.loc** server to the **Selected** list, followed by *Next>*.



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

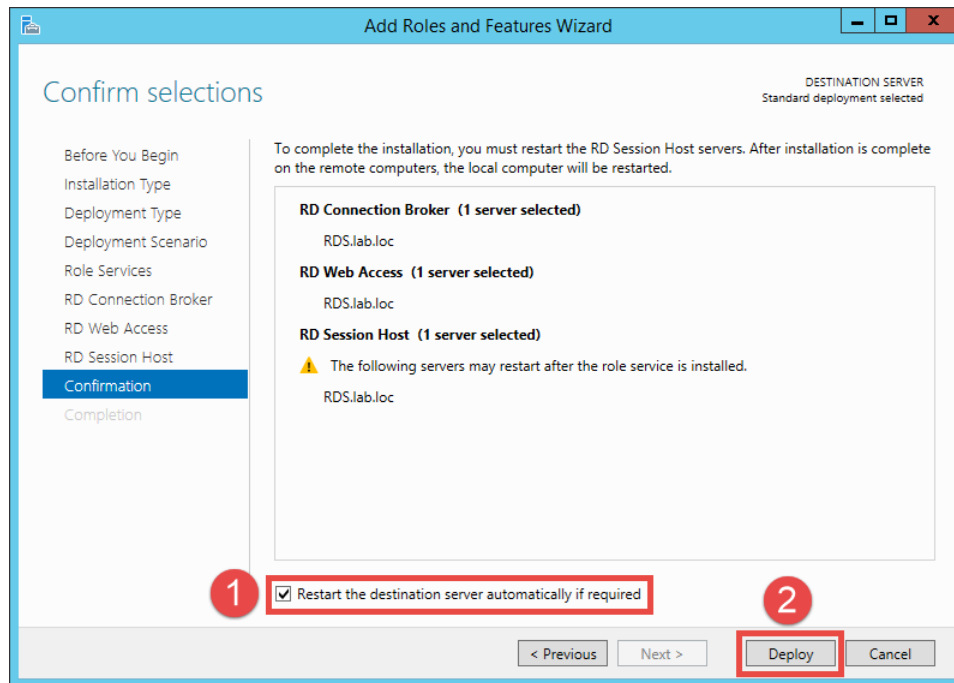



11. On the **RD Session Host** page of the **Add Roles and Features Wizard**, click the *Right Arrow* button to add the **RDS1.lab.loc** server to the **Selected** list, then click *Next>*.

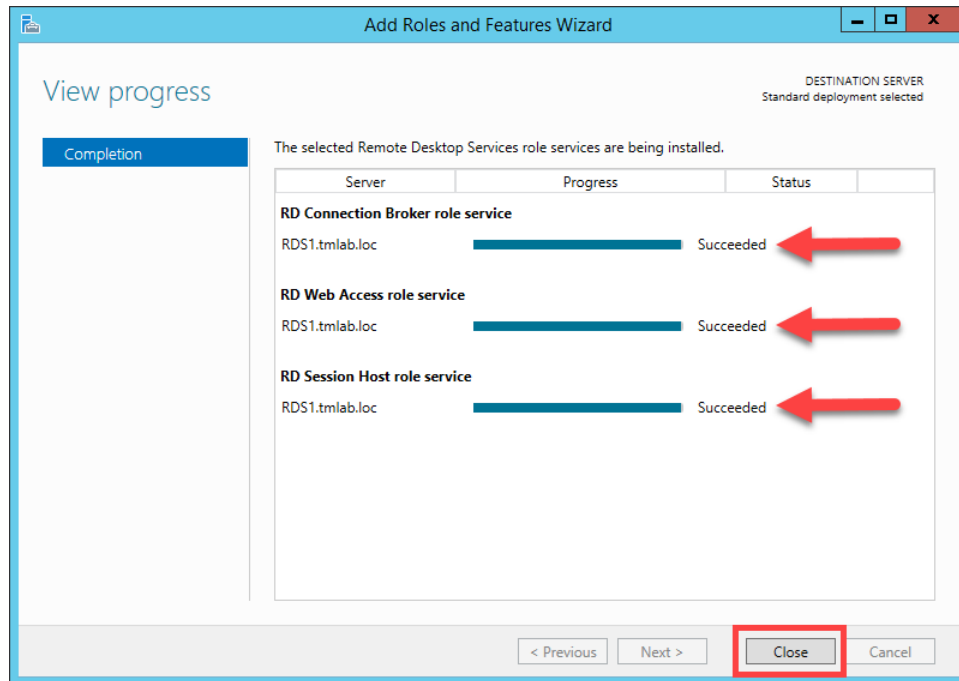


12. On the **Confirmation** page of the **Add Roles and Features Wizard**, check the **Restart the destination server automatically if required** checkbox followed by clicking the *Deploy* button. The installation process will start and continue for a few minutes. Once finished, **RDS1** will automatically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

Note: This process will take a few minutes to complete.



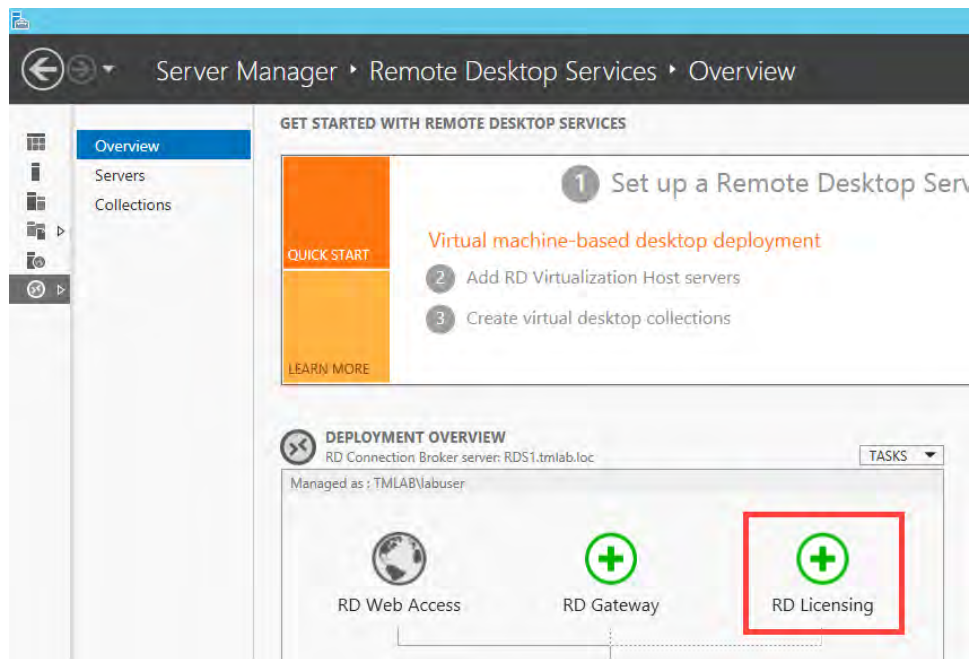
13. Once **RDS1** has restarted, click the *Server Manager*  icon next to the **Windows Start** button. The **Add Roles and Features Wizard** will reappear and provide status on the installation progress. Once the Status indicates **Succeeded** for each of the 3 role services, click the *Close* button.



Remote Desktop Services Licensing Role Installation

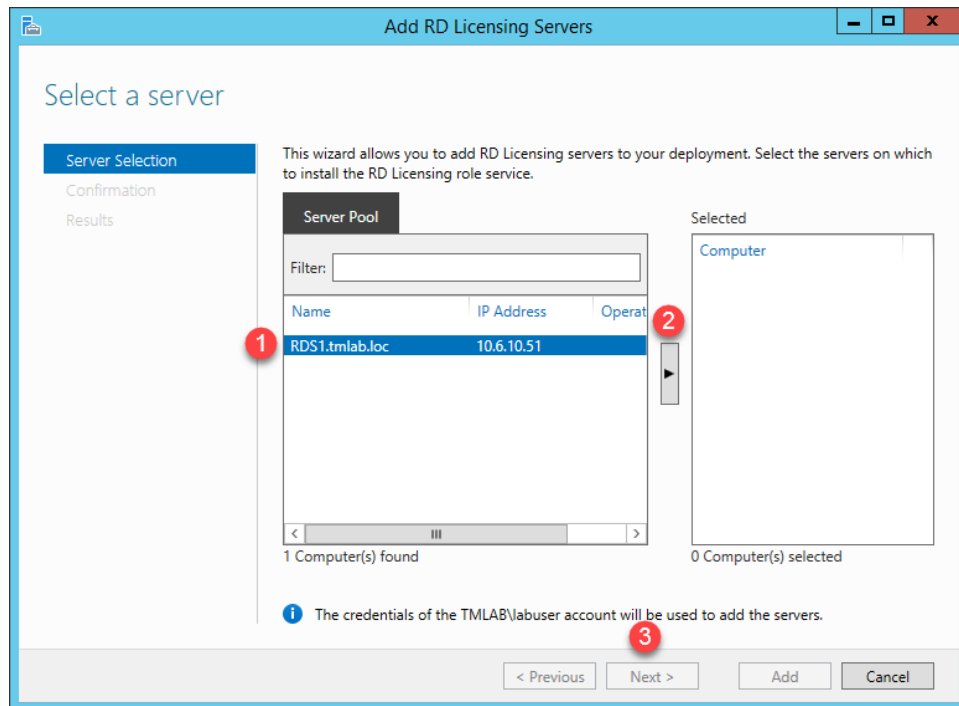
Next we will add the Remote Desktop Licensing service to **RDS1**. The Remote Desktop Licensing service is required for all Remote Desktop Services deployments, but this role can be installed on a separate server as well (i.e.: on a separate FactoryTalk Directory and/or FactoryTalk Activation Server).

1. In the Server Manager Dashboard, press *Remote Desktop Services* in the link on the left side of the window.
2. From the *Remote Desktop Services* panel of Server Manager on **RDS1**, select the *Overview* item and click the add *RD Licensing* button.

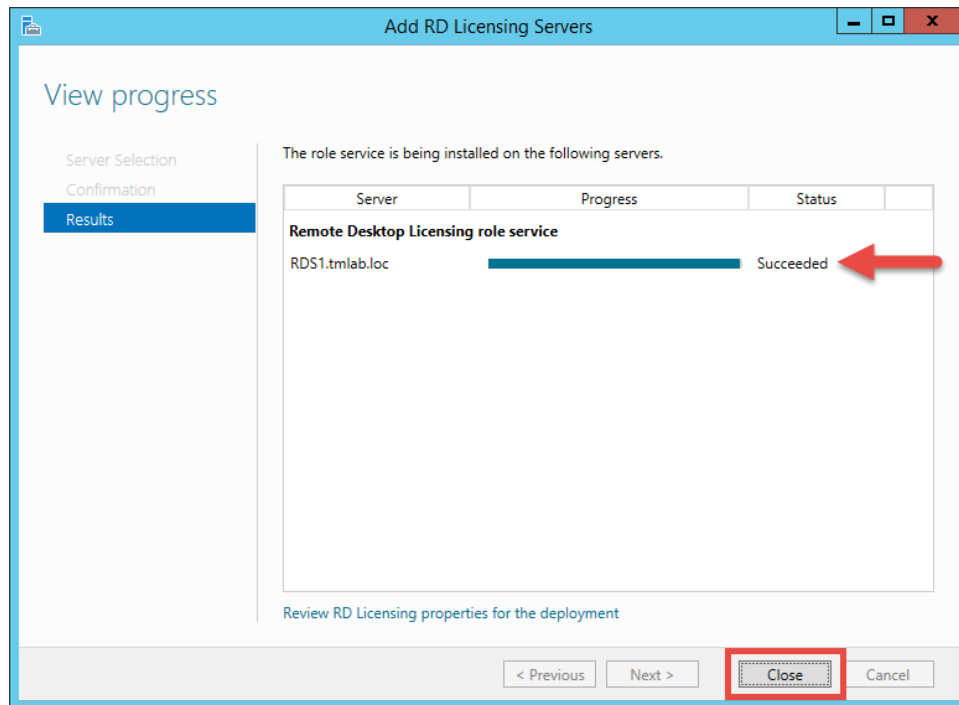


3. From the **Select a server** page of the **Add RD Licensing Servers** wizard, select the **RDS1** server from the **Server Pool** list, then click the Right arrow button to add each to the **Selected** list.
4. Click the **Next** button.

The screen shots below show adding the RD Licensing Role Service to RDS, however RDS2 can be included as well, but in general you only need 1 RD Licensing Server. If that RD Licensing Server becomes unavailable, licenses will continue to be issued for up to a 120 day grace period.

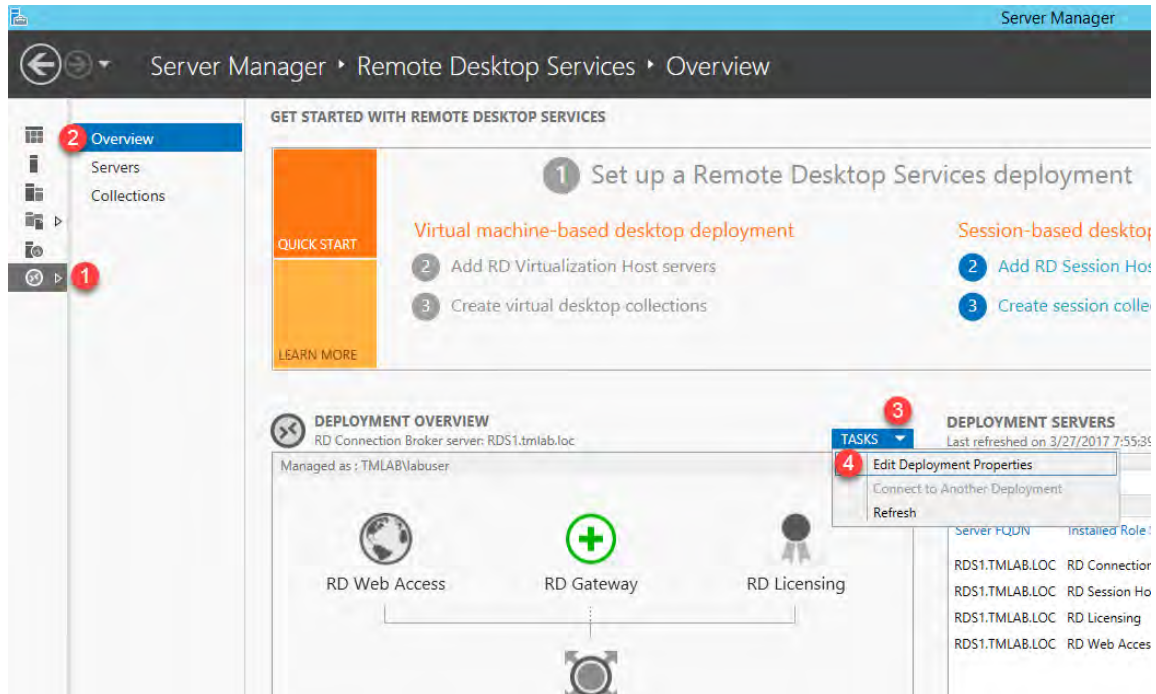


5. You may receive a “*Checking compatibility*” popup indicating that the servers have pending reboots, and therefore the deployment cannot proceed. If this is the case, click the *Cancel* button twice, and reboot each of the servers, then perform the previous 3 steps again.
6. Click the *Add* button from the **Confirmation selections** page of the wizard.
7. Once the Licensing role service completes, the status will indicate **Succeeded**. Click the *Close* button.



Remote Desktop Services Licensing Role Configuration

1. Now, the Licensing mode needs to be set. To do so, from the **Overview** page of the **Remote Desktop Services** role on **RDS1**, click the **TASKS** drop down button, followed by the **Edit Deployment Properties** menu item.



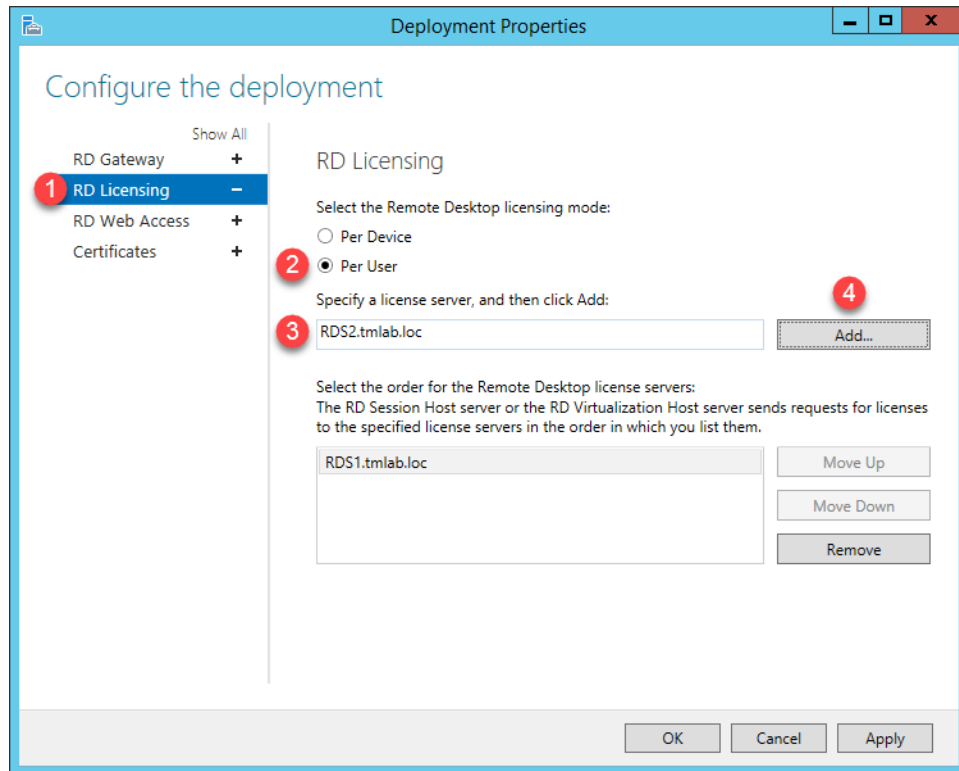
2. From the **Configure the deployment** page of the **Deployment Properties** wizard, select the **RD Licensing** item, and then select the desired **RD Licensing Mode**. This guide will use **Per User**. The end user will purchase either Per User or Per Device RDSCALs, and this setting needs to agree with the type purchased.

Use Per User licensing when individual users will be connecting from various devices and the number of users is generally smaller than the number of devices available to them for accessing the server.

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

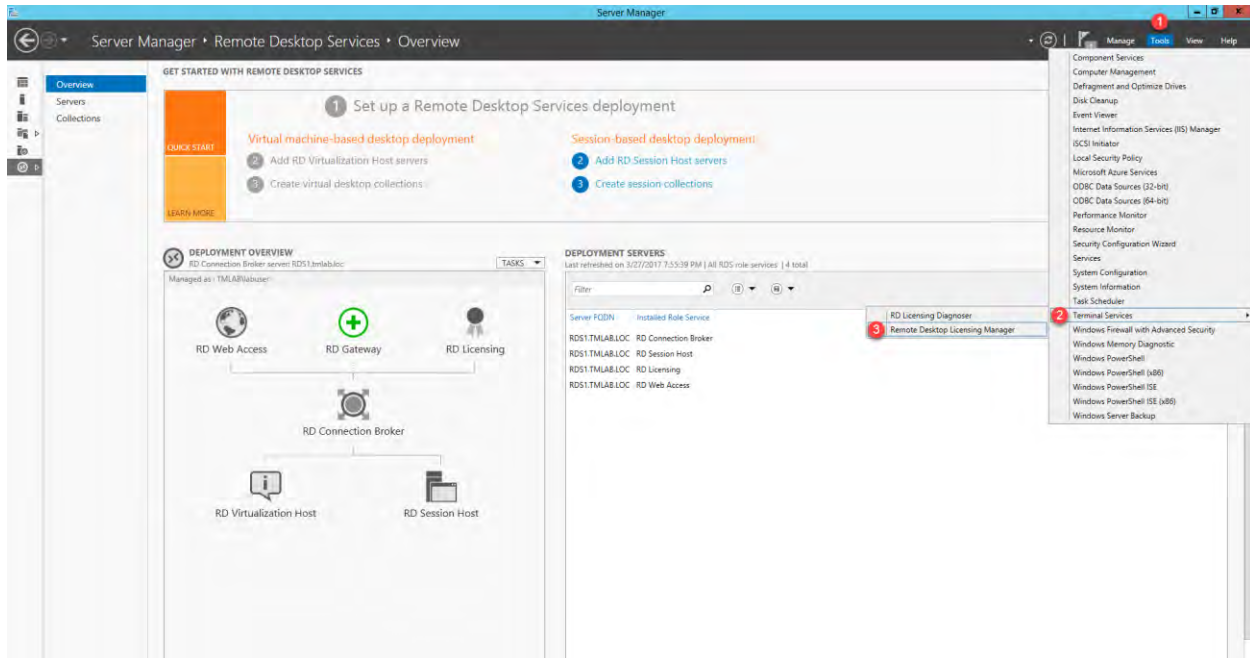
By default, 2 console administrative connections are allowed to the server. These connections do not require licenses from the license pool to be available. To start an administrative session, you must use the latest version of the Microsoft Remote Desktop Connection client and specify `<servername>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

3. Notice that **RDS1** has already been added as a Remote Desktop License server. Click the *OK* button.
4. From the **Deployment Properties** screen, select the **RD Licensing** panel, then click the **Per User** radio button. In addition if using a second Remote Desktop Server, enter `RDS2.tmlab.loc` in the license server field and click the *Add...* button.

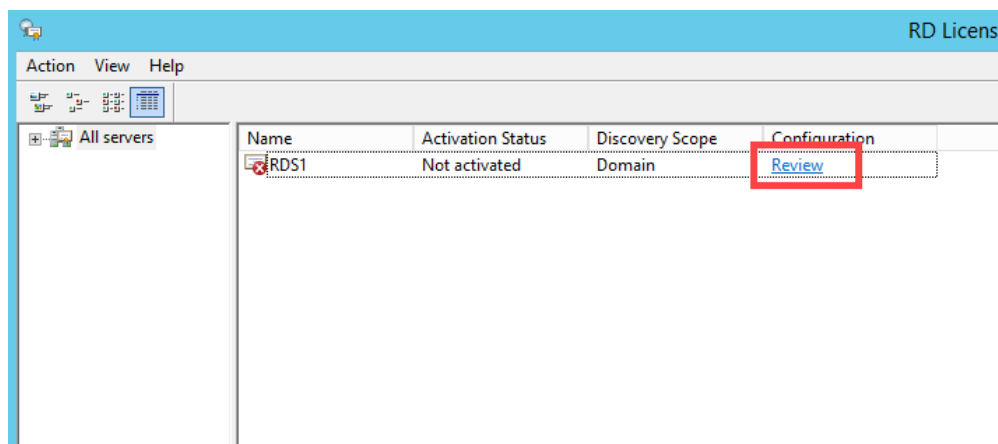


5. Click *OK* to apply the changes.

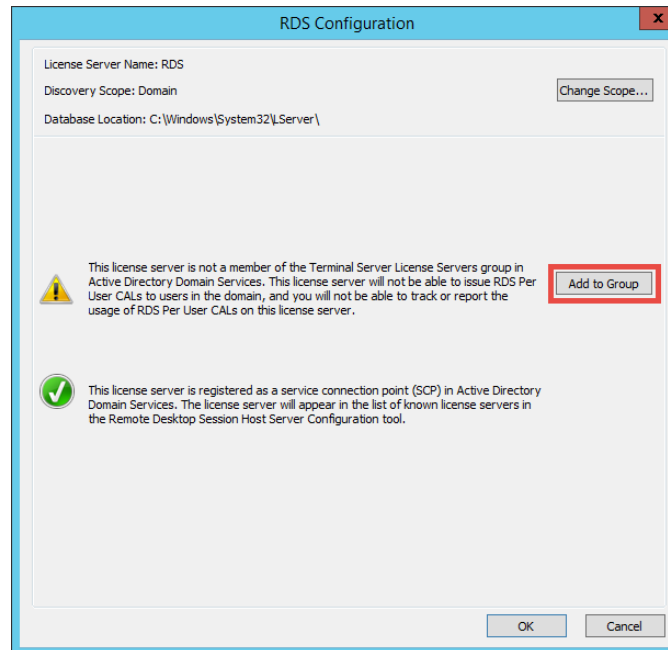
6. The Licensing Servers must now be activated. Starting with **RDS1**, from the **Server Manager**, click the **Tools** menu, followed by the **Terminal Services** folder item, then the **Remote Desktop Licensing Manager** menu item.



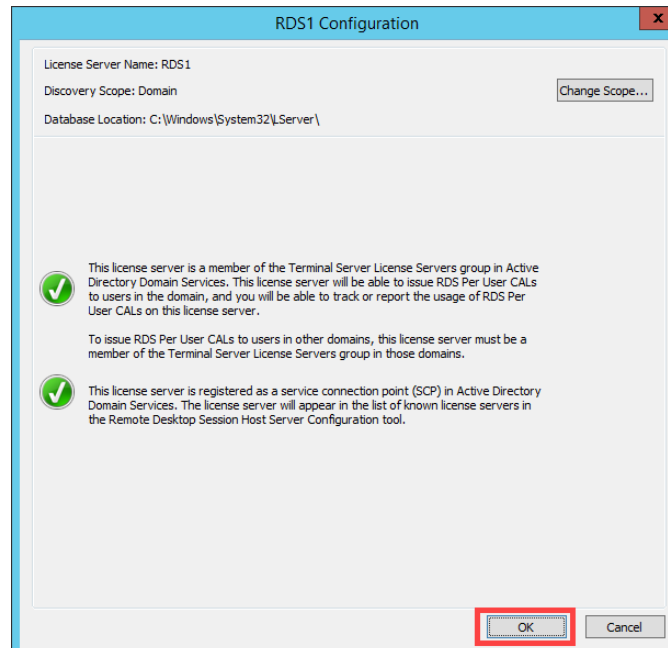
7. From the **RD Licensing Manager** window, notice the **Activation Status** of **RDS1** is **Not activated**. To activate it, right click **RDS1** and select **Activate Server**.
8. Using the **Activate Server Wizard**, fill in the required details. If your server does not have Internet access, you can select the **Web Browser** connection method to activate the Licensing Server from another machine that does have Internet access. In terms of **Company Information**, the wizard only requires **First Name**, **Last Name**, **Company** and **Country**.
9. At the end of the **Activate Server Wizard**, it is up to you if you would like to install your **RDSCALs** at this point. To do so, leave the **Start Install Licenses Wizard** now checkbox checked.
10. Once the Wizard is complete, the **Activation Status** should change to **Activated**.
11. Click the **Review** link.



12. Click the *Add to Group* button to add this Licensing Server to the Terminal Server License Servers group in Active Directory Domain Services.



13. Click the *Continue* button from the ensuing **RD Licensing Manager** popup.
14. A confirmation dialog will be presented. Click the *OK* button on it.



15. Click the *OK* button on the **RDS1 Configuration** window.
16. **RDS1** should now have a green check box beside it. Close the *RD Licensing Manager*.

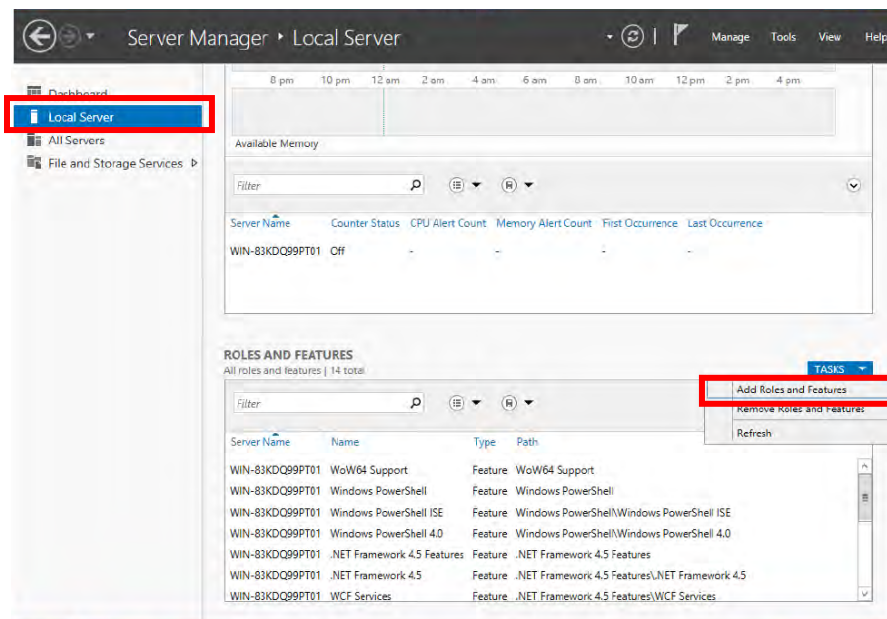
Workgroup Deployments

Remote Desktop Services can be configured in a Workgroup environment if a domain is not available. Please note that the RDS UI tools provided by Microsoft are unavailable if not using a domain and many of these settings must be configured using either the local group policy editor or PowerShell.

Install Remote Desktop Services RD Host and Licensing Server

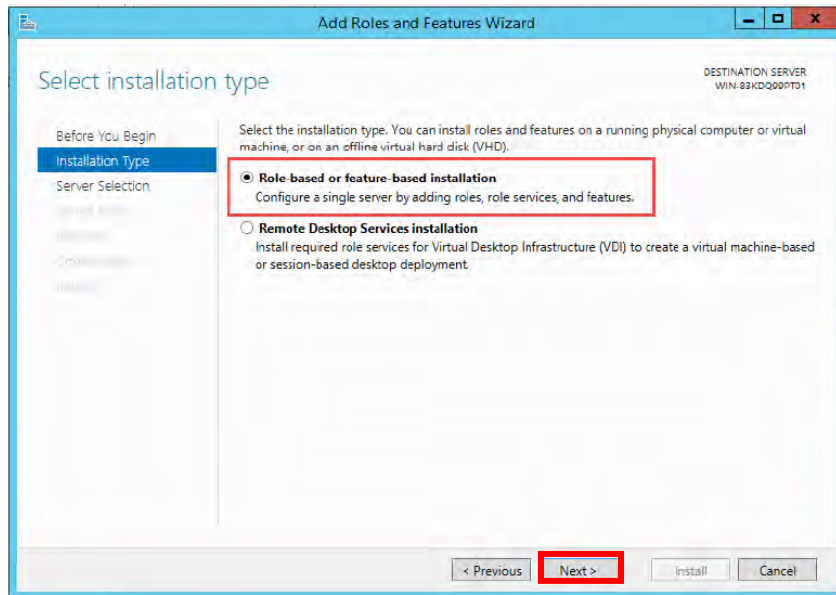
To install the RDS components in a Workgroup environment in Server 2012 the following steps can be used as a guideline.

1. Launch the **Server Manager** application from the start menu.
2. Select the **Local Server** tab on the left hand side from the navigation explorer.
3. From the **TASKS** drop down list, select *Add Roles and Features*.

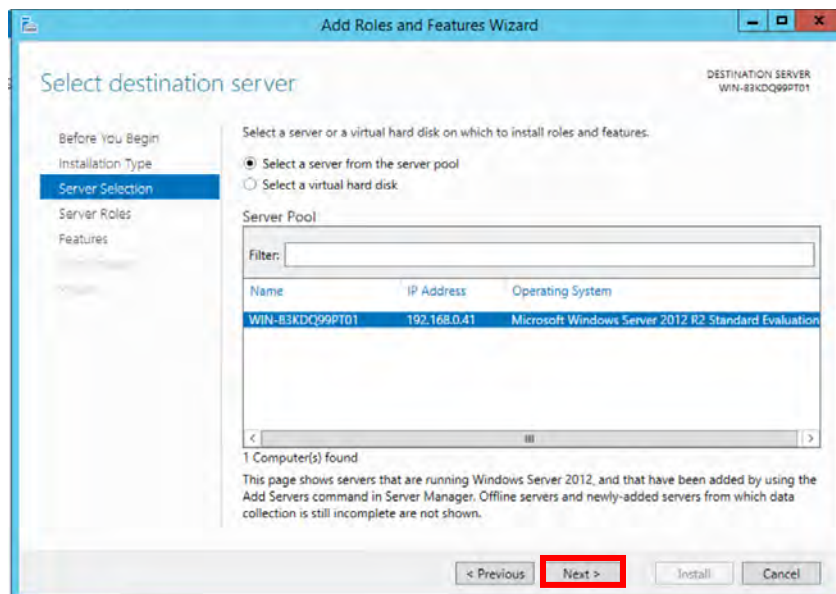


4. In the **Add Roles and Features** wizard, acknowledge the message on the first page by clicking *Next*.

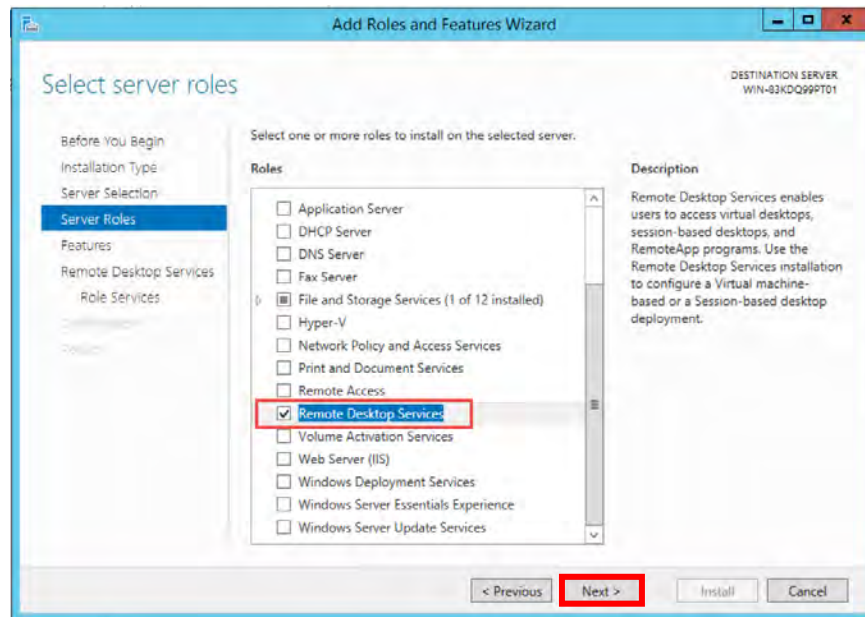
- For the Installation Type, select *Role based or feature based installation* radio button and click *Next*.



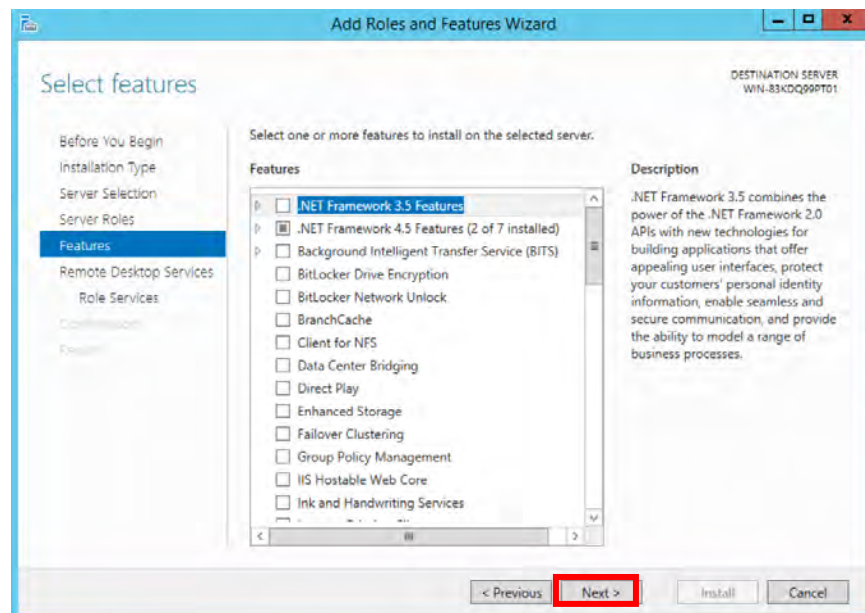
- On the Server Selection page, select the local server. Click *Next*.



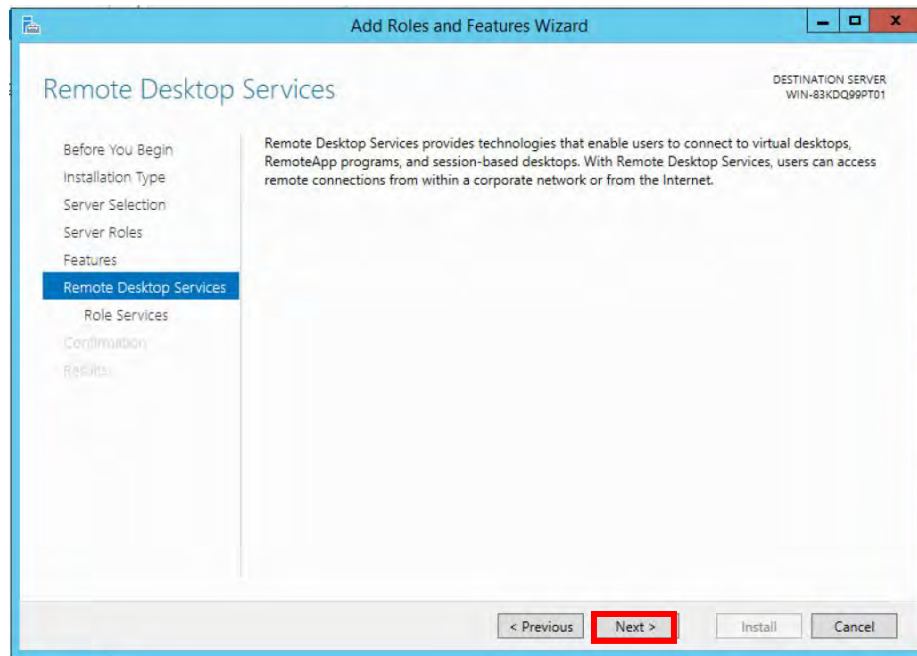
- From the **Server Roles** selection page, check the box next to *Remote Desktop Services*.



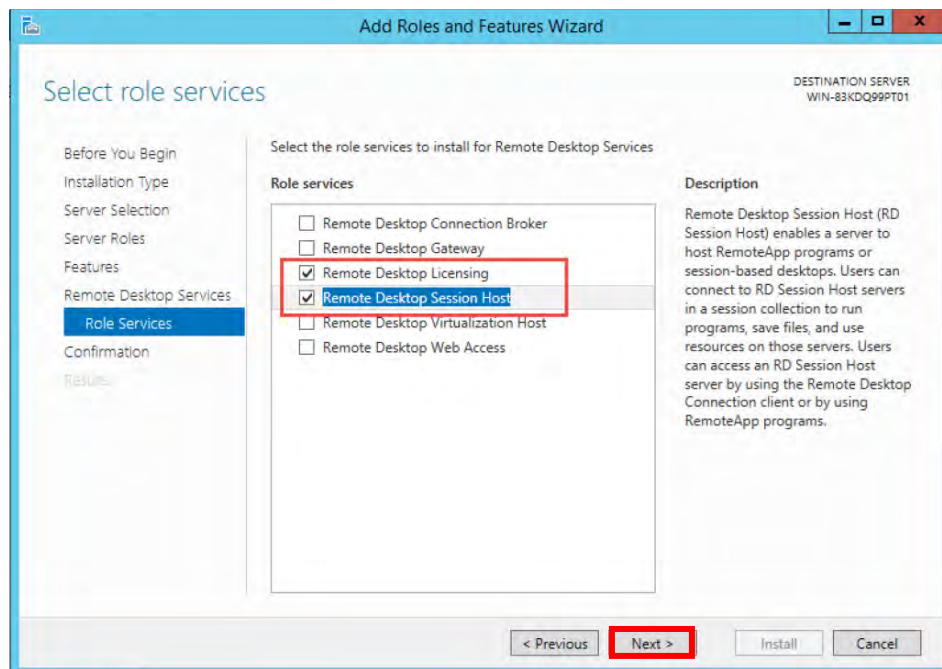
- Accept the default settings on the **Features** page by clicking *Next*.



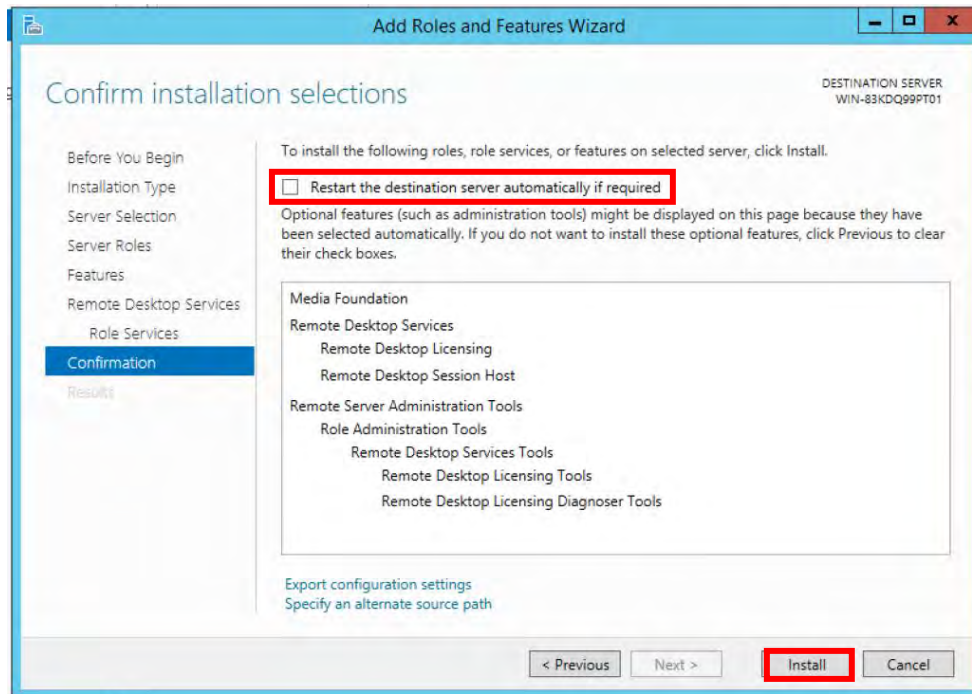
9. Select **Next** on the **Remote Desktop Services** page.



10. From the **Role Services** page:
 - a. Select the Remote Desktop Licensing role service
 - i. From the ensuing popup window, accept the defaults and click the *Add Features* button.
 - b. Select the Remote Desktop Session Host role service
 - i. From the ensuing popup window, accept the defaults and click the *Add Features* button.



11. On the **Confirmation** page check the checkbox for *Restart the destination server automatically if required*. To complete the installation, click *Install*.

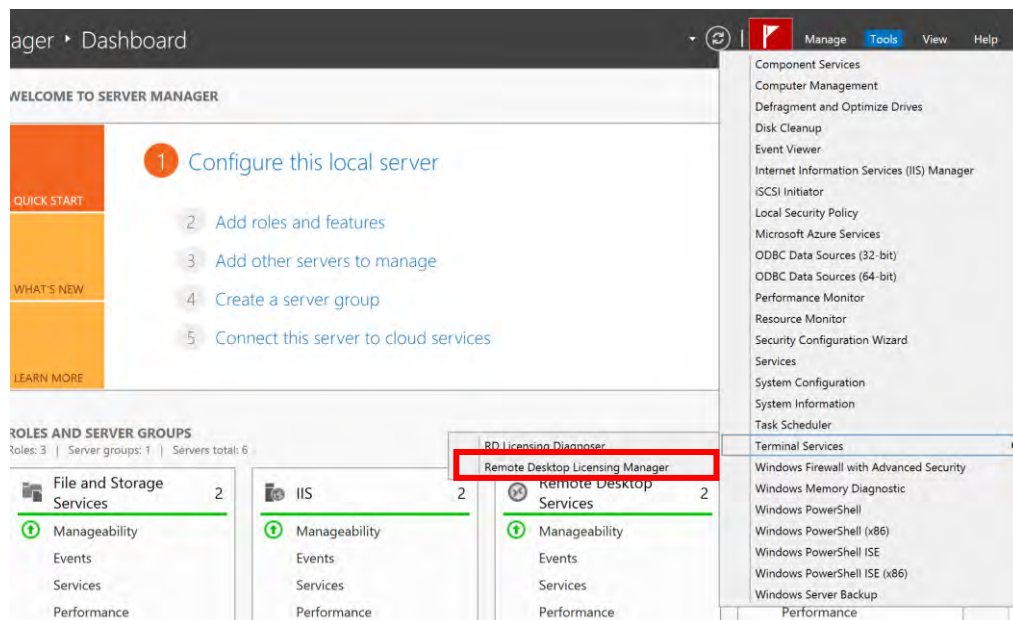


12. After the server installation is complete and the server has been restarted (this should happen automatically if allowed in the previous step) we will activate the Remote Desktop Licensing Server.

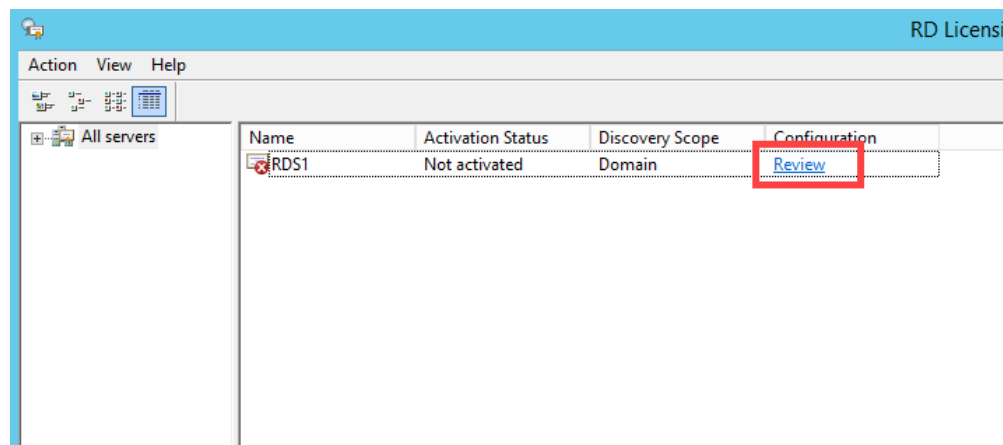
Configure Remote Desktop Licensing

The Remote Desktop Licensing component of the RDS architecture will be assumed to be located on the same box for the following deployment. If this is not the case, when it comes time in the procedure to specify the server name, use the remote server name hosting the RD Licensing component in place of the local host.

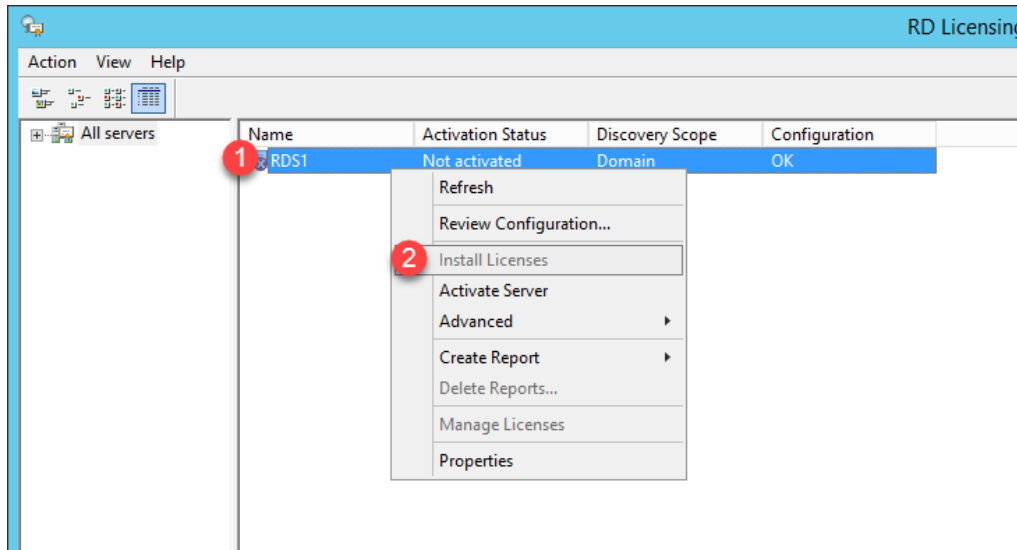
1. To configure the License Server, we must first activate it. To activate the server, launch the **RD Licensing Manager** tool. To do this, launch the **Server Manager** application and drop down the **Tools** tab. Locate the *Terminal Services* option and select *Remote Desktop Licensing Manager*.



2. From the **RD Licensing Manager** window, select the **Review** button next to the localhost computer name.



3. Click the *Add to Group* button to add the new licensing server to the Remote Desktop Server License Servers group in Active Directory, followed by the *Continue* button. You can then click the *OK* button.
4. Remote Desktop Client Access Licenses (RDS CAL's) can now be installed on the system. To install RDS CAL's, right-click the localhost name and then select *Install Licenses*.

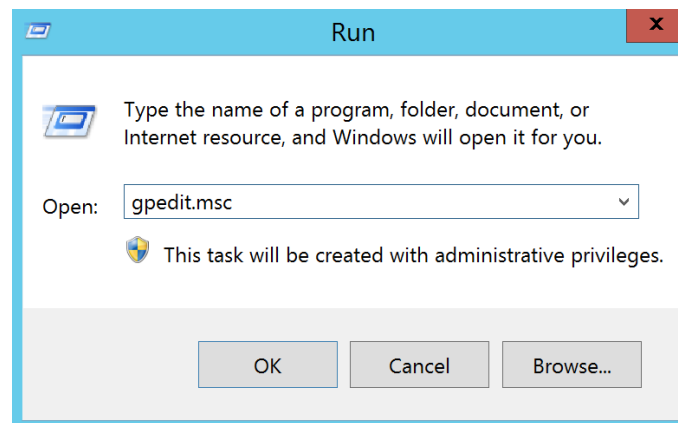


5. After licenses have been installed, can now close the RD Licensing Manager window.

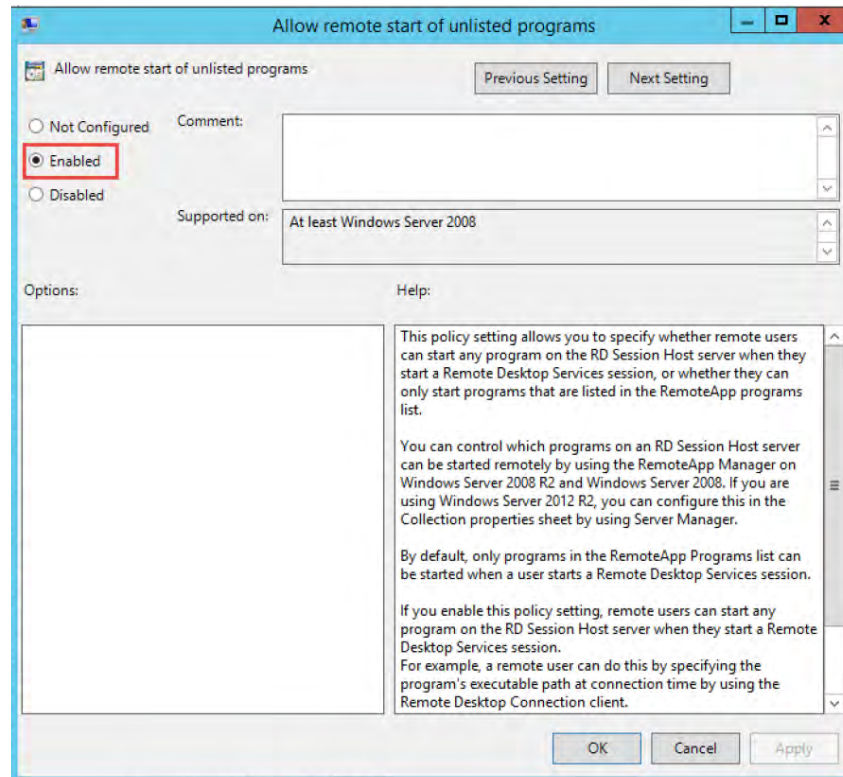
Configure Local Group Policy

As stated above, with the inability to make changes to the RDS deployment using the Server Manager UI, we will need to configure settings using either PowerShell or the local group policy editor. For this document, we will use the local group policy editor.

1. From the start menu, search 'Run' to launch the run dialog tool.
2. Enter the application name **gpedit.msc** and click *OK*.

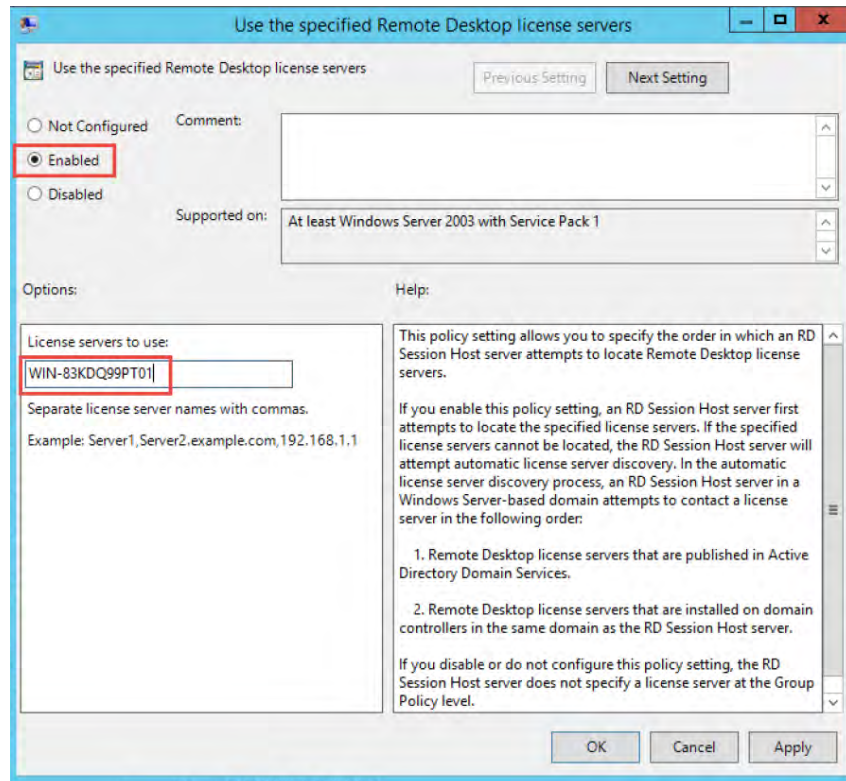


3. From the **Local Group Policy** editor, navigate to Local Computer Policy > Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Connections.
4. Double-click the policy *Allow remote start of unlisted programs*.
5. Select the radio button for *Enabled* for this policy. Click *OK* to accept.



6. From the **Local Group Policy** editor, navigate to Local Computer Policy > Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Licensing.
7. Locate and double-click the policy for *Use the specified Remote Desktop license servers*.

8. Enable this policy by checking the radio button next to *Enabled* and enter the localhost or remote computer name in the field as shown below.



Use the specified Remote Desktop license servers

Previous Setting Next Setting

☐ Not Configured
 ☒ **Enabled**
☐ Disabled

Comment:

Supported on: At least Windows Server 2003 with Service Pack 1

Options:

License servers to use:

WIN-83KDQ99PT01

Separate license server names with commas.
Example: Server1,Server2.example.com,192.168.1.1

Help:

This policy setting allows you to specify the order in which an RD Session Host server attempts to locate Remote Desktop license servers.

If you enable this policy setting, an RD Session Host server first attempts to locate the specified license servers. If the specified license servers cannot be located, the RD Session Host server will attempt automatic license server discovery. In the automatic license server discovery process, an RD Session Host server in a Windows Server-based domain attempts to contact a license server in the following order:

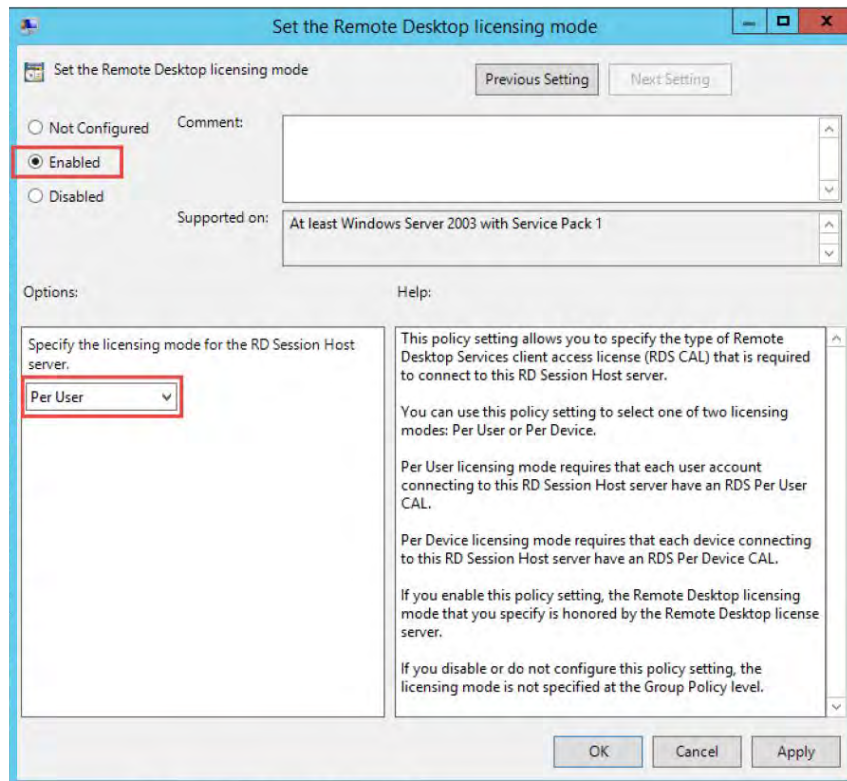
1. Remote Desktop license servers that are published in Active Directory Domain Services.
2. Remote Desktop license servers that are installed on domain controllers in the same domain as the RD Session Host server.

If you disable or do not configure this policy setting, the RD Session Host server does not specify a license server at the Group Policy level.

OK Cancel Apply

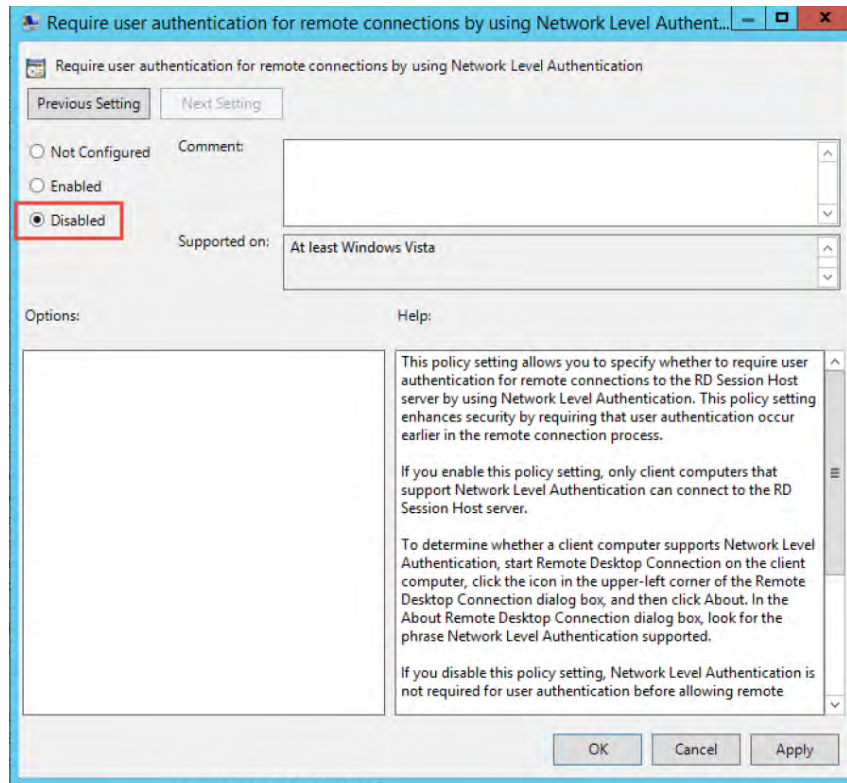
9. Now in the same location in the **Local Group Policy** editor tree, locate the policy for *Set the Remote Desktop licensing mode*. Double-click the policy to open the editor.

10. RDS CAL's can be purchased in two forms, Per Device or Per User. In this step use the drop down list to specify the mode based on the type of license you have purchased from Microsoft.

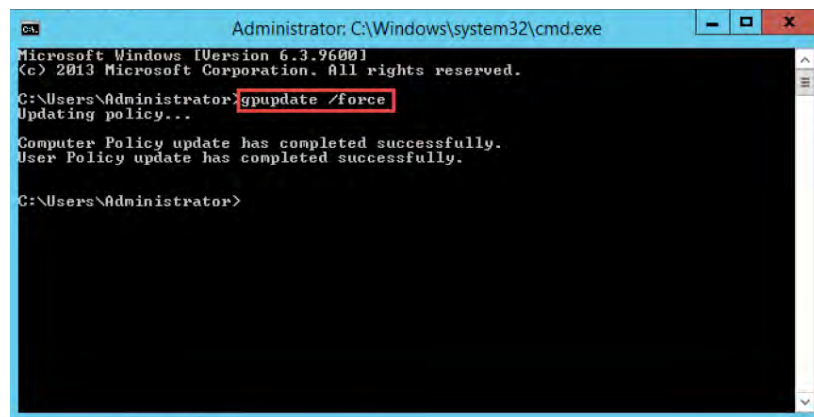


11. From the **Local Group Policy** editor, navigate to Local Computer Policy > Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Security.
12. Optional: Locate and double-click the policy for *Require user authentication for remote connections by using Network Level Authentication*.

13. Disable this policy by checking the radio button next to *Disabled* and click *OK* to apply the changes.



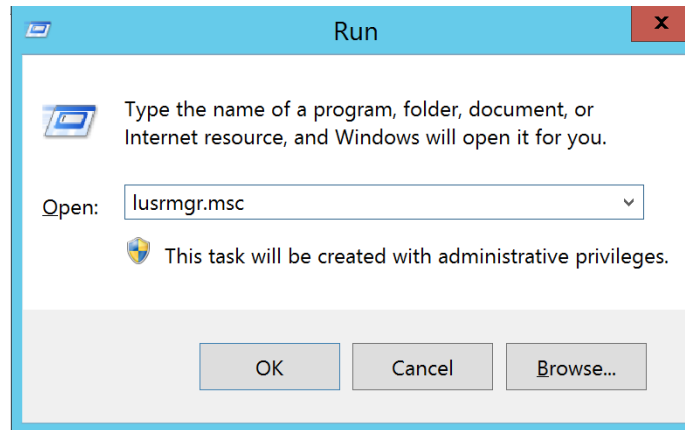
14. Close the **Local Group Policy** editor.
15. From the Windows start menu, open a **Command Prompt** with Administrator Privileges. This can be done by searching the command **cmd** in the windows search bar on the start menu, and right-clicking the **Command Prompt** icon. Select *Run as Administrator*.
16. In the **Command Prompt** window, enter **gpupdate /force** and hit enter to force the policy changes to the local host without having to restart the server.



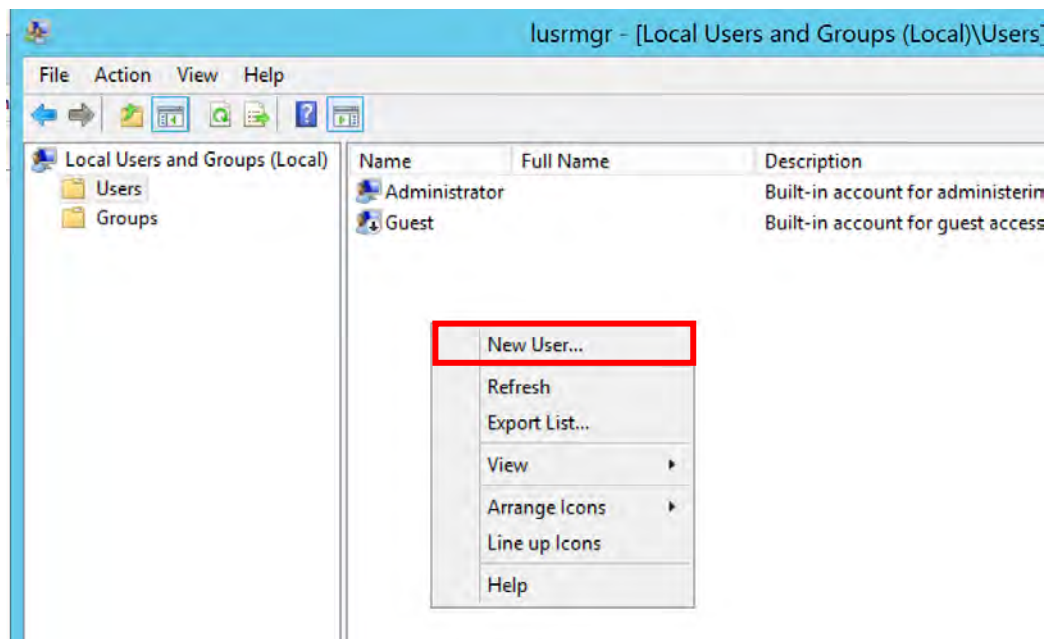
Create Local Users

Local users must be created on each Remote Desktop Session host that will be used to deliver content to a thin client. Please note that an identical set of users must be created and managed on each server if the desire is to use the failover capabilities of ThinManager to enhance system availability or if sessions on any thin client are to come from more than one RD Host server.

1. Launch the run prompt from the windows start menu and enter the command **lusrmgr.msc**. Click **OK**.

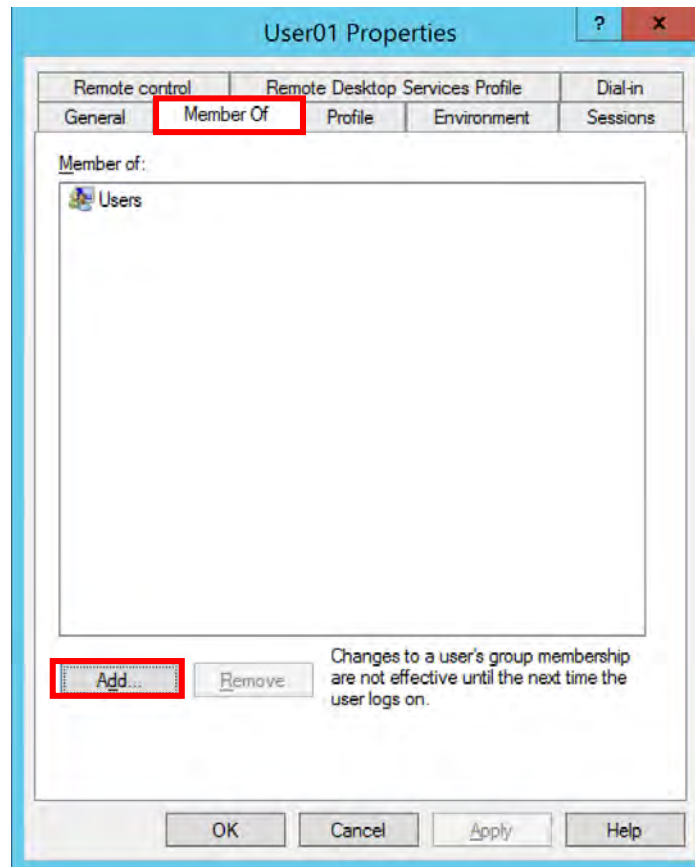


2. Expand the *Users* tab and right-click. Select *Add New User*.

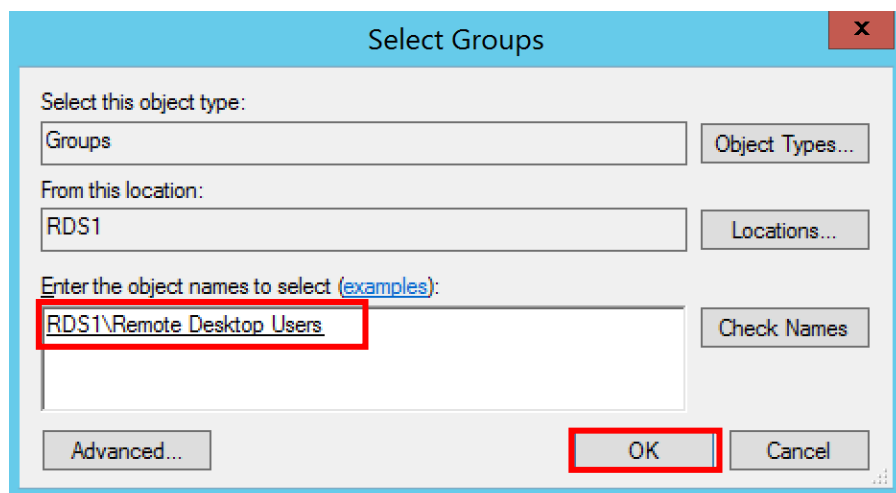


3. Generate the new user adding a name and password. Uncheck the box for *User must change password at next login* and select the box for *Password never expires*.
4. Click *Create*.
5. Right-click on the newly created user and select the *Properties* option.

6. In the **Properties** window, locate the *Member Of* tab.



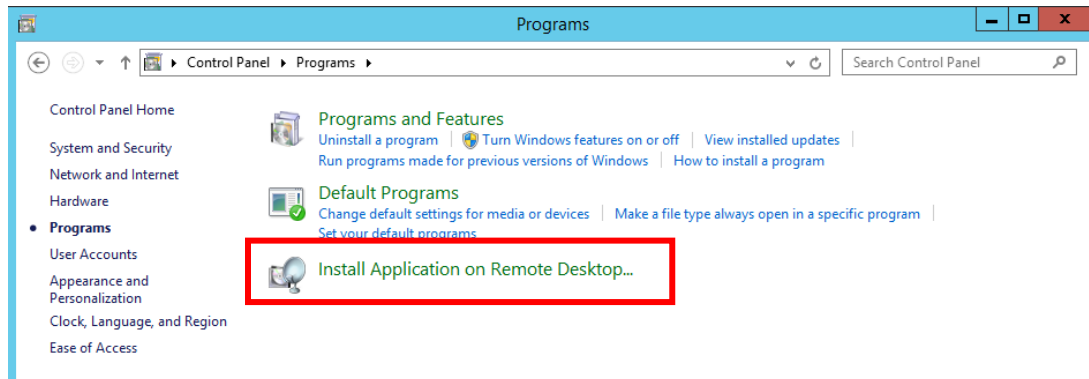
7. Click *Add* to add this user to another group. Browse to the Remote Desktop Users Group and click *OK*.



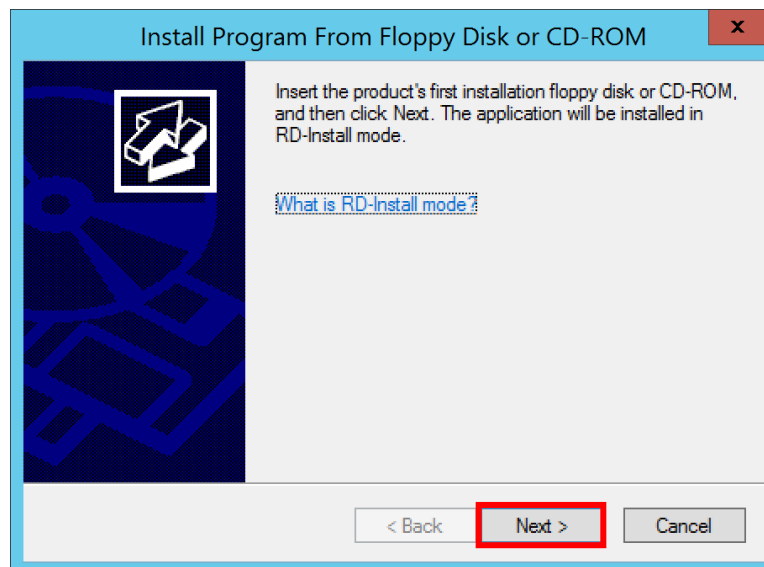
8. Click *Apply* to add this user to the **Remote Desktop Users** group.
9. Repeat this section for all users that will be used to deliver content to any device, user, or location. Repeat this process on all servers using identical users.

Install FTVSE

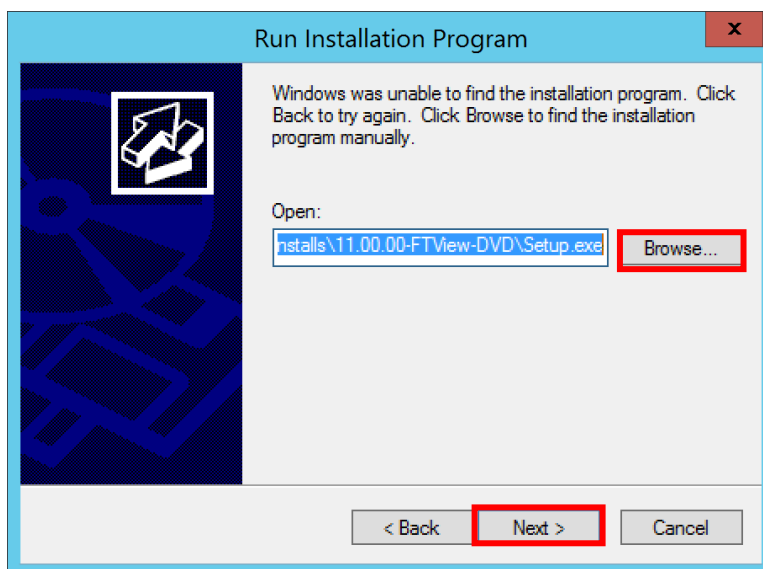
1. From the Remote Desktop Server computer, launch the control panel. In the search bar of the Control Panel, search for *Install Application on Remote Desktop Server*.
2. Locate the *Install Application on Remote Desktop Server* tool. This can also be found in the programs section of the Control Panel.



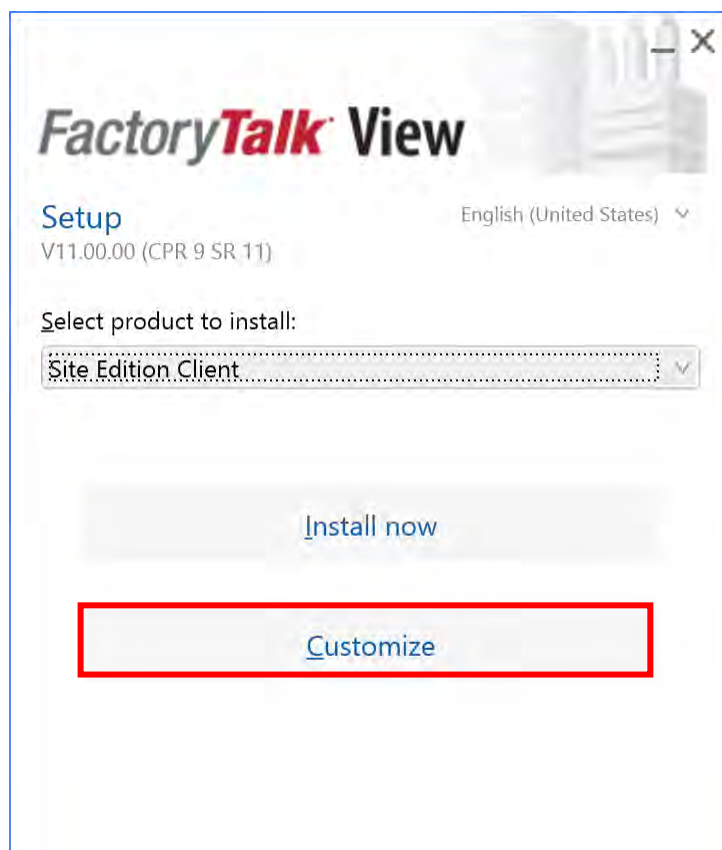
3. This will launch an application that will allow you to install an application for use in a remote desktop environment.



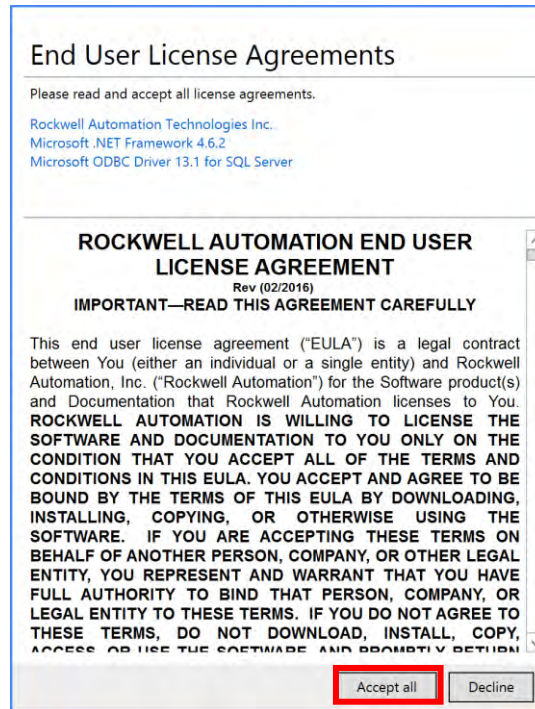
4. Browse to the **Setup.exe** file located in the 11.00.00-FTView-DVD installation folder. Click *Next*.



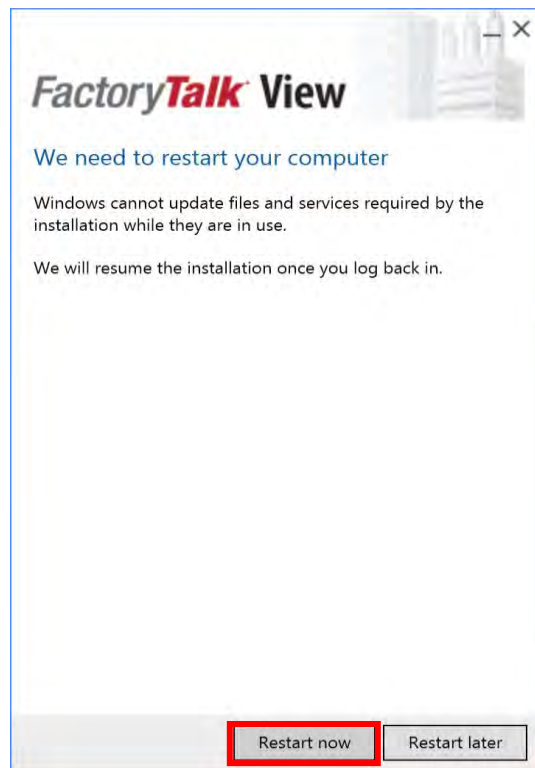
5. From the drop-down selector, locate *Site Edition Client* and click *Install Now*.



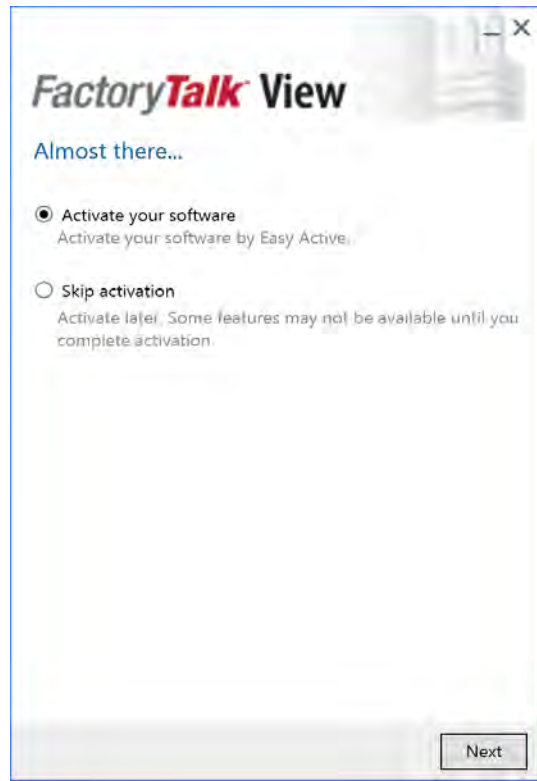
6. Click *Accept all* on the EULA page to begin the installation.



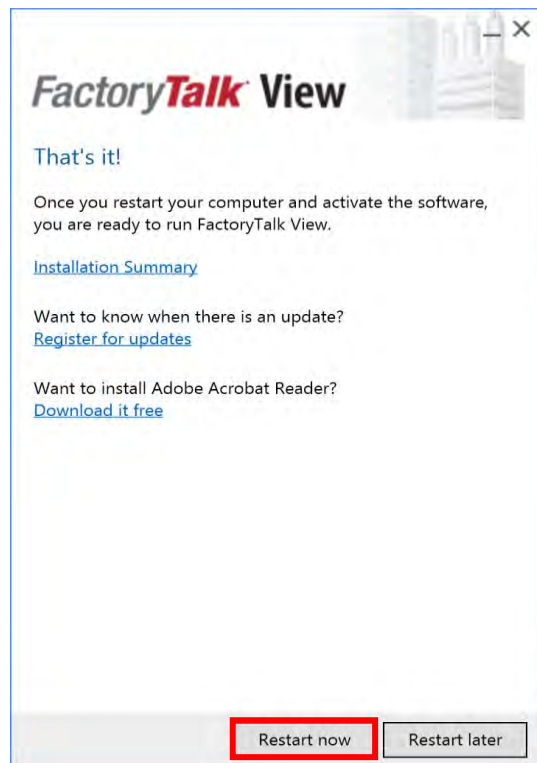
7. If .NET components need to be installed, the components will install automatically. If they are installed, you will be prompted to restart the computer. If prompted, click *Restart Now*.



8. Following the installation, you will be prompted to select the activation method. You may skip activating the software to finish the install.



9. Click *Restart Now* to complete the installation.

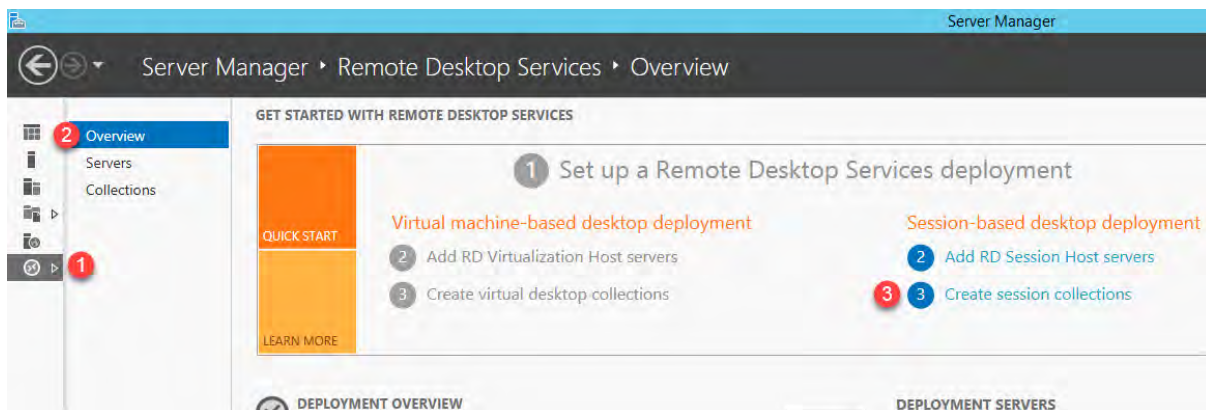


Publish Remote Applications (Domain Environment Only)

If it is desired to use the *AppLink* feature of ThinManager to deliver just a Windows application to the terminal as opposed to the full desktop experience, each application that is to be delivered should be published as a Remote Application in Remote Desktop Services. In a workgroup deployment, we allow the use of unlisted programs. This can also be configured as a group policy setting.

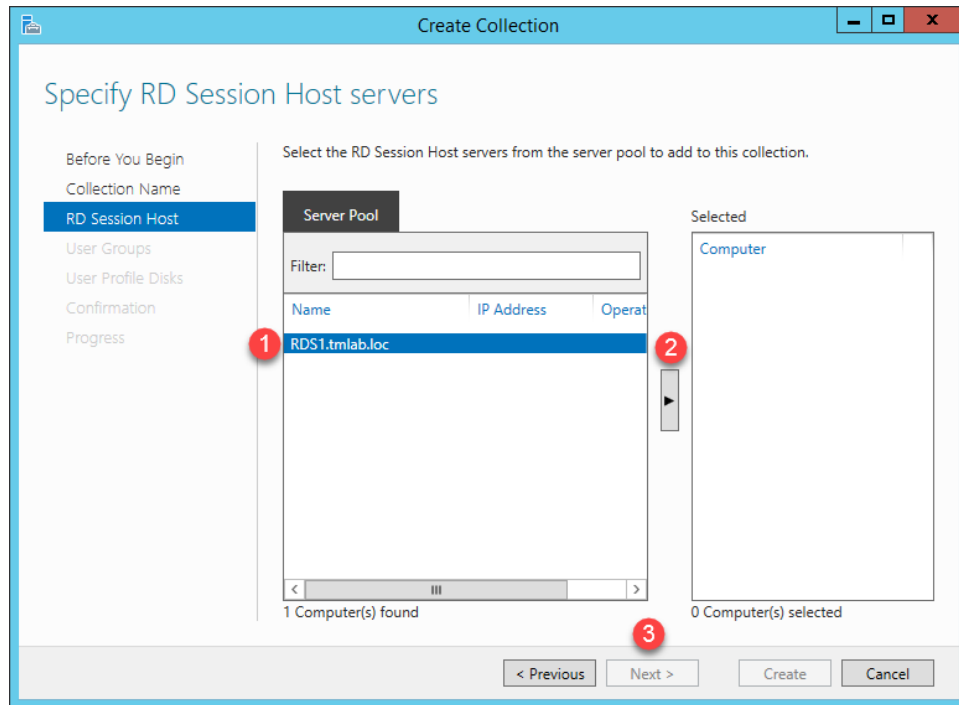
Session Collections are new to Windows Server 2012, and are only available for domain deployments. Collections allow you to group RD Session Host servers and manage their associated properties and published RemoteApps from a single location. A majority of the session based properties found in Server 2008 R2 and earlier can now be found at the Collection level.

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

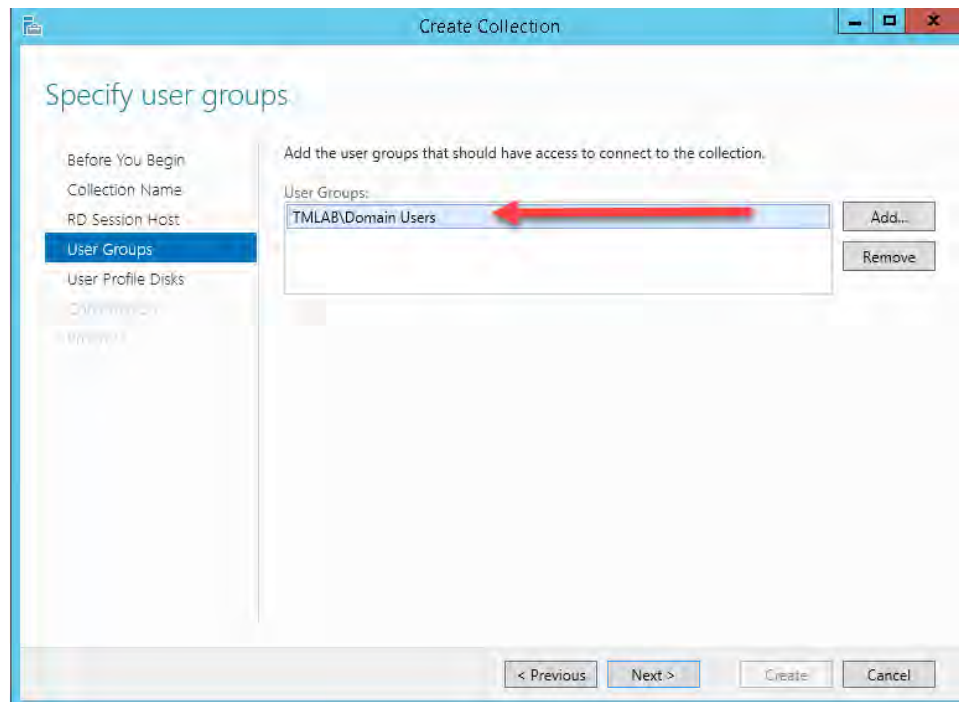


2. From the **Before You Begin** page of the **Create Collection** wizard, click *Next>*.
3. From the **Collection Name** page of the **Create Collection** wizard, enter *RDS1*, then click *Next>*.

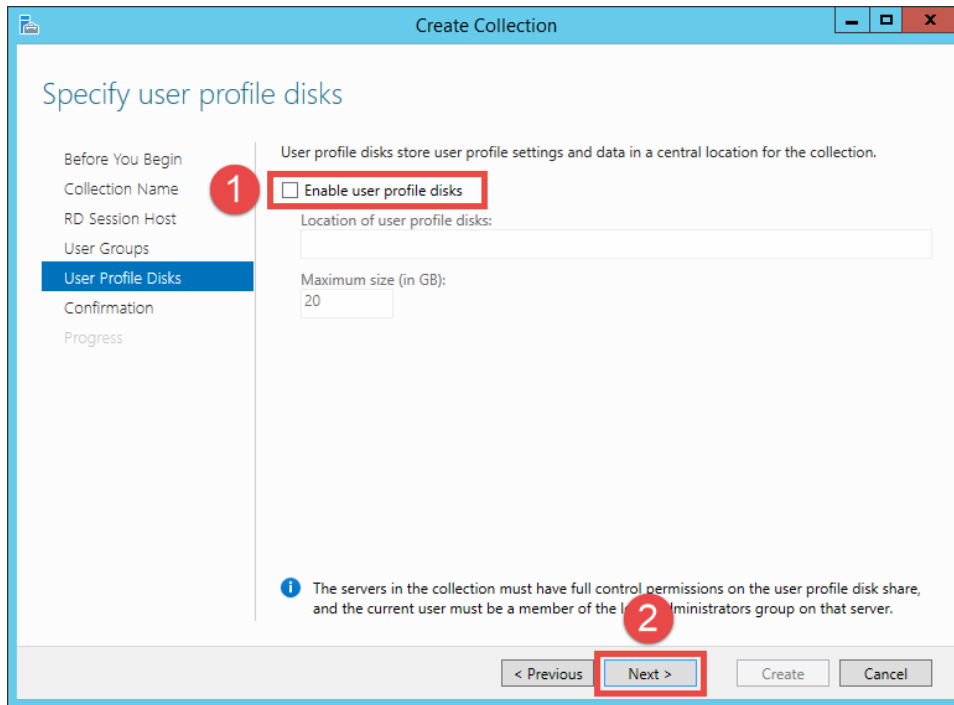
4. From the **RD Session Host** page of the **Create Collection** wizard, click the *Right Arrow* button to add **RDS1.tmlab.loc** to the Selected list and click *Next>*.



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



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



Create Collection

Specify user profile disks

Before You Begin
Collection Name
RD Session Host
User Groups
User Profile Disks
Confirmation
Progress

User profile disks store user profile settings and data in a central location for the collection.

☐ **Enable user profile disks**

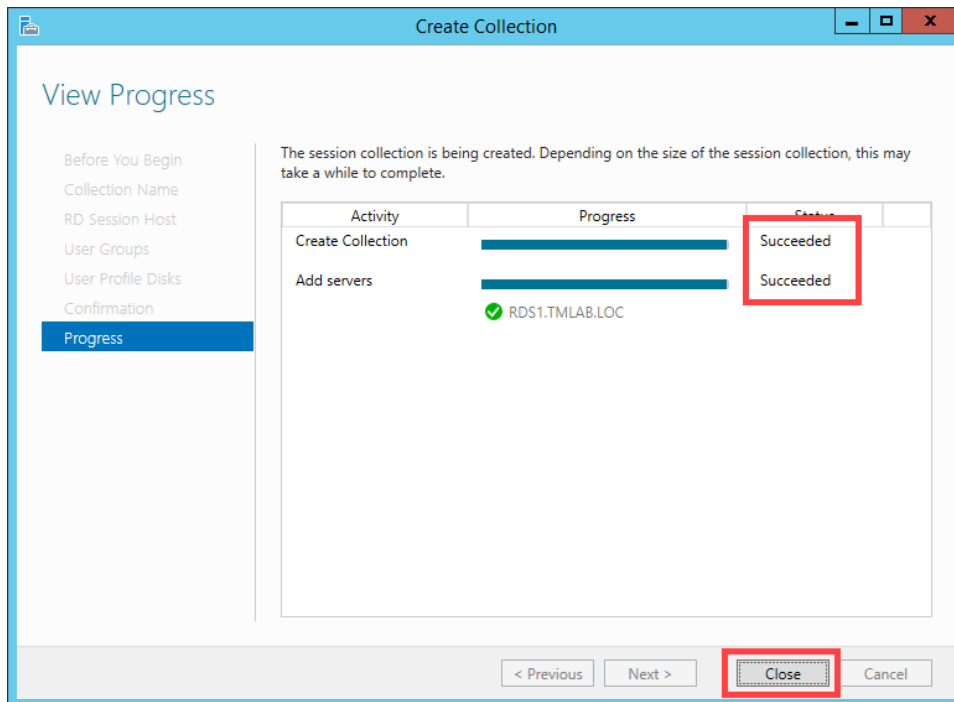
Location of user profile disks:

Maximum size (in GB):
20

i The servers in the collection must have full control permissions on the user profile disk share, and the current user must be a member of the local administrators group on that server.

< Previous **Next >** Create Cancel

7. Click the *Create* button from the **Confirmation** page of the **Create Collection** wizard.
8. Once complete, the **Status** indication should change to **Succeeded**. Click the *Close* button.



Create Collection

View Progress

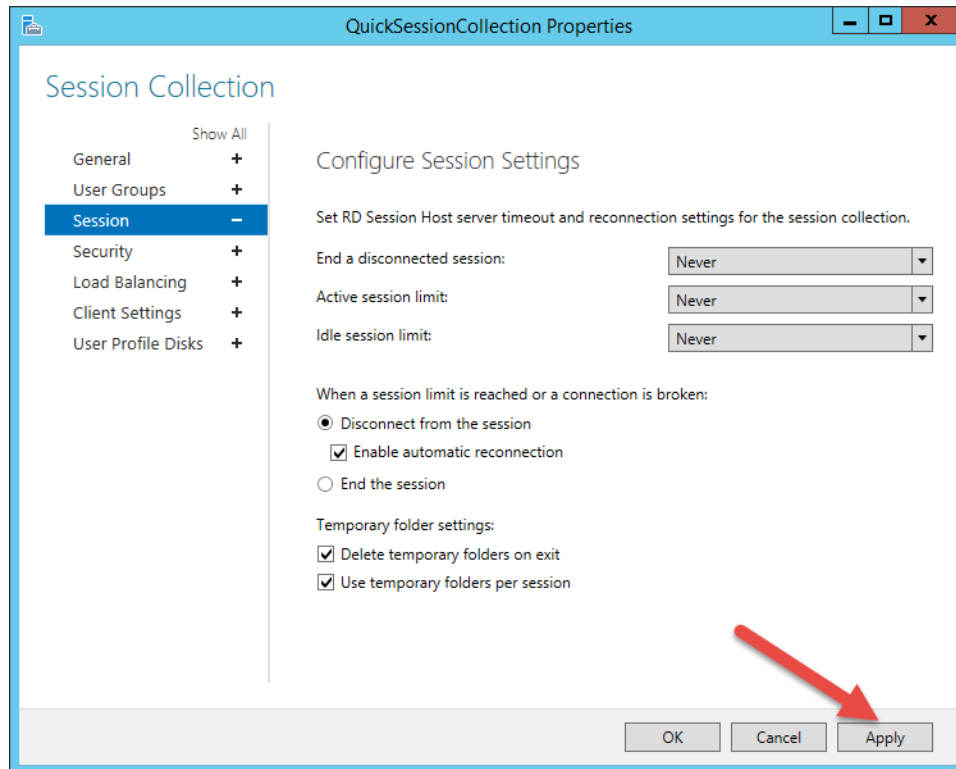
Before You Begin
Collection Name
RD Session Host
User Groups
User Profile Disks
Confirmation
Progress

The session collection is being created. Depending on the size of the session collection, this may take a while to complete.

Activity	Progress	Status
Create Collection	<div></div>	Succeeded
Add servers	<div></div>	Succeeded
✓ RDS1.TMLAB.LOC		

< Previous Next > **Close** Cancel

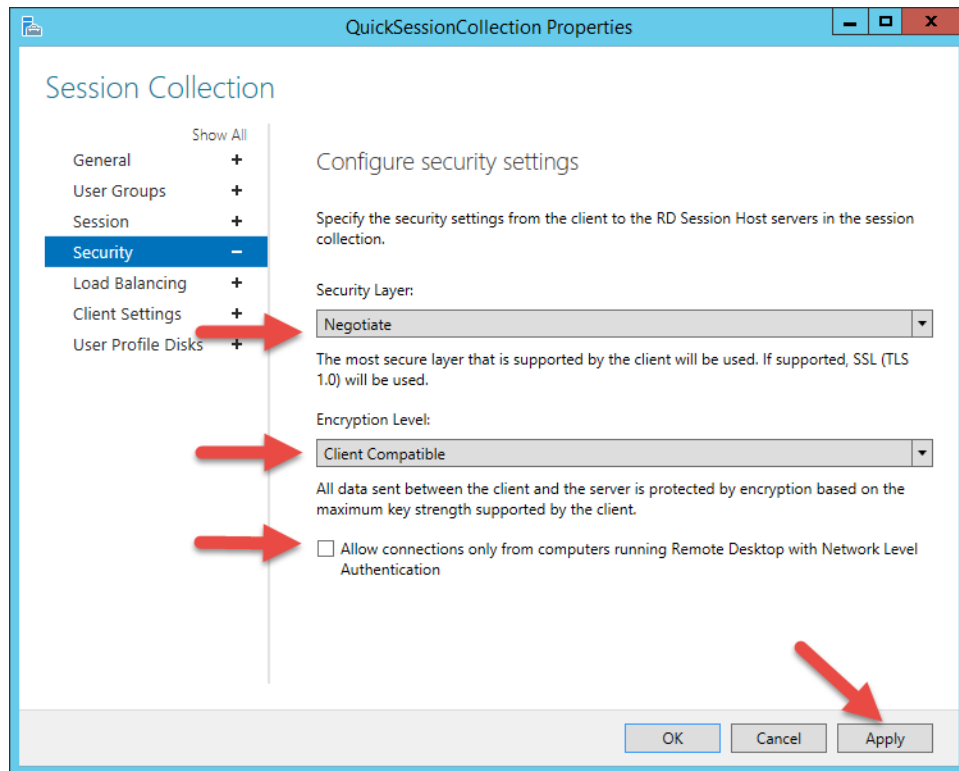
9. To edit the settings of the collection, right-click on the collection name from the **Server Manager** as shown below and select *Properties*.
10. Select the *Session* item in the left menu, and make any adjustments you would like to use for your system. The defaults here will work fine for ThinManager. Press *Apply* when complete.



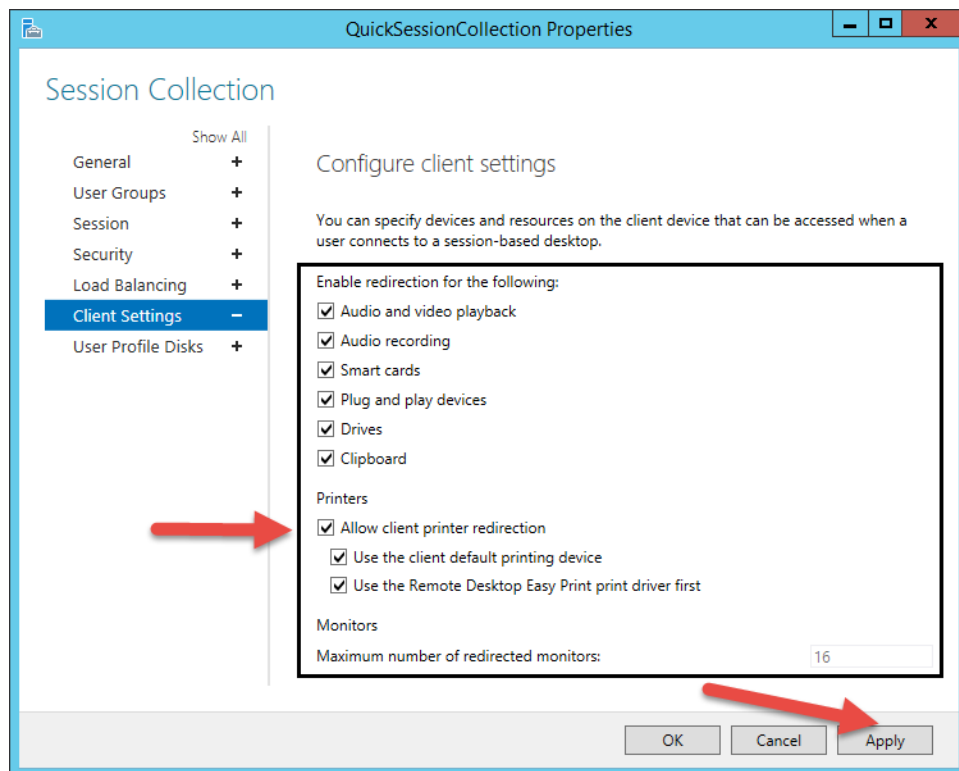
11. Press the *Security* item in the Menu to the left. Make sure your settings match those shown in the image below. Key for ThinManager clients is that you **UNCHECK** the *Allow Connections Only from...* item.

Note: [Network Level Authentication \(NLA\)](#) is supported in Firmware Package 7.1.3 and later. You can leave the *Allow Connections Only from...* item checked. The current firmware build as of the release of ThinManager 11.00.00 is 8.1.21.

12. Press *Apply* once finished.




13. Select the *Client Setting* item in the menu to the left. Select the items you wish to change, and press *Apply*. The default settings (shown below) will work for ThinManager.

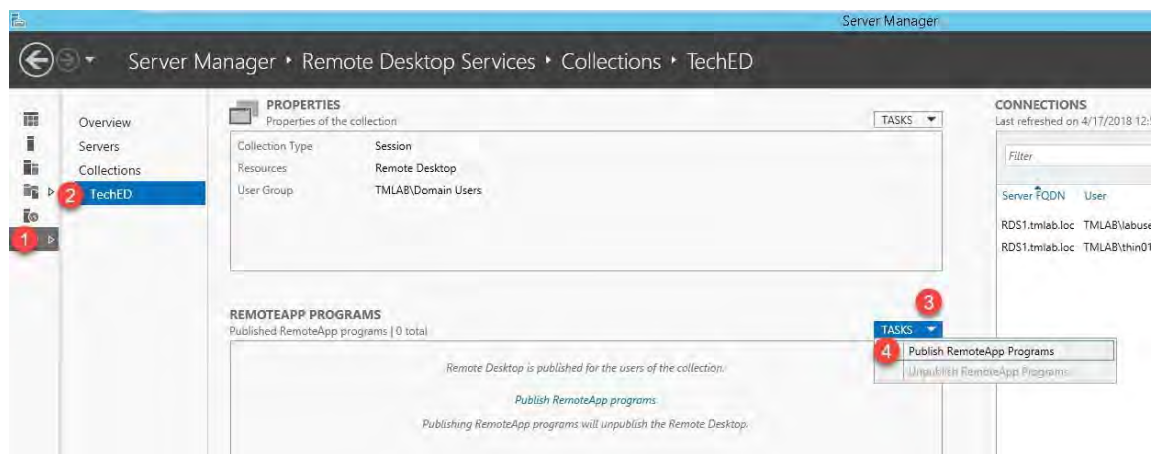


Create a RemoteApp for FactoryTalk View SE

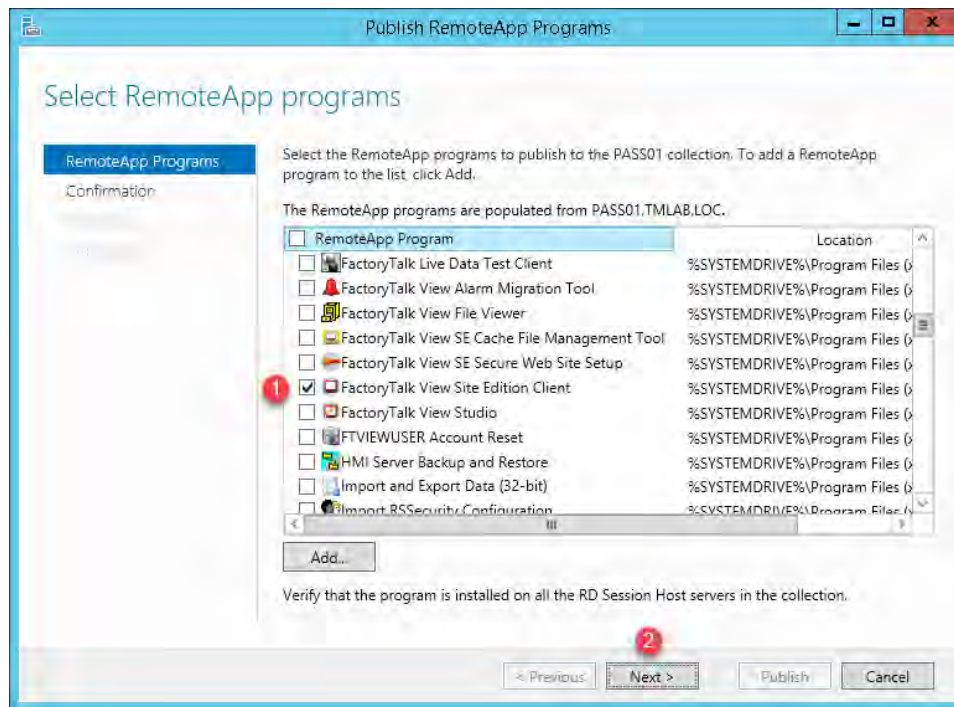
Remote Desktop Services considers any program configured to run initially - like the one you are about to configure with ThinManager ApplicationLink in this section - an “Initial Program.” By default, Windows Server 2008R2 and later Remote Desktop Services requires that each Initial Program be added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

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

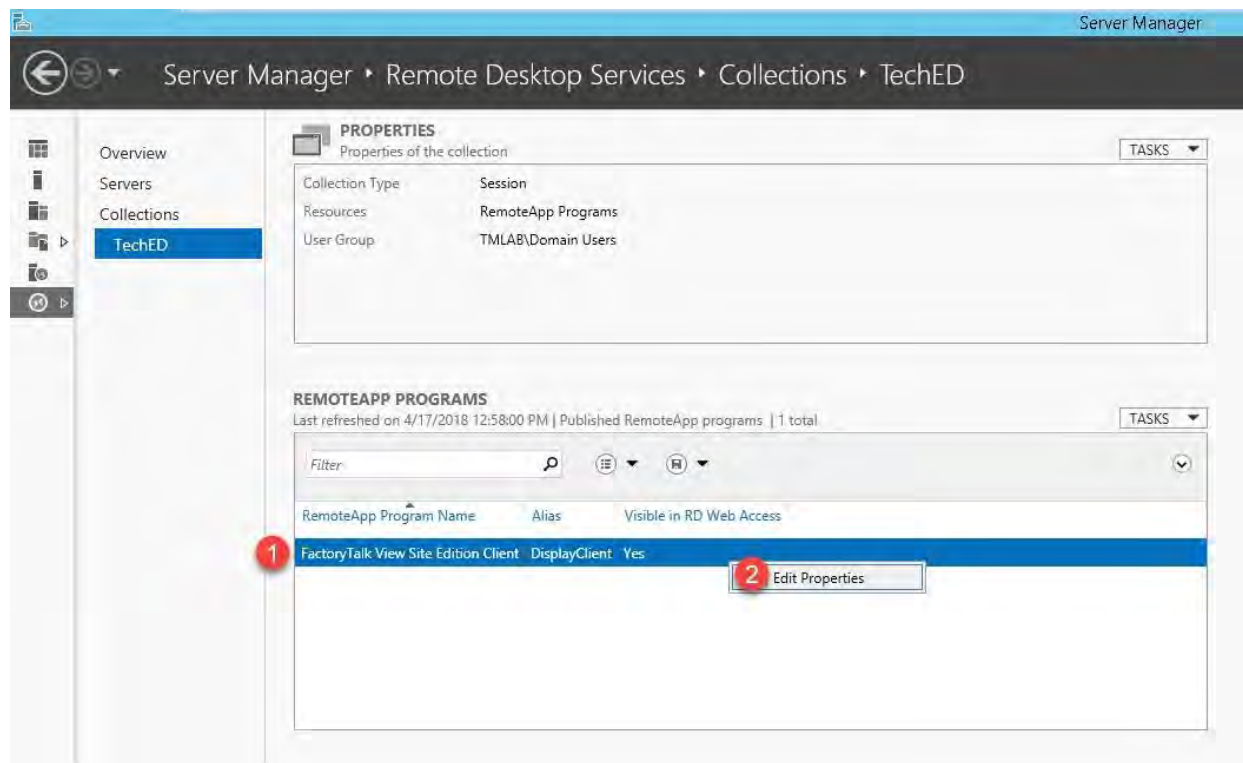
1. From the **RDS1** image, launch **Server Manager** by clicking the Server Manager icon  next to the Windows Start button on the taskbar
2. From **Server Manager**, select the *Remote Desktop Services* panel item, followed by the collection name panel item (under **Collections**).
3. Click the *Tasks* dropdown list in the **RemoteApp Programs** frame, followed by the *Publish RemoteApp Programs* item.



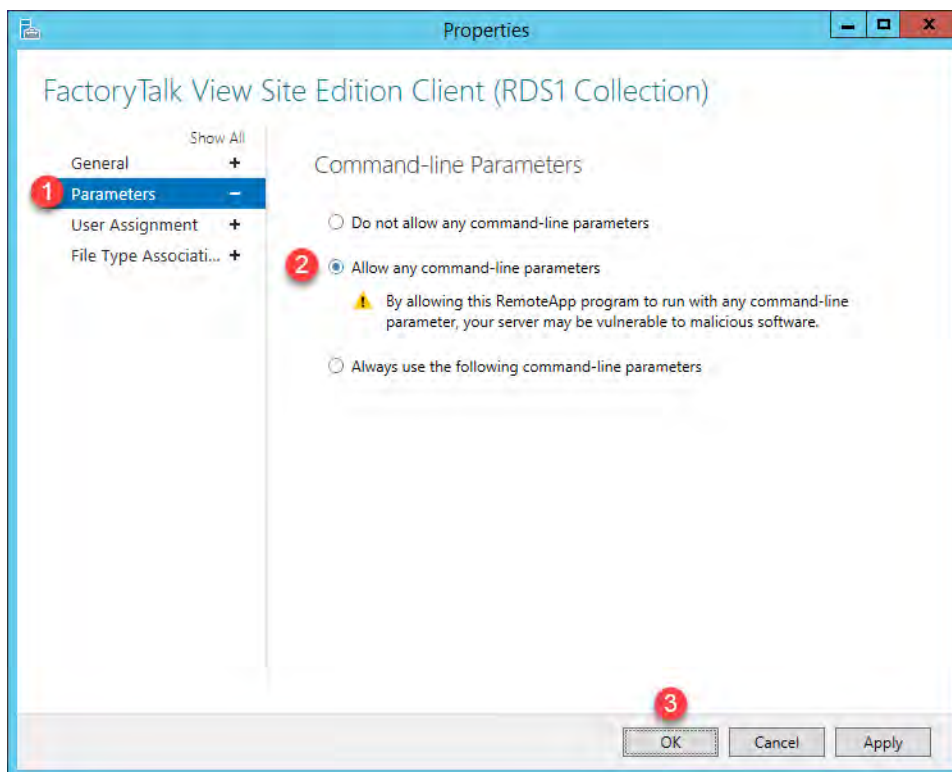
4. From the **Publish RemoteApp Programs** dialog, scroll down and check the **FactoryTalk View Site Edition Client** list item, followed by **Next>**.



5. Click the **Publish** button on the **Confirmation** page.
6. Once **Status** changes to **Published**, click the **Close** button.
7. Right click the newly listed **RemoteApp** and select **Edit Properties**.



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



FactoryTalk View SE Client Configuration

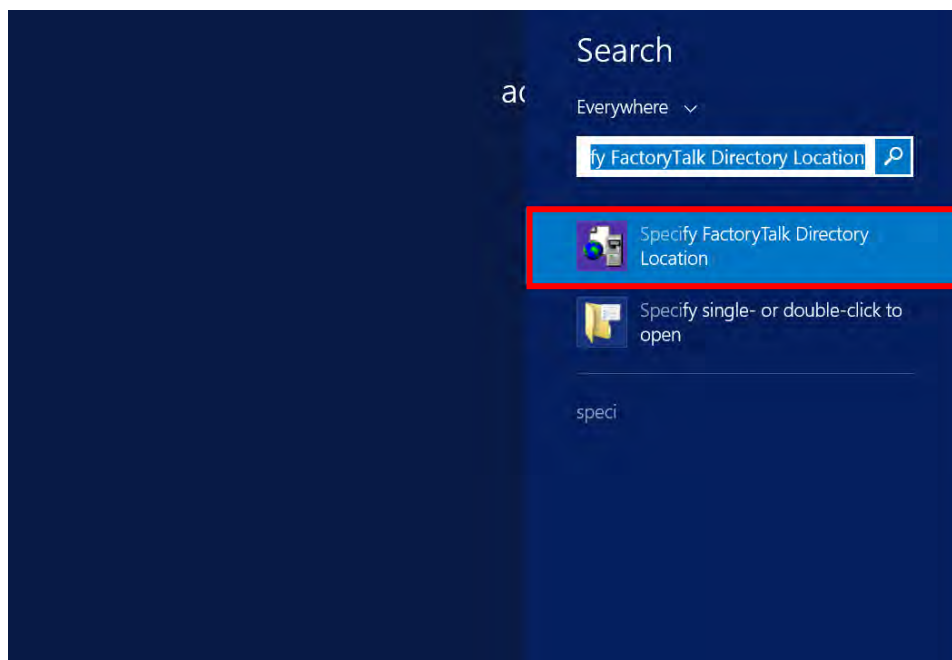
The FactoryTalk Directory and FactoryTalk View Site Edition Server should be located off the Remote Desktop Server that is used to deliver sessions to ThinManager managed terminals. While an ‘All-In-One’ deployment is supported, it is not a FactoryTalk View SE recommended architecture. For more information on setting up a FactoryTalk Directory and for reference architectures, please refer to the [FactoryTalk View SE Installation Guide](#).

FactoryTalk Security

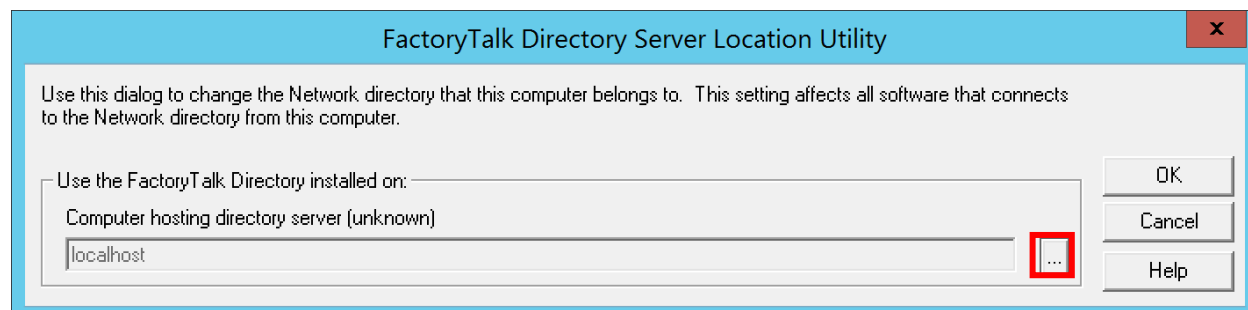
Before configuring the client file for FactoryTalk View SE, we must allow the connection to the HMI server using FactoryTalk Directory.

The first step will be to specify the network location of the FactoryTalk Directory.

1. From the Windows start menu, search for and locate the application named *Specify FactoryTalk Directory Location*.



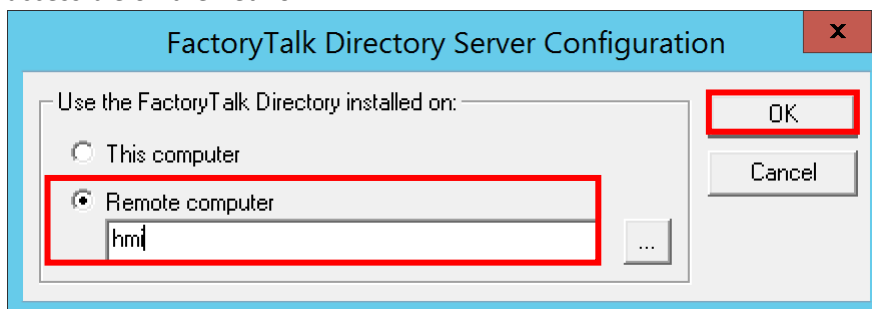
2. From the window that launches, select the ellipsis (...) button to specify the remote network location.



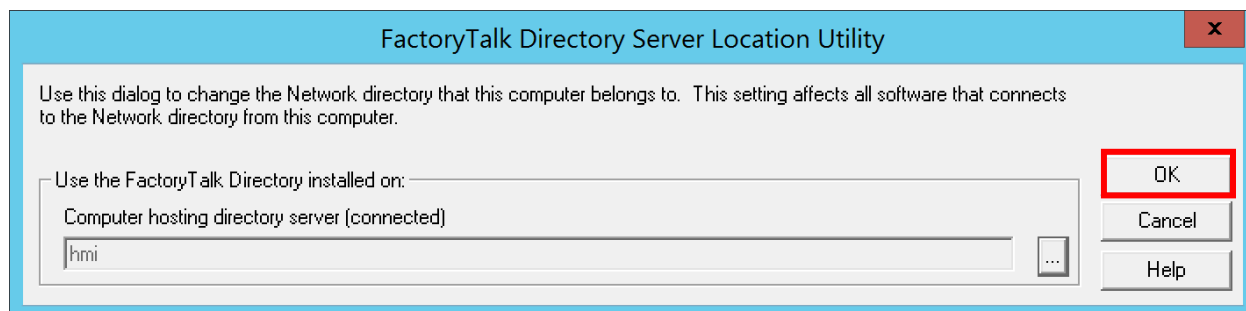
- Enter the administrator credentials that were used with configuring the Network Directory on the HMI server.



- From the ensuing window, select the radio button next to *Remote Computer* and enter or browse to the network location that hosts the **FactoryTalk Directory**. Click **OK**.
Note: If network discovery is not enabled, the browse feature may not find the remote server, even if it is accessible on the network.



- Click **OK** to confirm the changes. You will again be prompted for the **FactoryTalk Directory** administrator credentials.

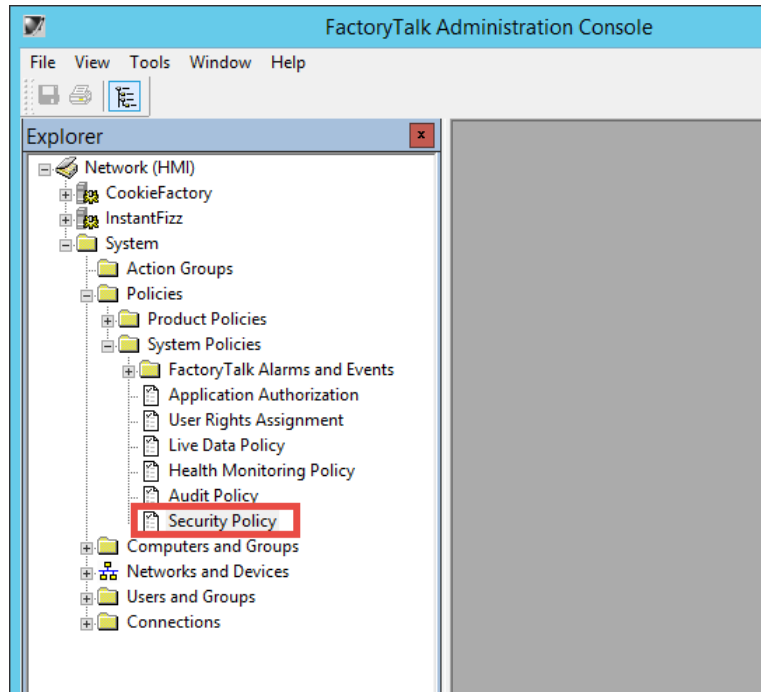


- You must now restart the server for these changes to take place.

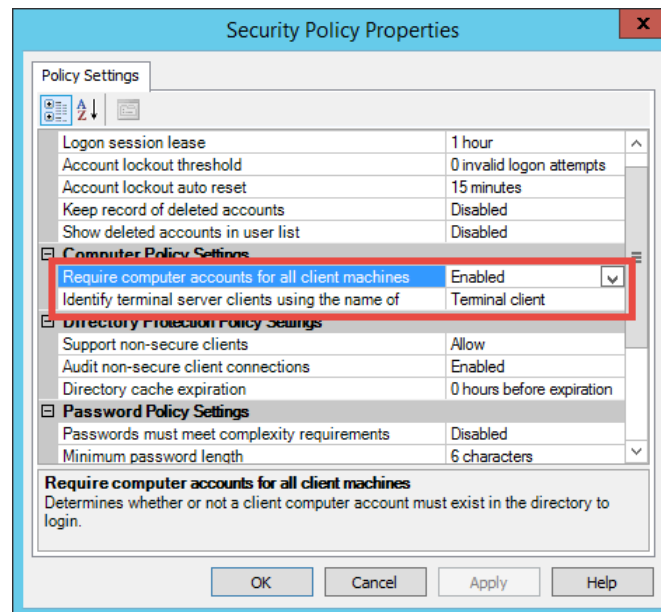
After specifying the network directory that hosts the directory, the security settings must be configured to allow the terminals to launch remote applications, such as FactoryTalk View SE.

FactoryTalk security will prevent unauthorized users and computers from accessing the HMI visualization tools that are used for critical plant wide control

7. From the Windows start menu, locate and launch the *FactoryTalk Administration Console*.
8. In the *Explorer* view, browse to *Network (HMI) >System>Policies>System Policies>Security Policy* and double click on *Security Policy* or right click on *Security Policy* and select *Properties...* from the menu.



9. Scroll down to the **Computer Policy Settings** section. The **Require computer accounts for all client machines** policy is by default set to *Enabled* and the **Identify terminal server clients using the name of** policy setting is set to *Terminal client*. Click *Apply* and close the dialog. Close the *FactoryTalk Administration Console*.



Require computer accounts for all client machines

Determines whether **client** computers can access the FactoryTalk Network Directory without having a computer account in the Directory.

Enabled allows users to log on to FactoryTalk only if they are logging on from a client computer that has an account in the FactoryTalk Directory. Even if set to Enabled, Terminal Services clients can still log on to FactoryTalk Directory without computer accounts if the **Identify terminal server clients using the name of** policy is set to **Server Computer**. See below.

- Advantage – tighter security...only authorized clients can access the system
- Disadvantage – you must add the name of every authorized computer to the FTD

Important! Even when this setting is disabled, you must still create computer accounts for any computers hosting **servers** — for example, Terminal Servers, Rockwell Automation Device Servers (RSLinx Enterprise), OPC data servers, Tag Alarm and Event Servers, or HMI servers. Without the server computer accounts, you will not be able to configure the servers from client computers on the network because the FactoryTalk Network Directory Server cannot locate these servers on the network without their computer accounts.

Identify terminal server clients using the name of

Determines what computer name identifies clients connecting to the FactoryTalk Directory through Terminal Services. This policy also affects whether client computers connecting through Terminal Services require computer accounts in the FactoryTalk Directory.

Server Computer allows client computers to connect through Terminal Services without requiring accounts in the FactoryTalk Directory, even if the **Require computer accounts for all client machines** policy is **Enabled**. This is possible because Remote Desktop clients are identified by the Remote Desktop Server name, and the Remote Desktop Server must always have an account configured in the FactoryTalk Directory.

- Advantage: There is no need to add the name of each RDP client to the FactoryTalk Directory.
- Disadvantage: Any computer can use an RDP client to remote into the system. Remote Desktop clients are identified by the Remote Desktop Server name, thus actions are logged using the server name instead of the client name, so troubleshooting and auditing actions may be more difficult.

Results of combining the two policies

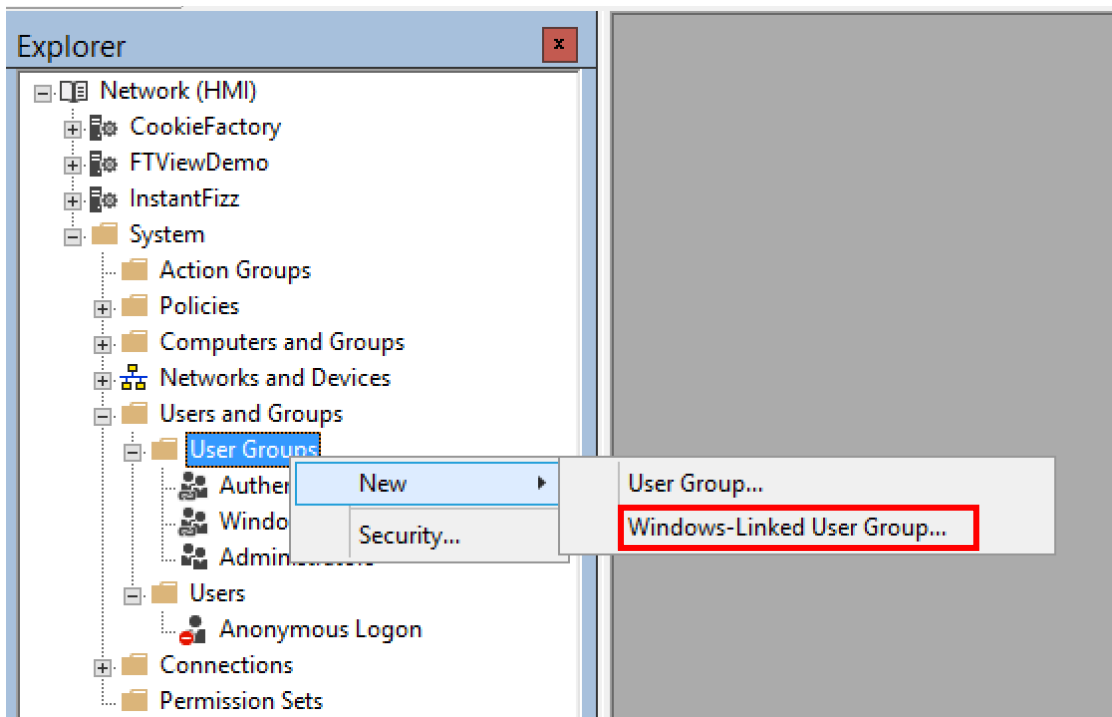
If set to **Terminal Client** and the **Require computer accounts for all client machines** policy is **Enabled**, client computers must have computer accounts in the FactoryTalk Directory to access FactoryTalk applications.

- Advantage: tighter security...only authorized clients can access the system, even using RDP. All activity is logged using the client name.
- Disadvantage: you must add the name of every authorized computer to the FTD, including RDP clients.

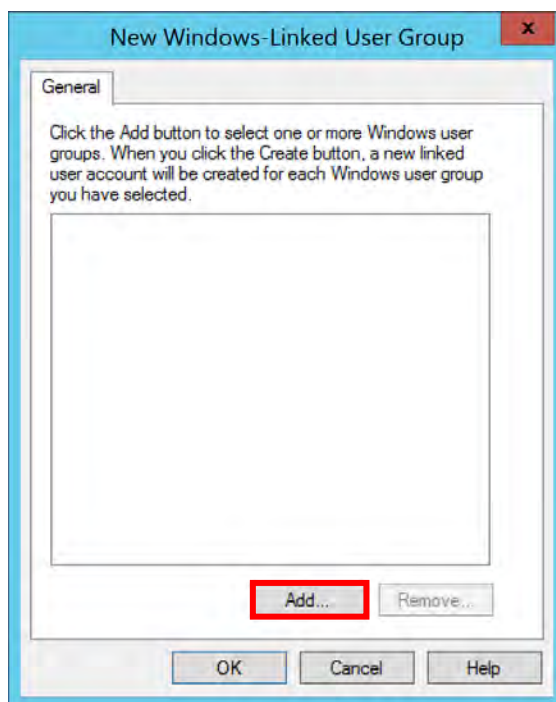
If set to **Terminal Client** and the **Require computer accounts for all client machines** policy is **Disabled**, client computers do not require computer accounts in the FactoryTalk Directory to access FactoryTalk applications. This combination of settings is useful for diagnostic logging because the name of the client computer where actions originate can be logged.

- Advantage: There is no need to add the name of each RDP client to the FactoryTalk Directory. The client name is used for logging.
- Disadvantage: Any computer can connect a client to the system. This include thick client as well as RDP clients.

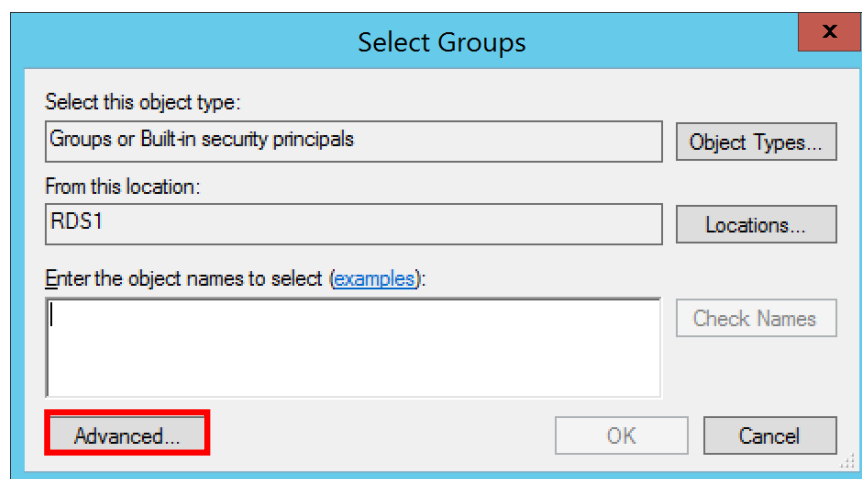
10. After setting the appropriate terminal security policy, the users that will be used should be added to the security profile to allow access to the application. From the *Network Directory*, expand *System>Users and Groups*. Right-click on *User Groups*, highlight *New* and select *Windows-Linked User Group...*



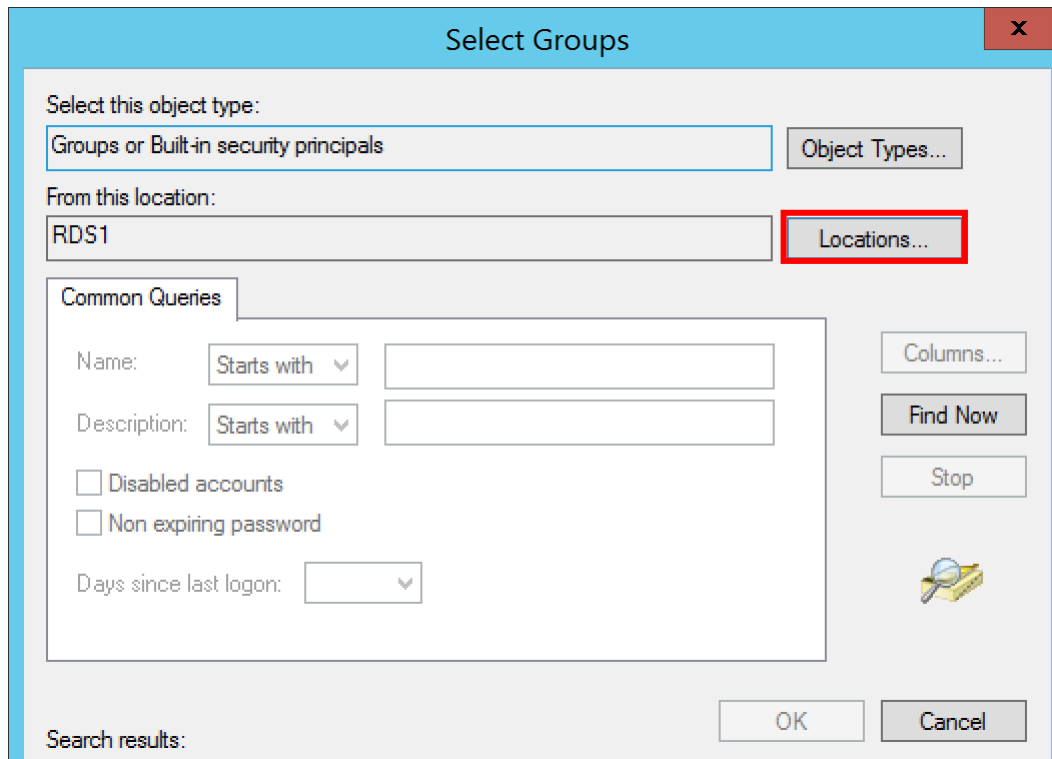
11. Click on *Add...*



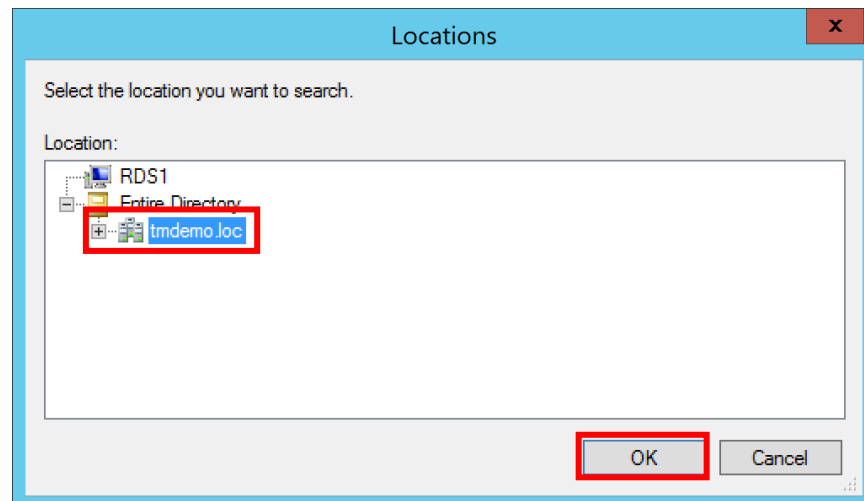
12. Click on the *Advanced...* button.



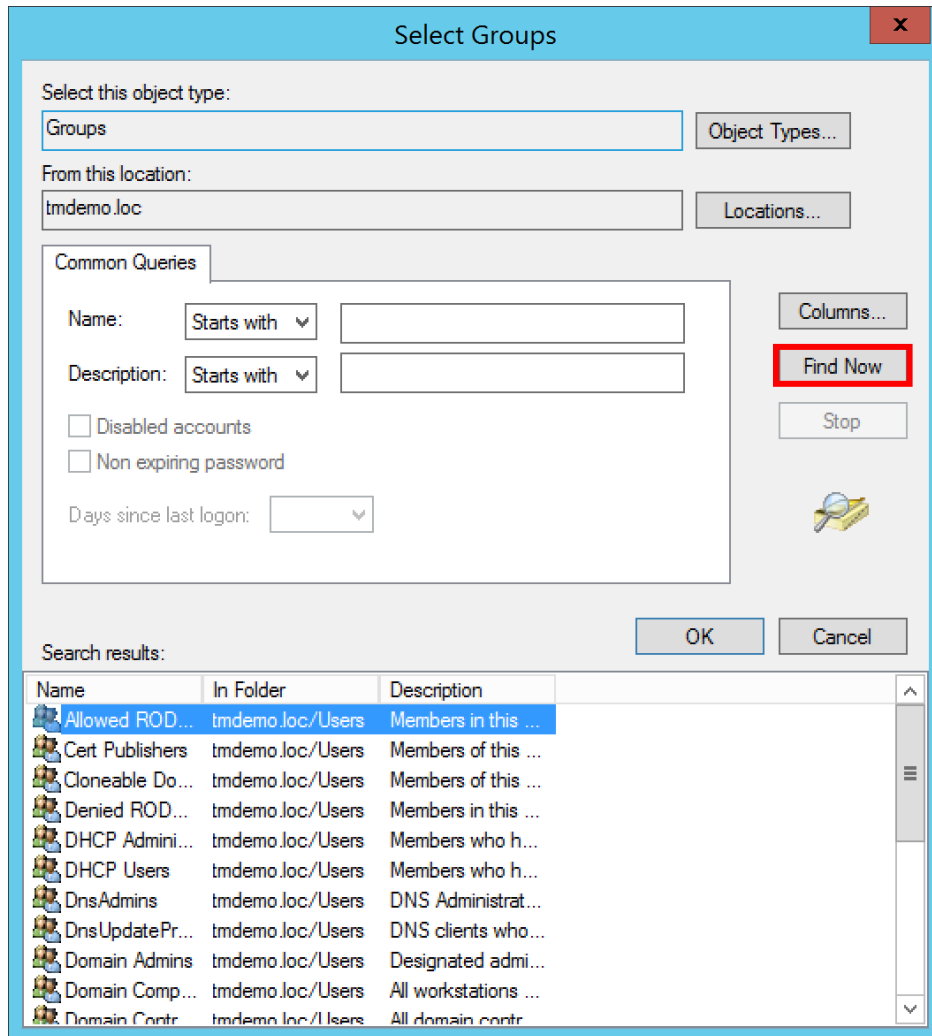
13. Select the *Locations...* button to change the scope from where user groups will be browsed from.



14. Change the scope to the domain present in the environment that is being configured. Click *OK*.



15. Click on *Find Now...* to display all user groups in the domain. Select the user groups that should have access to run a **FactoryTalk View SE Client** and click *OK*.



Select Groups

Select this object type:
Groups

From this location:
tmdemo.loc

Common Queries

Name: Starts with

Description: Starts with

☐ Disabled accounts

☐ Non expiring password

Days since last login:

Columns...

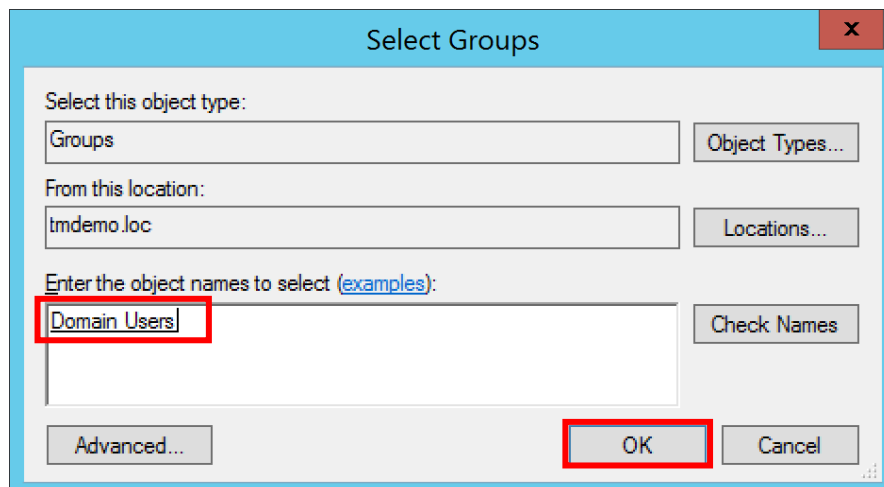
Find Now

Stop

OK Cancel

Name	In Folder	Description
Allowed ROD...	tmdemo.loc/Users	Members in this ...
Cert Publishers	tmdemo.loc/Users	Members of this ...
Cloneable Do...	tmdemo.loc/Users	Members of this ...
Denied ROD...	tmdemo.loc/Users	Members in this ...
DHCP Admini...	tmdemo.loc/Users	Members who h...
DHCP Users	tmdemo.loc/Users	Members who h...
DnsAdmins	tmdemo.loc/Users	DNS Administrat...
DnsUpdatePr...	tmdemo.loc/Users	DNS clients who...
Domain Admins	tmdemo.loc/Users	Designated admi...
Domain Comp...	tmdemo.loc/Users	All workstations ...
Domain Contr...	tmdemo.loc/Users	All domain contr...

16. Click *OK* to accept the selected user groups.



Select Groups

Select this object type:
Groups

From this location:
tmdemo.loc

Enter the object names to select (examples):

Domain Users

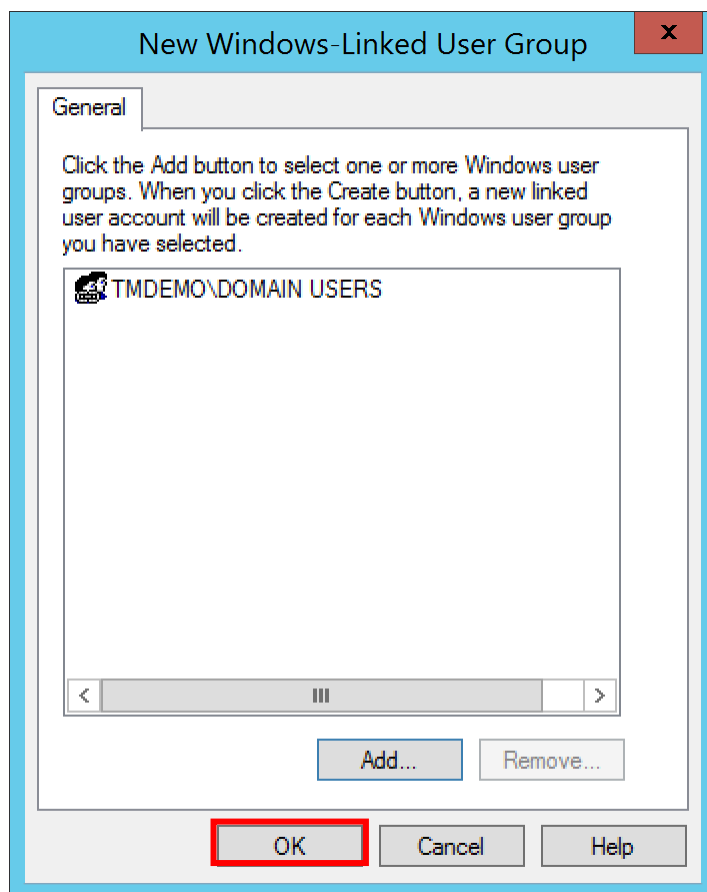
Check Names

Advanced...

OK

Cancel

17. Click *Ok* to accept the changes and complete the security configuration.



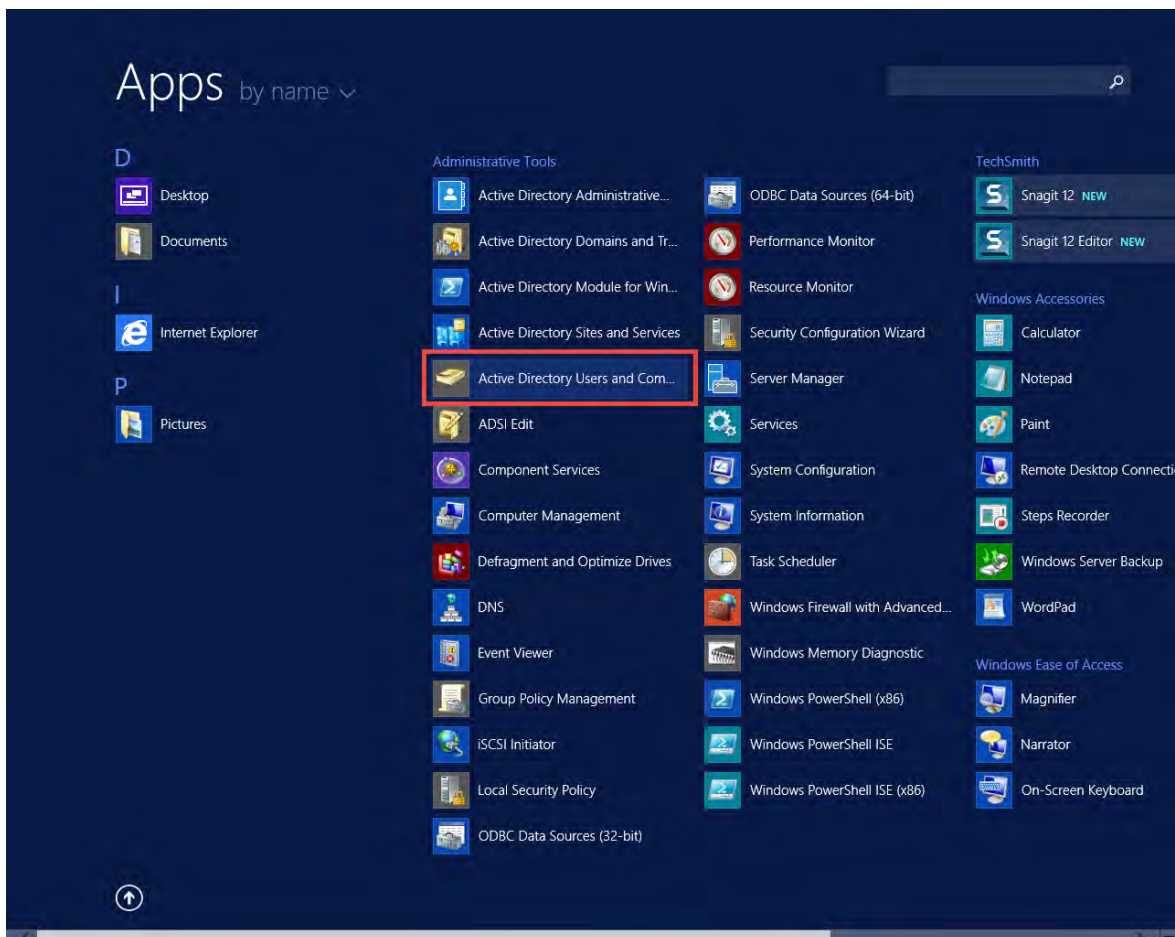
Note: In a workgroup environment, the local users created must all be added to the FactoryTalk Directory in place of the Domain Group that was added in the steps above.

ThinManager Installation

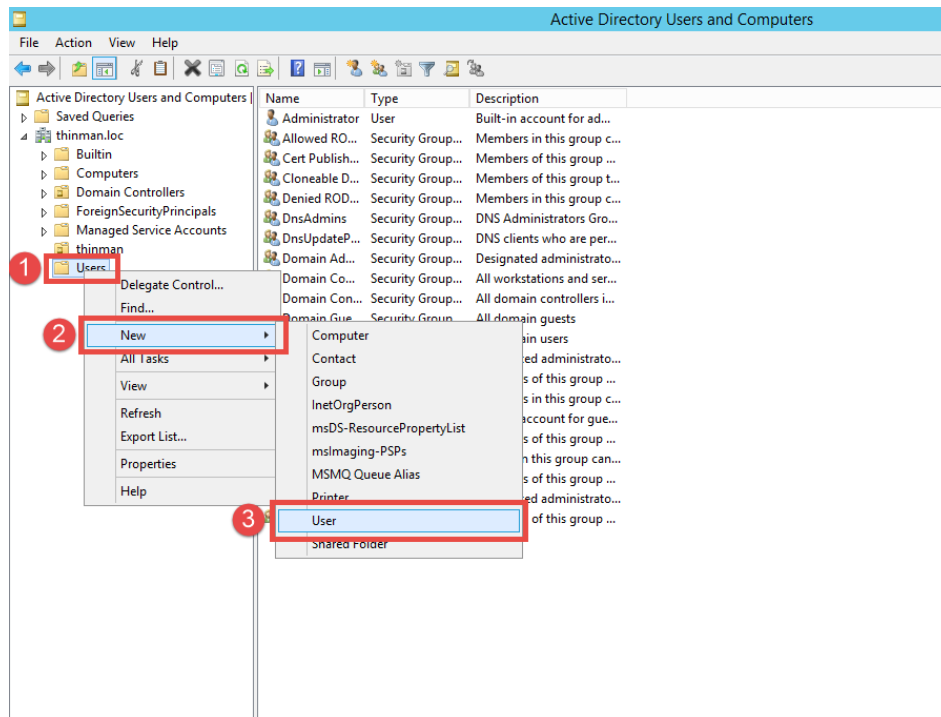
System Preparation

To prepare for the ThinManager installation, we will need to create a Domain service account to be used for the ThinServer service. It will be specified during the ThinManager installation steps that follow. Giving the ThinServer service a specific user context (as opposed to just Local System) will allow the service to communicate to other ThinManager servers (assuming the same user credentials and permissions exist on all servers), as well as expose the ActiveDirectory integration properly. For a workgroup deployment, the user creation steps on the domain controller can be skipped, and the local administrator account created earlier in this document will be used.

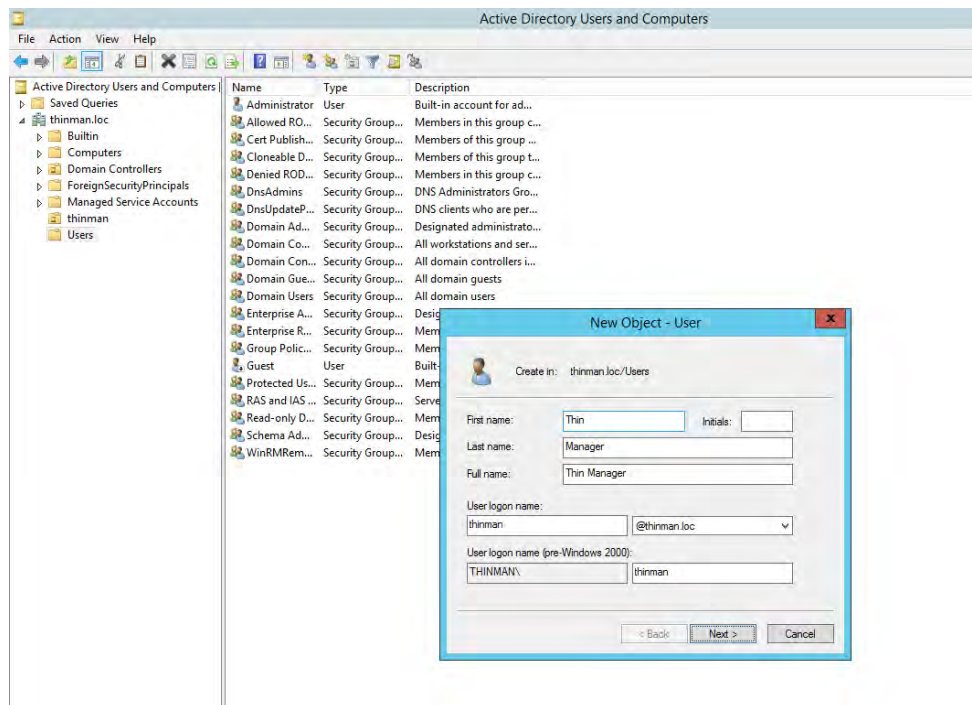
1. Login to your Domain Controller - in this Configuration Guide, that would be **DC** - with the Domain Administrator account.
2. Click the Windows Start button and locate the **Active Directory Users and Computers** shortcut.



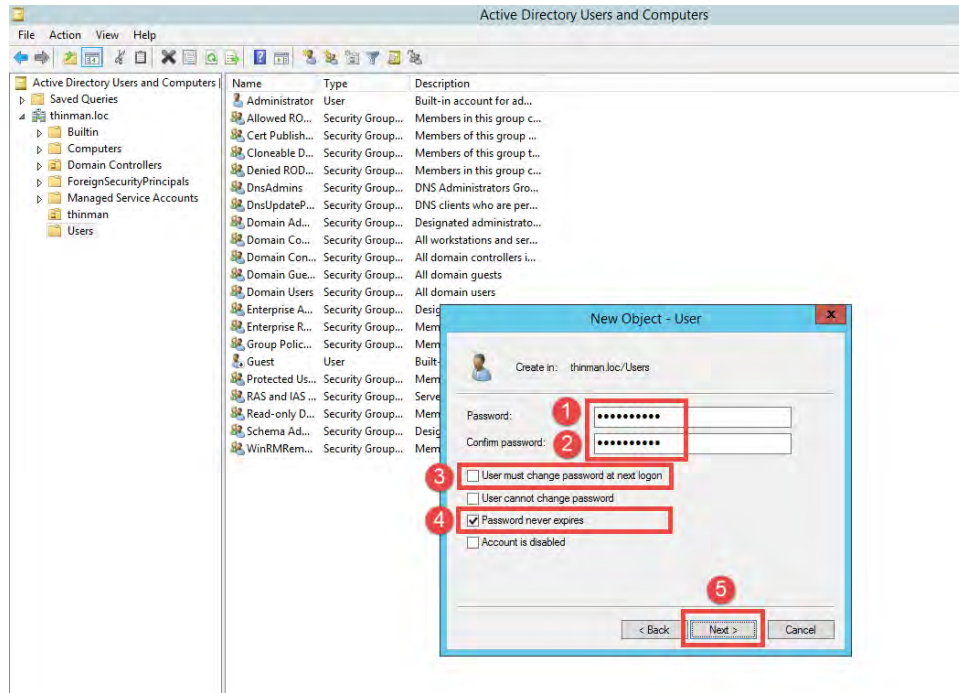
- Right click the *Users* menu item, then select the *New* item followed by the *User* item.



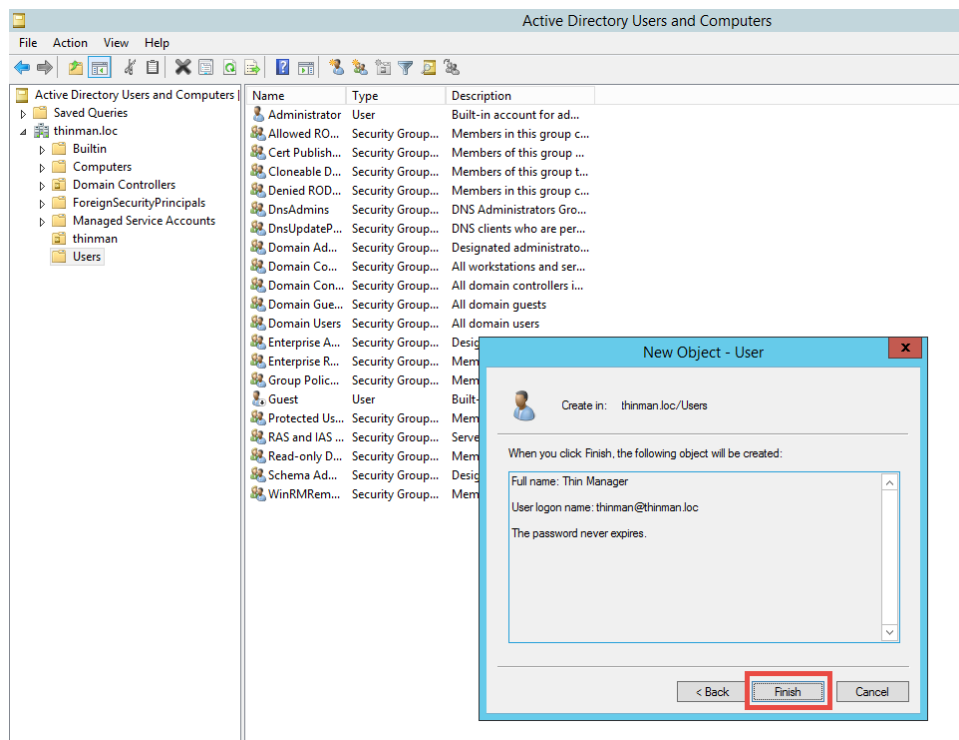
- From the *New Object – User* wizard, enter the *First name*, *Last name*, and *User login name* for the domain account to be used by the **ThinServer** service.
- Click the *Next* button.



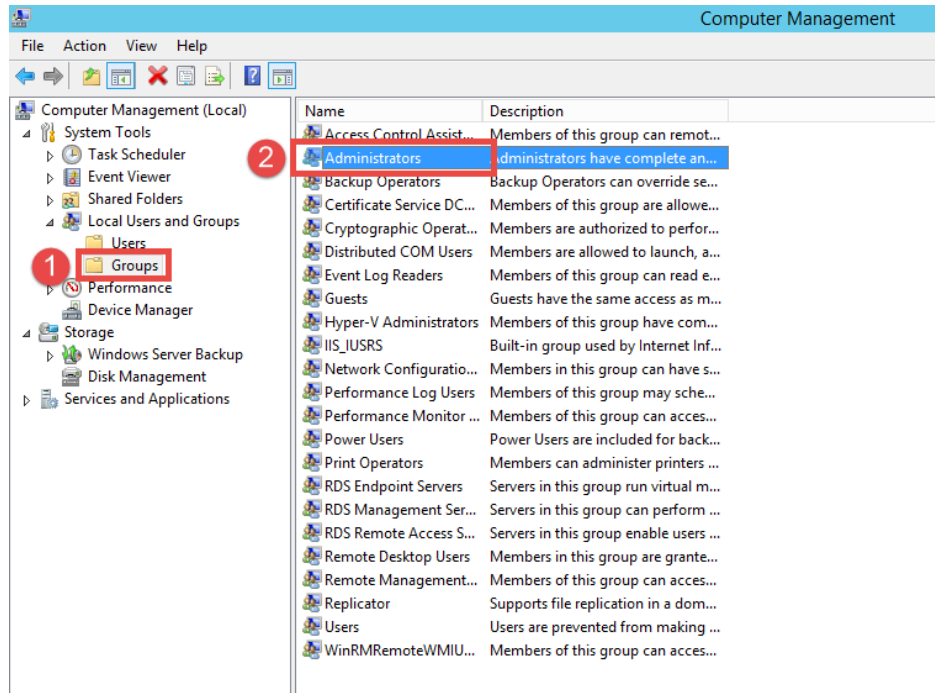
6. Enter and confirm the *Password*.
7. Uncheck the *User must change password at next logon*.
8. Check the *Password never expires* checkbox.
9. Click the *Next* button.



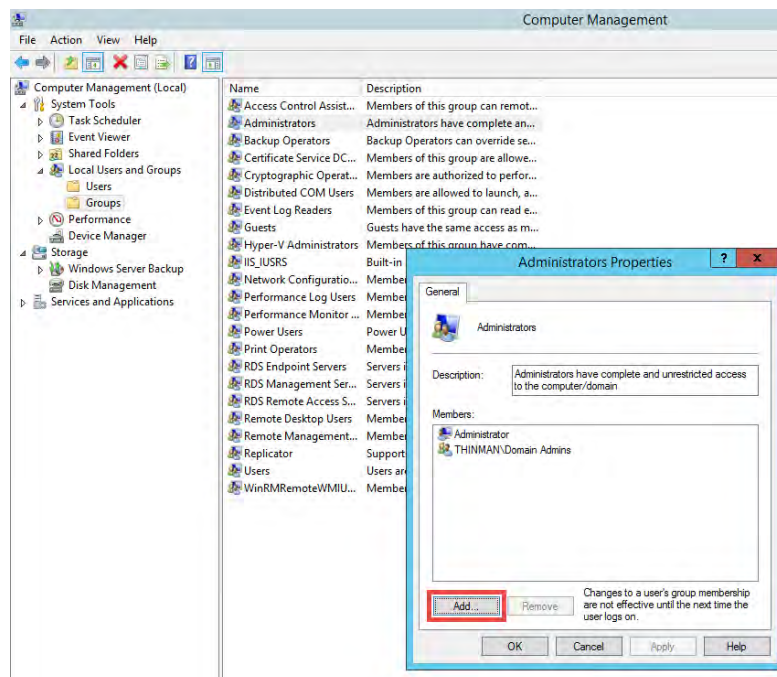
10. Click the *Finish* button.



11. Return to **RDS1** (the Remote Desktop Server) and login as the Domain Administrator account.
12. Right click the Windows Start button and select the **Computer Management** item.
13. From the **Computer Management** window, select the **Groups** item.
14. Double-click the **Administrators** group.



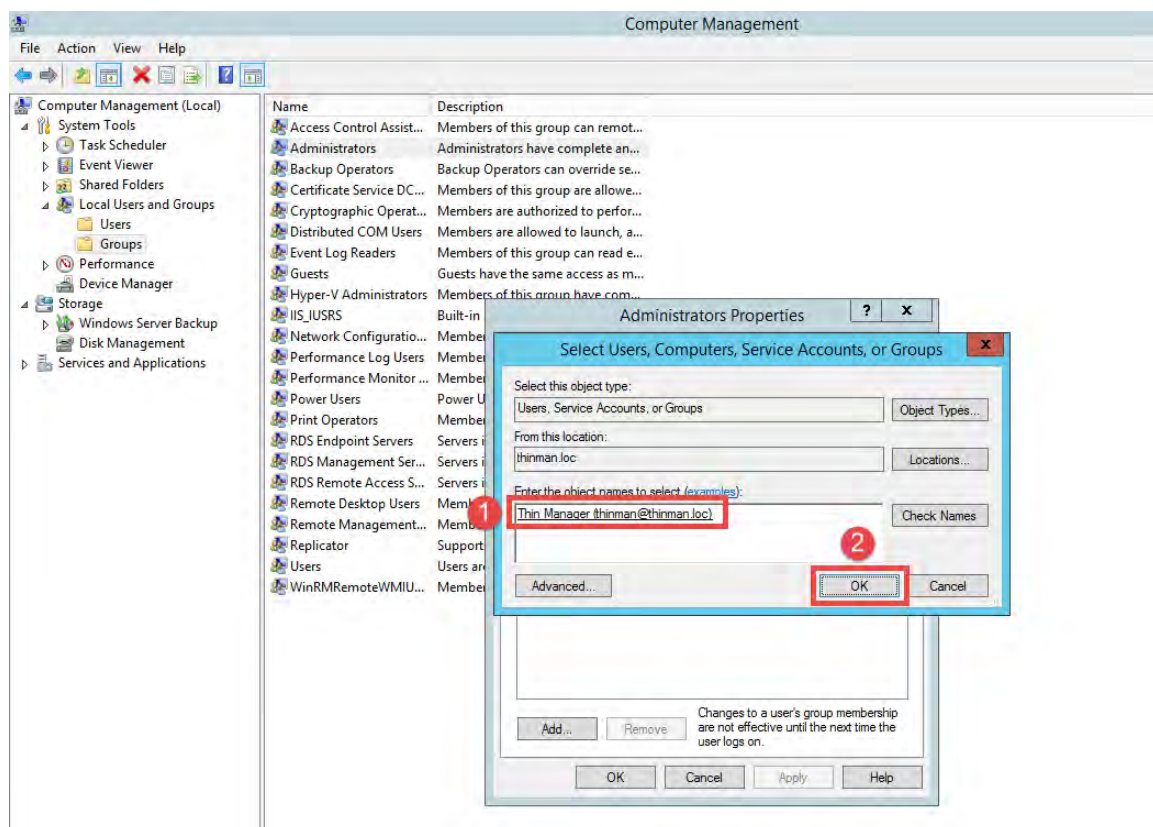
15. From the **Administrators Properties** popup, click the **Add...** button.



16. Enter the new fully qualified domain account created in the previous steps here. In the case of this Configuration Guide, *thinman@thinman.loc*. To verify the name, click the Check Names button. You can also browse for the user. To do so, make sure the Domain name is selected as the *From this location:*, click the *Advanced* button followed by the *Find Now* button.
17. Click the *OK* button.
18. Click the *OK* button on the **Administrators Properties** popup as well.
19. Close the **Computer Management** window.

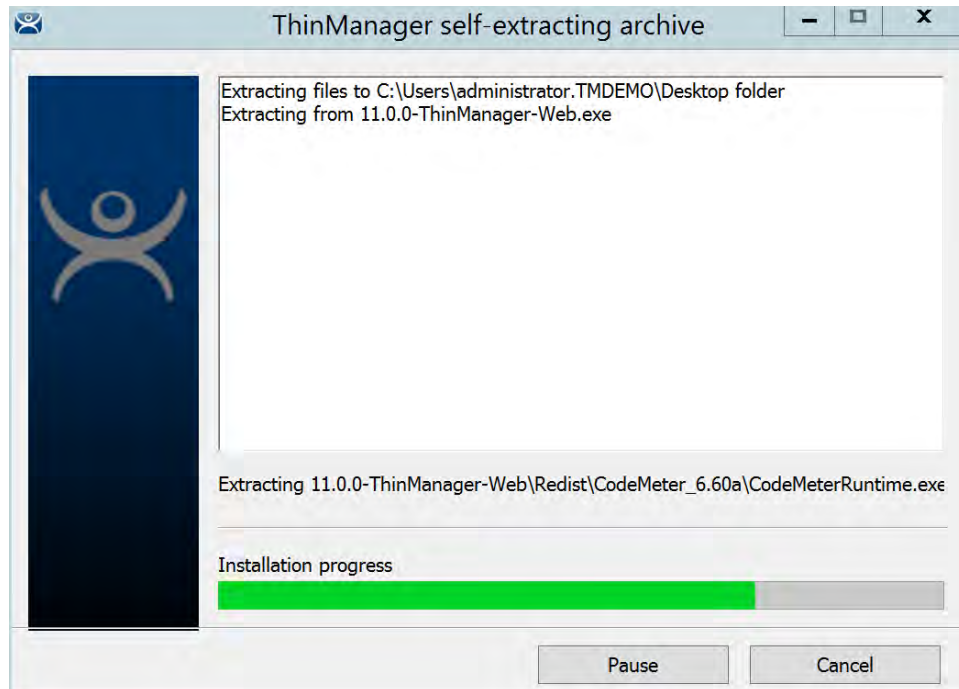
Note: You will want to add this new domain account as a local Administrator to each machine on which you have installed ThinManager (RDS2 in this Configuration Guide).

Note: It is not required to run the ThinServer service as an admin, but some functionality such as the ability to manage and reset sessions from within the ThinManager UI will be unavailable if the user running the ThinServer service is set to a non-admin or Local System type accounts.

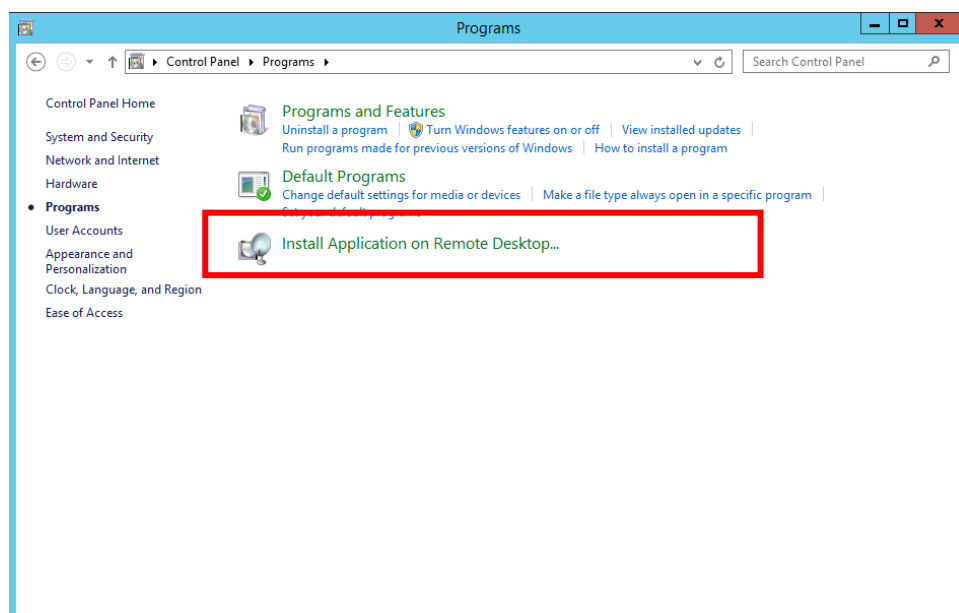


Software Installation

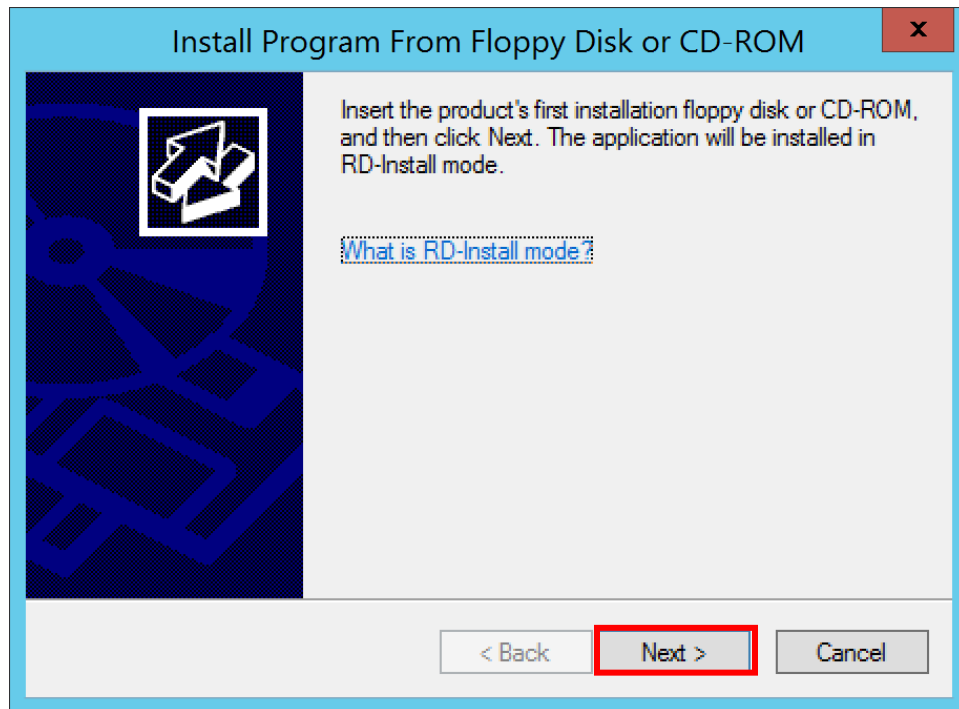
1. If the software package for ThinManager was downloaded from the web, it is possible the download will need to be extracted into the **11.0.0-ThinManager-DVD** before installation. Double-click the executable to initiate the extraction process.



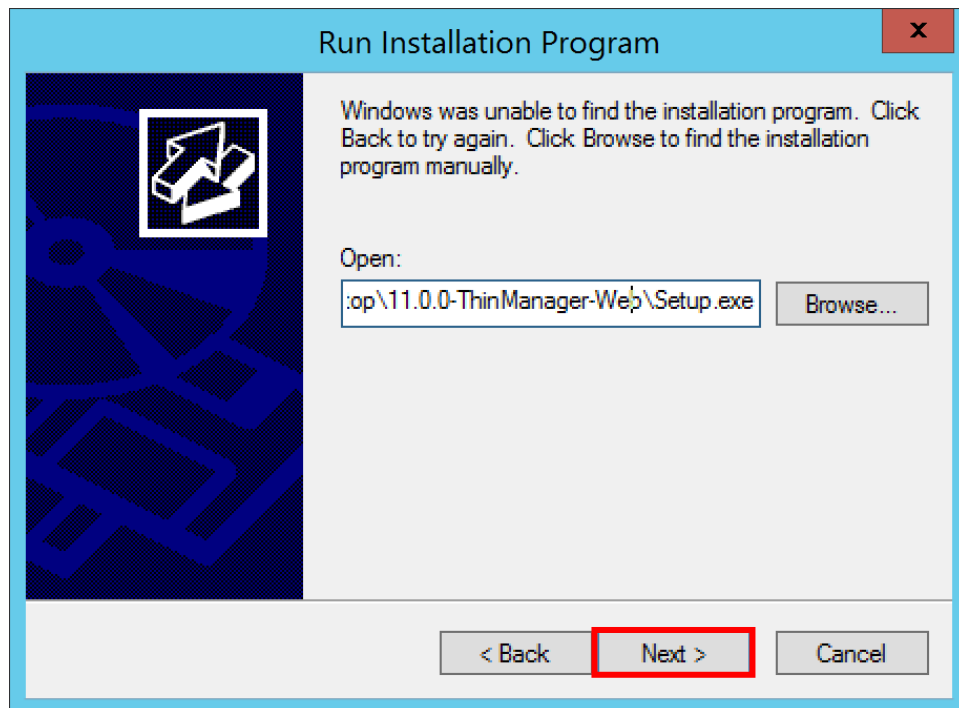
2. Launch the Control Panel from the Windows start menu and search for **install** to locate the *Install Application on Remote Desktop Server* program. This can also be found in Control Panel->Programs.



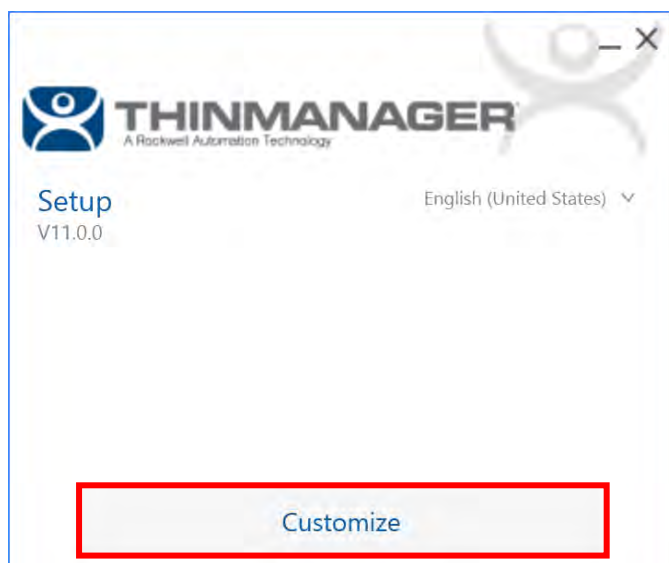
3. Click *Next* to proceed with the installation.



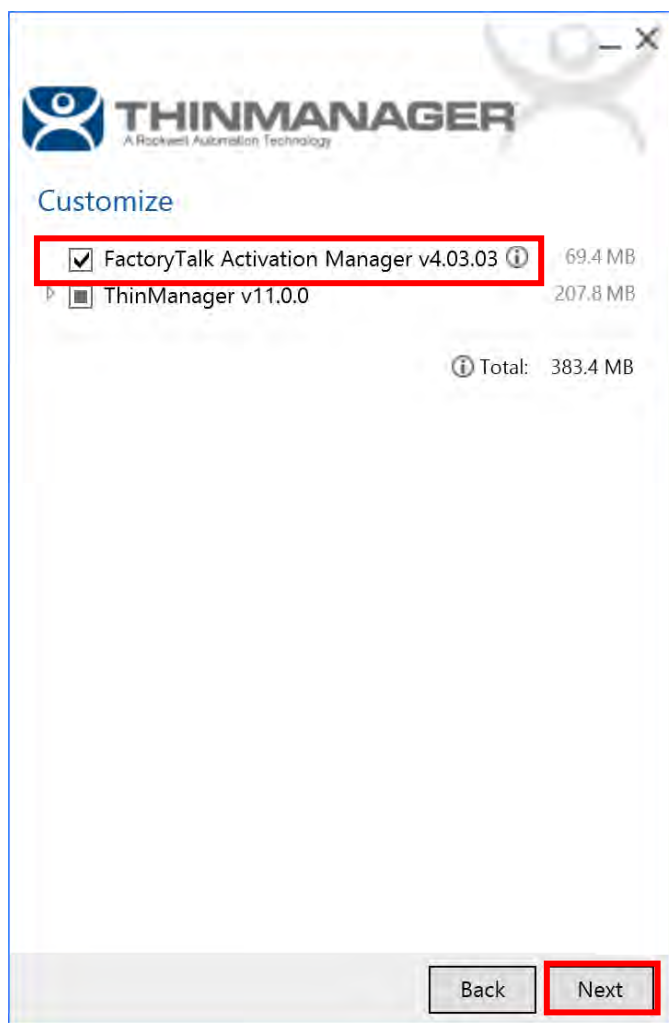
4. Browse to the extracted installation folder and select the **Setup.exe** file.



5. The Rockwell Automation common installer will now launch. Select the *Customize* option.




6. Select the checkbox next to *FactoryTalk Activation Manager*. Click *Next*.



7. Click *Accept All* to accept the EULA and continue to the install process.

and Documentation that Rockwell Automation licenses to You. ROCKWELL AUTOMATION IS WILLING TO LICENSE THE SOFTWARE AND DOCUMENTATION TO YOU ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS AND CONDITIONS IN THIS EULA. YOU ACCEPT AND AGREE TO BE BOUND BY THE TERMS OF THIS EULA BY DOWNLOADING, INSTALLING, COPYING, OR OTHERWISE USING THE SOFTWARE. IF YOU ARE ACCEPTING THESE TERMS ON BEHALF OF ANOTHER PERSON, COMPANY, OR OTHER LEGAL ENTITY, YOU REPRESENT AND WARRANT THAT YOU HAVE FULL AUTHORITY TO BIND THAT PERSON, COMPANY, OR LEGAL ENTITY TO THESE TERMS. IF YOU DO NOT AGREE TO THESE TERMS, DO NOT DOWNLOAD, INSTALL, COPY, ACCESS,

8. Specify the user that ThinServer should run as. This will be the account that was created in the previous section of this guide. In our example, the user was **tmlab\thinman**.

 **THINMANAGER**
A Rockwell Automation Technology

ThinServer Service Account

Specify the account that the ThinServer service should run as.

For example:
 .\LocalUser
 Domain\DomainUser
 DomainUser@Domain.com

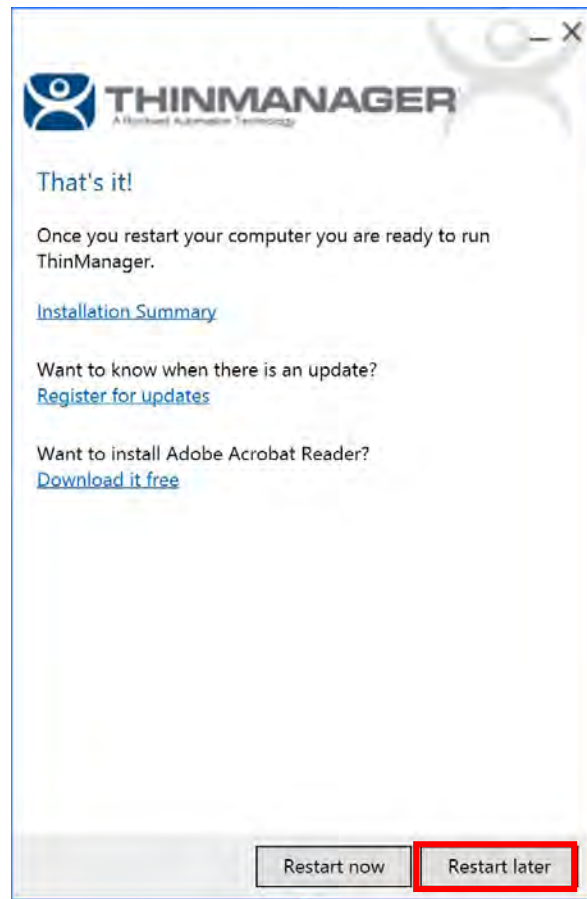
☐ Local System account

☒ This account:

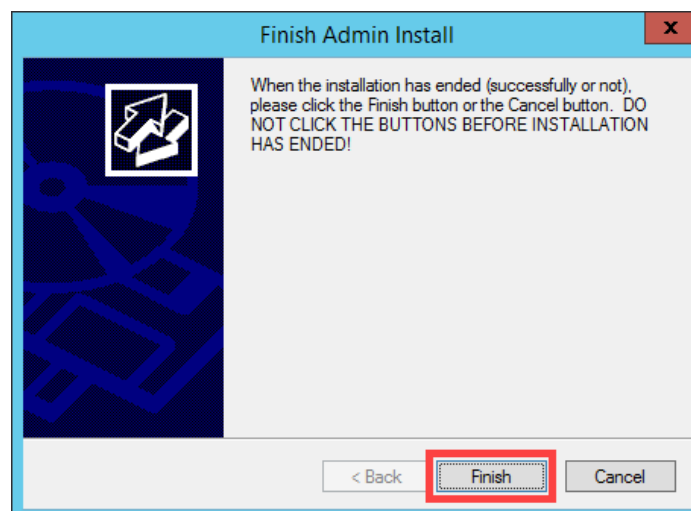
Password:

Confirm Password:

9. Click *Restart Later*.



10. Click *Finish* on the admin install tool.



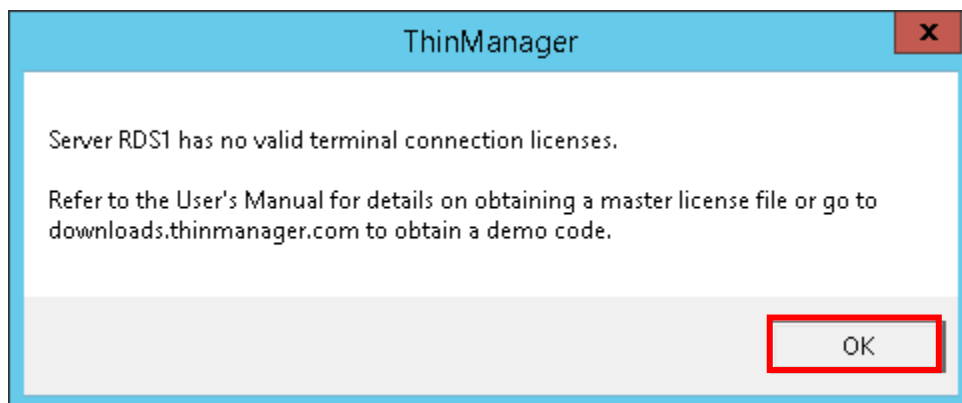
11. Restart the server to complete the installation of ThinManager.

FactoryTalk Activation

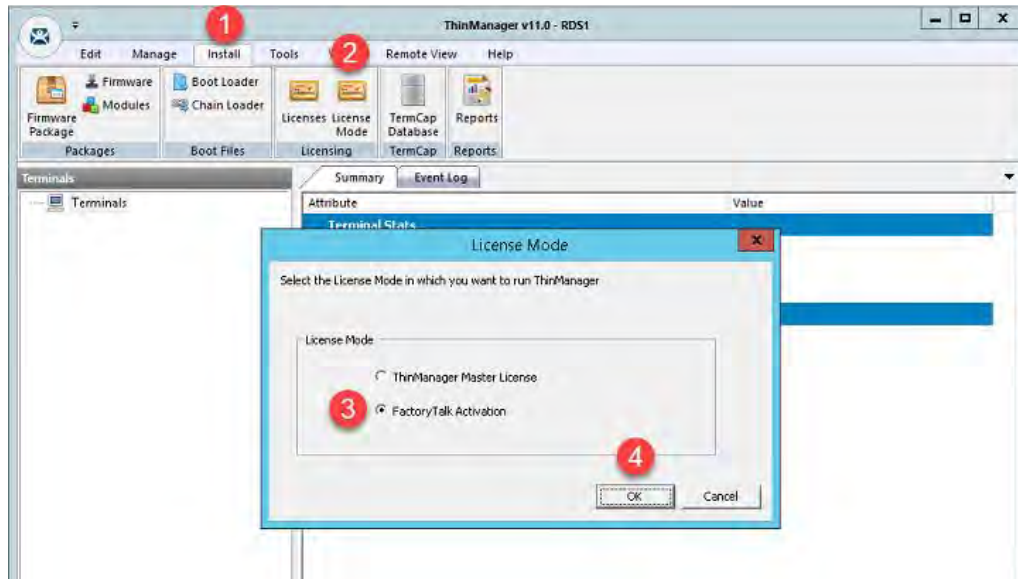
ThinManager 11.0 supports both the legacy ThinManager Master License and FactoryTalk Activation methods of licensing the ThinManager application. ThinManager utilizes CodeMeter FactoryTalk Activations and requires FactoryTalk Activation Manager 4.03.03 or later. This guide will demonstrate how to use FactoryTalk Activations with ThinManager. If you are unfamiliar with the process of downloading an activation using the product key and serial number, please visit reference [1083531-How To Use FactoryTalk Activation with ThinManager](#).

After adding the activations for ThinManager into FactoryTalk Activation Manager, the following steps can be used to activate ThinManager. Now that the FactoryTalk Activation Manager that is installed on your ThinManager machine has a valid ThinManager activation, you can assign it to your ThinManager installation. To do so, open the ThinManager Admin Console.

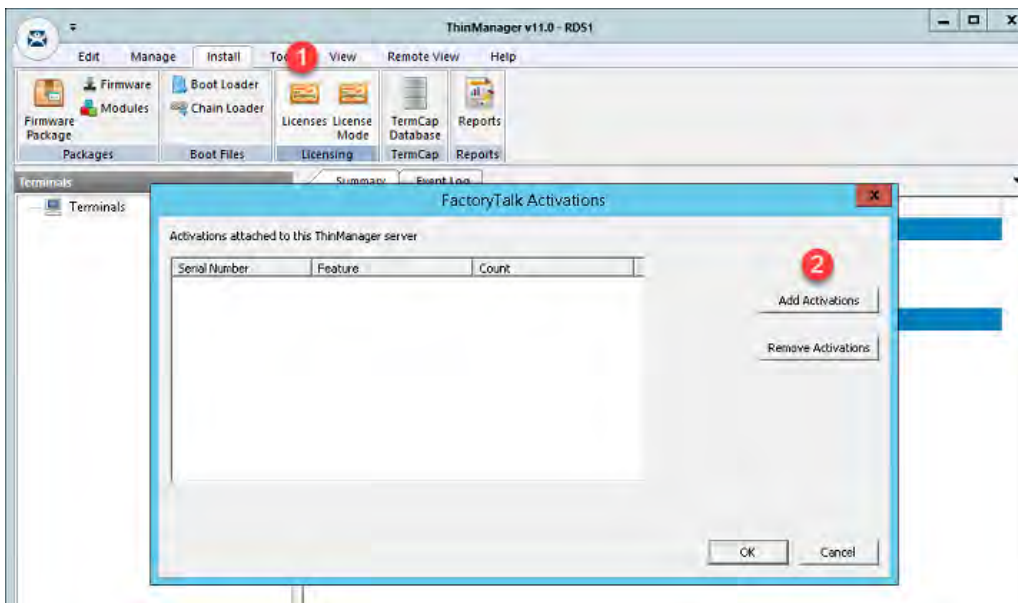
1. Upon first opening the Admin Console, you will be prompted with a message box indicating there are no valid terminal connection licenses. Click the *OK* button.



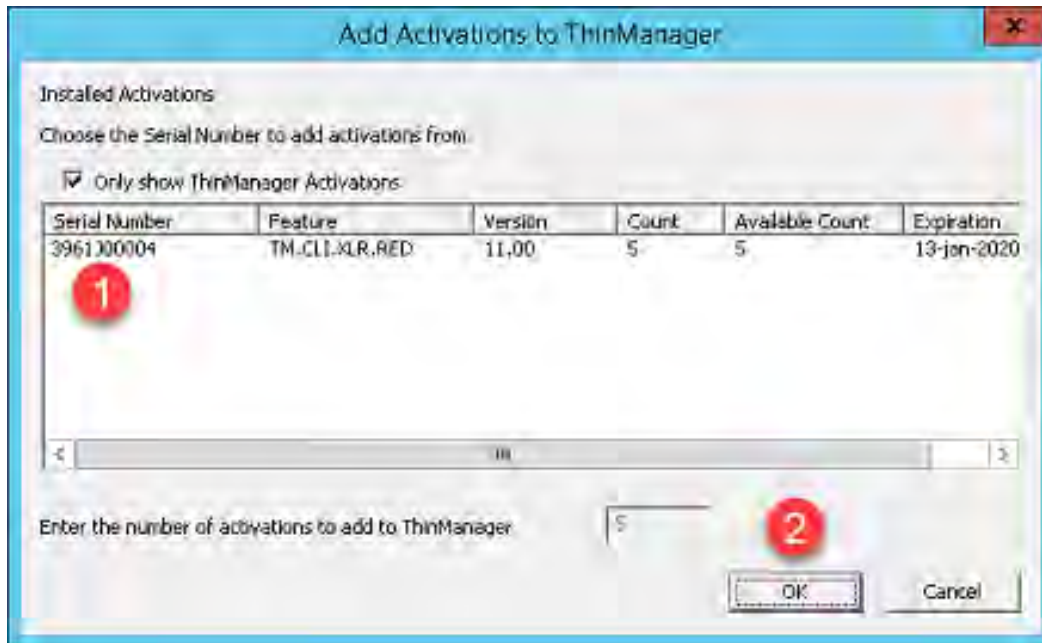
2. From the Admin Console, click the *Install* ribbon, followed by the *License Mode* icon. From the License Mode window, select the *FactoryTalk Activation* option button and click the *OK* button.
Note: ThinManager will only support one License Mode at a time – either **ThinManager Master Licensing** or **FactoryTalk Activation**. You cannot use both simultaneously.



3. With the License Mode changed to FactoryTalk Activation, now click the *Licenses* icon in the Install ribbon. From the ensuing FactoryTalk Activations window, click the *Add Activations* button.



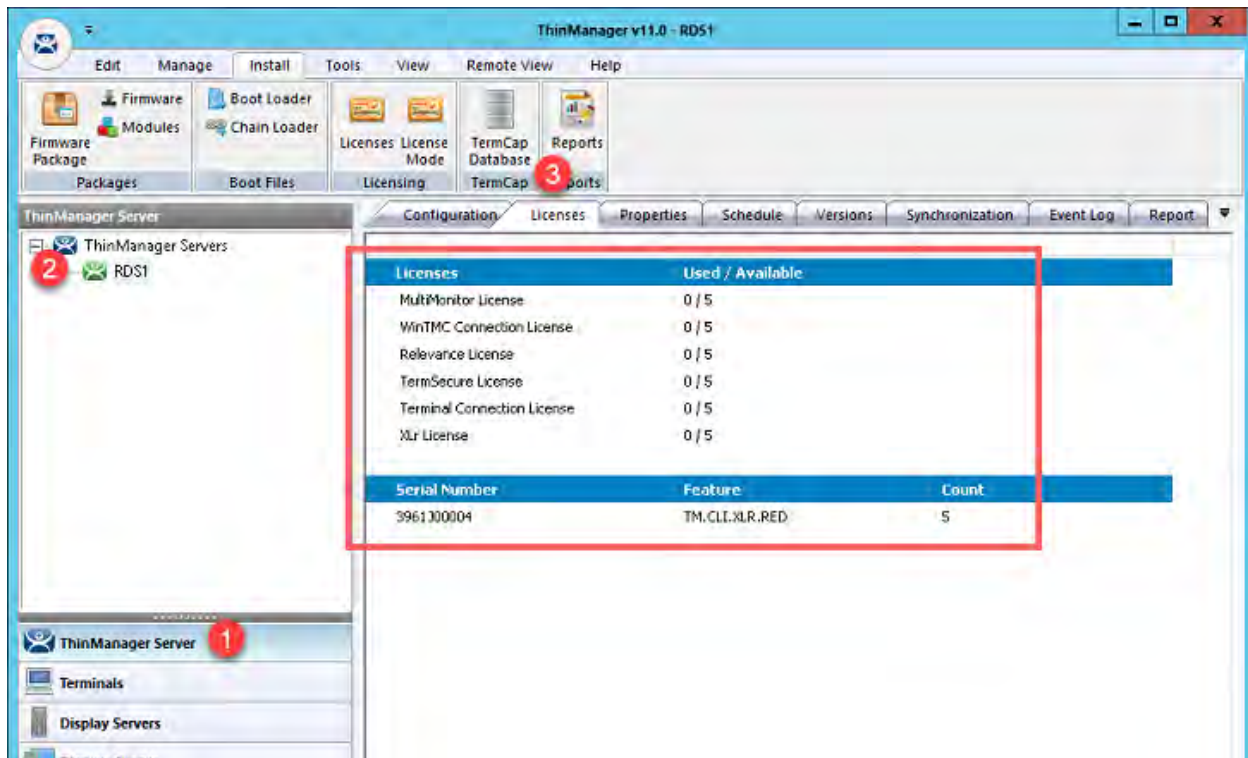
4. From the Add Activations to ThinManager window, select the Serial Number you would like to assign to this installation of ThinManager and click the *OK* button.



5. The assigned Serial Number should now be displayed in the FactoryTalk Activations window. Click the *OK* button.



To validate the license has been properly recognized by ThinManager, click the ThinManager Server button bar. From the ThinManager Server tree, select your ThinManager Server (RDS1 in the example provided). Click the Licenses tab. You should see your license's details listed.



Unlike ThinManager Master Licensing, if you are using ThinManager Redundancy with FactoryTalk Activation, you will need to separately activate the Primary ThinManager Server and the Secondary ThinManager Server. With traditional ThinManager Master Licensing, a single license is automatically shared between the Primary ThinManager Server and the Secondary ThinManager Server. If you have purchased a FactoryTalk Activated Redundant ThinManager license, you will receive a single serial number and product key pair that can be activated 2 times – once for the Primary ThinManager Server and once for the Secondary ThinManager Server.

Note: The ThinServer.exe service should be set to Delayed Start from the Services tool in Windows if using ThinManager 11.0 to prevent a false error stating no licenses are available. This has been addressed in the released Service Pack 1 for ThinManager 11.0.

If a GoldMaster license is to be used to activate ThinManager, please reference the RAID below

https://rockwellautomation.custhelp.com/app/answers/detail/a_id/1083532

FactoryTalk View SE Client Licenses

FactoryTalk View SE requires client licenses for each thin client that will run an instance of the `DisplayClient.exe` application. In version 11.0 of ThinManager and FT View SE, integration between the product allows for as many View SE clients as desired to be launched on a single thin client, regardless of the number of monitors, to consume a single FactoryTalk View SE license. Previous versions of the software packages would require a client license for each instance of FT View SE running. For information on the commercially advantageous licensing model system requirements, please visit [1083982 - ThinManager and FTView SE Client Licensing](#).

Redundancy

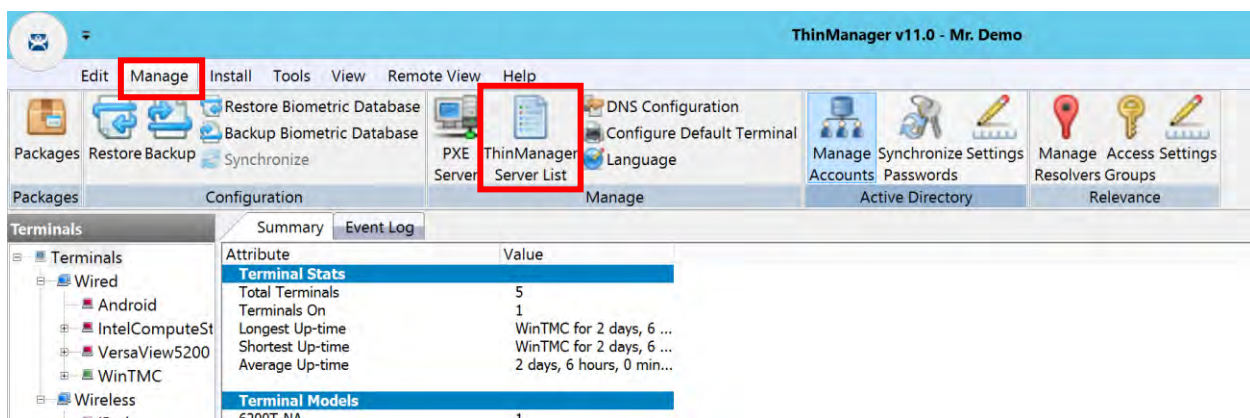
If the system is to be configured using redundancy (synchronized installations of the ThinManager server), the steps performed to install ThinManager on the primary server in the previous section should be repeated on what will be the secondary or redundant ThinManager server.

If failover will be configured in the deployment, Remote Desktop Services should be installed on the failover server. This can be done repeating the steps for the install and configure Remote Desktop Services sections.

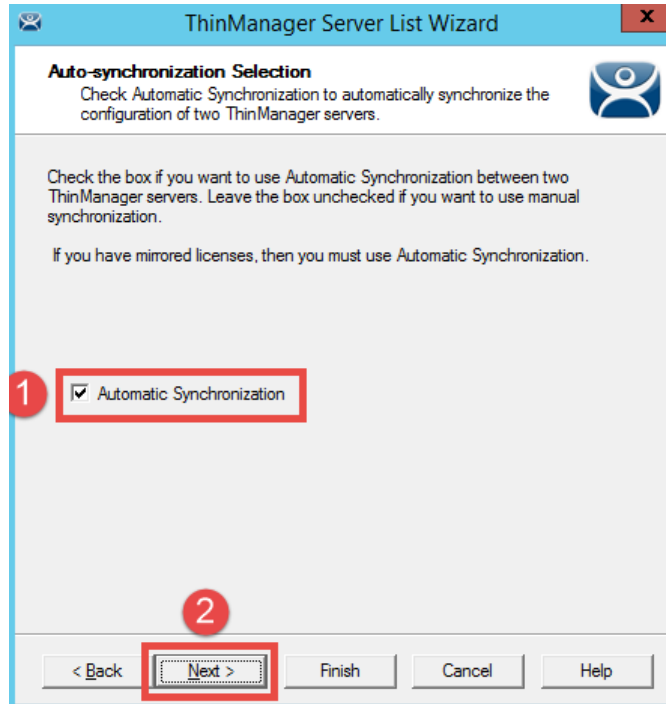
For reference architectures and other architecture notes and best practices, more information can be found by visiting [1076143 – ThinManager Architecture Review FAQ](#).

Synchronization

1. Still from **RDS1**, click the *Manage* ribbon, followed the *ThinManager Server List* icon.
2. From the Introduction page of the ThinManager Server List Wizard, click the *Next* button.



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



ThinManager Server List Wizard

Auto-synchronization Selection
Check Automatic Synchronization to automatically synchronize the configuration of two ThinManager servers.

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.

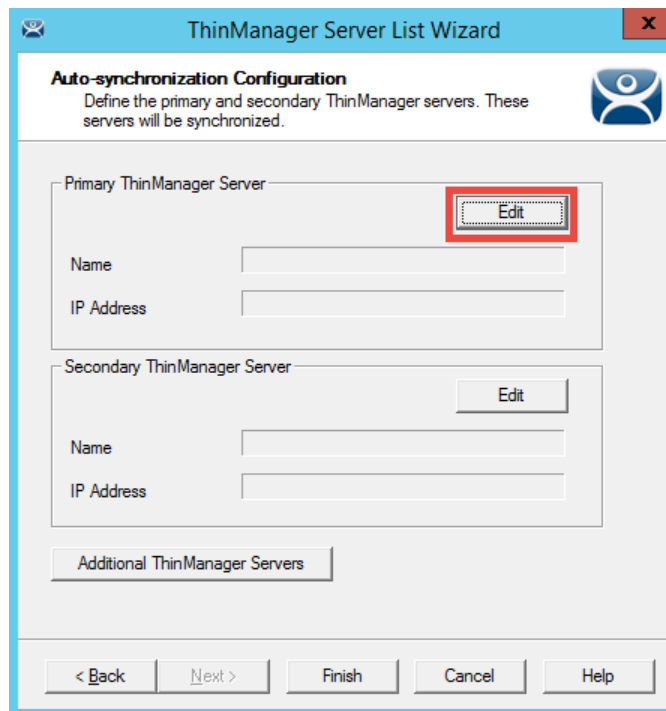
If you have mirrored licenses, then you must use Automatic Synchronization.

1 ☒ Automatic Synchronization

2

< Back Finish Cancel Help

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



ThinManager Server List Wizard

Auto-synchronization Configuration
Define the primary and secondary ThinManager servers. These servers will be synchronized.

Primary ThinManager Server

Name

IP Address

Secondary ThinManager Server


Name

IP Address

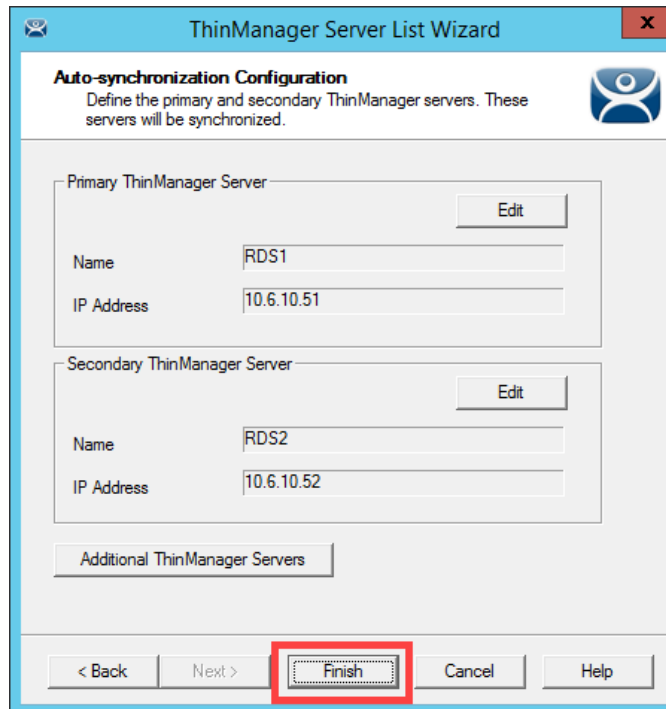
Additional ThinManager Servers

< Back Finish Cancel Help

5. Enter the Primary *ThinManager* Server name (**RDS1** in this Configuration Guide) and click the *Discover* button. The associated IP address should be displayed.
Note: In a workgroup deployment, the IP address may need to be manually entered.
6. Click the *OK* button.

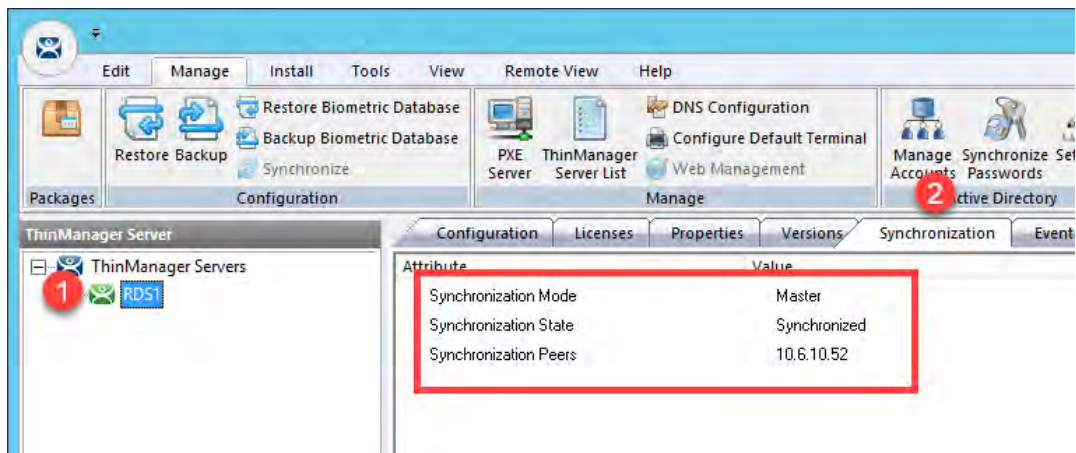


7. Repeat the previous 3 steps for the Secondary *ThinManager* Server (**RDS2** in this Configuration Guide).
8. The wizard should now show valid Primary and Secondary *ThinManager* Servers with correct IP addresses for each.
9. Click the *Finish* button.



10. To confirm synchronization, click the *ThinManager* icon in the button bar.
11. Select **RDS1** from the *ThinManager Servers* tree.
12. Click the *Synchronization* tab. You should see a *Synchronization State* of *Synchronized* (may take a minute or so to update).

Note: The master and slave designation is not specified in the ThinManager server and is assigned based on the order in which the ThinServer.exe services are started.



ThinManager Configuration

In this section general configuration will be created to deliver a FactoryTalk View SE client to the thin client. Multiple View SE clients will be used to demonstrate Multimonitor and Multisession functionalities.

Display Servers are the locations of the network assets such as the Remote Desktop Hosts that will serve as the source of content in our deployment.

Display Clients are the specific applications, camera views, or other specific application that we would like visualized on a device.

Terminals are the configuration of which display clients we would like and the associated hardware with the created terminal profile.

Display Servers

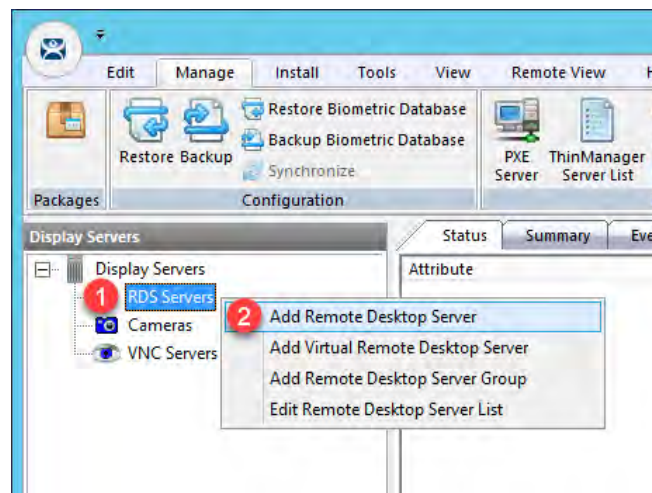
1. Launch the ThinManager user interface from the Windows start menu.

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

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



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

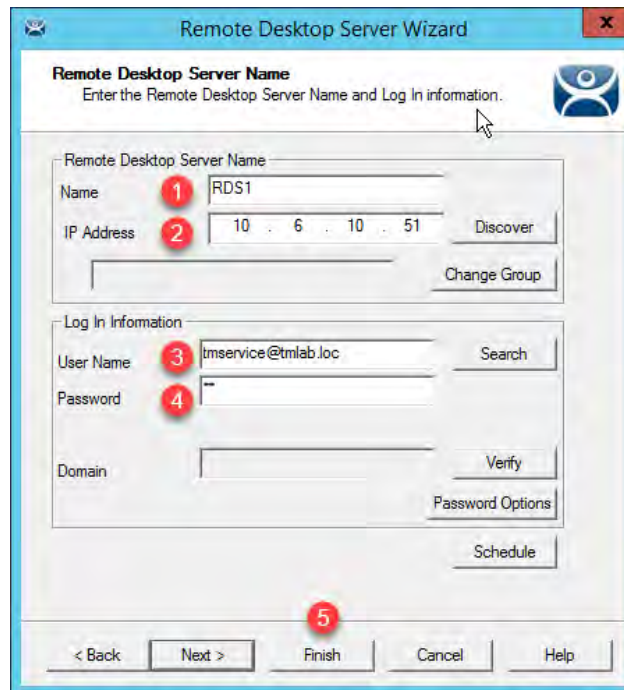


4. From the *Introduction* page of the Remote Desktop Server Wizard, click the *Next* button.
5. From the *Remote Desktop Server Name* page of the wizard, type *RDS1* in the Name field.

6. Click the *Discover* button. If the name is successfully resolved, the IP address of **RDS1** should be filled in automatically.
7. Type the qualified domain name of a user that is a local administrator in the *User Name* field, followed by the password.

Note: If a user name is not entered for the *Display Server*, ThinManager will still be able to deliver remote sessions to the terminals, however, some functionality will be lost from the ThinManager UI, such as the ability to manage and reset sessions on the localhost from within the ThinManager UI. Tools such as *Task Manager* or *Server Manager* must be used instead.

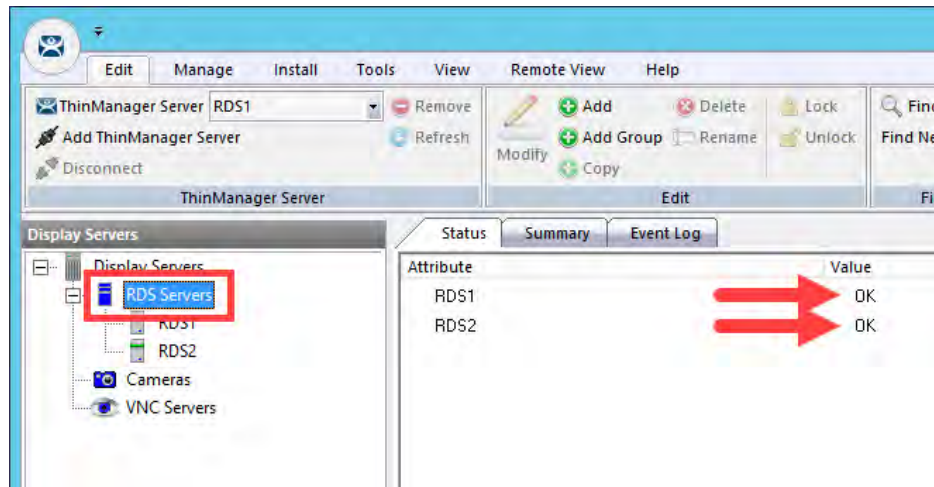
8. Click the *Verify* button which should confirm that the credentials entered are valid, followed by the *OK* button.
9. Click the *Finish* button.




10. **RDS1** should now be added to the Remote Desktop Servers group. You may have to click the Display Servers branch to refresh the Remote Desktop Servers group.
11. Repeat steps 3 through 10, but this time register any other Remote Desktop Servers that will be used as the source of content in the system.

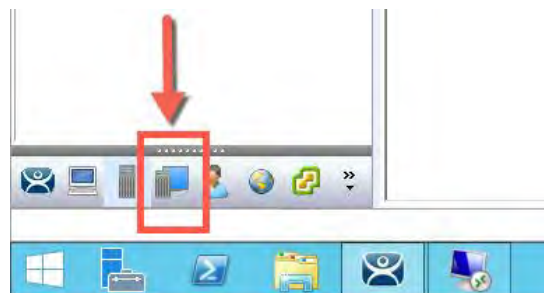
Note: Failover requires as least two Remote Desktop Servers be added to the deployment.

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

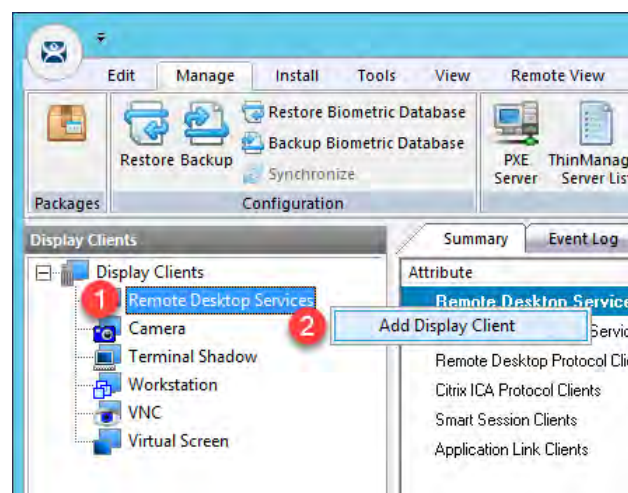


Display Clients

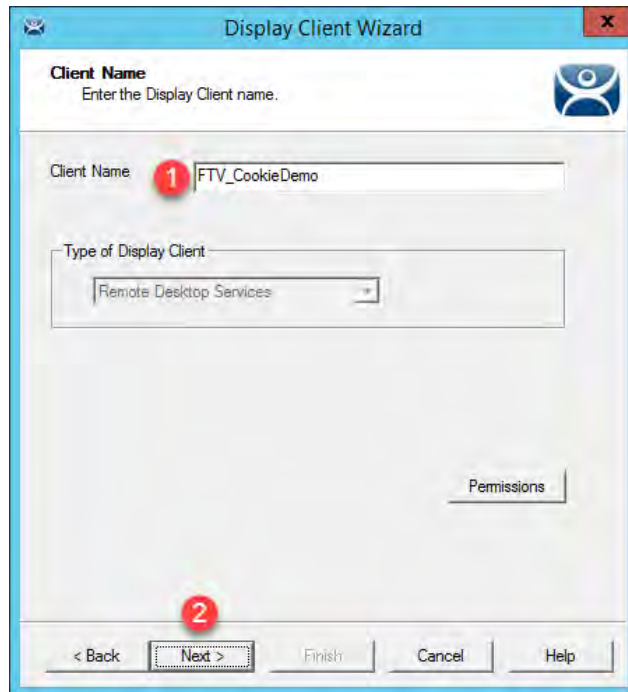
1. Click the *Display Clients*  icon from the ThinManager tree selector.



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

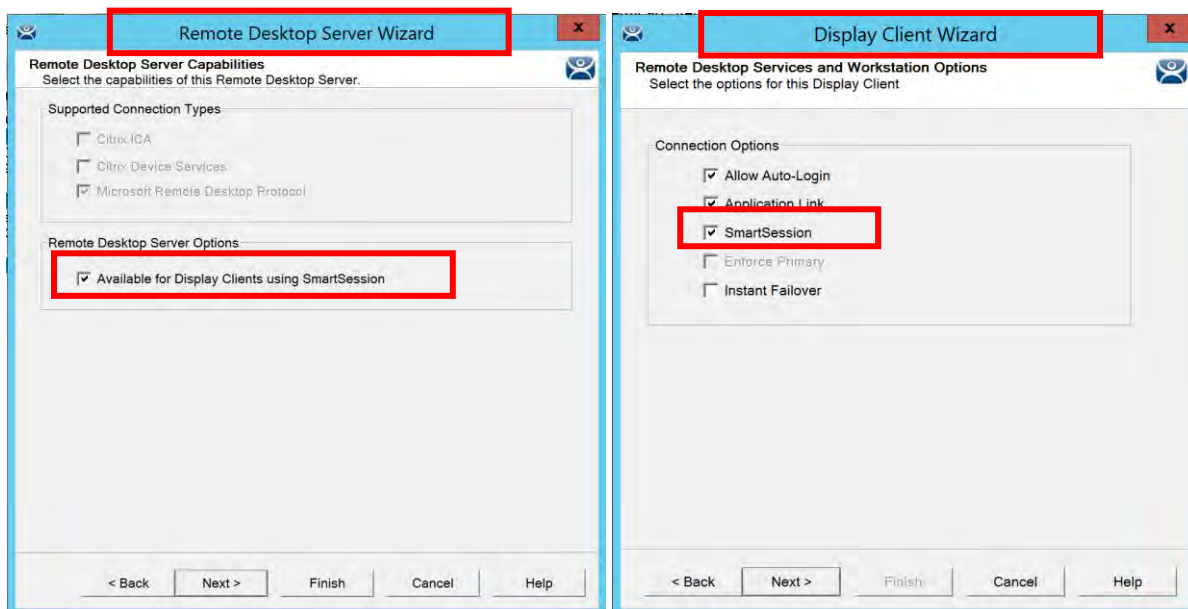


3. Type `FTV_CookieDemo` as the Client Name on the Client Name page of the wizard. Click the *Next* button.

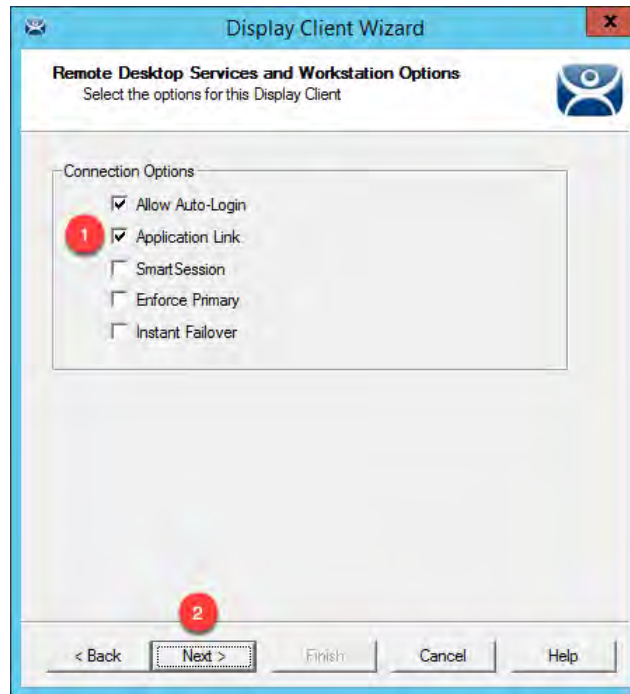


Smart Session

Smart Session is a feature of ThinManager that enables the product to 'load balance' the applications across the available Remote Desktop Servers. Smart session is not needed if load balancing is already configured from within the Microsoft environment. Ensure the following settings are made if this feature is desired:



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

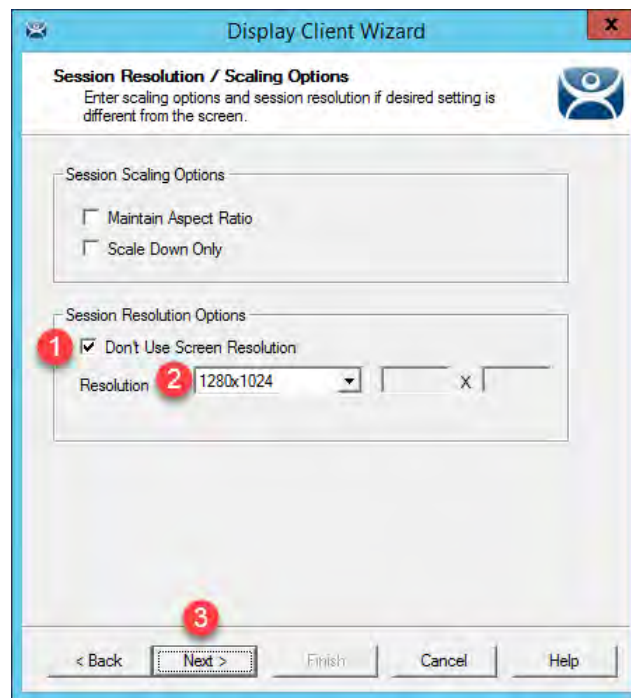


Session Scaling

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

This is especially useful when an application is to be delivered to a monitor which has a different resolution than what the HMI application was developed for.

6. From the *Screen Resolution / Scaling Options* page of the wizard, check the box for *Don't Use Screen Resolution*, and select the screen resolution of the monitor you will be driving content to from the Resolution drop down list. Click the *Next* button.



Failover

Failover is a function of ThinManager that is included with both standard and redundant ThinManager deployments.

Failover: Failover is the ability to switch between multiple terminal servers if a terminal server fails. This is built in to every ThinManager System and thin client. This is covered in Failover.

Instant Failover: Instant Failover is the ability of thin clients to connect and login to two terminal servers simultaneously. This allows applications to be pre-loaded so that a failure to one terminal server causes minimal impact because the terminal will quickly switch to an existing session. This is covered in Instant Failover.

Failover requires the client application to be installed and published as a Remote App on both servers that are added to the display client. A copy of the client file should be located in an identical location on both Remote Desktop Servers. In a workgroup environment, the same local user that will be used for the terminal is required to be created on both of the Remote Desktop Servers. To configure failover, more than one Remote Desktop Server are added on the **Display Client Members** page of the **Display Client Wizard** in the next step.

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



8. From the AppLink page of the wizard, enter the following path for the Program Path and Filename field and Command Line Options field.

Note: Please be sure to include quotations around application file names and paths, especially those that include spaces such as *RSView[space]Enterprise*.

Examples of these settings are found below:

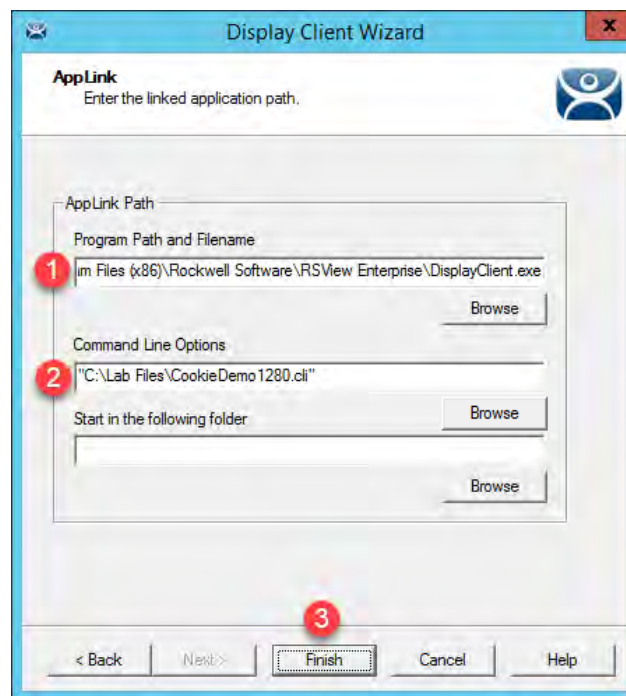
Program Path and Filename:

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

Command Line Options:

"C:\Lab Files\CookieDemo1280.cli"

9. Click the *Finish* button.



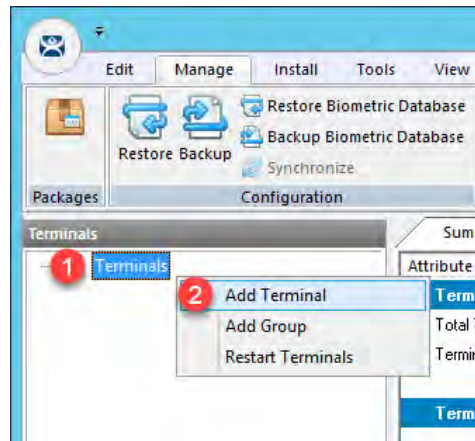
Terminal Configuration

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

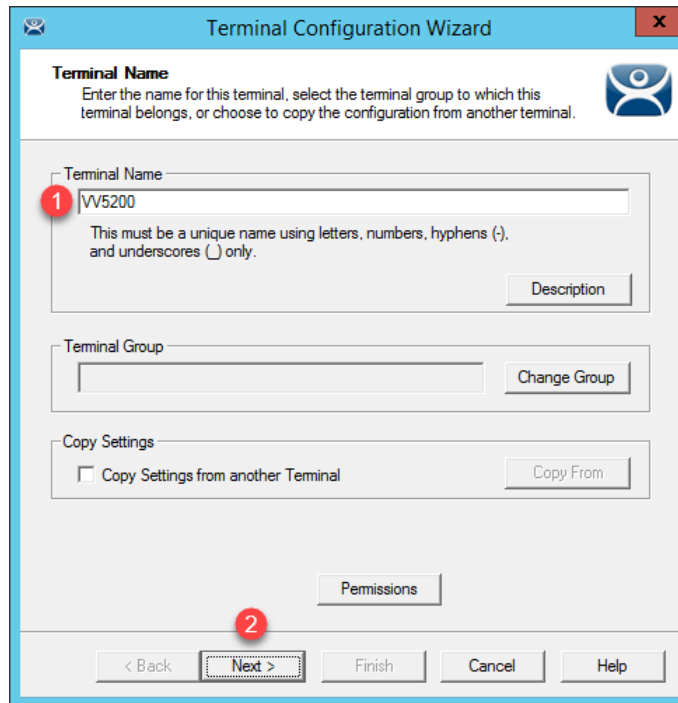
1. Click the *Terminals* icon  from the ThinManager tree selector.



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



3. Type **VV5200** as the Terminal Name on the Terminal Name page of the wizard. Click the *Next* button.



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: **VV5200**
This must be a unique name using letters, numbers, hyphens (-), and underscores (_) only.

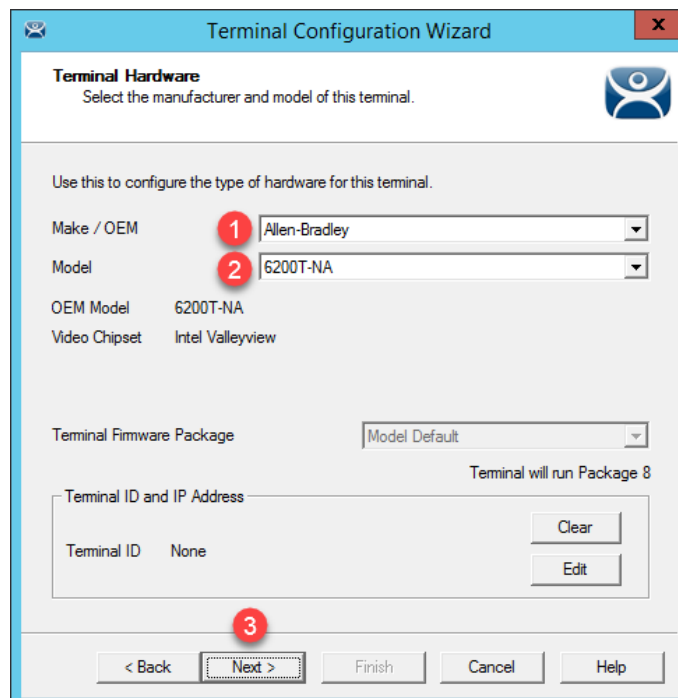
Terminal Group:
Change Group

Copy Settings
☐ Copy Settings from another Terminal
Copy From

Permissions

< Back **Next >** Finish Cancel Help

4. Select **Allen-Bradley** from the Make/OEM drop down list and **6200T-BA** from the Model drop down list. Click the *Next* button. 6200T-NA is the catalog number for the VersaView 5200 box thin client utilized.



Terminal Hardware
Select the manufacturer and model of this terminal.

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

Make / OEM: **Allen-Bradley**

Model: **6200T-NA**

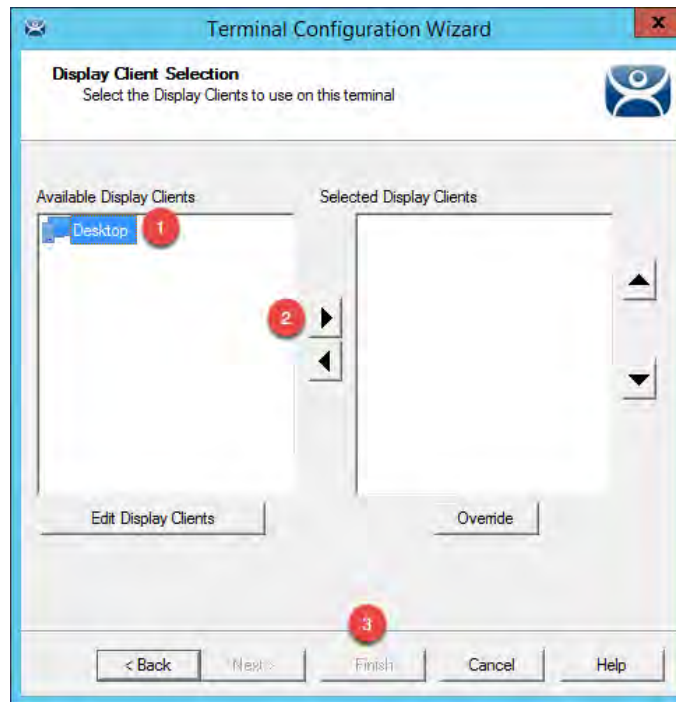
OEM Model: 6200T-NA
Video Chipset: Intel Valleyview

Terminal Firmware Package: Model Default
Terminal will run Package 8

Terminal ID and IP Address
Terminal ID: None
Clear Edit

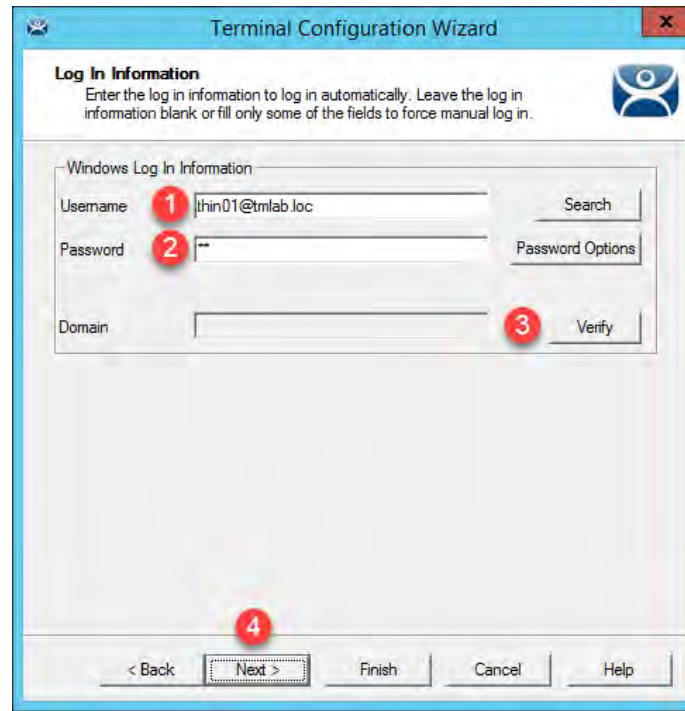
< Back **Next >** Finish Cancel Help

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



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

10. On the *Log In Information* page of the wizard, enter a domain user as the Username and enter the Password. The terminal will use these credentials to login to the Remote Desktop Server for those Display Clients applied to it that have the *Allow Auto Login* property enabled. Click the *Verify* button which should confirm that the credentials entered are valid. Click the *Next* button.



Terminal Configuration Wizard

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

Windows Log In Information

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

Password **2** Password Options

Domain Verify **3**

4

< Back Next > Finish Cancel Help

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



Terminal Configuration Wizard

Video Resolution
Select the video resolution for this terminal.

Select Video Resolution

These are the resolutions supported by the Thin Client model you selected.

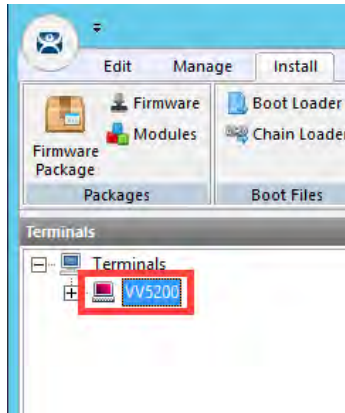
1 Resolution **2** Color Depth **3** Refresh Rate

1920x1080 64K Colors 60Hz

4

< Back Next > Finish Cancel Help

12. Click the *Next* button on the *Module Selection* page of the Terminal Configuration Wizard.
13. Click the *Next* button on the ThinManager Server Monitor List page of the Terminal Configuration Wizard.
14. Click *Finish* from the Monitoring Configuration page of the wizard.
15. You should see the **VV5200** terminal under the *Terminals* node.

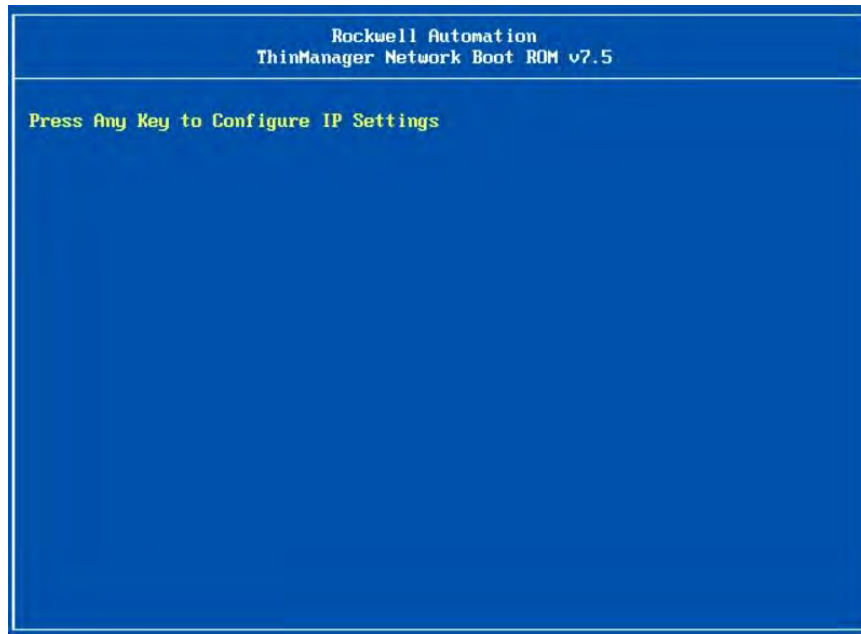


ThinManager Ready Terminals - VersaView 5200

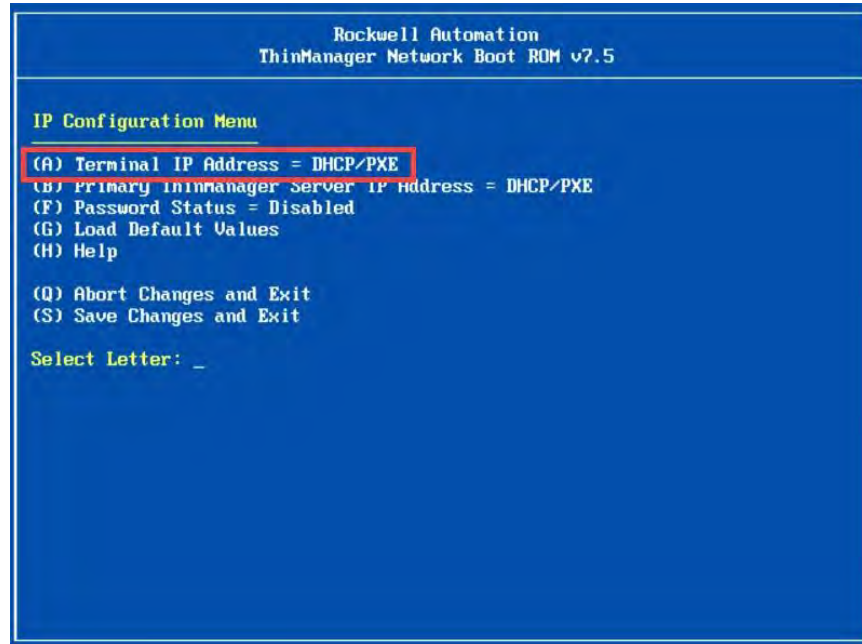
ThinManager ready terminals can support either the traditional TFTP boot or UEFI boot. For the purpose of this document, we will show the configuration and boot process for both boot methods. The single display model (6200T-BA) shown first will show the configuration process for the TFTP boot and the multi 4K models (6200T-RC and 6200T-RE) will be used to highlight the differences when booting via UEFI.

We have already created the terminal profile in the previous section, so the next step will be to assign that terminal profile to a device. This shows the by device delivery method, one of the three possible delivery methods in ThinManager: by device, by user, or by location.

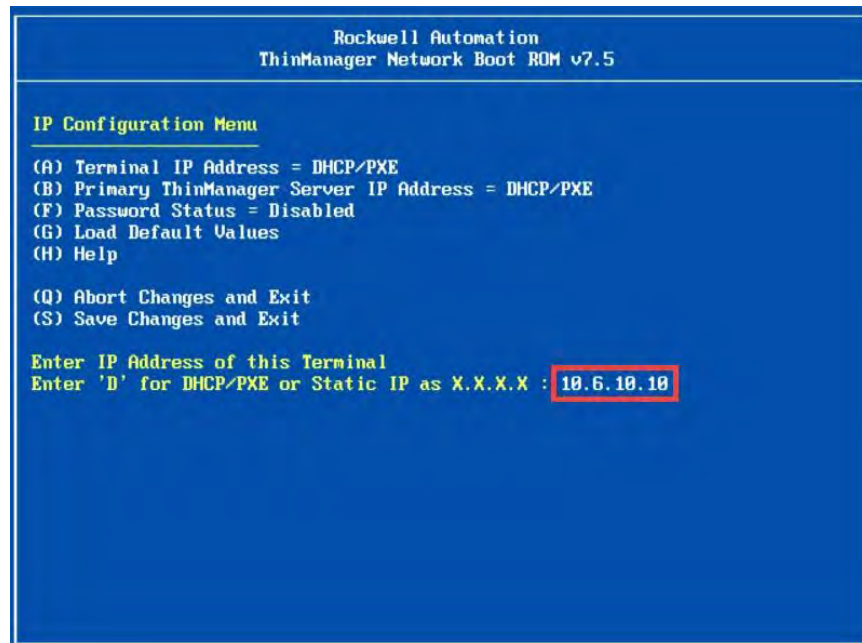
1. Once power is applied, start tapping the spacebar on the keyboard attached to the VersaView 5200 every few seconds to launch the *IP Configuration Menu*.



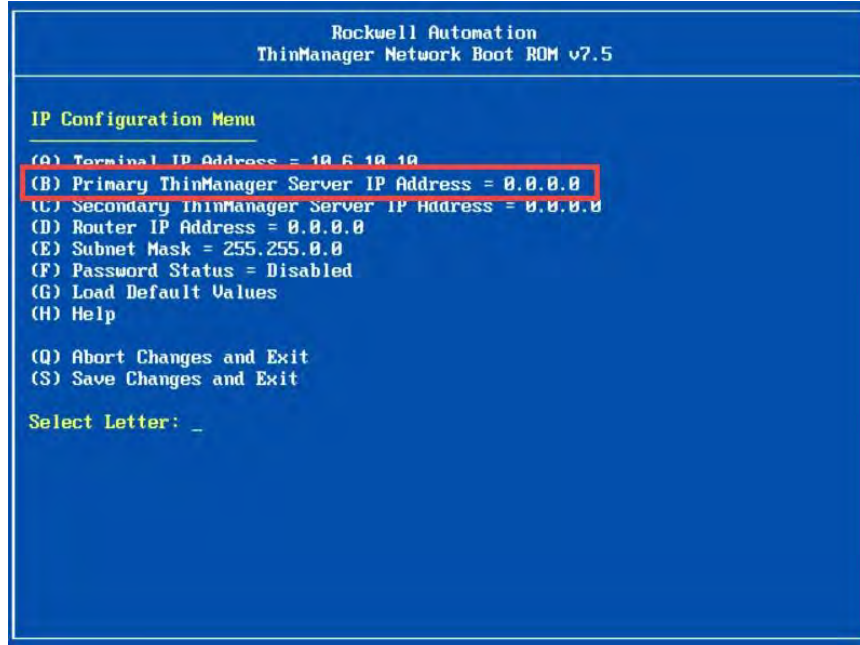
2. We are going to assign a static IP address to the VersaView 5200. From the *IP Configuration Menu*, press the A key on the keyboard attached to the *VersaView 5200*.



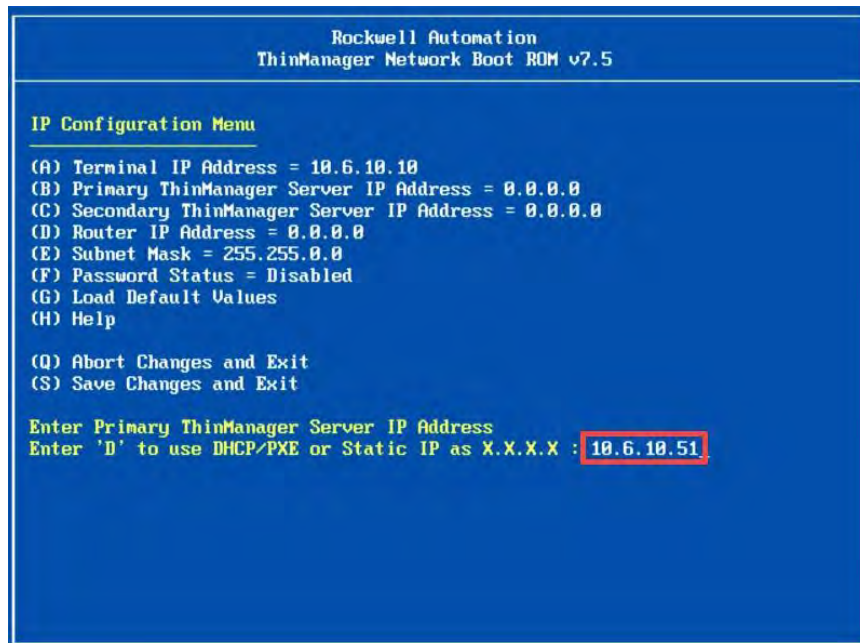
3. Enter an unused IP address in the same subnet as the ThinManager server as the *Terminal IP Address* followed by the *Enter* key to accept the entry.



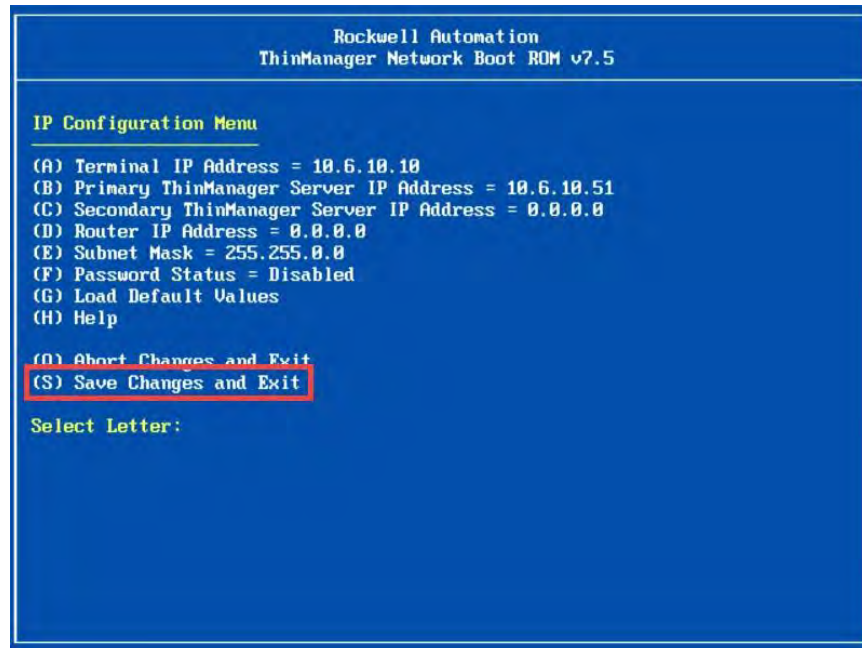
4. Now, we will need to tell the **VersaView 5200** where to find ThinManager. From the *IP Configuration Menu*, press the *B* key on the keyboard attached to the **VersaView 5200**.



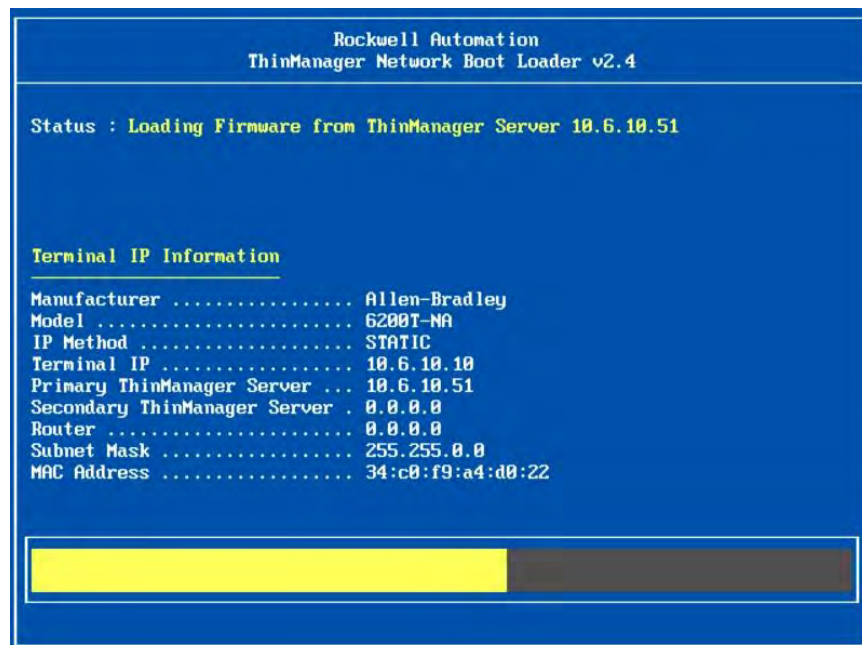
5. Enter the IP address of the ThinManager server as the *Primary ThinManager IP Address* followed by the *Enter* key to accept the entry.



6. We could enter a *Secondary ThinManager Server IP Address* if we had Redundant ThinManager servers present. If we are not using ThinManager Redundancy, hit the S key on the keyboard to Save Changes and Exit.



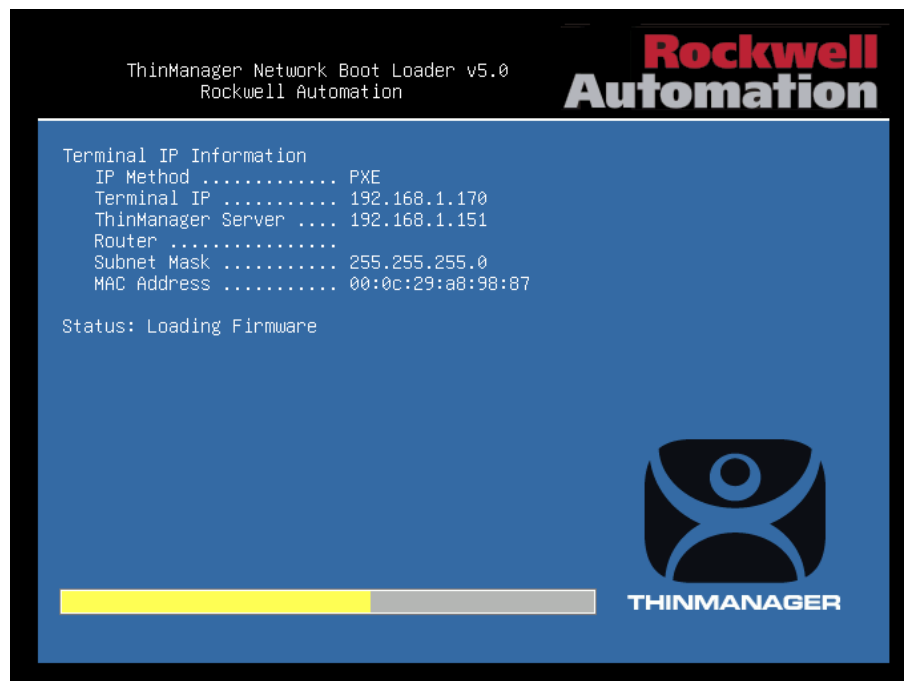
7. The ThinManager firmware, which is the ThinManager Operating System (OS), will be delivered to the **VersaView 5200**. It is approximately 13MB in size, and on today's networks gets delivered almost instantly. When complete, the **VersaView 5200** will have an Operating System and will continue by booting from it.



8. Once the VersaView 5200 has the ThinManager firmware, it will communicate with the ThinManager Server, asking for a *Terminal Profile*. ThinManager identifies terminals by their *MAC address*. Since we have not previously assigned a *Terminal Profile* to the MAC address of this VersaView 5200, ThinManager will ask which profile to assign to it. Hit the *down arrow key* to select the **VV5200** profile we created previously and hit the *Enter key*.



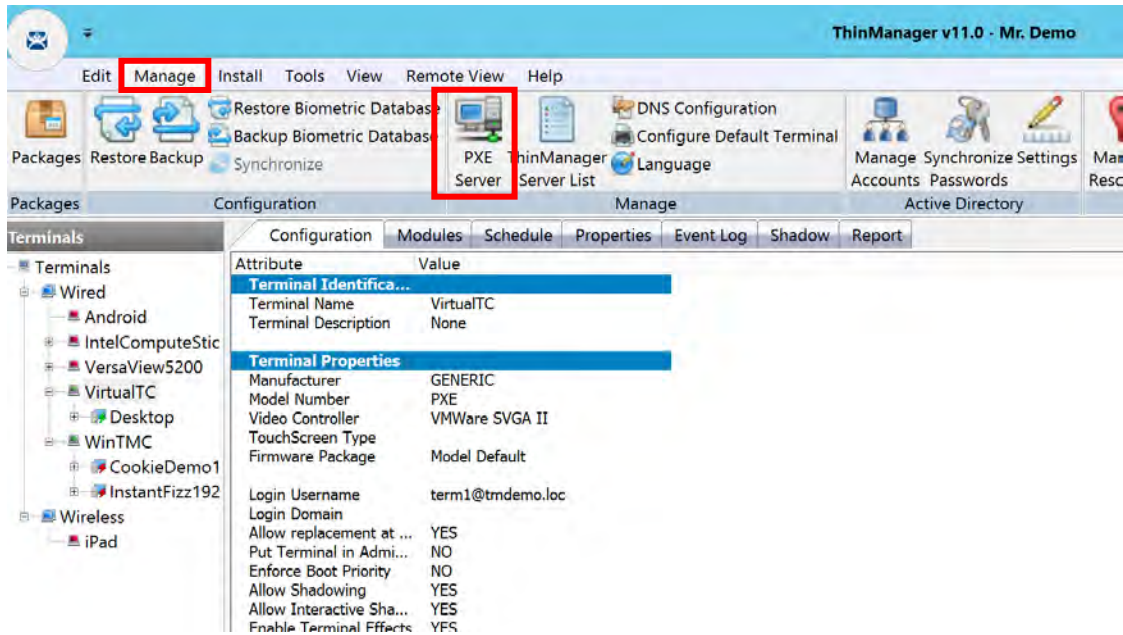
Note: If using a terminal such as the (6200T-RC or 6200T-RE), UEFI will be the boot method if the client cannot communicate via TFTP. Splash screens for devices that support the UEFI boot are slightly different and contain the Rockwell Automation logo as seen below.



ThinManager Compatible Terminals (PXE/UEFI)

In order to utilize ThinManager compatible terminals, we must enable the PXE server on ThinManager and specify the boot options.

1. Select the *PXE Server* icon from the **Manage** tab of the ThinManager application.

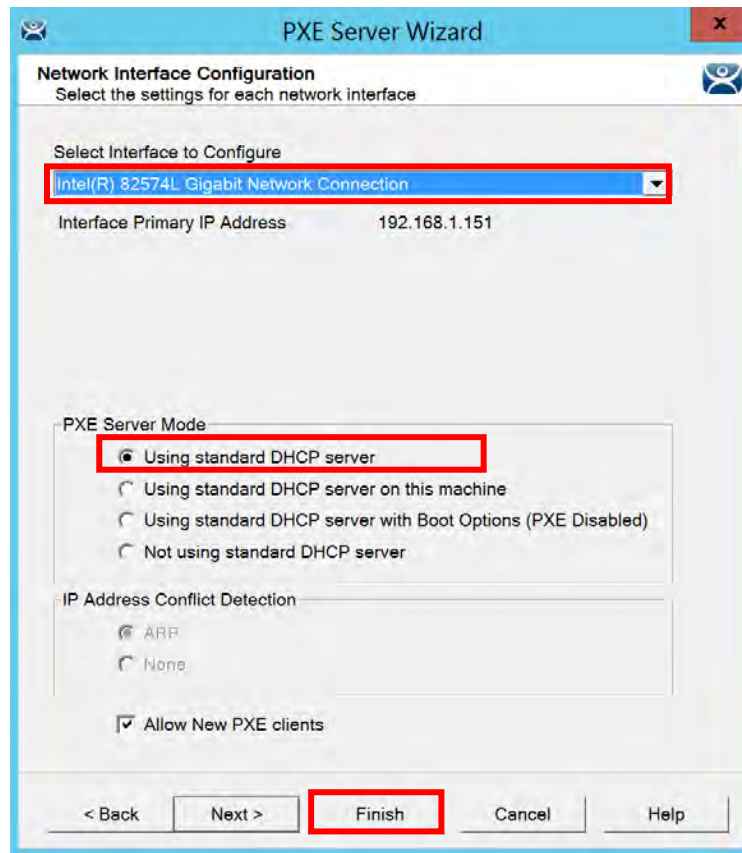


2. Check the checkbox next to the *Enable PXE Server* option. Click *Next*.

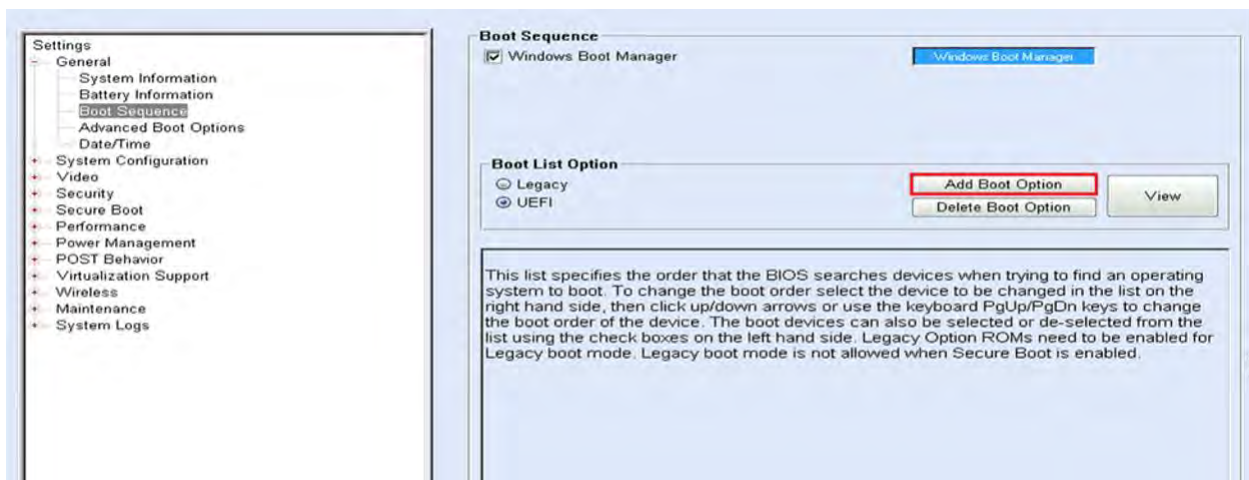


3. Select the network interface from which you would like the PXE server to respond on, and if using a domain with DHCP, select the radio button next to *Using standard DHCP server*. Click *Finish*.

Note: If you are not using a standard DHCP server, or if you have further questions, please visit [1075607 – How do I configure the PXE server in ThinManager?](#)



4. On the end device that is to be PXE booted, enter the bios of the machine. Set the boot order to list either PXE/UEFI (depending on the desired protocol) to be first in the boot order



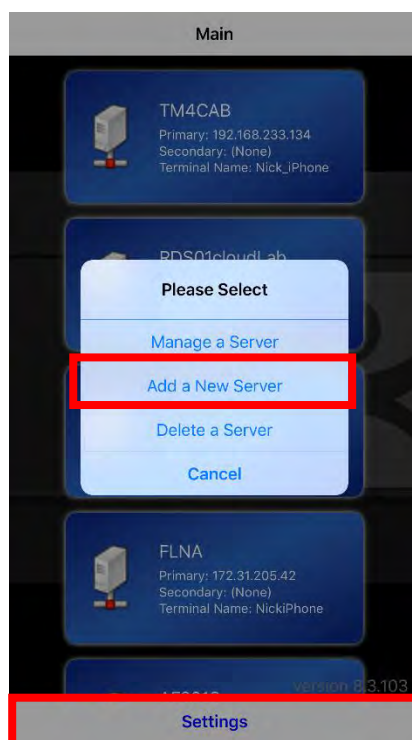
ThinManager Clients (iTMC, aTMC, WinTMC)

ThinManager can manage content delivery to mobile devices running Windows, iOS, or Android operating systems. As opposed to loading the firmware onto the device over the network, an application is installed into the mobile device and configured.

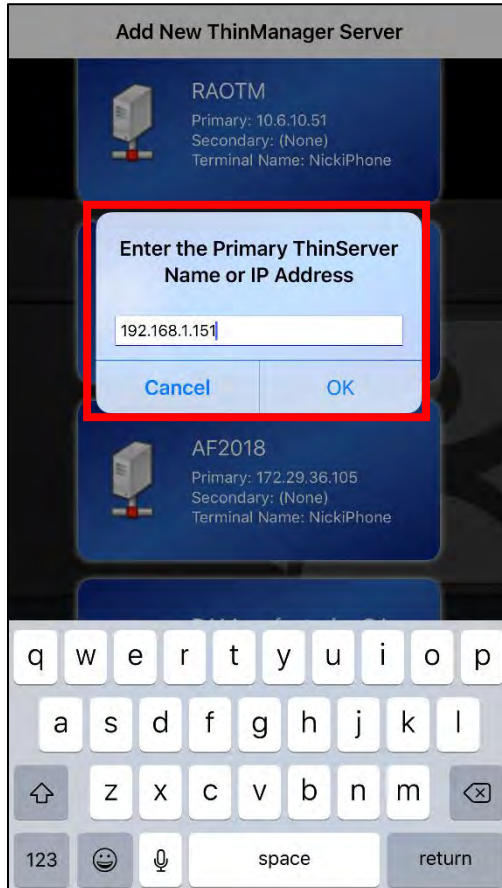
1. To create the terminal profile for the mobile device, launch the ThinManager UI and from terminals tab, right-click the Terminals group and select *Add Terminal*.
2. From the Terminal Name page of the Terminal Configuration Wizard, enter the name of the terminal and click *Next*.
3. For the Terminal Hardware settings, use the appropriate settings based on the table below:

OPERATING SYSTEM	IOS	ANDROID	WINDOWS
THINMANAGER APP	iTMC	aTMC	WinTMC
MAKE / OEM	Apple	GENERIC	GENERIC
MODEL	iOS Device	Android Device	WinTMC

4. Complete the Terminal Configuration Wizard as was completed for the previous terminals such as the VersaView 5200 terminals, using a unique user name for each device.
5. From the respective online application repository or store, install the supported ThinManager application on your device. The following steps will show the configuration for a iOS device.
6. Once iTMC is downloaded and installed on your compatible iOS device, iTMC will need to be configured to point to the correct ThinManager Server.
7. Select the *Settings* button on the bottom of the application and select *Add New Server* on the iTMC client to open the New Configuration window.



8. Enter the IP address or DNS name of the primary ThinManager server.
9. Specify a Configuration Description and a Primary ThinServer IP and save your configuration. A Secondary ThinServer IP may be entered to provide redundancy.



Add New ThinManager Server

RAOTM
Primary: 10.6.10.51
Secondary: (None)
Terminal Name: NickiPhone

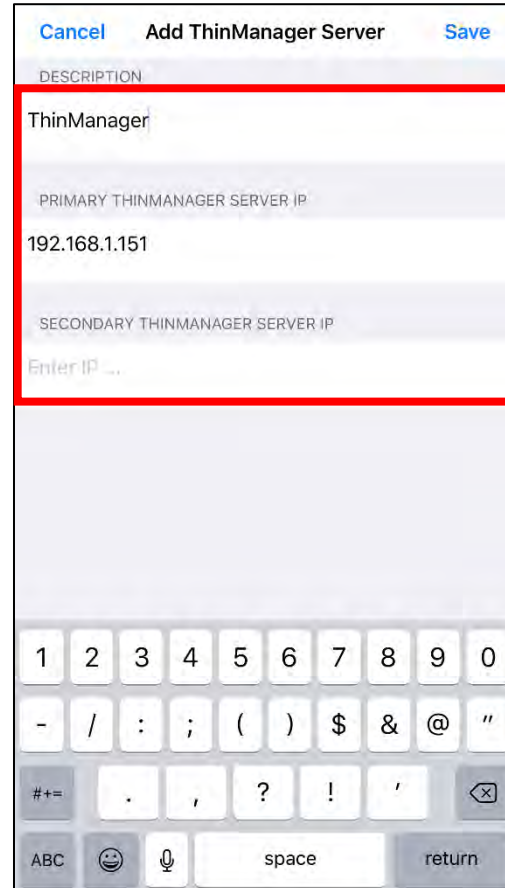
Enter the Primary ThinServer Name or IP Address

192.168.1.151

Cancel OK

AF2018
Primary: 172.29.36.105
Secondary: (None)
Terminal Name: NickiPhone

q w e r t y u i o p
a s d f g h j k l
z x c v b n m
123 space return



Cancel Add ThinManager Server Save

DESCRIPTION

ThinManager

PRIMARY THINMANAGER SERVER IP

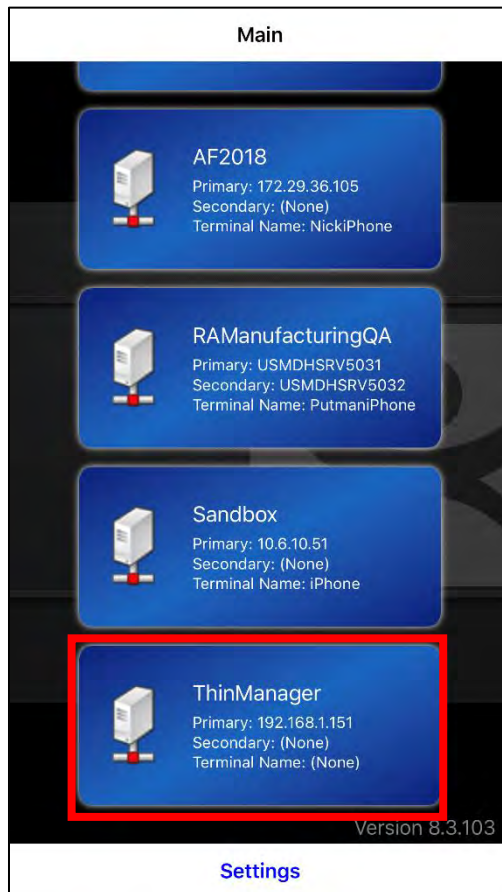
192.168.1.151

SECONDARY THINMANAGER SERVER IP

Enter IP ...

1 2 3 4 5 6 7 8 9 0
- / : ; () \$ & @ "
#+= . , ? ! ' <x>
ABC space return

10. Tap the newly created configuration and then tap Connect.
11. From the terminal replacement window, select the terminal created for the mobile device.

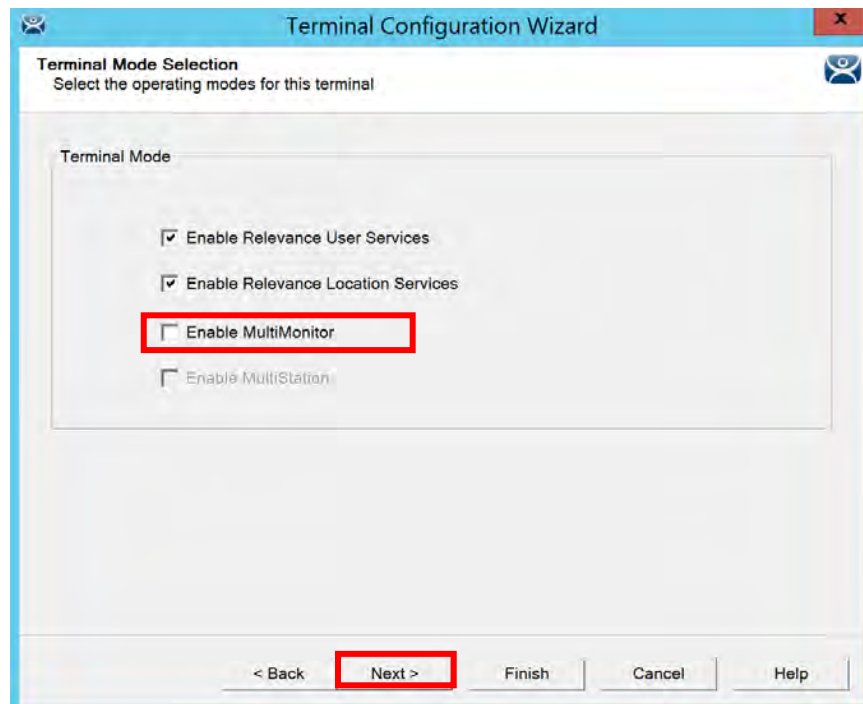


MultiMonitor and MultiSession

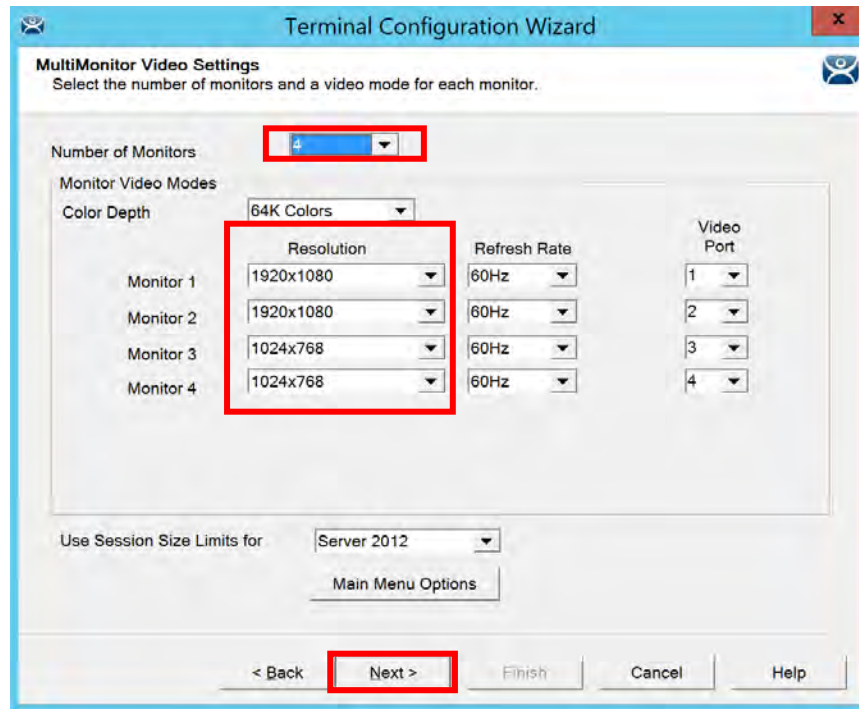
ThinManager supports multiple sessions being delivered to each monitor as well as multiple monitors being delivered from a single terminal. Current product limits are 25 sessions in a 5x5 grid when tiling on each monitor and up to 7 monitors from a single thin client.

To enable and configure MultiMonitor capabilities on a terminal:

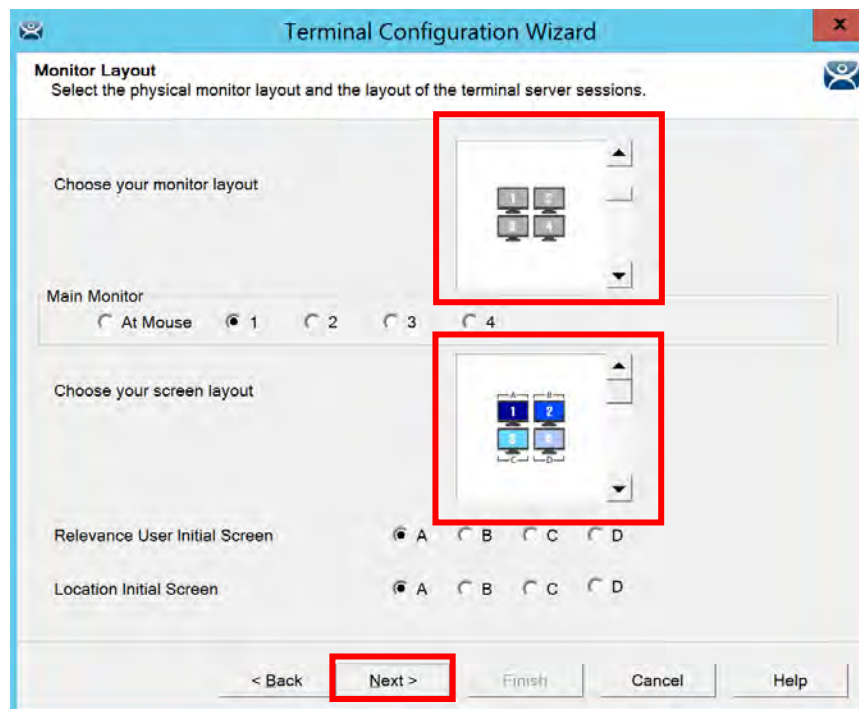
1. From the Terminal Configuration Wizard, select the checkbox next to *Enable MultiMonitor* on the Terminal Mode Selection page of the wizard. Click *Next*.



2. Select from the dropdown list the number of monitors connected to the terminal and set the resolution of each monitor. Click *Next*.

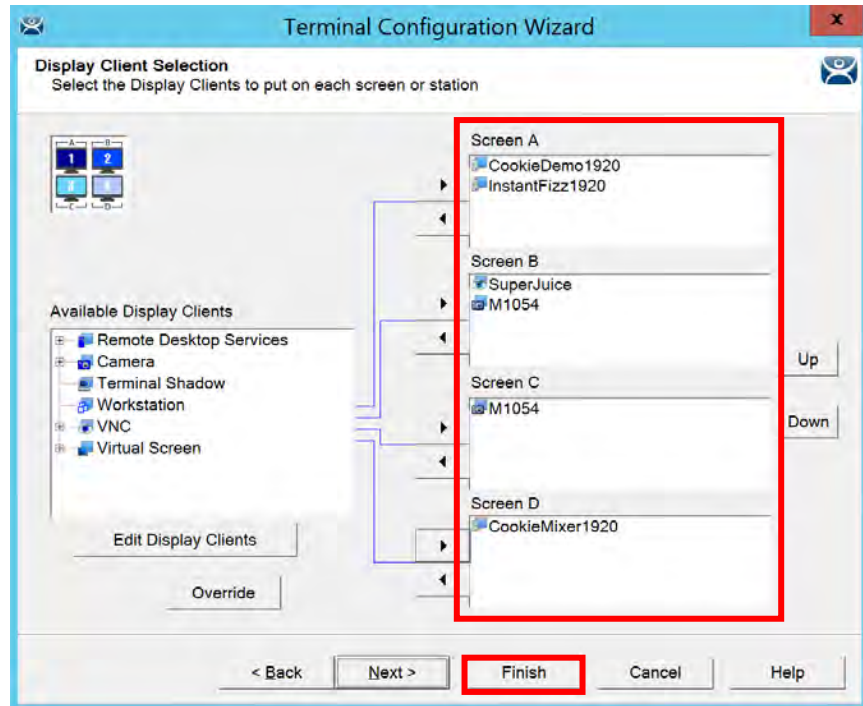


3. Select the monitor layout for how the displays are physically configured and the screen layout for how the displays are to be logically displayed.



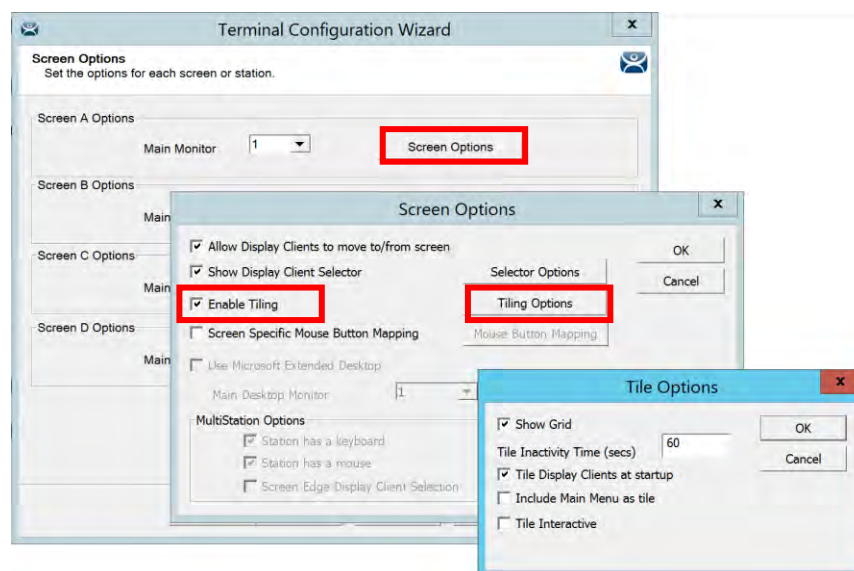
4. Using the available display clients and the right arrow buttons, assign display clients to each of the monitors added in the previous steps. Click *Finish*.

Note: MultiSession is the ability to deliver multiple display clients to a single monitor. To configure MultiSession, MultiMonitor is not required. MultiSession is configured by adding multiple display clients to a single monitor as seen in Screen A and Screen B below.



Tiling

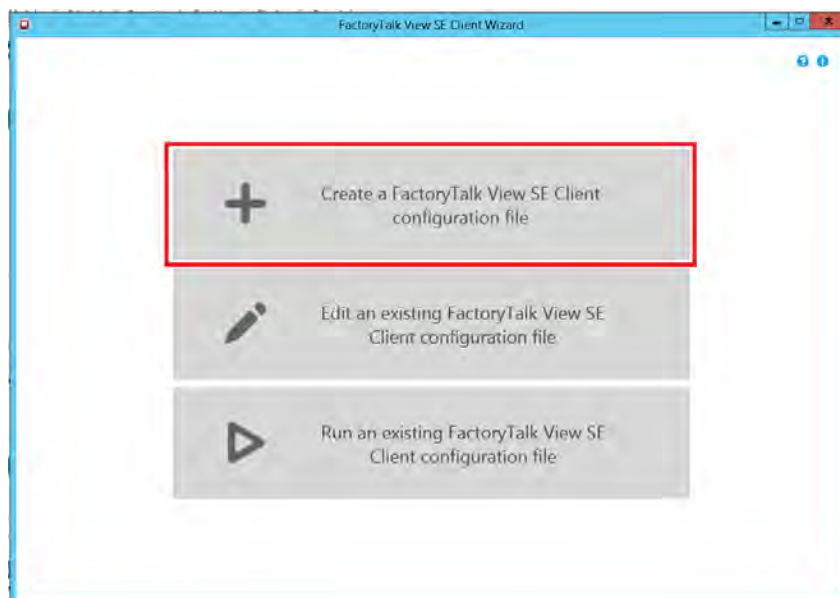
Tiling, or visualization of multiple sessions on a single monitor at the same time, can be enabled for each monitor in the Terminal Configuration Wizard's Screen Options page. Check the box for Enable Tiling on each monitor that should have this functionality.



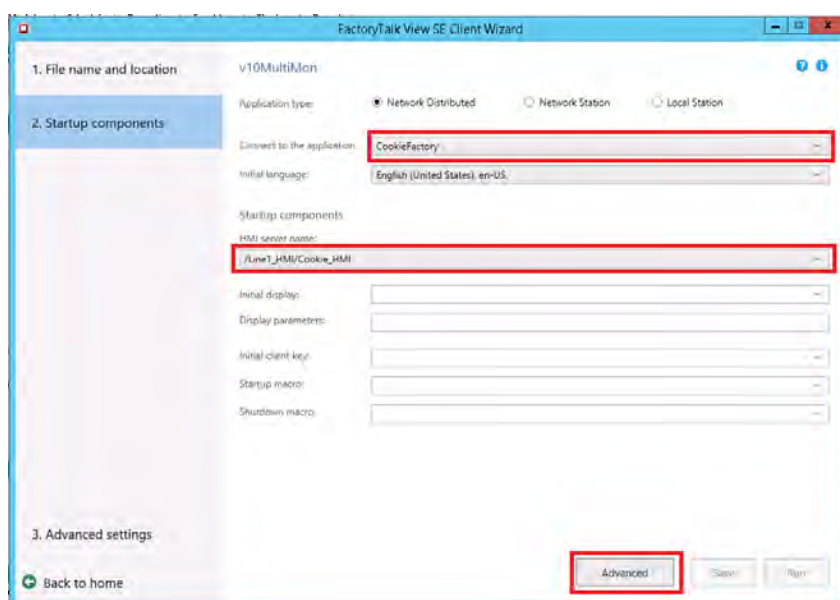
FactoryTalk View SE MultiMonitor Option with ThinManager

The FactoryTalk ViewSE v10.01 Client and newer Multi-monitor feature is compatible with ThinManager. This method should only be used if it is desired to span a single FTVIEW SE client across multiple monitors taking advantage of FTVIEW SE native functionality such as the ability to invoke filtering on one monitor by navigating to another area in a particular FTVIEW SE Display. To get this to work you have to first setup your FTVIEWSE client with the Multi-monitor:

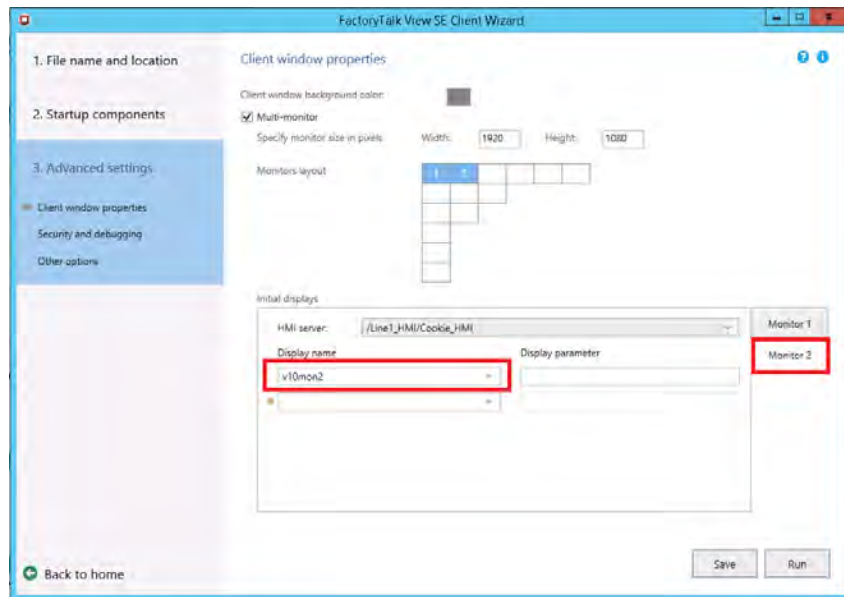
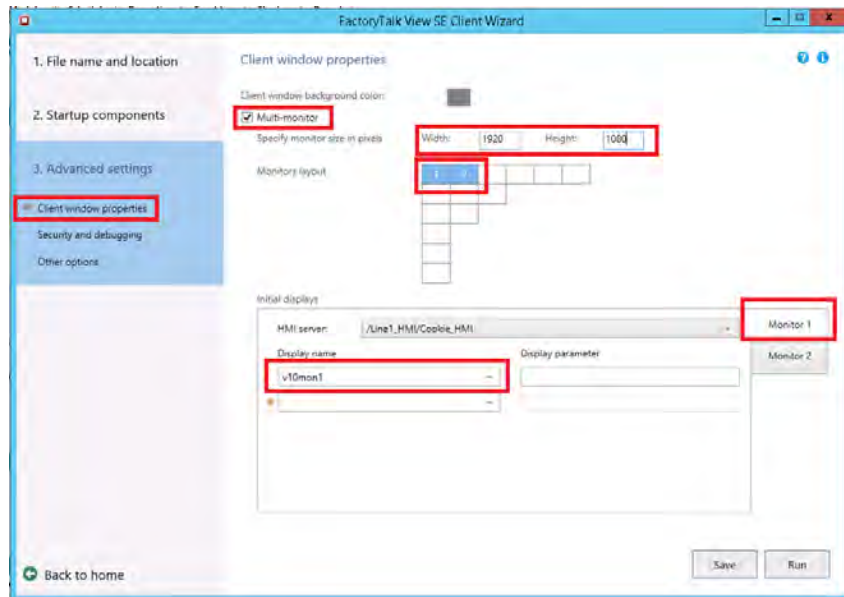
1. Open FactoryTalk View SE Client, Select Create a FactoryTalk View SE Client configuration file



2. On the File name and location tab, specify a file name and the save directory.
3. From the Startup components tab, specify your HMI application and HMI server, click Advanced.

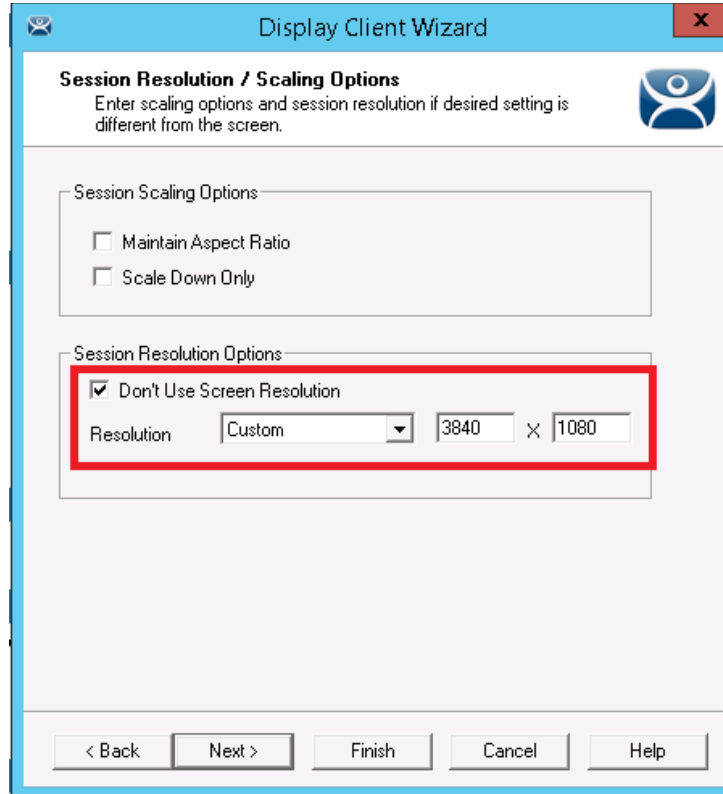


4. Check the Multi-Monitor checkbox and specify your monitor layout and resolution. Select the Display Name for Monitor 1 and separate Display Name for Monitor 2.



5. Specify any other options, save the client file.

6. Launch the ThinManager Admin UI. When configuring your Display Client, select Don't Use Screen Resolution checkbox and input custom resolution on the Session Resolution / Scaling Options page of the wizard. Pictured is the resolution for (2) 1920x1080 monitors arranged side-by-side.



Display Client Wizard

Session Resolution / Scaling Options
Enter scaling options and session resolution if desired setting is different from the screen.

Session Scaling Options

- ☐ Maintain Aspect Ratio
- ☐ Scale Down Only

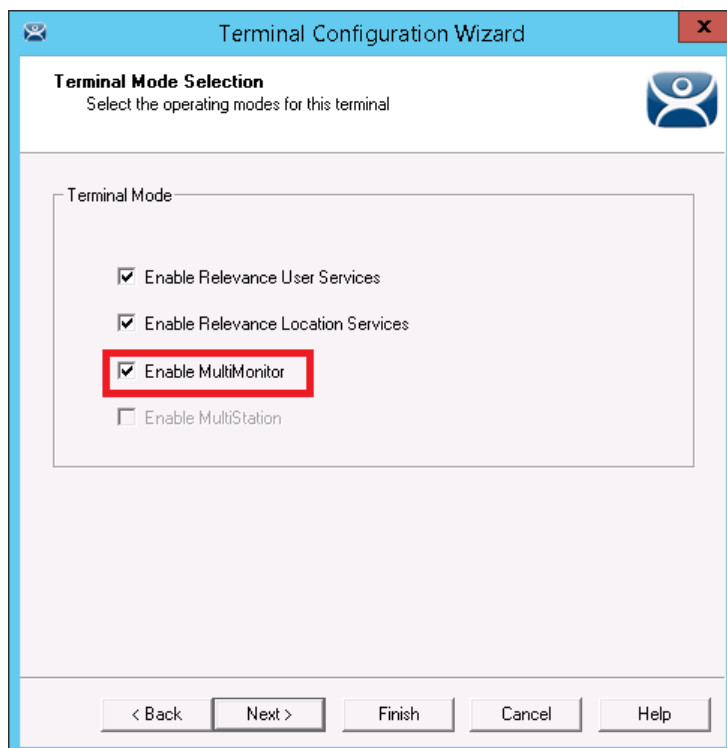
Session Resolution Options

☒ Don't Use Screen Resolution

Resolution: Custom 3840 × 1080

< Back Next > Finish Cancel Help

7. When creating your terminal profile, Enable Multimonitor on the Terminal Mode Selection page of the wizard.



Terminal Configuration Wizard

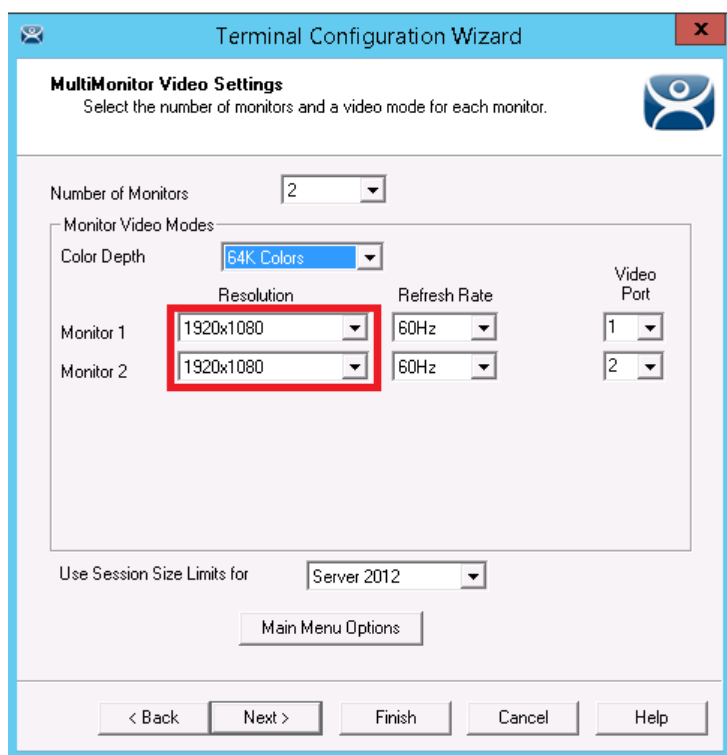
Terminal Mode Selection
Select the operating modes for this terminal

Terminal Mode

- ☒ Enable Relevance User Services
- ☒ Enable Relevance Location Services
- ☒ **Enable MultiMonitor**
- ☐ Enable MultiStation

< Back Next > Finish Cancel Help

8. Specify the resolution of each monitor on the MultiMonitor Video Settings page of the wizard.



Terminal Configuration Wizard

MultiMonitor Video Settings
Select the number of monitors and a video mode for each monitor.

Number of Monitors: 2

Monitor Video Modes

Color Depth: 64K Colors

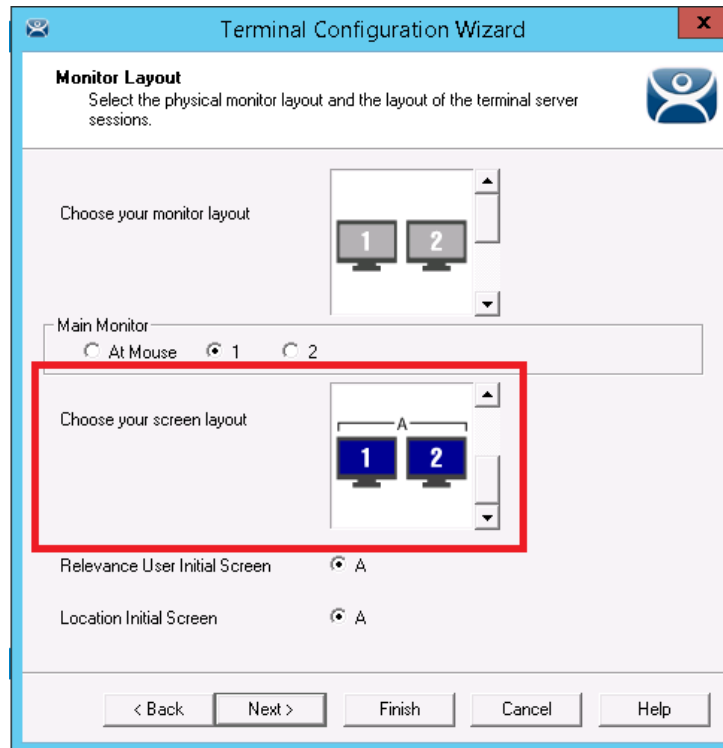
	Resolution	Refresh Rate	Video Port
Monitor 1	1920x1080	60Hz	1
Monitor 2	1920x1080	60Hz	2

Use Session Size Limits for: Server 2012

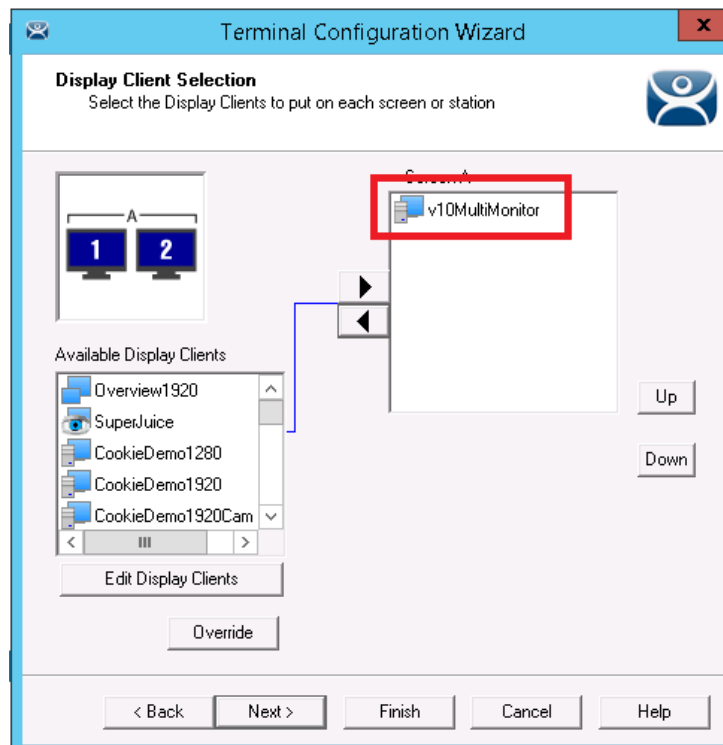
Main Menu Options

< Back Next > Finish Cancel Help

9. Enable spanning of the two displays on the Monitor Layout page of the wizard by scrolling down on the screen layout selection to enable screen A across both monitors.



10. Assign the Display Client configured in Step 1 to the monitor on the Display Client Selection page of the wizard.



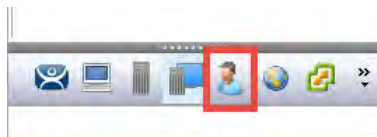
ThinManager Security

ThinManager incorporates security in its Relevance Users, Active Directory Integration, and many other ways. The scope of this document will focus on securely delivering a FactoryTalk View SE application to a terminal, however more information on security best practices can be found in ThinManager literature and on the web in the knowledgebase at [1082369 – ThinManager and Security Best Practices TOC](#).

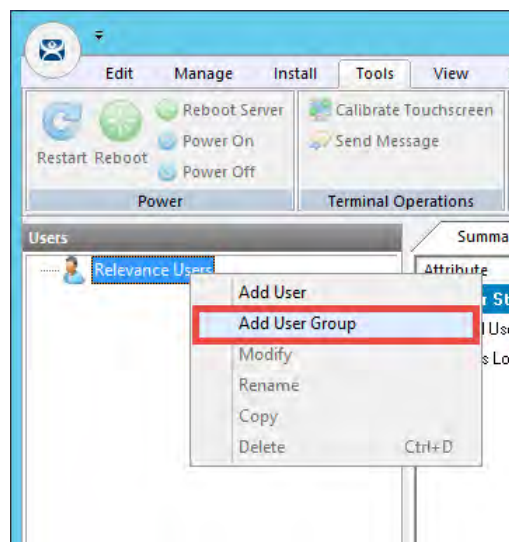
Active Directory Integration and Relevance Users

ThinManager supports Active Directory integration with its Relevance Users. An Active Directory group or users can be added into the ThinManager Relevance Users tree. To create active directory linked Relevance Users and assign content to those users and groups, the following steps can be used.

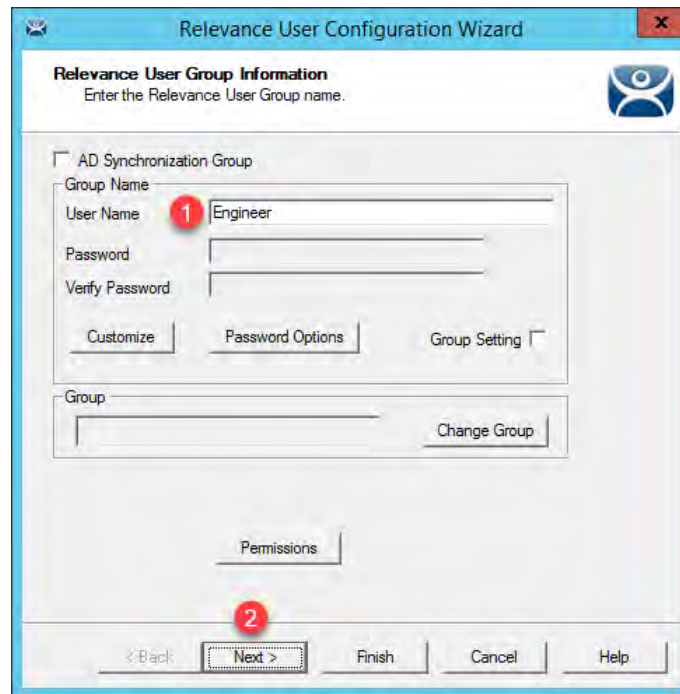
1. Click the **Users** icon  in the ThinManager tree selector.



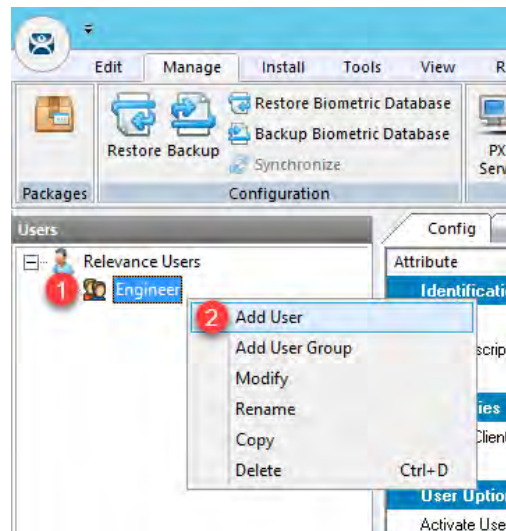
2. From the **Relevance Users** tree, right click the **Relevance Users** node and select **Add User Group**. This will launch the **Relevance User Configuration Wizard**.



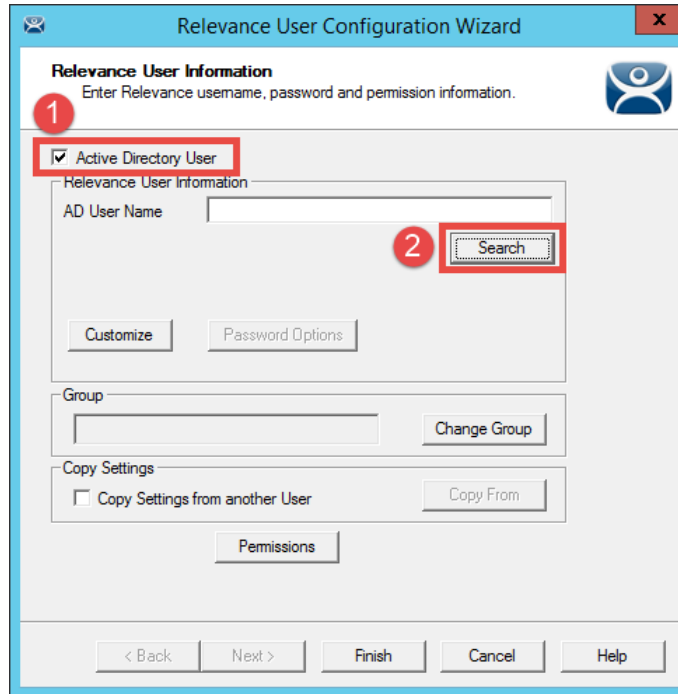
3. From the **Relevance User Group Information** page of the wizard, enter *Engineer* as the **User Name** in the **Group Name** frame. Click the **Finish** button. If you wish to assign specific content to the entire group, you may add group setting Display Clients later in the wizard.



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

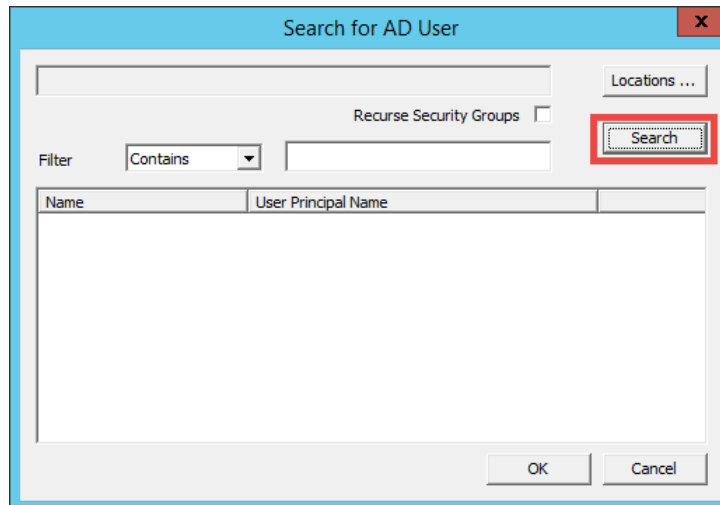


6. From the **Relevance User Information** page of the wizard, check the **Active Directory User** checkbox if it is not already checked. Click the **Search** button.



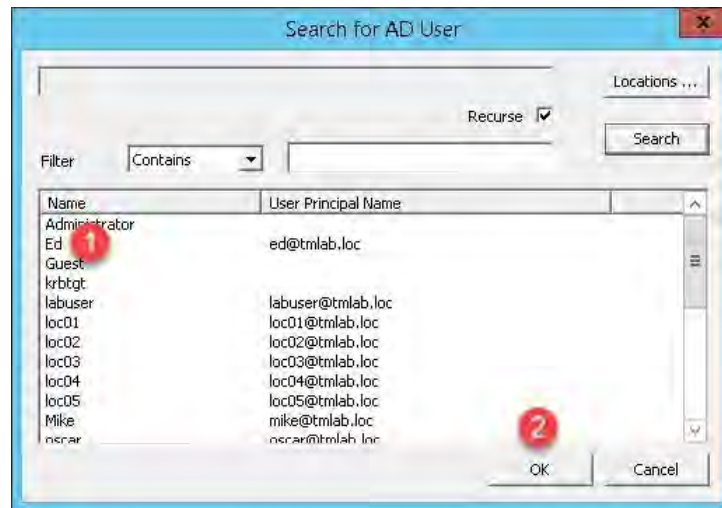
The screenshot shows the 'Relevance User Configuration Wizard' window, specifically the 'Relevance User Information' page. The page title is 'Relevance User Information' with a subtitle 'Enter Relevance username, password and permission information.' A red circle with the number '1' highlights the 'Active Directory User' checkbox, which is checked. Below this, there is a text field for 'AD User Name' and a 'Search' button, which is highlighted with a red circle and the number '2'. Other buttons visible include 'Customize', 'Password Options', 'Group', 'Change Group', 'Copy Settings', 'Copy From', 'Permissions', '< Back', 'Next >', 'Finish', 'Cancel', and 'Help'.

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

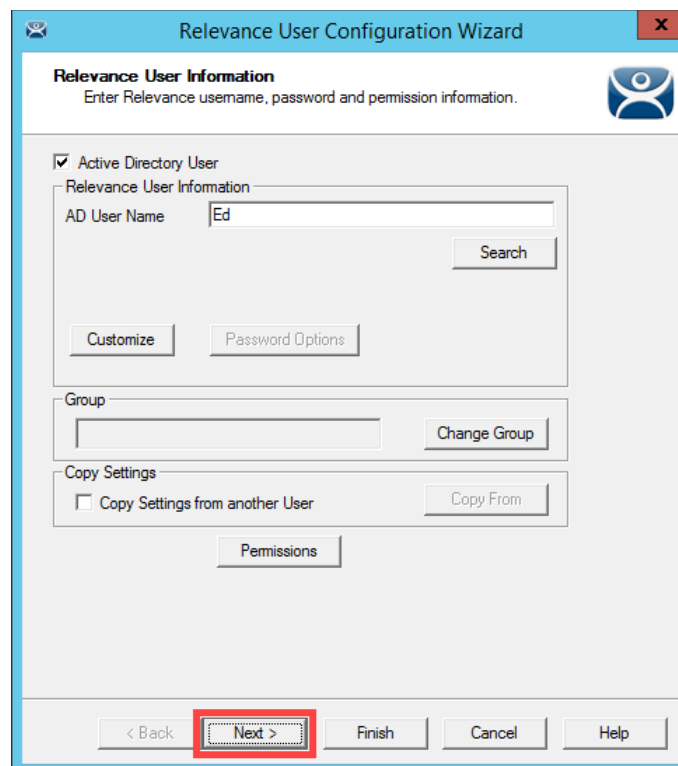


The screenshot shows the 'Search for AD User' dialog box. It features a text input field at the top, a 'Locations ...' button, and a 'Recurse Security Groups' checkbox. Below these is a 'Filter' dropdown menu set to 'Contains' and another text input field. A red box highlights the 'Search' button. At the bottom, there is a table with two columns: 'Name' and 'User Principal Name'. The table is currently empty. At the bottom right, there are 'OK' and 'Cancel' buttons.

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



9. By linking to an Active Directory User, this Relevance user's credentials will reside in Active Directory, not within ThinManager. You can also create local users in ThinManager, in which case their credentials would reside in ThinManager.
10. Back at the **Relevance User Information** page of the wizard, click the **Next** button.




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

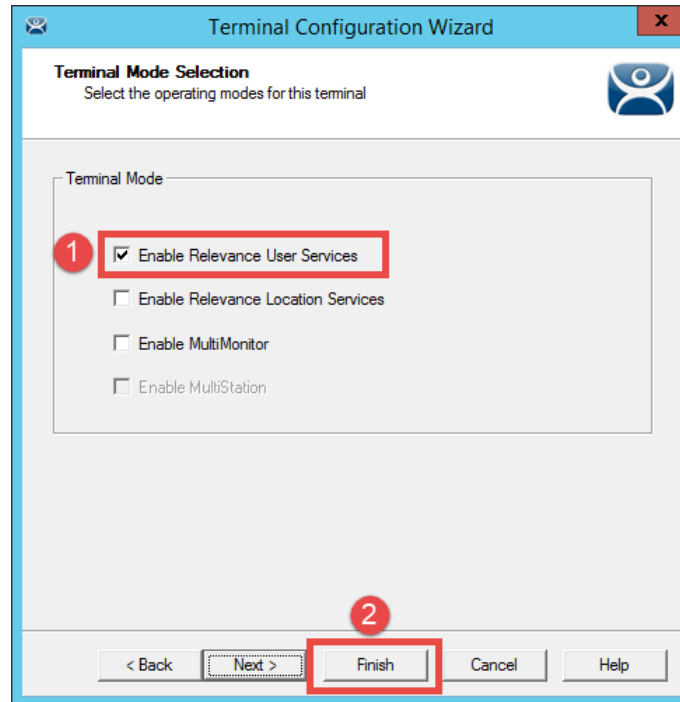
Note: You can choose to store the Active Directory password for this user within ThinManager. This is sometimes done when using badge readers or fingerprint scanners so the user can either scan his/her badge or scan his/her fingerprint only to login (i.e.: no password entry is required). If the Active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

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

12. From the **Card / Badge Information** page of the wizard, click the **Next** button.
13. From the **Relevance Resolver Selection** page of the wizard, click the **Next** button.
14. From the **Display Client Selection** page of the wizard, click the **Next** button.
15. From the **Display Client Specification** page of the wizard click the **Finish** button.

Note: In order to take advantage of relevance users on a terminal, Relevance User Services must be enabled on each terminal

16. Click the **Terminals** icon  from the ThinManager tree selector.
17. Under the **Terminals** node, double click the terminal name to launch the **Terminal Configuration Wizard**.
18. Click the **Next** button on the **Terminal Name** page of the wizard.
19. Click the **Next** button on the **Terminal Hardware** page of the wizard.
20. Click the **Next** button on the **Terminal Options** page of the wizard.
21. From the **Terminal Mode Selection** page of the wizard, check **Enable Relevance User Services**.
Click the **Finish** button.



Authentication Pass-Through

ThinManager can now pass Relevance User credentials natively to supported HMI products using a token-based technology. To experience Authentication Pass-Through, simply login to a terminal that is displaying a FactoryTalk View SE Client application as one of the Display Clients and the Relevance User will be automatically logged into not only the terminal, but the View SE application itself. This technology streamlines the productivity of the plant floor by reducing the number of login activities an operator must perform, while maintaining the security and integrity of the operating environment. There is no configuration required to take advantage of this feature. Authentication Pass-Through requires versions 10 or higher of both ThinManager and the FactoryTalk View SE product to be installed.