
# Installing Windows Rights Management Services with Service Pack 2 Step-by-Step Guide

Microsoft Corporation

Published: October 2006

Author: Brian Lich

Editor: Carolyn Eller

## Abstract

This step-by-step guide provides instructions for setting up a test environment to deploy and evaluate Microsoft® Windows® Rights Management Services (RMS) on Microsoft Windows Server® 2003. It includes the necessary information for preparing the RMS infrastructure, installing and configuring RMS, and verifying RMS features after configuration is complete.

Microsoft

# Contents

# Installing Windows Rights Management Services with Service Pack 2 Step-by-Step Guide

## About this Guide

This step-by-step walks you through the process of setting up a working Microsoft® Windows® Rights Management Services (RMS) with Service Pack 2 infrastructure in a test environment. During this process you create an Active Directory® domain, install a database server, install RMS, configure the RMS cluster, and configure the RMS client computer.

Once complete, you can use the test lab environment to evaluate RMS on Microsoft Windows Server 2003 and assess how it might be deployed in your organization.

As you complete the steps in this guide, you will:

- Prepare the RMS infrastructure.
- Install and configure RMS.
- Verify RMS functionality after you complete the configuration.

The goal of an RMS deployment is to be able to protect information, no matter where it goes. Once RMS protection is added to a digital file, the protection stays with the file. By default, only the content owner is able to remove the protection from the file. The owner can grant rights to other users to perform actions on the content, such as the ability to view, copy, or print the file. To learn more about the business reasons behind a RMS deployment, see the white paper "Windows Rights Management Services: Helping Organizations Safeguard Digital Information from Unauthorized Use" (http://go.microsoft.com/fwlink/?LinkId=64636).

### What this Guide Does Not Provide

This guide does not provide the following:

- Guidance for installing and configuring RMS in a production environment.
- Complete technical reference for RMS. For more in-depth technical information about RMS, see http://go.microsoft.com/fwlink/?LinkId=68637.

# Deploying RMS in a Test Environment

We recommend that you first use the steps provided in this guide in a test lab environment. Step-by-step guides are not necessarily meant to be used to deploy Microsoft products without accompanying documentation and should be used with discretion as a stand-alone document.

Upon completion of this step-by-step guide, you will have a working RMS with SP2 infrastructure. You can then test and verify RMS operations through the simple task of restricting permissions on a Microsoft Office Word 2007 document.

The test environment described in this guide includes three computers connected to the Internet and using a clean installation of the following operating systems, applications, and services:

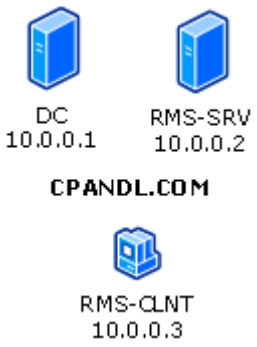
| Computer Name | Operating System | Applications and Services |
|---|---|---|
| RMS-SRV | Windows Server 2003 with Service Pack 1 (SP1) | RMS, Internet Information Services (IIS) 6.0, World Wide Web Publishing Service, Message Queuing (also known as MSMQ), and Microsoft SQL Server™ 2005 Standard Edition |
| DC | Windows Server 2003 with SP1 | Active Directory, Domain Name System (DNS) |
| RMS-CLNT | Windows XP Professional with Service Pack 2 (SP2) | Microsoft Office Word 2007 |

**Note**

If the RMS server is not connected to the Internet, it must be enrolled offline before the provisioning of the RMS server is complete.

The computers form a private intranet and are connected through a common hub or Layer 2 switch. This configuration can be emulated in a virtual server environment if desired. This step-by-step exercise uses private addresses throughout the test lab configuration. The private network ID 10.0.0.0/24 is used for the intranet. The domain controller is named DC for the domain named cpandl.com.

The following figure shows the configuration of the test environment:




# RMS Technology Review

RMS provides services to enable the creation of information-protection solutions. RMS is a format and application-agnostic technology. It will work with any RMS-enabled application to provide persistent usage policies for sensitive information. Content that can be protected using RMS includes e-mail messages and documents. RMS includes a set of core functions that allow developers to add information protection to the functionality of existing applications.

The RMS system, which includes both server and client components, performs the following processes:

- Licensing and distributing rights-protected information. An RMS system issues rights account certificates identifying trusted entities (such as users, groups, and services) that can publish rights-protected content. Once trust has been established, users can assign usage rights and conditions to content they want to protect. These usage rights specify who can access rights-protected content and what they can do with it. When the content is protected, a publishing license is created for the content. This license binds the specific usage rights to a given piece of content so that the content can be distributed. For example, a user can send a rights-protected document to other users inside or outside of their organization without losing the assigned rights.
- Acquiring licenses to decrypt rights-protected content and applying usage policies. Users who have been granted a rights account certificate can access rights-protected content by using an RMS-enabled client application that allows users to view and work with rights-protected content to preserve that content's integrity and to apply usage policies. When users attempt to access rights-protected content, requests are sent to the RMS system to access, or "consume," that content. When a user attempts to consume the protected content, the RMS licensing services on the RMS cluster issues a unique use license that reads, interprets, and applies the usage rights and conditions specified in the publishing licenses. The content is decrypted by using the electronic keys from the content and applications, and the certificates of the trusted

entities. The usage rights and conditions are persistent and automatically applied everywhere the content goes.

- Creating rights-protected files and templates. Users who are trusted entities in a RMS system can create and manage rights-protected content by using familiar authoring applications and tools in a RMS-enabled application that incorporates RMS technology features. In addition, RMS-enabled applications can use centrally defined and officially authorized usage rights templates to help users efficiently apply a predefined set of usage policies.

# Requirements for RMS with Service Pack 2

The following table describes the minimum hardware requirements and recommendations for running RMS with Service Pack 2.

| Requirement | Recommendation |
|---|---|
| Personal computer with one Pentium III processor (800 megahertz [MHz] or higher) | Computer with two Pentium 4 processors (1500 MHz or higher) |
| 256 megabytes (MB) of RAM | 512 MB of RAM |
| 20 gigabytes (GB) of free hard disk space | 40 GB of free hard disk space |
| One network adapter | One network adapter |

The following table describes the software requirements for running RMS on a Windows Server 2003–based computer.

| Software | Requirement |
|---|---|
| Operating system | Windows Server 2003, any editions except Web Edition |
| File system | NTFS file system is recommended |
| Messaging | Message Queuing |
| Web services | Internet Information Services (IIS)<br>ASP.NET must be enabled. |

| Software | Requirement |
|---|---|
| Active Directory | RMS must be installed in an Active Directory domain in which the domain controllers are running Windows Server 2000 with Service Pack 3 (SP3) or later. All users and groups who use RMS to acquire licenses and publish content must have an e-mail address that is configured in Active Directory. |
| Database server | RMS requires a database and stored procedures to perform operations. In this step-by-step guide you use Microsoft SQL Server 2005 Standard Edition. In a production environment, a separate database server is recommended. |

# Steps for Installing RMS with SP2

If your test environment does not have Internet access, you should copy the RMS with SP2 client to RMS client, and copy the RMS with Service Pack 2 server installation package to the RMS server.

- Step 1: Setting up the Infrastructure
- Step 2: Installing and Configuring RMS on RMS-SRV
- Step 3: Verifying RMS functionality on RMS-CLNT

## Step 1: Setting up the Infrastructure

To prepare your test environment for installing RMS, you must complete the following tasks:

- Configure the domain controller (DC)
- Configure the computer to be used as the RMS cluster (RMS-SRV)
- Configure the RMS client computer (RMS-CLNT)

### Configure the Domain Controller (DC)

To configure the domain controller DC, you must install Windows Server 2003, configure TCP/IP properties, install Active Directory, create user accounts, and then assign these user accounts an e-mail address.

First, install Windows Server 2003 as a stand-alone server.

### To install Windows Server 2003, Standard Edition

1. Start your computer by using the Windows Server 2003 product CD. (You can use any edition of Windows Server 2003 except the Web Edition to establish the domain).
2. Follow the instructions that appear on your computer screen, and when prompted for a computer name, type **DC**.

Next, configure TCP/IP properties so that DC has a static IP address of 10.0.0.1. In addition, configure 10.0.0.1 as the IP address for the DNS server.

### To configure TCP/IP properties on DC

1. Click **Start**, point to **Control Panel**, and point to **Network Connections**, double-click **Local Area Connection**, and then click **Properties**.
2. On the **General** tab, click **Internet Protocol (TCP/IP)**, and then click **Properties**.
3. Click the **Use the following IP address** option. In the **IP address** box, type **10.0.0.1**. In **Subnet mask** box, type **255.255.255.0**.
4. Click the **Use the following DNS server addresses** option. In the **Preferred DNS server** box, type **10.0.0.1**.
5. Click **OK**, and then click **OK** to close the **Local Area Connection Properties** dialog box.

Next, configure the computer as a domain controller.

### To configure DC as a domain controller

1. Click **Start**, and then click **Run**. In the **Open** box, type **dcpromo**, and then click **OK**.
2. On the Welcome page of the Active Directory Installation Wizard, click **Next**.
3. Click **Next**, click the **Domain controller for a new domain** option, and then click **Next**.
4. Select the **Domain in a new forest** option, and then click **Next**.
5. In the **Full DNS name for new domain** box, type **cpandl.com**, and then click **Next**.
6. In the **Domain NetBIOS name** box, type **CPANDL**, and then click **Next** three times.
7. Select the **Install and configure the DNS server on this computer, and set this computer to use this DNS server as its preferred DNS server** option.

8. Select the **Permissions compatible only with Windows 2000 or Windows Server 2003 operating systems** option, and then click **Next**.
9. In the **Restore Mode Password** box, type a strong password. In the **Confirm password** box, type the password again, and then click **Next**.
10. Click **Next**.
11. When the Active Directory Installation Wizard is done, click **Finish**.

**Note**

You must restart the computer after you complete this procedure.

Next, add the following user accounts: RMSSRVC, RMSADMIN, USER1, and USER2.

**To add new user accounts**

1. Click **Start**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**. This opens the **Active Directory Users and Computers** Microsoft Management Console (MMC) snap-in.
2. In the console tree, expand cpandl.com, right-click **Users**, point to **New**, and then click **User**.
3. In the **New Object – User** dialog box, type RMSSRVC in the **Full name** and **User logon name** boxes, and then click **Next**.
4. In the **New Object – User** dialog box, type a password of your choice in the **Password** and **Confirm password** boxes. Clear the **User must change password at next logon** check box, click **Next**, and then click **Finish**.
5. Perform the above steps 1-4 for each of the following users: RMSADMIN, USER1, and USER2.

Finally, add e-mail addresses to the USER1 and USER2 user accounts.

**To add e-mail addresses to user accounts**

1. In the **Active Directory Users and Computers** snap-in, right-click **USER1**, click **Properties**, type **user1@cpandl.com** in the **E-mail** box, and then click **OK**.
2. Repeat this step for USER2.
3. Close the **Active Directory Users and Computers** snap-in.

## Configure the computer to be used as the RMS cluster (RMS-SRV)

To configure the member server RMS-SRV so that you can install RMS on it, you must install Windows Server 2003, configure TCP/IP properties, and then join RMS-SRV to the domain cpandl.com. You must also add the account RMSADMIN as a member to the

local administrators group. This is needed for RMSADMIN to install RMS on RMS-SRV. Additionally, there are several prerequisite components that must be installed on the RMS cluster including Internet Information Services (IIS), ASP.NET, Message Queuing, and SQL Server 2005 Standard Edition.

First, install Windows Server 2003 as a stand-alone server.

### To install Windows Server 2003, Standard Edition

1. Start your computer by using the Windows Server 2003 product CD. (You can use any edition of Windows Server 2003 except the Web Edition to establish the domain.)
2. Follow the instructions that appear on your computer screen, and when prompted for a computer name, type **RMS-SRV**.

Next, configure TCP/IP properties so that RMS-SRV has a static IP address of 10.0.0.2. In addition, configure the DNS server of DC (10.0.0.1).

### To configure TCP/IP Properties

1. Click **Start**, point to **Control Panel**, and point to **Network Connections**, double-click **Local Area Connection**, and then click **Properties**.
2. On the **General** tab, click **Internet Protocol (TCP/IP)**, and then click **Properties**.
3. Click the **Use the following IP address** option. In the **IP address** box, type **10.0.0.2**. In **Subnet mask** box, type **255.255.255.0**.
4. Click the **Use the following DNS server addresses** option. In the **Preferred DNS server** box, type **10.0.0.1**.
5. Click **OK**, and then click **OK** to close the **Local Area Connection Properties** dialog box.

Next, join RMS-SRV to the cpandl.com domain.

### To join RMS-SRV to the cpandl.com domain

1. Log on to RMS-SRV as CPANDL\ADMINISTRATOR.
2. Click **Start**, right-click **My Computer**, and then click **Properties**.
3. Click **Computer Name** tab, click **Change**.
4. In the **Computer Name Changes** dialog box, click **Domain**, and then type **cpandl.com**.
5. Click **More**, and type **cpandl.com** in **Primary DNS suffix of this computer** box.
6. Click **OK** twice.
7. When a **Computer Name Changes** dialog box appears prompting you for

administrative credentials, provide the credentials, and click **OK**.

8. When a **Computer Name Changes** dialog box appears welcoming you to the cpandl.com domain, click **OK**.
9. When a **Computer Name Changes** dialog box appears telling you that the computer must be restarted, click **OK**, and click **Close**.
10. Close the **System** dialog box.

Finally, add RMSADMIN to the local administrators group on RMS-SRV.

**To add RMSADMIN to the local administrators group**

1. Click **Start**, point to **Control Panel**, point to **Administrative Tools**, and then click **Computer Management**.
2. Expand **Local Users and Group**, and then click **Groups**.
3. Right-click **Administrators**, click **Add to Group**, click **Add**, and then type **RMSADMIN** in the **Enter the object names to select (examples)** box.
4. Click **OK** twice and then close **Computer Management**.

## Configure RMS client computer (RMS-CLNT)

To configure RMS-CLNT, you must install Windows XP Professional, configure TCP/IP properties, join RMS-CLNT to the domain cpandl.com, create a shared folder to store rights-protected content, and then install the RMS client. You must also install an RMS-enabled application. In this example, you install Microsoft Office Word 2007 on RMS-CLNT.

**To install Windows XP Professional**

1. Start your computer by using the Windows XP Professional product CD.
2. Follow the instructions that appear on your screen, and when prompted for a computer name, type **RMS-CLNT**.

Next, configure TCP/IP properties so that RMS-CLNT has a static IP address of 10.0.0.3. In addition, configure the DNS server of DC (10.0.0.1).

**To configure TCP/IP properties**

1. Click **Start**, click **Control Panel**, and then double-click **Network Connections**. Right-click **Local Area Connection**, and then click **Properties**.
2. On the **General** tab, click **Internet Protocol (TCP/IP)**, and then click **Properties**.
3. Click the **Use the following IP address** option. In the **IP address** box, type

**10.0.0.3**. In **Subnet mask** box, type **255.255.255.0**.

4. Click the **Use the following DNS server addresses** option. In the **Preferred DNS server** box, type **10.0.0.1**.
5. Click **OK**, and then click **OK** to close the **Local Area Connection Properties** dialog box.
6. Restart your computer for the changes to take effect.

Next, join RMS-CLNT to the cpandl.com domain.

### To join RMS-CLNT to the cpandl.com domain

1. Log on to DC as CPANDL\ADMINISTRATOR.
2. Click **Start**, right-click **My Computer**, and then click **Properties**.
3. On the **Computer Name** tab, click **Change**.
4. In the **Computer Name Changes** dialog box, click **Domain**, and then type **cpandl.com**.
5. Click **More**, and in **Primary DNS suffix of this computer**, type **cpandl.com**.
6. Click **OK** twice.
7. When a **Computer Name Changes** dialog box appears prompting you for administrative credentials, provide the credentials, and then click **OK**.
8. When a **Computer Name Changes** dialog box appears welcoming you to the cpandl.com domain, click **OK**.
9. When a **Computer Name Changes** dialog box appears telling you that the computer must be restarted, click **OK**.
10. Click **OK** to close the **System Properties** dialog box
11. In the **System Settings Change** dialog box, click **Yes**.

Next, create a folder on RMS-CLNT so that USER1 and USER2 both have access to open documents created by the other person.

### To create a folder that can be modified by both USER1 and USER2

1. Log on to RMS-CLNT as CPANDL\ADMINISTRATOR.
2. Click **Start**, click **My Computer**, and then double-click **Local Disk (C:)**.
3. Click **File**, point to **New**, and then click **Folder**.
4. Type **RMSDocs** for the new folder, and then press ENTER.
5. Right-click **RMSDocs**, and then click **Properties**.
6. Click the **Security** tab, click **Users** in the **Group or user names** box, and select the **Modify** check box in the **Allow** column of the **Permissions for Users** box.

7. Click **OK**.

Next, the RMS client must be downloaded and installed on RMS-CLNT.

**To install the RMS 1.0 SP2 client**

1. Log on to RMS-CLNT as CPANDL\ADMINISTRATOR.
2. Download the RMS client from http://go.microsoft.com/fwlink/?LinkId=67736. If you are using a 64-bit version of Windows XP Professional or Windows Server 2003, download the 64-bit version of the RMS client http://go.microsoft.com/fwlink/?LinkId=67935.
3. Double-click **WindowsRightsManagementServicesSP2-KB917275-Client-ENU.exe** to start the installation.
4. Click **Next**.
5. Select the **I agree** option, and then click **Next** twice to start the installation.
6. Click **Close** to finish the installation.

Next, install Microsoft Office Word 2007 Professional.

**To install Microsoft Office Word 2007 Professional**

1. Click **setup.exe** on the Microsoft Office 2007 Professional product CD.
2. Click **Customize** as the installation type, set the installation type to **Not Available** for Microsoft Office Access, Microsoft Office Excel, Microsoft Office InfoPath, Microsoft Office Outlook, Microsoft Office PowerPoint, Microsoft Office Publisher, and Microsoft Office Visio Viewer, and then click **Install Now**. This may take several minutes to complete.

## Step 2: Installing and Configuring RMS on RMS-SRV

To install RMS, you must complete the following steps:

- Add the Application Server role to RMS-SRV
- Install Message Queuing
- Install SQL Server 2005 Standard Edition
- Install the RMS cluster
- Configure RMS settings
- Register the SCP in Active Directory

## Add Application Server role to RMS-SRV

RMS uses IIS and ASP.NET to communicate with the RMS clients. To install IIS and ASP.NET, you must complete the following steps:

**To add the Application Server role**

1. Log on to RMS-SRV as CPANDL\ADMINISTRATOR. The **Manage Your Server** window appears.
2. Click **Add or remove a role**.
3. On the **Preliminary Steps** page of the Configure your Server Wizard, click **Next**.
4. Click **Application Server (IIS, ASP.NET)**, and then click **Next**.
5. Select the **Enable ASP.NET** check box, and then click **Next** twice.
6. When asked for files from the Windows Server 2003 product CD, insert it into the CD-ROM drive of the computer.
7. Click **Finish** to complete the installation.

## Install Message Queuing

Message Queuing is used to send information from the RMS cluster to the RMS logging database and must be installed prior to installing RMS. To install Message Queuing, you must complete the following steps:

**To install Message Queuing**

1. Click **Start**, point to **Control Panel**, and then click **Add or Remove Programs**.
2. Click **Add/Remove Windows Components**.
3. In the **Windows Components Wizard** dialog box, click **Application Server**, and then click the **Details** button.
4. In the **Application Server** dialog box, select the **Message Queuing** check box, and then click **OK**.
5. Click **Next** to start the installation.
6. Click **Finish** and close the **Add or Remove Programs** dialog box.

## Install Microsoft SQL Server 2005 Standard Edition

RMS requires a database used for storing configuration and logging information. Microsoft SQL Server 2005 Standard Edition is the database that will be used in this guide. It will be installed on the same computer as the RMS cluster (RMS-SRV). In a

production environment, it is recommended to install the RMS database on a dedicated computer.

**Note**

Microsoft SQL Server 2005 Express Edition is also supported as the database server. However, Microsoft SQL Server 2005 Express Edition is not recommended for use in production environments because it does not support adding additional servers to the RMS cluster or the ability to view or modify data stored in the configuration and logging databases. To download Microsoft SQL Server 2005 Express Edition, go to http://go.microsoft.com/fwlink/?LinkId=73721.

To install Microsoft SQL Server 2005 Standard Edition, refer to the following steps:

**To install Microsoft SQL Server 2005 Standard Edition**

1. Log on to RMS-SRV as CPANDL\ADMINISTRATOR.
2. Start the installation from the Microsoft SQL Server 2005 product CD by double-clicking Setup.exe.
3. Select the **I accept the licensing terms and conditions** check box, and then click **Next**. When the **Installing Prerequisites** page reports that the required components were installed successfully, click **Next** again.
4. When the system configuration check is complete, click **Next** on the **Welcome to the Microsoft SQL Server Installation Wizard** page to start the installation.
5. If you see no errors on the **System Configuration Check** page, click **Next**.
6. Complete the **Registration Information** page, and then click **Next**.
7. On the **Components to Install** page, select the **SQL Server Database Services** check box, and then click **Next**.
8. On the **Instance Name** page, verify that **Default Instance** is selected and then click **Next**.
9. On the **Service Account** page, select the **Use the built-in System account** option, click **Next** four times, and then click **Install**. The installation may take several minutes to complete.
10. On the **Setup Progress** page, when the installation has completed and the status of all the products in the list is **Setup finished**, click **Next**, and then click **Finish**.

## Install the RMS Cluster

Now that all of the prerequisite software has been installed, it is time to install the RMS cluster. To download RMS, go to http://go.microsoft.com/fwlink/?LinkId=73722. From RMS-SRV, you should do the following in order to install RMS:

### To install the RMS cluster

1. Log on to RMS-SRV as CPANDL\RMSADMIN.
2. Start the installation by double-clicking the installation file that you downloaded from the Microsoft Web site.
3. Click **Next**.
4. Read the License Agreement, select the **I agree** option, and then click **Next**.
5. Accept the default installation folder, click **Next**, and then click **Install**.
6. When the installation completes, click **Close**.

## Configure RMS settings

RMS is provisioned and administered by using a local Web site automatically created during the RMS installation.

### To provision RMS using Global Administration Web site

1. Click **Start**, point to **All Programs**, point to **Windows RMS**, and then click **Windows RMS Administration**.
2. Click **Provision RMS on this Web site**.
3. In the **User name** box under **RMS Service Account**, type **CPANDL\RMSSRVC**, and then type the password for CPANDL\RMSSRVC in the **Password** box.
4. In the **RMS private key password** box under **Private key protection and enrollment**, enter a strong password, and then confirm this strong password in the **Enter password again** box.
5. Type **rmsadmin@cpandl.com** in the **Administrative contact** box.
6. Under **RMS Proxy Settings**, clear the **This computer uses a proxy server to connect to the Internet** check box.
7. Keep the default values for everything else on this page, and then click **Submit**. This might take a few minutes to complete.

### Register the SCP in Active Directory

The RMS service connection point (SCP) in Active Directory allows RMS clients to discover the RMS cluster automatically. Active Directory SCP registration is not done automatically during installation. To register the RMS SCP, you must do the following:

**To register RMS SCP in Active Directory**

1. Log on to RMS-SRV as CPANDL\ADMINISTRATOR or another Active Directory user account who is a member of the **Enterprise Admins** group in the CPANDL Active Directory domain.
2. Click **Start**, point to **All Programs**, point to **Windows RMS**, and then click **Windows RMS Administration**.
3. Click **Administer RMS on this Web site**.
4. Scroll to the bottom of the page and click **RMS service connection point**.
5. Click **Register URL**.

## Step 3: Verifying RMS Functionality on RMS-CLNT

To verify the functionality of the RMS deployment, you log on as USER1 and then restrict permissions on a Microsoft Word 2007 document so that USER2 is able to read the document but is unable to change, print, or copy. You will then log on as USER2, verifying that the proper permission to read the document has been granted and nothing else.

**To restrict permissions on a Microsoft Word document**

1. Log on to RMS-CLNT as USER1.

   **Note**

   Since USER1 is the author of this document, USER1 will have full rights to the document, regardless of the RMS rights that are applied to it.
2. Click **Start**, click **All Programs**, click **Microsoft Office**, and then click **Microsoft Office Word 2007**.
3. Type **Only USER2 can read this document, but cannot change, print, or copy** on the blank document page, click the **Microsoft Office Button**, point to **Prepare**, point to **Restrict Permission**, and then click **Restricted access**.
4. Select the **Restrict permission to this document** check box.
5. In the **Read** box, type **user2@cpandl.com**, and then click **OK** to close the **Permission** dialog box.
6. Click the **Microsoft Office Button**, click **Save As**, and then save the file as

C:\RMSDocs\RMS-TST.docx.

7. Log off as USER1.

Finally, log on as USER2 and open the document, RMS-TST.docx.

**To view a protected document**

1. Log on as USER2.
2. Click **Start**, point to **All Programs**, point to **Microsoft Office**, and then click **Microsoft Office Word 2007**.
3. Click the **Microsoft Office Button**, click **Open**, and then double-click C:\RMSDocs\RMS-TST.docx.

   The following message appears in the message bar: **Permission to this document is currently restricted. Microsoft Office must connect to http://rms-srv/_wmcs/licensing to verify your credentials and download your permissions.**
4. Click **OK**.

   The following message appears: **Verifying your credentials for opening content with restricted permissions…**.
5. When the document opens, click the **Microsoft Office Button**. Notice that the **Print** option is not available.
6. Click **View Permission** in the message bar. You should see that USER2 has been restricted to only read the document.
7. Click **OK** to close the **My Permission** dialog box, and then close Microsoft Word.

You have successfully deployed and demonstrated the functionality of RMS, using the simple scenario of applying restricted permissions to a Microsoft Word 2007 document. You can also use this deployment to explore some of the additional capabilities of RMS through additional configuration and testing.