

Remote Desktop Services Deployment Guide

Microsoft Corporation

Published: May 2010

Abstract

This guide provides instructions for deploying Remote Desktop Services in a production environment running the Windows Server® 2008 R2 operating system. It is intended for information technology (IT) professionals who want to implement an end-to-end, Remote Desktop Services solution. This guide covers deployment best practices for configuring Remote Desktop Services.



Copyright Information

This document supports a preliminary release of a software product that may be changed substantially prior to final commercial release, and is the confidential and proprietary information of Microsoft Corporation. It is disclosed pursuant to a non-disclosure agreement between the recipient and Microsoft. This document is provided for informational purposes only and Microsoft makes no warranties, either express or implied, in this document. Information in this document, including URL and other Internet Web site references, is subject to change without notice. The entire risk of the use or the results from the use of this document remains with the user. Unless otherwise noted, the companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted in examples herein are fictitious. No association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2009 Microsoft Corporation. All rights reserved.

Microsoft, and Active Directory, RemoteApp, Windows, and Windows Server are trademarks of the Microsoft group of companies.

All other trademarks are property of their respective owners.

Contents

[Remote Desktop Services Deployment Guide 7](#_Toc262465323)

[About this guide 7](#_Toc262465324)

[Planning to Deploy Remote Desktop Services 7](#_Toc262465325)

[Reviewing Remote Desktop Services concepts 7](#_Toc262465326)

[Implementing Your Remote Desktop Services Design Plan 8](#_Toc262465327)

[How to implement your Remote Desktop Services design by using this guide 9](#_Toc262465328)

[Checklist: Implementing a Virtual Desktop Infrastructure Design 9](#_Toc262465329)

[Checklist: Deploying a Personal Virtual Desktop 10](#_Toc262465330)

[Checklist: Deploying a Virtual Desktop Pool 11](#_Toc262465331)

[Checklist: Implementing a Session-based Design 13](#_Toc262465332)

[Checklist: Deploying a Remote Desktop Session Host Server 13](#_Toc262465333)

[Checklist: Deploying a Remote Desktop License Server 15](#_Toc262465334)

[Deploying Remote Desktop Session Host 15](#_Toc262465335)

[Deploying Remote Desktop Session Host 16](#_Toc262465336)

[Checklist: RD Session Host Installation Prerequisites 16](#_Toc262465337)

[About Remote Desktop Session Host 19](#_Toc262465338)

[What is Remote Desktop Services? 19](#_Toc262465339)

[Why use Remote Desktop Services? 19](#_Toc262465340)

[Remote Desktop Services role services 20](#_Toc262465341)

[What is RD Session Host? 20](#_Toc262465342)

[What is RD Web Access? 20](#_Toc262465343)

[What is RD Licensing? 21](#_Toc262465344)

[What is RD Gateway? 21](#_Toc262465345)

[Why use RD Gateway? 21](#_Toc262465346)

[What is RD Connection Broker? 22](#_Toc262465347)

[What is RD Virtualization Host? 22](#_Toc262465348)

[Using Remote Desktop 23](#_Toc262465349)

[Installing RD Session Host on a Domain Controller 24](#_Toc262465350)

[Remote Desktop Services and Windows Firewall 24](#_Toc262465351)

[Additional references 26](#_Toc262465352)

[Installing the RD Session Host Role Service 26](#_Toc262465353)

[Install the Remote Desktop Session Host role service 26](#_Toc262465354)

[Install the Remote Desktop Session Host role service (when Remote Desktop Services is already installed) 28](#_Toc262465355)

[Configuring the Network Level Authentication Setting for an RD Session Host Server 29](#_Toc262465356)

[Installing Programs on an RD Session Host Server 31](#_Toc262465357)

[Additional considerations 31](#_Toc262465358)

[Configuring the Remote Desktop Users Group 32](#_Toc262465359)

[Configuring the Client Experience on an RD Session Host Server 33](#_Toc262465360)

[Desktop Experience Feature 33](#_Toc262465361)

[What’s in the Desktop Experience feature 34](#_Toc262465362)

[Install Desktop Experience on an RD Session Host Server 34](#_Toc262465363)

[Install Desktop Experience 34](#_Toc262465364)

[Uninstall (Remove) Desktop Experience 35](#_Toc262465365)

[Configure Audio and Video Playback on an RD Session Host Server 36](#_Toc262465366)

[Manually configuring audio and video playback 37](#_Toc262465367)

[Install the Desktop Experience feature 37](#_Toc262465368)

[Start the Windows Audio service 37](#_Toc262465369)

[Enable the Allow audio and video playback redirection Group Policy setting 37](#_Toc262465370)

[Set the maximum color depth to 32 bits per pixel 38](#_Toc262465371)

[Configure Audio Recording Redirection on an RD Session Host Server 39](#_Toc262465372)

[Manually configuring audio recording redirection 39](#_Toc262465373)

[Start the Windows Audio service 39](#_Toc262465374)

[Enable the Allow audio recording redirection Group Policy setting 40](#_Toc262465375)

[Configure Desktop Composition on an RD Session Host Server 40](#_Toc262465376)

[Manually configuring desktop composition 40](#_Toc262465377)

[Install the Desktop Experience feature 41](#_Toc262465378)

[Start the Themes service 41](#_Toc262465379)

[Enable the Allow desktop composition for remote desktop sessions Group Policy setting 41](#_Toc262465380)

[Set the maximum color depth to 32 bits per pixel 41](#_Toc262465381)

[Group Policy Settings and Configuring the Client Experience 42](#_Toc262465382)

[Configuring License Settings on an RD Session Host Server 44](#_Toc262465383)

[Enabling Remote Desktop 45](#_Toc262465384)

[Enable Remote Desktop 45](#_Toc262465385)

[Verifying Remote Desktop Session Host Functionality 46](#_Toc262465386)

[Creating a New User Account 46](#_Toc262465387)

[Additional considerations 47](#_Toc262465388)

[Deploying a Simple Virtual Desktop Infrastructure 48](#_Toc262465389)

[Deploying a simple Virtual Desktop Infrastructure 48](#_Toc262465390)

[Checklist: Deploying the Virtual Machine for Remote Desktop Services 48](#_Toc262465391)

[About Virtual Desktop Infrastructure 50](#_Toc262465392)

[What is Virtual Desktop Infrastructure? 50](#_Toc262465393)

[Why use Virtual Desktop Infrastructure? 50](#_Toc262465394)

[Virtual Desktop Infrastructure role services 50](#_Toc262465395)

[Installing the Remote Desktop Virtualization Host Role Service 51](#_Toc262465396)

[Allowing Remote RPC 52](#_Toc262465397)

[Creating a Firewall Exception to Allow Remote Services Management 53](#_Toc262465398)

[Adding Permissions to the RDP Protocol 53](#_Toc262465399)

[Configuring Rollback for a Virtual Desktop Pool 54](#_Toc262465400)

[Creating a Virtual Machine 55](#_Toc262465401)

[Install Windows 7 on a virtual machine 55](#_Toc262465402)

[Joining RD Virtualization Host to RD Connection Broker 56](#_Toc262465403)

[Assigning a Personal Virtual Desktop 56](#_Toc262465404)

[Adding Virtual Machines to a Virtual Desktop Pool 57](#_Toc262465405)

[Enabling Rollback on a Virtual Machine 58](#_Toc262465406)

[Verifying Personal Virtual Desktop Functionality 59](#_Toc262465407)

[Verifying Virtual Desktop Pool Functionality 59](#_Toc262465408)

[Configuring Publishing 60](#_Toc262465409)

[Configure publishing 60](#_Toc262465410)

[Installing the Remote Desktop Web Access Role Service 61](#_Toc262465411)

[Install the Remote Desktop Web Access role service 61](#_Toc262465412)

[Populating the TS Web Access Computers Security Group 62](#_Toc262465413)

[Configuring the RD Web Access Server for RemoteApp and Desktop Connection 63](#_Toc262465414)

[Configuring RemoteApp and Desktop Connection 64](#_Toc262465415)

[Deploying Remote Desktop Connection Broker 65](#_Toc262465416)

[Installing the Remote Desktop Connection Broker Role Service 66](#_Toc262465417)

[Installation prerequisites 66](#_Toc262465418)

[Install the Remote Desktop Connection Broker role service 67](#_Toc262465419)

[Deploying Remote Desktop Licensing 67](#_Toc262465420)

[About Remote Desktop Licensing 68](#_Toc262465421)

[What is RD Licensing? 68](#_Toc262465422)

[Installing the Remote Desktop Licensing Role Service 69](#_Toc262465423)

[Activating the Remote Desktop License Server 71](#_Toc262465424)

[Activate a Remote Desktop License Server Automatically 71](#_Toc262465425)

[Activate a Remote Desktop License Server by Using a Web Browser 72](#_Toc262465426)

[Activate a Remote Desktop License Server by Using the Telephone 73](#_Toc262465427)

[Installing Remote Desktop Services Client Access Licenses 74](#_Toc262465428)

[Install Remote Desktop Services Client Access Licenses Automatically 75](#_Toc262465429)

[Install Remote Desktop Services Client Access Licenses by Using a Web Browser 76](#_Toc262465430)

[Install Remote Desktop Services Client Access Licenses by Using the Telephone 77](#_Toc262465431)

# Remote Desktop Services Deployment Guide

Remote Desktop Services, formerly Terminal Services, is a server role in Windows Server® 2008 R2 that provides technologies that enable users to access Windows-based programs that are installed on a Remote Desktop Session Host (RD Session Host) server, or to access the full Windows desktop. With Remote Desktop Services, users can access an RD Session Host server from within a corporate network or from the Internet.

Remote Desktop Services lets you efficiently deploy and maintain software in an enterprise environment. You can easily deploy programs from a central location. Because you install the programs on the RD Session Host server and not on the client computer, programs are easier to upgrade and to maintain.

### About this guide

This guide is intended for use by system administrators and system engineers. It provides detailed guidance for deploying a Remote Desktop Services design that has been preselected by you or an infrastructure specialist or system architect in your organization. You can then use this guide to deploy Remote Desktop Services in your production environment.

This guide provides steps for deploying the following Remote Desktop Services designs:

 Remote Desktop Services with Virtual Desktop Infrastructure (VDI)

 Remote Desktop Services with session-based desktops

 Remote Desktop Services with Add-ons

Use the checklists in [Implementing Your Remote Desktop Services Design Plan](#zbe61907ccc094e6baebc7381302d0c54) to determine how best to use the instructions in this guide to deploy your particular design.

# Planning to Deploy Remote Desktop Services

After you collect information about your environment and you decide on a Remote Desktop Services design, you can begin to plan the deployment of your organization’s Remote Desktop Services design.

## Reviewing Remote Desktop Services concepts

Use the following Step-by-Step Guides for more information about how Remote Desktop Services works and how to deploy Remote Desktop Services in a test environment:

 [Installing Remote Desktop Session Host Step-by-Step Guide](http://go.microsoft.com/fwlink/?LinkId=147292) (http://go.microsoft.com/fwlink/?LinkId=147292)

 [Deploying Remote Desktop Web Access with Remote Desktop Connection Broker Step-by-Step Guide](http://go.microsoft.com/fwlink/?LinkId=131927) (http://go.microsoft.com/fwlink/?LinkId=131927)

 [Customizing Remote Desktop Web Access by Using Windows SharePoint Services Step-by-Step Guide](http://go.microsoft.com/fwlink/?LinkId=159911) (http://go.microsoft.com/fwlink/?LinkId=159911)

 [Deploying RemoteApp Programs to the Start Menu by Using RemoteApp and Desktop Connection Step-by-Step Guide](http://go.microsoft.com/fwlink/?LinkId=154798) (http://go.microsoft.com/fwlink/?LinkId=154798)

 [Deploying Personal Virtual Desktops by Using Remote Desktop Web Access Step-by-Step Guide](http://go.microsoft.com/fwlink/?LinkId=147909) (http://go.microsoft.com/fwlink/?LinkId=147909)

 [Deploying Virtual Desktop Pools by Using Remote Desktop Web Access Step-by-Step Guide](http://go.microsoft.com/fwlink/?LinkId=147907) (http://go.microsoft.com/fwlink/?LinkId=147907)

 [Deploying Personal Virtual Desktops by Using RemoteApp and Desktop Connection Step-by-Step Guide](http://go.microsoft.com/fwlink/?LinkId=154801) (http://go.microsoft.com/fwlink/?LinkId=154801)

 [Deploying Virtual Desktop Pools by Using Remote Desktop Web Access Step-by-Step Guide](http://go.microsoft.com/fwlink/?LinkId=147906) (http://go.microsoft.com/fwlink/?LinkId=147906)

 [Deploying Virtual Desktop Pools by Using RemoteApp and Desktop Connection Step-by-Step Guide](http://go.microsoft.com/fwlink/?LinkId=154802) (http://go.microsoft.com/fwlink/?LinkId=154802)

 [Deploying Remote Desktop Gateway Step-by-Step Guide](http://go.microsoft.com/fwlink/?LinkId=142250) (http://go.microsoft.com/fwlink/?LinkId=142250)

 [Deploying Remote Desktop Licensing Step-by-Step Guide](http://go.microsoft.com/fwlink/?LinkId=141175) (http://go.microsoft.com/fwlink/?LinkId=141175)

 [Deploying Remote Desktop IP Virtualization Step-by-Step Guide](http://go.microsoft.com/fwlink/?LinkId=137795) (http://go.microsoft.com/fwlink/?LinkId=137795)

# Implementing Your Remote Desktop Services Design Plan

Consider the following factors before you implement your design plan:

 Complexity: The complexity of the scenario relative to other scenarios.

 Cost: The initial setup and sustained cost of this scenario.

 Fault tolerance: How the scenario supports the resiliency of the infrastructure, which ultimately affects the availability of the system.

 Performance: How the scenario affects the performance of the infrastructure.

 Scalability: The impact that the scenario has on the scalability of the infrastructure.

 Security: Whether the scenario has a positive or negative impact on overall infrastructure security.

## How to implement your Remote Desktop Services design by using this guide

The next step in implementing your design is to determine in what order each of the deployment tasks must be performed. This guide uses checklists to help you walk through the various server and application deployment tasks that are required to implement your design plan. Parent and child checklists are used as necessary to represent the order in which tasks for a specific Remote Desktop Services design must be performed.

Use the following parent checklists in this section of the guide to become familiar with the deployment tasks for implementing your organization's Remote Desktop Services design:

 [Checklist: Implementing a Virtual Desktop Infrastructure Design](#z35d528f4e073487381059429aed9fa10)

 [Checklist: Implementing a Session-based Design](#zfd7c46befdcb4efaa86cd8fd8263d280)

# Checklist: Implementing a Virtual Desktop Infrastructure Design

This parent checklist includes cross-reference links to important concepts about the Remote Desktop Services design. It also contains links to subordinate checklists that will help you complete the tasks that are required to implement this design.

Note

Complete the tasks in this checklist in order. When a reference link takes you to a procedure, return to this topic after you complete the steps in that procedure so that you can proceed with the remaining tasks in this checklist.

 Checklist: Implementing a virtual desktop infrastructure design

|  |  |  |
| --- | --- | --- |
|  | Task | Reference |
|  | Deploy a personal virtual desktop. | [Checklist: Deploying a Personal Virtual Desktop](#zac2931977ddc4099a405b450e269ca6c) |
|  | Deploy a virtual desktop pool. | [Checklist: Deploying a Virtual Desktop Pool](#z38cf48b9da7f43e4bbc5cb790497c447) |

# Checklist: Deploying a Personal Virtual Desktop

This parent checklist includes cross-reference links to important concepts about the Remote Desktop Services design. It also contains links to subordinate checklists that will help you complete the tasks that are required to implement this design.

Note

Complete the tasks in this checklist in order. When a reference link takes you to a procedure, return to this topic after you complete the steps in that procedure so that you can proceed with the remaining tasks in this checklist.

 Checklist: Deploying a personal virtual desktop

|  |  |  |
| --- | --- | --- |
|  | Task | Reference |
|  | Install the Remote Desktop Session Host (RD Session Host) role service. | [Checklist: Deploying a Remote Desktop Session Host Server](#z6de58af40ea44c53a26e99e176e298a2) |
|  | Install the Remote Desktop Virtualization Host (RD Virtualization Host) role service. | [Installing the Remote Desktop Virtualization Host Role Service](#z075e33b68dd94757a77081d68aed046d) |
|  | Install the Remote Desktop Connection Broker (RD Connection Broker) role service. | [Installing the Remote Desktop Connection Broker Role Service](#z338a5c0a03194606a9842f8b1731282a) |
|  | Install the Remote Desktop Web Access (RD Web Access) role service. | [Installing the Remote Desktop Web Access Role Service](#z954f8127ccd94bfaa144b73a0ddc2697) |
|  | Deploy the virtual machine for Remote Desktop Services. | [Checklist: Deploying the Virtual Machine for Remote Desktop Services](#z72557ba765744602b3df899349f70335) |
|  | Add the computer account of the RD Web Access server to the TS Web Access Computers group on RD Connection Broker. | [Populating the TS Web Access Computers Security Group](#zb8e7bf05c10f4050a0cf3b761ffb1d5f) |
|  | Configure RD Web Access to specify the source that provides the RemoteApp programs and virtual desktops that are displayed to users. | [Configuring the RD Web Access Server for RemoteApp and Desktop Connection](#z47ab101504404028a132da47849a650f) |
|  | Configure the RD Web Access server to use an RD Connection Broker server. | [Joining RD Virtualization Host to RD Connection Broker](#z9fd7b65971b0411eb154a52605d7207f) |
|  | Assign a personal virtual desktop by using the Assign Personal Virtual Desktop Wizard. | [Assigning a Personal Virtual Desktop](#z277cdeb866b44b02ab5a1b1082c13221) |
|  | Configure RemoteApp and Desktop Connection (optional). | [Configuring RemoteApp and Desktop Connection](#z625b694f9b8242828cf2acc32e534929) |
|  | Verify the functionality of the personal virtual desktop deployment. | [Verifying Personal Virtual Desktop Functionality](#ze45d37183ecc4bffa0431d9a191d698a) |

# Checklist: Deploying a Virtual Desktop Pool

This parent checklist includes cross-reference links to important concepts about the Remote Desktop Services design. It also contains links to subordinate checklists that will help you complete the tasks that are required to implement this design.

Note

Complete the tasks in this checklist in order. When a reference link takes you to a procedure, return to this topic after you complete the steps in that procedure so that you can proceed with the remaining tasks in this checklist.

 Checklist: Deploying a virtual desktop pool

|  |  |  |
| --- | --- | --- |
|  | Task | Reference |
|  | Install the Remote Desktop Session Host (RD Session Host) role service. | [Checklist: Deploying a Remote Desktop Session Host Server](#z6de58af40ea44c53a26e99e176e298a2) |
|  | Install the Remote Desktop Virtualization Host (RD Virtualization Host) role service. | [Installing the Remote Desktop Virtualization Host Role Service](#z075e33b68dd94757a77081d68aed046d) |
|  | Install the Remote Desktop Connection Broker (RD Connection Broker) role service. | [Installing the Remote Desktop Connection Broker Role Service](#z338a5c0a03194606a9842f8b1731282a) |
|  | Install the Remote Desktop Web Access (RD Web Access) role service. | [Installing the Remote Desktop Web Access Role Service](#z954f8127ccd94bfaa144b73a0ddc2697) |
|  | Deploy the virtual machine for Remote Desktop Services. | [Checklist: Deploying the Virtual Machine for Remote Desktop Services](#z72557ba765744602b3df899349f70335) |
|  | Add the computer account of the RD Web Access server to the TS Web Access Computers group on RD Connection Broker. | [Populating the TS Web Access Computers Security Group](#zb8e7bf05c10f4050a0cf3b761ffb1d5f) |
|  | Configure RD Web Access to specify the source that provides the RemoteApp programs and virtual desktops that are displayed to users. | [Configuring the RD Web Access Server for RemoteApp and Desktop Connection](#z47ab101504404028a132da47849a650f) |
|  | Configure the RD Web Access server to use an RD Connection Broker server. | [Joining RD Virtualization Host to RD Connection Broker](#z9fd7b65971b0411eb154a52605d7207f) |
|  | Add virtual machines to a virtual desktop pool. | [Adding Virtual Machines to a Virtual Desktop Pool](#ze202d82ea7a3430495bd7cb364187c74) |
|  | Configure RemoteApp and Desktop Connection (optional). | [Configuring RemoteApp and Desktop Connection](#z625b694f9b8242828cf2acc32e534929) |
|  | Verify the functionality of the virtual desktop pool deployment. | [Verifying Virtual Desktop Pool Functionality](#z512cfccdbbfb477ba6e3869a81a8a8ca) |

# Checklist: Implementing a Session-based Design

This parent checklist includes cross-reference links to important concepts about the Remote Desktop Services design. It also contains links to subordinate checklists that will help you complete the tasks that are required to implement this design.

Note

Complete the tasks in this checklist in order. When a reference link takes you to a procedure, return to this topic after you complete the steps in that procedure so that you can proceed with the remaining tasks in this checklist.

 Checklist: Implementing a session-based design

|  |  |  |
| --- | --- | --- |
|  | Task | Reference |
|  | Deploy an RD Session Host server. | [Checklist: Deploying a Remote Desktop Session Host Server](#z6de58af40ea44c53a26e99e176e298a2) |

# Checklist: Deploying a Remote Desktop Session Host Server

This parent checklist includes cross-reference links to important concepts about the Remote Desktop Services design. It also contains links to subordinate checklists that will help you complete the tasks that are required to implement this design.

Note

Complete the tasks in this checklist in order. When a reference link takes you to a procedure, return to this topic after you complete the steps in that procedure so that you can proceed with the remaining tasks in this checklist.

Please note the following:

 Installing the RD Session Host role service requires the computer to be restarted.

 Installing the RD Session Host role service on an Active Directory domain controller is not recommended.

 You should install the RD Session Host role service on the computer before you install any programs that you want to make available to users.

 Checklist: Deploying a Remote Desktop Session Host server

|  |  |  |
| --- | --- | --- |
|  | Task | Reference |
|  | Review prerequisites for installing the RD Session Host role service. | [Checklist: RD Session Host Installation Prerequisites](#z0c567046010a42d6b95e49e26857de0a) |
|  | Install the RD Session Host role service. | [Installing the RD Session Host Role Service](#z220419f829444c89ac3f7545d42a055d) |
|  | Install and configure the RD Licensing role service. | [Checklist: Deploying a Remote Desktop License Server](#zde72da670f424b92b6e533233a51f9a4) |
|  | Configure the license settings on the RD Session Host server. | [Configuring License Settings on an RD Session Host Server](#zcf2e128a89684118b7792d024cc04ede) |
|  | Configure the Network Level Authentication setting for the RD Session Host server. | [Configuring the Network Level Authentication Setting for an RD Session Host Server](#zbbbe7e354eba4efea9e3e5b858659bba) |
|  | Install programs on the RD Session Host server. | [Installing Programs on an RD Session Host Server](#ze7ab5ba3a2854ba599f7baab30e83ff3) |
|  | Configure the client experience on an RD Session Host server. (Optional) | [Configuring the Client Experience on an RD Session Host Server](#z17539f0c45504cd78b9ff147eae0ad0c) |
|  | Configure users that will remotely connect to the RD Session Host server.  Note  This step is optional if installing and configuring a Virtual Desktop Infrastructure. | [Creating a New User Account](#z90490add342e4453b44daacf81d60ad9)  [Configuring the Remote Desktop Users Group](#z11f0abf70ef548f2a207c56fcdafee9e) |
|  | Verify the functionality of the RD Session Host deployment. | [Verifying Remote Desktop Session Host Functionality](#zb5633f35da6f47779aaf93932feb76c6) |

# Checklist: Deploying a Remote Desktop License Server

This parent checklist includes cross-reference links to important concepts about the Remote Desktop Services design. It also contains links to subordinate checklists that will help you complete the tasks that are required to implement this design.

Note

Complete the tasks in this checklist in order. When a reference link takes you to a procedure, return to this topic after you complete the steps in that procedure so that you can proceed with the remaining tasks in this checklist.

 Checklist: Deploying a Remote Desktop license server

|  |  |  |
| --- | --- | --- |
|  | Task | Reference |
|  | Install the RD Licensing role service. | [Installing the Remote Desktop Licensing Role Service](#zd49bbea26cc549bea9445e5b5b60cf29) |
|  | Activate the Remote Desktop license server. | [Activating the Remote Desktop License Server](#z55c8644804ee4c38b885f1853b6a1565) |
|  | Install Remote Desktop Services client access licenses. | [Installing Remote Desktop Services Client Access Licenses](#zddcb964796d74178901458ec78bf6598) |

# Deploying Remote Desktop Session Host

An RD Session Host server is the server that hosts Windows-based programs or the full Windows desktop for Remote Desktop Services clients. Users can connect to an RD Session Host server to run programs, to save files, and to use network resources on that server. Users can access an RD Session Host server by using Remote Desktop Connection or by using RemoteApp.

Note

Installing the RD Session Host role service on an Active Directory® domain controller is not recommended. For more information, see [Installing RD Session Host on a Domain Controller](#ze0ff9cc653a640cebef772c7ca28d648).

#### Deploying Remote Desktop Session Host

Before you install and configure an RD Session Host server, be sure that you have reviewed the following conceptual topics:

 [Checklist: RD Session Host Installation Prerequisites](#z0c567046010a42d6b95e49e26857de0a)

# Checklist: RD Session Host Installation Prerequisites

This parent checklist includes cross-reference links to important concepts about the Remote Desktop Services design. It also contains links to subordinate checklists that will help you complete the tasks that are required to implement this design.

Note

Complete the tasks in this checklist in order. When a reference link takes you to a procedure, return to this topic after you complete the steps in that procedure so that you can proceed with the remaining tasks in this checklist.

This checklist provides tasks that an administrator should perform before installing and configuring an RD Session Host server.

 Checklist: Remote Desktop Session Host installation prerequisites

|  |  |  |
| --- | --- | --- |
|  | Task | Reference |
|  | Determine if you need an RD Session Host server. | To allow remote connections for administrative purposes only, you do not have to install an RD Session Host server.  For more information about remote connections for administrative purposes, see [Using Remote Desktop](#z790fea658644446d8c839c6393c1e08c). |
|  | Review licensing requirements for an RD Session Host server. | Each user or computing device that connects to an RD Session Host server must have a valid Remote Desktop Services client access license (RDS CAL).  An RD Session Host server running Windows Server 2008 R2 must be configured to use at least a license server running Windows Server 2008, and the license server must have valid RDS CALs installed.  For more information about licensing requirements for Remote Desktop Services, see the Remote Desktop Services Design Guide, to be published on the Windows Server 2008 R2 [Remote Desktop Services TechCenter](http://go.microsoft.com/fwlink/?LinkId=138055) (http://go.microsoft.com/fwlink/?LinkId=138055). |
|  | Decide which programs you want to host on the RD Session Host server. | You should install the RD Session Host role service on the computer before you install any programs that you want to make available to users. If you install the RD Session Host role service on a computer that already has programs installed, some of the existing programs may not work correctly in a multiple user environment. Uninstalling and then reinstalling the affected programs may resolve these issues.  For more information, see [Installing Programs on an RD Session Host Server](#ze7ab5ba3a2854ba599f7baab30e83ff3). |
|  | Review information about:  **** Hardware requirements  **** Capacity and scaling | For hardware requirements, see the Remote Desktop Services Design Guide, to be published on the Windows Server 2008 R2 [Remote Desktop Services TechCenter](http://go.microsoft.com/fwlink/?LinkId=138055) (http://go.microsoft.com/fwlink/?LinkId=138055).  For capacity and scaling, see the [Remote Desktop Session Host Capacity Planning in Windows Server 2008 R2](http://go.microsoft.com/fwlink/?LinkId=192412) (http://go.microsoft.com/fwlink/?LinkId=192412). |
|  | Determine if you need to deploy a load-balanced RD Session Host server farm. | For more information about RD Connection Broker, see the Remote Desktop Services Design Guide, to be published on the Windows Server 2008 R2 [Remote Desktop Services TechCenter](http://go.microsoft.com/fwlink/?LinkId=138055) (http://go.microsoft.com/fwlink/?LinkId=138055). |
|  | Determine the Remote Desktop licensing mode that the RD Session Host server will use. | The Remote Desktop licensing mode configured on an RD Session Host server must match the type of RDS CALs available on the Remote Desktop license server.  For more information, see [Configuring License Settings on an RD Session Host Server](#zcf2e128a89684118b7792d024cc04ede). |
|  | Determine the Remote Desktop license server from which the RD Session Host server will request RDS CALs. | An RD Session Host server must be configured to specify a Remote Desktop license server from which to request RDS CALs for users or computing devices that are connecting to the RD Session Host server.  For more information, see [Configuring License Settings on an RD Session Host Server](#zcf2e128a89684118b7792d024cc04ede). |
|  | Determine which users will be able to remotely connect to the RD Session Host server. | The Remote Desktop Users group on an RD Session Host server is used to give users and groups permission to log on remotely to an RD Session Host server.  For more information, see [Configuring the Remote Desktop Users Group](#z11f0abf70ef548f2a207c56fcdafee9e). |
|  | Determine if you need to deploy an RD Gateway server. | For more information about RD Gateway, see the Remote Desktop Services Design Guide, to be published on the Windows Server 2008 R2 [Remote Desktop Services TechCenter](http://go.microsoft.com/fwlink/?LinkId=138055) (http://go.microsoft.com/fwlink/?LinkId=138055). |
|  | Determine if the RD Session Host server will require Network Level Authentication. | You can enhance RD Session Host server security by providing user authentication earlier in the connection process when a client connects to an RD Session Host server. This early user authentication method is referred to as Network Level Authentication.  For more information, see [Configuring the Network Level Authentication Setting for an RD Session Host Server](#zbbbe7e354eba4efea9e3e5b858659bba). |
|  | Review information about Windows Firewall. | The installation of the Remote Desktop Services role changes the configuration of Windows Firewall.  For more information, see [Remote Desktop Services and Windows Firewall](#z89a42b0c245447a1828345069ba0b092). |

# About Remote Desktop Session Host

## What is Remote Desktop Services?

Remote Desktop Services, formerly Terminal Services, is a server role in Windows Server® 2008 R2 that provides technologies that enable users to access Windows-based programs that are installed on a Remote Desktop Session Host (RD Session Host) server, or to access the full Windows desktop. With Remote Desktop Services, users can access an RD Session Host server from within a corporate network or from the Internet.

Remote Desktop Services lets you efficiently deploy and maintain software in an enterprise environment. You can easily deploy programs from a central location. Because you install the programs on the RD Session Host server and not on the client computer, programs are easier to upgrade and to maintain.

When a user accesses a program on an RD Session Host server, the program runs on the server. Each user sees only their individual session. The session is managed transparently by the server operating system and is independent of any other client session. Additionally, you can configure Remote Desktop Services to use Hyper-V™ to either assign virtual machines to users, or have Remote Desktop Services dynamically assign an available virtual machine to a user upon connection.

## Why use Remote Desktop Services?

If you deploy a program on an RD Session Host server instead of on each device, there are many benefits. These include the following:

 Application deployment: You can quickly deploy Windows-based programs to computing devices across an enterprise. Remote Desktop Services is especially useful when you have programs that are frequently updated, infrequently used, or difficult to manage.

 Application consolidation: Programs are installed and run from an RD Session Host server, eliminating the need for updating programs on client computers. This also reduces the amount of network bandwidth that is required to access programs.

 Remote access: Users can access programs that are running on an RD Session Host server from devices such as home computers, kiosks, low-powered hardware, and operating systems other than Windows.

 Branch office access: Remote Desktop Services provides better program performance for branch office workers who need access to centralized data stores. Data-intensive programs sometimes do not have client/server protocols that are optimized for low-speed connections. Programs of this kind frequently perform better over a Remote Desktop Services connection than over a typical wide area network.

## Remote Desktop Services role services

Remote Desktop Services is a server role that consists of several role services. In Windows Server 2008 R2, Remote Desktop Services consists of the following role services:

 RD Session Host: Remote Desktop Session Host (RD Session Host), formerly Terminal Server, enables a server to host Windows-based programs or the full Windows desktop. Users can connect to an RD Session Host server to run programs, to save files, and to use network resources on that server.

 RD Web Access: Remote Desktop Web Access (RD Web Access), formerly TS Web Access, enables users to access RemoteApp and Desktop Connection through the Start menu on a computer that is running Windows 7 or through a Web browser. RemoteApp and Desktop Connection provides a customized view of RemoteApp programs and virtual desktops to users.

 RD Licensing: Remote Desktop Licensing (RD Licensing), formerly TS Licensing, manages the Remote Desktop Services client access licenses (RDS CALs) that are required for each device or user to connect to an RD Session Host server. You use RD Licensing to install, issue, and track the availability of RDS CALs on a Remote Desktop license server.

 RD Gateway: Remote Desktop Gateway (RD Gateway), formerly TS Gateway, enables authorized remote users to connect to resources on an internal corporate network, from any Internet-connected device.

 RD Connection Broker: Remote Desktop Connection Broker (RD Connection Broker), formerly TS Session Broker, supports session load balancing and session reconnection in a load-balanced RD Session Host server farm. RD Connection Broker is also used to provide users access to RemoteApp programs and virtual desktops through RemoteApp and Desktop Connection.

 RD Virtualization Host: Remote Desktop Virtualization Host (RD Virtualization Host) integrates with Hyper-V to host virtual machines and provide them to users as virtual desktops. You can assign a unique virtual desktop to each user in your organization, or provide them shared access to a pool of virtual desktops.

### What is RD Session Host?

An RD Session Host server is the server that hosts Windows-based programs or the full Windows desktop for Remote Desktop Services clients. Users can connect to an RD Session Host server to run programs, to save files, and to use network resources on that server. Users can access an RD Session Host server by using the Remote Desktop Connection client or by using RemoteApp programs.

### What is RD Web Access?

RD Web Access enables users to access RemoteApp and Desktop Connection through the Start menu on a computer that is running Windows 7 or through a Web browser. RemoteApp and Desktop Connection provides a customized view of RemoteApp programs and virtual desktops to users.

When a user starts a RemoteApp program, a Remote Desktop Services session is started on the RD Session Host server that hosts the RemoteApp program. If a user connects to a virtual desktop, a remote desktop connection is made to a virtual machine that is running on an RD Virtualization Host server.

To configure which RemoteApp programs and virtual desktops will be available through RemoteApp and Desktop Connection, you must install the RD Connection Broker role service on a computer that is running Windows Server 2008 R2, and then use the Remote Desktop Connection Manager tool.

You can also use RD Web Access if you only want to make RemoteApp programs on an RD Session Host server available to users through a Web browser.

### What is RD Licensing?

RD Licensing manages the RDS CALs that are required for each user or device to connect to an RD Session Host server. You use RD Licensing to install, issue, and track the availability of RDS CALs on a Remote Desktop license server.

To use Remote Desktop Services, you must have at least one license server. For small deployments, you can install both the RD Session Host role service and the RD Licensing role service on the same computer. For larger deployments, it is recommended that the RD Licensing role service be installed on a separate computer from the RD Session Host role service.

You must configure RD Licensing correctly for your RD Session Host server to continue to accept connections from clients.

### What is RD Gateway?

RD Gateway enables authorized remote users to connect to resources on an internal corporate network, from any Internet-connected device. The network resources can be RD Session Host servers running RemoteApp programs [hosting line-of-business (LOB) applications], virtual desktops, or computers with Remote Desktop enabled. RD Gateway encapsulates RDP over HTTPS to help form a secure, encrypted connection between users on the Internet and the internal network resources on which their productivity applications run.

#### Why use RD Gateway?

RD Gateway provides these benefits:

 RD Gateway enables remote users to connect to internal network resources over the Internet by using an encrypted connection, without needing to configure virtual private network (VPN) connections.

 RD Gateway provides a comprehensive security configuration model that enables you to control access to specific internal network resources.

 RD Gateway enables remote users to connect to internal network resources that are hosted behind firewalls in private networks and across network address translators (NATs).

 Remote Desktop Gateway Manager (RD Gateway Manager) enables you to configure authorization policies to define conditions that must be met for remote users to connect to internal network resources.

 RD Gateway Manager provides tools to help you monitor RD Gateway connection status, health, and events.

 You can configure RD Gateway servers and Remote Desktop Services clients to use Network Access Protection (NAP) to enhance security.

 You can use an RD Gateway server with Microsoft Internet Security and Acceleration (ISA) Server to further enhance security.

### What is RD Connection Broker?

RD Connection Broker keeps track of user sessions in a load-balanced RD Session Host server farm. The RD Connection Broker database stores session state information that includes session IDs, their associated user names, and the name of the server where each session resides. When a user with an existing session connects to an RD Session Host server in the load-balanced farm, RD Connection Broker redirects the user to the RD Session Host server where their session exists. This prevents the user from being connected to a different server in the farm and starting a new session.

If the RD Connection Broker Load Balancing feature is enabled, RD Connection Broker also tracks the number of user sessions on each RD Session Host server in the farm, and redirects users who do not have an existing session to the server with the fewest sessions. This functionality enables you to evenly distribute the session load between servers in a load-balanced RD Session Host server farm.

RD Connection Broker is also used to provide users with access to RemoteApp and Desktop Connection. RemoteApp and Desktop Connection provides a customized view of RemoteApp programs and virtual desktops to users. RD Connection Broker supports load balancing and reconnection to existing sessions on virtual desktops accessed by using RemoteApp and Desktop Connection.

To configure RemoteApp and Desktop Connection, use the Remote Desktop Connection Manager tool on the RD Connection Broker server.

### What is RD Virtualization Host?

RD Virtualization Host integrates with Hyper-V to provide virtual machines by using RemoteApp and Desktop Connection. RD Virtualization Host can be configured so that each user in your organization is assigned a unique virtual desktop, or users are redirected to a shared pool where a virtual desktop is dynamically assigned.

RD Virtualization Host requires RD Connection Broker to determine where the user is redirected. If a user is assigned a personal virtual desktop, RD Connection Broker will redirect the user to this virtual machine. If the virtual machine is not turned on, RD Virtualization Host turns the virtual machine on and then connects the user to the personal virtual desktop. If the user is connecting to a shared virtual machine pool, RD Connection Broker will first check to see if the user has a disconnected session in the pool. If the user has a disconnected session, they are reconnected to that virtual desktop. If the user does not have a disconnected session, a virtual desktop in that pool is dynamically assigned to the user.

# Using Remote Desktop

To allow remote connections for administrative purposes only, you do not have to install the RD Session Host role service. Instead, you can enable Remote Desktop on the computer that you want to remotely administer.

Note

Remote Desktop supports only two concurrent remote connections to the computer. You do not need Remote Desktop Services client access licenses (RDS CALs) for these connections.

You can use the following procedure to enable Remote Desktop on a Windows Server 2008 R2 computer.

Membership in the local Administrators group, or equivalent, on the computer that you plan to configure, is the minimum required to complete this procedure.

To enable Remote Desktop

|  |
| --- |
| 1. Start the System tool. To start the System tool, click Start, click Run, type control system and then click OK.  2. Under Tasks, click Remote settings.  3. In the System Properties dialog box, on the Remote tab, click either of the following, depending on your environment:   Allow connections from computers running any version of Remote Desktop (less secure)   Allow connections only from computers running Remote Desktop with Network Level Authentication (more secure)  For more information about the two options, click the Help me choose link on the Remote tab.  4. Click Select Users to add the users and groups that need to connect to the computer by using Remote Desktop. The users and groups that you add are added to the Remote Desktop Users group.  Note  Members of the local Administrators group can connect even if they are not listed. |

# Installing RD Session Host on a Domain Controller

Installing the RD Session Host role service on an Active Directory domain controller is not recommended. Allowing users to run programs on a domain controller could create security risks and performance issues.

If the RD Session Host role service is installed on a domain controller, the security settings of the domain controller will need to be adjusted to allow users to have remote access to the server. This remote access is controlled by the Allow logon through Remote Desktop Services user rights assignment, which can be configured by using the Group Policy Management Console (GPMC).

On a domain controller, by default, only the Administrators group is granted the Allow logon through Remote Desktop Services user right. To allow remote access to the RD Session Host server for users who are not members of the Administrators group, you should grant the Remote Desktop Users group the Allow logon through Remote Desktop Services user right.

For more information about using GPMC to configure user rights assignments, see the Group Policy Management Console Help in Windows Server 2008 R2.

For more information about licensing requirements for Remote Desktop Services, see the Remote Desktop Services Design Guide to be published on the Windows Server 2008 R2 [Remote Desktop Services TechCenter](http://go.microsoft.com/fwlink/?LinkId=138055) (http://go.microsoft.com/fwlink/?LinkId=138055).

# Remote Desktop Services and Windows Firewall

The Windows Firewall is on by default in Windows Server 2008 and Windows Server 2008 R2. Windows Firewall helps control which programs or ports can be used to communicate between the Windows Server 2008 or Windows Server 2008 R2 server and other computers on the network or the Internet. To allow a program or port to communicate through Windows Firewall, an exception needs to be enabled.

If you enable Remote Desktop, Windows Firewall automatically enables the Remote Desktop exception.

When the RD Session Host role service is installed, Windows Firewall automatically enables the following exceptions:

 Remote Desktop

 Remote Desktop Services

If you install other Remote Desktop Services role services, Windows Firewall will automatically enable other exceptions. For example, when you install the RD Licensing role service, Windows Firewall enables the Remote Desktop Licensing Server exception.

When you uninstall (remove) a role service from the computer, Windows Firewall automatically removes the exception for that role service.

Important

When the RD Session Host role service is uninstalled (removed), only the Remote Desktop Services exception is removed. The Remote Desktop exception is not removed.

Use the following procedure to view Windows Firewall exceptions.

Membership in the local Administrators group, or equivalent, is the minimum required to complete this procedure.

To view Windows Firewall exceptions

|  |
| --- |
| 1. Click Start, and then click Control Panel.  2. Click System and Security, and then click Windows Firewall.  3. Click Allow a program or feature through Windows Firewall.  4. If the check box associated with the program or port listed is selected, the Windows Firewall exception for that program or port is enabled.  Some programs only appear in the list when the role service is installed. For example, the Remote Desktop Licensing Server exception only appears in the list when the RD Licensing role service is installed on the computer. |

To view more detailed information about Windows Firewall settings, use the Windows Firewall with Advanced Security snap-in.

Use the following procedure to use Windows Firewall with Advanced Security.

Membership in the local Administrators group, or equivalent, is the minimum required to complete this procedure.

To use the Windows Firewall with Advanced Security snap-in

|  |
| --- |
| 1. Click Start, point to Administrative Tools, and then click Windows Firewall with Advanced Security.  2. To view detailed information about Windows Firewall settings, click either of the following nodes in the left pane:   Inbound rules   Outbound rules |

For more information about configuring Windows Firewall, see the Windows Firewall with Advanced Security Help in Windows Server 2008 R2.

### Additional references

 [Using Remote Desktop](#z790fea658644446d8c839c6393c1e08c)

 [Installing the RD Session Host Role Service](#z220419f829444c89ac3f7545d42a055d)

 [Checklist: RD Session Host Installation Prerequisites](#z0c567046010a42d6b95e49e26857de0a)

# Installing the RD Session Host Role Service

In Windows Server 2008 R2, you can use Server Manager to install the RD Session Host role service. Use the following procedure to install the RD Session Host role service by using Server Manager if Remote Desktop Services is not already installed on the server. If Remote Desktop Services is already installed on the server, see [Install the Remote Desktop Session Host role service (when Remote Desktop Services is already installed)](#z1).

Membership in the local Administrators group, or equivalent, is the minimum required to complete this procedure. Review details about using the appropriate accounts and group memberships at [Local and Domain Default Groups](http://go.microsoft.com/fwlink/?LinkId=83477) (http://go.microsoft.com/fwlink/?LinkId=83477).

## Install the Remote Desktop Session Host role service

To install the RD Session Host role service

|  |
| --- |
| 1. Open Server Manager. To open Server Manager, click Start, point to Administrative Tools, and then click Server Manager.  2. In the left pane, right-click Roles, and then click Add Roles.  3. In the Add Roles Wizard, on the Before You Begin page, click Next.  4. On the Select Server Roles page, under Roles, select the Remote Desktop Services check box.  Note  If Remote Desktop Services is already installed on the server, the Remote Desktop Services check box will be selected and dimmed, and followed by “(Installed).”  5. Click Next.  6. On the Remote Desktop Services page, click Next.  7. On the Select Role Services page, select the Remote Desktop Session Host check box, and then click Next.  Note  If you are installing the RD Session Host role service on a domain controller, you will receive a warning message because installing the RD Session Host role service on a domain controller is not recommended. For more information, see [Installing RD Session Host on a Domain Controller](#ze0ff9cc653a640cebef772c7ca28d648).  8. On the Uninstall and Reinstall Applications for Compatibility page, click Next.  9. On the Specify Authentication Method for Remote Desktop Session Host page, select the appropriate authentication method for the RD Session Host server, and then click Next. For more information about authentication methods, see [Configuring the Network Level Authentication Setting for an RD Session Host Server](#zbbbe7e354eba4efea9e3e5b858659bba).  10. On the Specify Licensing Mode page, select the appropriate licensing mode for the RD Session Host server, and then click Next. For more information about licensing modes, see [Configuring License Settings on an RD Session Host Server](#zcf2e128a89684118b7792d024cc04ede).  11. On the Select User Groups Allowed Access To This RD Session Host Server page, add the users or user groups that you want to be able to remotely connect to this RD Session Host server, and then click Next. For more information, see [Configuring the Remote Desktop Users Group](#z11f0abf70ef548f2a207c56fcdafee9e).  12. On the Configure Client Experience page, select the functionality that you want to be available to remote clients that are connected by using this RD Session Host server, and then click Next. For more information, see [Configuring the Client Experience on an RD Session Host Server](#z17539f0c45504cd78b9ff147eae0ad0c).  13. On the Confirm Installation Selections page, verify that the RD Session Host role service will be installed, and then click Install.  14. On the Installation Progress page, installation progress will be noted.  15. On the Installation Results page, you are prompted to restart the server to finish the installation process. Click Close, and then in the Add Roles Wizard window, click Yes to restart the server.  16. If you are prompted that other programs are still running, do either of the following:   To close the programs manually and restart the server later, click Cancel.   To automatically close the programs and restart the server, click Restart now.  17. After the server restarts and you log on to the computer, the remaining steps of the installation will finish. When the Installation Results page appears, confirm that the installation of RD Session Host succeeded.  You can also confirm that RD Session Host is installed by following these steps:  a. Start Server Manager.  b. Under Roles Summary, click Remote Desktop Services.  c. Under System Services, confirm that the status for Remote Desktop Services is Running.  d. Under Role Services, confirm that the status for Remote Desktop Session Host is Installed. |

## Install the Remote Desktop Session Host role service (when Remote Desktop Services is already installed)

Use the following procedure to install the RD Session Host role service when Remote Desktop Services is already installed on the server.

Membership in the local Administrators group, or equivalent, on the RD Session Host server that you plan to configure, is the minimum required to complete this procedure.

Important

The installation of the RD Session Host role service requires the computer to be restarted.

To install the Remote Desktop Session Host role service when Remote Desktop Services is already installed

|  |
| --- |
| 1. Open Server Manager. To open Server Manager, click Start, point to Administrative Tools, and then click Server Manager.  2. In the left pane, expand Roles.  3. Right-click Remote Desktop Services, and then click Add Role Services.  4. On the Select Role Services page, select the Remote Desktop Session Host check box, and then click Next.  Note  If you are installing the RD Session Host role service on a domain controller, you will receive a warning message because installing the RD Session Host role service on a domain controller is not recommended. For more information, see [Installing RD Session Host on a Domain Controller](#ze0ff9cc653a640cebef772c7ca28d648).  5. On the Uninstall and Reinstall Applications for Compatibility page, click Next.  6. On the Specify Authentication Method for Remote Desktop Session Host page, select the appropriate authentication method for the RD Session Host server, and then click Next. For more information about authentication methods, see [Configuring the Network Level Authentication Setting for an RD Session Host Server](#zbbbe7e354eba4efea9e3e5b858659bba).  7. On the Specify Licensing Mode page, select the appropriate licensing mode for the RD Session Host server, and then click Next. For more information about licensing modes, see [Configuring License Settings on an RD Session Host Server](#zcf2e128a89684118b7792d024cc04ede).  8. On the Select User Groups Allowed Access To This RD Session Host page, add the users or user groups that you want to be able to remotely connect to this RD Session Host server, and then click Next. For more information, see Configure the Remote Desktop Users Group.  9. On the Configure Client Experience page, select the functionality that you want to be available to remote clients that are connected by using this RD Session Host server, and then click Next. For more information, see [Configuring the Client Experience on an RD Session Host Server](#z17539f0c45504cd78b9ff147eae0ad0c).  10. On the Confirm Installation Selections page, verify that the RD Session Host role service will be installed, and then click Install.  11. On the Installation Progress page, installation progress will be noted.  12. On the Installation Results page, you are prompted to restart the server to finish the installation process. Click Close, and then in the Add Roles Wizard window, click Yes to restart the server.  13. If you are prompted that other programs are still running, do either of the following:   To close the programs manually and restart the server later, click Cancel.   To automatically close the programs and restart the server, click Restart now.  14. After the server restarts and you log on to the computer, the remaining steps of the installation will finish. When the Installation Results page appears, confirm that the installation of RD Session Host succeeded.  You can also confirm that RD Session Host is installed by following these steps:  a. Start Server Manager.  b. Under Roles Summary, click Remote Desktop Services.  c. Under System Services, confirm that the status for Remote Desktop Services is Running.  d. Under Role Services, confirm that the status for Remote Desktop Session Host is Installed. |

# Configuring the Network Level Authentication Setting for an RD Session Host Server

Network Level Authentication can be used to enhance RD Session Host server security by requiring that the user be authenticated to an RD Session Host server before a session is created.

Network Level Authentication is an authentication method that completes user authentication before you establish a remote desktop connection and the logon screen appears. This is a more secure authentication method that can help protect the remote computer from malicious users and malicious software. The advantages of Network Level Authentication are:

 It requires fewer remote computer resources initially. The remote computer uses a limited number of resources before authenticating the user, rather than starting a full remote desktop connection as in previous versions.

 It can help provide better security by reducing the risk of denial-of-service attacks.

To use Network Level Authentication, you must meet the following requirements:

 The client computer must be using at least Remote Desktop Connection 6.0.

 The client computer must be using an operating system, such as Windows® 7 or Windows Vista®, that supports the Credential Security Support Provider (CredSSP) protocol.

 The RD Session Host server must be using Windows Server 2008 R2 or Windows Server 2008.

You can configure an RD Session Host server to only support connections from clients running Network Level Authentication. The Network Level Authentication setting for an RD Session Host server can be set in the following ways:

 During the installation of the RD Session Host role service in Server Manager, on the Specify Authentication Method for Remote Desktop Session Host page in the Add Roles Wizard.

 On the Remote tab in the System Properties dialog box on an RD Session Host server.

If the Allow connections from computers running any version of Remote Desktop (less secure) is not selected and not enabled, the Require user authentication for remote connections by using Network Level Authentication Group Policy setting has been enabled and has been applied to the RD Session Host server.

 On the General tab of the Properties dialog box for a connection in the Remote Desktop Session Host Configuration tool by selecting the Allow connections only from computers running Remote Desktop with Network Level Authentication check box.

If the Allow connections only from computers running Remote Desktop with Network Level Authentication check box is selected and is dimmed, the Require user authentication for remote connections by using Network Level Authentication Group Policy setting has been enabled and has been applied to the RD Session Host server.

 By applying the Require user authentication for remote connections by using Network Level Authentication Group Policy setting.

This Group Policy setting is located in Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Security and can be configured by using either the Local Group Policy Editor or the Group Policy Management Console (GPMC). Note that the Group Policy setting will take precedence over the setting configured in Remote Desktop Session Host Configuration or on the Remote tab.

To determine whether a computer is running a version of Remote Desktop Connection that supports Network Level Authentication, start Remote Desktop Connection, click the icon in the upper-left corner of the Remote Desktop Connection dialog box, and then click About. In the About Remote Desktop Connection dialog box, look for the phrase Network Level Authentication supported.

For more information about Network Level Authentication and Remote Desktop Services, see the [Remote Desktop Services](http://go.microsoft.com/fwlink/?LinkID=138055) page on the Windows Server 2008 R2 TechCenter (http://go.microsoft.com/fwlink/?LinkID=138055).

For more information about Group Policy settings for Remote Desktop Services, see the [Remote Desktop Services Technical Reference](http://go.microsoft.com/fwlink/?LinkId=138134) (http://go.microsoft.com/fwlink/?LinkId=138134).

# Installing Programs on an RD Session Host Server

You should install the RD Session Host role service on the computer before you install any programs that you want to make available to users. If you install the RD Session Host role service on a computer that already has programs installed, some of the existing programs may not work correctly in a multiuser environment. Uninstalling and then reinstalling the affected programs may resolve these issues.

To ensure that an application is installed correctly to work in a multiuser environment, you must put the RD Session Host server into a special installation mode before you install the application on the RD Session Host server. This special installation mode ensures that the correct registry entries and .ini files that are needed to support running the application in a multiuser environment are created during the installation process.

You can put an RD Session Host server into this special installation mode by using either of the following:

 Install Application on Remote Desktop Session Host tool under Programs in Control Panel. This tool will run a wizard to help install the application.

 Change user /install command at a command prompt. You will have to start the installation of the application manually.

After the application is installed, you must put the RD Session Host server into execution mode before remote users begin using the application. The Install Application on Remote Desktop Session Host tool will automatically put the RD Session Host server into execution mode when it is finished running. To put the RD Session Host server into execution mode from a command prompt, use the change user /execute command.

#### Additional considerations

 Some programs may require minor setup modifications to run correctly on an RD Session Host server.

 If you have programs that are related to each other or have dependencies on each other, you should install the programs on the same RD Session Host server. For example, you should install Microsoft Office as a suite on the same RD Session Host server instead of installing individual Office programs on separate RD Session Host servers.

 You should consider installing individual programs on separate RD Session Host servers in the following circumstances:

 The program has compatibility issues that may affect other programs.

 A single program and the number of associated users may fill server capacity.

 For more information about command-line tools for Remote Desktop Services, see the [Remote Desktop Services Technical Reference](http://go.microsoft.com/fwlink/?LinkId=138135) (http://go.microsoft.com/fwlink/?LinkId=138135).

 For more information about RD Session Host, see the [Remote Desktop Services page](http://go.microsoft.com/fwlink/?LinkId=140438) on the Windows Server 2008 R2 TechCenter (http://go.microsoft.com/fwlink/?LinkId=140438).

# Configuring the Remote Desktop Users Group

The Remote Desktop Users group on an RD Session Host server is used to give users and groups permission to remotely connect to an RD Session Host server.

You can add users and groups to the Remote Desktop Users group in the following ways:

 Local Users and Groups snap-in

 Active Directory Users and Computers snap-in, if the RD Session Host server is installed on a domain controller

 On the Remote tab in the System Properties dialog box on an RD Session Host server

You can use the following procedure to add users and groups to the Remote Desktop Users group by using the Remote tab in the System Properties dialog box on an RD Session Host server.

Membership in the local Administrators group, or equivalent, on the RD Session Host server that you plan to configure, is the minimum required to complete this procedure.

To add users and groups to the Remote Desktop Users group by using the Remote tab

|  |
| --- |
| 1. Start the System tool. To start the System tool, click Start, click Run, type control system and then click OK.  2. Under Tasks, click Remote settings.  3. In the System Properties dialog box, on the Remote tab, click Select Users. Add the users or groups that need to connect to the RD Session Host server or to the virtual machine by using Remote Desktop. The users and groups that you add are added to the Remote Desktop Users group.  Note  Members of the local Administrators group can connect even if they are not listed.  If you select Don't allow connections to this computer on the Remote tab, no users will be able to connect remotely to this computer, even if they are members of the Remote Desktop Users group. |

# Configuring the Client Experience on an RD Session Host Server

You can configure a Remote Desktop Session Host (RD Session Host) server so that users connecting to a remote desktop session can use functionality similar to that provided by Windows 7.

Important

Providing this functionality requires additional system and bandwidth resources and may affect the scalability of the RD Session Host server.

During the installation of the RD Session Host role service in Server Manager, you can automatically configure the following functionality on the Configure Client Experience page in the Add Roles Wizard:

 Audio and video playback

 Audio recording redirection

 Desktop composition

If you configure the RD Session Host server to provide audio and video playback or desktop composition, the Desktop Experience feature will be installed on the RD Session Host server. For more information about Desktop Experience, see [Desktop Experience Feature](#zc7148b8917cc4666a7e13bd14946adf1).

To manually configure this functionality, see the following topics:

 [Configure Audio and Video Playback on an RD Session Host Server](#z53b14f633afe48eeb4c98a8006f531c8)

 [Configure Audio Recording Redirection on an RD Session Host Server](#z5baeba39a1824b559f0136e08cbe2f6d)

 [Configure Desktop Composition on an RD Session Host Server](#zfa4cffbf137845ac905a5886b849e2a8)

# Desktop Experience Feature

The Desktop Experience feature allows you to install a variety of components and features that are provided in the Windows 7 operating system onto a computer that is running the Windows Server 2008 R2 operating system. After you install Desktop Experience, the Windows 7 components and features, such as Windows Media Player, will appear under All Programs on the Start menu.

Note

Installing Desktop Experience does not automatically turn on any of its features or components. After installing Desktop Experience, you must manually enable or configure the features or components.

For information about installing Desktop Experience, see [Install Desktop Experience on an RD Session Host Server](#zd606d62e7b814201abd714f0f1226abd).

## What’s in the Desktop Experience feature

Desktop Experience includes the following Windows 7 components and features:

 Windows Media Player

 Desktop themes

 Video for Windows (AVI support)

 Windows SideShow

 Windows Defender

 Disk Cleanup

 Sync Center

 Sound Recorder

 Character Map

 Snipping Tool

# Install Desktop Experience on an RD Session Host Server

When a user uses Remote Desktop Connection to connect to a Remote Desktop Session Host (RD Session Host) server, the desktop that exists on the RD Session Host server is reproduced, by default, in the remote session. To make the remote session look and feel more like the user's local Windows 7 desktop experience, install the Desktop Experience feature on an RD Session Host server that is running Windows Server 2008 R2.

Desktop Experience installs components and features of Windows 7, such as Windows Media Player, Windows Defender, and Windows Calendar. For more information about Desktop Experience, see [Desktop Experience Feature](#zc7148b8917cc4666a7e13bd14946adf1).

## Install Desktop Experience

Use the following procedure to install Desktop Experience on the server.

Membership in the local Administrators group, or equivalent, on the RD Session Host server that you plan to configure, is the minimum required to complete this procedure. Review details about using the appropriate accounts and group memberships at [Local and Domain Default Groups](http://go.microsoft.com/fwlink/?LinkId=83477) (http://go.microsoft.com/fwlink/?LinkId=83477).

Important

The installation of Desktop Experience requires the computer to be restarted.

To install Desktop Experience

|  |
| --- |
| 1. Open Server Manager. Click Start, point to Administrative Tools, and then click Server Manager.  2. In the left pane, click Features, and then in the Features Summary section, click Add Features.  3. On the Select Features page, select the Desktop Experience check box.  4. Review the information about the required features that need to be installed with the Desktop Experience feature, and then click Add Required Features.  5. Click Next.  6. On the Confirm Installation Selections page, verify that the Desktop Experience feature will be installed, and then click Install.  7. On the Installation Progress page, installation progress will be noted.  8. On the Installation Results page, you are prompted to restart the server to finish the installation process. Click Close, and then click Yes to restart the server.  9. After the server restarts and you log on to the computer with the same user account, the remaining steps of the installation will finish. When the Installation Results page appears, confirm that the installation of Desktop Experience succeeded, and then click Close.  You can also confirm that Desktop Experience is installed by following these steps:  a. Start Server Manager.  b. In the left pane, click Features, and then in the Features Summary section, confirm that Desktop Experience is listed as installed. |

After you install Desktop Experience, the Windows 7 components and features, such as Windows Media Player, will appear under All Programs on the Start menu.

## Uninstall (Remove) Desktop Experience

Use the following procedure to uninstall (remove) Desktop Experience from the server.

Membership in the local Administrators group, or equivalent, on the RD Session Host server that you plan to configure, is the minimum required to complete this procedure. Review details about using the appropriate accounts and group memberships at [Local and Domain Default Groups](http://go.microsoft.com/fwlink/?LinkId=83477) (http://go.microsoft.com/fwlink/?LinkId=83477).

Important

The removal of Desktop Experience from the server requires the computer to be restarted.

To uninstall (remove) Desktop Experience

|  |
| --- |
| 1. Open Server Manager. Click Start, point to Administrative Tools, and then click Server Manager.  2. In the left pane, click Features, and then in the Features Summary section, click Remove Features.  3. On the Select Features page, clear the Desktop Experience check box, and then click Next.  4. On the Confirm Removal Selections page, verify that the Desktop Experience feature will be removed, and then click Remove.  5. On the Removal Progress page, removal progress will be noted.  6. On the Removal Results page, you are prompted to restart the server to finish the removal process. Click Close, and then click Yes to restart the server.  7. After the server restarts and you log on to the computer with the same user account, the remaining steps of the removal process will finish. When the Removal Results page appears, confirm that the removal of Desktop Experience succeeded, and then click Close.  You can also confirm that Desktop Experience is removed by following these steps:  a. Start Server Manager.  b. In the left pane, click Features, and then in the Features Summary section, confirm that Desktop Experience is no longer listed as installed. |

# Configure Audio and Video Playback on an RD Session Host Server

Audio and video playback allows users to redirect the remote computer’s audio in a remote session, and provides an improved experience for video playback in remote sessions. By default, audio and video playback is not allowed when connecting to a computer running Windows Server 2008 R2.

Note

Users can specify where to play the remote computer’s audio output by configuring the remote audio settings on the Local Resources tab in Remote Desktop Connection (RDC). Video playback can be configured by using the videoplayback setting in a Remote Desktop Protocol (.rdp) file. By default, video playback is enabled.

## Manually configuring audio and video playback

To manually configure audio and video playback on a Remote Desktop Session Host (RD Session Host) server, you need to do the following:

 Install the Desktop Experience feature.

 Start the Windows Audio service.

 Enable the Allow audio and video playback redirection Group Policy setting.

 Set the maximum color depth to 32 bits per pixel.

### Install the Desktop Experience feature

For information about installing Desktop Experience, see [Install Desktop Experience on an RD Session Host Server](#zd606d62e7b814201abd714f0f1226abd).

### Start the Windows Audio service

Use the following procedure to start the Windows Audio service on the RD Session Host server.

Membership in the local Administrators group, or equivalent, on the RD Session Host server that you plan to configure, is the minimum required to complete this procedure. Review details about using the appropriate accounts and group memberships at [Local and Domain Default Groups](http://go.microsoft.com/fwlink/?LinkId=83477) (http://go.microsoft.com/fwlink/?LinkId=83477).

To start the Windows Audio service

|  |
| --- |
| 1. On the RD Session Host server, open the Services snap-in. To open the Services snap-in, click Start, point to Administrative Tools, and then click Services.  2. If the User Account Control dialog box appears, confirm that the action it displays is what you want, and then click Continue.  3. In the Services pane, right-click Windows Audio, and then click Properties.  4. On the General tab, in the Startup type box, select Automatic, and then click Apply.  5. Under Service status, click Start.  6. Click OK to close the Windows Audio Properties dialog box.  7. Confirm that the Status column for the Windows Audio service displays Started. |

### Enable the Allow audio and video playback redirection Group Policy setting

To allow audio and video playback when connecting to a computer running Windows Server 2008 R2, you must enable the Allow audio and video playback redirection Group Policy setting. The Allow audio and video playback redirection Group Policy setting is located in Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Device and Resource Redirection and can be configured by using either Local Group Policy Editor or the Group Policy Management Console (GPMC).

For more information about Group Policy settings for Remote Desktop Services, see the [Remote Desktop Services Technical Reference](http://go.microsoft.com/fwlink/?LinkId=138134) (http://go.microsoft.com/fwlink/?LinkId=138134).

### Set the maximum color depth to 32 bits per pixel

Use the following procedure to set the maximum color depth to 32 bits per pixel on the RD Session Host server.

Membership in the local Administrators group, or equivalent, on the RD Session Host server that you plan to configure, is the minimum required to complete this procedure. Review details about using the appropriate accounts and group memberships at [Local and Domain Default Groups](http://go.microsoft.com/fwlink/?LinkId=83477) (http://go.microsoft.com/fwlink/?LinkId=83477).

To set the maximum color depth to 32 bits per pixel

|  |
| --- |
| 1. On the RD Session Host server, open Remote Desktop Session Host Configuration. To open Remote Desktop Session Host Configuration, click Start, point to Administrative Tools, point to Remote Desktop Services, and then click Remote Desktop Session Host Configuration.  2. If the User Account Control dialog box appears, confirm that the action it displays is what you want, and then click Continue.  3. Under Connections, right-click the name of the connection that you want to configure (for example, RDP-Tcp), and then click Properties.  4. On the Client Settings tab, in the Limit Maximum Color Depth box, select 32 bits per pixel.  5. Click OK. Changes to color depth settings are not applied to sessions that are connected when the change is made. The changes will take effect the next time the user establishes a new connection to the RD Session Host server. |

You can also set the maximum color depth by applying the Limit maximum color depth Group Policy setting. This Group Policy setting is located in Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Remote Session Environment and can be configured by using either Local Group Policy Editor or the Group Policy Management Console (GPMC). Note that the Group Policy setting will take precedence over the setting configured in Remote Desktop Session Host Configuration.

For more information about Group Policy settings for Remote Desktop Services, see the [Remote Desktop Services Technical Reference](http://go.microsoft.com/fwlink/?LinkId=138134) (http://go.microsoft.com/fwlink/?LinkId=138134).

# Configure Audio Recording Redirection on an RD Session Host Server

Audio recording redirection allows users to record audio to the remote computer in a remote session. By default, audio recording redirection is not allowed when connecting to a computer running Windows Server 2008 R2.

Note

Users can specify whether to record audio to the remote computer by configuring the remote audio settings on the Local Resources tab in Remote Desktop Connection (RDC). Users can record audio by using an audio input device on the local computer, such as a built-in microphone.

## Manually configuring audio recording redirection

To manually configure audio recording redirection on a Remote Desktop Session Host (RD Session Host) server, you need to do the following:

 Start the Windows Audio service.

 Enable the Allow audio recording redirection Group Policy setting.

### Start the Windows Audio service

Use the following procedure to start the Windows Audio service on the RD Session Host server.

Membership in the local Administrators group, or equivalent, on the RD Session Host server that you plan to configure, is the minimum required to complete this procedure. Review details about using the appropriate accounts and group memberships at [Local and Domain Default Groups](http://go.microsoft.com/fwlink/?LinkId=83477) (http://go.microsoft.com/fwlink/?LinkId=83477).

To start the Windows Audio service

|  |
| --- |
| 1. On the RD Session Host server, open the Services snap-in. To open the Services snap-in, click Start, point to Administrative Tools, and then click Services.  2. If the User Account Control dialog box appears, confirm that the action it displays is what you want, and then click Continue.  3. In the Services pane, right-click Windows Audio, and then click Properties.  4. On the General tab, in the Startup type box, select Automatic, and then click Apply.  5. Under Service status, click Start.  6. Click OK to close the Windows Audio Properties dialog box.  7. Confirm that the Status column for the Windows Audio service displays Started. |

### Enable the Allow audio recording redirection Group Policy setting

To allow audio recording redirection when connecting to a computer running Windows Server 2008 R2, you must enable the Allow audio recording redirection Group Policy setting. The Allow audio recording redirection Group Policy setting is located in Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Device and Resource Redirection and can be configured by using either Local Group Policy Editor or the Group Policy Management Console (GPMC).

For more information about Group Policy settings for Remote Desktop Services, see the [Remote Desktop Services Technical Reference](http://go.microsoft.com/fwlink/?LinkId=138134) (http://go.microsoft.com/fwlink/?LinkId=138134).

# Configure Desktop Composition on an RD Session Host Server

Desktop composition provides the user interface elements of Windows Aero, such as translucent windows, for remote desktop sessions. By default, desktop composition is not allowed when connecting to a computer running Windows Server 2008 R2.

Important

Because Windows Aero requires additional system and bandwidth resources, allowing desktop composition for remote desktop sessions can reduce connection performance, particularly over slow links, and increase the load on the Remote Desktop Session Host (RD Session Host) server.

Desktop composition is not available for RemoteApp sessions. In addition, the client computer must have the necessary hardware to support Windows Aero features.

## Manually configuring desktop composition

To manually configure desktop composition on an RD Session Host server, you need to do the following:

 Install the Desktop Experience feature.

 Start the Themes service.

 Enable the Allow desktop composition for remote desktop sessions Group Policy setting.

 Set the maximum color depth to 32 bits per pixel.

### Install the Desktop Experience feature

For information about installing Desktop Experience, see [Install Desktop Experience on an RD Session Host Server](#zd606d62e7b814201abd714f0f1226abd).

### Start the Themes service

Use the following procedure to start the Themes service on the RD Session Host server.

Membership in the local Administrators group, or equivalent, on the RD Session Host server that you plan to configure, is the minimum required to complete this procedure. Review details about using the appropriate accounts and group memberships at [Local and Domain Default Groups](http://go.microsoft.com/fwlink/?LinkId=83477) (http://go.microsoft.com/fwlink/?LinkId=83477).

To start the Themes service

|  |
| --- |
| 1. On the RD Session Host server, open the Services snap-in. To open the Services snap-in, click Start, point to Administrative Tools, and then click Services.  2. If the User Account Control dialog box appears, confirm that the action it displays is what you want, and then click Continue.  3. In the Services pane, right-click Themes, and then click Properties.  4. On the General tab, in the Startup type box, select Automatic, and then click Apply.  5. Under Service status, click Start.  6. Click OK to close the Themes Properties dialog box.  7. Confirm that the Status column for the Themes service displays Started. |

### Enable the Allow desktop composition for remote desktop sessions Group Policy setting

To allow desktop composition when connecting to a computer running Windows Server 2008 R2, you must enable the Allow desktop composition for remote desktop sessions Group Policy setting. The Allow desktop composition for remote desktop sessions Group Policy setting is located in Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Remote Session Environment and can be configured by using either Local Group Policy Editor or the Group Policy Management Console (GPMC).

For more information about Group Policy settings for Remote Desktop Services, see the [Remote Desktop Services Technical Reference](http://go.microsoft.com/fwlink/?LinkId=138134) (http://go.microsoft.com/fwlink/?LinkId=138134).

### Set the maximum color depth to 32 bits per pixel

Use the following procedure to set the maximum color depth to 32 bits per pixel on the RD Session Host server.

Membership in the local Administrators group, or equivalent, on the RD Session Host server that you plan to configure, is the minimum required to complete this procedure. Review details about using the appropriate accounts and group memberships at [Local and Domain Default Groups](http://go.microsoft.com/fwlink/?LinkId=83477) (http://go.microsoft.com/fwlink/?LinkId=83477).

To set the maximum color depth to 32 bits per pixel

|  |
| --- |
| 1. On the RD Session Host server, open Remote Desktop Session Host Configuration. To open Remote Desktop Session Host Configuration, click Start, point to Administrative Tools, point to Remote Desktop Services, and then click Remote Desktop Session Host Configuration.  2. If the User Account Control dialog box appears, confirm that the action it displays is what you want, and then click Continue.  3. Under Connections, right-click the name of the connection that you want to configure (for example, RDP-Tcp), and then click Properties.  4. On the Client Settings tab, in the Limit Maximum Color Depth box, select 32 bits per pixel.  5. Click OK. Changes to color depth settings are not applied to sessions that are connected when the change is made. The changes will take effect the next time the user establishes a new connection to the RD Session Host server. |

You can also set the maximum color depth by applying the Limit maximum color depth Group Policy setting. This Group Policy setting is located in Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Remote Session Environment and can be configured by using either Local Group Policy Editor or the Group Policy Management Console (GPMC). Note that the Group Policy setting will take precedence over the setting configured in Remote Desktop Session Host Configuration.

For more information about Group Policy settings for Remote Desktop Services, see the [Remote Desktop Services Technical Reference](http://go.microsoft.com/fwlink/?LinkId=138134) (http://go.microsoft.com/fwlink/?LinkId=138134).

# Group Policy Settings and Configuring the Client Experience

During the installation of the RD Session Host role service in Server Manager, you can automatically configure the following functionality on the Configure Client Experience page in the Add Roles Wizard:

 Audio and video playback

 Audio recording redirection

 Desktop composition

Server Manager automatically checks that there are no Group Policy settings currently being applied to the computer that would prevent the requested functionality from being correctly configured. If there is a Group Policy setting being applied to the computer that would prevent the requested functionality from being correctly configured, that selection will be dimmed and you will not be able to select the associated check box on the Configure Client Experience page.

The following is a list of Group Policy settings that Server Manager checks:

 Allow audio and video playback redirection

If the Allow audio and video playback redirection Group Policy setting is disabled, you cannot select the Audio and video playback check box on the Configure Client Experience page.

This Group Policy setting is located in Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Device and Resource Redirection.

 Allow audio recording redirection

If the Allow audio recording redirection Group Policy setting is disabled, you cannot select the Audio recording redirection check box on the Configure Client Experience page.

This Group Policy setting is located in Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Device and Resource Redirection.

 Allow desktop composition for remote desktop sessions

If the Allow desktop composition for remote desktop sessions Group Policy setting is disabled, you cannot select the Desktop composition check box on the Configure Client Experience page.

This Group Policy setting is located in Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Remote Session Environment.

 Limit maximum color depth

If the Limit maximum color depth Group Policy setting is enabled and the maximum color depth selected is less than 32 bits per pixel, you cannot select the Desktop composition check box on the Configure Client Experience page.

This Group Policy setting is located in Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Remote Session Environment.

These Group Policy settings can be configured by using either the Local Group Policy Editor or the Group Policy Management Console (GPMC).

For more information about Group Policy settings for Remote Desktop Services, see the [Remote Desktop Services Technical Reference](http://go.microsoft.com/fwlink/?LinkId=138134) (http://go.microsoft.com/fwlink/?LinkId=138134).

# Configuring License Settings on an RD Session Host Server

After you have installed and configured the license server, you need to do the following on your RD Session Host server to ensure that the RD Session Host server can contact the license server to request RDS CALs for clients:

 Specify the Remote Desktop licensing mode on an RD Session Host server.

 Specify a license server for an RD Session Host server to use.

To specify the Remote Desktop licensing mode

|  |
| --- |
| 1. On the RD Session Host server, open Remote Desktop Session Host Configuration. To open Remote Desktop Session Host Configuration, click Start, point to Administrative Tools, point to Remote Desktop Services, and then click Remote Desktop Session Host Configuration.  2. If the User Account Control dialog box appears, confirm that the action it displays is what you want, and then click Continue.  3. In the Edit settings area, under Licensing, double-click Remote Desktop licensing mode.  4. On the Licensing tab of the Properties dialog box, click either Per Device or Per User, depending on which is most appropriate for your environment.  5. Click OK to save your changes to the licensing settings. |

After you have specified a Remote Desktop licensing mode, you must specify a license server for the RD Session Host server to use.

To specify a license server for the RD Session Host server to use

|  |
| --- |
| 1. On the RD Session Host server, open Remote Desktop Session Host Configuration. To open Remote Desktop Session Host Configuration, click Start, point to Administrative Tools, point to Remote Desktop Services, and then click Remote Desktop Session Host Configuration.  2. If the User Account Control dialog box appears, confirm that the action it displays is what you want, and then click Continue.  3. In the Edit settings area, under Licensing, double-click Remote Desktop license servers.  4. In the Remote Desktop Session Host Configuration window, click Close.  5. On the Licensing tab of the Properties dialog box, click Add.  6. In the Add License Server dialog box, select a license server from the list of known license servers, and then click Add. If the license server that you want to add is not listed, in the License server name or IP address box, type the name or IP address of the license server, and then click Add.  7. Click OK to close the Add License Server dialog box, and then click OK to save your changes to the licensing settings. |

# Enabling Remote Desktop

To allow remote connections for administrative purposes only, you do not have to install the RD Session Host role service. Instead, you can enable Remote Desktop on the computer that you want to remotely administer.

Note

Remote Desktop supports only two concurrent remote connections to the computer. You do not need Remote Desktop Services client access licenses (RDS CALs) for these connections.

Membership in the local Administrators group, or equivalent, is the minimum required to complete this procedure. Review details about using the appropriate accounts and group memberships at [Local and Domain Default Groups](http://go.microsoft.com/fwlink/?LinkId=83477) (http://go.microsoft.com/fwlink/?LinkId=83477).

## Enable Remote Desktop

To enable Remote Desktop

|  |
| --- |
| 1. Log on as a member of the local Administrators security group.  2. Click Start, right-click Computer, and then click Properties.  3. Click Remote settings.  4. In the System Properties dialog box, on the Remote tab, click either of the following, depending on your environment:   Allow connections from computers running any version of Remote Desktop (less secure)   Allow connections only from computers running Remote Desktop with Network Level Authentication (more secure)  For more information about the two options, click the Help me choose link on the Remote tab.  5. Click Select Users to add the users and groups that need to connect to the computer by using Remote Desktop. The users and groups that you add are added to the Remote Desktop Users group.  Note  Members of the local Administrators group can connect even if they are not listed. |

# Verifying Remote Desktop Session Host Functionality

To verify the functionality of the RD Session Host deployment, log on to a remote desktop client and use Remote Desktop Connection (RDC) to connect to the RD Session Host server.

To connect to an RD Session Host server by using RDC

|  |
| --- |
| 1. Log on to a remote desktop client.  2. Click Start, point to All Programs, point to Accessories, and then click Remote Desktop Connection.  3. When the Remote Desktop Connection dialog box appears, type the name of the RD Session Host server in the Computer box, and then click Connect.  4. In the Windows Security dialog box, type the password for the remote desktop user, and then click OK.  5. If the connection is successful, a Windows desktop will appear on the screen for the RD Session Host server. |

# Creating a New User Account

To manage domain users, create user accounts in Active Directory Domain Services (AD DS). In contrast, to manage users that are specific to one computer, create local user accounts. For more information, see [Create a local user account](http://go.microsoft.com/fwlink/?LinkId=138393) (http://go.microsoft.com/fwlink/?LinkId=138393).

Membership in Account Operators, Domain Admins, or Enterprise Admins, or equivalent, is the minimum required to complete this procedure. Review details about using the appropriate accounts and group memberships at [Local and Domain Default Groups](http://go.microsoft.com/fwlink/?LinkId=83477) (http://go.microsoft.com/fwlink/?LinkId=83477).

To create a new user account using the Windows interface

|  |
| --- |
| 1. To open Active Directory Users and Computers, click Start, click Control Panel, double-click Administrative Tools, and then double-click Active Directory Users and Computers.  2. In the console tree, right-click the folder in which you want to add a user account.  3. Point to New, and then click User.  4. In First name, type the user's first name.  5. In Initials, type the user's initials.  6. In Last name, type the user's last name.  7. Modify Full name to add initials or reverse the order of first and last names.  8. In User logon name, type the user logon name, click the user principal name (UPN) suffix in the drop-down list, and then click Next.  If the user will use a different name to log on to computers running Microsoft® Windows® 95, Windows 98, or Windows NT® operating systems, you can change the user logon name as it appears in User logon name (pre-Windows 2000) to the different name.  9. In Password and Confirm password, type the user's password, and then select the appropriate password options. |

### Additional considerations

 To perform this procedure, you must be a member of the Account Operators group, Domain Admins group, or Enterprise Admins group in AD DS, or you must have been delegated the appropriate authority. As a security best practice, consider using Run as to perform this procedure.

 Another way to open Active Directory Users and Computers is to click Start, click Run, and then type dsa.msc.

 When you create a new user account, the full name attribute is created in the FirstNameLastName format by default. The full name attribute also governs the display name format that is shown in the global address list. You can change the display name format by using ADSI Edit. If you change the display name format, the full name format will also change. For more information, see [article 250455 in the Microsoft Knowledge Base](http://go.microsoft.com/fwlink/?LinkId=131264) (http://go.microsoft.com/fwlink/?LinkId=131264).

 You can also perform the task in this procedure by using the Active Directory module for Windows PowerShell™. To open the Active Directory module, click Start, click Administrative Tools, and then click Active Directory Module for Windows PowerShell. For more information, see [Create a New User Account](http://go.microsoft.com/fwlink/?LinkId=138369) (http://go.microsoft.com/fwlink/?LinkId=138369). For more information about Windows PowerShell, see [Windows PowerShell](http://go.microsoft.com/fwlink/?LinkID=102372) (http://go.microsoft.com/fwlink/?LinkID=102372).

# Deploying a Simple Virtual Desktop Infrastructure

Remote Desktop Virtualization Host (RD Virtualization Host) is a Remote Desktop Services role service included with Windows Server 2008 R2. RD Virtualization Host integrates with Hyper-V to provide virtual machines by using RemoteApp and Desktop Connection. RD Virtualization Host can be configured so that each user in your organization is assigned a unique virtual machine, or users are redirected to a shared virtual machine pool where a virtual machine is dynamically assigned.

RD Virtualization Host uses Remote Desktop Connection Broker (RD Connection Broker) to determine where the user is redirected. If a user is assigned and requests a personal virtual desktop, RD Connection Broker redirects the user to this virtual machine. If the virtual machine is not turned on, RD Virtualization Host turns on the virtual machine and then connects the user. If the user is connecting to a shared virtual machine pool, RD Connection Broker first checks to see if the user has a disconnected session in the pool. If the user has a disconnected session, they are reconnected to that virtual machine. If the user does not have a disconnected session, a virtual machine in that pool is dynamically assigned to the user, if one is available.

#### Deploying a simple Virtual Desktop Infrastructure

Before you install and configure the RD Virtualization Host server for Virtual Desktop Infrastructure, be sure that you have reviewed the following conceptual topics:

 [Checklist: RD Session Host Installation Prerequisites](#z0c567046010a42d6b95e49e26857de0a)

# Checklist: Deploying the Virtual Machine for Remote Desktop Services

This parent checklist includes cross-reference links to important concepts about the Remote Desktop Services design. It also contains links to subordinate checklists that will help you complete the tasks that are required to implement this design.

Note

Complete the tasks in this checklist in order. When a reference link takes you to a procedure, return to this topic after you complete the steps in that procedure so that you can proceed with the remaining tasks in this checklist.

 Checklist: Deploying the virtual machine for Remote Desktop Services

|  |  |  |
| --- | --- | --- |
|  | Task | Reference |
|  | Create a virtual machine that will be used as a virtual desktop. | [Creating a Virtual Machine](#z02a9286074ca496288cbfb9bea5e2db5) |
|  | Enable Remote Desktop on the virtual machine. | [Enabling Remote Desktop](#zbce9c21f4d644240806c567e2f743e42) |
|  | Allow Remote RPC on the virtual machine. | [Allowing Remote RPC](#z9d8d2a82958648d0a3b03751137c4a84) |
|  | Create a firewall exception to allow Remote Services Management. | [Creating a Firewall Exception to Allow Remote Services Management](#zd184512632754f5cb4edbe6f7a113635) |
|  | Add permissions to the RDP Protocol. | [Adding Permissions to the RDP Protocol](#ze056e87f190440f3a79ee3029a359115) |
|  | Add the user accounts that will be using this virtual machine to the local Remote Desktop Users security group.  Note  To create a new user account to add to the Remote Desktop Users Group, see [Creating a New User Account](#z90490add342e4453b44daacf81d60ad9). | [Configuring the Remote Desktop Users Group](#z11f0abf70ef548f2a207c56fcdafee9e) |
|  | Enable rollback on a virtual machine for virtual desktop pools. (Optional) | [Enabling Rollback on a Virtual Machine](#z0d54e48e0c22476a8d94ae56a4e85239) |

The following tasks can be performed by running the Visual Basic script or the Windows PowerShell™ script, available on the Microsoft TechNet Script Center.

 Enable Remote Desktop on the virtual machine.

 Allow Remote RPC on the virtual machine.

 Create a firewall exception to allow Remote Services Management.

 Add permissions to the RDP Protocol.

To configure the virtual machines, you can download and run the Visual Basic Script, [Configure Guest OS for Microsoft VDI (VB Script)](http://go.microsoft.com/fwlink/?LinkId=184805), or the Windows PowerShell script, [Configure Guest OS for Microsoft VDI (Windows PowerShell Script)](http://go.microsoft.com/fwlink/?LinkId=184804).

# About Virtual Desktop Infrastructure

## What is Virtual Desktop Infrastructure?

Remote Desktop Virtualization Host (RD Virtualization Host) is a new Remote Desktop Services role service included with Windows Server 2008 R2. RD Virtualization Host integrates with the Hyper-V role to provide virtual machines that can be used as personal virtual desktops or virtual desktop pools by using RemoteApp and Desktop Connection. User accounts can be assigned a unique personal virtual desktop or be redirected to a virtual desktop pool where a virtual desktop is dynamically assigned. RD Virtualization Host is an important component to the Virtual Desktop Infrastructure (VDI) solution offered by Microsoft.

## Why use Virtual Desktop Infrastructure?

The VDI solution includes the following scenarios:

 Personal virtual desktops are specific virtual machines that are hosted on an RD Virtualization Host server that can be assigned to a user account in Active Directory Domain Services (AD DS) to use as a personal virtual desktop, which the user can then access by using RemoteApp and Desktop Connection or RD Web Access.

 A virtual desktop pool is a group of identically configured virtual machines installed on an RD Virtualization Host server and managed through Hyper-V Manager. Users can access the virtual desktop pool through RemoteApp and Desktop Connection or RD Web Access. Because the virtual machines are identically configured, the user sees the same virtual desktop, regardless of which virtual machine in the virtual desktop pool the user connects to.

## Virtual Desktop Infrastructure role services

The following role services are included in a typical VDI deployment:

 RD Virtualization Host: RD Virtualization Host integrates with Hyper-V to host virtual machines and provide them to users as virtual desktops. You can assign a unique virtual desktop to each user in your organization, or provide them shared access to a virtual desktop pool.

An RD Virtualization Host server has the following functions:

 Monitoring virtual machine guest sessions and reporting these sessions to the RD Connection Broker server.

 Preparing the virtual machine for a remote desktop connection when requested by the RD Connection Broker server.

 RD Session Host: The RD Session Host server running in redirection mode helps to securely redirect an RDP client connection to a virtual machine. When a user requests a virtual machine, the RD Session Host queries the RD Connection Broker server. The RD Connection Broker server then provisions a virtual machine for the user, and returns its IP address to the RD Session Host server. The RD Session Host server running in redirection mode will then redirect the RDP client to connect to the virtual machine by using the IP address.

 RD Connection Broker: The main function of RD Connection Broker is to broker a user connection to an appropriate endpoint. Brokering of the connection involves:

 Identifying the virtual machine for the user to make a remote connection.

 Preparing the virtual machines for remote connections by communicating with the RD Virtualization Host server (for example, waking the VM from a saved state).

 Querying the IP address of the virtual machine by communicating with the RD Virtualization Host server. This IP address is returned to the RD Session Host server running in redirection mode.

 Monitoring user sessions in a virtual desktop pool scenario. A user with an existing session in a pool is redirected to the hosting virtual machine.

 RD Web Access: RD Web Access provides users with an aggregated view of remote applications and desktop connections by using a Web browser. Using RD Web Access, a user can view all remote applications and virtual desktops (virtual desktop pools and personal virtual desktops) published to that user.

 RD Licensing: RD Licensing manages the Remote Desktop Services client access licenses (RDS CALs) that are required for each device or user to connect to a virtual desktop. You use RD Licensing to install, issue, and track the availability of RDS CALs on a Remote Desktop license server.

 RD Gateway: RD Gateway is an optional role service in the VDI deployment. RD Gateway enables authorized remote users to securely connect to resources on an internal corporate network, from any Internet-connected device.

# Installing the Remote Desktop Virtualization Host Role Service

Remote Desktop Virtualization Host (RD Virtualization Host) is a Remote Desktop Services role service available in Windows Server 2008 R2. RD Virtualization Host is installed by using Server Manager. When the RD Virtualization Host role service is installed, Server Manager checks to see if Hyper-V is installed. If Hyper-V is not installed, Server Manager will install it.

Important

The RD Virtualization Host server must meet the hardware requirements for the Hyper-V server role. For more information about Hyper-V hardware requirements, see <http://go.microsoft.com/fwlink/?LinkId=129920>.

Membership in the local Administrators group, or equivalent, is the minimum required to complete this procedure. Review details about using the appropriate accounts and group memberships at [Local and Domain Default Groups](http://go.microsoft.com/fwlink/?LinkId=83477) (http://go.microsoft.com/fwlink/?LinkId=83477).

To install the RD Virtualization Host role service

|  |
| --- |
| 1. On the computer on which you want to install the RD Virtualization Host role service, open Server Manager. To open Server Manager, click Start, point to Administrative Tools, and then click Server Manager.  2. Under the Roles Summary heading, click Add Roles.  3. On the Before You Begin page, click Next.  4. On the Select Server Roles page, select the Remote Desktop Services check box, and then click Next.  5. On the Remote Desktop Services page, click Next.  6. On the Select Role Services page, select the Remote Desktop Virtualization Host check box.  7. Review the information about adding Hyper-V, click Add Required Role Services, and then click Next.  8. On the Confirm Installation Selections page, click Install.  9. After the installation is complete, click Close. |

# Allowing Remote RPC

After the virtual machines are installed and configured, you must allow Remote RPC for the clients to work with Remote Desktop Services.

Membership in the local Administrators group, or equivalent, is the minimum required to complete this procedure. Review details about using the appropriate accounts and group memberships at [Local and Domain Default Groups](http://go.microsoft.com/fwlink/?LinkId=83477) (http://go.microsoft.com/fwlink/?LinkId=83477).

To allow Remote RPC for Remote Desktop Services

|  |
| --- |
| 1. Log on as a member of the local Administrators security group.  2. Click Start, and in the Search programs and files box, type regedit.exe and then press ENTER.  Caution  Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on the computer.  3. Navigate to HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\TerminalServer.  4. Double-click the AllowRemoteRPC registry entry. In the Value data box, type 1 and then click OK.  5. Close Registry Editor. |

# Creating a Firewall Exception to Allow Remote Services Management

The Windows Firewall is on by default in Windows® 7, Windows Server 2008, and Windows Server 2008 R2. Windows Firewall helps control which programs or ports can be used to communicate between Windows Server 2008 and Windows Server 2008 R2 and other computers on the network or the Internet. To allow a program or port to communicate through Windows Firewall, an exception needs to be enabled.

Membership in the local Administrators group, or equivalent, is the minimum required to complete this procedure. Review details about using the appropriate accounts and group memberships at [Local and Domain Default Groups](http://go.microsoft.com/fwlink/?LinkId=83477) (http://go.microsoft.com/fwlink/?LinkId=83477).

To enable the Remote Service Management Windows Firewall exception

|  |
| --- |
| 1. Click Start, click Control Panel, and then click System and Security.  2. Under the Windows Firewall heading, click Allow a program through Windows Firewall.  3. Select the Remote Service Management check box, and then click OK. |

# Adding Permissions to the RDP Protocol

Allow Remote RPC on each virtual machine.

Membership in the local Administrators group, or equivalent, is the minimum required to complete this procedure. Review details about using the appropriate accounts and group memberships at [Local and Domain Default Groups](http://go.microsoft.com/fwlink/?LinkId=83477) (http://go.microsoft.com/fwlink/?LinkId=83477).

To add RDP protocol permissions to a virtual machine

|  |
| --- |
| 1. Click Start, point to All Programs, and then click Accessories.  2. Right-click Command Prompt, and then click Run as administrator.  3. If the User Account Control dialog box appears, confirm that the action it displays is what you want, and then click Yes.  4. At the command prompt, type the following commands:   wmic /node:localhost RDPERMISSIONS where TerminalName="RDP-Tcp" CALL AddAccount "<DOMAIN>\<SERVER\_NAME>$",1   wmic /node:localhost RDACCOUNT where "(TerminalName='RDP-Tcp' or TerminalName='Console') and AccountName='<DOMAIN>\\<SERVER\_NAME>$'" CALL ModifyPermissions 0,1   wmic /node:localhost RDACCOUNT where "(TerminalName='RDP-Tcp' or TerminalName='Console') and AccountName='<DOMAIN>\\<SERVER\_NAME>$'" CALL ModifyPermissions 2,1   wmic /node:localhost RDACCOUNT where "(TerminalName='RDP-Tcp' or TerminalName='Console') and AccountName='<DOMAIN>\\<SERVER\_NAME>$'" CALL ModifyPermissions 9,1   Net stop termservice   Net start termservice  5. Log off the computer. |

# Configuring Rollback for a Virtual Desktop Pool

Enable rollback on a virtual machine. Rollback is a feature in Remote Desktop Services that reverts all changes made by a user to a virtual machine when the user logs off from the virtual machine.

Membership in the local Administrators group, or equivalent, is the minimum required to complete this procedure. Review details about using the appropriate accounts and group memberships at [Local and Domain Default Groups](http://go.microsoft.com/fwlink/?LinkId=83477) (http://go.microsoft.com/fwlink/?LinkId=83477).

To enable rollback on a virtual machine

|  |
| --- |
| 1. Open Hyper-V Manager. To open Hyper-V Manager, click Start, point to Administrative Tools, and then click Hyper-V Manager.  2. Under Virtual Machines, right-click the virtual machine, and then click Snapshot.  3. Under Snapshots, right-click the virtual machine, and then click Rename.  4. Type RDV\_Rollback and then press ENTER.  5. Close Hyper-V Manager. |

# Creating a Virtual Machine

Install a Windows 7 client on a virtual machine, on a server running Hyper-V for a Remote Desktop Services Virtual Desktop Infrastructure (VDI) deployment.

Membership in the local Administrators group, or equivalent, is the minimum required to complete this procedure. Review details about using the appropriate accounts and group memberships at [Local and Domain Default Groups](http://go.microsoft.com/fwlink/?LinkId=83477) (http://go.microsoft.com/fwlink/?LinkId=83477).

## Install Windows 7 on a virtual machine

To install Windows 7 on a virtual machine

|  |
| --- |
| 1. Log on as a member of the local Administrators security group.  2. Insert the Windows 7 product DVD into the DVD drive on the Remote Desktop Virtualization Host (RD Virtualization Host) server.  3. Open Hyper-V Manager. To open Hyper-V Manager, click Start, point to Administrative Tools, and then click Hyper-V Manager.  4. Right-click the RD Virtualization Host server, point to New, and then click Virtual Machine.  5. On the Before You Begin page, click Next.  6. In the Name box, type the FQDN of the virtual machine, and then click Next.  7. On the Assign Memory page, click Next.  8. On the Configure Networking page, in the Connection box, select the appropriate virtual network, and then click Next.  9. On the Connect Virtual Hard Disk page, in the Name box, type the FQDN of the virtual machine, in the Size box, type the desired size for the virtual machine, and then click Next.  10. On the Installation Options page, click Install an operating system from a boot CD/DVD-ROM drive.  11. In the Physical CD/DVD drive box, select the DVD drive that contains the Windows 7 product DVD, and then click Next.  12. On the Completing the New Virtual Machine Wizard page, review the installation options, and then click Finish.  13. In the Virtual Machines area, right-click the virtual machine, and then click Connect.  14. On the Action menu, click Start to start the installation of Windows 7. |

# Joining RD Virtualization Host to RD Connection Broker

Specify the RD Virtualization Host server on the RD Connection Broker server, to enable the RD Virtualization Host server to perform the following:

 Monitor the virtual machine guest sessions and report these sessions to the RD Connection Broker server.

 Prepare the virtual machine for a remote desktop connection when requested by the RD Connection Broker server.

Membership in the local Administrators group, or equivalent, is the minimum required to complete this procedure. Review details about using the appropriate accounts and group memberships at [Local and Domain Default Groups](http://go.microsoft.com/fwlink/?LinkId=83477) (http://go.microsoft.com/fwlink/?LinkId=83477).

To join RD Virtualization Host to RD Connection Broker

|  |
| --- |
| 1. On the RD Connection Broker server, click Start, point to Administrative Tools, point to Remote Desktop Services, and then click Remote Desktop Connection Manager.  2. In the Actions pane, click Configure Virtual Desktops Wizard.  3. On the Before You Begin page, click Next.  4. On the Specify an RD Virtualization Host Server page, in the Server name box, type the NetBIOS name or FQDN of the RD Virtualization Host server, click Add, and then click Next.  5. On the Configure Redirection Settings page, in the Server name box, type the NetBIOS name or FQDN of the RD Session Host server, and then click Next.  6. On the Specify an RD Web Access Server page, click Next.  7. On the Confirm Changes page, click Apply.  8. Ensure that the Assign personal virtual desktop check box is cleared, and then click Finish. |

# Assigning a Personal Virtual Desktop

To specify a virtual desktop to be used by remote desktop users, configure the personal virtual desktop on the RD Connection Broker server and assign it to a remote desktop user.

Membership in the local Administrators group, or equivalent, is the minimum required to complete this procedure. Review details about using the appropriate accounts and group memberships at [Local and Domain Default Groups](http://go.microsoft.com/fwlink/?LinkId=83477) (http://go.microsoft.com/fwlink/?LinkId=83477).

To assign a personal virtual desktop by using the Assign Personal Virtual Desktop Wizard

|  |
| --- |
| 1. On the RD Connection Broker server, click Start, point to Administrative Tools, point to Remote Desktop Services, and then click Remote Desktop Connection Manager.  2. In the Content pane, under the Status heading, under Virtual Desktop Resource: Personal Virtual Desktop for Assign Personal Virtual Desktops, click Assign.  3. On the Assign Personal Virtual Desktop page, click Select User.  4. In the Enter the object name to select box, type the name of the user account, and then click OK.  5. In the Virtual machine list, click the name of the personal virtual desktop that is being configured, and then click Next.  6. Confirm that the User name and Virtual machine boxes are correct, and then click Assign.  7. If you do not want to assign another personal virtual desktop, clear the Assign another virtual machine to another user check box, and then click Finish. |

# Adding Virtual Machines to a Virtual Desktop Pool

To create a pool of virtual desktops to be used by remote desktop users, configure the virtual desktop pool on the RD Connection Broker server.

Membership in the local Administrators group, or equivalent, is the minimum required to complete this procedure. Review details about using the appropriate accounts and group memberships at [Local and Domain Default Groups](http://go.microsoft.com/fwlink/?LinkId=83477) (http://go.microsoft.com/fwlink/?LinkId=83477).

To add virtual machines to a virtual desktop pool

|  |
| --- |
| 1. Click Start, point to Administrative Tools, point to Remote Desktop Services, and then click Remote Desktop Connection Manager.  2. In the Actions pane, click Create Virtual Desktop Pool.  3. On the Welcome to the Create Virtual Desktop Pool Wizard page, click Next.  4. On the Select Virtual Machines page, click the virtual machine to add to the virtual desktop pool, and then click Next.  Note  You can select more than one virtual machine by holding the CTRL button when selecting the virtual machines.  5. On the Set Pool Properties page, in the Display name box, type a name for the virtual desktop pool. In the Pool ID box, type a pool ID, and then click Next.  6. On the Results page, verify the virtual desktop pool members, and then click Finish. |

# Enabling Rollback on a Virtual Machine

Rollback is a feature in Remote Desktop Services that reverts all changes made by a user to a virtual machine when the user logs off from the virtual machine.

Membership in the local Administrators group, or equivalent, is the minimum required to complete this procedure. Review details about using the appropriate accounts and group memberships at [Local and Domain Default Groups](http://go.microsoft.com/fwlink/?LinkId=83477) (http://go.microsoft.com/fwlink/?LinkId=83477).

To enable rollback on a virtual machine

|  |
| --- |
| 1. Log on to RD Virtualization Host using an Administrator account.  2. Open Hyper-V Manager. To open Hyper-V Manager, click Start, point to Administrative Tools, and then click Hyper-V Manager.  3. Under Virtual Machines, right-click the virtual machine to enable rollback, and then click Snapshot.  4. Under Snapshots, right-click the snapshot of the virtual machine, and then click Rename.  5. Type RDV\_Rollback and then press ENTER.  6. Close Hyper-V Manager.  7. Repeat these steps for each virtual machine. |

# Verifying Personal Virtual Desktop Functionality

To verify the functionality of the personal virtual desktop deployment, you will log on as a remote user and connect to the personal virtual desktop by using Remote Desktop Web Access (RD Web Access).

To connect to the personal virtual desktop

|  |
| --- |
| 1. Log on to a remote desktop client.  2. Click Start, point to All Programs, and then click Internet Explorer.  3. In the Address bar, type https://<FQDN of the RD Web Access Server>/RDWeb and then press ENTER.  4. Click Continue to this website (not recommended).  Important  This guide uses a self-signed certificate for the RD Web Access server. Self-signed certificates are not recommended in a production environment. You should use a certificate that is trusted from a certification provider when deploying RD Web Access in a production environment.  5. In the Domain\user name box, type the user name of the remote user.  6. In the Password box, type the password that you specified for the user, and then click Sign in.  Note  In you receive a prompt asking you to install the Microsoft Remote Desktop Services Web Access Control, click Run Add-on, and then click Run.  7. Click My Desktop, and then click Connect.  8. When prompted, enter the credentials for the remote user, and then click OK. |

You have successfully deployed and demonstrated the functionality of a personal virtual desktop by connecting a personal virtual desktop by using RD Web Access. You can also use this deployment to explore some of the additional capabilities of personal virtual desktops through additional configuration and testing.

# Verifying Virtual Desktop Pool Functionality

To verify the functionality of the virtual desktop pool deployment, you will log on as remote user and connect to the virtual desktop pool by using Remote Desktop Web Access (RD Web Access).

To connect to the virtual desktop pool

|  |
| --- |
| 1. Log on to a remote desktop client.  2. Click Start, point to All Programs, and then click Internet Explorer.  3. In the Address bar, type https://<FQDN of the RD Web Access Server>/RDWeb and then press ENTER.  4. Click Continue to this website (not recommended).  Important  This guide uses a self-signed certificate for the RD Web Access server. Self-signed certificates are not recommended in a production environment. You should use a certificate that is trusted from a certification provider when deploying RD Web Access in a production environment.  5. In the Domain\user name box, type user name of the remote user.  6. In the Password box, type the password that you specified for the remote user, and then click Sign in.  Note  In you receive a prompt asking you to install the Microsoft Remote Desktop Services Web Access Control, click Run Add-on, and then click Run.  7. Click the name of the virtual desktop pool, and then click Connect.  8. When prompted, enter the credentials for remote user, and then click OK. |

You have successfully deployed and demonstrated the functionality of virtual desktop pools by connecting to a virtual desktop pool by using RD Web Access. You can also use this deployment to explore some of the additional capabilities of virtual desktop pools through additional configuration and testing.

# Configuring Publishing

Configuring publishing provides users with an aggregated view of remote applications and desktop connections by using a Web browser. Using RD Web Access, a user can view all remote applications and virtual desktops published to that user.

# Installing the Remote Desktop Web Access Role Service

Install the RD Web Access role service on the server that you want users to connect to over the Web to access RemoteApp programs. When you install the RD Web Access role service, Microsoft Internet Information Services (IIS) is also installed.

The server where you install RD Web Access acts as the Web server. The server does not have to be a Remote Desktop Session Host (RD Session Host) server.

Membership in the local Administrators group, or equivalent, is the minimum required to complete this procedure. Review details about using the appropriate accounts and group memberships at [Local and Domain Default Groups](http://go.microsoft.com/fwlink/?LinkId=83477) (http://go.microsoft.com/fwlink/?LinkId=83477).

## Install the Remote Desktop Web Access role service

To install the RD Web Access role service

|  |
| --- |
| 1. On the computer on which you want to install the RD Web Access role service, open Server Manager. To open Server Manager, click Start, point to Administrative Tools, and then click Server Manager.  2. If the Remote Desktop Services role is not already installed:  a. Under Roles Summary, click Add Roles.  b. On the Before You Begin page, click Next.  c. On the Select Server Roles page, select the Remote Desktop Services check box, and then click Next.  d. Review the Remote Desktop Services page, and then click Next.  e. On the Select Role Services page, select the Remote Desktop Web Access check box.  If the Remote Desktop Services role is already installed:  a. Under Roles Summary, click Remote Desktop Services.  b. Under Role Services, click Add Role Services.  c. On the Select Role Services page, select the Remote Desktop Web Access check box.  3. Review the information about the required role services, and then click Add Required Role Services.  4. Click Next.  5. Review the Web Server (IIS) page, and then click Next.  6. On the Select Role Services page, where you are prompted to select the role services that you want to install for IIS, click Next.  7. On the Confirm Installation Selections page, click Install.  8. On the Installation Progress page, installation progress will be noted.  9. On the Installation Results page, confirm that the installation succeeded, and then click Close. |

# Populating the TS Web Access Computers Security Group

If the RD Web Access server and the Remote Desktop Session Host (RD Session Host) server that hosts the RemoteApp programs are separate servers, you must add the computer account of the RD Web Access server to the TS Web Access Computers security group on the RD Session Host server.

Membership in the local Administrators group, or equivalent, on the RD Session Host server that you plan to configure, is the minimum required to complete this procedure. Review details about using the appropriate accounts and group memberships at [Local and Domain Default Groups](http://go.microsoft.com/fwlink/?LinkId=83477) (http://go.microsoft.com/fwlink/?LinkId=83477).

To add the computer account of the RD Web Access server to the security group

|  |
| --- |
| 1. On the RD Session Host server, click Start, point to Administrative Tools, and then click Computer Management.  2. In the left pane, expand Local Users and Groups, and then click Groups.  3. Right-click TS Web Access Computers, and then click Add to Group.  4. Click Add.  5. In the Select Users, Computers, or Groups dialog box, click Object Types.  6. In the Object Types dialog box, select the Computers check box, and then click OK.  7. In the Enter the object names to select box, specify the computer account of the RD Web Access server, and then click OK.  8. Click OK to close the TS Web Access Computers Properties dialog box. |

# Configuring the RD Web Access Server for RemoteApp and Desktop Connection

To provide users access to RemoteApp and Desktop Connection, you must configure RD Web Access to specify the source that provides the RemoteApp programs and virtual desktops that are displayed to users. You can configure RD Web Access to use either of the following:

 Remote Desktop Connection Broker (RD Connection Broker) server

 RemoteApp source

An RD Connection Broker server provides users access to virtual desktops hosted on RD Virtualization Host servers and to RemoteApp programs hosted on Remote Desktop Session Host (RD Session Host) servers. To configure the RD Connection Broker server, use the Remote Desktop Connection Manager tool. For more information, see the Remote Desktop Connection Manager Help in Windows Server 2008 R2.

A RemoteApp source is an individual RD Session Host server or a farm of identically configured RD Session Host servers on which RemoteApp programs have been configured. You can specify multiple RemoteApp sources. To configure RemoteApp programs on an RD Session Host server, use RemoteApp Manager.

You must log on by using either the local Administrator account on the RD Web Access server or an account that is a member of the TS Web Access Administrators group on the RD Web Access server to complete this procedure. Review details about using the appropriate accounts and group memberships at [Local and Domain Default Groups](http://go.microsoft.com/fwlink/?LinkId=83477) (http://go.microsoft.com/fwlink/?LinkId=83477).

To specify the source for RemoteApp and Desktop Connection

|  |
| --- |
| 1. Connect to the RD Web Access Web site. To do this, use either of the following methods:   On the RD Web Access server, click Start, point to Administrative Tools, point to Remote Desktop Services, and then click Remote Desktop Web Access Configuration.   Use Internet Explorer to connect to the RD Web Access Web site. By default, the Web site is located at the following address, where server\_name is the fully qualified domain name (FQDN) of the RD Web Access server:  https://server\_name/rdweb  2. Log on to the site by using either the local Administrator account on the RD Web Access server or an account that is a member of the TS Web Access Administrators group on the RD Web Access server.  3. On the title bar, click Configuration.  Note  If you access the RD Web Access Web site by using the Remote Desktop Web Access Configuration option, the page automatically opens to the Configuration page.  4. Select either An RD Connection Broker server or One or more RemoteApp sources.  If you select An RD Connection Broker server, in the Source name box, enter the NetBIOS name or FQDN of the RD Connection Broker.  If you select One or more RemoteApp sources, in the Source name box, enter the NetBIOS name or FQDN of the RemoteApp source. If you are using an RD Session Host server farm as the RemoteApp source, specify the DNS name of the farm. If you are specifying multiple RemoteApp sources, separate each name with a semicolon.  5. Click OK to save the changes. |

If you selected One or more RemoteApp sources, you also need to specify a connection name and a connection ID. The connection name will be used to identify RemoteApp and Desktop Connection provided by the RD Web Access server to the user. To specify the connection name and connection ID, on the RD Web Access server, open the %windir%\Web\RDWeb\App\_Data\RDWebAccess.config file in a text editor, such as Notepad.

If you selected An RD Connection Broker server, you need to specify the connection name and connection ID by using the Remote Desktop Connection Manager tool on the RD Connection Broker server. For more information, see the Remote Desktop Connection Manager Help in Windows Server 2008 R2.

# Configuring RemoteApp and Desktop Connection

Remote Desktop Web Connection enables a user to connect to the desktop of a remote computer from the RD Web Access Web site. To connect to a remote computer, the following conditions must be true:

 The remote computer must be configured to accept Remote Desktop connections.

 The user must be a member of the Remote Desktop Users group on the remote computer.

A user can access Remote Desktop Web Connection by clicking the Remote Desktop tab on the RD Web Access page. As an administrator, you can configure whether the Remote Desktop tab is available to users. Additionally, you can configure settings such as the RD Gateway server to use, and the default device and resource redirection options.

Membership in the local Administrators group, or equivalent, is the minimum required to complete this procedure. Review details about using the appropriate accounts and group memberships at [Local and Domain Default Groups](http://go.microsoft.com/fwlink/?LinkId=83477) (http://go.microsoft.com/fwlink/?LinkId=83477).

To configure Remote Desktop Web Connection behavior

|  |
| --- |
| 1. On the RD Web Access server, start Internet Information Services (IIS) Manager. To do this, click Start, point to Administrative Tools, and then click Internet Information Services (IIS) Manager.  2. In the left pane, expand the server name, expand Sites, expand Default Web Site, expand RDWeb, and then click Pages.  3. In the middle pane, under ASP.NET, double-click Application Settings.  4. To change Remote Desktop Web Connection settings, modify the values in the Application Settings pane.   To configure a default RD Gateway server, double-click DefaultTSGateway, enter the fully qualified domain name (FQDN) of the server in the Value box (for example, server1.contoso.com), and then click OK.   To specify the RD Gateway authentication method, double-click GatewayCredentialsSource, type the number that corresponds to the desired authentication method in the Value box, and then click OK. The possible values include:  0 = Ask for password (NTLM)  1 = Smart card  4 = Allow user to select later   To configure whether the Remote Desktop tab appears on the RD Web Access Web page, double-click ShowDesktops. In the Value box, type true to show the Remote Desktop tab, or type false to hide the Remote Desktop tab. When you are finished, click OK.   To configure default device and resource redirection settings, double-click the setting that you want to modify (xClipboard, xDriveRedirection, xPnPRedirection, xPortRedirection, or xPrinterRedirection). In the Value box, type true to enable the redirection setting by default, or type false to disable the redirection setting by default, and then click OK.  5. When you are finished, close IIS Manager.  Your changes should take effect immediately on the RD Web Access Web site. If the Web page is open, refresh the page to view the changes. |

Note

You can also configure these settings by modifying the %windir%\Web\RDWeb\Pages\Web.config file directly by using a text editor such as Notepad.

# Deploying Remote Desktop Connection Broker

Remote Desktop Connection Broker (RD Connection Broker) supports session load balancing and session reconnection in a load-balanced RD Session Host server farm. RD Connection Broker is also used to provide users access to RemoteApp programs and virtual desktops through RemoteApp and Desktop Connection.

If a user is assigned and requests a remote desktop, RD Connection Broker redirects the user to the appropriate session. If the virtual machine is not turned on, RD Virtualization Host turns on the virtual machine and then connects the user. If the user is connecting to a shared virtual desktop pool, RD Connection Broker first checks to see if the user has a disconnected session in the pool. If the user has a disconnected session, they are reconnected to that virtual machine. If the user does not have a disconnected session, a virtual machine in that pool is dynamically assigned to the user, if one is available.

Before you install and configure the RD Session Host server in a farm or a Virtual Desktop Infrastructure (VDI), be sure that you have reviewed the following conceptual topics:

 [Checklist: RD Session Host Installation Prerequisites](#z0c567046010a42d6b95e49e26857de0a)

# Installing the Remote Desktop Connection Broker Role Service

You must install the RD Connection Broker role service on the server that you want to use to track user session information for a load-balanced RD Session Host server farm. The server where you install the RD Connection Broker role service does not have to be an RD Session Host server or have Remote Desktop enabled.

You can use a single RD Connection Broker server to track user sessions across multiple farms, as there is minimal performance overhead.

When you install the RD Connection Broker role service, the following changes occur on the local computer:

 The Remote Desktop Connection Broker service is installed. By default, the service is set to Started and to Automatic.

 The Session Broker Computers local group is created.

 The Remote Desktop Connection Manager tool is installed.

Membership in the local Administrators group, or equivalent, is the minimum required to complete this procedure. Review details about using the appropriate accounts and group memberships at [Local and Domain Default Groups](http://go.microsoft.com/fwlink/?LinkId=83477) (http://go.microsoft.com/fwlink/?LinkId=83477).

## Installation prerequisites

The server where you install RD Connection Broker must be a member of a domain.

Note

If you install the RD Connection Broker role service on a domain controller, the Session Broker Computers group will be a domain local group and available on all domain controllers.

## Install the Remote Desktop Connection Broker role service

To install the RD Connection Broker role service

|  |
| --- |
| 1. On the computer on which you want to install the RD Connection Broker role service, open Server Manager. To open Server Manager, click Start, point to Administrative Tools, and then click Server Manager.  2. Under Roles Summary, click Add Roles.  3. On the Before You Begin page, click Next.  4. On the Select Server Roles page, click the Remote Desktop Services check box, and then click Next.  5. On the Remote Desktop Services page, click Next.  6. On the Select Role Services page, select the Remote Desktop Connection Broker check box, and then click Next.  7. On the Confirm Installation Selections page, click Install.  8. After the installation is complete, click Close. |

# Deploying Remote Desktop Licensing

Remote Desktop Licensing (RD Licensing) manages the Remote Desktop Services client access licenses (RDS CALs) that are required for each device or user to connect to a Remote Desktop Session Host (RD Session Host) server. You use RD Licensing to install, issue, and track the availability of RDS CALs on a Remote Desktop license server.

Before you install and configure a Remote Desktop license server, be sure that you have reviewed the following conceptual topics:

 [Checklist: RD Session Host Installation Prerequisites](#z0c567046010a42d6b95e49e26857de0a)

# About Remote Desktop Licensing

## What is RD Licensing?

Remote Desktop Licensing (RD Licensing), formerly Terminal Services Licensing (TS Licensing), manages the Remote Desktop Services client access licenses (RDS CALs) that are required for each device or user to connect to a Remote Desktop Session Host (RD Session Host) server. You use RD Licensing to install, issue, and track the availability of RDS CALs on a Remote Desktop license server.

Note

In Windows Server 2008 R2, a terminal server is now called an RD Session Host server. Also, Terminal Services client access licenses (TS CALs) are now called Remote Desktop Services client access licenses (RDS CALs). In these topics, these new terms are used, even when referring to previous versions of Windows Server. Note that security group names have not changed in Windows Server 2008 R2.

When a client—either a user or a device—connects to an RD Session Host server, the RD Session Host server determines if an RDS CAL is needed. The RD Session Host server then requests an RDS CAL from a Remote Desktop license server on behalf of the client attempting to connect to the RD Session Host server. If an appropriate RDS CAL is available from a license server, the RDS CAL is issued to the client, and the client is able to connect to the RD Session Host server.

Although there is a licensing grace period during which no license server is required, after the grace period ends, clients must have a valid RDS CAL issued by a license server before they can log on to an RD Session Host server.

Important

Remote Desktop supports two concurrent connections to remotely administer a computer. You do not need a license server for these connections.

To use Remote Desktop Services, you must also have at least one license server deployed in your environment. For small deployments, you can install both the RD Session Host role service and the RD Licensing role service on the same computer. For larger deployments, it is recommended that the RD Licensing role service be installed on a separate computer from the RD Session Host role service.

You must configure RD Licensing correctly in order for your RD Session Host server to accept connections from clients. To allow ample time for you to deploy a license server, Remote Desktop Services provides a licensing grace period for the RD Session Host server during which no license server is required. During this grace period, an RD Session Host server can accept connections from unlicensed clients without contacting a license server. The grace period begins the first time the RD Session Host server accepts a client connection. The grace period ends after whichever of the following occurs first:

 A permanent RDS CAL is issued by a license server to a client connecting to the RD Session Host server.

 The number of days in the grace period is exceeded.

The length of the grace period is based on the operating system running on the RD Session Host server. The grace periods are as follows.

|  |  |
| --- | --- |
| Operating system running on the RD Session Host server | Grace period |
| Windows Server 2008 R2 | 120 days |
| Windows Server 2008 | 120 days |
| Windows Server 2003 R2 | 120 days |
| Windows Server 2003 | 120 days |
| Windows 2000 | 90 days |

By default, after you log on as a local administrator on an RD Session Host server, a message appears in the lower-right corner of the desktop that notes the number of days until the licensing grace period for the RD Session Host server expires.

Before the RD Licensing grace period ends, you must purchase and install the appropriate number of RDS CALs for each device or user that needs to connect to an RD Session Host server. In addition, you must verify that the Remote Desktop licensing mode that you specify on the RD Session Host server matches the type of RDS CAL available on the license server. The Remote Desktop licensing mode determines the type of RDS CAL that an RD Session Host server requests from a license server on behalf of a client connecting to the RD Session Host server.

# Installing the Remote Desktop Licensing Role Service

Use the following procedure to install the Remote Desktop Licensing (RD Licensing) role service by using Server Manager.

Note

The installation of the RD Licensing role service does not require the computer to be restarted.

Membership in the local Administrators group, or equivalent, on the RD Licensing server that you plan to configure, is the minimum required to complete this procedure. Review details about using the appropriate accounts and group memberships at [Local and Domain Default Groups](http://go.microsoft.com/fwlink/?LinkId=83477) (http://go.microsoft.com/fwlink/?LinkId=83477).

To install the RD Licensing role service

|  |
| --- |
| 1. On the server on which you want to install the RD Licensing role service, open Server Manager. To open Server Manager, click Start, point to Administrative Tools, and then click Server Manager.  2. If the Remote Desktop Services role is not already installed:  a. In the left pane, right-click Roles, and then click Add Roles.  b. On the Before You Begin page of the Add Roles Wizard, click Next.  c. On the Select Server Roles page, select the Remote Desktop Services check box, and then click Next.  d. On the Remote Desktop Services page, click Next.  e. On the Select Role Services page, select the Remote Desktop Licensing check box, and then click Next.  If the Remote Desktop Services role is already installed:  a. In the left pane, expand Roles.  b. Right-click Remote Desktop Services, and then click Add Role Services.  c. On the Select Role Services page, select the Remote Desktop Licensing check box, and then click Next.  3. On the Configure Discovery Scope for RD Licensing page, you can specify a discovery scope for the license server. For more information, see Remote Desktop License Server Discovery.  4. On the Configure Discovery Scope for RD Licensing page, you can also specify the location where the RD Licensing database will be stored. If you want to specify a database location other than the default location provided, click Browse. Note that the database location must be a local folder on the computer on which the RD Licensing role service is being installed.  5. Click Next.  6. On the Confirm Installation Selections page, verify that the RD Licensing role service will be installed, and then click Install.  7. On the Installation Progress page, installation progress is noted.  8. On the Installation Results page, confirm that installation of the RD Licensing role service succeeded, and then click Close. |

# Activating the Remote Desktop License Server

A Remote Desktop license server must be activated to certify the license server and allow the license server to issue Remote Desktop Services client access licenses (RDS CALs). You can activate a license server by using the Activate Server Wizard in the Remote Desktop Licensing Manager tool.

There are three methods by which you can activate your license server:

 [Activate a Remote Desktop License Server Automatically](#zb2c4c61306c84d73accb38d101901e36)

 [Activate a Remote Desktop License Server by Using a Web Browser](#zac830f32a3884ec5900cc3117c18da4f)

 [Activate a Remote Desktop License Server by Using the Telephone](#zfe8cec98fe1341c9acb1d7dafceea841)

When you activate the license server, Microsoft provides the server with a limited-use digital certificate that validates server ownership and identity. Microsoft uses an X.509 industry standard certificate for this purpose. By using this certificate, a license server can make subsequent transactions with Microsoft.

If a license server is not activated, the license server can only issue temporary RDS Per Device CALs, which are valid for 90 days, or RDS Per User CALs.

# Activate a Remote Desktop License Server Automatically

A license server must be activated to certify the license server and allow the license server to issue Remote Desktop Services client access licenses (RDS CALs). You can activate a license server by using the Activate Server Wizard in the Remote Desktop Licensing Manager tool.

To activate a Remote Desktop license server automatically

|  |
| --- |
| 1. On the license server, open Remote Desktop Licensing Manager. To open Remote Desktop Licensing Manager, click Start, point to Administrative Tools, point to Remote Desktop Services, and then click Remote Desktop Licensing Manager.  2. Right-click the license server that you want to activate, and then click Activate Server. The Activate Server Wizard starts.  3. In the Activate Server Wizard, on the Welcome to the Activate Server Wizard page, click Next.  4. On the Connection Method page, in the Connection method list, select Automatic connection (recommended), and then click Next.  5. On the Company Information page, type your name and company, select your country or region, and then click Next.  6. On the Company Information optional information page, specify any other information that you want to provide, such as e-mail and company address, and then click Next to activate your license server.  7. On the Completing the Activate Server Wizard pagedo one of the following:   To install Remote Desktop Services client access licenses (RDS CALs) onto your license server, ensure that the Start Install Licenses Wizard now check box is selected, click Next, and then follow the instructions.   To install RDS CALs later, clear the Start Install Licenses Wizard now check box, and then click Finish. |

# Activate a Remote Desktop License Server by Using a Web Browser

You can use the Web method to activate a license server when the computer running the Remote Desktop Licensing Manager tool does not have Internet connectivity, but you have access to the Web by means of a Web browser from another computer. The URL for the Web method is displayed in the Activate Server Wizard.

Membership in the local Administrators group, or equivalent, on the RD Licensing server that you plan to configure, is the minimum required to complete this procedure. Review details about using the appropriate accounts and group memberships at [Local and Domain Default Groups](http://go.microsoft.com/fwlink/?LinkId=83477) (http://go.microsoft.com/fwlink/?LinkId=83477).

To activate a Remote Desktop license server by using a Web browser

|  |
| --- |
| 1. On the license server, open Remote Desktop Licensing Manager. To open Remote Desktop Licensing Manager, click Start, point to Administrative Tools, point to Remote Desktop Services, and then click Remote Desktop Licensing Manager.  2. Right-click the license server that you want to activate, and then click Activate Server. The Activate Server Wizard starts.  3. Click Next.  4. On the Connection Method page, in the Connection method list, select Web Browser, and then click Next.  5. On the License Server Activation page, click the hyperlink to connect to the Remote Desktop Services Licensing Web site.  If you are running Remote Desktop Licensing Manager on a computer that does not have Internet connectivity, note the address for the Remote Desktop Services Licensing Web site, and then connect to the Web site from a computer that has Internet connectivity.  6. Under Select Option, click Activate a license server, and then click Next.  7. In the Product ID boxes, type your Product ID. Your Product ID is displayed on the License Server Activation page of the Activate Server Wizard. You must also complete the name, company, and country/region fields. Specify any other information that you want to provide, such as e-mail and company address, and then click Next.  8. Confirm your entries, and then click Next. Your license server ID is displayed.  9. On the License Server Activation page in the Activate Server Wizard, type the license server ID that you received in the previous step, and then click Next. Your license server is activated.  10. On the Completing the Activate Server Wizard page, do one of the following:   To install Remote Desktop Services client access licenses (RDS CALs) onto your license server, ensure that the Start Install Licenses Wizard now check box is selected, click Next, and then follow the instructions.   To install RDS CALs later, clear the Start Install Licenses Wizard now check box, and then click Finish. |

# Activate a Remote Desktop License Server by Using the Telephone

The telephone activation method allows you to talk to a Microsoft customer service representative to complete the activation process. The appropriate telephone number is determined by the country/region that you choose in the Activate Server Wizard and is displayed by the wizard.

Membership in the local Administrators group, or equivalent, on the RD Licensing server that you plan to configure, is the minimum required to complete this procedure. Review details about using the appropriate accounts and group memberships at [Local and Domain Default Groups](http://go.microsoft.com/fwlink/?LinkId=83477) (http://go.microsoft.com/fwlink/?LinkId=83477).

To activate a Remote Desktop license server by using the telephone

|  |
| --- |
| 1. On the license server, open Remote Desktop Licensing Manager. To open Remote Desktop Licensing Manager, click Start, point to Administrative Tools, point to Remote Desktop Services, and then click Remote Desktop Licensing Manager.  2. Right-click the license server that you want to activate, and then click Activate Server. The Activate Server Wizard starts.  3. Click Next.  4. On the Connection Method page, in the Connection method list, select Telephone, and then click Next.  5. On the Country or Region Selection page, click your country/region, and then click Next to view the appropriate telephone number to call.  6. Call Microsoft by using the telephone number that is displayed on the License Server Activation page, and then provide the Microsoft customer support representative with the Product ID that is displayed on your screen. The representative will also ask you to provide your name and the name of your company. The representative processes your request to activate the license server, and creates a unique ID for your license server.  7. On the License Server Activation page in the Activate Server Wizard, type the license server ID that the representative provides, and then click Next. Your license server is activated.  8. On the Completing the Activate Server Wizard page, do one of the following:   To install Remote Desktop Services client access licenses (RDS CALs) onto your license server, ensure that the Start Install Licenses Wizard now check box is selected, click Next, and then follow the instructions.   To install RDS CALs later, clear the Start Install Licenses Wizard now check box, and then click Finish. |

# Installing Remote Desktop Services Client Access Licenses

There are three methods by which you can install Remote Desktop Services client access licenses (RDS CALs) onto your license server:

 [Install Remote Desktop Services Client Access Licenses Automatically](#zd8c4045c9fd1437cb9d424d19b70f8c5)

 [Install Remote Desktop Services Client Access Licenses by Using a Web Browser](#z9806237e51294745b1ea3a32bcd9bffd)

 [Install Remote Desktop Services Client Access Licenses by Using the Telephone](#z2a71ca9eb61241dfa4edf19b7fae8fa0)

Before installing RDS CALs onto your license server, note the following:

 You must activate your Remote Desktop license server before you can install RDS CALs onto your license server. For more information, see [Activating the Remote Desktop License Server](#z55c8644804ee4c38b885f1853b6a1565).

 You need a license code to install RDS CALs onto your license server. A license code is provided when you purchase your RDS CALs. For more information, see Purchase Client Access Licenses (<http://go.microsoft.com/fwlink/?LinkId=81077>).

 You can install both Per User and Per Device CALs onto the same license server.

 You can install RDS CALs for different product versions onto the same license server. For example, you can install both Windows Server 2003 TS Per Device CALs and Windows Server 2008 TS Per User CALs onto a license server that is running Windows Server 2008 R2. This provides you the ability to have one license server provide RDS CALs to Remote Desktop Session Host (RD Session Host) servers running various versions of Windows Server.

Note

In Windows Server 2008 R2, Terminal Services client access licenses (TS CALs) are now called Remote Desktop Services client access licenses (RDS CALs).

# Install Remote Desktop Services Client Access Licenses Automatically

The automatic method for installing RDS CALs on a Remote Desktop license server requires Internet connectivity from the computer running the Remote Desktop Licensing Manager tool. Internet connectivity is not required from the license server itself.

To install Remote Desktop Services client access licenses automatically

|  |
| --- |
| 1. On the license server, open Remote Desktop Licensing Manager. To open Remote Desktop Licensing Manager, click Start, point to Administrative Tools, point to Remote Desktop Services, and then click Remote Desktop Licensing Manager.  2. Verify that the connection method for the Remote Desktop license server is set to Automatic connection (recommended) by right-clicking the license server on which you want to install Remote Desktop Services client access licenses (RDS CALs), and then clicking Properties. On the Connection Method tab, change the connection method if necessary, and then click OK.  3. Right-click the license server on which you want to install the RDS CALs, and then click Install Licenses.  4. In the Install Licenses Wizard, on the Welcome to the Install Licenses Wizard page, click Next.  5. On the License Program page, select the appropriate program through which you purchased your RDS CALs, and then click Next.  6. The License Program that you selected on the previous page in the wizard determines what information you need to provide on this page. In most cases, you must provide either a license code or an agreement number. Consult the documentation provided when you purchased your RDS CALs.  7. After you enter the required information, click Next.  8. On the Product Version and License Type page, select the appropriate product version, license type, and quantity of RDS CALs for your environment based on your RDS CAL purchase agreement, and then click Next.  The Microsoft Clearinghouse is automatically contacted and processes your request. The RDS CALs are then automatically installed onto the license server.  9. To complete the process, click Finish. The license server can now issue RDS CALs to clients that connect to an RD Session Host server. |

# Install Remote Desktop Services Client Access Licenses by Using a Web Browser

You can use the Web installation method when the computer running the Remote Desktop Licensing Manager tool does not have Internet connectivity, but you have access to the Web by means of a Web browser from another computer. The URL for the Web installation method is displayed in the Install Licenses Wizard.

Membership in the local Administrators group, or equivalent, on the RD Licensing server that you plan to configure, is the minimum required to complete this procedure. Review details about using the appropriate accounts and group memberships at [Local and Domain Default Groups](http://go.microsoft.com/fwlink/?LinkId=83477) (http://go.microsoft.com/fwlink/?LinkId=83477).

To install Remote Desktop Services client access licenses by using a Web browser

|  |
| --- |
| 1. On the license server, open Remote Desktop Licensing Manager. To open Remote Desktop Licensing Manager, click Start, point to Administrative Tools, point to Remote Desktop Services, and then click Remote Desktop Licensing Manager.  2. Verify that the connection method for the Remote Desktop license server is set to Web Browser by right-clicking the license server on which you want to install Remote Desktop Services client access licenses (RDS CALs), and then clicking Properties. On the Connection Method tab, change the connection method if necessary, and then click OK.  3. Right-click the license server on which you want to install the RDS CALs, and then click Install Licenses. The Install Licenses Wizard starts.  4. Click Next.  5. On the Obtain Client License Key Pack page, click the hyperlink to connect to the Remote Desktop Services Licensing Web site.  If you are running Remote Desktop Licensing Manager on a computer that does not have Internet connectivity, note the address for the Remote Desktop Services Licensing Web site, and then connect to the Web site from a computer that has Internet connectivity.  6. On the Remote Desktop Services Licensing Web page, under Select Option, select Install Client Access License tokens, and then click Next.  7. Provide the following required information:   License Server ID   A 35-digit number, in groups of 5 numerals, which is displayed on the Obtain Client License Key Pack page in the Install Licenses Wizard.   License Program   Select the appropriate program through which you purchased your RDS CALs.   Last name or surname   First name or given name   Company name   Country/region  You can also provide the optional information requested, such as company address, e-mail address, and phone number. In the organizational unit field, you can describe the unit within your organization that this license server serves.  8. Click Next.  9. The License Program that you selected on the previous page determines what information you need to provide on this page. In most cases, you must provide either a license code or an agreement number. Consult the documentation provided when you purchased your RDS CALs. In addition, you need to specify which type of RDS CAL and the quantity that you want to install on the license server.  10. After you have entered the required information, click Next.  11. Verify that all of the information that you have entered is correct. To submit your request to the Microsoft Clearinghouse, click Next. The Web page then displays a license key pack ID generated by the Microsoft Clearinghouse.  Important  Retain a copy of the license key pack ID. Having this information with you facilitates communications with the Microsoft Clearinghouse, should you need assistance with recovering RDS CALs.  12. In the Install Licenses Wizard, on the Obtain Client License Key Pack page, enter the license key pack ID in the boxes provided, and then click Next. The RDS CALs are installed on your license server.  13. On the Completing the Install Licenses Wizard page, click Finish. The license server can now issue RDS CALs to clients that connect to a Remote Desktop Session Host (RD Session Host) server. |

# Install Remote Desktop Services Client Access Licenses by Using the Telephone

The telephone installation method allows you to talk to a Microsoft customer service representative to complete the installation process. The appropriate telephone number is determined by the country/region that you choose in the Activate Server Wizard and is displayed by the wizard.

Membership in the local Administrators group, or equivalent, on the RD Licensing server that you plan to configure, is the minimum required to complete this procedure. Review details about using the appropriate accounts and group memberships at [Local and Domain Default Groups](http://go.microsoft.com/fwlink/?LinkId=83477) (http://go.microsoft.com/fwlink/?LinkId=83477).

To install Remote Desktop Services client access licenses by using the telephone

|  |
| --- |
| 1. On the license server, open Remote Desktop Licensing Manager. To open Remote Desktop Licensing Manager, click Start, point to Administrative Tools, point to Remote Desktop Services, and then click Remote Desktop Licensing Manager.  2. Verify that the connection method for the Remote Desktop license server is set to Telephone by right-clicking the license server on which you want to install Remote Desktop Services client access licenses (RDS CALs), and then clicking Properties. On the Connection Method tab, change the connection method if necessary, ensure that the correct country or region is selected in the Select Country or Region list, and then click OK.  3. Right-click the license server on which you want to install the RDS CALs, and then click Install Licenses. The Install Licenses Wizard starts.  4. Click Next.  5. On the Obtain Client License Key Pack page, use the telephone number that is displayed to call the Microsoft Clearinghouse, and give the representative your Remote Desktop license server ID and the required information for the licensing program through which you purchased your RDS CALs. The representative then processes your request to install RDS CALs, and gives you a unique ID for the RDS CALs. This unique ID is referred to as the license key pack ID.  Important  Retain a copy of the license key pack ID. Having this information with you facilitates communications with the Microsoft Clearinghouse should you need assistance with recovering RDS CALs.  6. In the Install Licenses Wizard, on the Obtain client license key pack page, enter the license key pack ID provided by the representative into the boxes provided, and then click Next. The RDS CALs are installed on your Remote Desktop license server.  7. To complete the process, click Finish. The Remote Desktop license server can now issue RDS CALs to clients that connect to a Remote Desktop Session Host (RD Session Host) server. |