Active Directory Rights Management Service

Integration Guide
Preface

© 2013 SafeNet, Inc. All rights reserved.

Part Number: 007-011230-001 (Rev F, 07/2013)

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

**Chapter 1 Introduction** ................................................................................................................................................. 1  
  Scope ............................................................................................................................................................................... 1  
  Prerequisites .................................................................................................................................................................. 2  

**Chapter 2 Integrate Microsoft AD RMS with Luna SA (Windows Server 2008 R2)** .......................... 3  
  Before You Begin ......................................................................................................................................................... 3  
  Setup ............................................................................................................................................................................ 3  
  Configure user accounts and groups .............................................................................................................................. 3  
  Configure AD RMS client computer (ADRMS-CLNT) ................................................................................................. 4  
  To install Microsoft Office Word 2007/2010 Enterprise ........................................................................................... 4  
  Install Luna Cryptographic Service Provider (CSP) on Windows Server 2008 R2 ................................................. 4  
  Install AD RMS with Luna Cryptographic Service Provider (CSP) on Windows Server 2008 R2 ...................... 5  

**Chapter 3 Integrate Microsoft AD RMS with Luna SA (Windows Server 2012)** .......................... 21  
  Before You Begin ......................................................................................................................................................... 21  
  Setup ............................................................................................................................................................................ 21  
  Configure user accounts and groups ............................................................................................................................ 21  
  Configure AD RMS client computer (ADRMS-CLNT) ................................................................................................. 22  
  To install Microsoft Office Word 2007 Enterprise ................................................................................................. 22  
  Install Luna Cryptographic Service Provider (CSP) on Windows Server 2012 ................................................. 22  
  Install AD RMS with Luna Cryptographic Service Provider (CSP) on Windows Server 2012 .................. 23  

**Chapter 4 Verifying AD RMS Functionality using ADRMS CLIENT** .......................................................... 52  

**Chapter 5 Troubleshooting Tips** ................................................................................................................................. 55
Chapter 1
Introduction

This document outlines the steps to configure and integrate Active Directory Rights Management Services with Luna SA.

Active Directory Rights Management Services (AD RMS) is an information protection technology that works with AD RMS-enabled applications to help safeguard digital information from unauthorized use. Content owners can define who can open, modify, print, forward, or take other actions with the information. 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 2007/2010 Enterprise Edition 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.

Luna SA secures the AD RMS Cluster Key generated and used by the AD RMS. You can integrate the AD RMS with the Luna SA by using the MSCAPI interface. The benefits of using Luna SA with the AD RMS are:

- Secure storage of the AD RMS Cluster Key
- FIPS 140-2 level 3 validated hardware
- Full life cycle management of the keys
- Failover support
- Load-balancing.

Scope

3rd Party Application Details

- Microsoft Active Directory Right Management Services

Supported Platforms

- Windows Server 2008 R2 Enterprise Edition

The following Luna version have been tested at Windows Server 2008 R2

1. Luna SA v4.4.3
2. Luna SA v5.0
3. Luna SA v5.1

- Windows Server 2012 Standard Edition

The following Luna version have been tested at Windows Server 2012 Standard Edition

1. Luna SA v5.2.1

HSMs and Firmware Version

- K5 HSM f/w 4.8.1
- K6 HSM f/w 6.0.8
- K6 HSM f/w 6.2.1
- K6 HSM f/w 6.10.1
Distributions

- Luna SA 1U Appliance s/w v4.4.3
- Luna SA 1U Appliance s/w v5.0
- Luna SA 1U Appliance s/w v5.1
- Luna SA 1U Appliance s/w v5.2
- Luna SA Client s/w v4.4.1
- Luna SA Client s/w v5.0
- Luna SA Client s/w v5.1
- Luna Client s/w v5.2.1

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 by CSP to register the client with the partition.
- Created and exchanged certificates between the Luna SA and the "Client" system.
- Registered the Client with the Partition and Run the command, vtl verify to display a partition from Luna SA. The general form of command is C:\Program Files\LunaSA>vtl verify.
- 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
Integrate Microsoft AD RMS with Luna SA (Windows Server 2008 R2)

This chapter outlines the steps to install and integrate Active Directory Rights Management Services with Luna SA.

Before You Begin

• You should familiarize yourself with Microsoft Active Directory Rights Management Services and the setup process for the AD RMS. Refer to the appropriate help files for more information and pre-installation requirements.

Setup

• The setup consists of the following 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 R2 Enterprise</td>
<td>Active Directory, Domain Name System (DNS).</td>
<td>Domain Controller</td>
<td>ADRMS-DC</td>
</tr>
<tr>
<td>Windows Server® 2008 R2 Enterprise</td>
<td>AD RMS, Internet Information Services (IIS) 7.0, and Message Queuing</td>
<td>AD RMS Server</td>
<td>ADRMS-SRV</td>
</tr>
<tr>
<td>Windows Vista®</td>
<td>Microsoft Office Word 2007 Enterprise Edition or</td>
<td>AD RMS Client</td>
<td>ADRMS-CLNT</td>
</tr>
<tr>
<td></td>
<td>Microsoft Office Word 2010 Enterprise Edition</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Configure the domain controller on ADRMS-DC
- Configure the AD RMS root cluster computer on ADRMS-SRV
- Configure the AD RMS client computer on ADRMS-CLNT

Configure user accounts and groups

In this section you create the user accounts and groups in the LUNARMS domain.

First, add the user accounts shown in the following table to Active Directory or AD DS. Use the procedure following the table to create the user accounts.

<table>
<thead>
<tr>
<th>Account Name</th>
<th>User Logon Name</th>
<th>E-mail address</th>
<th>Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADRMSADMIN</td>
<td>ADRMSADMIN</td>
<td><a href="mailto:nhollida@lunarms.com">nhollida@lunarms.com</a></td>
<td>Enterprise Admins</td>
</tr>
<tr>
<td>ADRMOSSRVC</td>
<td>ADRMOSSRVC</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nicole Holliday</td>
<td>NHOLLIDA</td>
<td></td>
<td>Employees, Finance</td>
</tr>
<tr>
<td>Limor Henig</td>
<td>LHENIG</td>
<td><a href="mailto:lhenig@lunarms.com">lhenig@lunarms.com</a></td>
<td>Employees, Marketing</td>
</tr>
<tr>
<td>Stuart Railson</td>
<td>SRAILSON</td>
<td><a href="mailto:srailson@lunarms.com">srailson@lunarms.com</a></td>
<td>Employees, Engineering</td>
</tr>
</tbody>
</table>

Once the user accounts have been created, Active Directory Universal groups should be created and these users added to them. The following table lists the Universal groups that should be added to Active Directory. Use the procedure following the table to create the Universal groups.
Finally, create a shared folder on ADRMS-SRV so that other users can find documents saved to the network. To create a shared network folder that can be modified by CP&L employees:

1. Click **Start**, click **My Computer**, and then double-click **Local Disk (C:)**.
2. Click **File**, point to **New**, and then click **Folder**.
3. Type **Public** for the new folder, and then press ENTER.
4. Right-click **Public** and then click **Sharing and Security**.
5. On the **Sharing** tab click the **Share this folder** option, and ensure that **Public** is in the **Share name** box.
6. Click **Permissions**.
7. In the **Group or user name** box click **Everyone**.
8. Select the **Full Control** check box in the **Allow** column of the Permissions for **Everyone** box.
9. Click **OK**.
10. Click the **Security** tab, and then click **Users (ADRMS-SRV\Users)** in the **Group or user name** box.
11. In the **Permissions for Users** box select the **Full Control** check box in the **Allow** column.
12. Click **OK**.

**Configure AD RMS client computer (ADRMS-CLNT)**

To configure ADRMS-CLNT, you must install Windows Vista, configure TCP/IP properties, and then join ADRMS-CLNT to the domain lunarms.com. You must also install an AD RMS-enabled application. In this example, Microsoft Office Word 2007 Enterprise Edition is installed on ADRMS-CLNT.

**To install Microsoft Office Word 2007/2010 Enterprise**

1. Log on to ADRMS-CLNT with the LUNARMS\Administrator account or another user account in the local Administrators group.
3. Click **Customize** as the installation type, set the installation type to **Not Available** for all applications except Microsoft Office Word 2007 Enterprise, and then click **Install Now**. This might take several minutes to complete.

**Install Luna Cryptographic Service Provider (CSP) on Windows Server 2008 R2**

For **Luna SA v4.4.1**:  
- Run the command, **register.exe** to register Luna CSP. The general form of command is  
  
  ```cmd
  C:\Program Files\LunaSA\CSP>Register.exe
  ```

  Follow the instruction to register the Luna SA partition and provide the partition password when it prompts for password.

For **Luna SA v5.0**:  
- Run the command, **registerCSP64.exe** to register Luna CSP. The general form of command is
C:\Program Files\LunaSA\CSP>RegisterCSP64.exe

- To list the Luna Cryptographic Services for Microsoft Windows. The general form of command is
  
  C:\Program Files\LunaSA\CSP>RegisterCSP64.exe /l

For Luna SA v5.1:

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

- To list the Luna Cryptographic Services for Microsoft Windows. The general form of command is
  
  C:\Program Files\LunaSA\CSP>Register.exe /l

Install AD RMS with Luna Cryptographic Service Provider (CSP) on Windows Server 2008 R2

To install the Microsoft Active Directory Rights Management Services:

1. Login to ADRMS-SRV as lunarms\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.**

![Add Roles Wizard](image)

7. Click **Add Required Role Services.**

![Add Roles Wizard](image)

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.

![Select Role Services](image)

11. Click **Next** to continue.
12. Select **Create a new AD RMS cluster**.

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 unencrypted connection (http://)** for the connection type for the AD RMS cluster. Give the FQDN then click **Validate**.

26. Click **Next** to continue.
27. Enter a name for the server licensor certificate.

28. Click **Next** to continue.

29. 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.
30. Click **Next** on the Web Server (IIS).

31. Click **Next** on the Select Role Services.
32. Click **Install** on the Confirm Installation Sections.

33. 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.
34. After restarting the system, open the Active Directory Rights Management Services console.

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

   **Trust Policies -> Trusted Publishing Domains**
## Trusted Publishing Domains

Trusted publishing domains are domains in which documents are published by an RMS cluster. These domains can contain content that is published, but they cannot be trusted publishing domains if another cluster is to publish the content to them. To configure trusted publishing domains for your cluster, you can use the Trusted Publishing Domains dialog box. This dialog box allows you to manage the trusted publishing domains for your cluster and to import and export trusted publishing domains between clusters.

### Trusted Publishing Domain Information

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Content</th>
<th>Key Container</th>
</tr>
</thead>
<tbody>
<tr>
<td>RMS</td>
<td>External</td>
<td>None</td>
<td>SANS Enterprises</td>
</tr>
</tbody>
</table>
Security Policies → Cluster Key Password

![Security Policies -> Cluster Key Password Diagram](image-url)
Chapter 3
Integrate Microsoft AD RMS with Luna SA (Windows Server 2012)

This chapter outlines the steps to install and integrate Active Directory Rights Management Services with Luna SA.

Before You Begin
- You should familiarize yourself with Microsoft Active Directory Rights Management Services and the setup process for the AD RMS. Refer to the appropriate help files for more information and pre-installation requirements.

Setup
- The setup consists of the following 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 2012</td>
<td>Active Directory, Domain Name System (DNS).</td>
<td>Domain Controller</td>
<td>ADRMS-DC</td>
</tr>
<tr>
<td>Standard</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows Server 2012</td>
<td>AD RMS, Internet Information Services (IIS), and Message Queuing</td>
<td>AD RMS Server</td>
<td>ADRMS-SRV</td>
</tr>
<tr>
<td>Standard</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Standard</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Configure the domain controller on ADRMS-DC
- Configure the AD RMS root cluster computer on ADRMS-SRV
- Configure the AD RMS client computer on ADRMS-CLNT

Configure user accounts and groups

In this section you create the user accounts and groups in the HSMServer domain.

First, add the user accounts shown in the following table to Active Directory or AD DS. Use the procedure following the table to create the user accounts.

<table>
<thead>
<tr>
<th>Account Name</th>
<th>User Logon Name</th>
<th>E-mail address</th>
<th>Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADRMSADMIN</td>
<td>ADRMSADMIN</td>
<td></td>
<td>Enterprise Admins</td>
</tr>
<tr>
<td>ADRMSSRVC</td>
<td>ADRMSSRVC</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nicole Holliday</td>
<td>NHOLLIDA</td>
<td><a href="mailto:nhollida@hsmserver.com">nhollida@hsmserver.com</a></td>
<td>Employees, Finance</td>
</tr>
<tr>
<td>Limor Henig</td>
<td>LHENIG</td>
<td><a href="mailto:lhenig@hsmserver.com">lhenig@hsmserver.com</a></td>
<td>Employees, Marketing</td>
</tr>
<tr>
<td>Stuart Railson</td>
<td>SRAILSON</td>
<td><a href="mailto:sraillon@hsmserver.com">sraillon@hsmserver.com</a></td>
<td>Employees, Engineering</td>
</tr>
</tbody>
</table>

Once the user accounts have been created, Active Directory Universal groups should be created and these users added to them. The following table lists the Universal groups that should be added to Active Directory. Use the procedure following the table to create the Universal groups.
Finally, create a shared folder on ADRMS-SRV so that other users can find documents saved to the network. To create a shared network folder that can be modified by CP&L employees:

1. Click **Start**, click **Computer**, and then double-click **Local Disk (C:)**.
2. Click **Home**, and then click **New Folder**.
3. Type **Public** for the new folder, and then press ENTER.
4. Click **Share** and then click **Specific people…**.
5. On the **File Sharing** window type **Everyone** and click **Add**.
6. In the **Permission Level** click **Everyone** and select **Read\Write**.
7. Click **Share** and verify that Public folder is displayed.
8. Click **Done**.

**Configure AD RMS client computer (ADRMS-CLNT)**

To configure ADRMS-CLNT, install Windows Server 2012, configure TCP/IP properties, and then join ADRMS-CLNT to the domain HSMServer.com. You must also install an AD RMS-enabled application. In this example, Microsoft Office Word 2007 Enterprise Edition is installed on ADRMS-CLNT.

**To install Microsoft Office Word 2007 Enterprise**

1. Log on to ADRMS-CLNT with the HSMSERVER\Administrator account or another user account in the local Administrators group.
2. Double-click **setup.exe** from the Microsoft Office 2007 Enterprise product disc.
3. Click **Customize** as the installation type, set the installation type to **Not Available** for all applications except Microsoft Office Word 2007 Enterprise, and then click **Install Now**. This might take several minutes to complete.

**Install Luna Cryptographic Service Provider (CSP) on Windows Server 2012**

**For Luna Client v5.2.1:**

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

  Follow the instruction to register the Luna SA partition and provide the partition password when it prompts for password.

- Run the command to list the CSP libraries. The general form of command is
  
  `C:\Program Files\SafeNet\LunaClient\CSP>Register.exe /library`
Install AD RMS with Luna Cryptographic Service Provider (CSP) on Windows Server 2012

To install the Microsoft Active Directory Rights Management Services:

1. Login to ADRMS-SRV as hsmserver\adrmsadmin.
2. Click Start, point to Administrative Tools, and then click Server Manager. The Server Manager snap-in appears.
3. Click Add Roles and Features in the Server Manager Dashboard.
4. Click Next on the Before You Begin page.

Before you begin

This wizard helps you install roles, role services, or features. You determine which roles, role services, or features to install based on the computing needs of your organization, such as sharing documents, or hosting a website.

To remove roles, role services, or features:
Start the Remove Roles and Features Wizard

Before you continue, verify that the following tasks have been completed:

- The Administrator account has a strong password
- Network settings, such as static IP addresses, are configured
- The most current security updates from Windows Update are installed

If you must verify that any of the preceding prerequisites have been completed, close the wizard, complete the steps, and then run the wizard again.

To continue, click Next.
5. Select **Role-based or feature-based installation** and then click **Next** on Installation Type page.

Select installation type

- **Role-based or feature-based installation**
  Configure a single server by adding roles, role services, and features.

- **Remote Desktop Services installation**
  Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.
6. Select the server from the server pool list and click **Next** on Server Selection page.
7. Select **Active Directory Rights Management Services** checkbox from **Roles** to install on this server.

8. You will receive a warning stating **Add features that are required for Active Directory Rights Management Services**. Click **Add Features**.
9. Click **Next** to continue on Server Roles page.
10. Click **Next** on the Active Directory Rights Management Services windows.
11. Select **Active Directory Rights Management Server** checkbox from the **Role Services** and click **Next** to continue.
12. Click **Next** to Web Server Roll (IIS) page.

![Add Roles and Features Wizard]

**Web Server Role (IIS)**

Before You Begin

Installation Type

Server Selection

Server Roles

Features

AD RMS

Role Services

Web Server Role (IIS)

Role Services

Confirmation

Results

Web servers are computers that let you share information over the Internet, or through intranets and extranets. The Web Server role includes Internet Information Services (IIS) 8.0 with enhanced security, diagnostic and administration, a unified Web platform that integrates IIS 6.0, ASP.NET, and Windows Communication Foundation.

Things to note:

* Using Windows System Resource Manager (WSRM) can help ensure equitable servicing of Web server traffic, especially when there are multiple roles on this computer.

* The default installation for the Web Server (IIS) role includes the installation of role services that enable you to serve static content, make minor customizations (such as default documents and HTTP errors), monitor and log server activity, and configure static content compression.
13. Use default selection and Click **Next** to continue on Role Services page.
14. Select **Restart the destination server automatically if required.**

15. A warning message about restarting the server will display, click **Yes.**
16. Click **Install** on the Confirmation page.
17. When installation completed, either Close the wizard or click on Perform additional configuration. You can open the configuration wizard later by clicking the Notification Flag.
18. When the AD RMS Configuration wizard opens, click **Next** to continue.
19. Select **Create a new AD RMS root cluster** and click Next on AD RMS Cluster page.
20. Select **Use Windows Internal Database on this server** and click **Next** to continue.
21. Click on **Specify**... to specify service account.

![Image of Service Account configuration]

**Service Account**

**Specify Service Account**

The AD RMS cluster requires a domain user account so that it can communicate with other services and network computers. Specify a standard domain user account with no additional permissions.

**Domain User Account**

More about the AD RMS service account
22. A window will open to add service account user, type the ADRMSSRVC and password and click **OK**. **Note**: ADRMSSRVC is the user that we have created in Active Directory, see Configure User Account and Group section above.
23. Click **Next** to continue on Service Account page.

**Service Account**

AD RMS
AD RMS Cluster
Configuration Database
**Service Account**
Cryptographic Mode
Cluster Key Storage
Cluster Key Password
Cluster Web Site
Cluster Address
Server Certificate
Licensor Certificate
SCP Registration
Confirmation
Progress
Results

**Specify Service Account**

The AD RMS cluster requires a domain user account so that it can communicate with other services and network computers. Specify a standard domain user account with no additional permissions.

**Domain User Account:**

HSMSERVER:ADRMSRVC

More about the AD RMS service account
24. Select Cryptographic Mode to generate the keys and click **Next** to continue.  
**Note**: you can select any mode here but select the Luna CSP from CSP list later.
25. Select **Use CSP key storage** and click **Next** to continue.
26. Select **Luna enhanced RSA and AES provider for Microsoft Windows** from CSP list and select **Create a new key with the selected CSP** then click **Next** to continue.
27. Click **Next** to continue on Cluster Web Site page, make sure that Default Web Site is listed.
28. Select **Use an unencrypted connection (http://)** and type the fully qualified domain name then click **Next** to continue.
29. Make sure that server name ADRMS-SRV is listed and click **Next** to continue.
30. Select Register the SCP now and click **Next** on SCP Registration page.
31. Click **Install** on the Confirmation page.
32. Click **Close** after successfully installation of the AD RMS Services.
33. After restarting the system, open the Active Directory Rights Management Services console by clicking Server Manager -> Tools -> Active Directory Rights Management Services.

34. Expand the Active Directory Rights Management Services tree and you will see the **Luna enhanced RSA and AES provider for Microsoft Windows** under:

   **Trust Policies** -> **Trusted Publishing Domains**

**Note:** Luna CSP that you have selected at configuring the AD RMS will show here.
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 data loss or disk failure, you can set a password that protects the AD RMS cluster key. If you used the centrally managed AD RMS encryption method in the cluster, the trusted publishing domain to be imported to protect the AD RMS cluster key, you can set the cluster key password.

Key protection method: CSP-based key
Cryptography provider: Enhanced RSA and AES provider for Microsoft Windows
Key container name: [RMS\Mode2 RMS-GUIDBFA02c-eaaf-165b-9896-00e452d405394427]

- Change cluster key password
Chapter 4
Verifying AD RMS Functionality using ADRMS CLIENT

To verify the functionality of the AD RMS deployment, you will log on as Nicole Holliday and then restrict permissions on a Microsoft Word document so that members of the CP&L Engineering group are able to read the document but unable to change, print, or copy. You will then log on as Stuart Railson, verifying that the proper permission to read the document has been granted, and nothing else. Then, you will log on as Limor Henig. Since Limor is not a member of the Engineering group, he should not be able to consume the rights-protected file.

Before you can consume rights-protected content, you must add the AD RMS cluster URL to the Local Intranet security zone.

Add the AD RMS cluster URL to the Local Intranet security zone for all users who will be consuming rights-protected content.

To add AD RMS cluster to Local Intranet security zone

1. Log on to ADRMS-CLNT as Nicole Holliday.
2. Click Start, 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. In the Add this website to the zone, type http://<fully qualified domain name of the server>, for example http://ADRMS-SRV.lunarms.com and then click Add.
6. Click Close and then OK.
7. Repeat steps 1–6 for Stuart Railson and Limor Henig.

Next, log on a Nicole Holliday and create a Microsoft Word 2007/2010 document and save it to the \ADRMS-SRV\Public folder.

To restrict permissions on a Microsoft Word document

1. Log on to ADRMS-CLNT as Nicole Holliday.
3. Type CP&L engineering employees can read this document, but they cannot change, print, or copy it on the blank document page after opening it.
4. Click the Microsoft Office Button, click Prepare, click Restrict Permission, and then click Restricted Access.
5. Click the Restrict permission to this document check box.
6. In the Read box, type email of the group for which you want to grant the permission, for example engineering@lunarms.com and then click OK to close the Permission dialog box.
7. Click the Microsoft Office Button, click Save As, and then save the file as \ADRMS-SRV\Public\ADRMS-TST.docx.
8. Log off as Nicole Holliday.
Next, log on as Stuart Railson and open the document, ADRMS-TST.docx.

To view a rights-protected document

1. Log on to ADRMS-CLNT as Stuart Railson.
2. Click Start, and then click Computer.
3. Click in the Address bar, type \ADRMS-SRV\Public\ADRMS-TST.docx, and then press Enter.

   The following message appears: “Permission to this document is currently restricted. Microsoft Office must connect to http://adrms-srv.lunarms.com/_wmcs/licensing to verify your credentials and download your permission.”
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.
7. Log off as Stuart Railson.

Finally, log on as Limor Henig and verify that he is not able to consume the rights-protected file.

To attempt to view a rights-protected document

1. Log on to ADRMS-CLNT as Limor Henig.
2. Click Start, and then click Computer.
3. Click in the Address bar, type \ADRMS-SRV\Public\ADRMS-TST.docx, and then press Enter.

   The following message appears: “Permission to this document is currently restricted. Microsoft Office must connect to http://adrms-srv.lunarms.com/_wmcs/licensing to verify your credentials and download your permission.”
4. Click OK.
5. The following message appears: “You do not have credentials that allow you to open this document. You can request updated permission from nhollida@lunarms.com. Do you want to request updated permission?”
6. Click No, and then close Microsoft Word.

You have successfully deployed and demonstrated the functionality of AD RMS, using the simple scenario of applying restricted permissions to a Microsoft Word 2007/2010 document. You can also use this deployment to explore some of the additional capabilities of AD RMS through additional configuration and testing.
**Trusted Publishing Domains (TPD)**

By default, an AD RMS Licensing Server can issue use licenses for only content where it originally issued the publishing license. It some situations, this may not be acceptable.

In order to specify a cluster that is allowed to issue use licenses for content protected by a different cluster, the first cluster must be defined as a trusted publishing domain. If content was published by another certification cluster either in your organization, for example, a subsidiary organization in another forest, or in a separate organization, your AD RMS cluster can grant use licenses to users for this content by configuring a Trusted Publishing Domain on your AD RMS cluster.

By adding a Trusted Publishing Domain, you set up a trust relationship between your AD RMS cluster and the other certification cluster by importing the Trusted Publishing Certificate of the other cluster.

Luna SA supports TPD with multiple forests. To enable Trust model TPD needs to be exported in the cluster where you protected the content and imported in the one where you are trying to consume it.

Luna SA is tested with two-way TPD between the two forests.
Chapter 5
Troubleshooting Tips

**Problem:** Error message "Password could not be contacted" when trying to register Service Account while installing AD RMS on the **Domain Controller**.

1. Make sure that the user must have the member of Domain Administrator groups or Enterprise Administrator group whose credentials you are supplying.
2. User Account user should be other than that user which is installing AD RMS.