Tech Note 782 Installing Remote Desktop Services on Windows 2008 Server R2 for Wonderware Products

All Tech Notes, Tech Alerts and KBCD documents and software are provided "as is" without warranty of any kind. See the Terms of Use for more information.

Topic#: 002563 Created: July 2011

Introduction

This installation procedure is the basis for all Wonderware products used on a Remote Desktop Session Host (Terminal Server), for example, InTouch View for System Platform (Managed Applications), InTouch (Standalone Applications), Historian Client, and the IDE (used by multiple developers via Remote Desktop Connections).

This *Tech Note* describes the installation steps for the Remote Desktop Services Server Role of Windows 2008 Server R2, formerly known as Terminal Services. It is assumed that the operating system has already been installed and Microsoft updates applied.

Application Versions

- InTouch 10.1 and later
- Microsoft Server 2008 R2

New Terminology

With Release 2 of Windows 2008 Server the Terminology of Terminal Services has changed. The following table shows the new nomenclature:

Old Terminology	Terminology of Windows 2008 Server R2
Terminal Services (TS)	Remote Desktop Services (RDS)
Terminal Server	Remote Desktop Session Host
Terminal Server Licensing	Remote Desktop Licensing (RD-Licensing)
Terminal Services Web Access (TS Web Access)	Remote Desktop Web Access
Terminal Services Gateway (TS Gateway)	Remote Desktop Gateway
Terminal Services Session Broker (TS Session Broker)	Remote Desktop Session Broker

Installation

You install and configure Roles using the Server Manager.

Adding the Remote Desktop Services Server Role

To add Server Roles

1. Click Start > Administrative Tools > Server Manager.



FIGURE 1: OPEN SERVER MANAGER

2. Right-click Roles, then click Add Roles (Figure 2 below).



FIGURE Z: ADD ROL

3. Click Next.



FIGURE 3: ADD ROLES WIZARD

- 4. Check Remote Desktop Services on the list to install and activate this role.
- 5. Click Next.



FIGURE 4: ACTIVATE REMOTE DESKTOP SERVICES ROLE

Selecting the Correct Role Services

Each Server Role includes several Role Services. For a simple environment the following components are required:

- Remote Desktop Session Host (formally Terminal Server)
- Remote Desktop Licensing

For **Remote Desktop Web Access** (formally Terminal Server Web Access), **Web Server (IIS)** is necessary. Selecting this Role Service causes the default installation of a Web Server (Figure 5 below)



FIGURE 5: ADD WEB SERVER SERVICES

Note: Additional Role Services can also be added at any time.

Authentication Mode

Two Authentication methods are available. In this example the second option is selected, because Network Level Authentication is supported since RDP 6.0. That means clients with older operating systems. For example Windows XP SP1 would not have access to the Remote Desktop Session Host.



FIGURE 6: DO NOT REQUIRE NETWORK LEVEL AUTHENTICATION

Licensing Mode

Microsoft offers a 120-Day Demo License. This license is used for this *Tech Note*. The original license can be added afterwards, so select the **Configure later** option. For more information about licensing contact Microsoft.



FIGURE 7: CONFIGURE LICENSE LATER

Add User Groups

The users and user groups are added here. These are the people who will have access to the Remote Desktop Session Host. They are added to the local Remote Desktop Users Group.

Add Roles Wizard		X
Select User Gr	oups Allowed Access To This RD Session Host Server	
Before You Begin Server Roles Remote Desktop Services Role Services	Add the users or user groups that can connect to this RD Session Host server. These users and user groups will be added to the local Remote Desktop Users group. The Administrators group is added by default and cannot be removed. Users or User Groups:	
Application Compatibility	Administrators Add	
Authentication Method	Stephanieb (RDS2008R2)Stephanieb) Remove	
Licensing Mode		
Client Experience RD Licensing Configuration Web Server (IIS)		
Role Services		
Confirmation		
Progress		
Results	More about the Remote Desktop Users group	
	< Previous Next > Instal Cancel	

FIGURE 8: CONFIGURING USER GROUPS FOR REMOTE DESKTOP USERS GROUP

Configuring the Client Experience

Keep the default settings (Figure 9 below)

Configure Clier	nt Experience
Before You Begin Server Roles Remote Desktop Services Role Services Application Compatibility Authentication Method Licensing Mode	You can configure the RD Session Host server so that users connecting to a remote desktop session can use functionality similar to that provided by Windows 7. Providing this functionality requires additional system and bandwidth resources and may affect the scalability of the RD Session Host server. Select the functionality that you want to provide. Additional functionality can be configured by using the Remote Desktop Session Host Configuration tool.
Client Experience	Selecting audio and video playback or desktop composition will install the <u>Desktop Experience</u> <u>feature</u> on the RD Session Host server.
RD Licensing Configuration	
Web Server (IIS)	Audio and video playback
Role Services	Audio recording redirection
Confirmation Progress	Desktop composition (provides the user interface elements of Windows Aero)
Results	 If a selection is dimmed, a Group Policy setting is currently being applied to the computer that prevents that functionality from being configured. For more information, see Group Policy Settings and Configuring the Client Experience. More about configuring the client experience.

FIGURE 9: LEAVE THE DEFAULT SETTINGS

Remote Desktop Licensing Configuration

Note: This option does not apply to Windows 2008 Server R2.



FIGURE 10: RD LICENSING CONFGURATION

Web Server (IIS and its Role Services)

For Remote Desktop Web Access the Web Server Role must be installed. Keep the default Role Services (Figure 11 below).



file:///C|/inetpub/wwwroot/t002563/t002563.htm[11/1/2011 9:01:20 AM]

FIGURE 11: LICENSING

Now the installation begins (Figure 12 below).

Add Roles Wizard	jress
Before You Begin Server Roles Remote Desktop Services Role Services Application Compatibility Authentication Method Licensing Mode User Groups Client Experience RD Licensing Configuration Web Server (IIS) Role Services Confirmation Progress	The following roles, role services, or features are being installed: Remote Desktop Services Web Server (IIS) Remote Server Administration Tools

FIGURE 12: BEGIN THE INSTALLATION

Restarting the System

Adding the Server Roles requires a restart (Figures 13 and 14 below).



FIGURE 13: RESTART AFTER INSTALLING THE ROLES



FIGURE 14: PROMPT FOR RESTART

Seminary					
tvents: 1 warning, 1 infor	national in the last 24 h	ours.			Go to Event Vere
7 Number of events: 2					Gr Filter Events
Level Event	Event ID Date and Time Source		Properties		
() Information	0 5/17/2011 5:49:4	8 PM	TerminalServices-Lic	rensing	Hide Al Events
System Services: Al Running Display Name	Service Name	Status	Startup Type	Monitor	Q, Go to Services
IIS Admin Service	isadmin	Running	Auto	Yes	Stop
Remote Desktop Licensing	TermServLicen	Running	Auto	Yes	Start
Remote Desktop Services	TermService	Running	Manual	Tes	I Restart
			res confin ration for	the GMTP and FTP services. If f	his service is stooped.
Description: Inables this server to administer the server will be unable to configu Best Practices Analyzer: To	e IIS metabase. The II re SMTP or FTP. If this start a Best Practices A	5 metabase sto service is disabl nalyzer scan, c	ed, any services that Sck Scan this Role	t explicitly depend on it will fail to	o start.
Description: Inables this server to administer the server will be unable to configu Best Practices Analyzer: To Noncompliant (0) Excluded (0)	e IIS metabase. The II re SMTP or FTP. If this start a Best Practices A Compliant (0) All (0)	5 metabase sto service is disabi nalyzer scan, c	ed, any services that Sck Scan this Role	explicitly depend on it will fail to	start.
Description: Inables this server to administer the server will be unable to configu Best Practices Analyzer: To Noncompliant (0) Excluded (0) Serverity Title	e IIS metabase. The III re SMTP or FTP. If this start a Best Practices A Compliant (0) All (0)	5 metabase sto service is disabi nalyzer scan, c	ed, any services that Sok Scan this Role Categ	explicitly depend on it will fail t	start.
Description: Enables this server to administer th the server will be unable to configu- Best Practices Analyzer: To Noncompliant (0) Excluded (0) Severity Title	e IIS metabase. The II re SMTP or FTP. If this start a Best Practices A Compliant (0) All (0)	S metabase sto service is disabl nalyzer scan, c	ed, any services that lock Scan this Role Categ	explicitly depend on it will fail to	Scan This Role Exclude Result Include Result Properties

FIGURE 15: REMOTE DESKTOP SERVICES RESTART

Remote Desktop Services are NOT started automatically by default (Figure 16 below).

Xeplay Name	Service Name	Status	Startup Type	Monitor
LIIS Admin Service	isadmin	Running	AUto	Yes
Remote Desktop Licensing	TermEervLicen	Running	AVC0	Yes
Remote Desktop Services	TermService	Running	Manual	Yes
World Wide Web Publishing Service	W38VC	KUNNING	Auto	Yes
escription:				

FIGURE 16: REMOTE DESKTOP SERVICES IS SET TO MANUAL BY DEFAULT

Enable Remote Access on the Server

file:///C|/inetpub/wwwroot/t002563/t002563.htm[11/1/2011 9:01:20 AM]

Remote Access must be enabled. When you start the Server Manager, the Server Summary is displayed.

- 1. Open Server Manager, then click **Configure Remote Desktop**.
- 2. To ensure that clients with RDP Versions earlier than 6.0 will have access to the server, click the second option in the **Remote Desktop** area (Figure 17 below).

Get an over	System Properties	server roles and features.
	Computer Name Hardware Advanced Remote	1
Server Summary	Remote Assistance	Server Summary Help
Computer Info		Change System Properties
Full Computer Nar		View Network Connections
Workgroup:	Advanced	Configure Remote Desktop
Local Area Conne		Management
Remote Desktop:	Remote Desktop	
Server Manager F	Click an option, and then specify who can connect, if needed.	
Management:	C Don't allow connections to this computer	
Product ID:	Allow connections from computers running any version of	
Do not show n	C Allow connections only from computers running Remote	
	Desktop with Network Level Authentication (more secure)	
 Security Inform 	Help me choose Select Users	Go to Windows Firewall
Windows Firewall:	1	Configure opdates
Windows Updates	OK Cancel Apply	Run Security Configuration Wizard
Last checked for u		Configure IE ESC
Last installed updat	es: 5/6/2011 3:05 AM	
IE Enhanced Securi	ty Configuration Off for Administrators	

FIGURE 17: ALLOW CONNECTIONS FROM ANY VERSION OF REMOTE DESKTOP

Network Discovery

By default, the node is not visible to other machines in the network environment. You change this setting in the **Network and Sharing** Center.

1. In the Control Panel select Network and Internet:





2. Click Changed advanced sharing settings.

Network and Sharing Center	
Control Panel 🔹 Netw	ork and Int
Control Panel Home	View you
Change adapter settings	
Change advanced sharing settings	1
	View your
	*

FIGURE 19: CHANGE ADVANCED SETTINGS

3. Change the Network Discovery settings to match Figure 20 (below) and click Save Changes.

😪 Advanced sharing settings			
🕒 🗢 🗟 🔹 Network and Sharing Center 🔹 Adv	anced sharing settings	 Search Control Panel 	2
Change sharing options for differ	ent network profiles		4
Windows creates a separate network	profile for each network you use. You can d	hoose specific options for each profile.	
Home or Work		•	
Public (current profile)		A	
Network discovery			
When network discovery is other network computers.	on, this computer can see other network co <u>What is network discovery?</u>	mputers and devices and is visible to	
 Turn on network di Turn off network di 	scovery		
File and printer sharing			
When file and printer sharin accessed by people on the r	g is on, files and printers that you have sha network.	ared from this computer can be	
Turn on file and pri	nter sharing		
C Turn off file and pr	inter sharing		
Public folder sharing			
When Public folder sharing is the Public folders. What are	s on, people on the network, including home the Public folders?	egroup members, can access files in	
Turn on sharing so	anyone with network access can read and	write files in the Public folders	
C Turn off Public fold	er sharing (people logged on to this comput	ter can still access these folders)	
Password protected sharing			-
	(Save changes Cancel	

FIGURE 20: CHANGING SHARING OPTIONS

4. Make sure you have a viable Network connection.



FIGURE 21: VIABLE NETWORK CONNECTION

Show Hidden Files and Folders

Using Windows Explorer, show hidden files, folders and drives.

• In Windows Explorer, click Organize > Folder and Search Options > Folder Options > View tab (Figure 22 below).



FIGURE 22: SHOW HIDDEN FILES, FOLDERS, AND DRIVES

Disable UAC

For the installation of Wonderware Software, UAC (User Access Control) should be disabled. More details are described in Technote 733 Disabling UAC for Wonderware® Product Support.

S. Bruder, M. Aguinaldo

Tech Notes are published occasionally by Wonderware Technical Support. Publisher: Invensys Systems, Inc., 26561 Rancho Parkway South, Lake Forest, CA 92630. There is also technical information on our software products at Wonderware Technical Support.

For technical support questions, send an e-mail to wwsupport@invensys.com.



©2011 Invensys Systems, Inc. All rights reserved. No part of the material protected by this copyright may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying, recording, broadcasting, or by anyinformation storage and retrieval system, without permission in writing from Invensys Systems, Inc. Terms of Use.