Microsoft® Office Sharepoint Server 2007 and Luna SA

Integration Guide

Copyright 2009 SafeNet, Inc. All rights reserved.
Preface

© 2009 SafeNet, Inc. All rights reserved.

Part Number: 009804-001 (Rev A, 06/2009)

All intellectual property is protected by copyright. All trademarks and product names used or referred to are the copyright of their respective owners. No part of this document may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, chemical, photocopy, recording or otherwise without the prior written permission of SafeNet.

SafeNet makes no representations or warranties with respect to the contents of this document and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Furthermore, SafeNet reserves the right to revise this publication and to make changes from time to time in the content hereof without the obligation upon SafeNet to notify any person or organization of any such revisions or changes.

SafeNet invites constructive comments on the contents of this document. These comments, together with your personal and/or company details, should be sent to the address below.
SafeNet, Inc.
4690 Millennium Drive
Belcamp, Maryland 21017
USA

Limitations

This document does not include the steps to set up the third-party software. The steps given in this document must be modified accordingly. Refer to Luna SA documentation for general Luna setup procedures.

Disclaimers

The foregoing integration was performed and tested only with the specific versions of equipment and software and only in the configuration indicated. If your setup matches exactly, you should expect no trouble, and Customer Support can assist with any missteps. If your setup differs, then the foregoing is merely a template and you will need to adjust the instructions to fit your situation. Customer Support will attempt to assist, but cannot guarantee success in setups that we have not tested.

Technical Support

If you encounter a problem while installing, registering or operating this product, please make sure that you have read the documentation. If you cannot resolve the issue, please contact your supplier or SafeNet support.

SafeNet support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between SafeNet and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Technical Support Contact Information:
Phone: 800-545-6608, 410-931-7520
Email: support@safenet-inc.com
Table of Contents

Preface........................................................................................................................................................................... i

Chapter 1 Introduction..................................................................................................................................................... 1
   Luna SA Setup........................................................................................................................................................... 2

Chapter 2 Integrating MS Office SharePoint Server 2007 with Luna SA................................................................. 3
   Generating a SSL Certificate to be used for Active Directory Rights Management Services Cluster Web Site using Luna Key Storage Provider (KSP) hosted on IIS 7.0................................................................. 4
   Install Microsoft Active Directory Rights Management Services using Luna Cryptographic Service Provider (CSP) on Windows Server 2008 ......................................................................................................................... 7
   Install and Configure Microsoft Office SharePoint Server 2007 on Windows Server 2008 ................................ 25
   Enable Transparent Database Encryption (TDE) on Office SharePoint Server 2007 database(s) hosted on MS SQL Server 2008 using Luna EKM (Extensible Key Management) ......................................................... 33
   Configuring Active Directory Rights Management Services to Work with Office SharePoint Server 2007 ...... 37
   Verifying AD RMS Functionality using ADRMS-CLNT........................................................................................... 39
   Enable SSL on Office SharePoint Server 2007 sites hosted on IIS 7.0 using Luna Key Storage Provider (KSP) ... 41
Chapter 1
Introduction

This document outlines the steps to configure and integrate Microsoft Office SharePoint Server 2007 with Luna SA.

The SharePoint Security solution will be a combination of Active Directory Rights Management Services, SQL Server 2008 Transparent Database Encryption and SSL using Internet Information Services (IIS) 7.0. A single HSM (Luna SA) will be deployed to provide a security framework to the data in use, data at rest and the data in transit.

Microsoft Office SharePoint Server 2007 will use Microsoft Active Directory Rights Management Services to implement document security utilizing Luna Cryptographic Service Provider (CSP) to store the AD RMS cluster keys on Luna SA and Microsoft SQL Server 2008 for Transparent Database Encryption utilizing Luna Extensible Key Management (EKM) to encrypt the Office SharePoint Server 2007 database(s) with the asymmetric key on Luna SA. Moreover, the AD RMS cluster web site and SharePoint web sites are hosted on Microsoft IIS 7.0, therefore Luna Key Storage Provider (KSP) can be utilized to store the SSL keys and certificates on Luna SA.
Scope

3rd Party Application Details

- Microsoft Office SharePoint Server 2007
- Microsoft Active Directory Right Management Services 2008
- Microsoft SQL Server 2008
- Microsoft IIS 7.0

Supported Platforms

The following platforms are supported for Luna SA:

- Windows Server 2008

HSMs and Firmware Version

- K5 HSM f/w 4.6.8

Distributions

- Luna SA 1U Appliance s/w 4.4
- Luna SA Client s/w v4.4 (32-bit)
- Luna EKM Client s/w 1.0.0 (32-bit)

Prerequisites

Luna SA Setup:

Please refer to the Luna SA documentation for installation steps and details regarding configuring and setting up the box on Windows systems. Before you get started ensure the following:

- Luna SA appliance has a secure admin password
- Luna SA has a hostname suitable for your network
- Luna SA network parameters are set to work with your network
- Initialized the HSM on the Luna SA appliance
- Created a partition on the HSM and allocated a partition password to be used later.
  Run the command, vtl verify to display a partition from Luna SA. The general form of command is
  C:\Program Files\LunaSA>vtl verify.
- Created and exchanged certificates between the Luna SA and the “Client” system (registered the Client
  with the Partition).
- Enabled Partition “Activation” and “Auto Activation” (Partition policy settings 22 and 23 (applies to Luna
  SA with Trusted Path Authentication [which is FIPS 140-2 level 3] only).
Chapter 2  
Integrating MS Office SharePoint Server 2007 with Luna SA

This chapter outlines the steps to install and integrate Microsoft Office SharePoint Server with Luna SA. This will be a combined solution of Office SharePoint Server 2007, Active Directory Rights Management Services, SQL Server 2008 and IIS 7.0.

Before You Begin

- You should familiarize yourself with Microsoft Office SharePoint Server 2007, Microsoft Active Directory Rights Management Services, Microsoft SQL Server 2008 and IIS 7.0. Refer to the appropriate help files for more information and pre-installation requirements.

Setup

- The setup consists of four systems in a private network as per the table below:

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Applications and Services</th>
<th>Description</th>
<th>Computer Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Server 2008 Enterprise</td>
<td>Active Directory, Domain Name System (DNS), Active Directory Certificate Services</td>
<td>Domain Controller Certificate Authority</td>
<td>Test-DC</td>
</tr>
<tr>
<td>Windows Server® 2008 Enterprise</td>
<td>AD RMS, Internet Information Services (IIS) 7.0, and Message Queuing</td>
<td>AD RMS Server</td>
<td>Test-ADRMS-SRV</td>
</tr>
</tbody>
</table>

- Test-DC is configured as domain controller with domain sharerms.com and a Certificate Authority.
- Join Test-ADRMS-SRV, Test-SPS-SRV, and Test-ADRMS-CLNT to the sharerms.com domain.
- Create users AdrmsAdmin, Ankit, Nicholas and Ben in the Active Directory.
- Enter the email addresses for these users as adrmsadmin@sharerms.com, ankit@sharerms.com, nicholas@sharerms.com, ben@sharerms.com respectively.
- Add AdrmsAdmin to local administrator group.
- Add AdrmsAdmin and Ankit to Enterprise Admins group.
Generating a SSL Certificate to be used for Active Directory Rights Management Services Cluster Web Site using Luna Key Storage Provider (KSP) hosted on IIS 7.0

Before you generate
- Install Internet Information Services (IIS) 7.0
- Install Luna Key Storage Provider

Install Microsoft IIS 7.0
1. Login to Test-ADRMS-SRV as Sharerms\AdrmsAdmin.
2. Click Start, point to Administrative tools, and then click Server Manager. The Server Manager snap-in appears.
3. Select Roles in the console tree.
4. Select the default (desired) components and finish the wizard to install IIS 7.0.

Install Luna Key Storage Provider
1. Luna KSP must be installed as a separate step following the completion of Luna SA client software.
2. After the KSP installation, traverse to C:\Program Files\SafeNet and run KspConfig.exe to register Luna KSP.

Create a certificate request using Luna KSP
IIS Manager does not support the creation of certificates protected by CNG Keys and these need to be created using the Microsoft command line utilities.

1. To generate a certificate request for a SSL certificate using an RSA 2048-bit key, create a file luna.inf with the following information:

[Version]
Signature= "$Windows NT$

[NewRequest]
Subject = "C=IN,CN=noi1-501705"
HashAlgorithm = SHA256
KeyAlgorithm = RSA
KeyLength = 2048
ProviderName = "SafeNet Key Storage Provider"
KeyUsage = 0xf0
MachineKeySet = True

[EnhancedKeyUsageExtension]
OID=1.3.6.1.5.5.7.3.1

Your inf file does not have to contain exactly the code given in the following step. These are examples, not definitive models.
2. To create the certificate request for the Certification Authority, execute the command:
Certreq.exe -new luna.inf request.req

Installing the certificate
After creating the certificate request, open the CA web interface and submit the request to the CA.
1. Open the browser and type http://Test-DC/certsrv.
2. Click on Request a certificate -> Advanced Certificate Request -> Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.
3. Paste the certificate request under Saved Request and click Submit.
4. Download the certificate and save the certificate.

Complete the certificate request
1. Open IIS Manager from Start -> Programs -> Administrative Tools -> Internet Information Services (IIS) Manager.
2. Select localhost on the left hand side of the IIS Manager window.
3. Double click Server Certificates.
4. Click on Complete Certificate Request.
5. Browse to the certificate obtained from the CA.
6. Specify some Friendly name and Click Ok.
Bind the certificate to the web site

1. Under sites on the left hand side of the IIS Manager window, select the desired web site.
2. On the right hand side of the IIS Manager, click on Bindings.

3. In the site Bindings, click Add.
4. Select the protocol https.
5. Select the certificate from the drop-down list.
6. Click OK to complete the certificate binding for SSL connection.
Install Microsoft Active Directory Rights Management Services using Luna Cryptographic Service Provider (CSP) on Windows Server 2008

Before you install

- Run the command, `register.exe` to register Luna CSP. The general form of command is `C:\Program Files\LunaSA\CSP>register.exe`

To install the Microsoft Active Directory Rights Management Services:

1. Login to **Test-ADRMS-SRV** as **Sharerms\AdrmsAdmin**.
2. Click **Start**, point to Administrative tools, and then click **Server Manager**. The **Server Manager** snap-in appears.
3. Select **Roles** in the console tree.
4. Right-click **Roles** and then click, **Add roles**. The **Add Roles** wizard appears.
5. Click **Next**.
6. Select **Active Directory Rights Management Services** checkbox from **Server Roles** to install on this server. You will receive a warning stating **Add roles services and features required for Active Directory Rights Management Services**.
7. Click **Add Required Role Services**.
8. Click **Next** to continue.
9. Click **Next** on the Active Directory Rights Management Services windows.
10. Select **Active Directory Rights Management Server** checkbox from the **Role Services**.
11. Click **Next** to continue.
12. Select **Create a new AD RMS cluster**.

---

**Active Directory Rights Management Server (AD RMS)** helps you protect information from unauthorized use. AD RMS establishes the identity of users and provides authorized users with licenses for protected information.
13. Click **Next** to continue.
14. Select **Use Windows Internal Database on this Server**.
15. Click **Next** to continue.

16. Specify the **Domain User Account**.

17. Click **OK** to continue.
18. Click **Next** to continue.
19. Select **Use CSP key storage** for AD RMS cluster key storage.
20. Click **Next** to continue.

21. Choose **Luna Cryptographic Services for Microsoft Windows** from the CSP dropdown to store the AD RMS cluster key and select **Create a new key with the selected CSP**.
22. Click **Next** to continue.
23. Select **Default Web Site** for the virtual directory.
24. Click **Next** to continue.
25. Select **Use an encrypted connection https://** for the connection type for the AD RMS cluster. Give the FQDN then click **Validate**.
26. Click **Next** to continue.

27. Select **Choose an existing certificate for SSL encryption (recommended)** for server authentication Certificate. Select the certificate generated in the above section using Luna KSP.
28. Enter a name for the server licensor certificate.
29. Click **Next** to continue.

30. Ensure that the Register **the AD RMS service connection point now** option is selected, and then click **Next** to register the AD RMS service connection point (SCP) in Active Directory during installation.
31. Click **Next** on the Web Server (IIS).
32. Click **Next** on the Select Role Services.

![Select Role Services](image)

33. Click **Install** on the Confirm Installation Sections.
34. Click **Install** to provision AD RMS on the computer.

35. Click **Close** to exit the **Add Roles** wizard after viewing the installation results. AD RMS root cluster keys will be generated and stored on Luna SA HSM.
36. Open the Active Directory Rights Management Services console.

37. You will see **Luna Cryptographic Services for Microsoft Windows** under:

   **Trust Policies -> Trusted Publishing Domains**
Security Policies –> Cluster Key Password

Cluster Key Password Settings

The administration for AD RMS Server Key Protection.

Cluster Key Password Settings

In the event of a data loss or disk failure, you can reset the password that protects the AD RMS cluster keys. If you used the centrally managed AD RMS encryption method to protect the AD RMS cluster keys, you can reset the cluster key password.

Key protection method:
CSP-based key

Cluster Key Password

Choose cluster key password
Install and Configure Microsoft Office SharePoint Server 2007 on Windows Server 2008

Before you install

- Install Microsoft .NET Framework 3.0.
- Install Microsoft SQL Server 2008.

Install Microsoft .NET Framework 3.0

1. Install Microsoft .NET Framework 3.0.

Install Microsoft SQL Server 2008 Setup

1. Install SQL Server 2008 (Enterprise, Developer, or Evaluation editions). For a detailed installation procedure of SQL Server 2008, please refer to the Microsoft SQL Server 2008 online documentation.

Install Office SharePoint Server 2007

1. Double-click setup.exe from the Office SharePoint Server 2007 product CD.
2. Enter your Product Key, and then click Continue.
3. Select the I accept the terms of this agreement check box, and then click Continue.
4. Click Advanced.
5. Select **Complete** and click **Install Now**.

6. The installation might take 10 minutes to complete.

**Configure Office SharePoint Server 2007**

1. After installation has completed, select the **Run the SharePoint Products and Technologies Configuration Wizard now** check box, and then click **Close**.
2. On the **Welcome to the SharePoint Products and Technologies** page, click **Next**.
3. Click **Yes** in the message confirming that the SharePoint services should be restarted. Office SharePoint Server 2007 will also be configured at this time.

4. Select **No, I want to create a new server farm** in Connect to a Server farm. Click **Next** to continue.
5. Enter name of the **Database server** in **Specify Configuration Database settings**. Enter the name of **SQL Server 2008** database server. Click **Next** to continue.
6. Click **Next** on the **Configure SharePoint Central Administration Web Application**.
7. Click **Next** on the **Completing the SharePoint Products and Technologies Configuration Wizard**.
Completing the SharePoint Products and Technologies Configuration Wizard

The following configuration settings will be applied:

- Configuration Database Server: NOI1-501341
- Configuration Database Name: SharePoint_Config
- Host the Central Administration Web Application: Yes
- Central Administration URL: http:// NOI1-501341:23392/
- Authentication provider: NTLM

Click Next to apply configuration settings.

8. Click Finish on Configuration Successful.
Configuration Successful

The following configuration settings were successfully applied:

- Configuration Database Server: NOI1-501341
- Configuration Database Name: SharePoint_Config
- Host the Central Administration Web Application: yes
- Central Administration URL: http://noi1-501341:22392/
- Authentication provider: NTLM

Click Finish to close the wizard and launch the SharePoint Central Administration homepage. Internet Explorer users may be prompted for a username in the form DOMAIN\User_Name and password to access the site. At that prompt, enter the credentials that you used to login to this computer. Add this site to the list of trusted sites when prompted.
Enable Transparent Database Encryption (TDE) on Office SharePoint Server 2007 database(s) hosted on MS SQL Server 2008 using Luna EKM (Extensible Key Management)

Once Office SharePoint Server 2007 has configured the database(s) on SQL Server 2008, Luna SA can be used to enable Transparent Database Encryption using the asymmetric key on HSM.

Install Luna EKM

1. A Windows-based installation program is provided to make the installation of the Luna EKM quick and easy. The installation CD can be obtained from the SafeNet Customer Connection Center.

Configure Luna EKM using LunaEKMConfig

LunaEKM includes a command line configuration utility “LunaEKMConfig”. This command line utility gets installed in LunaEKM installation folder. It provides command to register slots, view slots & to configure log settings.

Following commands are provided in LunaEKMConfig.

1. RegisterSlot
   Register/Edit the Slot for the LunaEKM to use.

2. ViewSlots
   View List of the Slots/HSM configured with this client.
LogSettings
Configure log settings for LunaEKM.

LogLevel (NONE=0,/info=1, DEBUG=2): <LogLevel>
LogFile name: <Name and location of LogFile>

To perform Luna SA integration with SQL Server 2008, Luna EKM software provides Luna EKM Provider in the form of EKM Library (i.e. LunaEKM.dll). The Luna EKM Provider can be used if the EKM Provider option is enabled in the SQL Server. This feature is available only on the Enterprise, Developer, and Evaluation editions of SQL Server. By default, Extensible Key Management is off.

Enabling EKM Provider option

To enable this feature, use the sp_configure command that has the following option and value, as in the following example:

To enable the Extensible Key Management option:

1. Open the SQL Server Management Studio.
2. Connect to the SQL Server.
3. Open a query window, and then run the following command:

   \[sp_configure 'show advanced', 1
   \] GO
   \[RECONFIGURE
   \] GO
   \[sp_configure 'EKM provider enabled', 1
   \] GO
   \[RECONFIGURE
   \] GO

If you use the sp_configure command for this option on editions other than Enterprise, Developer or Evaluation editions, you will receive an error.

Registering Luna EKM Provider

To setup the Luna EKM provider, Luna EKM Software must be installed and needs to be registered with the SQL Server 2008. Follow the below steps to create\register the provider:

To create\register the Luna EKM Provider:

1. Open the SQL Server Management Studio.
2. Connect to the SQL Server.
3. Open a query window, and then run the following command:

   \[CREATE CRYPTOGRAPHIC PROVIDER <Name of Cryptographic Provider>
   FROM FILE = '<Location of Luna EKM Provider Library>'\]

where CRYPTOGRAPHIC PROVIDER can be any user defined unique name.

Setting up Credential for Luna EKM Provider

The next step is to create a CREDENTIAL for the Luna EKM Provider. Then the CREDENTIAL must be mapped to SQL User or Login to be able to use the Luna EKM Provider. A CREDENTIAL is basically used to access any external SQL Server resource such as Luna SA HSM. Follow the below steps to create\map credential for the provider:

To create\map the CREDENTIAL for Luna EKM Provider:
1. Open a query window, and then run the following command:
    CREATE CREDENTIAL <Name of credential>
    WITH IDENTITY='<Name of EKM User>', SECRET='<HSM partition password>'
    FOR CRYPTOGRAPHIC PROVIDER LunaEKMProvider

    where CREDENTIAL and IDENTITY can be any user defined unique name.

2. To map the LunaEKMCred with SQL User or Login:
    ALTER LOGIN [Domain\ Login Name]
    ADD CREDENTIAL <Name of Credential created>

Enable Transparent Database Encryption using Asymmetric key on HSM

To enable Transparent Database Encryption using asymmetric key on HSM

1. Create an asymmetric key using Luna EKM Provider.
   Use master;
   CREATE ASYMMETRIC KEY SQL_EKM_RSA_2048_Key_TDE
   FROM Provider LunaEKMProvider
   WITH ALGORITHM = RSA_2048,
   PROVIDER_KEY_NAME = 'EKM_RSA_2048_Key_TDE',
   CREATION_DISPOSITION=CREATE_NEW

2. Create a credential for Luna EKM Provider.
   CREATE CREDENTIAL <Name of credential>
   WITH IDENTITY='<Name of EKM User>', SECRET='<HSM partition password>'
   FOR CRYPTOGRAPHIC PROVIDER LunaEKMProvider

3. Create a login based on the asymmetric key created above.
   CREATE LOGIN <Name of login>
   FROM ASYMMETRIC KEY SQL_EKM_RSA_2048_Key_TDE;

4. Map the credential created above to the login created above.
   ALTER LOGIN <Name of Login>
   ADD CREDENTIAL <Name of credential>;

5. Create a Database Encryption Key.
   Database encryption operations cannot be performed for 'master', 'model', 'tempdb', 'msdb', or 'resource' databases.

   We have chosen WSS_Content to enable TDE

   Use WSS_Content;
   CREATE DATABASE ENCRYPTION KEY
   WITH ALGORITHM = AES_128
   ENCRYPTION BY SERVER ASYMMETRIC KEY SQL_EKM_RSA_2048_Key_TDE;

6. Enable Transparent Database Encryption:
   ALTER DATABASE WSS_Content
   SET ENCRYPTION ON;
7. To query the status of database encryption and its percentage completion.

```sql
SELECT DB_NAME(e.database_id) AS DatabaseName,
       e.database_id,
       e.encryption_state,
       CASE e.encryption_state
           WHEN 0 THEN 'No database encryption key present, no encryption'
           WHEN 1 THEN 'Unencrypted'
           WHEN 2 THEN 'Encryption in progress'
           WHEN 3 THEN 'Encrypted'
           WHEN 4 THEN 'Key change in progress'
           WHEN 5 THEN 'Decryption in progress'
       END AS encryption_state_desc,
       c.name,
       e.percent_complete
FROM sys.dm_database_encryption_keys AS e
     LEFT JOIN master.sys.asymmetric_keys AS c
     ON e.encryptor_thumbprint = c.thumbprint
```

<table>
<thead>
<tr>
<th>DatabaseName</th>
<th>database_id</th>
<th>encryption_state</th>
<th>encryption_state_desc</th>
<th>name</th>
<th>percent_complete</th>
</tr>
</thead>
<tbody>
<tr>
<td>tempdb</td>
<td>2</td>
<td>3</td>
<td>Encrypted</td>
<td>NULL</td>
<td>0</td>
</tr>
<tr>
<td>WSS_Content</td>
<td>7</td>
<td>3</td>
<td>Encrypted</td>
<td>SQL_EKM_RSA_2048_Key_TDE</td>
<td>0</td>
</tr>
</tbody>
</table>
Configuring Active Directory Rights Management Services to Work with Office SharePoint Server 2007

After Office SharePoint Server 2007 has been installed, there are several tasks that must be completed to integrate Office SharePoint Server 2007 with AD RMS:

1. Add the Office SharePoint Server 2007 site to the Local Intranet Internet Explorer zone.
2. Add three user accounts, SHARERMS\Administrator, Nicholas, and Ben, to the SharePoint site.
3. Add the Office SharePoint Server 2007 server to the AD RMS server certification pipeline.
5. Restrict permissions by using AD RMS.

To add SPS-SRV to Local Intranet

1. Log on to Test-SPS-SRV as sharerms\administrator.
2. Click Start, point to Control Panel, and then click Internet Options.
3. Click the Security tab, click Local Intranet, and then click the Sites button.
4. Type http://Test-SPS-SRV, and then click Add.
5. Click Close, and then click OK.

To add Nicholas and Ben to the SharePoint site

1. Click Start, point to All Programs, and then click Internet Explorer.
2. Type http://Test-SPS-SRV in the address bar, and then click Go. This will open the default Office SharePoint Server 2007 site that was created during installation.
3. Click Site Actions, point to Site Settings, and then click People and Groups.
4. Click New, and then click Add Users.
5. Type nicholas@sharerms.com;ben@sharerms.com in the Users/Groups box, and then click OK. A list of users who have permission to use the SharePoint site is displayed.

Important

By default, the AD RMS cluster server certification pipeline ACL is configured to allow only the local System account. You must add the permissions in order for Office SharePoint Server 2007 to integrate with AD RMS.

To add Test-SPS-SRV to the AD RMS Certification Pipeline

1. Log on to Test-ADRMS-SRV as SHARERMS\administrator.
2. Click Start, and then click Computer.
3. Navigate to C:\inetpub\wwwroot\_wmcs\Certification.
4. Right-click ServerCertification.asmx, click Properties, and then click the Security tab.
5. Click Advanced, click Edit, select the Include inheritable permissions from this object’s parent check box, and then click OK two times.
6. Click Edit, and then click Add.
7. Click Object Types, select the Computers check box, and then click OK.
8. Type Test-SPS-SRV, and then click OK.
9. Click OK to close the ServerCertification.asmx Properties sheet.
   By default the Read & execute and the Read permissions are configured for the SPS-SRV computer account object and all other accounts inherited from the parent folder.
10. Click Start, and then click Command Prompt.
11. Type iisreset, and then press ENTER.

To enable Information Rights Management in Office SharePoint Server 2007

1. Log on to Test-SPS-SRV as SHARERMS\administrator.
2. Click Start, point to Administrative Tools, and then click SharePoint 3.0 Central Administration.
3. Click Operations, and then click Information Rights Management.
4. Select the Use the default RMS server specified in Active Directory option, and then click OK.
To restrict permissions using AD RMS
1. Log on as sharerms\Administrator.
2. Click Start, point to All Programs, and then click Internet Explorer.
3. Type http://Test-SPS-SRV in the address bar, and then click Go.
4. Click Document Center, click Documents, click Settings, and then click Document Library Settings.
5. Under the Permissions and Management heading, click Information Rights Management.
6. Select the Restrict permission to documents in this library on download check box.
7. Type SHARERMS Protected in the Permissions policy title box.
8. Type Restrict SHARERMS employees from printing in the Permission policy description box.
9. Click OK.

Note
Office SharePoint Server 2007 will automatically apply AD RMS rights to the document when it is downloaded from the Office SharePoint Server 2007 site. These rights are determined by the Office SharePoint Server 2007 group membership for that site. For example, a user who is in the Visitors Office SharePoint Server 2007 group will not be able to modify the document when it is downloaded from the Office SharePoint Server 2007 site.
Verifying AD RMS Functionality using ADRMS-CLNT

To verify the functionality of the AD RMS deployment, you log on as Nicole Holliday, create a new Microsoft Word 2007 document, and upload it to the Office SharePoint Server 2007 site into a rights-enabled document library configured such that users who download the document will not be able to print it. You then log on as Stuart Railson, download the document from the Office SharePoint Server 2007 site and verify that the ability to print the document has been restricted.

To add SPS-SRV to Local Intranet security zone
1. Log on to Test-ADRMS-CLNT as Nicholas (SHARERMS
icholas).
2. Click Start, click All Programs, and then click Internet Explorer.
3. Click Tools, and then click Internet Options.
4. Click the Security tab, click Local intranet, and then click Sites.
5. Click Advanced.
6. In the Add this website to the zone, type http://test-sps-srv, and then click Add.
7. Click close.
8. Repeat steps 1–7 for Ben (SHARERMS\ben).

Next, log on a Nicole Holliday and create a Microsoft Word 2007 document and upload it to the Office SharePoint Server 2007 site.

To create and upload a Microsoft Word document for testing
1. Click Start, point to All Programs, point to Microsoft Office, and then click Microsoft Office Word 2007.
2. Type This document is read-only. You cannot print it. in the new document, click the Microsoft Office Button, click Save As, and then save the file as ADRMS-TST.docx to a location on ADRMS-CLNT. This document will be uploaded to the Office SharePoint Server 2007 document library.
   Note
   Since Nicole Holliday is the author of this document, she will have full rights to the document, regardless of the AD RMS rights that are applied to it.
4. Click Start, point to All Programs, and then click Internet Explorer.
5. Type http://Test-SPS-SRV/ in the address bar, and then click Go.
6. Click Document Center, and then click Documents.
7. Click Upload, click Upload Document, click Browse to locate and select ADRMS-TST, and then click Open.
8. Click OK to upload the file, and then click Check In.
   By uploading the document into this library, the document receives the restrictions set on the library.
9. Log off as Nicole Holliday.

To open a protected document
1. Log on to Test-ADRMS-CLNT as Ben (SHARERMS\ben).
2. Click Start, click All Programs, and then click Internet Explorer.
3. Type http://Test-SPS-SRV/ in the address bar, and then click Go.
4. Click Document Center, and then click Documents.
5. Click ADRMS-TST, and then click OK to open the document as Read Only.
6. The following message will appear: “Permission to this document is currently restricted. Microsoft Office must connect to https://test-adrms-srv.sharerms.com/_wmcs/licensing to verify your credentials and download your permission.”
7. Click OK.
8. The following message will appear: “Verifying your credentials for opening content with restricted permissions”.
9. Click OK in the full screen reading view message, and then click Close to close the full screen reading view.
10. Click the Microsoft Office button. The Print command is disabled.

You have successfully deployed, integrated, and demonstrated the functionality of AD RMS and Office SharePoint Server 2007, using the simple scenario of uploading a Microsoft Office Word 2007 document to an
Office SharePoint Server 2007 site. You can also use this deployment to explore some of the additional capabilities of AD RMS through additional configuration and testing.
Enable SSL on Office SharePoint Server 2007 sites hosted on IIS 7.0 using Luna Key Storage Provider (KSP)

Before you enable

- Install Luna Key Storage Provider (KSP).

Install Luna Key Storage Provider

1. Luna KSP must be installed as a separate step following the completion of Luna SA client software.
2. After the KSP installation, traverse to C:\Program Files\SafeNet and run KspConfig.exe to register Luna KSP.

To enable SSL on “Sharepoint - 80” web application on IIS 7.0:

Create a certificate request using Luna KSP

IIS Manager does not support the creation of certificates protected by CNG Keys and these need to be created using the Microsoft command line utilities.

1. To generate a certificate request for a SSL certificate using an RSA 2048-bit key, create a file luna.inf with the following information:

   [Version]
   Signature= "$Windows NT$"
   [NewRequest]
   Subject = "C=IN,CN=noi1-501706"
   HashAlgorithm = SHA256
   KeyAlgorithm = RSA
   KeyLength = 2048
   ProviderName = "SafeNet Key Storage Provider"
   KeyUsage = 0xf0
   MachineKeySet = True
   [EnhancedKeyUsageExtension]
   OID=1.3.6.1.5.5.7.3.1

Your inf file does not have to contain exactly the code given in the following step. These are examples, not definitive models.
2. To create the certificate request for the Certification Authority, execute the command:
   `Certreq.exe -new luna.inf request.req`

**Installing the certificate**

After creating the certificate request, open the CA web interface and submit the request to the CA.

1. Open the browser and type `http://Test-DC/certsrv`.
2. Click on Request a certificate -> Advanced Certificate Request -> Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.
3. Paste the certificate request under Saved Request and click Submit.
4. Download the certificate and save the certificate.

**Complete the certificate request**

1. Open IIS Manager from Start -> Programs -> Administrative Tools -> Internet Information Services (IIS) Manager.
2. Select localhost on the left hand side of the IIS Manager window.
3. Double click Server Certificates.
4. Click on Complete Certificate Request.
5. Browse to the certificate obtained from the CA.
6. Specify some Friendly name and Click Ok.

![Complete Certificate Request](image)

**Specify Certificate Authority Response**

Complete a previously created certificate request by retrieving the file that contains the certificate authority’s response.

- **File name containing the certification authority’s response:**
  - `C:\Users\[username]\Computer\Desktop\certnew.cer`
- **Friendly name:**
  - `CertSPS`

[OK] [Cancel]
Bind the certificate to the web site

1. Under sites on the left hand side of the IIS Manager window, select the SharePoint - 80 web site.
2. On the right hand side of the IIS Manager, click on Bindings.

3. In the site Bindings, click Add.
4. Select the protocol https.
5. Select the certificate from the drop-down list.
6. Click OK to complete the certificate binding for SSL connection.

7. Open the browser and type https://Test-SPS-SRV.
END OF DOCUMENT