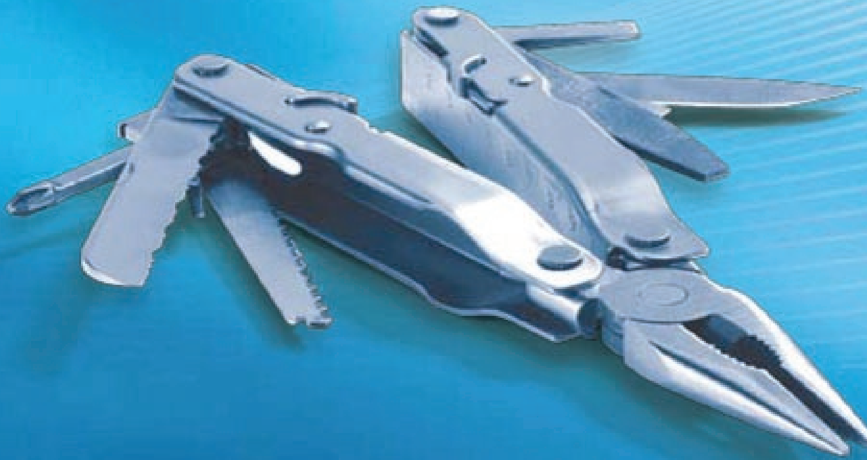
MCTS EXAM

70-653

Configuring Windows® Small Business Server 2008



Beatrice Mulzer,
Walter Glenn,
and Scott Lowe

SELF-PACED

Training Kit

How to access your CD files

The print edition of this book includes a CD. To access the CD files, go to http://aka.ms/626782/files, and look for the Downloads tab.

Note: Use a desktop web browser, as files may not be accessible from all ereader devices.

Questions? Please contact: mspinput@microsoft.com

Microsoft Press

Exam 70-653: Configuring Windows Small Business Server 2008

OBJECTIVE	LOCATION IN BOOK
DEPLOYING HARDWARE AND SOFTWARE FOR SBS SERVERS	
Install SBS on servers.	Chapter 1, Lesson 3
Configure a second server.	Chapter 7, Lesson 1
Configure Internet connectivity.	Chapter 1, Lesson 2 Chapter 1, Lesson 4
Configure Microsoft Exchange.	Chapter 6, Lesson 2
Configure SBS fax settings.	Chapter 4, Lesson 6
Configure the network firewall.	Chapter 1, Lesson 2 Chapter 1, Lesson 4
MIGRATING TO SBS 2008	
Prepare for migration.	Chapter 8, Lesson 1
Perform migration.	Chapter 8, Lesson 2 and 3
Verify migration.	Chapter 8, Lesson 4
DEPLOYING HARDWARE AND SOFTWARE FOR COMPUTERS ON THE NETWORK	
Prepare the computer.	Chapter 3, Lesson 1
Join computers to the domain.	Chapter 3, Lesson 2 Chapter 7, Lesson 1
Migrate local data.	Chapter 3, Lesson 3
MAINTAINING SYSTEMS AND SERVICES AVAILABILITY	
Modify software update settings.	Chapter 4, Lesson 1
Customize Windows Server Update Service (WSUS) and patches.	Chapter 4, Lesson 1
Modify server storage.	Chapter 4, Lesson 2
Configure backup and recovery.	Chapter 4, Lesson 3
Volume shadow copy	Chapter 4, Lesson 3
Server recovery	Chapter 4, Lesson 3
Database recovery	Chapter 4, Lesson 3
Active Directory object recovery	Chapter 4, Lesson 3
Maintain SBS client access license (CAL) compliance.	Chapter 3, Lesson 4
Modify reports settings.	Chapter 4, Lesson 5

OBJECTIVE	LOCATION IN BOOK
MAINTAINING REMOTE ACCESS	
Modify Remote Web Workplace (RWW).	Chapter 5, Lesson 2
Modify RAS.	Chapter 5, Lesson 3
User permissions	Chapter 5, Lesson 3
MAINTAINING USERS AND COMPUTERS	
Modify users.	Chapter 2, Lesson 3
Create, edit, and delete users	Chapter 2, Lesson 3
Modify groups.	Chapter 2, Lesson 1
Create, edit, and delete groups	Chapter 2, Lesson 1
Modify user roles.	Chapter 2, Lesson 2
Create, edit, and delete roles	Chapter 2, Lesson 2
MAINTAINING COLLABORATION	
Create new Microsoft SharePoint sites.	Chapter 6, Lesson 1
Modify site access.	Chapter 6, Lesson 1
Permissions	Chapter 6, Lesson 1
Modify shared folders.	Chapter 6, Lesson 1
Modify Web folder settings.	Chapter 6, Lesson 1
MAINTAINING MESSAGING	
Modify user messaging settings.	
Modify mailbox permissions	Chapter 6, Lesson 2
Add e-mail aliases to user accounts	Chapter 6, Lesson 2
Modify user distribution groups	Chapter 6, Lesson 2
Configure e-mail connectors.	Chapter 6, Lesson 3
Configure SMTP connectors	Chapter 6, Lesson 3
Configure POP3 connector	Chapter 6, Lesson 3
Configure mobile device settings.	Chapter 6, Lesson 4
Configure Microsoft Outlook settings.	Chapter 6, Lesson 5
RPC over HTTP (Outlook Anywhere)	Chapter 6, Lesson 5

Exam objectives The exam objectives listed here are current as of this book's publication date. Exam objectives are subject to change at any time without prior notice and at Microsoft's sole discretion. Please visit the Microsoft Learning Web site for the most current listing of exam objectives: *http://www.microsoft.com/learning/en/us/exams/70-653.mspx*.

PUBLISHED BY
Microsoft Press
A Division of Microsoft Corporation
One Microsoft Way
Redmond, Washington 98052-6399

Library of Congress Control Number: 2009930401

Printed and bound in the United States of America.

1 2 3 4 5 6 7 8 9   QWT   4 3 2 1 1 0

Distributed in Canada by H.B. Fenn and Company Ltd.

A CIP catalogue record for this book is available from the British Library.

Microsoft Press books are available through booksellers and distributors worldwide. For further information about international editions, contact your local Microsoft Corporation office or contact Microsoft Press International directly at fax (425) 936-7329. Visit our Web site at www.microsoft.com/mspress. Send comments to tkinput@microsoft.com.

The example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted 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.

This book expresses the author's views and opinions. The information contained in this book is provided without any express, statutory, or implied warranties. Neither the authors, Microsoft Corporation, nor its resellers, or distributors will be held liable for any damages caused or alleged to be caused either directly or indirectly by this book.

Acquisitions Editor: Ken Jones
Developmental Editor: Laura Sackerman
Project Editor: Maureen Zimmerman
Editorial Production: Christian Holdener, S4Carlisle Publishing Services
Technical Reviewer: Kurt Meyer; Technical Review services provided by Content Master, a member of CM Group, Ltd.
Cover: Tom Draper Design

Body Part No. X15-66442

To all Microsoft Small Business Specialists around the world.
Live long and prosper!

—Beatrice Mulzer

For my wife, Susan.

—Walter Glenn

For Amy; you make it all worth it!

—Scott Lowe

Contents at a Glance

Contents

List of Figures

List of Tables

Acknowledgements

I'd like to thank my co-authors, Walter Glenn and Scott Lowe, who brought their expertise and great work ethic to this project. It is a great pleasure working with you guys!

Many thanks are in order for some very special folks at Microsoft who consistently go above and beyond in every way. I want to thank Eric Ligman (*http://blogs.msdn.com/mssmallbiz*), who is always there to help—especially with licensing questions. Many thanks go out to Kevin Beares for his support, especially in emergency situations. I want to thank Sean Daniel (*http://sbs.seandaniel.com*), Nicholas King, David Fabritius, Bodhisatva Deb, Chris Almida, and everyone on the Windows SBS Development team for readily sharing their technical knowledge and expertise. You Rock!

A big thanks to the editors, Maureen Zimmerman and Laura Sackerman, who tirelessly worked on converting my sentences into English; and to our technical reviewer, Kurt Meyer, who is probably an SBS expert by now. ☺

—Beatrice Mulzer

I'd like to acknowledge all the great people at Microsoft Press for the opportunity and for helping to put this book together. I'd also like to thank my fellow authors, Beatrice Mulzer and Scott Lowe, for their great work. And as always, thanks also go to my agent, Neil Salkind.

—Walter Glenn

I'd like to acknowledge the other two people with their names on the book: Beatrice Mulzer and Walter Glenn. They are a joy to work with! I'd also like to acknowledge the hard-working editors, proofers, technical reviewers, and all the other people at Microsoft who put so much into this book.

—Scott Lowe

Introduction

This training kit is designed for Microsoft Small Business Specialists who want to update their current certification credentials as well as for consultants to small businesses and value-added resellers (VARs) who want to add credentials reflecting their experience with Windows Small Business Server 2008 (Windows SBS) server software. A Small Business Specialist is a server administrator who has at least three years experience managing Windows-based servers and infrastructure in an environment of 5 to 75 users in a single physical location. A Small Business Specialist is responsible for supporting network services and resources such as messaging, database servers, file and print servers, a firewall, Internet connectivity, an intranet, remote access, and client computers. The Specialist might be responsible for implementing connectivity requirements, for example, connecting branch offices and individual users in remote locations to the small business network and to the Internet.

The Preparation Guide for Exam 70-653 is available at *http://www.microsoft.com/learning/en/us/exams/70-653.aspx*.

By using this training kit, you learn how to do the following:

- Deploy hardware and software for servers running Windows SBS 2008.
- Migrate to Windows SBS 2008.
- Deploy hardware and software for computers on the network.
- Maintain systems and services availability.
- Implement and maintain remote access.
- Maintain user accounts and computers.
- Implement and maintain collaboration.
- Implement and maintain messaging.

Windows SBS 2008 might appear to be quite simple because it was designed with ease of use for the administrator in mind. When an administrator is familiar with the Windows SBS Console, managing the Windows Small Business Server network should be straightforward.

What most administrators—especially administrators who have an enterprise background—overlook is that the Windows SBS Console functions on top of the Windows Server 2008 operating system and uses most of the Windows Server 2008 native administrative tools, managed through the Windows SBS wizards. In previous releases of Windows Small Business Server, often administrators would forgo using the Windows SBS wizards because, for instance, they were certain that adding a user or group account should be done through the Active Directory Users And Computers console and not through a wizard! In the end, this resulted in user accounts that were only partially functional, with authentication and access problems. The basic knowledge that these administrators were missing was that Windows Small Business Server configures its own organizational units and applies preconfigured Group Policy settings. Using the Windows SBS Console to create the user or group accounts places the newly created accounts in the appropriate organizational unit, therefore minimizing administrative tasks while ensuring consistency.

The caveat here is to use Windows Small Business Server and its tools and wizards as intended. Only reach for additional tools when necessary—for instance, when you cannot perform an advanced task through the Windows SBS Console. Read this book, practice the exercises, and keep this thought in mind as you take Exam 70-653, and you are well on your way to becoming a Small Business Specialist.

MORE INFO **FIND ADDITIONAL CONTENT ONLINE**

As new or updated material that complements this book becomes available, it will be posted on the Microsoft Press Online Windows Server And Client Web site. The type of material you might find includes articles, links to companion content, errata, sample chapters, updates to book content, and more. This Web site is available at *http://www.microsoft.com/learning/books/online/serverclient* and will be updated periodically.

Hardware Requirements

In Chapters 1 through 6 you work with Windows SBS 2008 Standard and a client computer that runs the Windows Vista operating system. Windows Vista is the preferred client and will allow for the best user experience. However, you can substitute the Windows XP operating system with Service Pack 2 (SP2) if needed. All exercises in this book are written for Windows Vista. If you use Windows XP SP2, some steps will be slightly different from those outlined in the practice exercises.

Two options are available to set up the test environment. You can use a physical test server and test workstation to complete the practice exercises in each lesson, or you can complete all practice exercises in this book using virtual machines in Microsoft Hyper-V.

Physical Server Setup

To set up a server running Windows SBS 2008 to complete the practices in this book, the minimum system requirements are as follows:

- A server with 2 GHz or faster single core 64-bit (x64) processor, or 1.5 GHz or faster multicore 64-bit (x64) processors
- 4 GB of RAM or more (up to 32 GB)
- 60 GB of available hard disk space
- Network adapter

- DVD-ROM drive
- Super VGA (1,024 × 768) or higher resolution video adapter and monitor
- Keyboard and Microsoft Mouse or compatible pointing device
- Router/firewall device
- Internet connection

To set up a workstation that runs the Windows Vista (Enterprise, Business, or Ultimate) operating system to complete the practices, the minimum system requirements are as follows:

- Personal computer with a 1-GHz 32-bit (x86) or 64-bit (x64) processor
- 1 GB of RAM or more
- 40-GB hard drive with at least 15 GB of available space
- Network adapter
- CD-ROM drive or DVD-ROM drive
- Super VGA (1,024 × 768) or higher resolution video adapter and monitor
- Keyboard and Microsoft Mouse or compatible pointing device

NOTE **WORKING WITH A TOTAL OF TWO COMPUTERS TO COVER ALL CHAPTERS**

By meeting the minimum system requirements listed previously, you can repurpose the second physical computer in Chapters 7 and 8 for the practice exercises. In Chapter 7, you can modify it to function as the second server, and in Chapter 8 you can modify it to function as a server running Windows Small Business Server 2003.

If the second computer is a 32-bit machine, you must install the 32-bit version of Windows Server and 32-bit version of Microsoft SQL Server to perform the exercises in Chapter 7.

Virtual Machine Setup in Hyper-V

You can complete all practice exercises in this book using virtual machines in Microsoft Hyper-V rather than using hardware. Hyper-V ships as part of Windows Server 2008 and only requires downloading update packages from the Microsoft Download Center after the Hyper-V role is enabled on the server.

The minimum and recommended hardware requirements for Windows Server 2008 that runs Hyper-V to complete the exercises in this book are as follows:

- A server with a 2-GHz 64-bit (x64) processor with hardware-assisted virtualization. (This is available in processors that include a virtualization option; specifically, Intel VT or AMD Virtualization.) Hardware Data Execution Protection (DEP) must be available and enabled. Specifically, you must enable Intel XD bit (execute disable bit) or AMD NX bit (no execute bit).

- 6 GB of RAM (1 GB of RAM for the host system, 4 GB of RAM for the Windows SBS 2008 virtual machine, and 1 GB of RAM for the Windows Vista virtual machine), 8 GB of RAM or higher recommended.
- 160 GB of hard disk space (10 GB for the host system, and each minimum system hard disk space requirements for each virtual machine).
- 2 network adapters (one for the virtual network and one for Internet connectivity).
- DVD-ROM drive.
- Super-VGA (800 × 600) or higher resolution (1,024 × 768 recommended) video adapter and monitor.
- Keyboard and Microsoft Mouse or compatible pointing device.

NOTE **ENABLING HARDWARE-ASSISTED VIRTUALIZATION**

To ensure that the Hyper-V role will install properly and is working, make sure to get the latest BIOS from the motherboard manufacturer. You must turn on hardware-assisted virtualization in the BIOS (check with the manufacturer on the location of the settings). You might have to do a hard restart for the new settings to take effect.

Considerations for Chapter 7

In Chapter 7, you need to set up Windows SBS 2008 Premium (the second server) to perform the practice exercises using a second computer. You can continue to use the server that runs Windows SBS 2008 you created in the previous chapters. If you are using physical machines, you can repurpose the Windows Vista client machine used in earlier chapters as the second server that is running Windows Small Business Premium.

If you are using a virtual machine setup, you can simply create the second server that is running Windows SBS 2008 Premium in a virtual machine. Be sure that your host machine meets the minimum system requirements listed earlier.

Considerations for Chapter 8

To perform the practice exercise in Chapter 8 you need to set up an additional server running Windows Small Business Server 2003 or Windows Small Business Server 2003 R2. As with Chapter 7, if you are using physical machines, you can repurpose the Windows Vista client machine used in earlier chapters as the server running Windows Small Business Server 2003.

If you are using a virtual machine setup, you can simply create an additional virtual machine to set up Windows Small Business Server 2003. Be sure that your host machine meets the minimum system requirements listed earlier.

Software Requirements

You can use Windows SBS 2008 Premium edition or Windows SBS 2008 Standard edition to perform the practice exercises in Chapters 1 through 6.

- **Windows SBS 2008 Premium edition** You can order an evaluation version of Windows SBS 2008 Premium edition from the Microsoft TechNet Evaluation Center at *http://technet.microsoft.com/en-us/evalcenter/cc184870.aspx*. There will be a small shipping charge and it can take four to six weeks for delivery. (Currently, a download for Windows SBS 2008 Premium edition is not available.)
- **Windows SBS 2008 Standard edition** You can download an evaluation version of Windows SBS 2008 Standard edition from the Microsoft TechNet Evaluation Center at *http://technet.microsoft.com/en-us/evalcenter/cc184870.aspx*. This way you can get started right away with the practice exercises. You can improvise for not having the Premium edition by downloading additional trial software for SQL Server and Windows Server 2008 as listed later.

You will also need either Windows Vista or Windows XP SP2—there is currently no free download link available at Microsoft.com.

For Chapters 7 and 8, you must download additional software if you do not have the Windows SBS 2003 Premium edition:

- **Windows Server 2008** You can download an evaluation version of Windows Server 2008 from the Microsoft Download Center at *http://www.microsoft.com/downloads/details.aspx?FamilyId=B6E99D4C-A40E-4FD2-A0F7-32212B520F50&displaylang=en*.
- **Microsoft SQL Server 2008 64-bit or 32-bit (or Windows Server 2003 and SQL Server 2005)** You can download SQL Server 2008 Enterprise edition from the Microsoft SQL Server 2008 Web site at *http://www.microsoft.com/sqlserver/2008/en/us/trial-software.aspx?WT.mc_id=82ADC32B-77F7-46F6-8B85-3FBD6FF82CFD&WT.srch=1*.

For Chapter 8, you need a fully configured server running Windows Small Business Server 2003 or Windows Small Business Server 2003 R2. There is currently no free download link available at Microsoft.com.

Practice Setup Instructions

The practice exercises in this training kit require a minimum of two computers or virtual machines:

- **Chapters 1 through 6** One server running Windows SBS 2008 configured as a domain controller and one computer running Windows Vista (Enterprise, Business, or Ultimate) or Windows XP SP2.

- **Chapter 7** One server running Windows SBS 2008 (primary server) and configured as a domain controller, and one server running Windows SBS 2008 Premium edition (second server). If you do not have Windows SBS 2008 Premium edition, you can use Windows Server 2008, which will act as the second server for the purpose of the exercises.
- **Chapter 8** One server on which you can install Windows SBS 2008 and one server running Windows Small Business Server 2003 or Windows Small Business Server 2003 R2.

All computers must be physically connected to the same network. It is recommended that you use an isolated network that is not part of your production network to perform the practices in this book. To minimize the time and expense of configuring physical computers, you might consider using virtual machines.

The companion CD of this book contains a Microsoft Office Word document (Contoso Company Profile.doc) that was used by the content developers to create the fictitious company profile and all user accounts. You can use this document to assist you when working through the practice exercises.

To perform the exercises in Chapters 1 through 6, you must follow the exercise steps in Chapter 1, and then follow the chapters numerically. Each chapter builds on the preceding chapters.

To perform the exercises in Chapter 7, you can continue using the Windows SBS 2008 server built and configured in Chapters 1 through 6. You will need to install the second server using Windows SBS 2008 Premium edition (or if you do not have this edition, install Windows Server 2008, which will act as the second server for the purpose of the exercises).

To perform the exercises in Chapter 8, you will need to perform a new installation of Windows SBS 2008 by following the instructions provided in the exercises in Chapter 8. You must first build the server running Windows Small Business Server 2003, configure it for networking, and add user accounts. (This process is briefly outlined later in this introduction and in Chapter 8.) You can then follow the instructions provided in Chapter 8 to perform the migration.

Preparing the Network Environment

All practice exercises should be performed on an isolated network. The router configuration is part of the Windows SBS 2008 installation and setup. If you are using physical machines, be sure to connect practice machines using a designated router, separate from your production network. The same applies if you are setting up a virtual environment. The physical network adapter to which the virtual network is bound, must also be connected to a designated router.

Preparing the Computer Running Windows Small Business Server 2008

To install the computer running Windows SBS 2008 for the practice exercises in this book, you need to perform the practice exercises in Lesson 3 of Chapter 1, "Installing Windows Small Business Server 2008 Standard Edition." The practice in Lesson 4 of Chapter 1 walks you through the initial tasks and prepares the server running Windows SBS 2008 for the remaining chapter practices. Chapters 2 through 6 in the book build on the preceding chapters, so it is recommended that you perform the practice exercises in order. Chapters 7 and 8 contain stand-alone practices that require you to repurpose the computers used in Chapters 1 through 6.

Preparing the Computer Running Windows Vista

Perform the following actions to prepare the computer running Windows Vista for the practices in this training kit.

- **Check operating system version requirements** In System Control Panel (found in the System And Maintenance category), verify that the operating system version is Windows Vista Enterprise, Windows Vista Business, or Windows Vista Ultimate. If necessary, choose the option to upgrade to one of these versions.
- **Name the computer** In Control Panel, under System, specify a computer name.
- **Configure networking** To configure networking, carry out the following tasks:
  - In Control Panel, click Set Up File Sharing. In the Network And Sharing Center, verify that the network is configured as a private network and that File Sharing is enabled.
  - In the Network And Sharing Center, click Manage Network Connections. In Network Connections, open the properties of the Local Area Connection, select the Network Adapter, and select Internet Protocol Version 4 (TCP/IPv4). Configure the TCP/IP properties to obtain an IP address automatically. You do not require a default gateway.

Preparing the Computer Running Windows Small Business Server 2008 Premium (Second Server)

For Chapter 7, perform the following actions to prepare the computer running Windows SBS 2008 Premium (or Windows Server 2008) for the practices in this training kit:

- Install Windows SBS 2008 Premium (or Windows Server 2008) following the instructions on the installation media.
- On the Configure Your Server screen, name the computer Server02.
- Assign an IP address of 192.168.1.3 with a subnet mask 255.255.255 and the default gateway 192.168.1.1.

Preparing the Computer Running Windows Small Business Server 2003

For Chapter 8, perform the following actions to prepare the computer running Windows Small Business Server 2003 or Windows Small Business Server 2003 R2 for the practices in this training kit:

- Install the server running Windows Small Business Server 2003 following the default settings during setup. Name the server SBS2003 and use the domain name Contoso.com.
- Use the To Do List to start the Connect To The Internet Wizard and Email Connection Wizard (CEICW). In the CEICW, configure the server to use a single NIC only and assign an IP address of 192.168.1.27, subnet mask of 255.255.255, and the default gateway 192.168.1.1. Configure the DNS server address as 192.168.1.2, leave all other settings at their default, and complete the wizard.
- Create several user accounts using the Contoso Company Profile.doc from this book's companion CD. Set up Gregory Weber as an administrator (with the user name gregoryw) and Jay Hamlin as a user (with the user name jayh) and preferably several other user accounts from the Contoso Company Profile.doc, with a password of P@ssword.
- Install all the latest service packs required by Windows Small Business Server 2003. (This information is found in Chapter 8 in the section titled “Prepare the Source Server for Migration.”)
- Optional: If you would like to test the mailbox migration, add additional user accounts and open some of the users’ mailboxes and send e-mail among them. This way you can later verify the Exchange Server 2007 mailbox migration functioned successfully.
- Optional: Use the Windows SBS Best Practice Analyzer contained on the companion CD or download it at *http://www.microsoft.com/downloads/details.aspx?familyid=3874527A-DE19-49BB-800F-352F3B6F2922&displaylang=en* and run it on the server running Windows Small Business Server 2003 to verify its integrity.

System Requirements for the Companion CD

To use the companion CD-ROM, you need a computer running Windows Server 2008, Windows Vista, Windows Server 2003, or Windows XP. The computer must meet the following minimum requirements:

- 1-GHz 32-bit (x86) or 64-bit (x64) processor
- 1 GB of system memory

- A hard disk partition with at least 1 GB of available space
- A monitor capable of at least 800 × 600 display resolution
- A keyboard
- A mouse or other pointing device
- An optical drive capable of reading CD-ROMs

The computer must also have the following software:

- A Web browser such as Internet Explorer version 6 or later
- An application that can display PDF files, such as Adobe Acrobat Reader, which can be downloaded at *http://www.adobe.com/reader*
- An application that can display Word files, such as Microsoft Word or a Word document viewer

These requirements support use of the companion CD-ROM. To perform the practice exercises in this training kit, you will require additional hardware or software, as detailed previously.

Using the Companion CD

The companion CD included with this training kit contains the following:

- **Practice tests** You can practice for the 70-653 certification exam by using tests created from a pool of 200 realistic exam questions, which give you many practice exams to ensure that you are prepared.
- **Practice files** A company profile including user names has been added to provide a quick small business challenges overview and add context to the practice exercises. The companion CD includes the Windows Small Business Server 2003 Best Practices Analyzer as well as the Migration documentation and Migration Help file, which should be used in conjunction with Chapter 8.
- **An eBook** An electronic version (eBook) of this book is included for when you do not want to carry the printed book with you. The eBook is in Portable Document Format (PDF), and you can view it by using Adobe Acrobat or Adobe Reader.
- **Sample chapters** This CD includes sample chapters from related Microsoft Press titles. These chapters are in PDF format.

Digital Content for Digital Book Readers: If you bought a digital-only edition of this book, you can enjoy select content from the print edition's companion CD.
Visit **http://www.microsoftpressstore.com/title/9780735626782** to get your downloadable content. This content is always up-to-date and available to all readers.

How to Install the Practice Tests

To install the practice test software from the companion CD to your hard disk, perform the following steps:

1. Insert the companion CD into your CD drive and accept the license agreement. A CD menu appears.

> ***NOTE*** **IF THE CD MENU DOES NOT APPEAR**
>
> **If the CD menu or the license agreement does not appear, AutoRun might be disabled on your computer. Refer to the Readme.txt file on the CD for alternate installation instructions.**

2. Click Practice Tests and follow the instructions on the screen.

How to Use the Practice Tests

To start the practice test software, follow these steps:

1. Click Start, click All Programs, and then click Microsoft Press Training Kit Exam Prep. A window appears that shows all the Microsoft Press training kit exam prep suites installed on your computer.
2. Double-click the lesson review or practice test you want to use.

Lesson Review Options

When you start a lesson review, the Custom Mode dialog box appears so that you can configure your test. You can click OK to accept the defaults, or you can customize the number of questions you want, how the practice test software works, which exam objectives you want the questions to relate to, and whether you want your lesson review to be timed. If you are retaking a test, you can select whether you want to see all the questions again or only the questions you missed or did not answer.

After you click OK, your lesson review starts.

- To take the test, answer the questions and use the Next and Previous buttons to move from question to question.
- After you answer an individual question, if you want to see which answers are correct—along with an explanation of each correct answer—click Explanation.
- If you prefer to wait until the end of the test to see how you did, answer all the questions, and then click Score Test. You will see a summary of the exam objectives you chose and the percentage of questions you got right overall and per objective. You can print a copy of your test, review your answers, or retake the test.

Practice Test Options

When you start a practice test, you choose whether to take the test in Certification Mode, Study Mode, or Custom Mode:

- **Certification Mode** Closely resembles the experience of taking a certification exam. The test has a set number of questions. It is timed, and you cannot pause and restart the timer.
- **Study Mode** Creates an untimed test during which you can review the correct answers and the explanations after you answer each question.
- **Custom Mode** Gives you full control over the test options so that you can customize them as you like.

In all modes, the user interface when you are taking the test is basically the same but with different options enabled or disabled depending on the mode. When you review your answer to an individual practice test question, a "References" section is provided that lists where in the training kit you can find the information that relates to that question and provides links to other sources of information. After you click Test Results to score your entire practice test, you can click the Learning Plan tab to see a list of references for every objective.

How to Uninstall the Practice Tests

To uninstall the practice test software for a training kit, use the Programs And Features option in Windows Control Panel.

Microsoft Certified Professional Program

The Microsoft certifications provide the best method to prove your command of current Microsoft products and technologies. The exams and corresponding certifications are developed to validate your mastery of critical competencies as you design and develop, or implement and support, solutions with Microsoft products and technologies. Computer professionals who become Microsoft-certified are recognized as experts and are sought after industry-wide. Certification brings a variety of benefits to the individual and to employers and organizations.

> ***MORE INFO*** **ALL THE MICROSOFT CERTIFICATIONS**
>
> **For a full list of Microsoft certifications, go to *http://www.microsoft.com/learning/mcp/default.asp*.**

Small Business Specialist Community

When you pass Exam 70-653: TS: Windows Small Business Server 2008, Configuring, you qualify to become a Microsoft Small Business Specialist. The Microsoft Small Business Specialists community is a group of Microsoft Partners that specialize in the design, deployment, and customization of small-business solutions using Microsoft technologies such as Windows SBS 2008.

Microsoft Small Business Specialists enjoy special benefits within the Microsoft Partner Program after they have successfully met several requirements put forth by Microsoft. Some of the benefits include access to exclusive resources such as the Small Business Specialist Online Technical Community, product launch resources, training, offers and promotions, and technical and sales resources. To become a Small Business Specialist, you have to complete the following steps:

1. First you must enroll in the Microsoft Partner Program (MSPP). Becoming a Microsoft Registered Partner is free of charge and it only takes a couple of minutes to join. After you enroll, you have access to free Microsoft resources. You can enroll in the Microsoft Partner Program by going to *https://partner.microsoft.com/US/40032508*.
2. Next, you must complete the Small Business Sales and Marketing Skills Assessment. You can take an online tutorial on the Microsoft Partner Program Site before taking the Skills Assessment, which consists of approximately 20 questions. The questions asked in the Skills Assessment are not technical and are more a scenario-based assessment of your knowledge of selling Microsoft Solutions to small business. No worries, the Small Business Sales and Marketing Skills Assessment is an on-demand assessment free of charge that you can take online (and repeat any time if necessary). To take the online tutorial, visit *https://training.partner.microsoft.com/plc/details.aspx?systemid=8748&page=/plc/search.aspx* (you must be a Microsoft Partner to access this site). To take the online Small Business Sales and Marketing Skills Assessment, visit *https://training.partner.microsoft.com/plc/register.aspx?publisher=3&courseid=542*.
3. You must also sign up for the Microsoft Action Pack Subscription (MAPS) at *http://partner.microsoft.com/actionpack*, which costs $299 a year in the United States and varies in price depending on which country you live in. Even if you do not plan on becoming a Small Business Specialist, subscribing to MAPS is one of the best benefits of being a Microsoft Registered Partner in terms of receiving loads of Microsoft products. You will receive full version software and sales resources once every three months so that you can test and use (in-house) Not-For-Distribution Software including Windows SBS 2008 Standard edition (localized version) and many more products. Visit *https://partner.microsoft.com/40016455* to learn more about MAPS and the software content you will receive. Once you have become

a Small Business Specialist, you will also receive the Small Business Specialist Community Special Edition Toolkit in addition to the MAPS regular software shipment.

4. Take the 70-653: TS: Windows Small Business Server 2008, Configuring exam. Based on the fact that you are holding this book in your hand, you are well on your way to passing the exam and fulfilling this part of the requirements for becoming a Small Business Specialist. But remember, you must also fulfill the preceding three steps.

For more information about the Small Business Specialist Community partner program, see the Microsoft Partner site at *https://partner.microsoft.com/US/program/smallbusinessspecialist*.

You can also connect with a Small Business Specialist Partner Area Lead (PAL) in your country. Go to *https://partner.microsoft.com/global/40011087* and select your region. Contact a PAL to learn more about what the Small Business Specialist Community has to offer and how to get involved with the Small Business Specialist Community.

Technical Support

Every effort has been made to ensure the accuracy of this book and the contents of the companion CD. If you have comments, questions, or ideas regarding this book or the companion CD, please send them to Microsoft Press by using either of the following methods:

E-mail:

- tkinput@microsoft.com

Postal Mail:

- *Microsoft Press*

  Attn: MCTS Self-Paced Training Kit (Exams 70-653): Configuring Windows
  Small Business Server 2008, *Editor*

  One Microsoft Way

  Redmond, WA 98052–6399

For additional support information regarding this book and the CD (including answers to commonly asked questions about installation and use), visit the Microsoft Press Technical Support Web site at *www.microsoft.com/learning/support/books/*. To connect directly to the Microsoft Knowledge Base and enter a query, visit *http://support.microsoft.com/search/*. For support information regarding Microsoft software, connect to *http://support.microsoft.com*.

CHAPTER 2

Managing Users

Although managing users might seem like one of the more mundane aspects of managing Windows Small Business Server (Windows SBS) 2008, a good plan for creating and managing user accounts goes a long way toward ensuring that users have access to the proper resources they need to perform their jobs. A good plan also helps improve security by ensuring that people who don’t need access to particular resources do not have it.

If you work for a small business, the day-to-day management of users might be your task to handle. If you consult for small businesses, your task more likely is to set up a good user management structure and then train an employee of the business to take on day-to-day responsibilities.

In this chapter, you learn to manage users with three features:

- **User accounts** A user account is a collection of information about a user on the network. This information includes the person’s user account name, password, group memberships, and so on.
- **User roles** A user role is essentially a user account template that you can use to standardize common user account needs, such as permissions, disk quotas, Windows SharePoint memberships, and so on. Creating a user account based on a user role saves you from having to configure user accounts individually and also reduces the likelihood of errors when creating user accounts. You enter unique information, such as the user name and password, and the user role is used as a template for the rest of the user account information.
- **Groups** A group is a collection of users or other groups. Windows SBS 2008 supports two types of groups: the security group, which allows members to access network resources, and the distribution group, which allows a message to be sent to a number of users without having to address that message to each individual user.

Most documentation you read discusses these three features in the order presented here, and many administrators like to jump right in creating user accounts. However, when you are designing a user management structure it is more efficient to think about groups and user roles first. Because a group is typically used to provide access to a particular resource, you should design your groups first. Because user roles often involve group membership (among other things), they should come second. And after you have a good group and user role structure set up, then it's time to start adding user accounts.

This chapter introduces you first to groups, then to user roles, and then to user accounts.

Exam objectives in this chapter:

- Modify groups.
  - Create, edit, and delete groups.
- Modify user roles.
  - Create, edit, and delete roles.
- Modify users.
  - Create, edit, and delete users.

Before You Begin

To complete this chapter, you must have:

- Basic knowledge of Windows-based operating systems.
- Experience working with Windows-based networks.
- A server running Windows SBS 2008.

Lesson 1: Managing Groups

Groups provide a logical way to manage resources on a network. Instead of assigning access to a resource to a number of individual user accounts, you can place those user accounts into a group and then assign the group access to the resource. For example, if certain users require access to a high-end color printer, you can create a group that has access to that printer and then place the user accounts for those users into that group.

Estimated lesson time: 20 minutes

Understanding Types of Groups

Windows SBS 2008 supports two basic types of groups:

- **Distribution group** A distribution group is used to send e-mail messages to a group of user accounts at one time. For example, you might create a distribution group for part-time employees so that management could send them targeted messages more easily. Management would simply send an e-mail message to a single address for the group rather than having to send messages to (and keep up with) the individual accounts.
- **Security group** A security group is used to control access to a network resource, such as a shared folder or printer.

Exploring Built-In Groups

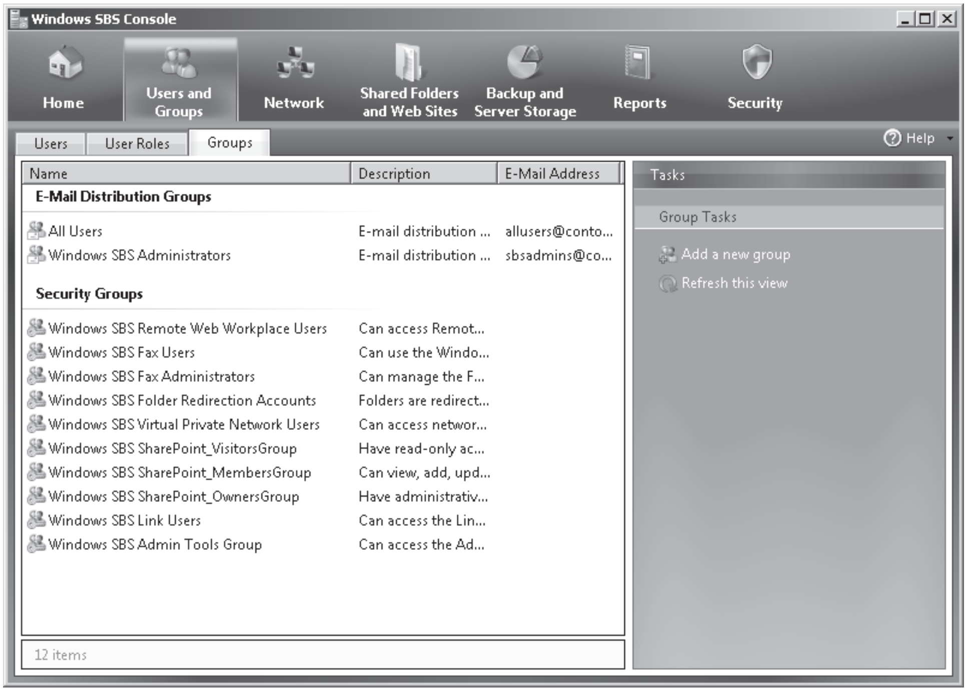
Windows SBS 2008 creates a number of groups automatically during installation. These built-in groups cover the basic functionality of Windows SBS 2008. The built-in groups are described in Table 2-1.

TABLE 2-1 Built-In Groups in Windows SBS 2008

GROUP NAME	GROUP TYPE	DESCRIPTION
All Users	Distribution	Used for sending e-mail messages to all the users in the Windows SBS 2008 network
Windows SBS Administrators	Distribution	Used for sending e-mail messages to all the administrators in the Windows SBS 2008 network
Windows SBS Remote Web Workplace Users	Security	Contains members who can access Remote Web Workplace
Windows SBS Fax Users	Security	Contains members who can use the Windows SBS Fax service
Windows SBS Fax Administrators	Security	Contains members who can manage the Windows SBS Fax service

GROUP NAME	GROUP TYPE	DESCRIPTION
Windows SBS Folder Redirection Accounts	Security	Contains members who have their folders redirected to the server
Windows SBS Virtual Private Network Users	Security	Contains members who can access network resources remotely
Windows SBS SharePoint_VisitorsGroup	Security	Contains members who can read the internal Web site
Windows SBS SharePoint_MembersGroup	Security	Contains members who can view, add, delete, update, approve, and customize the content on the internal Web site
Windows SBS SharePoint_OwnersGroup	Security	Contains members who have administrative access to the internal Web site
Windows SBS Link Users	Security	Contains members who can access the Link list in Remote Web Workplace
Windows SBS Admin Tools Users	Security	Contains members who can access the Administration tools in Remote Web Workplace

You can view these groups, and any groups you have created, in the Windows SBS Console. Just click the Users And Groups tab on the Navigation bar, and then click the Groups tab, as shown in Figure 2-1.



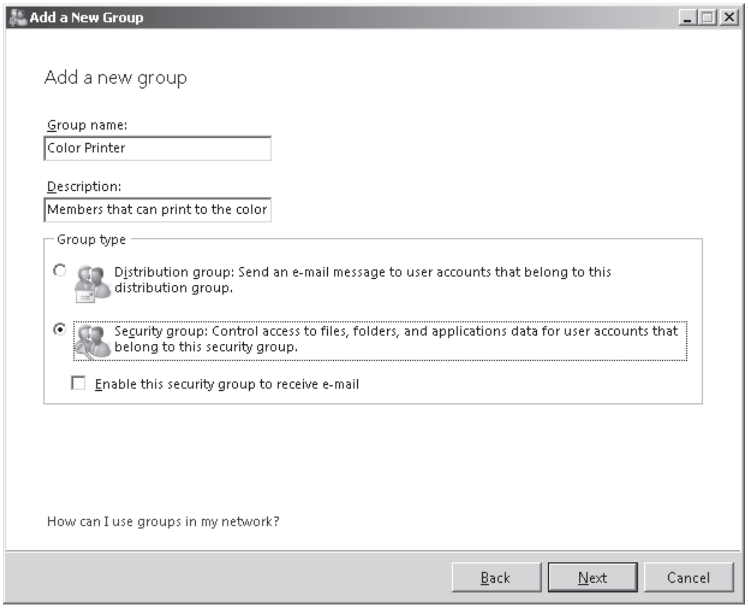
Name	Description	E-Mail Address
E-Mail Distribution Groups		
All Users	E-mail distribution ...	allusers@conto...
Windows SBS Administrators	E-mail distribution ...	sbsadmins@co...
Security Groups		
Windows SBS Remote Web Workplace Users	Can access Remot...	
Windows SBS Fax Users	Can use the Windo...	
Windows SBS Fax Administrators	Can manage the F...	
Windows SBS Folder Redirection Accounts	Folders are redirect...	
Windows SBS Virtual Private Network Users	Can access networ...	
Windows SBS SharePoint_VisitorsGroup	Have read-only ac...	
Windows SBS SharePoint_MembersGroup	Can view, add, upd...	
Windows SBS SharePoint_OwnersGroup	Have administrativ...	
Windows SBS Link Users	Can access the Lin...	
Windows SBS Admin Tools Group	Can access the Ad...	

12 items

FIGURE 2-1 Viewing groups in the Windows SBS Console

Creating a Group

Creating a new group is simple. In the Groups tab, in the Tasks pane, click Add A New Group. The Add A New Group Wizard, shown in Figure 2-2, asks you to perform the following tasks:



Add a new group

Group name: Color Printer

Description: Members that can print to the color

Group type

○ Distribution group: Send an e-mail message to user accounts that belong to this distribution group.

● Security group: Control access to files, folders, and applications data for user accounts that belong to this security group.

□ Enable this security group to receive e-mail

How can I use groups in my network?

FIGURE 2-2 Creating a new group

- **Type a group name and description** Although you can name a group anything you like, you should make the group name descriptive of the function the group performs or the resource to which it allows access.
- **Choose a group type** Choose whether you are creating a distribution group or security group. The choice you make determines the options you see in the rest of the Add A New Group Wizard.
- **Set an e-mail address** If you choose a distribution group or enable a security group to receive e-mail, you will see an additional wizard page on which you can set the group e-mail address and configure additional e-mail delivery options, including whether people outside the company can send messages to the group or (for security groups only) whether messages sent to the group on a SharePoint Services Web site are archived.
- **Choose members for the group** You are presented with a list of user accounts you can add to the group.

EXAM TIP

For the exam, you should know that you can set an e-mail address for both security and distribution groups. However, to archive messages sent to the group using a SharePoint Services Web site, you must use an e-mail-enabled security group.

***IMPORTANT* USE THE WINDOWS SBS CONSOLE**

You should use the Windows SBS Console rather than Active Directory Users And Computers to create groups and other network objects. Although some administrators balk at using the wizard interface, they should not. The wizards are quite powerful and perform many actions behind the scenes to ensure a correct setup. With groups particularly, creating a group in Active Directory Users And Computers does not ensure that Group Policy settings in Windows SBS 2008 are properly applied. In fact, groups created in Active Directory Users And Computers often don't even show up in the Windows SBS Console. The lesson here is that you should always use the Windows SBS Console to perform tasks whenever possible.

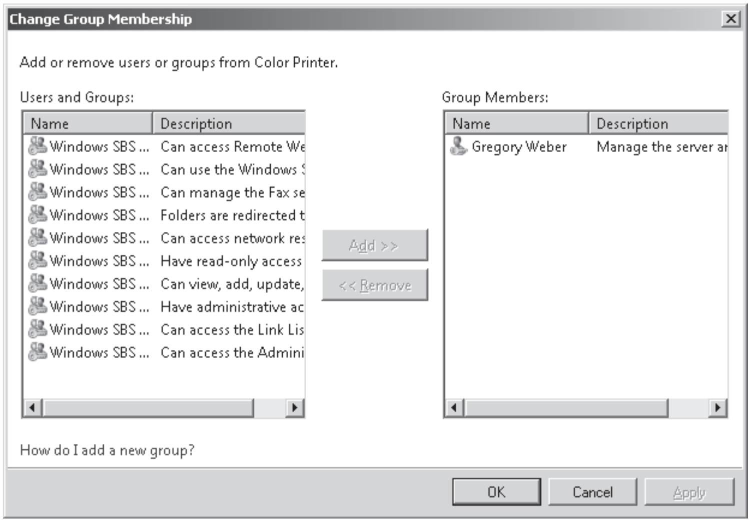
Removing a Group

Removing a group is even easier than creating one. In the Groups tab, select the group, and then in the Tasks pane, click Remove Group. You are asked to confirm your choice, and then the group is gone.

Keep in mind that when you remove a group, members of that group lose any access rights they are granted by the group, such as access to shared folders and printers.

Changing Group Membership

After a group has been created, you can change membership in that group. In the Groups tab, select the group, and then in the Tasks pane, click Change Group Membership. On the Change Group Membership page, shown in Figure 2-3, select users and groups from the list on the left, and then click Add to add those members to the group. Select users and groups from the list on the right, and then click Remove to remove those users from the group.



Change Group Membership

Add or remove users or groups from Color Printer.

Users and Groups:

Name	Description
Windows SBS ...	Can access Remote We
Windows SBS ...	Can use the Windows S
Windows SBS ...	Can manage the Fax se
Windows SBS ...	Folders are redirected t
Windows SBS ...	Can access network res
Windows SBS ...	Have read-only access
Windows SBS ...	Can view, add, update,
Windows SBS ...	Have administrative ac
Windows SBS ...	Can access the Link Lis
Windows SBS ...	Can access the Admini

Group Members:

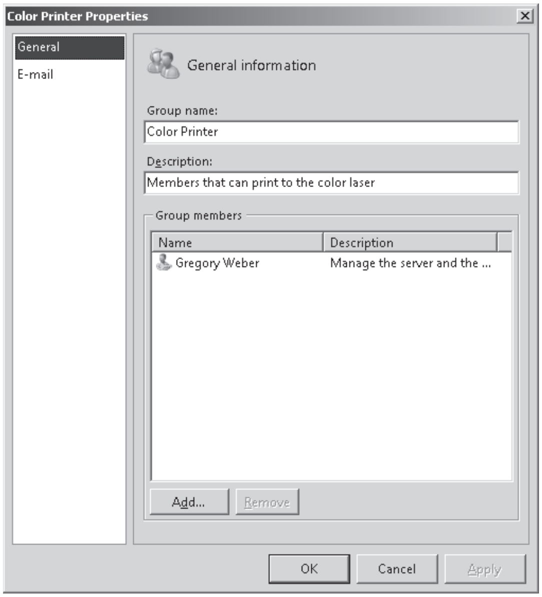
Name	Description
Gregory Weber	Manage the server ar

How do I add a new group?

FIGURE 2-3 Changing group membership

Editing Group Properties

By editing group properties, you can change general information about the group, such as the group name and description, as well as the e-mail address associated with the group. In the Group tab, select the group, and then in the Tasks pane, click Edit Group Properties. On the Properties page, shown in Figures 2-4 and 2-5, you can make these changes.



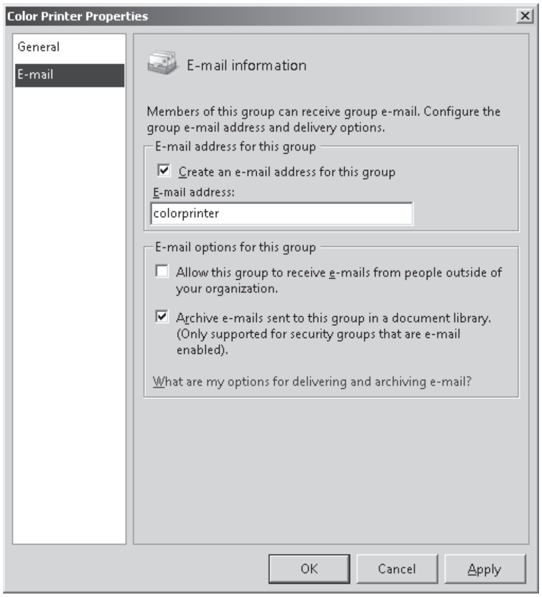
Group name: Color Printer

Description: Members that can print to the color laser

Group members

Name	Description
Gregory Weber	Manage the server and the ...

FIGURE 2-4 Editing general group information



Members of this group can receive group e-mail. Configure the group e-mail address and delivery options.

E-mail address for this group

☑ Create an e-mail address for this group

E-mail address: colorprinter

E-mail options for this group

☐ Allow this group to receive e-mails from people outside of your organization.

☑ Archive e-mails sent to this group in a document library. (Only supported for security groups that are e-mail enabled).

FIGURE 2-5 Editing a group e-mail address

PRACTICE Managing Groups

The exercises in this Practice familiarize you with creating and modifying a group in Windows SBS 2008.

EXERCISE 1 Create a Group

In this exercise, you create a new group.

1. In the Windows SBS Console, click the Users And Groups tab on the Navigation bar.
2. Click the Groups tab.
3. In the Tasks pane, click Add A New Group.
4. On the Getting Started page of the Add A New Group Wizard, click Next.
5. On the Add A New Group page, provide the following information, and then click Next:
   - Group Name: **Color Printer**
   - Description: **Color Laser Printer on 2nd Floor**
   - Group Type: Select the Security Group option
6. On the Select Group Members For Color Printer page, click Add Group.
7. Click Finish.

EXERCISE 2 Modify a Group's Properties

In this exercise, you practice modifying a group's properties by changing the group name.

1. In the Windows SBS Console, click the Users And Groups tab on the Navigation bar.
2. Click the Groups tab.
3. In the list of groups, select the Color Printer group.
4. In the Tasks pane, click Edit Group Properties.
5. Change the Group Name from Color Printer to **Color Laser Printer** and click OK.

EXERCISE 3 Modify a Group's Membership

In this exercise, you add a member to an existing group.

1. In the Windows SBS Console, click the Users And Groups tab on the Navigation bar.
2. Click the Groups tab.
3. In the list of groups, select the Color Laser Printer group.
4. In the Tasks pane, click Change Group Membership.
5. In the Users And Groups list, click Gregory Weber.
6. Click Add and then click OK.

✓ Quick Check

- What are the two types of groups in Windows SBS 2008?
- What does an e-mail-enabled security group support that a distribution group does not?
- When you remove a security group, what happens to the access rights that group provides to its members?

Quick Check Answers

- The two types of groups in Windows SBS 2008 are distribution and security groups.
- With an e-mail-enabled security group, you can archive messages sent to the group through a SharePoint Services Web site.
- When you delete a security group, its members lose all access rights granted to them by the group. This can result in loss of access to shared folders, printers, and other resources.

Lesson 2: Managing User Roles

A user role is a template for creating a user account. User roles contain user account information such as group, disk space quotas, e-mail quotas, Windows SharePoint Services site group memberships, organizational unit placement, remote access permissions, and company address information. By using user roles, you can easily create new user accounts by supplying only the unique information such as the user name and password.

Estimated lesson time: 20 minutes

Exploring Built-In User Roles

Windows SBS 2008 includes three built-in user roles:

- **Standard User** User accounts based on this user role have access to shared folders, printers and faxes, e-mail, Remote Web Workplace, Windows SharePoint Services, and the Internet. Standard users cannot perform administrative tasks such as installing new applications or hardware drivers or changing many system settings.
- **Standard User With Administration Links** User accounts based on this user role have all the permissions of the Standard User role. In addition, these accounts can view the Administration links from the Remote Web Workplace and the Desktop Links gadget. After clicking one of these links, the user must enter network administrator credentials to access server Administration links.
- **Network Administrator** User accounts based on this user role are members of the Domain Administrators group and have unrestricted system and network access.

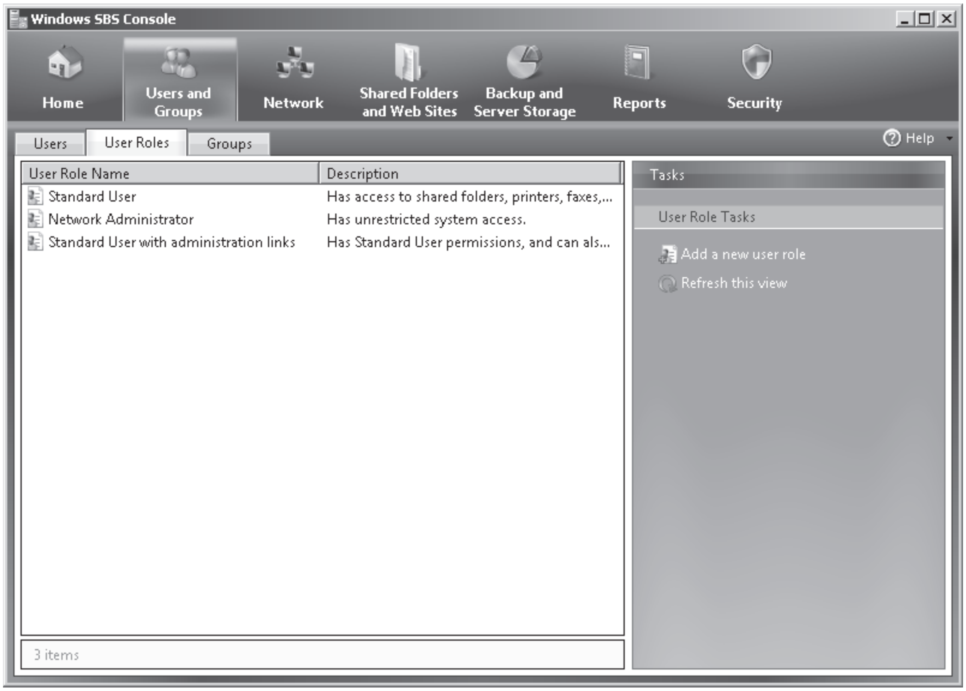
For the most part, these user roles cover most users in most installations of Windows SBS 2008. You can simply edit the properties of the Standard User role to include group memberships, company information, and so on.

However, at times you will need to create a new user role. For example, if a business has part-time employees that require different rights and permissions than regular employees do, you might want to create a new user role to make it easier to create and modify user accounts for the part-time employees.

> ***IMPORTANT*** **DO NOT USE ADMINISTRATIVE ACCOUNTS FOR DAILY ACTIVITIES**
>
> **Because administrative user accounts have powerful rights, you should not use them for performing daily work even though it can be tempting to do so. Instead, use a standard user account for daily work and use an administrative account only when necessary.**

Creating a User Role

Creating a new user role is, like most tasks in Windows SBS 2008, very simple. In the Windows SBS Console, click the Users And Groups tab on the Navigation bar, and then click the User Roles tab, shown in Figure 2-6. In the Tasks pane, click Add A New User Role to open the Add A New User Role Wizard.

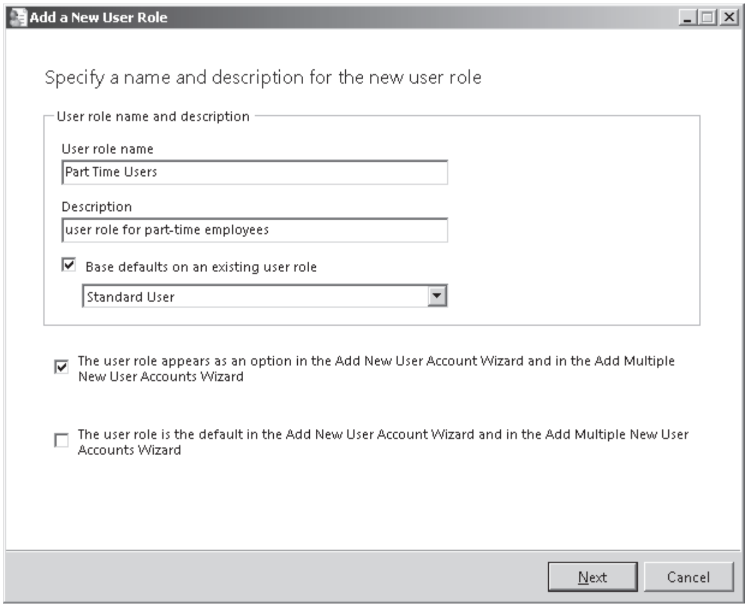


User Role Name	Description
Standard User	Has access to shared folders, printers, faxes,...
Network Administrator	Has unrestricted system access.
Standard User with administration links	Has Standard User permissions, and can als...

3 items

FIGURE 2-6 Viewing user roles in the Windows SBS Console

The Add A New User Role Wizard, shown in Figure 2-7, asks you to provide the following information:



Specify a name and description for the new user role

User role name and description

User role name: Part Time Users

Description: user role for part-time employees

☑ Base defaults on an existing user role

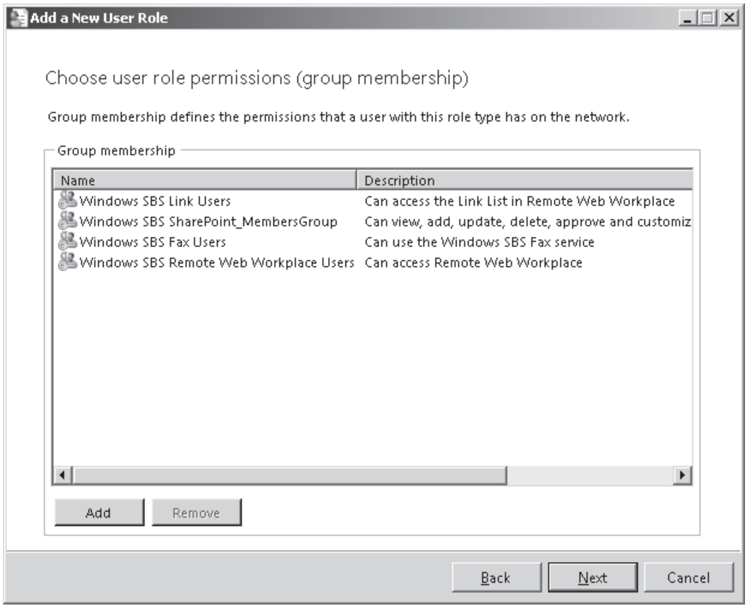
Standard User

☑ The user role appears as an option in the Add New User Account Wizard and in the Add Multiple New User Accounts Wizard

☐ The user role is the default in the Add New User Account Wizard and in the Add Multiple New User Accounts Wizard

FIGURE 2-7 Creating a new user role

- **User Role Name And Description** Type a name and description that befit the new user role.
- **Whether you want to base the user role on an existing user role** If you have a user role that is close in functionality to the user role you are creating, you can base the new user role on the existing user role. For example, if you are creating a user role for part-time employees, it is likely that much of the information will be the same as the Standard User role.
- **How the user role interacts with the Add A New User Account Wizard** You can choose whether the new user role appears as an option in the Add A New User Account Wizard and the Add Multiple New User Accounts Wizard and also whether the new role should be the default choice in those wizards.
- **Permissions for the user role** Permissions for the new user role are handled through group memberships. You can choose to which groups users defined by this user role should belong, as shown in Figure 2-8.



Choose user role permissions (group membership)

Group membership defines the permissions that a user with this role type has on the network.

Name	Description
Windows SBS Link Users	Can access the Link List in Remote Web Workplace
Windows SBS SharePoint_MembersGroup	Can view, add, update, delete, approve and customiz
Windows SBS Fax Users	Can use the Windows SBS Fax service
Windows SBS Remote Web Workplace Users	Can access Remote Web Workplace

FIGURE 2-8 Choosing permissions for the new user role

- **E-mail settings** You can enforce mailbox quotas for users based on the role and specify whether users should be able to use Outlook Web Access to connect to the Exchange server. By default, a mailbox quota of 2 GB is configured and access to Outlook Web Access is allowed. Mailbox quotas are covered in the section titled "Modifying a User Role" later in this chapter. Outlook Web Access is covered in Chapter 6, "Managing Messaging and Collaboration."

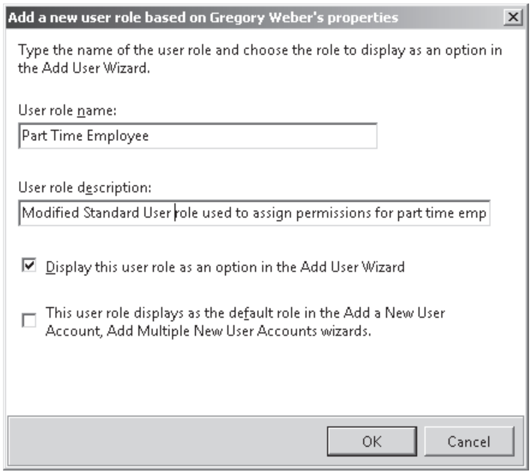
- **Remote access settings** You can specify whether user accounts based on this user role have access to Remote Web Workplace and the virtual private network (VPN). The default settings include access to Remote Web Workplace, but not to the VPN. You learn more about Remote Web Workplace and virtual private networking in Chapter 5, "Managing and Configuring Remote Access."
- **Shared folder access** You can enforce a quota for shared folders for users based on the role. By default, a new role enforces a 2-GB quota for shared folders. You can also choose whether folder redirection is enabled for the user role. By default, it is not. You can learn more about folder redirection in Chapter 3, "Joining Clients to the Windows Small Business Server Domain."

After creating a new user role, you are given the option of adding new user accounts immediately. You can also just create the new role and add user accounts later. You learn how to do this in the section titled "Creating User Accounts" later in this chapter.

Creating a User Role Based on a User Account

Another way to create a new user role is to base the role on an existing user account. In the Windows SBS Console, click the Users And Groups tab on the Navigation bar, and then click the Users tab. Select the account on which you want to base the new user role, and then in the Tasks pane, click Add A New User Role Based On This User Account's Properties.

All you have to do is type a user role name and description, as shown in Figure 2-9, and specify whether the new user role appears as an option in the Add A New User Account Wizard and the Add Multiple New User Accounts Wizard and also whether the new role should be the default choice in those wizards.



Add a new user role based on Gregory Weber's properties

Type the name of the user role and choose the role to display as an option in the Add User Wizard.

User role name: Part Time Employee

User role description: Modified Standard User role used to assign permissions for part time emp

☑ Display this user role as an option in the Add User Wizard

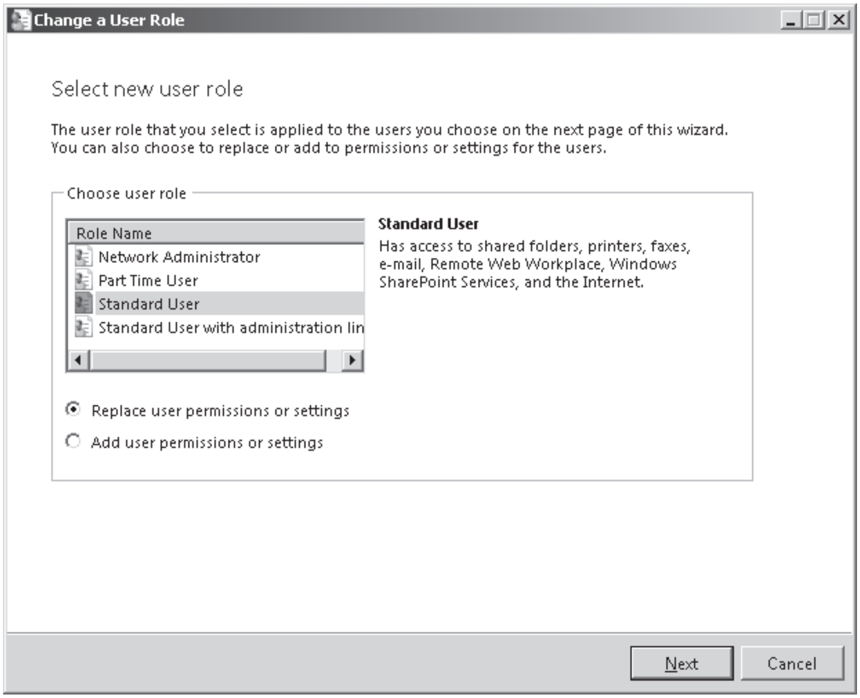
☐ This user role displays as the default role in the Add a New User Account, Add Multiple New User Accounts wizards.

FIGURE 2-9 Creating a new user role based on an existing user account

Removing a User Role

To remove a user role, you must first remove any user accounts from the role by changing the accounts to a different role. You can do this in two different ways:

- After selecting the user role you want to remove and clicking Remove User Role, the Windows SBS Console warns you if there are users you need to remove. It automatically starts the Change A User Role Wizard, shown in Figure 2-10, so that you can assign a new role to the users.
- You can start the Change A User Role Wizard yourself by clicking the Users tab, and then in the Tasks pane, clicking Change User Role For User Accounts.



Change a User Role

Select new user role

The user role that you select is applied to the users you choose on the next page of this wizard. You can also choose to replace or add to permissions or settings for the users.

Choose user role

Role Name
Network Administrator
Part Time User
Standard User
Standard User with administration lin

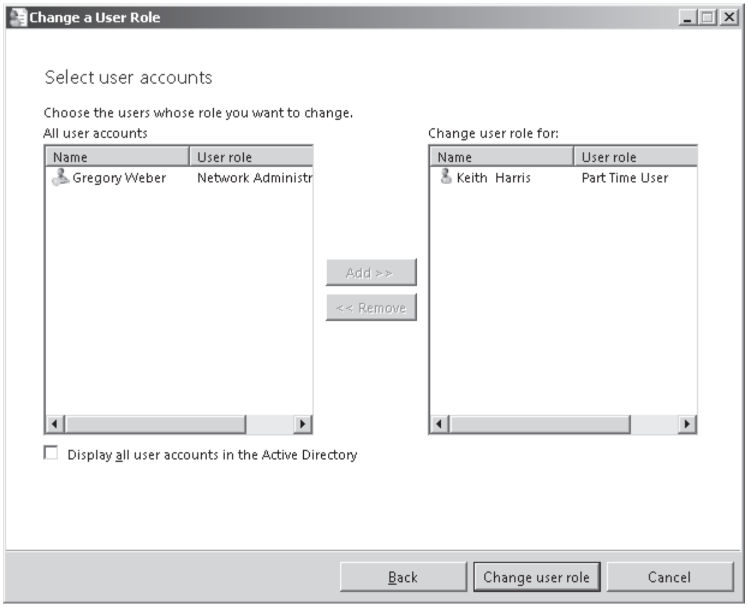
Standard User
Has access to shared folders, printers, faxes, e-mail, Remote Web Workplace, Windows SharePoint Services, and the Internet.

● Replace user permissions or settings

○ Add user permissions or settings

FIGURE 2-10 Changing user roles for user accounts

Choose the new role to associate with the user accounts. You also need to choose whether the permissions and settings from the new role should replace those from the existing role or be added to them. After clicking Next, you can choose the user accounts whose role you want to change, as shown in Figure 2-11. If you are removing a user role, you need to change all associated accounts.



Change a User Role

Select user accounts

Choose the users whose role you want to change.

All user accounts

Name	User role
Gregory Weber	Network Administr

Change user role for:

Name	User role
Keith Harris	Part Time User

□ Display all user accounts in the Active Directory

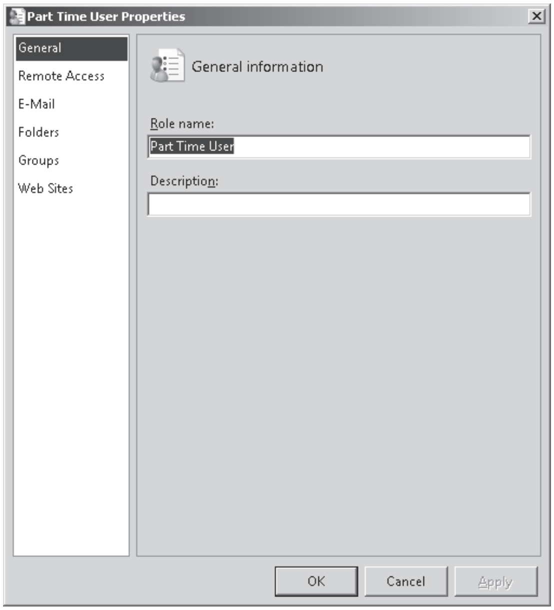
FIGURE 2-11 Choosing user accounts for which to change roles

Modifying a User Role

By editing user role properties, you can change all the same information about the user role that you configured when you created the user role. To edit a user role's properties, in the Windows SBS Console, click the Users And Groups tab on the Navigation bar, and then click the User Roles tab. Select the user role you want to modify, and then click Edit User Role Properties. The user role properties page is shown in Figure 2-12.

You can modify user role information in the following tabs:

- **General** Change the user role name and description.
- **Remote Access** Change whether user accounts based on this role can access Remote Web Workplace and the VPN.
- **E-Mail** Enable, disable, or change the mailbox quota for user accounts based on the role.
- **Folders** Change whether a quota is enforced for shared folders and the quota size, as well as folder redirection options.
- **Groups** Change the group membership for user accounts based on the user role.
- **Web Sites** Change whether user accounts based on the user role can access Remote Web Workplace, the internal Web site, and Outlook Web Access.



Role name: Part Time User

Description:

FIGURE 2-12 Editing a user role's properties

PRACTICE Managing User Roles

The exercises in this Practice walk you through the management of user roles. You create a new user role and modify the user role's properties.

EXERCISE 1 Create a User Role

In this exercise, you create a new user role. You provide a name and description, assign permissions, and set shared folder and remote access.

1. In the Windows SBS Console, click the Users And Groups tab on the Navigation bar.
2. Click the User Roles tab.
3. In the Tasks pane, click Add A New User Role.
4. On the Specify A Name And Description For The New User Role page of the Add A New User Role Wizard, type the following information:
   - User Role Name: **Part Time Employee**
   - Description: **Modified Standard User account for part time employees**
5. Leave the remaining options at their default settings, and click Next.
6. Because part-time employees might not need access to the Windows SBS Link and Remote Web Workplace, on the Choose User Role Permissions (Group Membership) page, remove the following group memberships, and then click Next:
   - Windows SBS Link Users
   - Windows SBS Remote Web Workplace Users

7. On the Choose E-Mail Settings page, change the Size Of Mailbox Quota (In GB) setting to 1.0, and then click Next.
8. On the Choose Remote Access For This User Role page, leave the options at their default settings, and then click Next.
9. In this example, you limit the amount of space provided to part-time employees to 1 GB to preserve space on the server. To do so, on the Choose Shared Folder Access For This User Role page, change the Quota In GB setting to 1.0, and then click Add User Role.
10. Click Finish.

EXERCISE 2 Modify a User Role's Properties

Sometimes the needs of an organization change. In this exercise, you practice modifying a user role's properties by changing the settings applied to the Part Time Employee user role.

1. In the Windows SBS Console, click the Users And Groups tab on the Navigation bar.
2. Click the User Roles tab.
3. In the list of user roles, select the Part Time Employee user role.
4. In the Tasks pane, click Edit User Role Properties.
5. In the list of categories on the left, click the Remote Access tab.
6. Select This User Role Can Access Remote Web Workplace.
7. In the list of categories on the left, click the Folders tab.
8. Because the organization has decided to increase the size of shared folders allowed for part-time employees, change the Maximum Shared Folder Size (In GB) setting to 2.0 GB.
9. Click OK.
10. In the Apply User Role Changes dialog box, click Yes, and then click OK.

✓ Quick Check

- **What are the three built-in user roles in Windows SBS 2008?**
- **Does a Standard User account have permission to install a new application on a workstation?**
- **What steps must you take when removing a user role?**

Quick Check Answers

- **The three built-in user roles in Windows SBS 2008 are Standard User, Standard User With Administration Links, and Network Administrator.**
- **No. A Standard User account does not have permission to install a new application on a workstation.**
- **When removing a user role, you must first remove any user accounts from the role by reassigning them to a different role.**

Lesson 3: Managing User Accounts

Any person who logs on to computers on the network needs a user account. User accounts provide a way to identify users who log on to a network, control which resources those users can access, and provide information about those users.

Estimated lesson time: 20 minutes

Understanding User Account Management

Before you get started adding users to your network, you need to take care of a few things first, including the following:

- Create a good structure of groups that control access to the various resources on the network. Although it's possible to (and likely that you will need to) create additional groups later on, taking the time to create groups up front forces you to think about resource allocation on the network. And the more up-front planning you do, the better it is in the long run.
- Create any necessary user roles. Although it's probable that the built-in user roles cover most needs, take the time to determine whether a business would be well served by additional user roles. Again, up-front planning is easier than making changes later.
- Plan a user account naming strategy. Although this is less important on small networks than on networks with thousands of users, with a good user account naming strategy, you can standardize the way user accounts are named.
- Create a strong password policy. Passwords are a vital part of network security. Taking the time to create and enforce a strong password policy is essential.

Naming User Accounts

By creating a naming plan for user accounts, you can standardize the way users are named, which in turn helps users and administrators more easily recognize and remember user names and e-mail addresses. You can choose from many different conventions for naming user accounts, but the following list shows a few popular strategies:

- The user's full first and last name, separated by a period
- The user's first initial and last name
- The user's first name and last initial

The naming convention you choose for a business really isn't that important. What is important is that you choose and follow a convention.

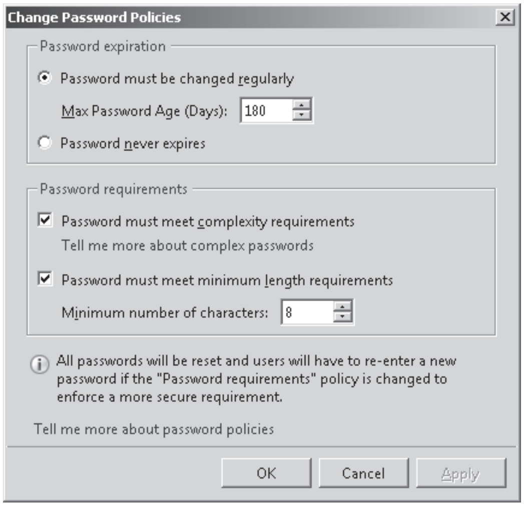
Creating Strong Passwords

Password policies are enabled during Windows SBS 2008 installation. By default, the following policies are set:

- Passwords must be changed every 180 days. It is sometimes hard to strike a balance between forcing passwords to be changed often enough to optimize security, but not so often as to unduly annoy users. The default 180 days is actually a bit on the long side, with a period closer to 42 days (every six weeks) much more secure.
- Passwords must meet complexity requirements. To meet the complexity requirements in a US-English localized installation, a password must be at least six characters long and must contain three out the following four characteristics: uppercase English characters, lowercase English characters, numbers, and nonalphabetic characters.
- Passwords must meet minimum length requirements. Windows SBS 2008 by default enforces a minimum password length of eight characters (superseding the six-character length defined by password complexity).

You can change the password policy for a server using the following steps:

1. In the Windows SBS Console, click the Users And Groups tab on the Navigation bar.
2. Click the Users tab.
3. In the Tasks pane, click Change Password Policies.
4. Use the Change Password Policies dialog box, shown in Figure 2-13, to change the policies.



Change Password Policies

Password expiration

● Password must be changed regularly

Max Password Age (Days): 180

○ Password never expires

Password requirements

☑ Password must meet complexity requirements

Tell me more about complex passwords

☑ Password must meet minimum length requirements

Minimum number of characters: 8

All passwords will be reset and users will have to re-enter a new password if the "Password requirements" policy is changed to enforce a more secure requirement.

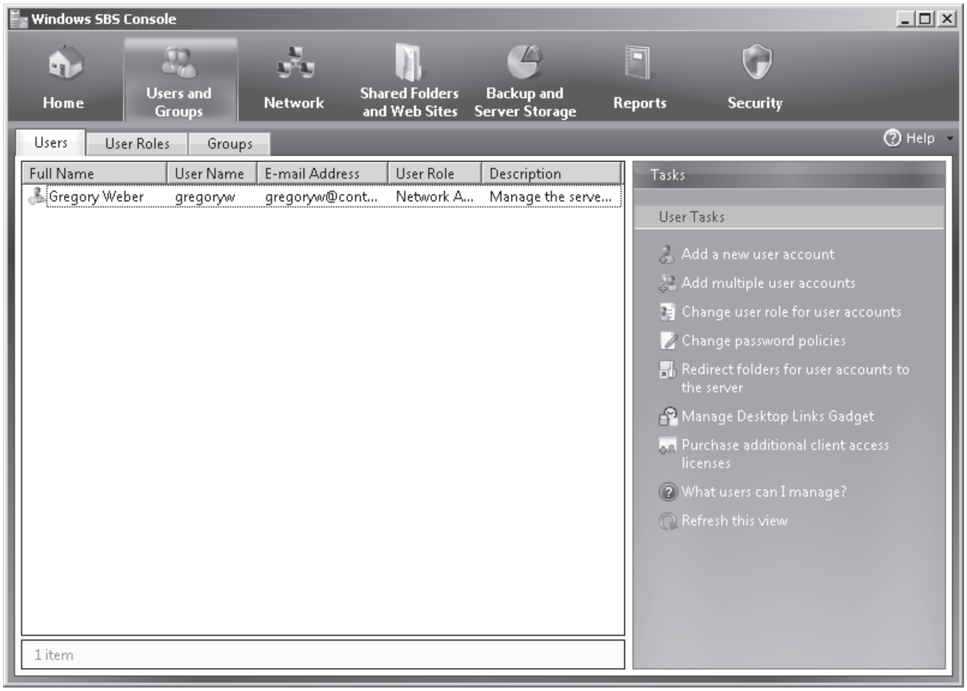
Tell me more about password policies

FIGURE 2-13 Changing password policies

For more information about creating strong passwords, see *http://technet.microsoft.com/en-us/library/cc794302.aspx*. For information about educating users to select strong passwords, see *http://technet.microsoft.com/en-us/library/dd353107.aspx*.

Creating User Accounts

Creating a new user account uses a simple wizard interface, just like most tasks in Windows SBS 2008. In the Windows SBS Console, click the Users And Groups tab on the Navigation bar, and then click the Users tab, as shown in Figure 2-14. In the Tasks pane, click Add A New User Account to open the Add A New User Account Wizard.


Windows SBS Console
Home
Users and Groups
Network
Shared Folders and Web Sites
Backup and Server Storage
Reports
Security
Users
User Roles
Groups
Help
Tasks
User Tasks
Add a new user account
Add multiple user accounts
Change user role for user accounts
Change password policies
Redirect folders for user accounts to the server
Manage Desktop Links Gadget
Purchase additional client access licenses
What users can I manage?
Refresh this view

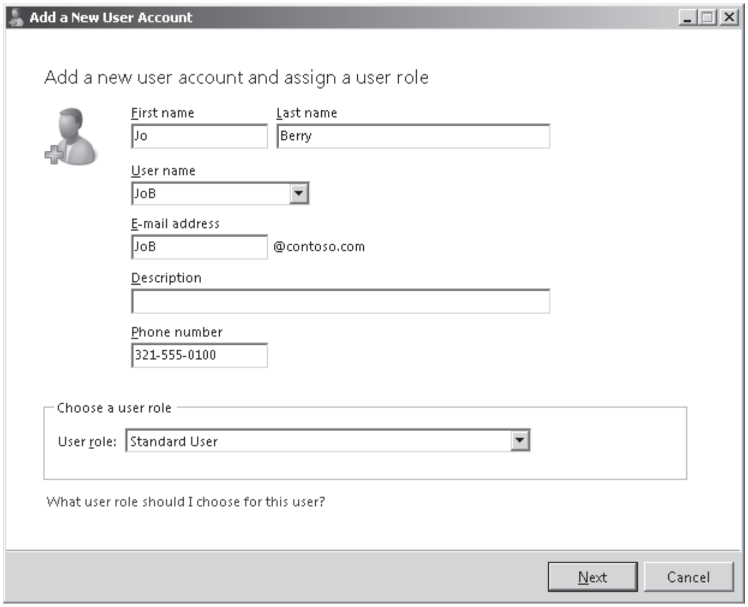
Full Name	User Name	E-mail Address	User Role	Description
Gregory Weber	gregoryw	gregoryw@cont...	Network A...	Manage the serve...

1 item

FIGURE 2-14 Viewing user accounts in the Windows SBS Console

The Add A New User Account Wizard, shown in Figure 2-15, asks you to provide the following information:

- **User account general information and user role** Type a first and last name, a user name (if you want to use something different from the default suggestions that Windows SBS 2008 provides in the drop-down box), a description, and a phone number. Also choose a user role on which to base the new user account.
- **Password** Type and confirm a password for the user. Passwords must conform to the current password policies.
- **Computer** After the user account is created, the Add A New User Account Wizard gives you the option to associate an existing computer in the domain with the user account or to add a new computer for the user account. A user account can be associated with multiple computers. You must add a computer to a user account for each computer in the domain to which the user is allowed to log on. You can learn more about creating computer accounts in Chapter 3.



Add a New User Account

Add a new user account and assign a user role

First name: Jo

Last name: Berry

User name: JoB

E-mail address: JoB @contoso.com

Description:

Phone number: 321-555-0100

Choose a user role

User role: Standard User

What user role should I choose for this user?

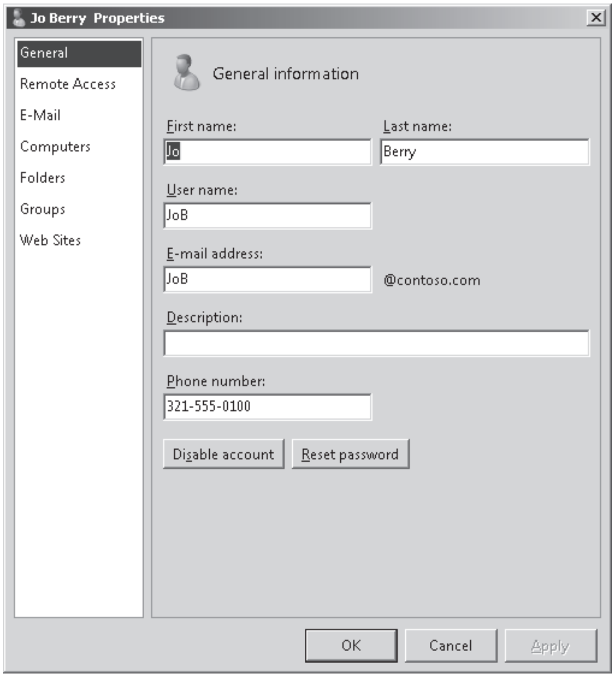
FIGURE 2-15 Adding a new user account

Editing a User Account

You can change information about the user account by editing user account properties. To edit a user account's properties, in the Windows SBS Console, click the Users And Groups tab on the Navigation bar, and then click the Users tab. Select the user account you want to modify, and then click Edit User Account Properties. The user account properties page is shown in Figure 2-16.

You can modify user role information using the following tabs:

- **General** Change the first and last names, user name, e-mail, description, and phone number. You can also use this page to disable an account and to reset a user's password. (Disabling a user account is discussed in the section titled "Disabling and Enabling a User Account" later in this chapter.)
- **Remote Access** Change whether user accounts based on this role can access Remote Web Workplace and the VPN.
- **E-Mail** Enable, disable, or change the mailbox quota for user accounts based on the role. Changing the quota for an individual user overrides settings provided by the user role with which the account is associated.
- **Computers** Add or remove computers in the domain to which the user account can log on.
- **Folders** Change whether a quota is enforced for shared folders and the quota size, as well as folder redirection options.



Jo Berry Properties

General information

First name: Jo

Last name: Berry

User name: JoB

E-mail address: JoB @contoso.com

Description:

Phone number: 321-555-0100

FIGURE 2-16 Editing a user account's properties

- **Groups** Change the group membership for user accounts based on the user role.
- **Web Sites** Change whether user accounts based on the user role can access Remote Web Workplace, the internal Web site, and Outlook Web Access.

Removing a User Account

After you remove a user account, you cannot retrieve it. To remove a user account, select the user account in the Users tab, and then in the Tasks pane, click Remove User Account. Windows SBS 2008 confirms that you want to remove the account and also allows you to specify whether to delete the user's mailbox and shared folders at the same time.

Resetting a User Account Password

If a user forgets his or her password, you can reset it. To do so, select the user account in the Users tab, and then in the Tasks pane, click Reset User Account Password. There is also a link to this same tool on the General page when you edit a user account's properties. Type and confirm the new password, and then click OK. After you have reset the user account's password, the user can and should change the password as soon as possible.

Disabling and Enabling a User Account

When you disable a user account, the account can no longer be used to log on to the network. Disabling a user account is useful when you need to deny log on to the user, but do not want to delete the account or the rights and permissions associated with it.

You can also disable accounts automatically if the user tries to log on with a bad password too many times.

To disable a user account, select the user account in the Users tab, and then click Disable User Account. When an account is disabled, the Disable User Account link changes to Enable User Account. Click that link to enable the user account.

You should also note that when you disable a user account for a user that is currently logged on, the user can still access the network as long as he or she stays logged on. After logging off, the user will not then be able to log on again while the account is disabled.

PRACTICE Managing User Accounts

The exercises in this Practice walk you through the management of user accounts. You create a new user account, modify the user account's properties, reset the user account's password, and disable and then re-enable the account.

EXERCISE 1 Create a User Account

In this exercise, you practice creating a user account for Patrick Hines. You specify a first and last name, user account name, and password.

1. In the Windows SBS Console, click the Users And Groups tab on the Navigation bar.
2. Click the Users tab.
3. In the Tasks pane, click Add A New User Account.
4. On the Add A New User Account And Assign A User Role page of the Add A New User Account Wizard, type the following information:
   - First Name: **Patrick**
   - Last Name: **Hines**
   - User Name: **PatrickH**
5. Leave the remaining options at their default settings, and click Next.
6. On the Create A Password For Accessing Your Network page, type the following information, and then click Add User Account:
   - Password: **P@ssw0rd**
   - Confirm Password: **P@ssw0rd**
7. Click Finish.

EXERCISE 2 Modify a User Account's Properties

In this exercise, you practice modifying a user account's properties by allowing the user account access to virtual private networking and increasing the allowed shared folder size to 3 GB.

1. In the Windows SBS Console, click the Users And Groups tab on the Navigation bar.
2. Click the Users tab.
3. In the list of user accounts, select the Patrick Hines user account.

4. In the Tasks pane, click Edit User Account Properties.
5. In the list of categories on the left, click the Remote Access tab.
6. Select User Can Access Virtual Private Network.
7. In the list of categories on the left, click the Folders tab.
8. Change the Maximum Shared Folder Size (In GB) setting to 3.0 GB.
9. Click OK.

EXERCISE 3 Reset User Account's Password

In this exercise, you reset a user account's password. If a user forgets the password for a user account, you cannot recover the forgotten password. You must reset the password by creating a new one, and then provide the new password to the user.

1. In the Windows SBS Console, click the Users And Groups tab on the Navigation bar.
2. Click the Users tab.
3. In the list of user accounts, select the Patrick Hines user account.
4. In the Tasks pane, click Reset User Account Password.
5. In the Reset The User Password Wizard, type the following information, and then click OK:
   - Password: **Lion24dunk**
   - Confirm Password: **Lion24dunk**

EXERCISE 4 Disable and Reenable a User Account

In this exercise, you practice disabling and reenabling a user account. Disabling a user account is useful when a user should no longer have access to the network (such as when that user leaves the company) but the permissions and rights assigned to that user account should remain intact. For example, a new user might take over the responsibilities of the previous user. User accounts can also become disabled automatically if the user attempts to log on with an invalid password more times than is allowed by server policy.

1. In the Windows SBS Console, click the Users And Groups tab on the Navigation bar.
2. Click the Users tab.
3. In the list of user accounts, select the Patrick Hines user account.
4. In the Tasks pane, click Disable User Account.
5. Click OK.
6. In the Tasks pane, click Enable User Account and then click OK.

✓ Quick Check

- By default, what is the minimum-length password enforced for user accounts by Windows SBS 2008?
- Can a single user account be associated with more than one computer?
- If you disable a user account while a user is currently logged on, what happens?

Quick Check Answers

- By default, Windows SBS 2008 enforces an eight-character minimum password length.
- Yes. A user account can be associated with multiple computers. You must add a computer to a user account for each computer in the domain to which the user is allowed to log on.
- If you disable a user account while a user is currently logged on, the user can still access the network as long as he or she stays logged on. After logging off, the user cannot log on again while the account is disabled.

Case Scenario: Managing Users and Computers

You are setting up Windows SBS 2008 for Contoso, Ltd., a 35-person law firm in Orlando, Florida, that practices real estate, condemnation/eminent domain, estate planning, civil rights/discrimination, business torts, and class action lawsuits. The firm consists of four managing partners, eight additional lawyers, and six paralegals, two receptionists, eight clerical office staff, and seven interns. The firm has 35 workstations in the office and a laptop for each attorney (12 total).

The company has the following requirements:

- The managing partners should have no disk quota set for either shared folders or mailboxes. Interns should have a disk quota of 1 GB set for both shared folders and mailboxes. Other employees should have a disk quota set to the default value.
- The managing partners should have access to the virtual private network. Other employees should not.
- All employees except for the interns should have access to a set of shared folders named Clients on the server.
- A new large-format color laser printer has been installed. Managing partners, other lawyers, and their receptionists should have access to the printer. Other employees and interns should not.
- All employees and interns should have access to the other laser printers on the network. There are six other laser printers.
- All employees and interns should have access to the Windows SBS 2008 Fax service.

Answer these questions for your manager:

1. What new groups should you create for the network to suit the preceding criteria?
2. What new user roles should you create? How should they be configured?

Suggested Practices

To help you successfully master the exam objectives presented in this chapter, complete the following tasks.

Modify Groups

- **Practice 1** Explore the memberships of each of the built-in groups.
- **Practice 2** Create a new distribution group and send an e-mail message to the group.

Modify Users

- **Practice 1** Add multiple users by using the Add Multiple New User Accounts Wizard.

Chapter Summary

- A user account is a collection of information about a user on the network. This information includes the person's user account name, password, group memberships, and so on.
- A user role is essentially a user account template that you can use to standardize common user account needs, such as permissions, disk quotas, SharePoint memberships, and so on.
- A group is a collection of users or other groups. Windows SBS 2008 supports two types of groups: the security group, which allows members to access network resources, and the distribution group, which allows a message to be sent to a number of users without having to address that message to each individual user.
- You should plan your group and user roles before creating new user accounts.
- Use the Windows SBS Console rather than other Windows Server operating system tools to add groups, user roles, and user accounts to ensure a correct setup.
- Use standard user accounts rather than administrator accounts for daily work.
- Use password policies and teach employees about strong passwords and safe password practices.

CHAPTER 5

Managing and Configuring Remote Access

Once considered an enterprise-only feature, remote access to network resources such as e-mail and scheduling functions has become affordable and widely popular for small businesses today. The Windows Small Business Server 2008 (Windows SBS) server software embraces remote access wholeheartedly and comes with remote access capabilities preconfigured, requiring only minimal input on the administrator's part.

Out-of-the-box features include a self-issued certificate, a Web portal for remote access called Remote Web Workplace (RWW), and Microsoft Exchange Server features for mobile device access. Users can access business contact information, calendars, e-mail, files, and other important desktop and network resources from a Web browser on any Internet-connected computer, including from a mobile device, at any time and from anywhere.

Naturally, the server and remote access clients must meet certain specifications, and some businesses will modify the default settings and customize users' remote access permissions to certain resources. Most of this can be done in the Windows SBS Console, and administrators can use native Windows Server 2008 tools to perform advanced configurations without breaking functionality in the Windows SBS Console.

This chapter discusses secure access to the server using self-issued and third-party certificates, default Remote Web Workplace settings, how to configure Remote Web Workplace, as well as how to enable and configure a virtual private network (VPN) in Windows SBS. Chapter 6, "Managing Messaging and Collaboration," discusses Outlook Anywhere and mobile device connectivity in greater detail.

Exam objectives covered in this chapter:

- Modify Remote Web Workplace (RWW).
- Modify RAS.
    - User permissions.

Before You Begin

To complete this chapter you must have a server and a client computer set up in a physical or virtual environment as follows:

- A server running Windows SBS 2008 that is configured per the instructions given in Chapter 1, "Installing Windows Small Business Server 2008 Standard Edition"
- A client computer running the Windows XP Professional operating system with Service Pack 2 (SP2), the Windows Vista Business operating system, the Windows Vista Enterprise operating system, or the Windows Vista Ultimate operating system

Lesson 1: Managing Certificates

Having remote access to organization resources is great, but some Windows Small Business Server users will wonder whether it is secure. Small business owners tend to be frugal and expect a high return on their investment without having to spend additional money. Therefore, Windows SBS offers two types of certificates to secure remote access and communication: a self-issued certificate option, and the option to install a third-party certificate. Regardless of the choice, Windows SBS 2008 makes it easy to implement certificates on the network.

Estimated lesson time: 60 minutes

Understanding Certificates in Windows Small Business Server

Consider a certificate. It is issued by a certification authority (CA) and is an electronic representation of an object (user, computer, service, or network device). A certificate is used with a public and a private key pair. When the CA issues a public key certificate (such as the self-issued certificate in Windows Small Business Server), two keys are created:

- **A private key** This key is known only to the key's owner.
- **A public key** This key is known by other entities on the network.

The public key is published or shared with others. Other users can also retrieve the public key from the certificate and use it to encrypt communication data. The data encrypted by the public key can be decrypted only by using the private key.

In general, a certificate contains the following information:

- Information about the issuing CA
- Information about the object holding the private key created by the certificate
- The public key of the certificate
- Information about the validity or revocation status of the certificate
- Name of the digital signing algorithms supported by the certificate

During installation of Windows SBS 2008, the Active Directory Certificate Services (AD CS) and Certificate Authority (CA) are installed automatically.

- The AD CS creates, manages, and removes x.509 certificates for applications such as Secure/Multipurpose Internet Mail Extensions (S/MIME) and Secure Sockets Layer (SSL). This service is required to create certificates.
- The CA issues and manages the certificates. It accepts certificate requests, verifies the information according to the CA policy, and issues its private key to apply its digital signature to the certificate.

NOTE **PROOF OF IDENTITY**

The Certificate Authority (CA) requires distinct proof of identity of the certificate requester. In this case, the Microsoft CA uses a user's account credentials as proof of identity, authenticating the requester based on the account in Active Directory Domain Services.

For more information about how AD CS works, see "Active Directory Certificate Services" at Microsoft TechNet (*http://technet.microsoft.com/en-us/library/cc534992.aspx*).

Self-Issued Certificates

Every CA has a certificate to confirm its identity. Often, this certificate is issued by another, trusted CA and is called the trusted CA root certificate. Windows SBS 2008 differs in that it can use its own self-issued certificate. During Windows SBS installation, a root certificate is self-issued using the internal domain name. The self-issued root certificate is stored in the certificate store from where it is pushed out through Group Policy to all domain-joined client computers.

EXAM TIP

The root certificate uses the internal domain name, is distributed to all domain-joined client computers through Group Policy, and is valid for five years. To renew the root certificate you must run the Fix My Network Wizard.

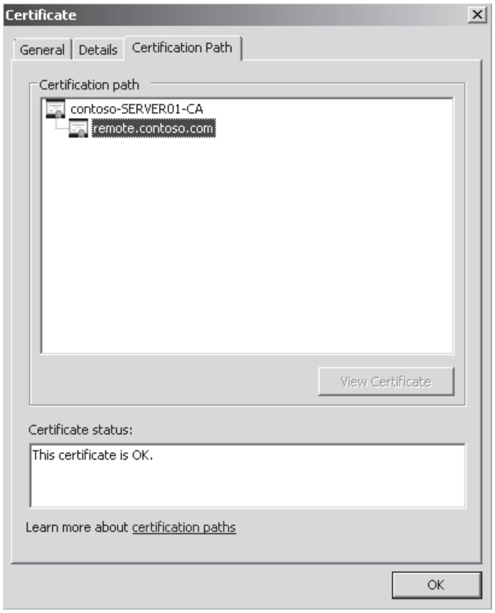
When you run the Internet Address Management Wizard, Windows SBS uses the internal domain name (when running the Internet Address Management Wizard) and creates a leaf certificate, as shown in Figure 5-1. The leaf certificate is considered a self-issued certificate and is bound to the Windows SBS 2008 Web sites in Internet Information Services (IIS) to secure communication and help protect remote access for the following components:

- Remote Web Workplace (RWW)
- Outlook Anywhere
- Windows Mobile devices
- Secure VPN (if configured)
- Secure wireless (if configured)
- Internet Protocol Security (IPSec; if configured)

The leaf certificate is valid for two years from the date of issue and uses a 1,024-bit key. At the end of two years, it is automatically renewed without affecting the users' connectivity to the server.

Third-Party Certificates

In certain situations, a third-party certificate is required, such as when a mobile operator or device does not accept a self-issued certificate. Using a self-signed certificate in these situations will cause a failure when a mobile device attempts to connect to the server. (For information about mobile device integration, see Chapter 6.)



contoso-SERVER01-CA
remote.contoso.com

This certificate is OK.

FIGURE 5-1 Path of self-issued Windows SBS certificates: The leaf certificate remote.contoso.com is displayed under the root certificate Contoso-SERVER01-CA.

The good news is that third-party certificates have become less expensive over time and are easy to manage in Windows Small Business Server. In Windows SBS 2008, you can easily integrate a third-party certificate on the network. Often people ask whether third-party certificates are more secure than self-issued certificates are. The answer is that there is no difference in terms of security from one type of certificate to the other; the difference between self-issued and third-party certificates is in the effort expended to distribute the certificates to mobile devices and remote users.

The benefit of a third-party certificate over a self-issued certificate is that most third-party root certificates are already installed on mobile devices. (Look at the certificate store on your mobile device, for example.) Most self-issued certificates must be deployed to and installed on each mobile device or remote client, which requires more effort, depending on how many client devices you have to manage if the certificate must be distributed to remote locations.

For instance, say you have 40 sales agents in the field who need to have remote access from their mobile devices and non-domain-joined laptops. If you use a self-issued certificate, you must install the self-issued certificate on each mobile device and laptop. That could turn into quite a task, especially if the sales agents come to the office only randomly or you have to travel to their location for the installation. On the other hand, the root certificate of a third-party certificate will already be installed on the mobile devices and laptops, and you will need to install only the corresponding code-signing certificate on the server. Even the most cost-conscious small business can agree that a one-time $60 fee for the third-party certificate and 10 minutes of a technician's time to install a third-party certificate is less expensive than installing a self-issued certificate on multiple non-domain-joined clients!

Administering Third-Party Certificates

The Add A Trusted Certificate Wizard in Windows SBS 2008 can assist you in requesting and installing a third-party certificate from a CA. The trusted certificate will replace the default self-issued certificate when it is installed on the server.

Before you can request a third-party certificate you must have run the Internet Address Management Wizard and registered and configured a public Internet address for the server. (See Chapter 1 Lesson 4, "Performing Initial Getting Started Tasks," for more information.)

The Add A Trusted Certificate Wizard is located in the Windows SBS Console, in the Network tab, in the Connectivity tab, in the task pane. The Add A Trusted Certificate Wizard administers the following tasks:

- Requesting and installing a trusted certificate
- Importing a trusted certificate
- Importing a trusted certificate request
- Removing a trusted certificate request
- Removing a trusted certificate

NOTE **MANAGING THE LEAF CERTIFICATE**

The leaf certificate is valid for two years and is easily renewed when you run the Internet Address Management Wizard. Windows SBS 2008 creates and renews a leaf certificate by default using the supplied domain name and extension.

Request and Install a Trusted Certificate

The Add A Trusted Certificate Wizard generates a request for a trusted certificate from a CA using the information provided during installation and when the Internet Address Management Wizard was run. It generates a certificate request using encoded data based on this information. After the certificate request is generated, you can save the request to file and send the file to the CA, or you can copy the request using the Copy function, and then paste it into the space provided on the CA's Web site.

Depending on which CA you use, the request for the trusted certificate may be handled immediately and a trusted certificate made available right away, or the request may be validated offline, in which case you have to wait to receive and install the certificate.

Once the certificate request is in process, the Add A Trusted Certificate Wizard offers the following options:

- **My Certificate Provider Needs More Time To Process The Request** Choose this option when you have to wait to receive the trusted certificate. At this point a new task, Remove This Certificate Request, is added to the Connectivity task pane. Later, when you receive the certificate file from the CA, return to the Add A Trusted Certificate Wizard and select the I Have A Certificate From My Certificate Provider option.

- **I Have A Certificate From My Certificate Provider** Select this option when you receive a trusted certificate immediately from the certificate provider or when you receive a certificate later and return to this page to install it. You can paste the encoded text from the certificate provider into the message box in the Import A Trusted Certificate dialog box, or you can browse to the location where you stored the certificate file.
- **I Want To Cancel My Request** Select this option to remove a pending certificate request and reinstate the original self-issued certificate.

Import and Export a Trusted Certificate

If you already have a trusted third-party certificate in use on another server and would like to use it on the server running Windows SBS 2008, you can export the certificate and install it using the Add A Trusted Certificate Wizard. Follow these three steps:

1. **Exporting a certificate** Open Certmgr.msc (click Start, click Run, and type **certmgr.msc** in the Open box) and select the certificate to export. Several certificates may have the same name, and in that case be sure to verify that the certificate you are exporting has a valid expiration date and was issued by a trusted authority.

   You can choose from the following certificate file formats:

   - **Personal Information Exchange (PKCS #12)** This format enables the transfer of certificates and their private keys between computers or to removable media. The PKCS #12 format (.pfx) is the only format supported in the Windows Server 2008 operating system to export a certificate and its private key and requires a password.
   - **Cryptographic Message Syntax Standard (PKCS #7)** This format enables transfer between computers or to removable media of a certificate and all the certificates in its certification path.
   - **Distinguished Encoding Rules (DER) Encoded Binary X.509** This format uses the .cer extension and can be used by certification authorities to support interoperability for computers not running the Windows Server 2003 operating system or later.
   - **Base64 Encoded X.509** This encoding method was developed for S/MIME. All MIME-compliant clients can decode Base64 files. This format uses the .cer extension and can be used by CAs to support interoperability for computers not running Windows Server 2003 or later.

EXAM TIP

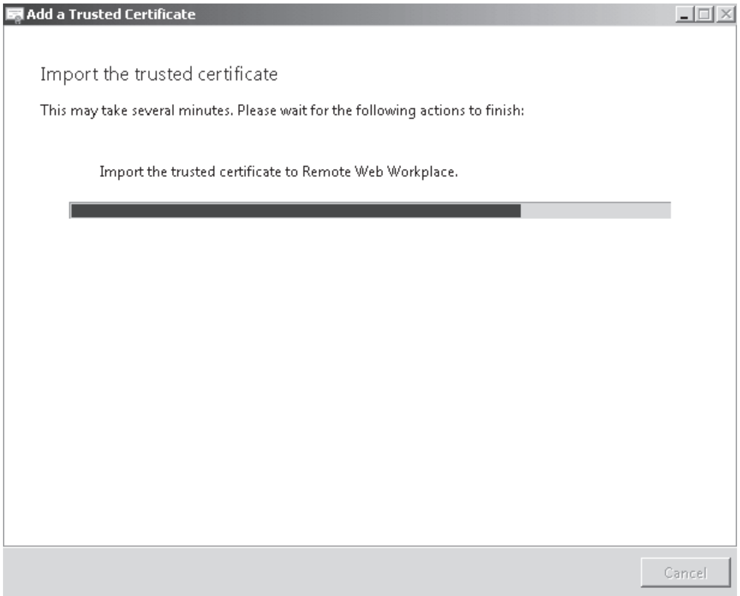
When you are exporting a certificate to be used on the server running Windows SBS 2008, select the Personal Information Exchange (PKCS #12) file format. This is the only certificate file format that will work with the Add A Trusted Certificate Wizard. When you export the certificate, you should also select the following options: Export The Private Key, Include All Certificates In The Certificate Path If Possible, and Export All Extended Properties.

During the export of the PKCS #12 file, you will be asked to provide a password and a file location for where to store the .pfx file.

2. **Importing a certificate** To import the certificate on Windows SBS 2008, use the Windows SBS Console (Advanced Mode). The Windows SBS Console (Advanced Mode) is almost identical to the standard Windows SBS Console but offers some additional options not found in the standard console. You access it by clicking Start, pointing to Administrative Tools, and clicking Windows SBS Console (Advanced Mode). In the Network tab, in the Connectivity tab, in the task pane, click Manage Certificates to open the local certificates snap-in. In the Certificates (Local Computer) console, expand Certificates, expand Personal, right-click Certificates, click All Tasks, and then click Import. Click through the Certificate Import Wizard and browse to the location where you saved the .pfx file. Next, enter the password that you created in the export procedure, ensure that the Mark This Key As Exportable and Include All Extended Properties options are selected, verify the certificate is imported into the Personal folder, and click Finish.

   Now that you have imported the certificate, you must bind it to the Windows SBS 2008 Web sites and import it using the Add A Trusted Certificate Wizard to replace the self-issued certificate.

3. **Bind the trusted certificate with Windows Small Business Server** Once you have imported the trusted certificate, run the Add A Trusted Certificate Wizard to bind the imported certificate with Windows SBS 2008. Select the I Want To Use A Certificate That Is Already Installed On The Server option, and then select the certificate from the list of certificates installed on the server. By default, this list displays only certificates with the .pfx extension. Then, click Finish. To indicate a successful binding the message The Trusted Certificate Is Imported Successfully is displayed, as shown in Figure 5-2. From now on, the trusted certificate will be used as the default certificate in Windows SBS 2008.



Import the trusted certificate

This may take several minutes. Please wait for the following actions to finish:

Import the trusted certificate to Remote Web Workplace.

FIGURE 5-2 The Add A Trusted Certificate Wizard message that signals a successful import of a third-party certificate

Remove a Trusted Certificate

If you no longer want to use a third-party certificate or the certificate has expired and will not be renewed, you can remove the third-party certificate. In the Windows SBS Console, in the Network tab, in the Connectivity tab, in the task pane, click the Remove My Trusted Certificate task. When you remove a third-party certificate, Windows SBS 2008 replaces it with the self-issued certificate and uses that.

> ***NOTE*** **MANAGING REMOTE ACCESS AFTER A TRUSTED CERTIFICATE HAS BEEN REMOVED**
>
> **When you remove a third-party certificate, remote users will have to reinstall the self-issued certificate on their mobile devices and non-domain-joined clients to access the Windows SBS 2008 network.**

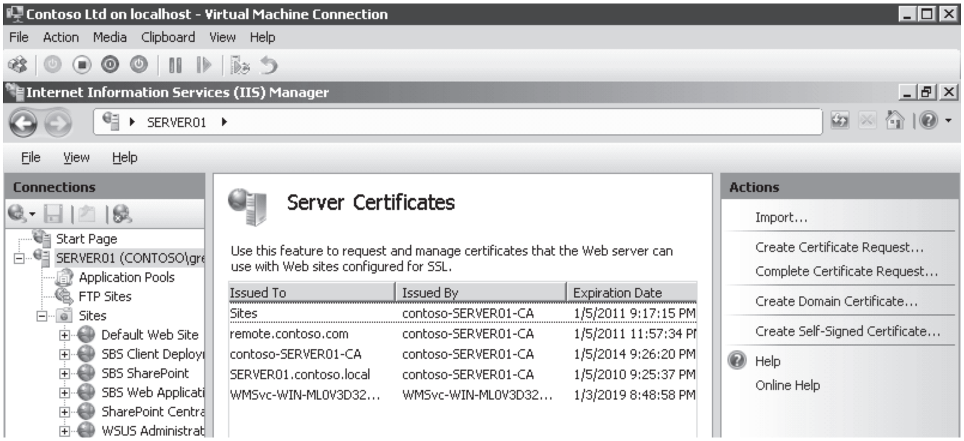
Repair a Trusted Certificate

After a third-party certificate is installed in Windows SBS 2008, a new task, Fix My Web Site Certificate, appears in the task pane of the Connectivity tab in the Windows SBS Console. If any issues should arise with the third-party certificate, consider this task as your first level of support and run the Fix My Web Site Certificate Wizard.

The wizard searches for a third-party certificate and, if one is found, rebinds it to the Web site. If the Fix My Web Site Certificate Wizard cannot find a third-party certificate, it will bind the self-issued certificate to the Windows SBS Web site instead.

> ***NOTE*** **VIEWING CERTIFICATES IN IIS**
>
> **You can view the certificates managed by the Windows Small Business Server wizards in the Internet Information Services (IIS) Manager. Click Start, point to Administrative Tools, click Internet Information Services (IIS) Manager, and then select the Server node. Scroll down and double-click the Server Certificates icon in the middle pane to open the Server Certificates feature, as shown in Figure 5-3. In the Actions pane, you can request and import trusted certificates that cannot be managed through the Add A Trusted Certificate Wizard, and you can bind trusted certificates to individual Web sites. However, administrators that use the Windows SBS Console should not need to venture into IIS Manager.**

For more details about managing common administrative tasks in IIS, see “IIS 7.0: Common Administrative Tasks” at Microsoft TechNet (*http://technet.microsoft.com/en-us/library/cc771979.aspx*) and “IIS 7.0: Configuring Server Certificates in IIS 7.0” at Microsoft TechNet (*http://technet.microsoft.com/en-us/library/cc732230.aspx*).


Contoso Ltd on localhost - Virtual Machine Connection
File Action Media Clipboard View Help
Internet Information Services (IIS) Manager
SERVER01
File View Help
Connections
Start Page
SERVER01 (CONTOSO\gre
Application Pools
FTP Sites
Sites
Default Web Site
SBS Client Deployi
SBS SharePoint
SBS Web Applicati
SharePoint Centra
WSUS Administrat
Server Certificates
Actions
Import...
Create Certificate Request...
Complete Certificate Request...
Create Domain Certificate...
Create Self-Signed Certificate...
Help
Online Help

Use this feature to request and manage certificates that the Web server can use with Web sites configured for SSL.

Issued To	Issued By	Expiration Date
Sites	contoso-SERVER01-CA	1/5/2011 9:17:15 PM
remote.contoso.com	contoso-SERVER01-CA	1/5/2011 11:57:34 PI
contoso-SERVER01-CA	contoso-SERVER01-CA	1/5/2014 9:26:20 PM
SERVER01.contoso.local	contoso-SERVER01-CA	1/5/2010 9:25:37 PM
WMSvc-WIN-ML0V3D32...	WMSvc-WIN-ML0V3D32...	1/3/2019 8:48:58 PM

FIGURE 5-3 The Internet Information Services (IIS) Manager Server Certificates page lists the self-issued certificates currently in use.

Distributing Self-Issued Certificates

By default, all domain-joined clients receive the root certificate through Group Policy regardless of whether the certificate is self-issued or from a third-party. Clients receive this certificate as long as it has been added to the certificate store and bound to the Windows Small Business Server Web sites.

The certificate file and an executable file (InstallCertificate.exe) are compressed into a certificate distribution package (Install Certificate Package.zip) and stored in the %systemdrive%\users\public\public downloads shared folder. The certificate distribution package can be downloaded onto a USB device or other removable media and taken to remote devices not joined to the domain.

NOTE **THIRD-PARTY CERTIFICATE DISTRIBUTION**

The certificate distribution package is required by Windows SBS 2008 to distribute only the self-issued root certificate. If you have a third-party certificate installed on the server, you do not need to complete the certificate distribution and installation procedure. (See the section titled "Third-Party Certificates" earlier in this chapter for details.)

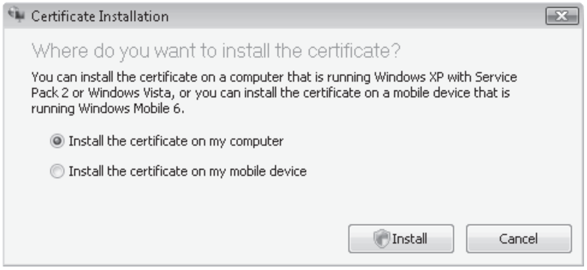
Install Certificates on Non-Domain-Joined Client Computers

To install the self-issued certificate on a remote client computer or mobile device, copy the certificate installation package from the USB device or removable media to the remote client. If you are installing the certificate to a mobile device, ensure that the mobile device is physically connected to the remote client computer.

Extract the files from Install Certificate Package.zip and open the InstallCertificate.exe file on the remote client. In the Certificate Installation dialog box that opens, you can choose where you want to install the certificate, as shown in Figure 5-4. You have two options:

- **Install The Certificate On My Computer** Choose this option on computers running Windows XP SP2 or Windows Vista.
- **Install The Certificate On My Mobile Device** Choose this option on mobile devices running Windows Mobile 6.

The Certificate Installation Wizard then installs the certificate on the device of your choice. If you are installing the certificate on a device running Windows Mobile 5.0 or Windows Mobile 2003, you must use the Windows Mobile Device Center or the SPAddCert.exe utility to install the self-issued certificate.



Certificate Installation

Where do you want to install the certificate?

You can install the certificate on a computer that is running Windows XP with Service Pack 2 or Windows Vista, or you can install the certificate on a mobile device that is running Windows Mobile 6.

● Install the certificate on my computer

○ Install the certificate on my mobile device

FIGURE 5-4 The Certificate Installation Wizard installs the self-issued certificate at the proper location on the computer or mobile device.

PRACTICE Managing Certificates in Windows Small Business Server 2008

The following exercises help familiarize you with managing self-issued and third-party trusted certificates in Windows SBS 2008. You must be logged on as the network administrator and have run the Internet Address Management Wizard on the Home page and set up your Internet address to complete this exercise successfully.

EXERCISE 1 Verify the Self-Issued Certificate

In this exercise, you learn where to view certificates in the certificate store.

1. On the server running Windows SBS 2008, click Start, point to All Programs, click Windows Small Business Server, and then click Windows SBS Console (Advanced Mode).
2. On the navigation bar, click the Network tab, and then click the Connectivity tab.
3. In the task pane, click Manage Certificates. This opens the Certificates (Local Computer) window.
4. Expand Certificates, expand Trusted Root Certification Authorities, click Certificates, and then double-click Contoso-SERVER01-CA.
5. In the General tab, observe who the certificate was issued to, who it was issued by, and the validity period (five years).

6. Click the Details tab, scroll down, and observe the fields and their values.
7. Click the Certification Path tab to observe the certification path and status. Click OK.
8. Double-click a third-party trusted certificate, and then compare the information in the tabs with information given for the self-issued certificate. Notice that the certificates are very similar except for the issuer, validity length, and intended purpose.
9. In the Certificates (Local Computer) window, in the left pane, expand the Remote Desktop store, click Certificates, and then observe the certificate stored there.
10. In the left pane, expand Personal, click Certificates, and observe the certificates stored there. Check the Intermediate Certification Authority, Certificates store. Windows Small Business Server places all certificates in the appropriate stores.
11. Double-click each certificate and check its validity period (two or five years) and intended use. Then, click the Certification Path tab to see a leaf certificate.
12. Close the Certificates (Local Computer) window and the Windows SBS Console.

EXERCISE 2 Request a Third-Party Certificate

In this exercise, you request a third-party certificate using the Add A Trusted Certificate Wizard.

1. Log on as network administrator, and open the Windows SBS Console.
2. On the navigation bar, click Network, and then click the Connectivity tab.
3. Click Add A Trusted Certificate in the task pane.
4. Review the information on the Welcome page, and then click Next.
5. On the Get The Certificate page, click I Want To Buy A Certificate From A Certificate Provider, and then click Next.
6. Change any incorrect information used to generate the request for the certificate, and then click Next.
7. Windows SBS 2008 generates the encoded information that the CA requires. On the Generate A Certificate Request page, click Save To File to save the encoded information to a file. Name the file **CertRequest**, and click Save. By default, the file will be saved in the user's Documents folder. Click Next.
8. Select My Certificate Provider Needs More Time To Process The Request, and click Next.
9. Review the warning information, and then close the wizard.

EXERCISE 3 Export a Trusted Certificate

In this exercise, you export a trusted certificate.

Note: In this exercise, you must have an existing trusted certificate. For this demonstration, you can use the self-issued certificate. In a real-world situation, the certificate provider would provide instructions on how to import and export the third-party certificate. On the server running Windows SBS 2008, click Start, point to All Programs, click Windows Small Business Server, and then click Windows SBS Console (Advanced Mode).

1. On the navigation bar, click the Network tab, and then click the Connectivity tab.
2. In the task pane, click Manage Certificates.
3. Expand Certificates (Local Computer), Trusted Root Certification Authorities, Certificates. Right-click Contoso-SERVER01-CA, select All Tasks, and then click Export.
4. After you have read the information on the Welcome To The Certificate Export Wizard page, click Next.
5. Click Yes, Export The Private Key.
6. On the Export File Format page, select Include All Certificates In The Certificate Path If Possible and Export All Extended Properties. Be sure that the Delete The Private Key If The Export Is Successful option is cleared. Click Next.
7. Type a password such as **abcd1234** to protect the certificate file, and then click Next.
8. Save the .pfx file to your desktop. Name the file **TrustedCert**, click Save, click Next, and then click Finish.

EXERCISE 4 Import a Trusted Third-Party Certificate

In this exercise, you import a certificate.

Note: In this exercise, you must have an existing trusted certificate. For this demonstration, you can use the self-issued certificate. In a real-world situation, the certificate provider would provide instructions on how to import and export the third-party certificate. Also, in a realistic situation you would move the trustedcert.pfx file to the server that is running Windows SBS 2008 by using the network or a USB flash drive. (In this set of exercises, it is already located on the desktop.)

1. Open the Windows SBS Console in Advanced Mode.
2. On the navigation bar, click the Network tab, and then click the Connectivity tab.
3. In the task pane, click Manage Certificates.
4. In the Certificates (Local Computer) window, expand Certificates, expand Personal, right-click Certificates, click All Tasks, and then click Import.
5. On the Certificate Import Wizard Welcome page, click Next.
6. Browse to the desktop, and select trustedcert.pfx. If the file is not showing, change the file type in the Open dialog box to All Files (*.*). Click Open, and then click Next.
7. Type the password **abcd1234**, select Mark This Key As Exportable and Include All Extended Properties, and then click Next.
8. Leave the default setting Place All Certificates In The Following Store: Personal Folder, click Next, and then click Finish.

EXERCISE 5 Bind a Trusted Certificate to Windows Small Business Server

In this exercise, you bind a third-party certificate to the Windows Small Business Server Web sites using the Add A Trusted Certificate Wizard.

Because you do not have a real trusted certificate, you will not be able to finish the steps of this exercise. You will be able to follow the steps to the point when the file is requested, and then you can cancel out of the exercise.

1. Open the Windows SBS Console.
2. On the navigation bar, click the Network tab, and then click the Connectivity tab.
3. In the task pane, click Add A Trusted Certificate.
4. On the Welcome page, read the information, and then click Next.
5. On the Get The Certificate page, click I Have A Certificate From My Certificate Provider, and then click Next.
6. On the Import The Trusted Certificate File page, either paste the information that you received from the provider or browse to the location where you saved the trusted certificate file, and then click Next.
7. When the wizard finishes, click Finish.
8. If you are using a real trusted certificate, now the certificate is bound to the Windows SBS 2008 Web sites.

EXERCISE 6 Remove a Third-Party Certificate Request

In this exercise, you remove a third-party certificate request. There are two options available to remove the third-party certificate request. Follow these steps in the Windows SBS Console for the first option:

1. In the Network tab, in the Connectivity tab, in the task pane, click Add A Trusted Certificate, and then click Next.
2. Click I Want To Cancel My Request, and then click Next.
3. In the warning dialog box, click Yes.
4. On The Certificate Request Is Removed page, click Finish.

Follow these steps in the Windows SBS Console for the second option:

1. In the Network tab, in the Connectivity tab, in the task pane, click Remove This Certificate Request.
2. Click Yes when prompted.

EXERCISE 7 Install the Self-Issued Certificate on a Non–Domain-Joined Client Computer

In this exercise, you install a self-issued certificate on a non-domain-joined computer using the Install Certificate Wizard.

1. Open Internet Explorer either on the server that runs Windows SBS 2008 or on a domain-joined client computer.

2. Type **\\server01\public\public downloads** in the address bar to open the Public Downloads folder.
3. Copy the Install Certificate Package to a USB storage device (if you are using Windows Server 2008 Hyper-V, for this exercise copy to a shared folder that you will be able to access from the non-domain-joined client computer).
4. Create a folder in the My Documents folder and name it Certificate. Copy Install Certificate Package.zip file to this folder. Right-click the Install Certificate Package.zip file, and select Extract All. In the Select A Destination dialog box, click Next to extract files to the same folder.
5. Double-click InstallCertificate.exe to open the Certificate Installation dialog box.
6. Select the Install The Certificate On My Computer option, and click Install.
7. You will get a certificate installed message. You can verify the installation by checking certmgr.msc.

✓ Quick Check

- **When does Windows SBS 2008 install the self-issued root certificate, and what information does it use to determine the CA name?**
- **When is the leaf certificate created and what name is used for it?**
- **How long is the root certificate valid? How long is the leaf certificate valid?**
- **On which devices can InstallCertificate.exe install the certificate?**
- **Which tool should you use to renew the self-issued certificate time period?**
- **Where is Install Certificate Package.zip stored?**

Quick Check Answers

- **The root certificate is created during the installation of Windows SBS 2008 using the internal domain name (for example, Contoso.local).**
- **The leaf certificate is created when you run the Internet Address Management Wizard using the registered domain name (for example, Contoso.com).**
- **The root certificate is valid for five years, and the leaf certificate is valid for two years.**
- **InstallCertificate.exe can install the certificate on computers running Windows XP SP2 and Windows Vista, and on Windows Mobile 6 devices that are physically connected to the computer.**
- **You can run the Fix My Network Wizard to renew the time period of the self-issued root certificate.**
- **The certificate file along with an executable file (InstallCertificate.exe) are compressed into a certificate distribution package (Install Certificate Package.zip) and stored in the %systemdrive%\users\public\public downloads shared folder.**

Lesson 2: Managing Remote Web Workplace

One incredible out-of-the-box experience is Remote Web Workplace (RWW), a preconfigured Web site that, along with a static IP address and a registered domain name, makes remote network access in Windows Small Business Server a breeze. Being able to use a single Web site as a portal to the Windows Small Business Server network makes life much easier for small business owners and their employees. No longer is there a need to drive to the office on Sunday afternoon to check Monday's schedule and prepare documents for the next day. Windows Small Business Server users can do it from home on the couch using their wireless laptop computer. If an employee has to stay home to care for a sick family member, it doesn't mean that work won't get done. The employee can remotely log on to the office workstation from home and complete a project. This is not only efficient, but truly improves quality of life—especially because only an Internet browser, a certificate, and the proper Web site address and user name and password are required.

For administrators, having happy customers is a great thing, but spending very little effort on administering Remote Web Workplace is priceless!

Estimated lesson time: 75 minutes

Understanding Remote Web Workplace Prerequisites

Users can access Remote Web Workplace using the single Internet address required to navigate to the Windows SBS 2008 resources. The external address can be a URL (for example, *http://remote.contoso.com*) or the network's external IP address (for example, 24.227.13.8). If you have a registered domain, you must run the Internet Address Management Wizard to configure the Internet domain name that will be used by Remote Web Workplace.

By default, Windows Small Business Server assigns the *remote* prefix to the Remote Web Workplace URL. You can modify this prefix to be anything you like in the Internet Address Management Wizard. In the Store Your Domain Name Information dialog box, click the Advanced Settings link, and then type the new prefix in the Domain Prefix box. For example, type **office** to make the URL *http://office.contoso.com.*

Some additional requirements must be met before users can access Remote Web Workplace:

- Users must be members of the Remote Web Workplace Users or Domain Admins security groups. (By default, any standard user is a member of the Remote Web Workplace Users group unless this access right has been removed from the user's account.)
- The router that connects the server running Windows SBS 2008 to the Internet must allow Internet traffic on ports 80, 443, and 987.
- The Windows SBS 2008 server ports must allow traffic through TCP ports 80, 443, 987, and 3389.
- The client computer must allow traffic through TCP ports 80, 443, 987, and 3389.

- The client computer must run RDP 6.0 client software or later if a desktop connection to an office computer must be established.
- The client browser used to access RWW must accept cookies or RWW will refuse the connection.

If the client computer is a not a member of the Windows Small Business Server domain, it must have the server certificate installed or you will experience Certificate Error “Navigation Blocked” and other errors and will not be able to connect to Remote Web Workplace.

EXAM TIP

The router does not need to have port 3389 open for a remote user to establish a desktop connection. When a remote client requests a connection to an internal resource through a Microsoft Remote Desktop Protocol (RDP) connection, after authentication and authorization, a Secure Sockets Layer (SSL) tunnel is established through the Terminal Server gateway server over HTTPS port 443. Therefore, it is not necessary to open port 3389 on the router. Only the server running Windows SBS 2008, the client computer in the office, and the remote computer must have port 3389 open.

Configuring Remote Web Workplace

You can find most administrative tasks for managing Remote Web Workplace in the Windows SBS Console. As an administrator, you can add, remove, and customize Remote Web Workplace features on the Remote Web Workplace Tasks list. In the Shared Folders And Web Sites tab, click the Web Sites tab, and then click the Remote Web Workplace link to open the Tasks list.

Enable or Disable Remote Web Workplace

By default, access to Remote Web Workplace is enabled, but you might want to modify this setting to prevent remote users from accessing network resources through Remote Web Workplace.

1. Open the Windows SBS Console, and in the Shared Folders And Web Sites tab, click the Web Sites tab.
2. Right-click Remote Web Workplace, and then do one of the following:
    - To enable Remote Web Workplace so that users can remotely access network features, click Enable This Site.
    - To prevent users from accessing Remote Web Workplace, click Disable This Site.

Disabling Remote Web Workplace makes the Web service unavailable. When you select this option, IIS will not serve the /remote login page and will display an HTTP Error 503 message.

You can also enable or disable Remote Web Workplace in the General tab on the Remote Web Workplace Properties page by selecting or clearing the Enable Remote Web Workplace option.

Manage Remote Web Workplace Properties

The Remote Web Workplace home page, shown in Figure 5-5, is the page that greets users who are signed in. You can customize this page using the Remote Web Workplace Properties and Remote Web Workplace Link List Properties pages.

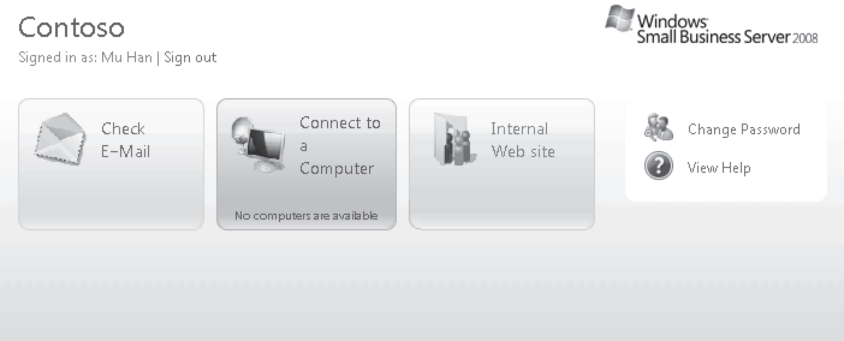

Contoso
Signed in as: Mu Han | Sign out
Windows Small Business Server 2008
Check E-Mail
Connect to a Computer
No computers are available
Internal Web site
Change Password
View Help

FIGURE 5-5 Remote Web Workplace home page

You can access the Remote Web Workplace Properties page in the Windows SBS Console. Under Shared Folders And Web Sites, select Remote Web Workplace, and click View Site Properties in the task pane. On the Remote Web Workplace Properties page, you can manage access, customize the home page look and feel, and access the Link List properties. The following links appear in the left pane:

- **General link** You can use the General link to enable and disable Remote Web Workplace.
- **Permissions link** You can use the Permissions link to manage which users have access to Remote Web Workplace. This link is covered in more detail in the section titled “Manage Access to Remote Web Workplace.”
- **Home Page Links link** You can use the Home Page Links link to select which standard features you want to appear on the Remote Web Workplace home page. This link is discussed in more detail in the next section titled “Manage Remote Web Workplace Link List Properties.” The Home Page Links tab also contains a Manage Links link that opens the Remote Web Workplace Link List Properties page. (Be sure not to confuse the Remote Web Workplace Link List Properties page with the Remote Web Workplace Properties because they look and feel similar.)
- **Customization link** You can use the Customization link to modify the organization name, change the organization logo, and change the background image on the sign-in and sign-out pages. Remote Web Workplace supports the GIF, PNG, BMP, and JPG image formats. Background image files are stored in the %system%\Program Files\Windows Small Business Server\Bin\webapp\Remote\Images folder on the server.
- **Advanced Settings link** The Advanced Settings link opens IIS 7.0 Manager.

Manage Remote Web Workplace Link List Properties

When users first log on, the Remote Web Workplace home page displays a variety of links that are enabled by default for all standard users. The following links provide quick access to features on the Windows Small Business Server network:

- Check E-Mail (Outlook Web Access)
- Connect To Computer
- Internal Web Site (Windows SharePoint Services)
- Change Password
- Help
- Organization Links

Additional links are displayed for administrators:

- Connect To Server
- Administration Links

You might find that navigating to the Remote Web Workplace Link List Properties page is cumbersome because it is somewhat hidden in the interface and can easily be overlooked.

You can review and modify the links displayed on the Remote Web Workplace home page. To do so, in the Windows SBS Console, click the Shared Folders And Web Sites tab, and then click Remote Web Workplace. Click View Site Properties in the task pane to open the Remote Web Workplace Properties page. Next, click the Home Page Links link, and click Manage Links to access the Remote Web Workplace Link List Properties page.

The tabs on the Remote Web Workplace Link List Properties page are similar to the links displayed on the Remote Web Workplace Properties page, but they contain different functions. It is a good idea to take the time to explore this part of the Windows SBS Console to familiarize yourself with it.

Here is a description of the tabs you will find on the Remote Web Workplace Link List Properties page:

- **General** In the General tab, you can enable or disable the Remote Web Workplace Link List containing the Organization Links or Administration Links.
- **Permissions** In the Permissions tab, you can configure which users can access the Link List as well as who can access the Administration section. Note that this also determines which links are displayed in the Windows Vista Desktop Links gadget.
- **Organization Links** Use this link to do the following:
  - Remove a link from the list. Select the link, and then click Remove.
  - Add a new link. Type a description and a Web address or path for the new link, and then click Add.
  - Move a link. Click Move Up or Move Down to position the links where you want them to appear in the list. This is also the order in which the links will appear on the Remote Web Workplace home page.

- **Administration Links** Use this link to do the following:
  - Remove a link from the list. Select the link, and then click Remove.
  - Add a new link. Type a description and a Web address or file path for the new link, and then click Add.
  - Move a link. Click Move Up or Move Down to position the links where you want them to appear in the list. This is also the order in which the links will appear on the Remote Web Workplace home page.
- **Customization** In the Customization tab, you can modify the titles for the Remote Web Workplace Link List Organization and Administration sections.

> ***NOTE*** **ACCESSING THE ADMINISTRATION LINKS SECTION**
>
> **By default, all network users with a Standard User account have permissions to log on to Remote Web Workplace and use the links in the Organization Links list (when it is enabled). However, only members of the Windows SBS Admin Tools Group can use the links in the Administration Links section.**

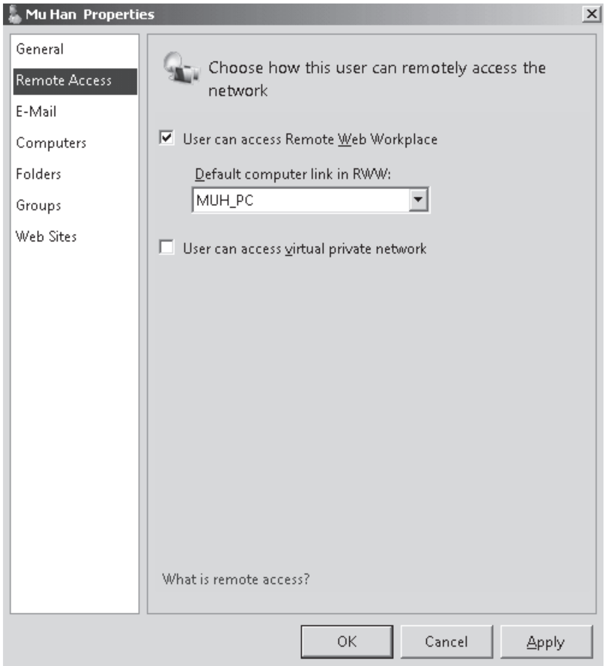
Manage Access to Remote Web Workplace

You can assign user access to Remote Web Workplace by using the Manage Permissions task. You can find this task in the Windows SBS Console. Click Shared Folders And Web Sites, and then click the Web Sites tab.

In the Manage Permissions task, click Modify to open the Change Group Membership dialog box. Under Users And Groups, select the user account or group for which you want to grant access, and click Add to add this user account or group to the Windows SBS Remote Web Workplace Users security group. Note that you can add individual user accounts as well as other security groups.

You will find that the Windows SBS Console links allow you to accomplish a single task in different ways. For instance, you can configure access to Remote Web Workplace in the user account properties under the Remote Access link, as shown in Figure 5-6. (You can open the user account properties in the Windows SBS Console by double-clicking the account name in the Users tab under the Users And Groups tab.) Select or clear the User Can Access Remote Web Workplace check box to add or remove the user account from the Windows SBS Remote Web Workplace Users group. Don’t let this confuse you; just be aware that there are different ways to go about achieving the same outcome.

Also under the Remote Access link of the user account properties, you can select a default computer to which users will automatically connect every time they log on to Remote Web Workplace. All the computers to which a user has access are listed in the Default Computer Link In RWW drop-down list. Select the default computer from this list. Computers to which the user does not have access are not shown in the list.



Choose how this user can remotely access the network

☑ User can access Remote Web Workplace

Default computer link in RWW: MUH_PC

□ User can access virtual private network

FIGURE 5-6 Enabling access to Remote Web Workplace and selecting a default computer in the user account properties

EXAM TIP

When you use the Windows SBS Console, it can be easy to forget that you are actually modifying permission settings in Active Directory and IIS. Every time you change permissions on a user account or change a setting on Remote Web Workplace, consider what actions are actually being performed. One way that you can do this is to make changes in the Windows SBS Console and then open Active Directory Users And Computers or IIS Manager to examine the effects of the changes.

Connecting to Remote Web Workplace

To connect to Remote Web Workplace, type the Internet address into the address box in your browser (for example, type **http://remote.contoso.com**). You need not use the *https://* prefix in the Internet address for a Secure HTTP connection. Instead, you can use the *http://* prefix and be sure that port 80 is open on the router and the server running Windows SBS 2008 so that traffic that requests port 80 is redirected to port 447 and switched to a secure connection automatically. Also, be sure to have the server certificate installed on the client computer or you will be blocked from accessing resources.

Check E-Mail

When you are signed in to Remote Web Workplace you have several options, one of which is to check e-mail. Outlook Web Access is a Web-based version of Microsoft Office Outlook that you can access through a Web browser.

The first page in Outlook Web Access verifies your language and time zone settings, and then allows you to access your mailbox. No further authentication is required because Outlook Web Access uses the credentials you provided to sign on to Remote Web Workplace for access.

In Outlook Web Access, you can do the following:

- Check your e-mail, calendar, contacts, and other Outlook folders
- Send e-mail and meeting requests
- Receive notification when e-mail arrives
- Receive meeting reminders
- Attach files, audio clips, or video clips to a message
- Move e-mail messages to other folders
- Remotely reset the password on a mobile device or wipe the device

When you log off Outlook Web Access, you return to the Remote Web Workplace home page.

For more information about configuring Outlook Web Access, see Chapter 6.

EXAM TIP

You can connect directly to Outlook Web Access by typing *https://remote.contoso.com/owa* in the browser address bar. You will then be prompted for your user name and password.

Connect to a Computer

Every user has remote access permissions to their own desktop by default. When a client computer is joined to the Windows Small Business Server domain, the user account is automatically added to the client computer's local Remote Desktop Users group. Also, any user account that is a member of the local Administrators group on the client computer has remote access permissions by default and need not be added to the Remote Desktop Users group.

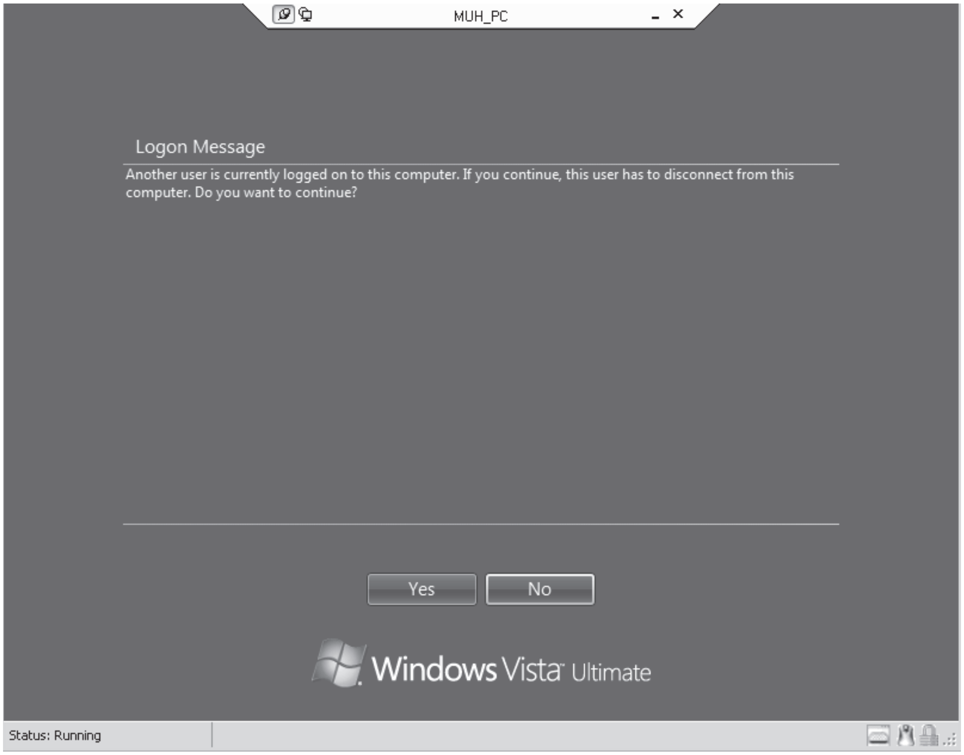
Therefore, to access a client computer users must be the primary user or a local administrator, or their user account must be added to the Remote Desktop Users group on that client computer. After access permissions are configured on the client computer, users can then use Remote Web Workplace to connect to a computer using the Connect To A Computer link. The first time a user clicks this link, he or she is asked to install the Terminal Services ActiveX Client (which is an RDP client control) on the remote computer. Users can click the notification, select Run ActiveX Control, and then click Run again.

The client requesting the connection will receive a Remote Desktop Connection notice that the Web site wants to start a remote connection. The section titled "Terminal Services Gateway Manager" later in this chapter explains the background process on how the connection is established. Users can click Connect and provide network credentials to authenticate on the resource to which they are trying to connect.

By default, the Clipboard and Printers options are selected so that the client computer on the Windows Small Business Server network can access the resources on the local computer the user is connecting from. Users can leave these default options selected to copy or print items locally while working on the client computer.

When a user attempts to connect to a resource that is currently in use by another user, the Logon Message shown in Figure 5-7 appears. The following things can happen:

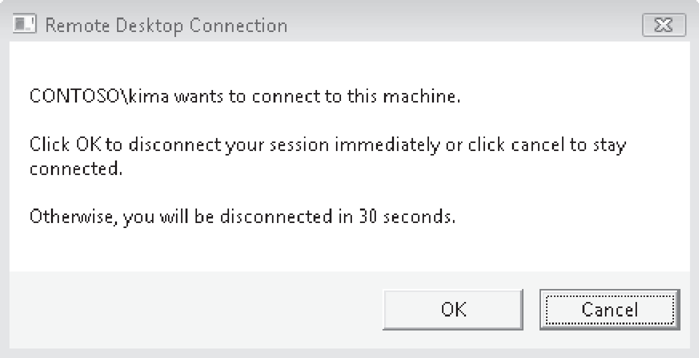
- If the user selects Yes on the Logon Message page, the user is asked to wait for the logged-on user's response.
- The currently logged on user can accept or refuse the Remote Desktop Connection request, as shown in Figure 5-8.
- If the user selects No on the Logon Message page, the request is canceled, the user is disconnected from the resource, and the currently logged on user is not interrupted.



Logon Message

Another user is currently logged on to this computer. If you continue, this user has to disconnect from this computer. Do you want to continue?

FIGURE 5-7 The Logon Message that appears when another user is already logged on to a requested resource


Remote Desktop Connection

CONTOSO\kima wants to connect to this machine.

Click OK to disconnect your session immediately or click cancel to stay connected.

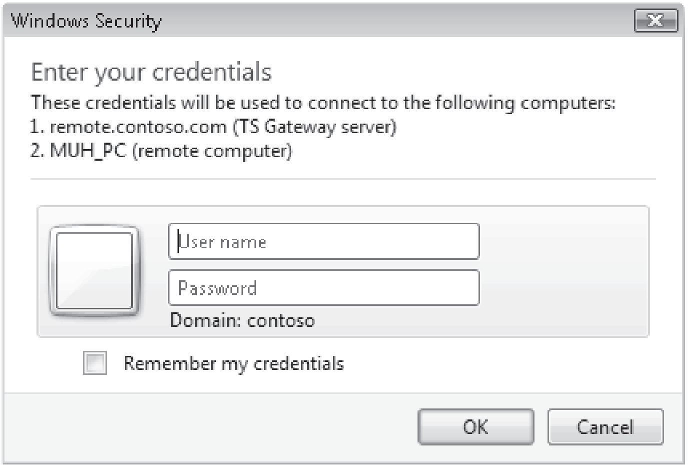
Otherwise, you will be disconnected in 30 seconds.

FIGURE 5-8 The logged-on user can accept or deny a remote connection request.

Understand Remote Desktop Connection

Clients intending to connect to a computer on the Windows Small Business Server network through Remote Web Workplace must have Remote Desktop Protocol 6.0 installed. The new version of Remote Desktop Connection (RDC) is native to Windows Vista and Windows Server 2008. For clients running Windows XP, you can download an upgrade at *http://support.microsoft.com/kb/925876* to make Remote Desktop compatible with Windows Server 2008 and Windows Vista.

The Remote Desktop version in Windows Vista includes new security features. Network Level Authentication (NLA) ensures that a user performs a standard logon process before the connection to the remote computer on the Windows SBS 2008 network is established, as shown in Figure 5-9. The user name and password provided are passed to the Credential Security Service Provider (CredSSP), which then passes the credentials to the terminal server over a secure channel. Once the credentials are accepted, the remote desktop connections session is built by the server.


Windows Security

Enter your credentials

These credentials will be used to connect to the following computers:
1. remote.contoso.com (TS Gateway server)
2. MUH_PC (remote computer)

User name

Password

Domain: contoso

□ Remember my credentials

FIGURE 5-9 The standard logon process required before the connection to the remote computer can be established

If users connect using Windows XP, they still must authenticate to the client computer that they are trying to connect to. The difference is that a session to the client computer is established first, and then the credentials are processed.

When users connect through Remote Web Workplace using the Connect To A Computer link, they do not have control over the Remote Desktop Connection session options and will be directly connected to the remote computer with a fully shared desktop.

Understand Preconfigured RDP-TCP Properties

By default, the Terminal Services configuration on the server running Windows SBS 2008 is set to allow access to all users in the Administrators and Remote Desktop Users security groups. Administrators have Full Control whereas Remote Desktop Users have Guest and User access rights so that they can log on, connect, and query data.

The server authentication is set to the default level, Negotiate, which means that client and server will both use Transport Layer Security (TLS) for server authentication if TLS is supported. If so, the server uses the self-issued certificate (unless you imported a third-party certificate).

The encryption level is set to Client Compatible so that RDP traffic will be encrypted as strongly as a client can support. The server and client are configured so that they can negotiate the highest level of encryption they both support. RDP clients support three levels of encryption: low, high, and FIPS-compliant:

- **Low Security** This level uses a 56-bit key to encrypt traffic and only encrypts traffic going from the client computer to the server. This level of encryption is not appropriate for any connection that requires a bidirectional flow of data.
- **High Security** This encryption level uses a 128-bit key to encrypt traffic going both directions. High Security supports server authentication.
- **FIPS-Compliant** Federal Information Processing Standard (FIPS)–compliant security uses FIPS-compliant algorithms for encrypting the traffic between the client computer and the server. FIPS is not an encryption type but a standard for key generation and management.

The option Allow Connections Only From Computers Running Remote Desktop With Network Level Authentication is not selected on the server running Windows SBS 2008 by default. This option allows access only to client computers that support NLA authentication, namely, computers running Windows Vista and Windows XP SP3.

EXAM TIP

Remote Desktop Connection (RDC) is the tool you use to connect to another computer through a terminal server. Remote Desktop Protocol (RDP) is the protocol that enables communications between client computers and servers.

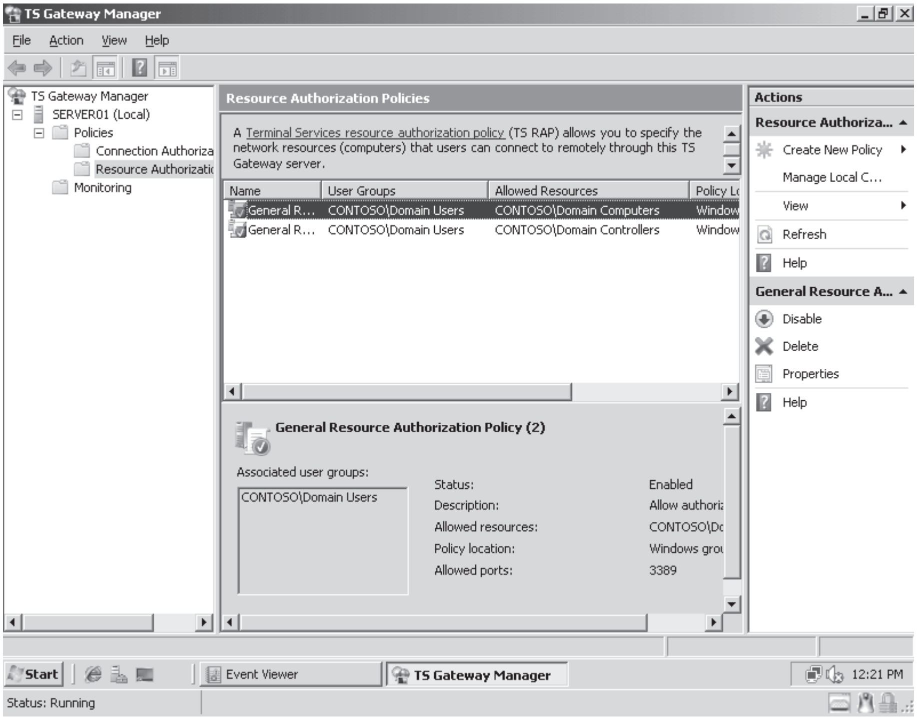
Understand Terminal Services Gateway Manager

The Connect To A Computer link in Remote Web Workplace uses the Terminal Services Gateway Manager (TS Gateway Manager). The TS Gateway is a server role installed by default on the server running Windows SBS 2008. This server role allows authorized remote users to connect to internal resources using Remote Desktop Protocol (RDP) over Secure HTTP (HTTPS). The TS Gateway transmits RDP traffic to port 443 instead of port 3389 using an HTTP Secure Sockets Layer (SSL) tunnel. This functionality is deliberate because many corporations block port 3389 but leave port 443 open.

Before the TS Gateway establishes the SSL tunnel, it checks the connection authorization policies (CAPs) and resource authorization policies (RAPs) that have been configured using the TS Gateway Manager, as shown in Figure 5-10. Connection authorization policies authenticate and authorize the remote user, and resource authorization policies verify the name of the resource requested against the names of resources (client computers running Windows Small Business Server) listed in the policy.

If the name of the requested resource exists in at least one RAP and the name of the user requesting the connection also exists in at least one RAP, the TS Gateway server authorizes the request. Then, the SSL connection is established between the remote user and the resource.

The remote user must use the standard logon process on the resource to validate his or her identity and access permissions for the requested resource. This is done using Windows Authentication in the Windows Security logon dialog box.



A Terminal Services resource authorization policy (TS RAP) allows you to specify the network resources (computers) that users can connect to remotely through this TS Gateway server.

Name	User Groups	Allowed Resources	Policy Lc
General R...	CONTOSO\Domain Users	CONTOSO\Domain Computers	Window
General R...	CONTOSO\Domain Users	CONTOSO\Domain Controllers	Window

General Resource Authorization Policy (2)

Associated user groups:

CONTOSO\Domain Users

Status:	Enabled
Description:	Allow authori:
Allowed resources:	CONTOSO\Dc
Policy location:	Windows grou
Allowed ports:	3389

FIGURE 5-10 Resource authorization policies listed in the TS Gateway Manager

NOTE **USING A TERMINAL SERVICES SERVER**

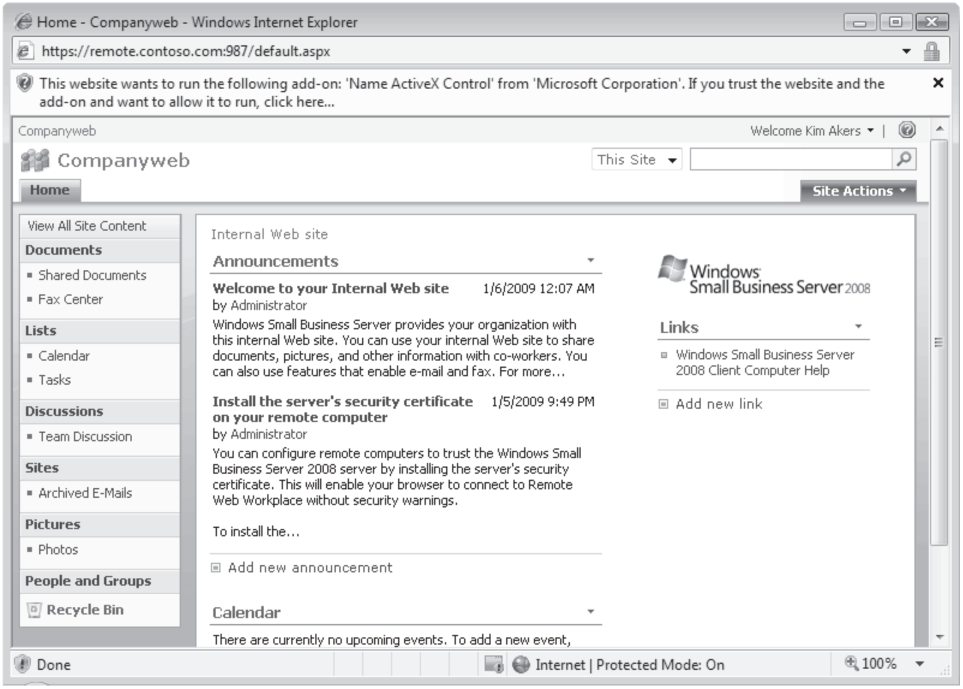
Do not confuse the TS Gateway Manager with Terminal Services. Windows SBS 2008 cannot be used as a Terminal Services server. (See Chapter 8, "Migrating to Windows Small Business Server 2008," for more information about using a Terminal Services server on the Windows SBS 2008 network.) For a quick overview of the TS Gateway, go to *http://technet.microsoft.com/en-us/library/cc732122.aspx*.

Connect to the Internal Web Site (*http://companyweb*)

You can connect to *http://companyweb* through Remote Web Workplace by clicking the Internal Web Site link. The first time you connect you are asked to run an ActiveX control, as shown in Figure 5-11. You can click the notification to allow the ActiveX control to run. The Active-X add-on needs to be run only once.

Thereafter, each time you connect to the internal Web site through Remote Web Workplace you are asked to authenticate against the site to establish your access role and permissions. *http://companyweb* is served over port 987 externally. If you connect through a Favorites link from a client computer on the internal Windows Small Business Server network, *http://companyweb* is served over port 80 and no authentication is required.

For more information about configuring *http://companyweb*, see Chapter 6.



Home - Companyweb - Windows Internet Explorer

https://remote.contoso.com:987/default.aspx

This website wants to run the following add-on: 'Name ActiveX Control' from 'Microsoft Corporation'. If you trust the website and the add-on and want to allow it to run, click here...

Internal Web site

Announcements

Welcome to your Internal Web site 1/6/2009 12:07 AM
by Administrator
Windows Small Business Server provides your organization with this internal Web site. You can use your internal Web site to share documents, pictures, and other information with co-workers. You can also use features that enable e-mail and fax. For more...

Install the server's security certificate on your remote computer 1/5/2009 9:49 PM
by Administrator
You can configure remote computers to trust the Windows Small Business Server 2008 server by installing the server's security certificate. This will enable your browser to connect to Remote Web Workplace without security warnings.

To install the...

Calendar

There are currently no upcoming events. To add a new event,

FIGURE 5-11 Accessing *http://companyweb* through Remote Web Workplace

Change a Password Remotely

In Remote Web Workplace, by using the Change Password link, users can change their network password from a remote location. When users click this link, the Change Password dialog box opens and users must enter their user name, the old password, and a new password. This immediately makes the change on the network.

PRACTICE Managing Remote Web Workplace

By completing the following exercises, you can become familiar with managing and modifying Remote Web Workplace. This practice must be completed on the server running Windows SBS 2008 and a non-domain-joined computer that runs Windows Vista.

EXERCISE 1 Enable and Disable Remote Web Workplace

In this exercise, you disable and then enable Remote Web Workplace.

1. Log on to the server running Windows SBS 2008 as a network administrator. Use **Gregoryw** as your user name and **P@ssw0rd** as your password.
2. Open the Windows SBS Console, click the Shared Folders And Web Sites tab, and then click the Web Sites tab.
3. In the Web Sites tab, click Remote Web Workplace. In the task pane, click Disable This Site.
4. Open Internet Explorer on the server (it's OK for this exercise), and type **https://remote.contoso.com** in the address bar. A Service Unavailable page should appear. Minimize the browser.
5. Go back to the Windows SBS Console and enable the site by clicking Enable This Site in the task pane.
6. Switch back to the browser, and press F5. The Remote Web Workplace logon page should open. Close the browser.

EXERCISE 2 Configure Access to Remote Web Workplace

In this exercise, you manage user access permissions for Remote Web Workplace for specific users and groups.

1. Open the Windows SBS Console.
2. On the navigation bar, click Shared Folders And Web Sites, and then click the Web Sites tab.
3. Right-click Remote Web Workplace, and then click Manage Permissions. The Remote Web Workplace Properties page opens.
4. Click Modify in the permissions pane. The Change Group Membership dialog box opens.

5. Notice that by default all individual users are listed in the Group Members dialog box. Select Stefan Hesse and Don Richardson (hold down the CTRL key as you click the user names), and then click Remove.
6. Click Apply, and then click OK. The dialog box will close, and you can see the permissions pane again.
7. On the computer running Windows Vista, open Internet Explorer.
8. Type **https:\\remote.contoso.com** in the address bar to open the Remote Web Workplace logon page.
9. Log on with the user name **MUH** and the password **P@ssw0rd**. Logon should be successful. Observe all the links and options available on the home page (for the next exercise), and then click Sign Out in the left-hand corner.
10. Click Sign In, and this time use the user name **STEFANH** and the password **P@ssw0rd**. The logon should fail because you removed Stefan Hesse from the Remote Web Workplace Users security group. Close the browser but leave the client computer running.

EXERCISE 3 Customize Remote Web Workplace

In this exercise, you modify Remote Web Workplace and navigate the its properties.

1. On the server running Windows SBS 2008, open the Windows SBS Console, click the Shared Folders And Web Sites tab, and then click the Web Sites tab.
2. Double-click Remote Web Workplace to open the Remote Web Workplace Properties page.
3. Click the Home Page Links link and clear the Connect To Computer, Change Password, and Remote Web Workplace Link List options, and then click OK.
4. Switch to the non-domain-joined client computer, and open Internet Explorer. Type **http://remote.contoso.com** in the address bar and observe how you are switched to HTTPS on the Sign In page.
5. Sign in with the user name **MUH** and the password **P@ssw0rd.** Observe the available links: Only the Check E-Mail, Internal Web Site, and View Help links should be available. Sign out and close the browser but leave the client computer running.

EXERCISE 4 Modify Remote Web Workplace Link List Properties Access for Individual Users

In this exercise, you modify the Remote Web Workplace Link List and navigate its properties.

1. On the server running Windows SBS 2008, click the Shared Folders And Web Sites tab, and then click the Web Sites tab.
2. Select Remote Web Workplace, and click View Site Properties in the task pane. Click the Home Page Links link, and select the Connect To Computer, Change Password, and Remote Web Workplace Link List options (the options you cleared in the previous exercise).

3. When you activate the Remote Web Workplace Link Lists link, the Manage Links button becomes available. Click the Manage Links button to open the Remote Web Workplace Link List Properties page. Notice that this interface is the same one that you worked with in the Lesson 2 exercises in Chapter 2, "Joining Clients to the Windows Small Business Server Domain." (The organization and administration links configured for the Remote Web Workplace home page also appear in the Desktop Links gadget.)
4. Click the Permissions link, and under Users Who Can Access The Link List, click Modify.
5. In the Change Group Membership dialog box, remove Mu Han from the Group Members, and click OK. Click OK two more times to close the dialog boxes.
6. Switch to the non-domain-joined client computer, open the browser, and connect to Remote Web Workplace. Sign in with the user name **KIMA** and the password **P@ssw0rd**. Note that all links are available to Kim. Sign out.
7. Sign in with the user name **MUH** and the password **P@ssw0rd**. Note that the Remote Web Workplace Link List is not available. Sign out and close the browser but leave the client computer running.

EXERCISE 5 Customize Remote Web Workplace

In this exercise, you customize Remote Web Workplace.

1. On the server running Windows SBS 2008, open the Windows SBS Console, click the Shared Folders And Web Sites tab, and click the Web Sites tab.
2. Double-click Remote Web Workplace to open the Remote Web Workplace Properties page.
3. Below the Home Page Links link, click Customization.
4. In the Organization Name dialog box, type **Hamlin, Han, Akers, & Raj**. Leave the dialog box open.
5. Click Start, click Computer, and navigate to C:\Windows\web\Wallpaper. Copy server.jpg and paste it in C:\Program Files\Windows Small Business Server\Bin\webapp\Remote\Images.
6. Switch back to the Customization tab of the Remote Web Workplace Properties page. In the Sign-In Page section, for the Background Image, click Choose, and then select the server.jpg file you just copied into the folder.
7. In the Home Page section, for the Organization Logo, click Choose, and then select alert.png. (In this exercise, you use an existing image, but in the real world you would add your company's logo and branded background image here.) Click OK.
8. Switch back to the client computer and open the browser (or press F5 if you didn't close it). Connect to Remote Web Workplace.
9. The Sign-In page should display the gray server background image. Sign in with the user name **KIMA** and the password **P@ssw0rd** and observe that the company logo is alert.png.

EXERCISE 6 Check E-Mail

In this exercise, you access Exchange Server mail using Remote Web Workplace.

1. Connect to *http://remote.contoso.com* on the non-domain-joined client computer and sign in with the user name **MUH** and the password **P@ssw0rd**.
2. On the Remote Web Workplace home page, click Check E-Mail. Click OK to accept the Outlook Web Access settings and access the mailbox.
3. In the Outlook Web Access mailbox, click Options to open the Message Options dialog box. Scroll through the options in the left pane and configure as needed. The very last option is a Mobile Devices option that will allow users to remotely wipe the mobile device or reset the password or wipe all data from the device in case the device gets misplaced.
4. Switch back to the Inbox by clicking the mail icon in the left bottom corner, and double-click the Welcome e-mail message to read it. Close the message, and then right-click it to see the available options.
5. Click Log Off, and then click Close Window to get back to the Remote Web Workplace home page.

EXERCISE 7 Connect to a Computer

In this exercise, you connect to an office workstation through Remote Web Workplace. To complete this exercise, you must start the domain-joined client computer.

1. On the Remote Web Workplace home page, click Connect To A Computer, and then click Connect in the Remote Desktop Connection dialog box.
2. Use the user name **MUH** and password **P@ssw0rd**, and then click OK in the Windows Security dialog box. You should be connected to the computer assigned to Mu Han.
3. You should be connected directly through to the Windows Vista desktop. If you switch to the domain-joined client computer, you will notice that the desktop is locked.
4. Switch back to the non-domain-joined computer. You can now work on this desktop just as if you were working on the domain-joined client computer.
5. Note that you can minimize the Remote Desktop Connection and work simultaneously on both computers.
6. If you have documents on the domain-joined computer, you can copy these documents and paste them directly in the non-domain-joined client computer and vice versa.
7. Log off the computer you are connected to remotely. This returns you to the Remote Web Workplace home page.

EXERCISE 8 Access the Internal Web Site (*http://companyweb*)

In this exercise, you access *http://companyweb* through Remote Web Workplace.

1. On the Remote Web Workplace home page, click the Internal Web Site link. You will be asked to authenticate.

2. Use the user name **MUH** and the password **P@ssw0rd**, and then click OK. It might take a moment to make the connection and open the *http://companyweb* page. Note that you can interact with SharePoint Services just as if you were on the network. You can upload files directly from the non-domain-joined client computer.
3. Close *http://companyweb* and sign out of Remote Web Workplace.

✓ Quick Check

- **You try to access Remote Web Workplace from a non-domain-joined computer and get an error message stating that there is a problem with the Web site's security certificate. What could be the problem?**
- **Which port numbers should be open on the server running Windows SBS 2008 for users to be able to access Remote Web Workplace and Windows Small Business Server resources? Why?**
- **Why is opening port 3389 on the router not required to establish a Remote Desktop Connection from a remote client computer to a resource on the Windows SBS 2008 network?**
- **A user calls you and asks whether she can easily transfer files between the remote computer she is connecting from and the office computer she is connecting to. What do you tell her?**

Quick Check Answers

- **Most likely, the server certificate was not installed on the client computer and the server does not trust the computer. You should copy the certificate from the server Public\Public Downloads shared folder to a USB storage device or removable media and install it on the domain-joined client computer.**
- **Ports 80, 443, 987, and 3389 should be open on the server. Port 80 should be open so that users can use the *http://* prefix instead of the *https://* prefix. Port 80 automatically redirects to port 443, which uses the certificate to encrypt traffic. Port 987 is used for SharePoint access through Remote Web Workplace, and port 3389 is used for Remote Desktop Connections.**
- **The TS Gateway transmits RDP traffic to port 443 instead of port 3389 using an HTTP SSL tunnel. This is done because many organizations block port 3389 but leave port 443 open.**
- **You can tell the user that, yes, she can use RDC to copy and paste files between the two connected client computers just as if she were performing a copy and paste operation on a single computer.**

Lesson 3: Managing a Virtual Private Network

Even though Remote Web Workplace is the preferred choice for remote access to the Windows Small Business Server network and its resources, in some cases virtual private network (VPN) access is required. A VPN connection uses encryption and tunneling to transfer data from a remote computer across the Internet to the VPN server, in this case the server running Windows Small Business Server. The virtual private network is considered an extension of the private Windows Small Business Server network across a public network such as the Internet.

In the past, VPNs were used for secure remote access connections across the Internet to negate the cost of dedicated dial-up or leased lines without sacrificing privacy. Most tasks that are performed by remote users can now be easily and securely handled by Remote Web Workplace.

Nevertheless, you still have the option to enable and use VPN access in Windows SBS 2008, which provides several protocol choices for a VPN: Point-to-Point Tunneling Protocol (PPTP), Layer 2 Tunneling Protocol with Internet Protocol Security (L2TP/IPSec), and Secure Socket Tunneling Protocol (SSTP). By default, Windows Small Business Server uses PPTP.

One of the benefits of using PPTP is that it does not require a certificate for remote access and still provides a good level of security that is acceptable to most organizations.

Estimated lesson time: 75 minutes

Configuring a Virtual Private Network

In Windows SBS 2008, you can enable or disable a virtual private network from the Windows SBS Console. Click the Network tab, click the Connectivity tab, and then click Configure A Virtual Private Network in the task pane. The Set Up Virtual Private Networking Wizard opens and offers two choices:

- Allow Users To Connect To The Server By Using A VPN
- Do Not Allow Users To Connect To The Server By Using A VPN

If the router is Universal Plug and Play (UPnP) enabled, the wizard will configure the server and the router. If the router is not UPnP enabled, you must manually configure the ports.

The Set Up Virtual Private Networking Wizard enables the Routing and Remote Access service and sets up PPTP using TCP port 1723 and Generic Routing Encapsulation (GRE) IP port 47. Table 5-1 lists commonly used ports and protocols for VPNs.

NOTE **CONFIGURING THE HOST-BASED FIREWALL**

Windows SBS 2008 also configures the Inbound and Outbound Windows Firewall rules and enables or disables Routing and Remote Access based on VPN access.

PPTP by itself creates, maintains, and disconnects a virtual private network between two end points (hence the term "tunnel"), but it does not encrypt the data. PPTP allows multiprotocol traffic to be encrypted; therefore, GRE is used to encapsulate the data, or payload, in a secure manner, and then the payload is encapsulated in an IP header that is sent across the internetwork connection. Often, small office and home office (SOHO) routers offer an option for VPN pass-through. Because these routers do not support VPN end points, they can be configured to pass through GRE packets.

In some cases, certain organizations cannot use PPTP for VPN connectivity. Instead, they must configure an L2TP/IPSec VPN connection. L2TP/IPSec VPNs are supported in Windows SBS 2008 but must be configured manually. The L2TP/IPSec VPN uses UDP ports 500 and 4500 and IP port 50, and uses Internet Key Exchange (IKE) or preshared or public keys for authentication. Considerations for working with L2TP/IPSec VPNs are beyond the scope of this chapter, so for more information, see the article titled "Virtual Private Networks" at Microsoft TechNet (*http://technet.microsoft.com/en-us/network/bb545442.aspx*).

TABLE 5-1 Commonly Used VPN Ports and Protocols

PROTOCOL	DESCRIPTION
Point-to-Point Protocol (PPTP)	PPTP establishes the session and uses TCP port 1723 to create and maintain the connections between the VPN client and VPN server.
Generic Routing Encapsulation (GRE)	GRE is used to encapsulate the data, and IP port 47 is used to send the data.
Layer 2 Tunneling Protocol/Internet Protocol Security (L2TP/IPSec)	L2TP uses UDP port 1701 to negotiate and establish the L2TP tunnel, and UDP port 500 (IKE) and UDP port 4500 (IPSec NAT-T) to create the connection.
IP Protocol ID 50	IP Protocol ID 50 is used to send Encapsulated Security Protocol (ESP) traffic.
Secure Socket Tunneling Protocol (SSTP)	SSTP uses HTTPS port 443.

NOTE **UNDERSTANDING SSTP**

Secure Socket Tunneling Protocol (SSTP) is a new tunneling protocol that uses HTTP encapsulation over an SSL channel. Because SSTP uses SSL traffic (TCP port 443), SSTP can be used in many different network configurations, for example, when VPN clients or servers are behind network address translators (NATs), firewalls, or proxy servers. SSTP is supported by Windows SBS 2008, Windows Server 2008, and Windows Vista Service Pack 1.

The VPN is not enabled during the Windows SBS 2008 installation. You must first configure a valid Internet address using the Internet Address Management Wizard (on the Windows SBS Console home page) before you can enable a VPN.

EXAM TIP

Windows SBS 2008 requires a broadband Internet connection for VPN access to the server and does not support dial-up modem connections.

Configure Access to the Virtual Private Network

By default, all users assigned the Network Administrator role in Windows SBS 2008 have VPN access permissions. You must assign VPN access permissions for other users. You can assign permissions in two ways in the Windows SBS Console:

- Click the Users And Groups tab, click the Users tab, and then click the user account you want to configure. Click Edit User Account Properties in the task pane, and then click the Remote Access link. In the right pane, select the User Can Access Virtual Private Network option to add the user account to the Windows SBS Virtual Private Network Users security group and clear this option to remove the account from the security group.
- Click the Network tab, click the Connectivity tab, and then click Virtual Private Network. In the task pane, click View Virtual Private Network Properties. In the General Properties dialog box, click Modify to open the Change Group Membership dialog box. In this dialog box, you can select which users and groups to add to the Windows SBS Virtual Private Network Users security group and which to remove.

In both cases the users or groups are added to or removed from the preconfigured Windows SBS Virtual Private Network Users security group in Active Directory.

NOTE **ENABLING VPN ACCESS**

Setting up the server running Windows SBS 2008 for VPN access is a two-step process. First, you must enable the VPN settings on the server, and then you must assign VPN access permissions to users or groups.

Manage Routing and Remote Access

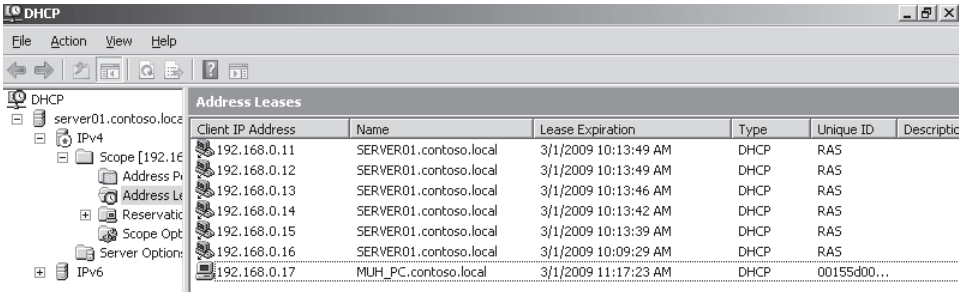
By default, when you run the Set Up Virtual Private Networking Wizard Windows SBS 2008 is configured to enable five PPTP VPN ports. This can cause a problem on a network where, for instance, 20 users try to connect using the VPN at the same time! You can reconfigure this setting in the Routing And Remote Access console. You can open the Routing And Remote Access console by clicking Start, pointing to Administrative Tools, and clicking Routing And Remote Access, or by clicking Start and typing **rrasmgmt.msc** in the Start Search box.

ADDING VPN PORTS

You can add an unlimited number of VPN ports in Routing And Remote Access. Expand the Server node, right-click the Ports node, and then click Properties. There you can see a list of all the Routing And Remote Access devices (Point-to-Point Protocol over Ethernet (PPPoE), PPTP, L2TP, and SSTP). Select the WAN Miniport (PPTP) option, and then click Configure to open the Configure Device–WAN Miniport (PPTP) dialog box. In this dialog box, you can increase the number of ports available for remote access.

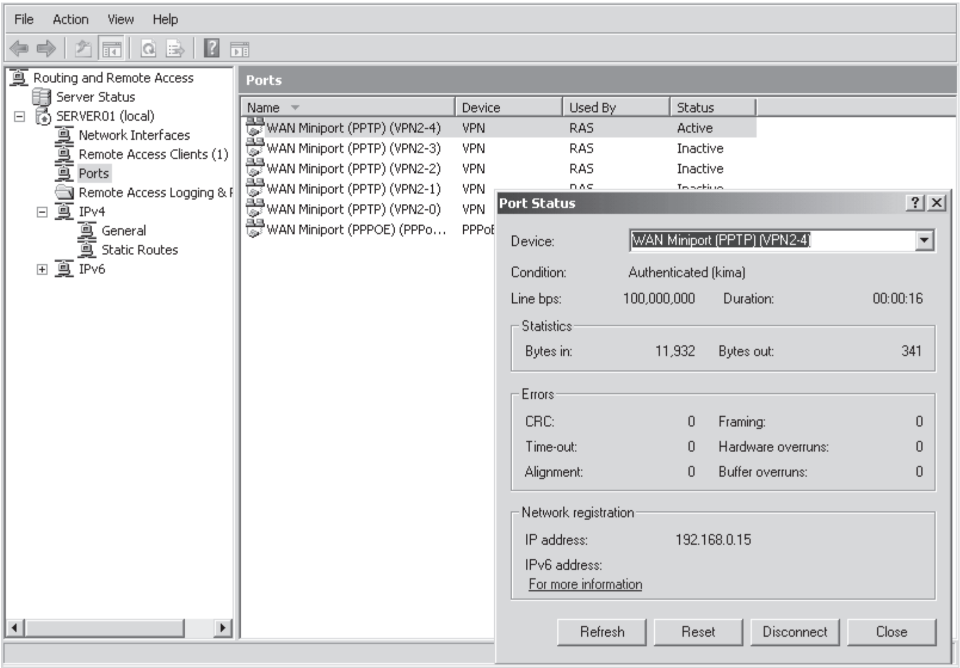
ASSIGNING IP ADDRESSES

When the remote client initiates the connection with the server running Windows SBS 2008, it creates a virtual interface and requests an IP address from the server. By default, the server grabs five Dynamic Host Configuration Protocol (DHCP) address leases. Five PPTP ports are enabled on the server running Windows Small Business Server, as shown in Figure 5-12. When a remote client connects to the server, an IP address from the available pool is assigned using the Internet Protocol Control Protocol (IPCP), as shown in Figure 5-13.



Client IP Address	Name	Lease Expiration	Type	Unique ID	Descriptic
192.168.0.11	SERVER01.contoso.local	3/1/2009 10:13:49 AM	DHCP	RAS	
192.168.0.12	SERVER01.contoso.local	3/1/2009 10:13:49 AM	DHCP	RAS	
192.168.0.13	SERVER01.contoso.local	3/1/2009 10:13:46 AM	DHCP	RAS	
192.168.0.14	SERVER01.contoso.local	3/1/2009 10:13:42 AM	DHCP	RAS	
192.168.0.15	SERVER01.contoso.local	3/1/2009 10:13:39 AM	DHCP	RAS	
192.168.0.16	SERVER01.contoso.local	3/1/2009 10:09:29 AM	DHCP	RAS	
192.168.0.17	MUH_PC.contoso.local	3/1/2009 11:17:23 AM	DHCP	00155d00...	

FIGURE 5-12 The server grabs five IP addresses for lease to remote clients.



Name	Device	Used By	Status
WAN Miniport (PPTP) (VPN2-4)	VPN	RAS	Active
WAN Miniport (PPTP) (VPN2-3)	VPN	RAS	Inactive
WAN Miniport (PPTP) (VPN2-2)	VPN	RAS	Inactive
WAN Miniport (PPTP) (VPN2-1)	VPN		
WAN Miniport (PPTP) (VPN2-0)	VPN		
WAN Miniport (PPPOE) (PPPo...	PPPoE		

Port Status

Device: WAN Miniport (PPTP) (VPN2-4)

Condition: Authenticated (kima)

Line bps: 100,000,000 Duration: 00:00:16

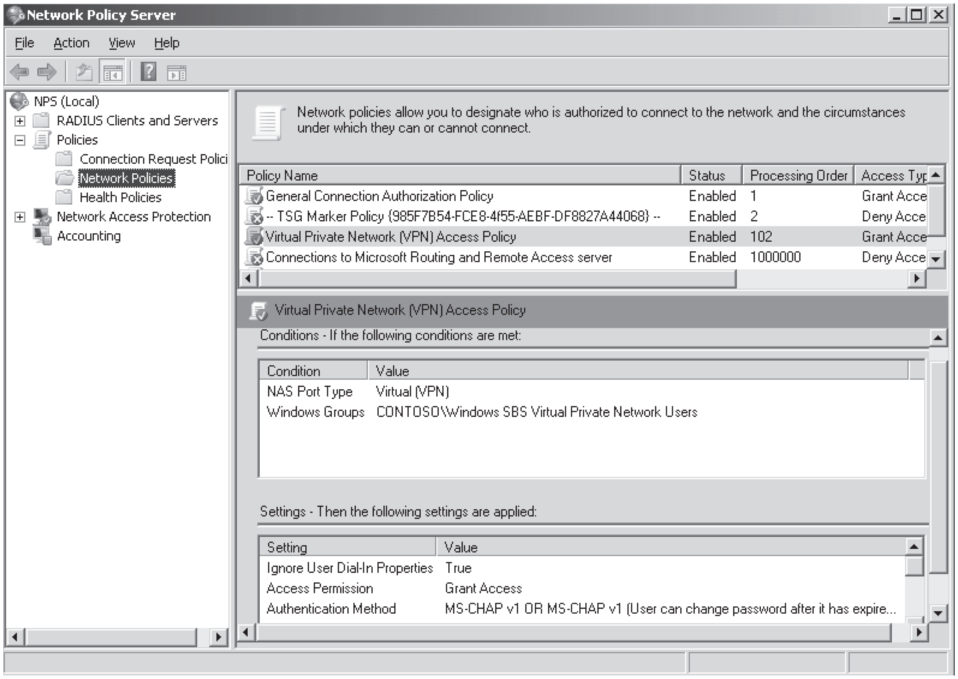
Statistics
Bytes in: 11,932 Bytes out: 341

Errors
CRC: 0 Framing: 0
Time-out: 0 Hardware overruns: 0
Alignment: 0 Buffer overruns: 0

Network registration
IP address: 192.168.0.15
IPv6 address:
For more information

FIGURE 5-13 The port status in Routing And Remote Access, which reveals that the client was assigned an IP address that was set aside in the Remote Access Service (RAS) DHCP pool.

The Network Policy Server (NPS) manages the Network policy for VPN access as well as the connection request authentication and connection request authorization in Windows SBS 2008, as shown in Figure 5-14. You can open the Network Policy Server by clicking Start, pointing to Administrative Tools, and clicking Network Policy Server, or by clicking Start and typing **nps.msc** in the Start Search box. A fuller description of NPS is beyond the scope of this training kit, but for more information you can visit *http://www.microsoft.com/nps*.



Network policies allow you to designate who is authorized to connect to the network and the circumstances under which they can or cannot connect.

Policy Name	Status	Processing Order	Access Typ
General Connection Authorization Policy	Enabled	1	Grant Acce
-- TSG Marker Policy {985F7B54-FCE8-4f55-AEBF-DF8827A44068} --	Enabled	2	Deny Acce
Virtual Private Network (VPN) Access Policy	Enabled	102	Grant Acce
Connections to Microsoft Routing and Remote Access server	Enabled	1000000	Deny Acce

Virtual Private Network (VPN) Access Policy

Conditions - If the following conditions are met:

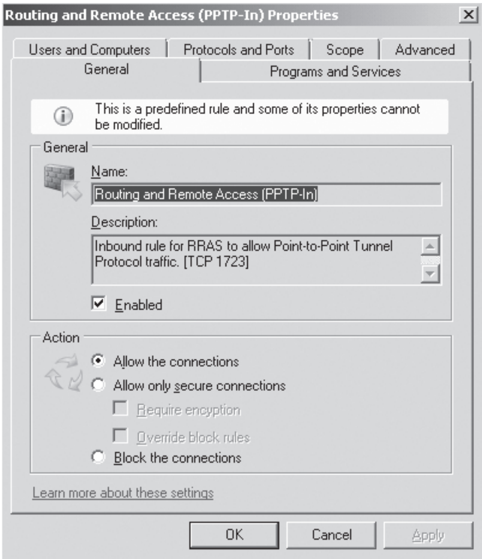
Condition	Value
NAS Port Type	Virtual (VPN)
Windows Groups	CONTOSO\Windows SBS Virtual Private Network Users

Settings - Then the following settings are applied:

Setting	Value
Ignore User Dial-In Properties	True
Access Permission	Grant Access
Authentication Method	MS-CHAP v1 OR MS-CHAP v1 (User can change password after it has expire...

FIGURE 5-14 The Network Policy Server (NPS) in Windows SBS 2008 is preconfigured to manage connection requests and authorization.

The Windows Firewall with Advanced Security rules are configured by default when enabling the VPN in Windows Small Business Server. You can access the firewall rules by clicking Start and typing **wf.msc** in the Start Search box or by clicking Start, pointing to Administrative Tools, and clicking Windows Firewall With Advanced Security. One of the many rules that is configured is the Routing And Remote Access (PPTP-In) rule, which defines the port number for Point-to-Point Tunneling Protocol (PPTP) traffic and enables Windows Firewall with Advanced Security to filter connections based on the rule criteria, as shown in Figure 5-15. The informational notice in the General tab states that this is a predefined rule and some of its properties cannot be modified. You cannot modify the port number; however, you can modify which user accounts and computers are authorized to connect, and you can configure a scope of local and remote addresses for the firewall rule if needed. If you use the Set Up Virtual Private Networking Wizard, you should not have to open the Windows Firewall with Advanced Security (or Routing And Remote Access and NPS, for that matter), but it is good to know that you can fine-tune VPN access using the native Windows tools if so desired.



Routing and Remote Access (PPTP-In) Properties

Users and Computers | Protocols and Ports | Scope | Advanced | General | Programs and Services

This is a predefined rule and some of its properties cannot be modified.

General

Name: Routing and Remote Access (PPTP-In)

Description: Inbound rule for RRAS to allow Point-to-Point Tunnel Protocol traffic. [TCP 1723]

☑ Enabled

Action

● Allow the connections

○ Allow only secure connections

□ Require encyption

□ Override block rules

○ Block the connections

Learn more about these settings

FIGURE 5-15 One of many predefined rules in Windows Firewall with Advanced Security

Configure Clients for the Virtual Private Network

You can configure client computers running Windows XP and Windows Vista for access to the Windows SBS 2008 virtual private network. This is a straightforward process that is documented in each operating system's Help files.

For step-by-step instructions, see the article titled "Set Up a VPN on Client Computers" at the Windows Small Business Server TechCenter (*http://technet.microsoft.com/en-us/library/cc513974.aspx*).

PRACTICE Configuring a Virtual Private Network

EXERCISE 1 Enable a Virtual Private Network

In this exercise, you enable a VPN.

1. Open the Windows SBS Console.
2. On the navigation bar, click the Network tab, and then click the Connectivity tab.
3. Click Configure A Virtual Private Network in the task pane to open the Set Up Virtual Private Networking Wizard.
4. Click Allow Users To Connect To The Server By Using A VPN. The wizard enables the Routing and Remote Access service, configures the router (if it is UPnP enabled), and sets up a PPTP VPN.
5. When the wizard finishes, click Finish.

EXERCISE 2 Set Up a VPN on a Computer Running Windows XP

Perform this exercise only if you are using a client computer that runs Windows XP.

1. On the computer running Windows XP, confirm that the connection to the Internet is correctly configured.
2. Click Start, and then click Control Panel.
3. In Control Panel, double-click Network Connections.
4. Click Create A New Connection.
5. On the Network Connection Wizard Welcome page, click Next.
6. On the Network Connection Type page, click Connect To The Network At My Workplace, and then click Next.
7. On the Network Connection page, click Virtual Private Network Connection, and then click Next.
8. On the Connection Name page, type a descriptive name for the connection, and then click Next.
9. On the Public Network page, click Do Not Dial The Initial Connection, and then click Next.
10. On the VPN Server Selection page, type the IP address of the computer that you want to connect to (**192.168.0.2** or the external IP address in the real world), and then click Next.
11. Select the Add A Shortcut To This Connection To My Desktop check box if you want to create a shortcut on the desktop, and then click Finish.
12. If you are prompted to connect, click No.
13. In the Network Connections window, right-click the new connection, and then click Properties.
14. Click the Options tab, and then click the Include Windows Logon Domain option to specify that you want to request Windows logon domain information before you try to connect.

EXERCISE 3 Set Up a VPN on a Computer Running Windows Vista

Perform this exercise only if you have a client computer that runs Windows Vista.

1. On the computer that is running Windows Vista, confirm that the connection to the Internet is correctly configured.
2. Click Start, and then click Control Panel.
3. In Control Panel, click Network And Internet, and click Network And Sharing Center.
4. Click Set Up A Connection Or Network.
5. Click Connect To A Workplace, and then click Next. Select No, Create A New Connection, and then click Next.
6. Type the user name **KIMA** and password **Pa$$w0rd** in the text boxes, click Create, and then click Close.

EXERCISE 4 Configure Permissions for a Virtual Private Network Connection

In this exercise, you configure access permissions for users. Switch to the server running Windows SBS 2008 for this exercise, which has the Windows SBS Console open.

1. On the navigation bar, click Users And Groups, and then click the Users tab.
2. Double-click the Kim Akers user account, and click the Remote Access link on the Kim Akers Properties page.
3. Select the User Can Access Virtual Private Network check box, and click OK. This action adds Kim Akers to the Windows SBS Virtual Private Network Users security group.
4. On the navigation bar, click the Network tab, click the Connectivity tab, and then right-click VPN Connection.
5. Click View Virtual Private Network Properties. On the General Properties page, click Modify.
6. Select Mu Han and Don Richardson in the left pane, and then click Add. You can add multiple user accounts at once to the Windows SBS Virtual Private Network Users group. Click OK, and then click OK again.

EXERCISE 5 Use the Virtual Private Network Connection

To use the VPN connection, switch to the non-domain-joined client computer and complete this exercise.

1. To start a VPN connection, click Start, point to Connect To, and then click the new connection. (If you added a connection shortcut to the desktop, double-click the shortcut on the desktop.)
2. If you are not currently connected to the Internet, Windows on the client computer offers to connect to the Internet.
3. After your computer connects to the Internet, the VPN server prompts you for the user name and password. Type the user name **KIMA** and password **P@ssw0rd**, and then click Connect. Close the window.

4 You can now access network resources the same way you do when you are connected directly to the local area network.

5. Open the command prompt and type **ipconfig/ all**, and find the IP address assigned to the client computer using the PPP adapter VPN connection.
6. Switch to the server running Windows SBS 2008, click Start, and type **rrasmgmt.msc** in the Start Search box to open Routing And Remote Access.
7. Expand the server node, and then click the Remote Access Clients node. You should see Contoso\Kima listed as a remote access client. Right-click Contoso\Kima, and click Status. Under Network Registration you will see the assigned IP address listed. Here you could also reset the connection or disconnect the remote access client. Close Routing And Remote Access.
8. To disconnect from the VPN, switch back to the client computer. Click Start, point to Connect To, and click Disconnect in the Connect To A Network dialog box.

EXERCISE 6 Disable a Virtual Private Network Connection

In this exercise, you disable a virtual private network connection.

1. In the Windows SBS Console, on the navigation bar, click the Network tab, and then click the Connectivity tab.
2. Click Configure A Virtual Private Network in the task pane to open the Set Up Virtual Private Networking Wizard.
3. Click Do Not Allow Users To Connect To The Server By Using A VPN. This causes the wizard to disable the Routing and Remote Access service, close port 1723 on the router (if it is UPnP enabled), and remove the VPN configuration.
4. When the wizard finishes disabling the VPN, click Finish.

✓ Quick Check

- **Does a certificate need to be installed before you use a virtual private network?**
- **Does PPTP provide encryption?**
- **Which VPN protocols does Windows SBS 2008 support, and which one is the default protocol used by the Set Up Virtual Private Networking Wizard?**
- **Which ports need to be open on the router for the Windows Small Business Server default VPN configuration to work?**

Quick Check Answers

- **No certificate needs to be installed to use a VPN. One of the benefits of using PPTP is that it does not require a certificate for remote access.**
- **PPTP by itself creates, maintains, and disconnects a virtual private network between two end points but does not encrypt the data. PPTP allows multiprotocol traffic to be encrypted; therefore, GRE is used to encapsulate the data or payload in a secure manner.**
- **Windows SBS 2008 supports PPTP, L2TP/IPSec, and SSTP. L2TP/IPSec and SSTP have to be configured manually. PPTP is the default protocol used by the Set Up Virtual Private Networking Wizard.**
- **TCP port 1723 needs to be open for PPTP to create and maintain the connections between the VPN client and VPN server, and IP port 47 needs to be open for GRE to send encapsulated data.**

Case Scenario: Implementing a Windows Small Business Server 2008 Solution

Contoso, Ltd., a 35-person law firm, has many employees working remotely. Employees must have the ability to store documents on the company server and pull documents from the server at any given time. Some staff should have the ability to access their office workstations from their remote laptops while traveling.

The firm uses third-party proprietary legal software that was designed to work with VPN access for remote access. You must implement the best solutions to enable and support all access methods with the best security available based on the company budget (meaning use all free Windows Small Business Server security features). Answer the following questions for your manager:

1. What tasks must you perform to ensure that all users have access to Remote Web Workplace?
2. What tasks must you perform to enable virtual private network access and ensure that only employees that really need VPN access have permission to use it?
3. What is the best way to deploy the self-issued certificate to remote users with non-domain-joined client computers?
4. Not all users should have remote access to their office workstations through Remote Web Workplace. How can you ensure this is the case?
5. Some users need access to other office workstations besides their own. How can you accomplish this?
6. A managing partner wants to know whether a self-issued certificate is as safe as a third-party certificate. What can you tell the partner about the differences between the two types of certificates?
7. How can you bind third-party certificates to the default Windows Small Business Server Web sites?

Suggested Practices

To help you successfully master the exam objectives presented in this chapter, complete the following tasks.

Modify Remote Web Workplace (RWW)

- **Practice 1** Familiarize yourself with the default Windows Small Business Server Web sites. Go to Internet Information Services Manager and take a closer look at the default Web sites and their settings, including the certificate.
- **Practice 2** Familiarize yourself with self-issued and third-party certificates. Open certmgr.msc and look closely at the options available for managing certificates. On the server running Windows SBS 2008, open the CA and look at the settings and options for certificates there.

- **Practice 3** Familiarize yourself with VPN connections. Create several VPN connections from a client computer and explore opening *http://companyweb* and other folders through the VPN connection.
- **Practice 4** Familiarize yourself with Remote Web Workplace customization. Modify Remote Web Workplace and use user accounts with different permissions to access it. Add links to the Remote Web Workplace Link List and allow users to access more than one computer. See how this is displayed in Remote Web Workplace.
- **Practice 5** Familiarize yourself with the TS Gateway Manager. Open the TS Gateway Manager and review the settings for the resource authorization policy and connection authorization policy.

Modify RAS

- **Practice 1** Increase the number of VPN connections allowed to the server. Open Routing and Remote Access and review the different types of available connections. Modify the available number of VPN connections.

Chapter Summary

- Remote access to Windows Small Business Server is secured by using self-issued or third-party certificates. The self-issued certificate is installed and bound to Remote Web Workplace when you run the Internet Address Management Wizard. Alternatively, you can use the Add A Trusted Certificate Wizard to install and manage a third-party certificate on the server.
- You can enable and disable access to Remote Web Workplace and select available features on the Remote Web Workplace Properties page for individual users or entire groups. You can create and modify organization links that are displayed in the Windows Vista Desktop Links gadget using the Remote Web Workplace Links List properties. For remote access to a client computer on the Windows SBS 2008 network, Remote Web Workplace uses Remote Desktop Connection, Remote Desktop Protocol, and the Terminal Services Gateway Manager. You can use the certificatepackage.zip file to distribute and install the self-issued certificate on non-domain-joined client computers or mobile devices.
- You can implement a virtual private network connection in Windows Small Business Server using the Set Up Virtual Private Networking Wizard. To configure additional ports you must use Routing and Remote Access.
- Not only should you know which administrative tasks you can accomplish in the Windows SBS Console, you should also understand what actual changes are made in the background when you run a wizard and which processes are involved. This chapter covers the functions of the main Windows Small Business Server wizards that you can use to manage remote access. It also explains the processes launched by the wizards in the background.

Index