Active Directory Rights Management Services

Integration Guide



All information herein is either public information or is the property of and owned solely by Gemalto and/or its subsidiaries who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/or industrial property rights of or concerning any of Gemalto's information.

This document can be used for informational, non-commercial, internal and personal use only provided that:

- The copyright notice below, the confidentiality and proprietary legend and this full warning notice appear in all copies.
- This document shall not be posted on any publicly accessible network computer or broadcast in any media and no modification of any part of this document shall be made.

Use for any other purpose is expressly prohibited and may result in severe civil and criminal liabilities.

The information contained in this document is provided "AS IS" without any warranty of any kind. Unless otherwise expressly agreed in writing, Gemalto makes no warranty as to the value or accuracy of information contained herein.

The document could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Furthermore, Gemalto reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

Gemalto hereby disclaims all warranties and conditions with regard to the information contained herein, including all implied warranties of merchantability, fitness for a particular purpose, title and non-infringement. In no event shall Gemalto be liable, whether in contract, tort or otherwise, for any indirect, special or consequential damages or any damages whatsoever including but not limited to damages resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.

Gemalto does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms' resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Gemalto be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Gemalto products. Gemalto disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service or loss of privacy.

© 2016 Gemalto. All rights reserved. Gemalto and the Gemalto logo are trademarks and service marks of Gemalto and/or its subsidiaries and are registered in certain countries. All other trademarks and service marks, whether registered or not in specific countries, are the property of their respective owners.

Document Part Number: 007-011230-001, Rev. J Release Date: August 2016

Contents

Pr	eface	. 4
	Scope	4
	Document Conventions	4
	Command Syntax and Typeface Conventions	5
	Support Contacts	6
1	Introduction	. 7
	Overview	7
	Scope	7
	3rd Party Application Details	7
	Supported Platforms	8
	Prerequisites	8
	SafeNet Network HSM Setup	8
2	Integrating Microsoft AD RMS with SafeNet Luna HSM (Windows Server 2008 R2)	. 9
	Before You Begin	9
	Set up	9
	Configure AD RMS client computer (ADRMS-CLNT)	.11
	Install Luna Cryptographic Service Provider (CSP) on ADRMS-SRV	.11
	Install AD RMS with Luna Cryptographic Service Provider (CSP) on Windows Server 2008 R2	.12
3	Integrating Microsoft AD RMS with SafeNet Luna HSM (Windows Server 2012/R2)	24
	Before You Begin	.24
	Setup	.24
	Configure AD RMS client computer (ADRMS-CLNT)	.25
	Install Luna Cryptographic Service Provider (CSP) on Windows Server 2012/R2	.26
	Install AD RMS with Luna Cryptographic Service Provider (CSP) on Windows Server 2012	.26
4	Verifying AD RMS Functionality using AD RMS CLIENT	43
	Trusted Publishing Domains (TPD)	.45
5	Troubleshooting Tips	46

Preface

This guide provides instructions for setting up a small test lab with Microsoft AD RMS running with SafeNet Luna HSM for securing the rights management keys.

Scope

This document describes how to install and configure Microsoft AD RMS with SafeNet Luna HSM. Refer to the SafeNet Luna HSM documentation for general SafeNet Luna HSM setup procedures.

Document Conventions

This section provides information on the conventions used in this template.

Notes

Notes are used to alert you to important or helpful information. These elements use the following format:



NOTE: Take note. Contains important or helpful information.

Cautions

Cautions are used to alert you to important information that may help prevent unexpected results or data loss. These elements use the following format:



CAUTION: Exercise caution. Caution alerts contain important information that may help prevent unexpected results or data loss.

Warnings

Warnings are used to alert you to the potential for catastrophic data loss or personal injury. These elements use the following format:



WARNING: Be extremely careful and obey all safety and security measures. In this situation you might do something that could result in catastrophic data loss or personal injury.

Convention	Description
bold	The bold attribute is used to indicate the following:
	Command-line commands and options (Type dir /p .)
	Button names (Click Save As.)
	Check box and radio button names (Select the Print Duplex check box.)
	Window titles (On the Protect Document window, click Yes.)
	Field names (User Name: Enter the name of the user.)
	Menu names (On the File menu, click Save.) (Click Menu > Go To > Folders.)
	User input (In the Date box, type April 1 .)
italic	The italic attribute is used for emphasis or to indicate a related document. (See the <i>Installation Guide</i> for more information.)
Consolas	Denotes syntax, prompts, and code examples.

Command Syntax and Typeface Conventions

Support Contacts

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, contact your supplier or Gemalto Customer Support. Gemalto Customer 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 Gemalto and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Contact Method	Contact Information	
Address	Gemalto 4690 Millennium Drive Belcamp, Maryland 21017, USA	
Phone	US International	1-800-545-6608 1-410-931-7520
Technical Support https://serviceportal.safenet-inc.com Customer Portal Existing customers with a Technical Support Customer Port manage incidents, get the latest software upgrades, and access		net-inc.com a Technical Support Customer Portal account can log in to e latest software upgrades, and access the Gemalto Knowledge

1 Introduction

Overview

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

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 (SafeNet Luna HSM) is 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 uses Microsoft Active Directory Rights Management Services to implement document security utilizing Luna Cryptographic Service Provider (CSP) to store the AD RMS cluster keys on SafeNet Luna HSM.

SafeNet Luna HSM 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 SafeNet Luna HSM 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 Rights Management Services

Supported Platforms

Active Directory Rights Management Services Integration with SafeNet Luna HSM has been tested with the following:

Platforms Tested	Luna Client Software Version	SafeNet Luna HSM Appliance Software Version	Appliance Firmware Version
Widows Server 2012 R2 Standard	6.2.1	6.2.1	6.10.9
Widows Server 2012 R2 Standard	6.2.0	6.2.0	6.10.9
Widows Server 2012 Standard	5.3.0 5.2.1	Luna SA v5.3.0 Luna SA v5.2.1	6.20.0 6.10.1
Windows Server 2008 R2	5.1 5.0 4.4.3	Luna SA v5.1.0 Luna SA v5.0.0 Luna SA v4.4.3	6.2.1 6.0.8 4.8.1

Prerequisites

SafeNet Network HSM Setup

Refer to the SafeNet Network HSM documentation for installation steps and details regarding configuring and setting up the box on Windows systems. Before you get started, ensure the following:

- 1. SafeNet Network HSM appliance and a secure admin password
- 2. SafeNet Network HSM, and a hostname, suitable for your network
- 3. SafeNet Network HSM network parameters are set to work with your network
- 4. Initialize SafeNet Network HSM.
- 5. Create and exchange certificates between SafeNet Network HSM and Client system.
- 6. Create a partition on SafeNet Network HSM. Remember the partition password that will be later used by Microsoft ADRMS.
- 7. Register the client with the partition. Run the "vtl verify" command on the client system to display a registered partition. The general form of command for Windows is

C:\Program Files\SafeNet\LunaClient>vtl verify.

8. 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).

2 Integrating Microsoft AD RMS with SafeNet Luna HSM (Windows Server 2008 R2)

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

Before You Begin

It is recommended that 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 provided by Microsoft for more information and pre-installation requirements.

Set up

Requirements to setup the ADRMS is given below.

1. The setup comprises the following systems in a private network as per the table below:

Operating System	Applications and Services	Description	Computer Name
Windows Server 2008 R2 Enterprise	Active Directory, Domain Name System (DNS)	Domain Controller	ADRMS-DC
Windows Server® 2008 R2 Enterprise	AD RMS, Internet Information Services (IIS) 7.0, and Message Queuing	AD RMS Server	ADRMS-SRV
Windows Vista®	Microsoft Office Word 2007 Enterprise Edition or Microsoft Office Word 2010 Enterprise Edition	AD RMS Client	ADRMS-CLNT

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

Configure user accounts and groups

Create following 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.

Account Name	User Logon Name	E-mail Address	Group
ADRMSADMIN	ADRMSADMIN	-	Enterprise Admins
ADRMSSRVC	ADRMSSRVC	-	
Nicole Holliday	NHOLLIDA	nhollida@lunarms.com	Employees, Finance
Limor Henig	LHENIG	lhenig@lunarms.com	Employees, Marketing
Stuart Railson	SRAILSON	srailson@lunarms.com	Employees, Engineering

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.

Group Name	E-mail address
Finance	finance@lunarms.com
Marketing	marketing@lunarms.com
Engineering	engineering@lunarms.com
Employees	employees@lunarms.com

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, install Windows Vista operating system, configure TCP/IP properties, and then join ADRMS-CLNT to the domain **lunarms.com**. AD RMS-enabled application also needs to be installed. In this example, Microsoft Office Word 2007/2010 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.
- 2. Double-click setup.exe from the Microsoft Office 2007/2010 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 ADRMS-SRV

For Luna Client 4.4.1 & 5.1:

• Run the command, register.exe to register Luna CSP. The general form of command is

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.

• To list the Luna Cryptographic Services for Microsoft Windows. The general form of command is C:\Program Files\LunaSA\CSP>Register.exe /1

For Luna Client 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 /1

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 displays.
- 3. Select **Roles** in the console tree.

SRV) Server Manager (ADRMS-SRV)		
Get an overview of the status of this server	, perform top management tasks, and add or remove server roles and features.	
Server Summary		Server Summary Help
Computer Information		Change System Properties
Full Computer Name:	ADRMS-SRV.lunarms.com	Rev Network Connections
Domain:	kinarms.com	Su Configure Remote Desktop
Local Area Connection:	172.25.13.63, IPv6 enabled	Management
Remote Desktop:	Enabled	
Server Manager Remote Management:	Dicabled	
Product ID:	55041-507-0210031-04200 (Activated)	
P Do not show me this console at logon		
Security Information		Go to Windows Firewall
Windows Firewall:	Domain: On	Configure Updates
Windows Updates:	Not configured	Run Security Configuration Wiza
Last checked for updates:	Never	Toofigure IE ESC
Last installed updates:	Never	
IE Enhanced Security Configuration (ESC):	On for Administrators On for Users	
Roles Summary		Roles Summary Help
Roles: 4 of 17 installed		Go to Roles
Active Directory Certificate Services		Add Roles
Active Directory Domain Services		Be Remove Roles
DNS Server DNS Server		
Features Summary		🔽 Features Summary Help
Features: 5 of 42 installed		Add Features
Group Policy Management		Remove Features

4. Right-click **Roles** and then click, **Add roles**. The **Add Roles** wizard displays.

Add Roles Wizard	×
Before You Begin	
Before You Begin Server Roles Confirmation Progress Results	This wizard helps you install roles on this server. You determine which roles to install based on the tasks you want this server to perform, such as sharing documents or hosting a Web site. Before you continue, verify that: • The Administrator account has a strong password • Network settings, such as static IP addresses, are configured • The latest security updates from Windows Update are installed If you have to complete any of the preceding steps, cancel the wizard, complete the steps, and then run the wizard again. To continue, click Next. Is gkip this page by default Previous Next > Install Cancel

- 5. Click Next.
- 6. Select the Active Directory Rights Management Services check box from Server Roles to install on this server. You receive a warning stating Add roles services and features required for Active Directory Rights Management Services.

Add Roles Wizard		×
Select Server Rol	es	
Before You Begin Server Roles AD RMS Role Services AD RMS Cluster Configuration Database Service Account Cluster Key Storage Cluster Key Password Cluster Web Site Cluster Web Site Cluster Address Server Authentication Certi, Licensor Certificate Name SCP Registration Web Server (IIS) Role Services Confirmation Progress	Select one or more roles to install on this server. Roles: Active Directory Certificate Services Active Directory Domain Services Active Directory Federation Services Active Directory Rights Management Services Application Server DHCP Server Fax Server File Services Network Policy and Access Services Terminal Services UDDI Services Veb Server (IIS) Windows Deployment Services 	Description: Active Directory Rights Management Services (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.
		t > Install Cancel

7. Click Add Required Role Services.

Add role services and features rea Management Services? You cannot install Active Directory Rights Managem are also installed.	quired for Active Directory Rights	98
Role Services:	Description:	
 Web Server (IIS) Web Server Management Tools Windows Process Activation Service Process Model .NET Environment Configuration APIs Message Queuing Message Queuing Services 	Web Server (IIS) provides a reliable, manageable, and scalable Web application infrastructure.	
	Add Required Role Services Cance	

- 8. Click **Next** to continue.
- 9. Click **Next** on the Active Directory Rights Management Services window.

Add Roles Wizard	×
Active Directory	Rights Management Services
Before You Begin Server Roles AD RMS Role Services AD RMS Cluster Configuration Database Service Account Cluster Key Storage Cluster Key Password Cluster Web Site Cluster Web Site Cluster Address Server Authentication Certi Licensor Certificate Name SCP Registration Web Server (IIS) Role Services Confirmation Progress Results	 Introduction to Active Directory Rights Management Services 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 within the organization and with other federated identities. Content owners can define who can open, modify, print, forward, or take other actions with the information. Organizations can create rights policy templates such as "Confidential – Read Only" that can be applied directly to financial reports, product specifications, customer data, and e-mail messages. Things to Note To deploy AD RMS, you must create an AD RMS root cluster for certification and licensing which can consist of one or more servers, depending on the capacity requirements of your environment. After deploying AD RMS, you cannot change the name of the domain to which this AD RMS server is joined. Changing the domain name will cause this AD RMS server to stop functioning. Additional Information AD RMS Overview AD RMS Overview AD RMS Overview AD RMS Pre-Deployment Checklist Scaling Your AD RMS Environment Securing Your AD RMS Deployment
	< Previous Next > Install Cancel

10. Select the Active Directory Rights Management Server check box from the Role Services.

Add Roles Wizard		×
Select Role Servi	ices	
Before You Begin Server Roles AD RMS Role Services AD RMS Cluster AD RMS Cluster Configuration Database Service Account Cluster Key Storage Cluster Key Password Cluster Web Site Cluster Web Site Cluster Web Site Cluster Address Server Authentication Certi Licensor Certificate Name SCP Registration Web Server (IIS) Role Services Confirmation Progress Results	Select the role services to install for Active Directory Rights M Role services: Active Directory Rights Management Server Identity Federation Support More about role services	Anagement Services: Description: 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.
	_< Previous	Next > Install Cancel

- 11. Click **Next** to continue.
- 12. Select the Create a new AD RMS cluster radio button.

dd Roles Wizard Create or Join ar	AD RMS Cluster
Before You Begin Server Roles AD RMS Role Services AD RMS Cluster Configuration Database Service Account Cluster Key Storage Cluster Key Password Cluster Web Site Cluster Address Server Authentication Certi Licensor Certificate Name SCP Registration Web Server (IIS) Role Services Confirmation Progress Results	 You can configure AD RMS using two types of AD RMS clusters: an AD RMS root cluster for certification and licensing, or an AD RMS licensing-only cluster. To deploy AD RMS, you must initially set up an AD RMS root cluster with one or more servers joined to the cluster. Choose this option if you want to create an AD RMS root cluster as part of a new AD RMS deployment, or if cluster. An existing AD RMS root cluster was not detected in this forest. This server will host the AD RMS root cluster. Join an existing AD RMS cluster. Choose this option if you want to add this server to an existing root or licensing-only cluster to increase capacity. You will be required to provide the name of the existing AD RMS configuration database and the name of the database server.
	< Previous Next > Install Cancel

14. Select the Use Windows Internal Database on this Server radio button.

Add Roles Wizard	×
Select Configurat	tion Database
Before You Begin Server Roles AD RM5 Role Services AD RMS Cluster	AD RMS clusters use a database to store configuration and policy information. The database can be hosted either by Windows Internal Database or another database server. Use Windows Internal Database on this server Using Windows Internal Database will limit this AD RMS cluster to a single-server cluster. If you intend to join more servers to this AD RMS cluster, do not use this option.
Configuration Database Service Account Cluster Key Storage Cluster Key Password Cluster Web Site Cluster Address Server Authentication Certi Licensor Certificate Name SCP Registration Web Server (IIS) Role Services Confirmation Progress	Usg a different database server Server: Database Instance: Validate
Results	More about AD RMS databases < Previous Next > Install Cancel

- 15. Click **Next** to continue.
- 16. Specify the **Domain User Account**.

Windows Securit	у		×
Add Roles Wiz Please enter a u	ard ser name and password.		
	ADRMSSRVC •••••• Domain: LUNARMS		
		ОК	Iancel

17. Click **OK** to continue.

18. Click **Next** to continue.

Add Roles Wizard	×
Specify Service /	Account
Before You Begin Server Roles AD RMS Role Services AD RMS Cluster Configuration Database	A domain user account is required to provide a network identity for AD RMS so that it can communicate with other services on this computer and the network. The domain account should be a standard domain user account with no additional permissions. Although installing AD RMS on a domain controller is not recommended, if you are installing AD RMS on a domain controller, the domain account that you specify must be a member of the Domain Administrators group or of the Enterprise Administrators group. Specify the account under which the AD RMS cluster will run, using the format DomainName\UserName. The AD RMS service account will be a member of the AD RMS service group and will have the permissions defined for that group.
Service Account	Domain User Account:
Cluster Key Storage	LUNARMS\ADRMSSRVC Specify
Cluster Key Password	
Cluster Web Site	
Cluster Address	
Server Authentication Certi	
Licensor Certificate Name	
SCP Registration	
Web Server (IIS)	
Role Services	
Confirmation	
Progress	
Results	
	< Previous Next > Install Cancel

19. Select the Use CSP key storage radio button for AD RMS cluster key storage.

Add Roles Wizard	×
Configure AD RM	IS Cluster Key Storage
Before You Begin Server Roles AD RMS Role Services AD RMS Cluster Configuration Database Service Account	AD RMS clusters use an AD RMS cluster key to sign certificates and licenses issued by the cluster. This key is required for disaster recovery and by other AD RMS servers joining the cluster. Select how you want to store the AD RMS cluster key.
Cluster Key Storage Cluster Key Cluster Web Site Cluster Address Server Authentication Certi Licensor Certificate Name SCP Registration Web Server (IIS) Role Services Confirmation	 Uge CSP key storage This is an advanced option that requires you to select a cryptographic service provider (CSP) to store the AD RMS cluster key. You will need to distribute this key manually when new servers join this cluster.
Progress Results	More about cluster key storage and protection
	< Previous Next > Install Cancel

21. Choose Luna Cryptographic Services for Microsoft Windows from the CSP drop-down menu to store the AD RMS cluster key and select the Create a new key with the selected CSP radio button.

Add Roles Wizard	×
Specify AD RMS	Cluster Key
Before You Begin Server Roles AD RMS Role Services AD RMS Cluster Configuration Database Service Account Cluster Key Storage Cluster Key Cluster Web Site Cluster Address Server Authentication Certi Licensor Certificate Name SCP Registration Web Server (IIS) Role Services Confirmation Progress Results	A cryptographic service provider (CSP) is used to store the AD RMS cluster key. Select whether to create a new key or use an existing key with the selected CSP. Luna Cryptographic Services for Microsoft Windows Cpate a new key with the selected CSP This option is recommended if you are creating a new AD RMS cluster. Use an existing key with the selected CSP This option should be used to recover an AD RMS cluster only if the configuration database is unrecoverable and had content protected by the previous cluster key. keys: Image: Comparison of the configuration database is unrecoverable and had content protected by the previous cluster key. More about AD RMS cluster keys More about AD RMS cluster keys
	< Previous Next > Install Cancel

- 22. Click Next to continue.
- 23. Select **Default Web Site** for the virtual directory.

Add Roles Wizard	×
Select AD RMS C	uster Web Site
Before You Begin Server Roles AD RMS Role Services AD RMS Cluster Configuration Database Service Account Cluster Key Storage	AD RMS is hosted in an Internet Information Services (IIS) virtual directory, which is set up on one of the existing Web sites on this server. Select a Web site for the virtual directory: Default Web Site
Cluster Web Site Cluster Web Site Cluster Address Server Authentication Certi Licensor Certificate Name SCP Registration Web Server (IIS) Role Services Confirmation Progress Results	More about selecting the cluster Web site
	< Previous Next > Install Cancel

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

Add Roles Wizard	×
Specify Cluster A	ddress
Before You Begin Server Roles AD RMS Role Services AD RMS Cluster Configuration Database Service Account Cluster Key Storage Cluster Key Cluster Web Site	A cluster address enables AD RMS clients to communicate with this cluster over the network. It is recommended that you configure AD RMS to use the Secure Sockets Layer (SSL) protocol to encrypt network traffic between AD RMS clients and the cluster. Specify a connection type for this AD RMS cluster. © Use an SSL-encrypted connection (https://) ① The Web site you have selected does not have SSL enabled. After you click Next, you will be given the choice to select an SSL certificate for this Web site. © Use an unencrypted connection (http://) ① You cannot use this option if you want to add Identity Federation Support.
Cluster Address Licensor Certificate Name SCP Registration Web Server (IIS) Role Services Confirmation Progress Results	Specify an internal address for this AD RMS cluster. You cannot change this address or port number after AD RMS is installed and configured. Internal Address Eully-Qualified Domain Name: Pgrt: http:// ADRMS-SRV.lunarms.com Preview of cluster address for clients on the network: http://ADRMS-SRV.lunarms.com
	< Previous Next > Install Cancel

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

Add Roles Wizard	×
Name the Server	Licensor Certificate
Before You Begin Server Roles AD RMS Role Services AD RMS Cluster Configuration Database Service Account Cluster Key Storage Cluster Key Cluster Web Site Cluster Web Site Cluster Address <u>Licensor Certificate Name</u> SCP Registration Web Server (IIS) Role Services Confirmation Progress Results	AD RMS creates a server licensor certificate that establishes the identity of this AD RMS cluster to clients. Enter a name that can help you easily identify this certificate. Name: ADRMS-SRV
	< Previous Next > Install Cancel

29. Ensure that the **Register the AD RMS service connection point now** radio button is selected, and then click **Next** to register the AD RMS service connection point (SCP) in Active Directory during installation.

Add Roles Wizard	×
Register AD RM	1S Service Connection Point
Before You Begin Server Roles AD RMS Role Services AD RMS Cluster Configuration Database Service Account Cluster Key Storage Cluster Key Cluster Web Site Cluster Address Licensor Certificate Name SCP Registration Web Server (IIS) Role Services Confirmation Progress Results	 The AD RMS service connection point (SCP) is created in Active Directory Domain Services when an AD RMS cluster is created. The SCP provides clients with intranet URLs for the AD RMS cluster. To register the SCP, you must be a member of the Enterprise Admins group. If you are not a member of the Enterprise Admins group, select Register later. Register the AD RMS service connection point now Select this option if you are a member of Enterprise Admins group and you want to start using this AD RMS cluster as soon as the installation finishes. Register the AD RMS service connection point later Select this option if you are not a member of Enterprise Admins group. If you are not a member of Enterprise Admins group and you want to start using it available to clients or if you are not a member of Enterprise Admins group.
	< Previous Next > Install Cancel

30. Click Next on the Web Server (IIS) page.

Add Roles Wizard	×
Web Server (III	S)
Before You Begin Server Roles AD RMS Role Services AD RMS Cluster Configuration Database Service Account Cluster Key Cluster Key Cluster Key Cluster Web Site Cluster Address Licensor Certificate Name SCP Registration Web Server (IIS) Role Services Confirmation Progress Results	 Introduction to Web Server (IIS) Web servers are computers that have specific software that allows them to accept requests from client computers and return responses to those requests. Web servers let you share information over the Internet, or through intranets and extranets. The Web Server role includes Internet Information Services (IIS) 7.0, a unified Web platform that integrates IIS 7.0, ASP.NET, and Windows Communication Foundation. IIS 7.0 also features enhanced security, simplified diagnostics, and delegated administration. Ibigs to Note Ibigs Undows System Resource Manager (WSRM) can help ensure equitable servicing of Web server raffic 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. Additional Information Overview of Web Server (IIS) Overview of Available Role Services in IIS 7.0 Using Common Administrative Tasks in IIS Overview of WSRM
	< Previous Next > Install Cancel

31. Click **Next** on the Select Role Services page.

Add Roles Wizard		×
Select Role Servi	ces	
Before You Begin Server Roles AD RMS Role Services AD RMS Cluster Configuration Database Service Account Cluster Key Storage Cluster Key Cluster Web Site Cluster Web Site Cluster Address Licensor Certificate Name SCP Registration Web Server (IIS) Role Services Confirmation Progress Results	Select the role services to install for Web Server (IIS): Role services: Web Server Gommon HTTP Features Static Content Default Document Directory Browsing HTTP Redirection WebDAV Publishing Application Development ASP.NET NET Extensibility ASP CGI J ISAPI Extensions J ISAPI Extensions Server Side Includes Health and Diagnostics HTTP Logging Logging Tools Request Monitor Tracina	Description: Web Server provides support for HTML Web sites and optional support For BSP.NET, ASP, and Web server extensions. You can use the Web Server to host an internal or external Web site or to provide an environment for developers to create Web-based applications.
	< <u>P</u> revious <u>N</u> e:	xt > Install Cancel

32. Click Install on the Confirm Installation Selections page.

Add Roles Wizard	tion Selections	X
Before You Begin Server Roles AD RMS Role Services AD RMS Cluster	To install the following roles, role services, or features, click Install.]
Configuration Database Service Account Cluster Key Storage Cluster Key Cluster Web Site Cluster Address Licensor Certificate Name SCP Registration Web Server (IIS)	Cluster Type : Root cluster Trust Hierarchy : Production Configuration Database Server : Windows Internal Database Service Account : LUNARMS\admsadmin Cluster Key Storage : CSP key storage CSP for Key Storage : Luna Cryptographic Services for Microsoft Windows Cluster Web Site : Default Web Site Cluster Internal Address : http://adms-srv.lunarms.com:80/ Licensor Certificate Name : ADRMS-SRV Register SCP : Register now C Web Server (IIS)	
Role Services Confirmation Progress Results	Find out more about Windows System Resource Manager (WSRM) and how it can help optimize CPU usage Web Server Common HTTP Features Static Context Print, e-mail, or save this information < <u>Previous</u> <u>Next</u> > <u>Install</u> <u>Cancel</u>	1

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 SafeNet Luna HSM.

Add Roles Wizard	×
Installation Resu	lts
Before You Begin Server Roles AD RMS Role Services AD RMS Cluster Configuration Database Service Account Cluster Key Storage	The following roles, role services, or features were installed successfully: 2 warning messages below Windows automatic updating is not enabled. To ensure that your newly-installed role or feature is automatically updated, turn on Windows Update in Control Panel. Active Directory Rights Management Services Installation succeeded Before you can administer AD RMS on this server, you must log off and log on again. The following role services were installed: Artive Directory Rights Management Server Installation succeeded
Cluster Key Cluster Web Site	Web Server (IIS) Visual Server (IIS)
Cluster Address Licensor Certificate Name SCP Registration Web Server (IIS) Role Services Confirmation Progress Results	The following role services were installed: Web Server Common HTTP Features Static Content Default Document Directory Browsing HTTP Errors HTTP Redirection Application Development Print, e-mail, or save the installation report
	< Previous Next > Close Cancel

- 34. After restarting the system, login as **lunarms\adrmsadmin** and open the Active Directory Rights Management Services console. You will see Luna Cryptographic Services for Microsoft Windows under:
 - Trust Policies -> Trusted Publishing Domains

📸 Active Directory Rights Management S	iervices	_ 8 ×
Elle Action Yiew Help		
💠 🔿 🔟		
Active Directory Rights Management Service	Trusted Publishing Domains	Actions
adrms-srv.lunarms.com (Local)	Import, export and modify trusted publishing domains for this cluster.	Trusted Publishing Domains 🔶
Trusted User Domains		Import Trusted Publishing Domain
Rights Policy Templates		View F
Rights Account Certificate Policies	Trusted Publishing Domain Information	G Refresh
Exclusion Policies Security Policies	Trusted publishing domains define which publishing licenses are trusted by this cluster. The cluster automatically trusts content that it publishes, but it can trust explicitly cluster in the cluster is the cluster is an order of the cluster is an order of the cluster.	🕜 Help
E B Reports	are configured for this cluster. Select a domain to modify its properties or to export its settings to a file.	ADRM5-SRV
		🏦 Export Trusted Publishing Domain
	▲ Name Type CSP Key Container	Properties
	RADRMS-SRV Internal Luna Cryptographic Services for Microsoft WindowsDRMS:MS-GUID: (0406b7	Pelp Help
	1	1

• Security Policies -> Cluster Key Password

🐻 Active Directory Rights Management Services		
Elle Action Yiew Help		
🧇 🐟 📶		
Active Directory Rights Management Service	Cluster Key Password Settings	Actions
 With a drink-sty-Junarms.com (Local) Interference in the style of the	The administration for AD RMS Server Key Protection.	Cluster Key Password 🔺
Trusted User Domains		View
Rights Policy Templates		Refresh
Rights Account Certificate Policies	Cluster Key Password Settings	Properties
Exclusion Policies Security Policies	In the event of data loss or dak failure, you can reset the password that protects the AD RMS cluster law. If you used the centrally managed AD RMS	🔽 Help
Super Users	encryption mediate and an outside or the ordered postering domains to be imported to protect the AD King observery, you can reset the observery passiverd.	
Cluster Key Password	Key protection method: CSP-based key	
E Beports	Key container name: Luna Lryptographic services for Microsoft Windows DRMS:MS-GUID:(04666/MT-c270-4578-8055-98/49acbedc2)	
	Change cluster key password	

3

Integrating Microsoft AD RMS with SafeNet Luna HSM (Windows Server 2012/R2)

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

Before You Begin

It is recommended that 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 provided by Microsoft for more information and pre-installation requirements.

Setup

Operating System	Applications and Services	Description	Computer Name
Windows Server 2012 Standard	Active Directory, Domain Name System (DNS).	Domain Controller	ADRMS-DC
Windows Server 2012 Standard	AD RMS, Internet Information Services (IIS), and Message Queuing	AD RMS Server	ADRMS-SRV
Windows Server 2012 Standard	Microsoft Office Word 2007 Enterprise Edition	AD RMS Client	ADRMS-CLNT

1. The setup consists of the following systems in a private network as per the table below:

- 2. Configure the domain controller on ADRMS-DC.
- 3. Configure the AD RMS root cluster computer on ADRMS-SRV.
- 4. 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.

Account Name	User Logon Name	E-mail address	Group
ADRMSADMIN	ADRMSADMIN		Enterprise Admins
ADRMSSRVC	ADRMSSRVC		
Nicole Holliday	NHOLLIDA	nhollida@hsmserver.com	Employees, Finance
Limor Henig	LHENIG	lhenig@hsmserver.com	Employees, Marketing
Stuart Railson	SRAILSON	srailson@hsmserver.com	Employees, Engineering

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.

Group Name	E-mail address
Finance	finance@hsmserver.com
Marketing	marketing@hsmserver.com
Engineering	engineering@hsmserver.com
Employees	employees@hsmserver.com

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/R2, configure TCP/IP properties, and then join ADRMS-CLNT to the HSMSERVER domain. AD RMS-enabled application also needs to be installed. In this example, Microsoft Office Word 2007/2010 Enterprise Edition is installed on ADRMS-CLNT.

To install Microsoft Office Word 2007/2010 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 2007/2010 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/R2

• Open the command prompt, run the 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 displays.
- 3. Click Add Roles and Features in the Server Manager Dashboard.

4. Click Next on the Before You Begin page.

a	Add Roles and Features Wizard	
Before you begin	DESTINATION SERVER ADRMS-SRV.HSMServer.com	
Before You Begin Installation Type Server Selection Server Roles Features Confirmation Results	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: <u>Start the Remove Roles and Features Wizard</u> 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	
	 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. 	
	< <u>Previous</u> <u>Install</u> Cancel	

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

L	Add Roles and Features Wizard
Before You Begin Installation Type Server Selection Server Roles Features	Add Roles and Features Wizard
Confirmation Results	install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.
	< Previous Install Cancel

6. Select the server from the server pool list and click **Next** on the Server Selection page.

B	Add Roles and Features Wizard		
Select destination	Server Adrms-Srv.HSMServer.com		
Before You Begin Installation Type	Select a server or a virtual hard disk on which to install roles and features. Select a server from the server pool		
Server Selection Server Roles Features Confirmation	Server Pool		
Results	Name IP Address Operating System ADRMS-SRV.HSMServer 172.25.11.108 Microsoft Windows Server 2012 Standard		
	1 Computer(s) found This page shows servers that are running Windows Server 2012, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.		
	< Previous Next > Install Cancel		

7. Select the Active Directory Rights Management Services check box from Roles to install on this server.

A	Add Roles and Features Wizard	
Select server roles Before You Begin	Select one or more roles to install on the selected server.	DESTINATION SERVER ADRMS-SRV.HSMServer.com
Server Selection Server Roles Features Confirmation Results	Active Directory Certificate Services Active Directory Domain Services Active Directory Federation Services Active Directory Federation Services Active Directory Lightweight Directory Services Active Directory Rights Management Services Active Directory Rights Management Services Active Directory Rights Management Services Application Server DHCP Server DNS Server Fax Server ✓ File And Storage Services (Installed) Hyper-V Network Policy and Access Services Print and Document Services Remote Access Remote Desktop Services	Active Directory Certificate Services (AD CS) is used to create certification authorities and related role services that allow you to issue and manage certificates used in a variety of applications.
	< <u>P</u> revious <u>N</u> e	xt >InstallCancel

8. You receive a warning stating Add features that are required for Active Directory Rights Management Services. Click Add Features.

Þ	Add Roles and Features Wizard						
	Add features that are required for Active Directory Rights Management Services? You cannot install Active Directory Rights Management Services unless the following role services or features are also installed.						
	 .NET Framework 4.5 Features WCF Services HTTP Activation ASP.NET 4.5 Remote Server Administration Tools Role Administration Tools [Tools] Active Directory Rights Management Services To 						
	Web Server (IIS)						
	Include management tools (if applicable)						
	Add Features Cancel						

9. Click **Next** to continue on the Server Roles page.

a	Add Roles and Features Wizard			
Select server roles	Select one or more roles to install on the selected server.	DESTINATION SERVER ADRMS-SRV.HSMServer.com		
Installation Type Server Selection	Roles	Description Active Directory Rights Management		
Server Roles Features	Active Directory Domain Services Active Directory Federation Services Active Directory Federation Services	Services (AD RMS) helps you protect information from unauthorized use. AD RMS establishes the identity of users and provides authorized users		
Role Services Web Server Role (IIS)	Active Directory Lightweight Directory Services Active Directory Rights Management Services Application Server	with licenses for protected information.		
Role Services Confirmation	DHCP Server = DNS Server Fax Server			
Results	File And Storage Services (Installed) Hyper-V Network Policy and Access Services			
	Print and Document Services Remote Access Remote Desktop Services			
< <u>Previous</u> <u>Next > Install</u> Cancel				

10. Click **Next** on the Active Directory Rights Management Services window.

a	Add Roles and Features Wizard	_ D X	
Confirmation Results	Add Roles and Features Wizard Rights Management Services (AD RMS) is an information pro- can be integrated with other applications to help safeguard digital informatio use. With AD RMS, content owners can take steps to define who can open, me take other actions with the information they choose to protect. Organizations create rights policy templates for applying rights restrictions directly to custor their confidentiality. Things to note: • To deploy AD RMS, you must create a root cluster for certification and licen- servers. • After deploying AD RMS, you cannot change the name of the domain to wh is joined.	DESTINATION SERVER ADRMS-SRV.HSMServer.com tection technology that n from unauthorized odify, print, forward, or can also use AD RMS to mer data to help ensure asing using one or more hich this AD RMS server	
	More about deploying AD RMS		
< Previous Install Cancel			

11. Select the **Active Directory Rights Management Server** check box from the **Role Services** and click **Next** to continue.

L	Add Roles and Features Wizard	_ D X
Before You Begin Installation Type Server Selection Server Roles Features AD RMS Role Services Web Server Role (IIS) Role Services Confirmation Results	Add Roles and Features Wizard S Select the role services to install for Active Directory Rights Ma Role services Active Directory Rights Management Server Identity Federation Support	DESTINATION SERVER ADRMS-SRV.HSMServer.com anagement Services Description Active Directory Rights Management Services (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.
Results	< <u>P</u> revious <u>N</u> ext	: > Install Cancel

12. Click **Next** to continue on the Web Server Roll (IIS) page.

b	Add Roles and Features Wizard			
Web Server Role (IIS) Destination server Adrms-srv.hsmServer.com				
Before You Begin Installation Type Server Selection Server Roles Features AD RMS Role Services Web Server Role (IIS) Role Services Confirmation Results	 Ce (IIS) ADRMS-SRV.HSMServer.com 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 8.0, 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. 			
	More information about Web Server IIS			
< <u>Previous</u> <u>Next ></u> <u>Install</u> Cancel				

13. Use default selection and Click Next to continue on the Role Services page.

B	Add Roles and Features Wizard	_ D X
Select role service	S	DESTINATION SERVER ADRMS-SRV.HSMServer.com
Before You Begin	Select the role services to install for Web Server (IIS)	
Installation Type	Role services	Description
Server Selection	▲ ✓ Web Server	Web Server provides support for
Server Roles	▲ ✓ Common HTTP Features	HTML Web sites and optional support for ASP NET ASP and Web
Features	✓ Default Document ■	server extensions. You can use the
AD RMS	 Directory Browsing 	Web Server to host an internal or
Role Services	✓ HTTP Errors	environment for developers to
Web Server Role (IIS)	✓ Static Content	create Web-based applications.
Role Services	✓ HTTP Redirection	
Confirmation	WebDAV Publishing	
Results	Health and Diagnostics Health Logging	
	ODBC Logging	
	Request Monitor	
	< <u>P</u> revious <u>N</u> ext	> <u>I</u> nstall Cancel

14. Select the **Restart the destination server automatically if required** check box.

a	Add Roles and Features Wizard	_ 🗆 🗙				
Confirm installation selections						
Before You Begin	To install the following roles, role services, or features on selected server, click Install.					
Installation Type	Restart the destination server automatically if required					
Server Selection	Optional features (such as administration tools) might be displayed on this page because	they have				
Server Roles	been selected automatically. If you do not want to install these optional features, click Pre their check boxes.	vious to clear				
Features						
AD RMS	.NET Framework 4.5 Features	^				
Role Services	ASP.NET 4.5	=				
Web Server Role (IIS)	WCF Services					
Role Services	HTTP Activation					
Confirmation	Active Directory Rights Management Services					
Results	Remote Server Administration Tools Role Administration Tools Active Directory Rights Management Services Tools Web Server (IIS)	~				
	Export configuration settings Specify an alternate source path					
	< <u>P</u> revious <u>N</u> ext > <u>I</u> nstall	Cancel				

- 15. A warning message about restarting the server displays, click Yes.
- 16. Click **Install** on the Confirmation page.

a	Add Roles and Features Wizard					
Confirm installation selections						
Before You Begin	Before You Begin To install the following roles, role services, or features on selected server, click Install.					
Installation Type	Restart the destination server automatically if required					
Server Selection Server Roles	Optional features (such as administration tools) might be displayed or been selected automatically. If you do not want to install these option their check boxes.	on this page because they have nal features, click Previous to clear				
AD RMS	.NET Framework 4.5 Features	^				
Role Services	ASP.NET 4.5	=				
Web Server Role (IIS)	WCF Services					
Role Services Confirmation	Active Directory Rights Management Services Active Directory Rights Management Server					
	Remote Server Administration Tools Role Administration Tools Active Directory Rights Management Services Tools Web Server (IIS)	_				
	Export configuration settings Specify an alternate source path					
	< <u>P</u> revious <u>N</u> ext >	Install Cancel				

17. When installation is completed, either **Close** the wizard or click **Perform additional configuration**. You can open the configuration wizard later by clicking the Notification Flag.

b	Add Roles and Features Wizard
Installation progre	DESTINATION SERVER ADRMS-SRV.HSMServer.com
Before You Begin	View installation progress
Installation Type	i Feature installation
Server Selection	
Server Roles	Configuration required. Installation succeeded on ADRMS-SRV.HSMServer.com.
Features	Active Directory Rights Management Services
AD RMS	AD RMS is installed but additional configuration is needed.
Role Services	Perform additional configuration.
Web Server Role (IIS)	Active Directory Rights Management Server
Role Services	NET Framework 4.5 Features
Confirmation	WCF Services
Results	HTTP Activation
	Remote Server Administration Tools Role Administration Tools Active Directory Rights Management Services Tools
	You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details. Export configuration settings
	< <u>P</u> revious <u>N</u> ext > Close Cancel

18. The AD RMS Configuration wizard displays, click Next to continue.

	TARGET SERVER
	ADRMS-SRV.HSMServer.com
AD RMS	Active Directory Rights Management Services
AD RMS Cluster	
Configuration Database	Active Directory Rights Management Services (AD RMS) is an information protection technology
Service Account	unauthorized use. With AD RMS, content owners can take steps to define who can open, modify,
Cluster Key Storage	print, forward, or take other actions with the information they choose to protect. Organizations
Cluster Key Password	customer data to help ensure their confidentiality.
Cluster Web Site	
Cluster Address	
Server Certificate	
Licensor Certificate	
Confirmation	
Progress	
Results	
	More about deploying AD RMS

19. Select the Create a new AD RMS root cluster radio button and click Next on the AD RMS Cluster page.

a	AD RMS Configuration: ADRMS-SRV.HSMServer.com
AD RMS Cluster	TARGET SERVER ADRMS-SRV.HSMServer.com
AD RMS	Create or Join an AD RMS Cluster
AD RMS Cluster	
Configuration Database	AD RMS supports two types of clusters: a root cluster for certification and licensing and a
Service Account	can then set up one or more licensing-only clusters in the same forest, depending on your needs.
Cryptographic Mode	
Cluster Key Storage	Oreate a new AD RMS root cluster
Cluster Key Password	○ Join an existing AD RMS cluster
Cluster Web Site	
Cluster Address	
Server Certificate	
Licensor Certificate	
SCP Registration	
Confirmation	
Progress	
Results	More about AD RMS clusters
	< <u>Previous</u> <u>Next</u> <u>Install</u> Cancel

20. Select the Use Windows Internal Database radio button on this server and click Next to continue.

A	AD RMS Configuration: ADRMS-SRV.HSMServer.com		_ D ×		
TAI Configuration Database Adrms-srv.Hs					
AD RMS	AD RMS Select Configuration Database Server				
AD RMS Cluster					
Configuration Database	Your AD RMS cluster uses a database to store configuration and poli	icy information	. The database		
Service Account	can be hosted either by Windows Internal Database or on a separate (recommended). If you choose Windows Internal Database, you can	e SQL database not add more A	AD RMS		
Cryptographic Mode	servers to this cluster. You can specify the SQL database server by se	lecting it from	a list, or you		
Cluster Key Storage	can type its name or CNAME alias (recommended).				
Cluster Key Password	O Specify a database server and a database instance.				
Cluster Web Site	S <u>e</u> rver:				
Cluster Address	Select				
Server Certificate	Database Instance:				
Licensor Certificate		▼ <u>L</u> ist			
SCP Registration	: Use Windows Internal Database on this server				
Confirmation	. Ose windows internal Database on disserver				
Progress					
Results	Mana about the AD DMS configuration database				
	More about the AD KMS configuration database				
< <u>P</u> revious <u>N</u> ext > <u>Install</u> Cancel					

21. Click **Specify...** to specify service account.

B

	AD RMS Configuration: ADRMS-SRV.HSMServer.com
Service Account	TARGET SERVER ADRMS-SRV.HSMServer.com
AD RMS	Specify Service Account
AD RMS Cluster	
Configuration Database	The AD RMS cluster requires a domain user account so that it can communicate with other
Service Account	services and network computers. Specify a standard domain user account with no additional permissions.
Cryptographic Mode	
Cluster Key Storage	Domain User Account:
Cluster Key Password	Specify
Cluster Web Site	
Cluster Address	
Server Certificate	
Licensor Certificate	
SCP Registration	
Confirmation	
Progress	
Results	More shout the AD RMS service account
	More about the AD NMO SERVICE account
	< <u>Previous</u> <u>Next</u> > <u>Install</u> Cancel

22. A window displays to add service account user, type the ADRMSSRVC and password and click OK

NOTE: ADRMSSRVC is the user that you have created in Active Directory, see Configure User Account and Group section above.

	Windows Security	
Type User Account Name and Password Type the name and password of a standard domain user account. For example, user@example.contoso.com, or domain\user name.		
P	ADRMSSRVC	
	Connect a smart card	

23. Click **Next** to continue on the Service Account page.

a	AD RMS Configuration: ADRMS-SRV.HSMServer.com
Service Account	TARGET SERVER ADRMS-SRV.HSMServer.com
AD RMS	Specify Service Account
AD RMS Cluster	
Configuration Database	The AD RMS cluster requires a domain user account so that it can communicate with other
Service Account	services and network computers. Specify a standard domain user account with no additional permissions.
Cryptographic Mode	
Cluster Key Storage	Domain User Account:
Cluster Key Password	HSMSERVER\ADRMSSRVC
Cluster Web Site	
Cluster Address	
Server Certificate	
Licensor Certificate	
SCP Registration	
Confirmation	
Progress	
Results	More about the AD RMS service account
	< <u>Previous</u> <u>Next</u> <u>Install</u> Cancel

24. Select Cryptographic Mode to generate the keys and click **Next** to continue.

B

NOTE: You can select any mode on the Specify Cryptographic Mode page. Based on the selected mode, the supported Luna CSP displays.

b	AD RMS Configuration: ADRMS-SRV.HSMServer.com		
Cryptographic Mo	Dde TARGET SERVER ADRMS-SRV.HSMServer.com		
AD RMS	Specify Cryptographic Mode		
AD RMS Cluster			
Configuration Database	AD RMS can operate under two modes which differ on the basis of the cryptographic key length		
Service Account	deployments where you have ensured that all AD RMS client computers have been updated to		
Cryptographic Mode	support it. As cryptographic mode 2 cannot be undone, if you are unsure of full support within this cluster or any other clusters that it will share a trusted user domain (TUD) relationship with, select cryptographic mode 1 instead.		
Cluster Key Storage			
Cluster Key CSP			
Cluster Web Site	Oryptographic Mode 2 (RSA 2048-bit keys/SHA-256 hashes)		
Cluster Address	Companyabis Made 1 (PSA 1024 bit loss (SUA 1 bester)		
Server Certificate	Cryptographic Mode 1 (KSA 1024-bit keys/SHA-1 hashes)		
Licensor Certificate			
SCP Registration			
Confirmation			
Progress			
Results	More about the AD RMS cryptographic mode		
	< Previous Next > Install Cancel		

25. Select the Use CSP key storage radio button and click Next to continue.

a	AD RMS Configuration: ADRMS-SRV.HSMServer.com	
Cluster Key Storag	TARGET SERVER ADRMS-SRV.HSMServer.com	
AD RMS	Specify AD RMS Cluster Key Storage	
AD RMS Cluster		
Configuration Database	An AD RMS cluster uses the AD RMS cluster key to sign certificates and licenses that the cluster	
Service Account	issues. The cluster key is required for disaster recovery and when additional AD KMS servers are joined to the cluster. You can allow AD RMS to encrypt and store the key, or you can store the	
Cryptographic Mode	key by using a cryptographic service provider (CSP). If the cluster key is stored in a CSP, you must	
Cluster Key Storage	manually distribute the key to servers that join the cluster later.	
Cluster Key CSP	○ <u>U</u> se AD RMS centrally managed key storage	
Cluster Web Site	Iteo CSD key storage	
Cluster Address	O Se CSP key stolage	
Server Certificate		
Licensor Certificate		
SCP Registration		
Confirmation		
Progress		
Results	More shout cluster key storage	
	More about cluster key storage	
	< Previous Next > Install Cancel	

26. Choose Luna enhanced RSA and AES provider for Microsoft Windows from the CSP drop-down menu and select the Create a new key with the selected CSP radio button and then click Next to continue.

a	AD RMS Configuration: ADRMS-SRV.HSMServer.com
Cluster Key CSP	TARGET SERVER ADRMS-SRV.HSMServer.com
AD RMS AD RMS Cluster Configuration Database Service Account Cryptographic Mode Cluster Key Storage Cluster Key CSP Cluster Web Site Cluster Address Server Certificate Licensor Certificate SCP Registration Confirmation Progress Results	Specify AD RMS Cluster Key CSP A cryptographic service provider (CSP) can be used to store the AD RMS cluster key. Select an option to create a new key or use an existing key with the selected CSP. CSP: Luna enhanced RSA and AES provider for Microsoft Windows Create a new key with the selected CSP (recommended) Use an existing key with the selected CSP Key: Tore about cluster key storage
	< Previous Next > Install Cancel

27. Click Next to continue on the Cluster Web Site page. Ensure that the Default Web Site is listed.

a	AD RMS Configuration: ADRMS-SRV.HSMServer.com	_		x
Cluster Web Site	TAF ADRMS-SRV.HSI	RGET S MServ	ERVEI er.con	R n
AD RMS AD RMS Cluster Configuration Database Service Account Cryptographic Mode Cluster Key Storage Cluster Key CSP Cluster Web Site Cluster Address Server Certificate Licensor Certificate SCP Registration Confirmation Progress Results	Select AD RMS Cluster Web Site AD RMS is hosted in an Internet Information Services (IIS) virtual directory, which is a of the existing Web sites on this server. Select a Web site for the virtual directory: Default Web Site	et up o	on on	2
	< <u>P</u> revious <u>N</u> ext > <u>I</u> nstall	С	ancel	

28. Select **Use an unencrypted connection (http://)** and type the fully qualified domain name then click **Next** to continue.

B	AD RMS Configuration: ADRMS-SRV.HSMServer.com	_ D X
Cluster Address	T. ADRMS-SRV.H	ARGET SERVER ISMServer.com
AD RMS AD RMS Cluster	Specify Cluster Address	
Configuration Database Service Account Cryptographic Mode Cluster Key Storage Cluster Key CSP Cluster Web Site Cluster Address	A cluster address makes it possible for AD RMS clients to communicate with this cl network. We recommend that you configure AD RMS to use the Secure Sockets La protocol to encrypt network traffic between AD RMS clients and this cluster. You n SSL-encrypted connection if you intend to federate this cluster. Connection Type: <u>U</u> se an SSL-encrypted connection (https://) <u>U</u> se an unencrypted connection (https://)	luster over the iyer (SSL) nust use an
Licensor Certificate	<u>F</u> ully-Qualified Domain Name:	P <u>o</u> rt:
Confirmation Progress Results	http:// ADRMS-SRV.HSMServer.com You cannot change this address or port number after AD RMS is installed and	80 configured.
	More about the cluster web site	
	< <u>Previous</u> <u>N</u> ext > <u>Install</u>	Cancel

29. Ensure that the server name ADRMS-SRV is listed and click **Next** to continue.

a	AD RMS Configuration: ADRMS-SRV.HSMServer.com
Licensor Certificat	Ce TARGET SERVER ADRMS-SRV.HSMServer.com
AD RMS	Name the Server Licensor Certificate
AD RMS Cluster	
Configuration Database	AD RMS creates a server licensor certificate that establishes the identity of this AD RMS cluster to clients. Because of the significance of this certificate, we recommend that you make a backup of
Service Account	this certificate to safeguard your deployment and improve disaster recovery efforts in the event
Cryptographic Mode	of hardware failure or loss of the AD RMS database server.
Cluster Key Storage	N <u>a</u> me:
Cluster Key CSP	ADRMS-SRV
Cluster Web Site	
Cluster Address	
Licensor Certificate	
SCP Registration	
Confirmation	
Progress	
Results	
	< Previous Next > Install Cancel

30. Select Register the SCP now and click **Next** on the SCP Registration page.

B	AD RMS Configuration: ADRMS-SRV.HSMServer.com			
SCP Registration	TARGET SERVER ADRMS-SRV.HSMServer.com			
AD RMS AD RMS Cluster	Register AD RMS Service Connection Point			
Service Account	(AD DS) when an AD RMS cluster is created. The SCP provides clients with intranet URLs for the AD RMS cluster.			
Cryptographic Mode Cluster Key Storage Cluster Key CSP	To register the service connection point (SCP) now, you must be a member of the Enterprise Admins group. If you are not a member of the Enterprise Admins group, you must have a member of the Enterprise Admins group register the SCP after you finish installing AD RMS. Clients cannot access this AD RMS cluster until its SCP is registered.			
Cluster Web Site Cluster Address	<u>R</u> egister the SCP now			
Licensor Certificate SCP Registration	Register the SCP later			
Confirmation Progress				
Results				
	More about SCP registration			
	< Previous Next > Install Cancel			

31. Click **Install** on the Confirmation page.

a	AD RMS Configuration: A	DRMS-SRV.HSMServer.com	_ D ×
Confirmation		ADRMS-SRV.	ARGET SERVER HSMServer.com
AD RMS Cluster Configuration Database Service Account	To install the following roles, n	ple services, or features, click Install.	
Cryptographic Mode Cluster Key Storage Cluster Key CSP Cluster Web Site Cluster Address Licensor Certificate SCP Registration Confirmation Progress Results	Cluster Type: Database Server: Service Account: Cryptographic Mode: Cluster Key Storage: CSP for Key Storage: Cluster Web Site: Cluster Uternal Address: Licensor Certificate Name: Register SCP:	Root cluster Windows Internal Database HSMSERVER\ADRMSSRVC Cryptographic Mode 2 CSP key storage Luna enhanced RSA and AES provider for Micros Default Web Site http://adrms-srv.hsmserver.com/ ADRMS-SRV Register Now	oft Windows
		< <u>P</u> revious <u>N</u> ext > <u>Install</u>	Cancel

32. Click **Close** after successful installation of the AD RMS Services.

b	AD RMS Configuration: ADRMS-SRV.HSMServer.com
Results	TARGET SERVER ADRMS-SRV.HSMServer.com
AD RMS	Installation Results
AD RMS Cluster	The following roles role services or features were installed successfully:
Service Account	C Active Directory Rights Management Services
Cryptographic Mode	Before you can administer AD RMS on this server, you must log off and log on again.
Cluster Key Storage Cluster Key CSP	The following role services were installed:
Cluster Web Site	Active Directory Rights Management Server
Cluster Address	
SCP Registration	
Confirmation	
Progress	
Results	
	Troubleshooting AD RMS setup
	< Previous Next > Close Cancel

33. After restarting the system, log on as **hsmserver/adrmsadmin** and 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

B

NOTE: Luna CSP that you have selected at configuring the AD RMS displays here.

3	Artive Directory Pichts Management Services	
File Action View Help		
← ⇒ 2 2		
Active Directory Rights M		Actions
adrms-srv.hsmserver.c	Irusted Publishing Domains	Trusted Publishing Domains
⊿ 🃑 Trust Policies ➡ Trusted User D	🛜 Import, export and modify trusted publishing domains for this cluster.	Timport Trusted Publishing Dom
Trusted Publisł	- n	View
Rights Policy Temp	Terret of Delifection Description	🔍 Refresh
Rights Account Ce Rights Account Ce		🖉 Help
Security Policies	Trusted publishing domains define which publishing licenses are trusted by this cluster. The cluster automatically trusts content that it publishes, but it	No selected item in view
Reports	domains are configured for this cluster. Select a domain to modify its properties or to export its settings to a file.	Export Trusted Publishing Dom
		7 Help
	A Name Time CCD KeyContriner Contament	
	Register Register	

• Security Policies -> Cluster Key Password

3	Active Directory Rights Management Services		- 0 X
<u>File</u> <u>Action</u> <u>V</u> iew <u>H</u> elp			
🗢 🄿 🙎			
Active Directory Rights M	Cluster Key Password Settings	Actions	
⊿ i adrms-srv.hsmserver.c		Cluster Key Passwor	d 🔺
👢 Trusted User D	The administration for AD KMS Server Key Protection.	View	•
Trusted Publisk		 🖪 Refresh	
 Trusted Devidisity Rights Policy Territy Rights Policy Territy Rights Account Ce Security Policies Super Users Cluster Key Pare Cluster Key Pare Decommission ■ Reports 	Cluster Key Password Settings	Properties	
	Cluster Key Password Settings In the event of data loss or disk failure, you can reset the password that protects the AD RMS cluster key, If you used the centrally managed AD RMS encryption method in this cluster or the trusted publishing domains to be imported to protect the AD RMS cluster key, you can reset the cluster key password. Cyptographic service provider name: Cyptographic serv	Help	
< III >			

4 Verifying AD RMS Functionality using AD RMS CLIENT

To verify the functionality of the AD RMS deployment, log on ADRMS-CLNT 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. Log out form ADRMS-CLNT and then log on as Stuart Railson, verifying that the proper permission to read the document has been granted, and nothing else. Then, 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, 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 rightsprotected content.

- 1. To add AD RMS cluster to Local Intranet security zone
 - Log on to ADRMS-CLNT as Nicole Holliday.
 - Click Start, and then click Internet Explorer.
 - Click **Tools**, and then click Internet Options.
 - Click the Security tab, click Local intranet, and then click Sites.
 - In the Add this website to the zone, type http://<fully qualified domain name of the server>, for example http://ADRMS-SRV.hsmserver.com and then click Add.
 - Click Close and then OK.
 - 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.

- 2. To restrict permissions on a Microsoft Word document
 - Log on to ADRMS-CLNT as Nicole Holliday.
 - Right click on the screen and select New -> Microsoft Office Word Document.
 - 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.
 - Click the Microsoft Office Button, click Prepare, click Restrict Permission, and then click Restricted Access.
 - Click the Restrict permission to this document check box.

- In the **Read** box, type email of the group for which you want to grant the permission, for example **engineering@hsmserver.com** and then click **OK** to close the Permission dialog box.
- Click the **Microsoft Office Button**, click **Save As**, and then save the file as \\ADRMS-SRV\Public\ADRMS-TST.docx.
- Log off as Nicole Holliday.

Next, log on as Stuart Railson and open the document, ADRMS-TST.docx

- 3. To view a rights-protected document
 - Log on to ADRMS-CLNT as Stuart Railson.
 - Click Start, and then click Computer.
 - Click in the Address bar, type \\ADRMS-SRV\Public\ADRMS-TST.docx, and then press Enter.
 - The following message displays: "Permission to this document is currently restricted. Microsoft Office must connect to http://adrms-srv.hsmserver.com/_wmcs/licensing to verify your credentials and download your permission."

Click OK.

- The following message displays: "Verifying your credentials for opening content with restricted permissions..."
- When the document opens, click the **Microsoft Office** Button. Notice that the Print option is not available.
- Close Microsoft Word.
- Log off as Stuart Railson.

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

- 4. To attempt to view a rights-protected document.
 - Log on to ADRMS-CLNT as Limor Henig.
 - Click Start, and then click Computer.
 - Click in the Address bar, type \\ADRMS-SRV\Public\ADRMS-TST.docx, and then press Enter.
 - The following message displays: "Permission to this document is currently restricted. Microsoft Office must connect to http://adrms-srv.hsmserver.com/_wmcs/licensing to verify your credentials and download your permission."
 - Click OK.
 - The following message displays: "You do not have credentials that allow you to open this document. You can request updated permission from nhollida@hsmserver.com. Do you want to request updated permission?"
 - Click No, and then close Microsoft Word.

This demonstrates the AD RMS functionality, using the simple scenario of applying restricted permissions to a Microsoft Word 2007/2010 document. This deployment can be to explore to 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. In 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.

SafeNet Luna HSM 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.

SafeNet Luna HSM is tested with two-way TPD between the two forests.

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**.

Solution:

- 1. Ensure 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.