Azure HYOK

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: 007-013642-001, Rev. A **Release Date:** December 2016

Contents

Scope 4 Gemalto Rebranding 4 Document Conventions 4 Command Syntax and Typeface Conventions 5 Support Contacts 6 1 Introduction 7 Overview 7 Understanding the HYOK 7 3rd Party Application Details 8 Supported Platforms 9 On Premise AD RMS Setup 9 Integrating Azure HYOK with On Premise AD RMS 12 Configuring Azure RMS Services with On Premise AD RMS 12 Configuring Azure RMS Services with On Premise AD RMS 12 Configuring Azure RMS Services with On Premise AD RMS 12 Configuring Azure RMS Services with On Premise AD RMS 12 Configuring Azure RMS Services with On Premise AD RMS 12 Configuring Azure RMS Services with On Premise AD RMS 13 Verifying Azure HYOK feature with On Premise AD RMS using ADRMS Client	Pr	eface	4
Gemalto Rebranding. 4 Document Conventions 4 Command Syntax and Typeface Conventions. 5 Support Contacts. 6 1 Introduction 7 Overview 7 Understanding the HYOK 7 Junderstanding the HYOK 7 Supported Platforms. 8 Supported Platforms. 8 Prerequisites 9 On Premise AD RMS Setup 9 2 Integrating Azure HYOK with On Premise AD RMS. 12 Azure HYOK with AD RMS. 12 Configuring Azure RMS Services with On Premise AD RMS 12 Configuring a label for protection, a watermark, and a condition to prompt for classification 18 Verifying Azure HYOK feature with On Premise AD RMS using ADRMS Client 20		Scope	4
Document Conventions 4 Command Syntax and Typeface Conventions 5 Support Contacts 6 1 Introduction Overview 7 Understanding the HYOK 7 3rd Party Application Details 8 Supported Platforms 8 Prerequisites 9 On Premise AD RMS Setup 9 2 Integrating Azure HYOK with On Premise AD RMS 12 Configuring Azure RMS Services with On Premise AD RMS 12 Configuring a label for protection, a watermark, and a condition to prompt for classification 18 Verifying Azure HYOK feature with On Premise AD RMS using ADRMS Client 20		Gemalto Rebranding	4
Command Syntax and Typeface Conventions. 5 Support Contacts. 6 1 Introduction 7 Overview 7 Understanding the HYOK 7 3rd Party Application Details 8 Supported Platforms. 8 Prerequisites 9 On Premise AD RMS Setup 9 2 Integrating Azure HYOK with On Premise AD RMS. 12 Azure HYOK with AD RMS 12 Configuring Azure RMS Services with On Premise AD RMS 12 Configuring a label for protection, a watermark, and a condition to prompt for classification. 18 Verifying Azure HYOK feature with On Premise AD RMS using ADRMS Client. 20		Document Conventions	4
Support Contacts.		Command Syntax and Typeface Conventions	5
1 Introduction 7 Overview 7 Understanding the HYOK 7 3rd Party Application Details 8 Supported Platforms 8 Prerequisites 9 On Premise AD RMS Setup 9 On Premise AD RMS Setup 9 2 Integrating Azure HYOK with On Premise AD RMS 12 Azure HYOK with AD RMS 12 Configuring Azure RMS Services with On Premise AD RMS 12 Configuring a label for protection, a watermark, and a condition to prompt for classification 18 Verifying Azure HYOK feature with On Premise AD RMS using ADRMS Client 20		Support Contacts	6
Overview 7 Understanding the HYOK 7 3rd Party Application Details 8 Supported Platforms 8 Prerequisites 9 On Premise AD RMS Setup 9 2 Integrating Azure HYOK with On Premise AD RMS 12 Azure HYOK with AD RMS 12 Configuring Azure RMS Services with On Premise AD RMS 12 Configuring a label for protection, a watermark, and a condition to prompt for classification 18 Verifying Azure HYOK feature with On Premise AD RMS using ADRMS Client 20	1	Introduction	7
Understanding the HYOK 7 3rd Party Application Details 8 Supported Platforms 8 Prerequisites 9 On Premise AD RMS Setup 9 2 Integrating Azure HYOK with On Premise AD RMS 12 Azure HYOK with AD RMS 12 Configuring Azure RMS Services with On Premise AD RMS 12 Configuring a label for protection, a watermark, and a condition to prompt for classification 18 Verifying Azure HYOK feature with On Premise AD RMS using ADRMS Client 20		Overview	7
3rd Party Application Details 8 Supported Platforms 8 Prerequisites 9 On Premise AD RMS Setup 9 2 Integrating Azure HYOK with On Premise AD RMS 12 Azure HYOK with AD RMS 12 Configuring Azure RMS Services with On Premise AD RMS 12 Configuring a label for protection, a watermark, and a condition to prompt for classification 18 Verifying Azure HYOK feature with On Premise AD RMS using ADRMS Client 20		Understanding the HYOK	7
Supported Platforms		3rd Party Application Details	8
Prerequisites 9 On Premise AD RMS Setup 9 2 Integrating Azure HYOK with On Premise AD RMS 12 Azure HYOK with AD RMS 12 Configuring Azure RMS Services with On Premise AD RMS 12 Configuring a label for protection, a watermark, and a condition to prompt for classification 18 Verifying Azure HYOK feature with On Premise AD RMS using ADRMS Client 20		Supported Platforms	8
On Premise AD RMS Setup 9 2 Integrating Azure HYOK with On Premise AD RMS 12 Azure HYOK with AD RMS 12 Configuring Azure RMS Services with On Premise AD RMS 12 Configuring a label for protection, a watermark, and a condition to prompt for classification 18 Verifying Azure HYOK feature with On Premise AD RMS using ADRMS Client 20		Prerequisites	9
2 Integrating Azure HYOK with On Premise AD RMS. 12 Azure HYOK with AD RMS. 12 Configuring Azure RMS Services with On Premise AD RMS. 12 Configuring a label for protection, a watermark, and a condition to prompt for classification. 18 Verifying Azure HYOK feature with On Premise AD RMS using ADRMS Client. 20		On Premise AD RMS Setup	9
Azure HYOK with AD RMS	2	Integrating Azure HYOK with On Premise AD RMS	. 12
Configuring Azure RMS Services with On Premise AD RMS		Azure HYOK with AD RMS	12
Configuring a label for protection, a watermark, and a condition to prompt for classification		Configuring Azure RMS Services with On Premise AD RMS	12
Verifying Azure HYOK feature with On Premise AD RMS using ADRMS Client20		Configuring a label for protection, a watermark, and a condition to prompt for classification	18
		Verifying Azure HYOK feature with On Premise AD RMS using ADRMS Client	20

Preface

This document is intended to guide administrators through the steps for Azure HYOK integration with on premise AD RMS that uses SafeNet Network HSM for securing the tenant key. This guide provides the necessary information to install, configure, and integrate Azure HYOK with on premise AD RMS.

Scope

This guide provides instructions for setting up a small test lab with AD RMS running with SafeNet Network HSM for securing the tenant key and integrate with Azure HYOK feature for protected documents. It explains how to install and configure the software that is required for setting up Azure HYOK with on premise AD RMS while storing tenant key on SafeNet Network HSM.

Gemalto Rebranding

In early 2015, Gemalto completed its acquisition of SafeNet, Inc. As part of the process of rationalizing the product portfolios between the two organizations, the Luna name has been removed from the SafeNet HSM product line, with the SafeNet name being retained. As a result, the product names for SafeNet HSMs have changed as follows:

Old product name	New product name
Luna SA HSM	SafeNet Network HSM
Luna PCI-E HSM	SafeNet PCI-E HSM
Luna G5 HSM	SafeNet USB HSM
Luna Client	SafeNet HSM Client

I

NOTE: These branding changes apply to the documentation only. The SafeNet HSM software and utilities continue to use the old names.

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.

Command Syntax and Typeface Conventions

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.

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 Customer Portal	https://serviceportal.safenet-inc.com Existing customers with a Technical Support Customer Portal account can log in to manage incidents, get the latest software upgrades, and access the Gemalto Know Base.							

1 Introduction

Overview

In August 2016, Microsoft announced a preview of Hold Your Own Key (HYOK) designed to support organizations that need to comply with complex regulation and compliance policies. HYOK enables organizations to retain sole control over encryption keys and over the authorization process. For the majority of organizations, HYOK enables keying material to be generated and stored within their on-premise HSM as opposed to storing keying material in the Azure Cloud.

HYOK is implemented via a new Azure Information Protection client that now supports multiple RMS services within a singular Azure Information Protection environment (Azure RMS and AD RMS). End users simply select and apply the appropriate classification label for the document that will be shared. i.e. A label of "Internal and Confidential' would be based upon an AD RMS Rights Policy, while a label of "For Partners and 3rd parties" would be based upon an Azure RMS rights policy and enables documents to be shared externally.

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 will be deployed to provide a security framework to the data in use, data at rest and the data in transit.

SafeNet Network HSM secures the AD RMS Cluster Key generated and used by the AD RMS. You can integrate the AD RMS with the SafeNet Network HSM by using the MSCAPI interface. The benefits of using SafeNet Network 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.

Understanding the HYOK

The Azure Information Protection HYOK – Hold Your Own Key – feature is about enabling an organization to protect data in a way where, well, you hold the key. Whereas BYOK (Bring Your Own Key) requires

organizations to give control of keying material to Azure and store their keys in the Azure Cloud. For many organizations, this loss of control over keying material to a cloud provider limits their use of the cloud.

The HYOK concept is quite simple: You deploy multiple RMS services within a singular Azure Information Protection environment. At a top level, here's what you would do:

You deploy Azure Information Protection in your organization as per usual guidance. In effect, the Azure Information Protection services (Azure RMS, Admin Information protection configuration in Azure) are always cloud hosted but they enable you to operate in a cloud-only, hybrid, or on-premises only (via the RMS connector) deployment.

- 1. Azure RMS is where you define your Azure RMS protection policies for sensitive data.
- 2. AD RMS is where you define your AD RMS protection policies, for 'top-secret' data.
- 3. Your Azure Information Protection service is where you define all your classification labels. Labels can be bound to an Azure RMS server as well as AD RMS server.

When an end user makes use of their classification user interface, they see labels not really knowing which RMS server is used... by design! They pick the label and you, as IT, set the policy that gets applied. That's it! By way of example, in this label taxonomy, My Group could be bound to AD RMS (for internal sharing) and All Employees bound to Azure RMS (for third party and external users). Your users need not care.

Personal			Not Restricted					Internal					Confidential				tia		Secret 🝷 💼								
1.1		•	3	1	•	•	ï	•	÷	4	•	•	÷	ï		2	•	5	ł.		•	1	•	My Group			X
																								All Employee	25		

3rd Party Application Details

- AD RMS
- Microsoft Azure Premium P2 Subscription
- Microsoft Office

Supported Platforms

The following platforms are tested with SafeNet Network HSM:

Operating Systems	SafeNet HSM	Microsoft Office
Windows Server 2012 R2	SafeNet Network HSM Appliance Software v6.2.1	Office 2013 SP1
	Firmware 6.10.9 or 6.24.2	
	SafeNet HSM Client 6.2.1	

Prerequisites

On Premise AD RMS Setup

First you need to setup on premise AD RMS using SafeNet Network HSM. Follow the *Active Directory Rights Management Services Integration Guide with SafeNet HSM* to setup and configure AD RMS with SafeNet Network HSM. AD RMS Integration guide is available on SafeNet support.

Operating System	Applications and Services	Description	Computer Name
Windows Server® 2012 R2 Enterprise	Active Directory, Domain Name System (DNS)	Domain Controller	ADRMS-DC
Windows Server® 2012 R2 Enterprise	AD RMS, Internet Information Services (IIS) 7.0, and Message Queuing	AD RMS Server	ADRMS-SRV
Windows 7 Enterprise Edition with Service Pack1	Microsoft Office Word 2013 Enterprise Edition with Service Pack1	AD RMS Client	ADRMS-CL

On premise AD RMS setup must have the following:

You need to have AD RMS working in your environment, with single sign-on setup, and only use one root cluster of AD RMS servers. After setting up everything mentioned in the integration guide make the following changes to work with the Azure HYOK.

AD RMS integration guide uses the HTTP to connect with licensing URL but Azure HYOK require the HTTPS. To enable the HTTPS protocol you need to generate the SSL certificate for the IIS and bind it to start working with HTTPS. Steps to enable the HTTPS are provided below:

- 1. Log on to the ADRMS server as administrative permission.
- 2. Click Start -> Administrative Tools -> Internet Information Services (IIS) Manager.
- 3. Click on Server Name in the left pane tree and double click Server Certificates.
- 4. On the right side under Actions pane, click on the Create Self-Signed Certificate...
- 5. Specify the Friendly Name and click OK. It generates the certificate.
- 6. Now expand the Sites and click on Default Web Site.
- 7. Click on SSL Settings and then in Actions pane click Bindings...
- 8. A **Site Bindings** window will pop up. Click **Add** and then select **Type** as **https** and **SSL certificate** that you have generated.
- 9. Click **OK** and then **Close** to close the **Site Binding** window.
- 10. Now browse the licensing URL to check it is accessible on HTTPS.

https://adrms-srv.hsmserver.com/_wmcs/licensing/license.asmx

	- 0 X
🗘 🖗 🖉 https://admis-six.komserver.com/_winciplicensing license.asmix 🖉 + 🖬 C 🖉 License Web Service x	⊕ ★ \$
License	ſ
The following operations are supported. For a formal definition, please review the <u>Service Description</u> .	
AcquireLicense	
<u>AcquirePrelicense</u>	

After configuring the ADRMS on HTTPS you need couple of settings to work with Azure HYOK. To do these settings follow the steps below:

- 1. Open the Active Directory Rights Management Services console.
- 2. Click on the ADRMS server in the left pane and from Actions pane at right side click on Properties.
- 3. Click on the **Cluster URLs** tab and select **Extranet URLs**. Select https in **Licensing** and **Certification** and provide the IP Address of ADRMS server.

à		Active Directory Rights Management Services	- 0 X					
File Action View Help								
(* · •) 21 🖬								
Active Directory Rights Management Services	AD BME Comme Churches		Actions					
a 👹 adms-srv.hsmserver.com (Local)	AD KMS Server cluster	AU MMS Server Cluster						
Trust Policies Trusted User Domains Trusted Publishing Domains	Configure settings for a cluster. All servers i	n a cluster share common configuration and logging databases.	Change Service Account					
Rights Policy Templates	Cluster Details	adms-srv.hsmserver.com (Local) Properties	Contraction Contraction					
Rights Account Centificate Poices Build Control Poices Success Success Success People People People	Cluster Details Cluster Details Cluster Summay Cuter type Cyter name Cyter type Content when (winker) Heranet totate UB(s Licening Centification Detailsen Centification Centification Database Centification	October 1000000000000000000000000000000000000	Context C					
	1							
	<u>1</u>		10/3/2016					

4. Click **OK** to close the **Properties**. Extranet URL setting is required to reach the ADRMS server from outside.

5. Now click on **Rights Policy Templates** and note down the **GUID**. Both GUID and Licensing URL is required later when setting up the AD RMS template in Azure RMS. If no any GUID is listed under Rights Policy Templates then click on the **Create Distributed Rights Policy Templates...** in **Actions** pane and follow the wizard with default options to create it.

emplates 🔺
buted Rights Policy Templates
ved Rights Policy Templates
•
m in view
uted Rights Policy Template
ights Policy Template
ımmary
er bu ve

Now you are ready to deploy the Azure HYOK with on premise AD RMS.

2 Integrating Azure HYOK with On Premise AD RMS

Azure HYOK with AD RMS

To set up Azure HYOK with AD RMS, first you need the Azure account and Azure Premium P2 subscription for Azure RMS services. You can subscribe it from Microsoft Azure Portal online.

Configuring Azure RMS Services with On Premise AD RMS

- 1. After you have signed up for your Azure account, sign in to the Azure classic portal. Use a global administrator account such as the account you used to get the subscription that includes Azure Rights Management.
- 2. In the left pane, click **ACTIVE DIRECTORY**.
- 3. From the active directory page, click RIGHTS MANAGEMENT.
- 4. Select the directory to manage for Rights Management, click ACTIVATE, and then confirm your action.



NOTE: If you see an activation error, it might be because your service plan or product version does not include the Azure Rights Management service for Azure Information Protection.

Use the subscription information to confirm that your subscription includes Azure Rights Management. For help with this issue, contact Microsoft Azure support.

The RIGHTS MANAGEMENT STATUS should now display Active and the ACTIVATE option is replaced with DEACTIVATE.

Azure AD Identity Prote: x				<u>(1) (1) (1) (1) (1) (1) (1) (1) (1) (1) </u>
$\leftarrow \ni \mathbf{C} \left[\bullet \text{ https://manage.windowsazure.com/gemalto2.onmicrosoft.com#Worksp} \right]$	aces/ActiveDirectoryExtension/rightsManagement			ź.
Microsoft Azure 🔍 🗸	Overk out the new portal	⊕ mariti	lgemaitoZonnicrosoft.com	
AL ITAN	active directory			
🛞 WE APPS	DIRECTORY ACCESS CONTROL NAMESPACES MI	ULTI-FACTOR AUTH PROVIDERS RIGHTS MANAGEMENT		
	NAME	RIGHTS MANAGEMENT STATUS	P	
MODELS SERVICES	ment	+ A04	_	
DB SOL DATABASIS				
STORAGE				
ининскат				
The server me				
VISUAL STUDIO YFAM S				
Cont Cont				
🦚 🕬				
+ NEW		Discovan	0	
	Security and			

Next step is to synchronize Azure Active Directory and local Active Directory for password synchronization. To do this download the Azure AD Connect from Microsoft official site:

https://www.microsoft.com/en-us/download/details.aspx?id=47594

- 5. Sign in as a local administrator to the server (Local AD) you wish to install Azure AD Connect on. You should do this on the server you wish to be the sync server.
- 6. Navigate to and double-click AzureADConnect.msi.
- 7. On the Welcome screen, select the box agreeing to the licensing terms and click Continue.

8. On the Express Settings screen, click Use express settings.

🚸 Microsoft Azure Active D	Directory Connect –	×
Welcome Express Settings	Express Settings	
	If you have a single Windows Server Active Directory forest, we will do the following: Configure synchronization of identities in the current AD forest of FABRIKAM Configure password synchronization from on-premises AD to Azure AD Start an initial synchronization Synchronize all attributes Enable Auto Upgrade Learn more about express settings If you would like different settings, click Customize.	
	Customize Use express settings	

9. On the **Connect to Azure AD** screen, enter the username and password of a global administrator for your Azure AD. Click **Next**.

Microsoft Azure Active D	irectory Connect		_ ×
Microsoft Azure Active D Welcome Express Settings Connect to Azure AD Connect to AD DS Configure	irectory Connect Connect to Azure AD Enter your Azure AD credentials: ? USERNAME username@contoso.onmicrosoft.com PASSWORD		_ X
		Previous	Next

10. On the **Connect to AD DS** screen, enter the username and password for an enterprise admin account. Like HSMSERVER\Administrator and click **Next**.

I dicrosoft Azure Active D	irectory Connect	_ ×
Welcome Express Settings Connect to Azure AD Connect to AD DS Configure	CONNECT TO ADD DS Enter the Active Directory Domain Services enterprise administrator credentials: USERNAME CONTOSOLUSERname PASSWORD	
	Previous	Next

11. On the Ready to configure screen, select Start the synchronization process as soon as the configuration completes. Click Install.

< Microsoft Azure Active D	irectory Connect	_ ×
Welcome Express Settings Connect to Azure AD Connect to AD DS Configure	 Ready to configure Drice you click Install/Upgrade, we will do the following: Install the synchronization engine Configure AAD Connector Configure fabrikamonline.com Connector Enable Password synchronization Enable Auto Upgrade Configure synchronization services on this computer Start the synchronization process as soon as the configuration completes. Exchange hybrid deployment ? 	
	Previous	Install

12. When the installation completes, click Exit.

13. Now sign off from the Azure Classic Portal and sign in again to see the synchronization. After sync it will show you the local users and groups in Azure portal.



- 14. Now log on to Microsoft Azure Portal and create Azure RMS Protection policy using the steps provided below.
- 15. In a new browser window, sign in to the Azure portal as a global admin for your tenant.

16. On the hub menu, click New, and then, from the **MARKETPLACE** list, select **Security + Identity**. In the Security + Identify blade, from the **FEATURED APPS** list, select **Azure Information Protection**.



17. Select **Pin to dashboard** to create an Azure Information Protection tile on your dashboard, so that you can skip browsing to the service the next time you sign in to the portal. Click **Create**.



18. Click Azure Information Protection on dashboard.

- 19. Explore the main Azure Information Protection blade, which shows the default Information Protection policy that's automatically created:
 - Labels for classification: **Personal**, **Public**, **Internal**, **Confidential**, and **Secret**. Read the tooltip for each to understand how the labels are intended to be used. Note that Secret has two sub-labels: All-Employees and My-Group, which provides an example of how a classification can have subcategories.
- 20. Select **On** for All documents and emails must have a label. For **Select the default label**, set this to **Internal**. For **Users must provide justification to set a lower classification label, remove a label, or remove protection**, set this to **On**.



Configuring a label for protection, a watermark, and a condition to prompt for classification

Now, you need to change the settings of one of the labels, Confidential:

- 1. Click on the label: Confidential.
- 2. In the Label: Confidential blade, locate the section Set RMS template for protecting documents and emails containing this label:
- 3. For the Select RMS template from option, click AD RMS (PREVIEW)
- 4. Enter the GUID of your AD RMS Server in the **Type the template GUID** section.
- 5. Enter the licensing URL of your AD RMS server in the **Type the licensing URL of the AD RMS cluster** section.

6. Change the settings for **Header**, **Footer**, **Watermark** and other settings as you needed and click on **Save** to save the changes.

oft Azure 🐱 🗛	re Information Protection 🗲 Label: Confidential		P Search resources	× 🖓 🏽 🖸 🔿	marif@gemalto2
Azure Information	Protection	.★ _ □ ×	Label: Confidential -	□ ×	
III Columns III See	🗙 Decard 🟥 Publish 👱 Expert		🕂 Save 🗙 Decard 📑 Orders this label		
Configure a title and tool * Tide Sensitivity Tooltip. Information Sensitivity co- ordermation to use theory	ip for the Information Protection client on user devices	e user to identify the risk of exposing the	Specify how this label is displayed in the Information Protection client on user devices Institut Of Ca Autor Can Autor Candemai Condemai		
Configure the name, toolt	lip, and additional settings of each label; Order the labels according to toorne MARRING	their sensitivity level	Tability Dire data includes another business information. Exposing this data to unaperturbate users cause damage to the business. Complete to: Confidential information are employee inform individual customer projects or contracts and tales account data.	may ahion.	
Demont	Encountered use only. This data will not be mentored		Color Orange		
Public	This information can be used by everyone inside or ou This information includes a wide spectrum of internal I 💙		Set RMS template for protecting documents and emails containing this label Setect RMS template from		
Confidential	This data includes sensitive business information. Expo	AD RMS	Type the template GBID	-	
Secret Add a new label All documents and emails in	This data includes highly sensitive information for the V		6000944c-b788-416e-8d79-7002140031c9 Type the licensing URL of the AD RMS cluster Imper/10.164.76.178		
Select the default label		•]	Set visual marking (such as header or footer) Documents with this label have a header		
Users must provide justificat	ton to set a lower classification label, remove a label, or remove protection		Con C	_	

7. Now click on **Publish** to publish the changes you made. Click **Yes** when the confirmation message displays.

soft Azure V Azure Information Protection S Label: Confidential		P Search resources	× 🗘 🕸 🛈 🔿	marif@gemalto
Azure Information Protection	* _ = ×	Label: Confidential	_ = ×	
III Columns I Save X Discard 11 Publish & Export		E Saver X Discard B Delete this label		
Click Publish to deploy changes to all users		0909944c-b788-41be-8d79-7032140031c9		
		Type the licensing URL of the AD RMS sluster		
Configure a title and toolitp for the information Protection client on user devices		https://10.164.76.175	· • ·	
Sensitivity		terrenterterter etter ernet		
Toolite		Set visual marking (such as header or footer)		
Information Sensitivity consists of four distinct levels (Public, Internal, Confidential, Secret)	allowing the user to identify the risk of exposing the	Of On		
information to unauthorized users inside or outside the business.		Processory with the fabric land a schedure		
		Off On		
	200 00000	* Ecolor land		
Configure the name, tooltip, and additional settings of each label; Order the labels ad	cording to their sensitivity level	Sensitivity: Confidential		
LARE NOVE TOOLS	PROTECTION	* Fort size		
Personal For personal use only. This data will not be monitored		8	-	
Public This information can be used by everyone inside or ou		Color		
Internal This information includes a wide spectrum of internal 1	e	Black	·	
Confidential This data includes sensitive business information. Expo	AD BMS	Alignment		
This data includes highly cancillate information for the		Left Center Right		
Cardon Contractor		Documents with this label have a watermark		
		Off On		
Off Cm		* Watermark test		
Salari the default label		Gemalto Confidential		
Internal	*	Size		
Users must provide sustification to set a lower classification label, remove a label, or remove	protection	Auto Custom		
CH CN		Color		
		1980X		
		Layout		
		Horgontal Chagonal		

You are now ready to apply this label to our documents and protect them using on premise AD RMS protection.

Verifying Azure HYOK feature with On Premise AD RMS using ADRMS Client

To verify the HYOK with AD RMS, first make sure that your AD RMS client computer must have Windows 7 Enterprise Edition with Service Pack 1 or higher and either Microsoft Office 2013 or Microsoft Office 2016. Office 2010 does not support HYOK feature.

In case of Office 2013, Ensure that you have Office 2013 with Service Pack 1 is installed and you have applied the Office 2013 update **KB3054853**. Also you have installed the **.Net 4.5.1** on AD RMS client computer.

Above updates are needed to install the Azure Information Protection Client. You can download the Azure Information Protection Client from Microsoft download center.

https://www.microsoft.com/en-us/download/details.aspx?id=53018

- 1. Log on to ADRMS-CL as an Administrator.
- 2. Run AzInfoProtection_v233.exe and select the license agreement. Click Install.

👌 AzInfoProtection - Preview 📃 📼 📼		
Microsoft Azure Information Protection		
MICROSOFT PRE-RELEASE SOFTWARE LICENSE TERMS		
MICROSOFT AZURE INFORMATION PROTECTION - PREVIEW		
These license terms are an agreement between Microsoft Corporation (or based on where you live, one of its affiliates) and you. Please read them. They apply to the pre-release software named above, which includes the media on which you received it, if any. The terms also apply to any Microsoft		
✓ I <u>agree to the license terms and conditions</u> Install a <u>demo policy until another policy applied</u>		
Privacy Statement Install Version 1.0.233.0		

3. Click Close when installation finish.

AzInfoProtection - Preview	
Microsoft Azure Information Protection	
Setup Successful	
	Close

4. Now logoff from the system and login with domain user to create a restricted documents.

5. Log on to **ADRMS-CL** as **NHOLLIDA**.

- 14	-
- 1	11
	~
	~

NOTE: If AD RMS setup is done as per the AD RMS Integration Guide then all these users would be there.

- 6. Create a new word document and write something in the document. You can see the Azure Information Protection labels in the document.
- 7. Click on the Confidential that you configured for AD RMS (PREVIEW) in Azure Portal.
- 8. A security alert message will display as you are using the self-signed certificate for HTTPS. Click Yes.

Security A	lert	×
P	This page requires a secure connection which includes server authentication.	
	The Certificate Issuer for this site is untrusted or unknown. Do you wish to proceed?	
	Yes No View Certificate More Info	

9. A security window will pop up that requires the username and password to connect with On Premise AD RMS Server. Provide the credentials. Click **OK**.

Windows Security	×
Connecting to adrms-srv.hsmserver.com.	
HSMSERVER\nhollida •••••• Domain: HSMSERVER Remember my credentials	
Insert a smart card	
OK Can	cel

10. After verifying the credentials it will apply the label Confidential on the opened doc. It shows that it uses the Azure RMS label defined for AD RMS that uses On Premise AD RMS Server for verification of user account and licensing information.

	Westman Marine Marine	1 10 - 20 9
THE HOME INCERT DESIGN REAFLAVOUT REFERENCES MAILUNGS REVIEW VIEW	Letteranie - Mous (Lived	Nicole Hallida +
		al Atos +
Calbri (Body) • 11 • A* A* A* • 9 12 • 12 • 12 • 12 • 12	ANBECCER ANBECCER ANBECCE ANBECCE ANBECCE ANBECCE ANBECCE ANBECCE ANBECCE ANBECCE ANBECCE	CKDK A080CKDA A080CKDA A488CKDK A488CKDK A080CKDK
Parte Format Painter B J U + an X, X' A + Z + A + E = = = D + A + E + Pet	teet Thiormal This Spat Heading 1 Heading 2 Title Subtitle Subtle Em Emphasis Intense E	ng Quote Intense Q., Sobtle Ref., Intense Re., Book Title 🔽 👌 Select +
Clipboard IS Fort IS Paragraph IS Pro	ed	6 Eating A
🔖 Sensitivity: 📕 Confidential 🥆		×
This	doument is protected by On-Premise AD RMS and using the services from Azure RMS.	
	10.1	
	(A / %	
	/ 0////a.	
	6, 3/3/10.	
	PILLE 1,	
	ellin.	
	NIIV.	
	11.001	
	1811.0	
	0,7119	
	N/N/S	
	P ALLIN.	
	(()///	
	I AT I'	
PAGE 1 OF 1 15 WORDS DB ENGLISH (UNITED STATES)		単 図 時

- 11. Save this document at any shared location that is accessible by all domain users.
- 12. Logoff from the system and again login with another domain user.
- 13. Log on to ADRMS-CL as LHENIG. Open the document from the shared location. Click Yes when Security Alert window pop up.
- 14. A window for the credential will pop up. Provide the credentials for LHENIG and click OK.

Windows Security	×
Connecting to adrms-srv.hsmserver.com.	
HSMSERVER\LHENIG HSMSERVER\LHENIG Domain: HSMSERVER Remember my credentials	
Insert a smart card	
OK Can	cel

15. When the document opened click on the View Permission button to see the permission provided to the user you logged in.

FLE TOOLS VEW	TestAssive (Invid-Coty) - Wood (Trail)	X _ 5 X
ADRMS-SRV.HSMSERVER.COM On-Premise AD-RMS Server View Permission		х
Sensitivity: Confidential \		x
This document is protected by On-Premise AD RMS and using the services from Azure	RMS.	
	Drý sť moznest.	
	My Permission Tou are concernity authenticated to view this document File Filesop@filesiseer.com	
	ADBMS-SRV/nomenet.com - On-Premise AD-BMS Seher	
	You have the following permissions: View: Yes	
	Edit: No Copy: Tes	
	Print Tes Save: No	
	Lapart No Access the decument pergrammaticity Tes Full control No	
	Resect additional pressuonium OK	
304E0110F1		単 Ⅲ 略+ 14%
🚯 🙆 🗒 🔍 🔳		FN - 📷 🐨 4 10/2/2008

It successfully applied the Azure RMS labels with on premise AD RMS protection. When applying any label that is configured for the AD RMS (PREVIEW) in Azure portal it restricts the permission on the documents to domain users. No one other than your internal AD users can open the document. To open the documents RMS enabled application must connect with AD RMS server that is configured with on premise SafeNet Network HSM for storing the tenant key. When any request is coming for user license on AD RMS server HSM stored tenant key is used to sign the license.

It demonstrates how to use Azure HYOK feature for protecting the secret data. We have configured the built-in Azure RMS label (Confidential) for demonstration. However you can create your own label and configured it to use the on premise AD RMS for internal user and Azure RMS for external users or third party. To create a new label, log on to Azure portal and click on Azure Information Protection blade. You can find the "Add a new label" link on Azure Information Protection page below the built-in labels. Click on this link and add the required information to create a new label which uses on Premise AD RMS for protecting the documents.

