Windows 2008 Server

Adding Terminal Server Role

Windows 2008 Server, like Windows 2003 Server, allows two RDP connections for administrative purposes. To make the Windows 2008 Server a terminal server where many people can access applications requires adding the Terminal Services Role.

Open the Server Manager window.

Server Manager		
<u>File Action View H</u> elp		
🗢 🔿 🙍 📊		
 Server Manager (2008TSE49) Roles Features Diagnostics Configuration Task Scheduler Windows Firewall with Advant Services WMI Control Local Users and Groups Storage 	Roles View the health of the roles installer roles and features. Roles Summary Roles: 0 of 16 installed	ed on your server and add or remove Roles Summary Help Add Roles Remove Roles
	Last Refresh: 4/12/2010 4:24:54 PM Conf	igure refresh
		_

Server Manager Window

Highlight **Roles** in the tree and select *Add Roles* in the right pane. A wizard will launch allowing you to add Terminal Services as a role.

Highlights of the Role Wizard include:

Add Roles Wizard

Select Server Roles Before You Begin Select one or more roles to install on this server. Server Roles Roles: Description: Terminal Services Active Directory Certificate Services Terminal Services provides technologies that enable user Role Services Active Directory Domain Services Terminal Services provides technologies that enable user	
Before You Begin Select one or more roles to install on this server. Server Roles Roles: Description: Terminal Services Active Directory Certificate Services Terminal Services provides technologies that enable user technologies that enable user technologies that enable user	
Confirmation Active Directory Federation Services actess Windows dased program Progress Active Directory Lightweight Directory Services access the full Windows desk Progress Active Directory Rights Management Services access the full Windows desk Progress Active Directory Rights Management Services terminal Services, users can a terminal server from within you corporate network or from the Internet. DHCP Server DHCP Server Internet. Prist Services Network Policy and Access Services Print Services Web Server (IIS) Windows Deployment Services Web Server (IIS)	ers to grams that server or to sktop. With n access a your the
< Previous Next > Install Can	ancel

Role Wizard - Select Server Roles

The **Role Wizard** lists a dozen roles that are available.

Check the *Terminal Services* checkbox and any other roles desired.

Select Next to continue.

Y

Add Roles Wizard		X
Select Role Serv	ices	
Before You Begin Server Roles Terminal Services Role Services Application Compatibility Authentication Method Licensing Mode User Groups Confirmation Progress Results	Select the role services to install for Terminal Services: Role services: Select the role services TS Licensing TS Session Broker TS Gateway TS Web Access	Description: Terminal Server enables a server to host Windows-based programs or the full Windows desktop. Users can connect to a terminal server to run programs, save files, and use network resources on that server.
	< Previous	Next > Install Cancel

Role Wizard –Select Role Services

Terminal Services has several options:

- **Terminal Server** the basic terminal services option. Check this option
- TS Licensing This makes the server a 2008 License Server. You need a 2008 License Server and 2008 Terminal Services Client Access Licenses (TS CALs) to operate. Select this if this server will be your Terminal Services License Server.

Select Next to continue.

Add Roles Wizard

Specify Licensin	ng Mode
Before You Begin Server Roles Terminal Services Role Services Application Compatibility Authentication Method	The <u>Terminal Services licensing mode</u> determines the type of Terminal Services client access licenses (TS CALs) that a license server will issue to clients that connect to this terminal server. Specify the Terminal Services licensing mode that you want this terminal server to use. C <u>Configure later</u> Remind me to use the Terminal Services Configuration tool or Group Policy to configure the licensing mode within the next 120 days.
Licensing Mode User Groups Confirmation Progress Results	 Per Device A TS Per Device CAL must be available for each device that connects to this terminal server. Per User A TS Per User CAL must be available for each user that connects to this terminal server. The licensing mode that you specify must match the TS CALs that are available from your Terminal Services license server.

Role Wizard – Specify Licensing Mode

Windows 2008 TS CALs, like Windows 2003 TS CALs, are available as *Per Device* or *Per User*.

The terminal server should match the mode that the license server is using.

Select Next to continue.

×

Add Roles Wizard

Confirm Installat	ion Selections
Before You Begin Server Roles Terminal Services Role Services Application Compatibility Authentication Method	To install the following roles, role services, or features, dick Install. 1 warning, 2 informational messages below 1 This server must be restarted after the installation completes. Terminal Services Terminal Server
Licensing Mode User Groups Confirmation Progress Results	▲ You may need to reinstall existing applications. ④ IE Enhanced Security Configuration will be turned off. Authentication method: Do not require Network Level Authentication Licensing mode: Per user Groups allowed access: Administrators
	Print, e-mail, or save this information < Previous Next > Install Cancel

Role Wizard – Confirm Installation Selections

The Add Roles Wizard will end with a list of the configurations that will be installed.

Select *Install* to add the role(s). Once the wizard is finished it will assume the role of a terminal server.

X

Adding Applications in Windows 2008

Applications on terminal servers need to be installed in the **Install Mode**. Open the Control Panel and click on the **Install Application on Terminal Server** icon to start the installation wizard.



Install Application on Terminal Server Icon

A wizard will run that allows the installation of the application.

The **Install Mode** can also be entered by typing **change user** /**install** at a command prompt. You can then run the **setup.exe** to install your application.

Type **change user** /**execute** when finished installing to leave the Install Mode.

Create Users

Users management is located in the Server Manager console.

📕 Server Manager				
<u>File Action View Help</u>				
🗢 🔿 🖄 🛅 🗱 🛙 🛃				
Server Manager (2008TSE49)	Groups 17 Group(s)		Actions	
🗆 🔐 Roles	Name	Description 🔺	Groups	
Features Diagnostics	Administrators Backup Operators	Administrators k Backup Operato Members of this	More Actions Remote Desktop Users	•
 Configuration	Certificate Service DCO Cryptographic Operators Distributed COM Users Event Log Readers Guests IIS_IUSRS Network Configuration Performance Log Users Performance Monitor U Power Users Print Operators Replicator Network	Members of this Members are au Members are all Members of this Guests have the Built-in group us Members in this Members of this Members of this Power Users are Members can ac Members in this Supports file rep	More Actions	•

Server Manager – Local Users and Groups

Users need to be members of the Remote Desktop Users group to access the terminal server.

Allowing Application Access

Applications installed on a terminal server are not available to remote users unless the Terminal Server Settings are changed to allow access to the applications. You can either allow access to all applications or allow access to specific applications in the **TS RemoteApp Manager**.

Allowing Application Access – All Applications

Applications installed on a terminal server are not available to remote users unless the Terminal Server Settings are changed to allow access to the applications.

You can change the settings to allow access to all installed applications in the TS RemoteApp Manager.



TS RemoteApp Manager

Highlight TS RemoteApp Manager under the Terminal Services branch of the Server Manager tree.

Select the *Change* link for the **Terminal Server Settings** to launch the **RemoteApp Deployment Settings** page.

RemoteApp Deploymer	nt Settings			×
Common RDP S	Settings	1	Custom RDP Se	ettings
Terminal Server	Terminal Server TS Gateway Digital Signature			
Clients will use these settir	ngs while connectir	ng to this ter	minal server.	
Connection settings -				
Server name:	2008TSE49			
	If the terminal serv farm.	ver is in a far	m, enter the DN	S name of the
<u>R</u> DP port:	3389			
Require server auth	entication			
If you use server au name in the Server	thentication, you n name box.	nay have to	provide a fully qu	ualified DNS
Remote desktop acces	is			
Show a remote <u>d</u> esk	ctop connection to	this terminal	server in TS We	eb Access
Access to unlisted prog	jrams			
C Do not allow users to (Recommended)	o start unlisted prog	rams on initi	al connection	
 Allow users to start b 	ooth listed and unlis	ted program	s on initial conne	ection
			1	
	<u>0</u> K		<u>C</u> ancel	<u>A</u> pply

RemoteApp Deployment Settings

Select the Terminal Server tab of the **RemoteApp Deployment Settings** page.

Select the *Allow users to start both listed and unlisted programs on initial connection* radio button in the **Access to unlisted programs** section.

This will allow any program to be run by an authorized user.

You can also select and define specific applications that can be run by configuring them in the **TS RemoteApp Manager**.

Allowing Application Access – Specific Applications

You can control application access on Windows 2008 Server by only allowing access to specific applications.



TS RemoteApp Manager

Highlight TS RemoteApp Manager under the Terminal Services branch of the Server Manager tree.

Select the *Add RemoteApp Programs* link in the **Actions** column on the right of the screen to launch the **RemoteApp Wizard**.

RemoteApp Wizard	×
Choose programs to add to the RemoteApp Programs list Select the programs that you want to add to the RemoteApp Programs list. You can also configure individual RemoteApp properties, such as the icon to display.	
	_
Name	-
Calculator	
🗖 🚎 Data Sources (ODBC)	
🗆 👪 Disk Defragmenter	
🗆 🔍 iSCSI Initiator	
Memory Diagnostics Tool	
🗹 🦌 Paint	
🗆 🦥 Paint Shop Pro 5	
Problem Reports and Solutions	
Remote Desktop Connection	
🗆 🌆 Security Configuration Wizard	
Server Manager	
System Configuration	
System Information	
Windows Contacts	-
	_
Select All Select None Properties Browse	
	_
(Deals News) Course	.
< <u>Back</u> <u>Next</u> > Cance	

RemoteApp Wizard

The **RemoteApp Wizard** shows a list of applications installed on the Windows 2008 Server.

Select the checkbox for each application that you want available for deployment as a ThinManager Display Client.

Select *Next* to complete the wizard. A remote user can run any checked application.

Installing ThinManager

It is a common practice to install ThinManager on a terminal server but ThinManager is independent of terminal services and doesn't need to be installed on a terminal server.

Applications on terminal servers need to be installed in the **Install Mode**. Open the Control Panel and click on the **Install Application on Terminal Server** icon to start the installation wizard.



Install Application on Terminal Server Icon

Once the wizard begins navigate to the ThinManager setup.exe program and continue with the wizard. See Installation of ThinManager for details.

The Install Mode can also be entered by typing **change user** /**install** at a command prompt. You can then run the **setup.exe** to install ThinManager.

Type **change user** /**execute** when finished installing to leave the Install Mode.

Allow Inbound Traffic to Firewall

ThinManager requires communications to the ThinManager Ready thin clients. This communication is blocked by default in the firewall and needs to be allowed.

You can either open the firewall to all traffic or open the specific ports needed.

Allow All Inbound Traffic

You can configure the firewall by selecting *Windows Firewall with Advanced Security* in the Server **Manager** tree.



Windows Firewall with Advanced Security

Highlight **Windows Firewall with Advanced Security** in the **Server Manager** tree. Right click and select **Properties** to launch the **Properties** window.

Windows Firewall with Advanced Security	×
Domain Profile Private Profile Public Profile IPsec Settings	
Specify behavior for when a computer is connected to a public network location.	
Eirewall state: On (recommended)	
Inbound connections: Allow	
Outbound connections: Allow (default)	
Settings Specify settings that control Windows Firewall behavior.	
Logging Specify logging settings for Customize	
Learn more about these settings	
OK Cancel Apply	

Windows Firewall with Advanced Security Properties

Select the profile tab that matches the type of network you are using, *Domain*, *Private*, or *Public* profile. Change the **Inbound connections** to *Allow* and select *OK* to accept the change.

This will allow the thin clients to connect to ThinManager through the firewall.

Open Ports in Firewall

You can open specific ports in the Windows 2008 Server firewall instead of allowing all inbound connections if you prefer.

Open the Local Security Policy by selecting the Start > Administrative Tools > Local Security Policy.



Local Security Policy

Expand the Windows Firewall with Advanced Security to show the Inbound Rules.

Right click on the **Inbound Rules** and select **New Rule**. A wizard will launch that allows configuration of a new port.

You need to run the wizard twice, once to allow UDP 4900 and once to allow TCP 2031.

💮 New Inbound Rule Wizard		×
Rule Type		
Select the type of firewall rule to cr	eate.	
Steps:	What type of rule would you like to create?	
 Protocol and Ports Action Profile Name 	Program Rule that controls connections for a program. Pgrt Rule that controls connections for a TCP or UDP port. Predefined: ITS Peercaching Rule that controls connections for a Windows experience. Qustom Custom rule. Learn more about rule types	
	< <u>B</u> ack <u>N</u> ext > Cancel	

Rule Wizard – Rule Type

Select *Port* as the rule you are configuring and select *Next* to continue.

New Inbound Rule Wizard	×
Protocol and Ports Specify the protocol and ports that	t this rule matches.
Steps: Protocol and Ports Action Profile Name	Does this rule apply to TCP or UDP?
	< <u>B</u> ack <u>N</u> ext > Cancel

Rule Wizard – Protocols and Ports

You will need to select the protocol and port for each rule. You will need to run the wizard once for UDP 4900 and once for TCP 2031.

Select the protocol and enter the port as shown in *Rule Wizard – Protocols and Ports*.

Select *Next* to continue.

Action	
Specify the action that is taken	when a connection matches the conditions specified in the rule.
Steps:	
Rule Type	What action should be taken when a connection matches the specified conditions?
Protocol and Ports	
Action	<u>Allow the connection</u>
Profile	Allow connections that have been protected with IPsec as well as those that have not.
Name	C Allow the connection if it is secure
	Allow only connections that have been authenticated and integrity-protected through the use of IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.
	Learn more about actions

Rule Wizard – Action

Select Allow the Connection.

Select *Next* to continue.

🍻 New Inbound Rule Wizard	×
Profile	
Specify the profiles for which this	rule applies.
Steps:	
Rule Type	When does this rule apply?
Protocol and Ports	
Action	☑ <u>D</u> omain
🥔 Profile	Applies when a computer is connected to its corporate domain.
Name	 Private Applies when a computer is connected to a private network location. Public Applies when a computer is connected to a public network location.
	Learn more about profiles < Back Next > Cancel

Rule Wizard – Profile

Select the network(s) that the rule will apply to.

Select *Next* to continue.

A **Name** page will allow you to name the rule and add a description for management and organizational purposes.

Select *Finish* to save and apply the rule.

Local Security Policy		
<u>File Action View H</u> elp		
🗇 🔿 🖄 🔐 😹 🛛 🖬		
 Security Settings Account Policies Local Policies Windows Firewall with Advanced Security Windows Firewall with Advanced Secur	Name	Group 🔺

Applied Rules

Repeat for UDP 4900 or TCP 2031.

This will allow thin clients to use port 4900 to download the firmware and allow the thin client to use port 2031 to download the configuration but will keep other ports closed on the firewall.

Local Security Policy – User Access Controls

You may need to go to the Local Security Policy and change the **User Account Control: Behavior of the** elevation prompt for administrators in Admin Approval Mode to *Elevate without prompting* for ThinManager to run properly.

Open the Local Security Policy by selecting the Start > Administrative Tools > Local Security Policy.

🚡 Local Security Policy		
<u>File Action View H</u> elp		
💠 🔿 🚺 🖬 😫		
 Security Settings Account Policies Local Policies Audit Policy Security Options Windows Firewall with Adva Network List Manager Policie Public Key Policies Software Restriction Policie: IP Security Policies on Local 	Policy Recovery console: Allow floppy copy and access to all drives and all fol Shutdown: Allow system to be shut down without having to log on Shutdown: Clear virtual memory pagefile System cryptography: Force strong key protection for user keys stored System cryptography: Lee FIPS compliant algorithms for encryption, ha System objects: Require case insensitivity for non-Windows subsystems System objects: Strengthen default permissions of internal system obje System settings: Optional subsystems System settings: Use Certificate Rules on Windows Executables for Sof User Account Control: Admin Approval Mode for the Built-in Administrat User Account Control: Allow UIAccess applications to prompt for elevati User Account Control: Behavior of the elevation prompt for standard us User Account Control: Detect application installations and prompt for el User Account Control: Only elevate executables that are signed and va User Account Control: Only elevate UIAccess applications that are insta User Account Control: Run all administrators in Admin Approval Mode User Account Control: Run all administrators in Admin Approval Mode User Account Control: Switch to the secure desktop when prompting fo User Account Control: Switch to the secure desktop when prompting fo User Account Contr	Security Setting Disabled Disabled Disabled Disabled Not Defined Disabled Enabled Enabled Disabled Disabled Disabled Elevate without promptin Prompt for credentials Enabled Disabled Enabled

Local Security Policy – User Account Controls

Highlight *Local Policies > Security Options* in the tree.

Browse to User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode and change the setting to *Elevate without prompting*.

This may be needed to run ThinManager as a non-administrator.

Command Prompt

Terminal Services has several commands that aid in managing the terminal server. Some useful ones are:

Command	Action
change logon	Temporarily disables logons to a Terminal Server
change port	Changes COM port mappings for MS-DOS program compatibility
change user /install	Puts the server into "Install Mode"
change user /execute	Removes the server from "Install Mode"
Ipconfig	Displays the IP addresses of the network card
Logoff	Logs off a user from a session and deletes the session from the server
net send <i>username "message</i> "	Sends a message to a user. <i>username</i> is the NT/2000 user name that the person or terminal is logged in as. " <i>message</i> " is the text of the message. Quotation marks are needed for any messages containing a space.
query process	Displays information about processes running on a Terminal server
query session	Displays information about sessions on a Terminal server
query termserver	Displays a list of all Terminal servers on the network
query user	Displays information about user sessions on a Terminal server
reset session	Resets a session to known initial values
Shadow	Monitors another user's session
Tsdiscon	Disconnects a client from a terminal server session
Tsshutdn	Shuts down the terminal server in an orderly manner

See the Windows online help for additional commands and parameters.

Other useful commands include:

Command	Action
gpedit.msc	Launches the Group Policy Editor
tscc.msc	Launches the Terminal Services Configuration Console
tsadmin	Launches the Terminal Services Manager

Alternative Terminal Keystrokes

Certain keystrokes are not available in a terminal session. Microsoft has provided these alternatives.

Keystroke	Function	
ALT+PAGE UP	Switches between programs from left to right.	
ALT+PAGE DOWN	Switches between programs from right to left.	
ALT+INSERT	Cycles through the programs in the order they were started.	
ALT+HOME	Displays the Start menu.	
CTRL+ALT+BREAK	Switches the client between a window and full screen.	
CTRL+ALT+END	Brings up the Windows 2000 Security dialog box.	
ALT+DELETE	Displays the Windows menu.	
CTRL+ALT+Minus (-) symbol on the numeric keypad	Places a snapshot of the active window, within the client, on the Terminal server clipboard (provides the same functionality as pressing PrintScrn on a local computer.)	
CTRL+ALT+Plus (+) symbol on the numeric keypad	Places a snapshot of the entire client window area on the Terminal server clipboard (provides the same functionality as pressing ALT+PrintScrn on a local computer.)	

DHCP Server Setup

Dynamic Host Configuration Protocol (DHCP) is a program that assigns IP addresses to devices on a network. DHCP server can be used to provide IP addresses to ThinManager Ready thin clients. It can also be configured to point the thin clients to the ThinManager Servers with **Option 66, Boot Server Host Name**.

Scope Options

The DHCP Server needs **Option 066** configured before it will provide the ThinManager Server IP address that the terminal needs to boot.

Scope Options	? ×
General Advanced	
Available Options	Description 🔺
064 NIS+ Domain Name	The name o
065 NIS+ Servers	A list of IP a
🗹 066 Boot Server Host Name	TFTP boot 💷
L 067 Bootfile Name	Bootfile Nan 🗸
- Data entru	
String value:	
1921681119216812	
132.100.111132.100.1.q	
OK Cancel	Apply

Boot Server Host Name

The Boot Server Host Name, Option 066, assigns a ThinManager server to the terminal.

Open the Scope Options dialog box by highlighting the **Scope Option** folder in the tree pane of the Computer Management Console under the **Services and Application > DHCP** folder and selecting **Action > Configure Options**.

Scroll through the list window and check the **Option 066** check box.

Enter the IP address of the desired ThinManager server in the String Value field.

The DHCP Server can issue the IP address for a Primary ThinManager Server and a Secondary ThinManager Server by listing the IP addresses of both, separated with a space.

DHCP Properties

The DHCP Server can be configured to check for duplicate IP addresses before issuing a new address. This is a good feature to use.

Highlight DHCP under Services and Applications in the Computer Management tree and select Action > *Properties*, or right-click on DHCP and select *Properties*. The DHCP Properties window will launch.

DHCP Properties	? ×	
General DNS Advanced		
Specify the number of times the DHCP server should attempt conflict detection for an IP address before the server leases the address to a client.		
Conflict detection attempts:		
Audit log file path: C:\WINDOWS\System32\dhcp	<u>B</u> rowse	
Database path: C:\WINDOWS\System32\dhcp	B <u>r</u> owse	
Backup gath: C:\WINDOWS\System32\dhcp\ba	Br <u>o</u> wse	
Change server connections bindings:	Bindings	
DNS dynamic updates registration credentials:	Credentials	
OK Cancel	Apply	

DHCP Properties – Advanced Tab

Select the *Advanced* tab. Replace the zero in the *Conflict detection attempts* field with an integer. This will prompt the DHCP Server to check for duplicate IP addresses before assigning an IP address. Select *OK* when finished.

Group Policy

Windows has a number of features that can be allowed or prevented with a Group Policy. Group Policy is configured in the Group Policy Object Editor snap-in to the Microsoft Management Console.

Access the Group Policy Editor by typing **gpedit.msc** at a command prompt to launch the Microsoft Group Policy Editor.



Group Policy Settings

Expanding the tree will show Group Policy settings that can affect the terminal server experience.

Please refer to Microsoft documentation for information on using these features.