

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

- Preface 4
 - 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 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

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



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: <ul style="list-style-type: none"> • 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.)
<i>italic</i>	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	1-800-545-6608
	International	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 Knowledge Base.	

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

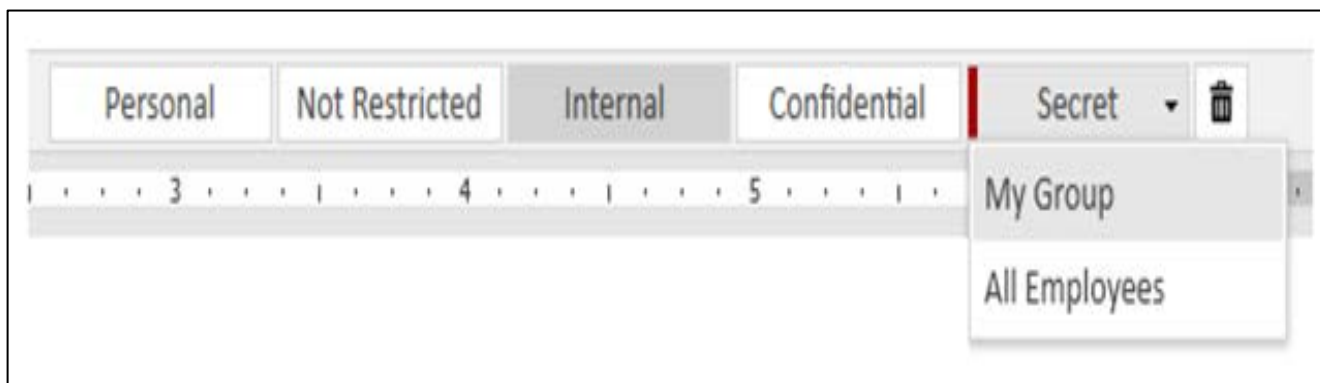
organizations to give control of keying material to Azure and store their keys in the Azure Cloud. For many organizations, this loss of control over keying material to a cloud provider limits their use of the cloud.

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.



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 Firmware 6.10.9 or 6.24.2 SafeNet HSM Client 6.2.1	Office 2013 SP1

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.

On premise AD RMS setup must have the following:

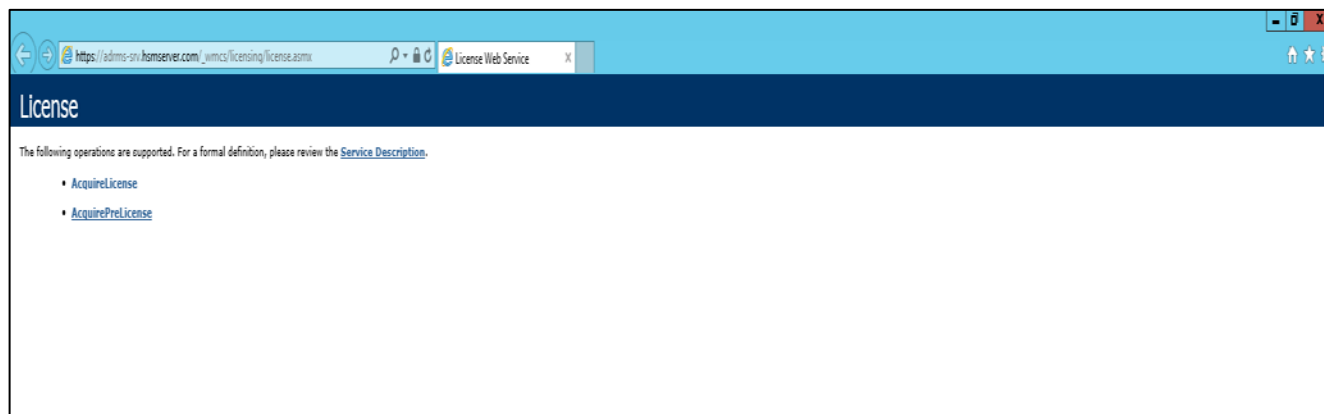
Operating System	Applications and Services	Description	Computer Name
Windows Server® 2012 R2 Enterprise	Active Directory, Domain Name System (DNS)	Domain Controller	ADRMS-DC
Windows Server® 2012 R2 Enterprise	AD RMS, Internet Information Services (IIS) 7.0, and Message Queuing	AD RMS Server	ADRMS-SRV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

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:

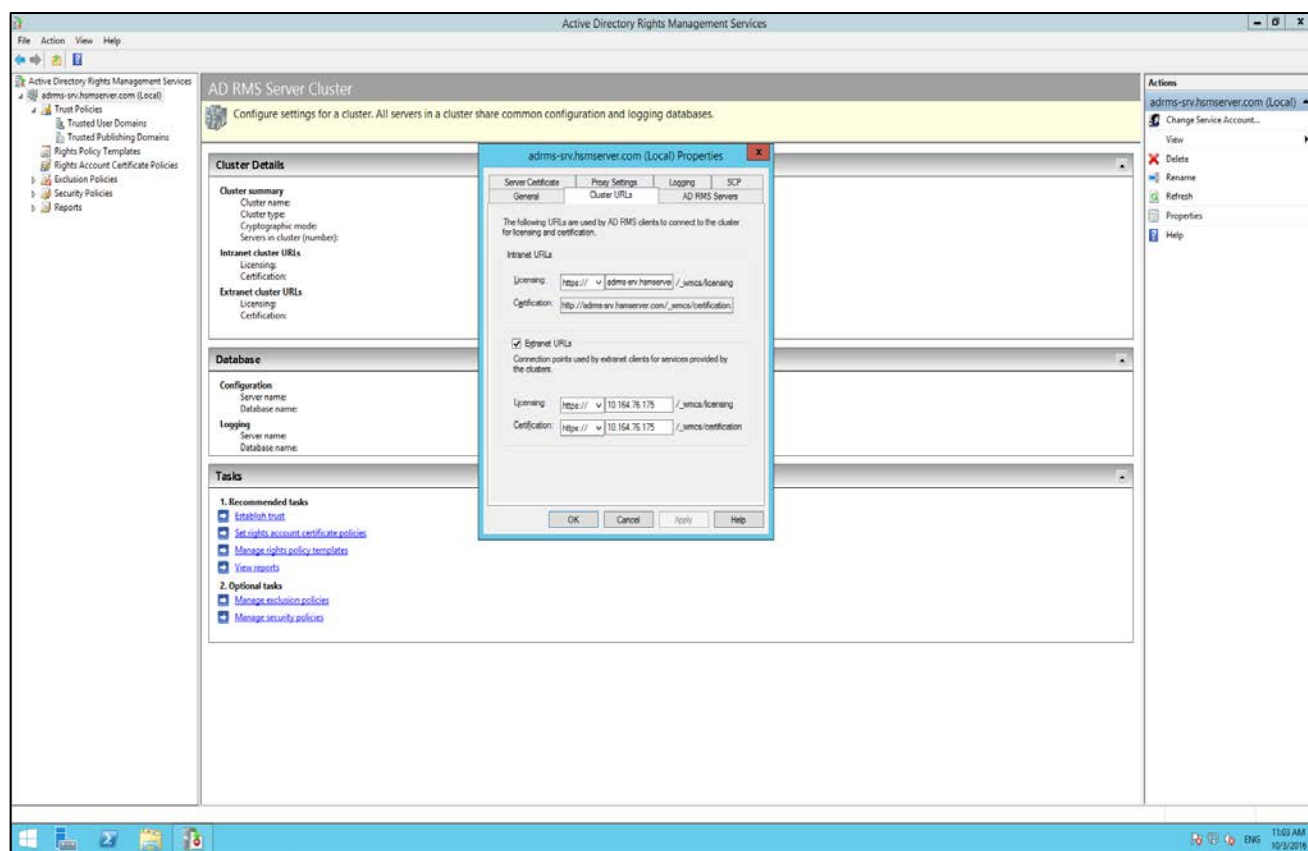
1. Log on to the ADRMS server as administrative permission.
2. Click **Start -> Administrative Tools -> Internet Information Services (IIS) Manager**.
3. Click on Server Name in the left pane tree and double click **Server Certificates**.
4. On the right side under **Actions** pane, click on the **Create 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.aspx



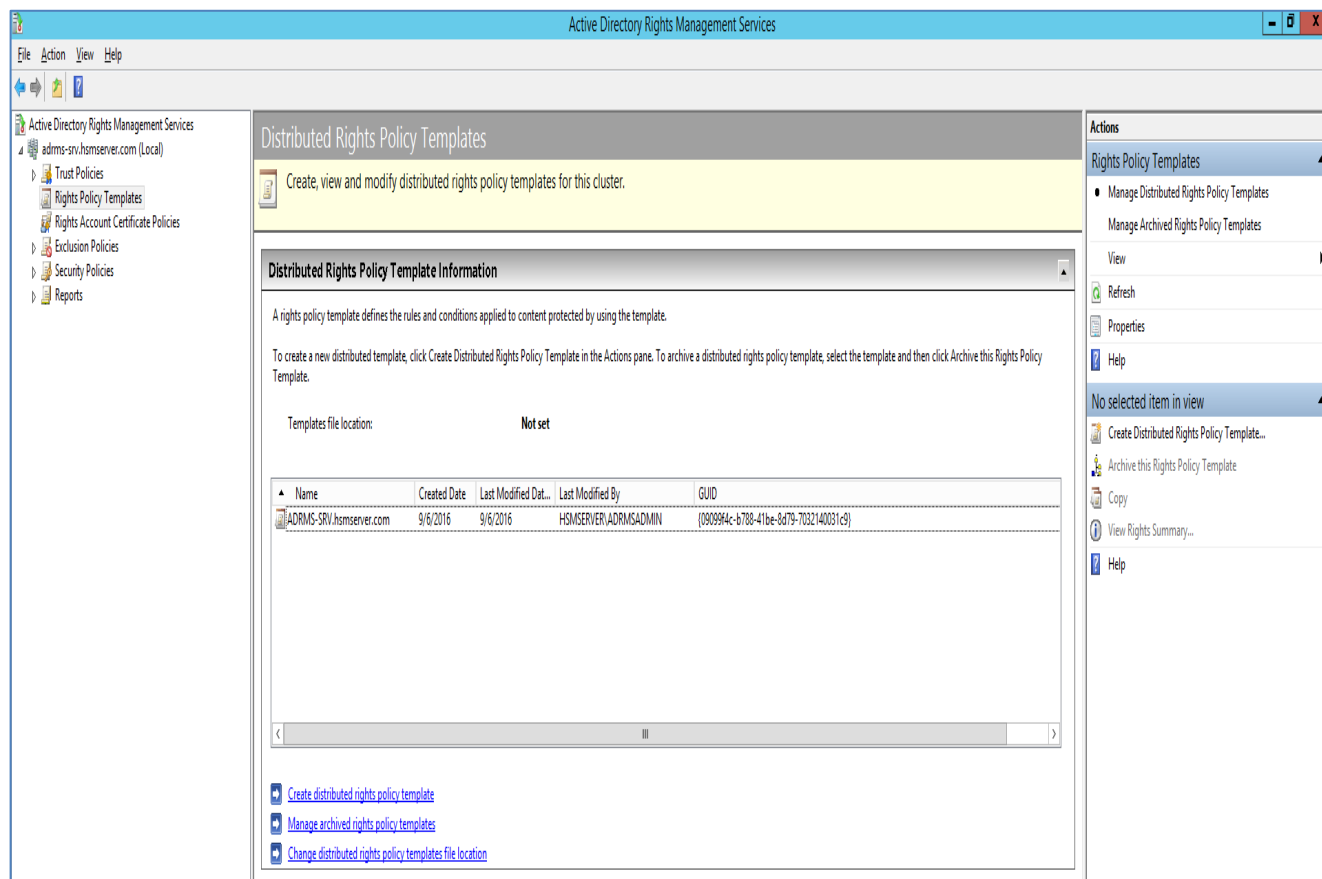
After configuring the ADRMS on HTTPS you need couple of settings to work with Azure HYOK. To do these settings follow the steps below:

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.



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.



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

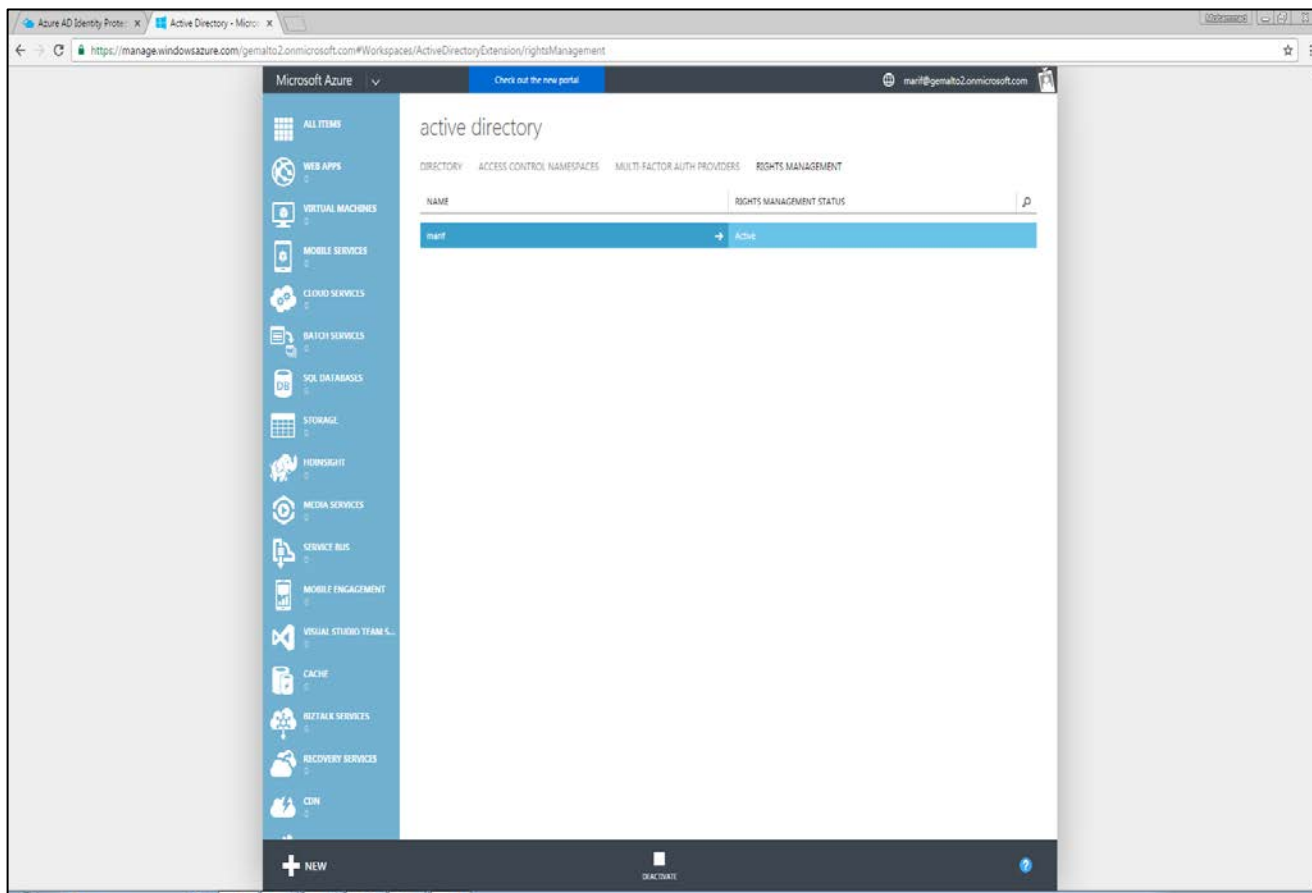
1. After you have signed up for your Azure account, sign in to the Azure classic portal. Use a global administrator account such as the account you used to get the subscription that includes Azure Rights Management.
2. In the left pane, click **ACTIVE DIRECTORY**.
3. From the active directory page, click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

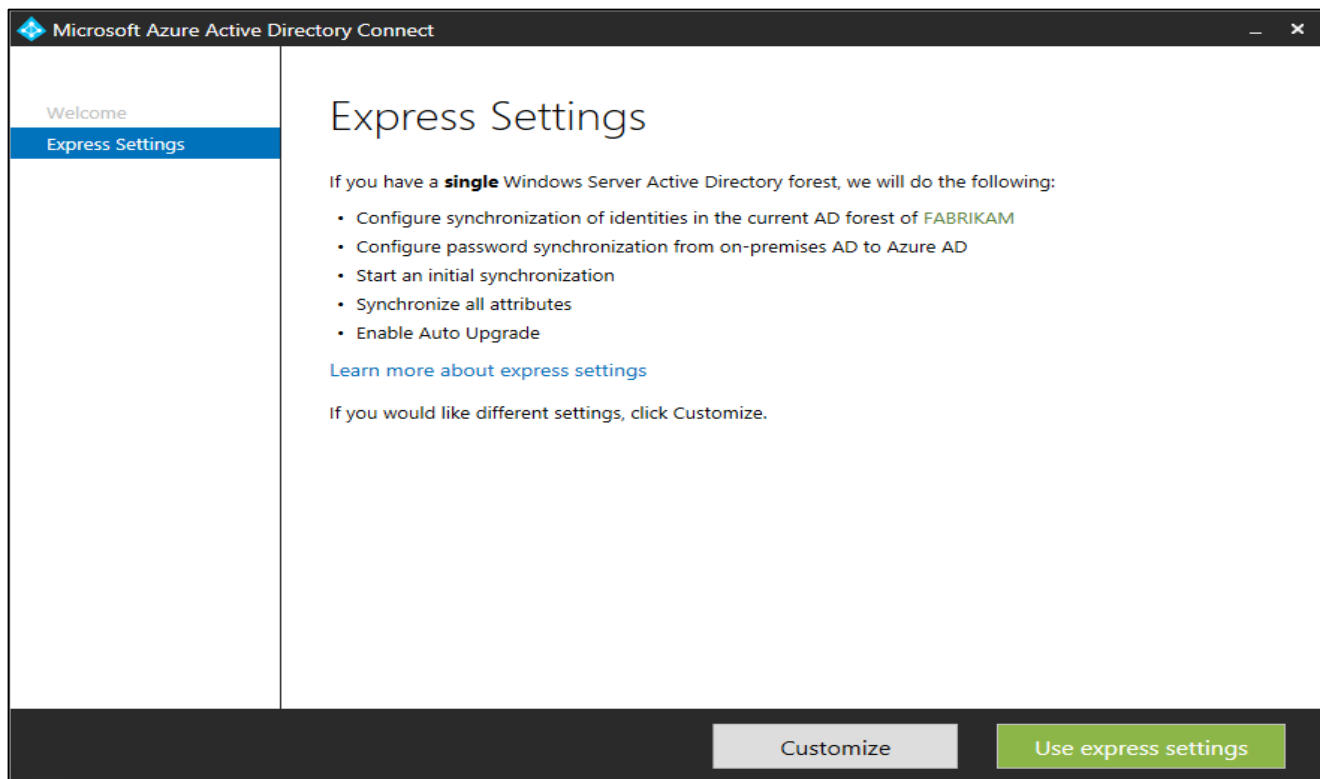


Next step is to synchronize Azure Active Directory and local Active Directory for password synchronization. To do this download the Azure AD Connect from Microsoft official site:

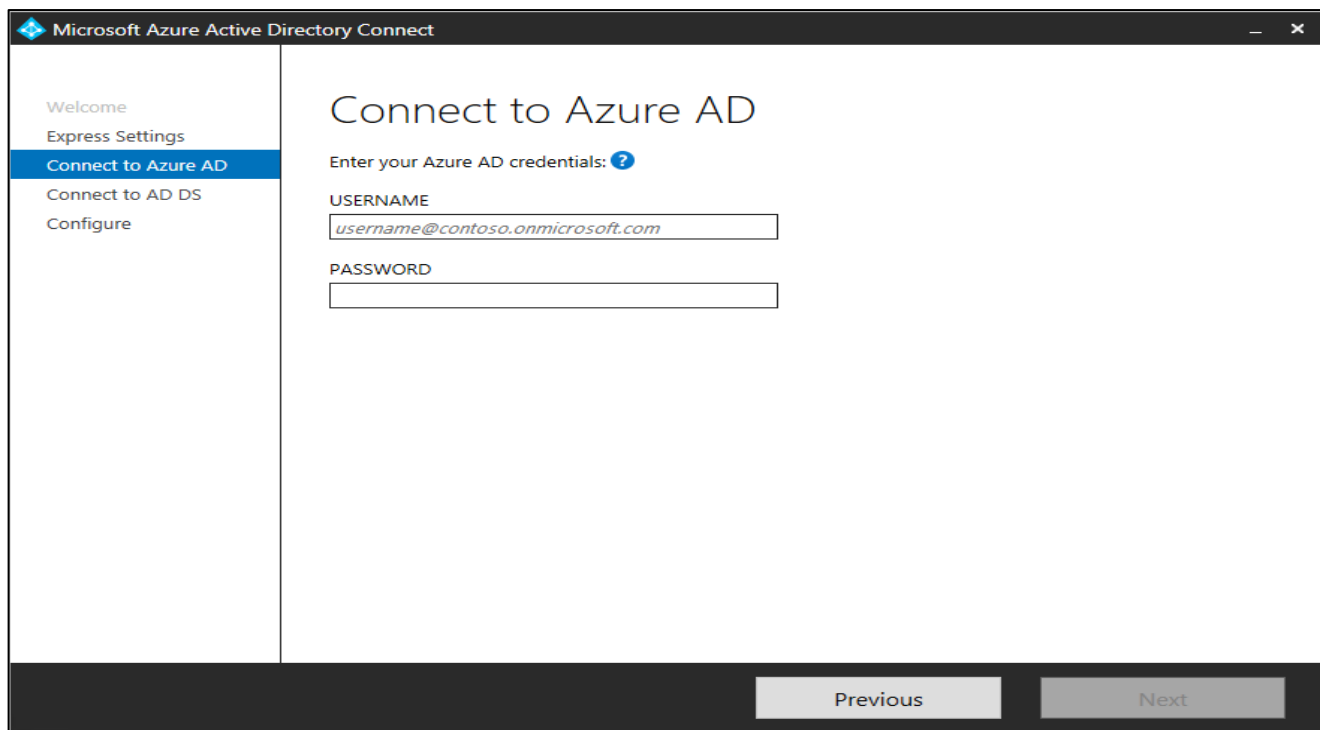
<https://www.microsoft.com/en-us/download/details.aspx?id=47594>

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**.

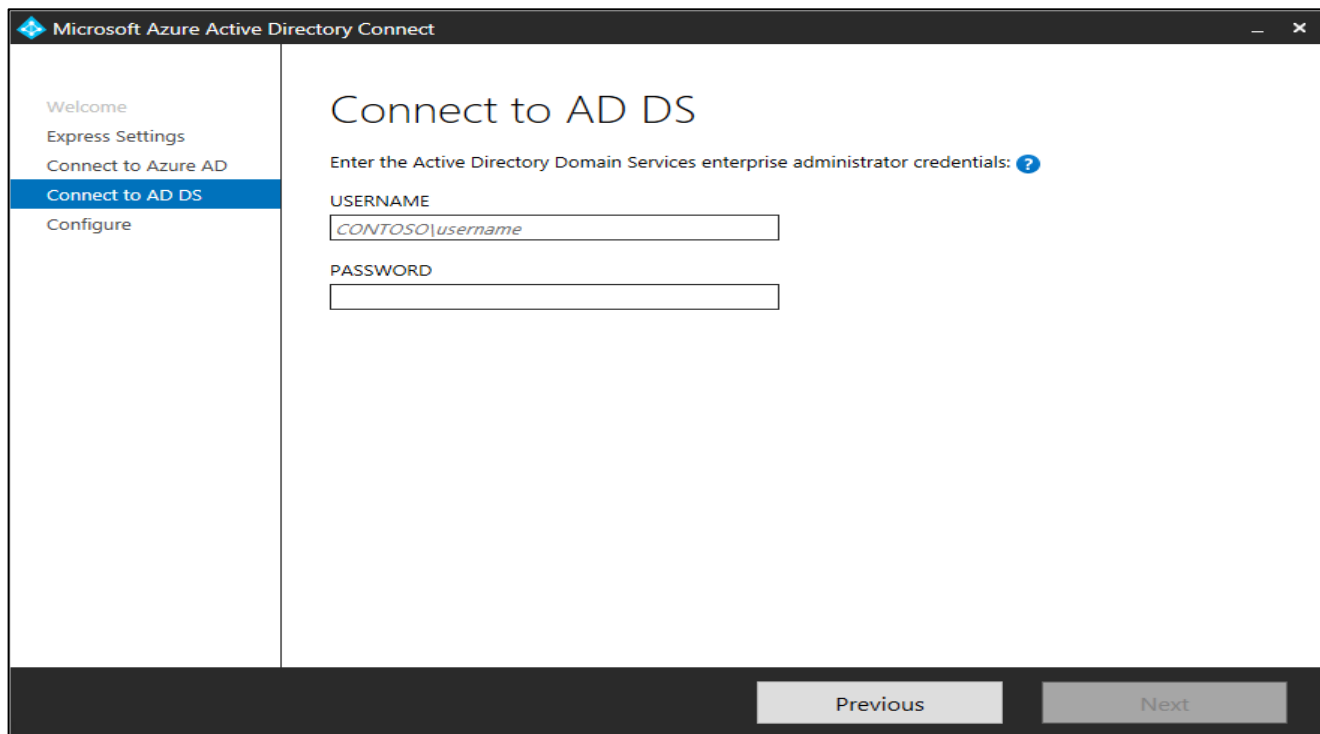
8. On the **Express Settings** screen, click **Use express settings**.



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

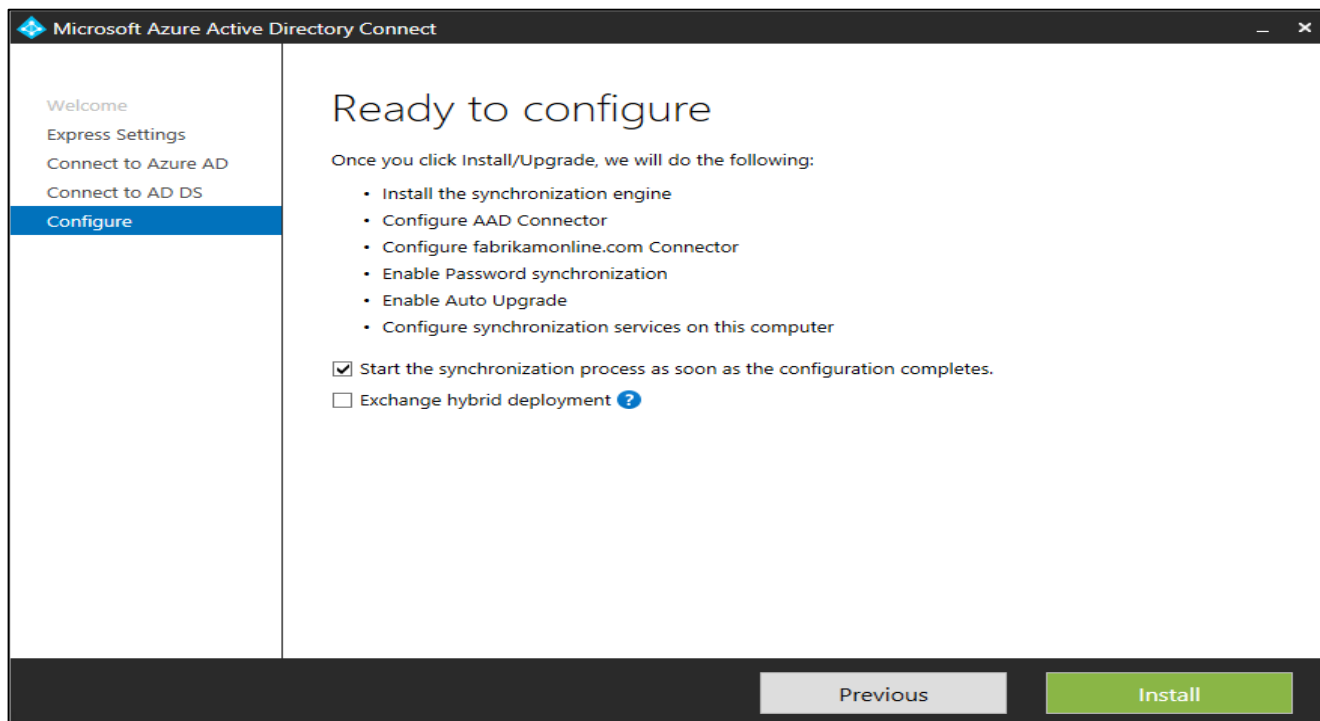


10. On the **Connect to AD DS** screen, enter the username and password for an enterprise admin account. Like HSMSEVER\Administrator and click **Next**.



The screenshot shows the 'Microsoft Azure Active Directory Connect' window. The left sidebar contains a navigation menu with the following items: 'Welcome', 'Express Settings', 'Connect to Azure AD', 'Connect to AD DS' (highlighted in blue), and 'Configure'. The main content area is titled 'Connect to AD DS' and contains the text 'Enter the Active Directory Domain Services enterprise administrator credentials: ?'. Below this text are two input fields: 'USERNAME' with the placeholder text 'CONTOSO\username' and 'PASSWORD'. At the bottom of the window, there are two buttons: 'Previous' and 'Next'.

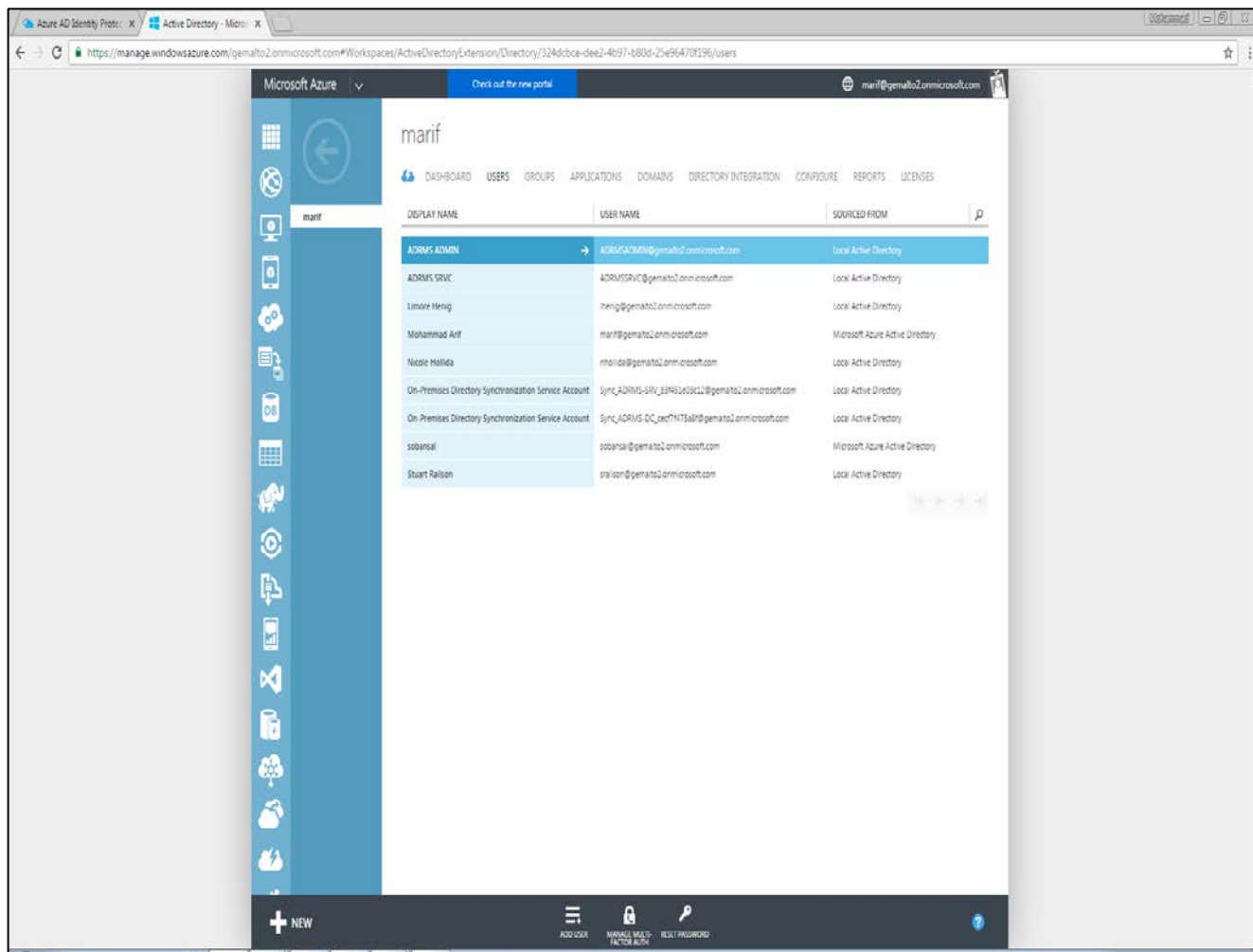
11. On the **Ready to configure** screen, select **Start the synchronization process as soon as the configuration completes**. Click **Install**.



The screenshot shows the 'Microsoft Azure Active Directory Connect' window. The left sidebar contains a navigation menu with the following items: 'Welcome', 'Express Settings', 'Connect to Azure AD', 'Connect to AD DS', and 'Configure' (highlighted in blue). The main content area is titled 'Ready to configure' and contains the text 'Once you click Install/Upgrade, we will do the following:'. Below this text is a list of actions: 'Install the synchronization engine', 'Configure AAD Connector', 'Configure fabrikamonline.com Connector', 'Enable Password synchronization', 'Enable Auto Upgrade', and 'Configure synchronization services on this computer'. There are two checkboxes: 'Start the synchronization process as soon as the configuration completes.' (checked) and 'Exchange hybrid deployment ?' (unchecked). At the bottom of the window, there are two buttons: 'Previous' and 'Install'.

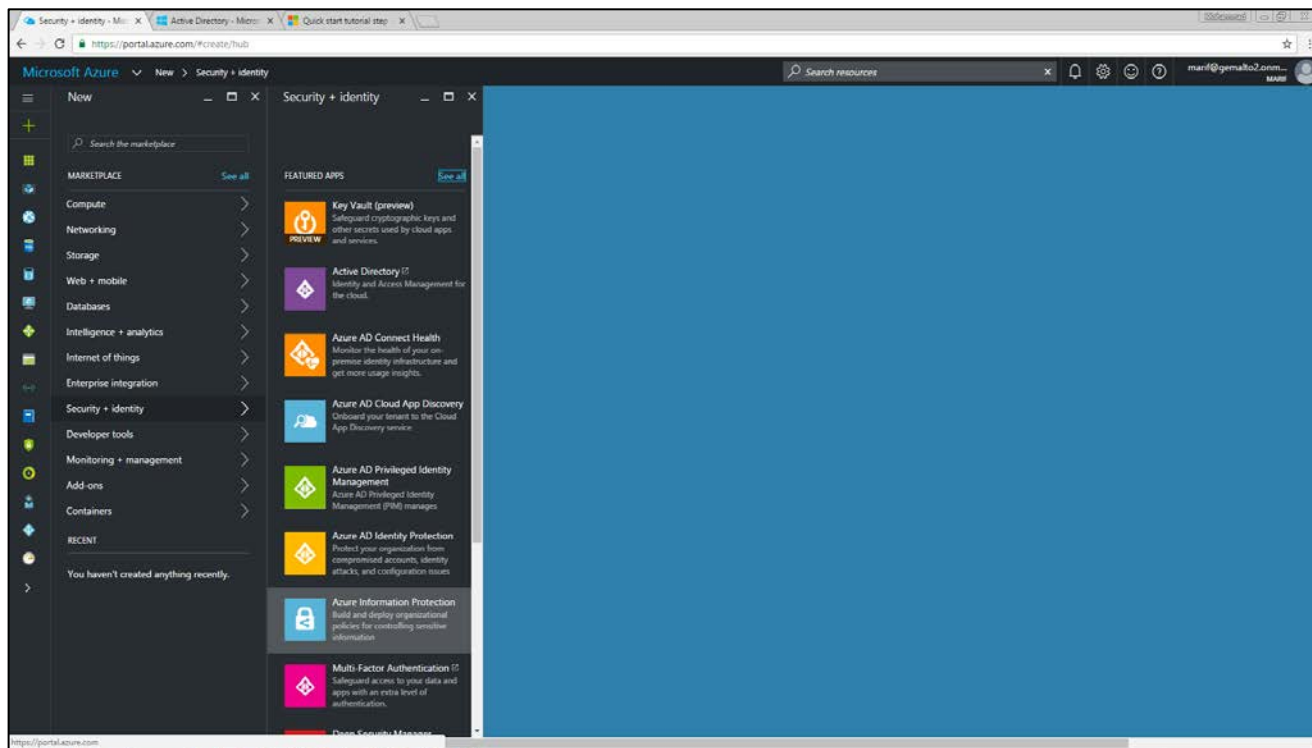
12. When the installation completes, click **Exit**.

- 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.

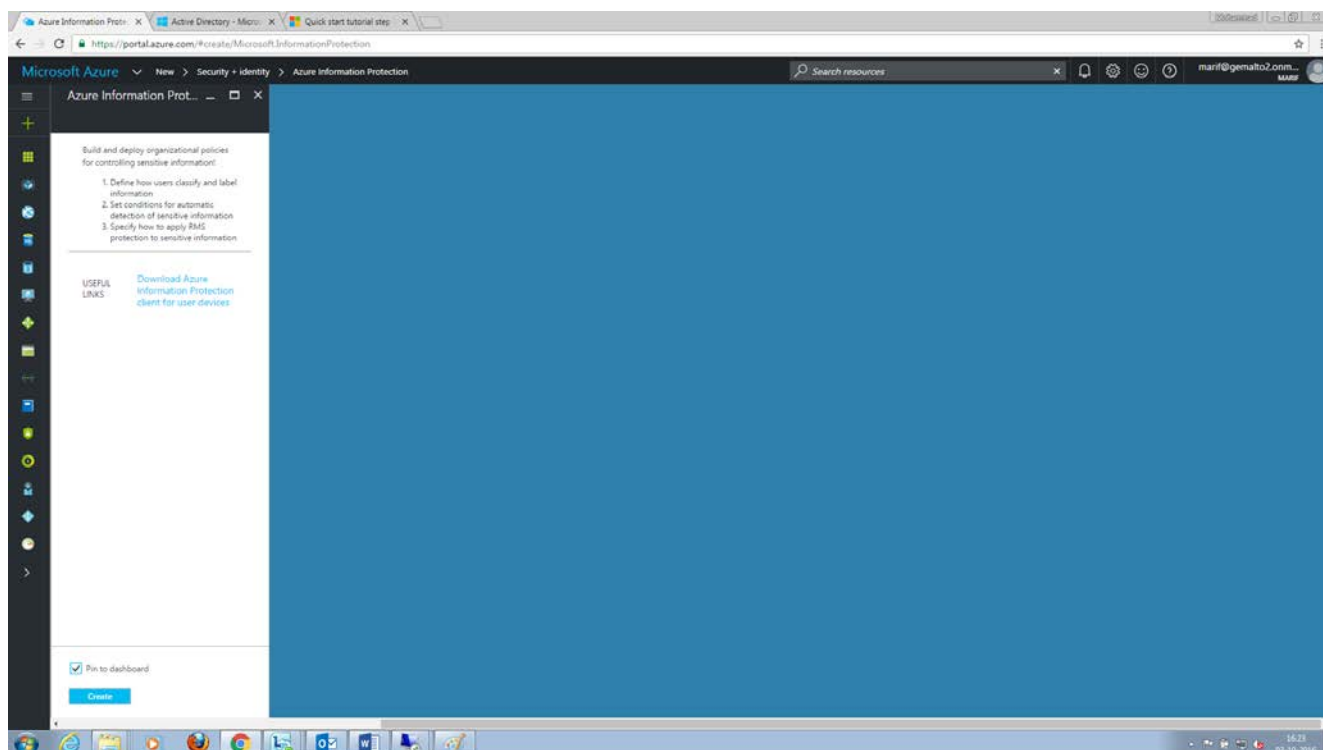


- Now log on to Microsoft Azure Portal and create Azure RMS Protection policy using the steps provided below.
- In a new browser window, sign in to the Azure portal as a global admin for your tenant.

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

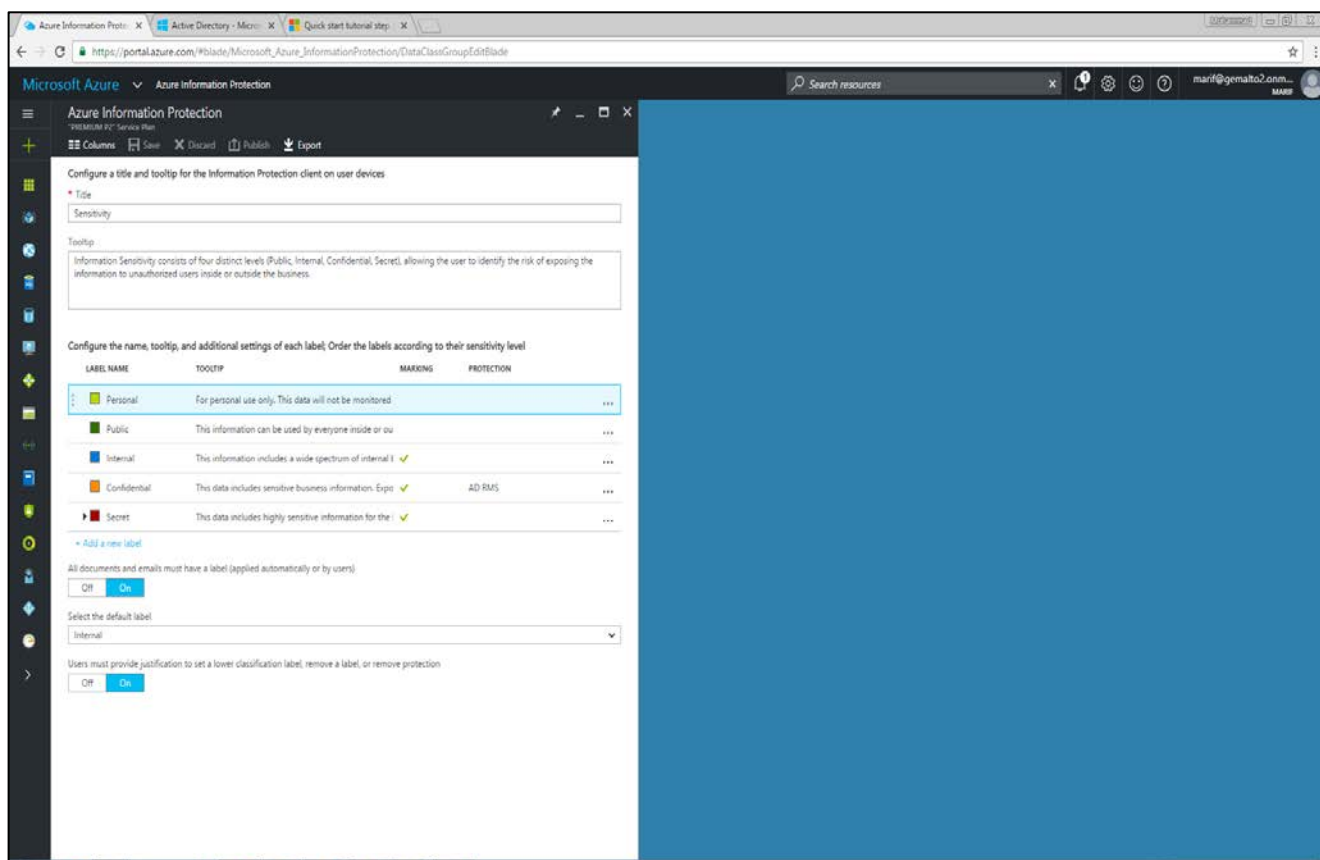


17. Select **Pin to dashboard** to create an Azure Information Protection tile on your dashboard, so that you can skip browsing to the service the next time you sign in to the portal. Click **Create**.



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**.

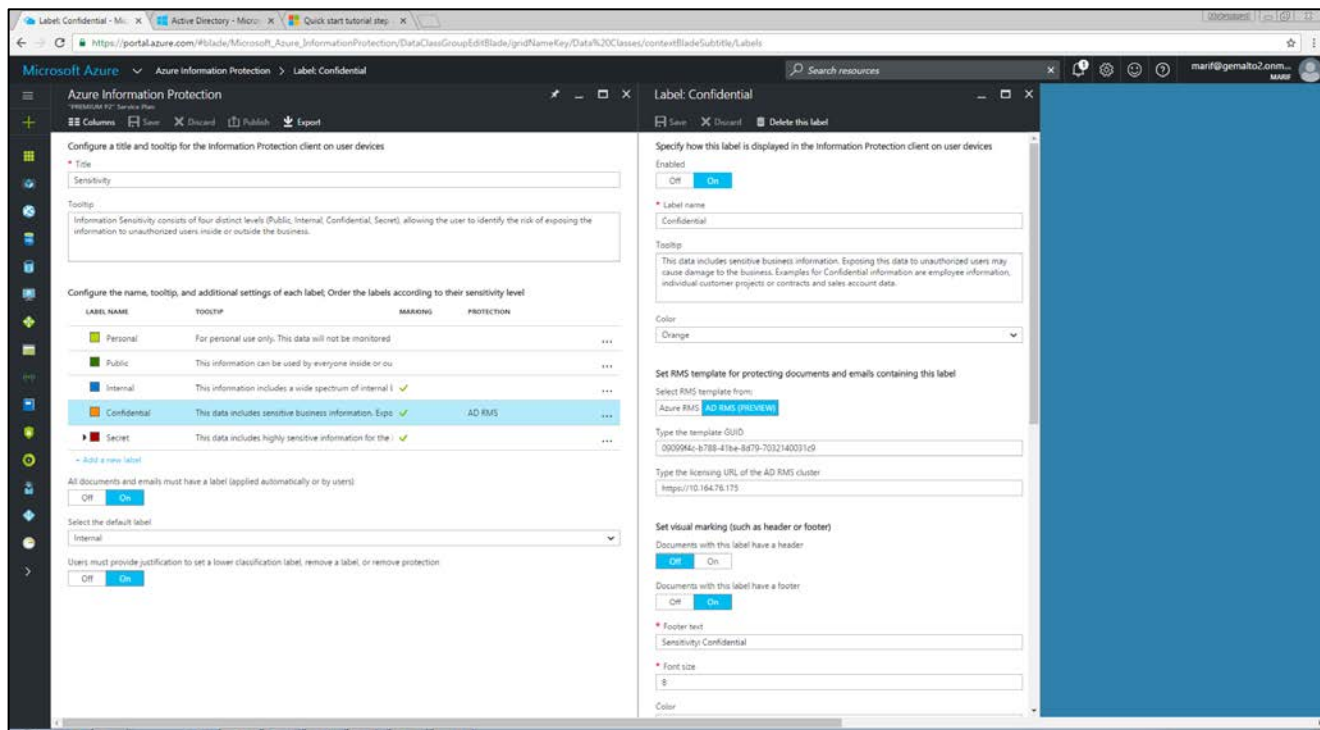


Configuring a label for protection, a watermark, and a condition to prompt for classification

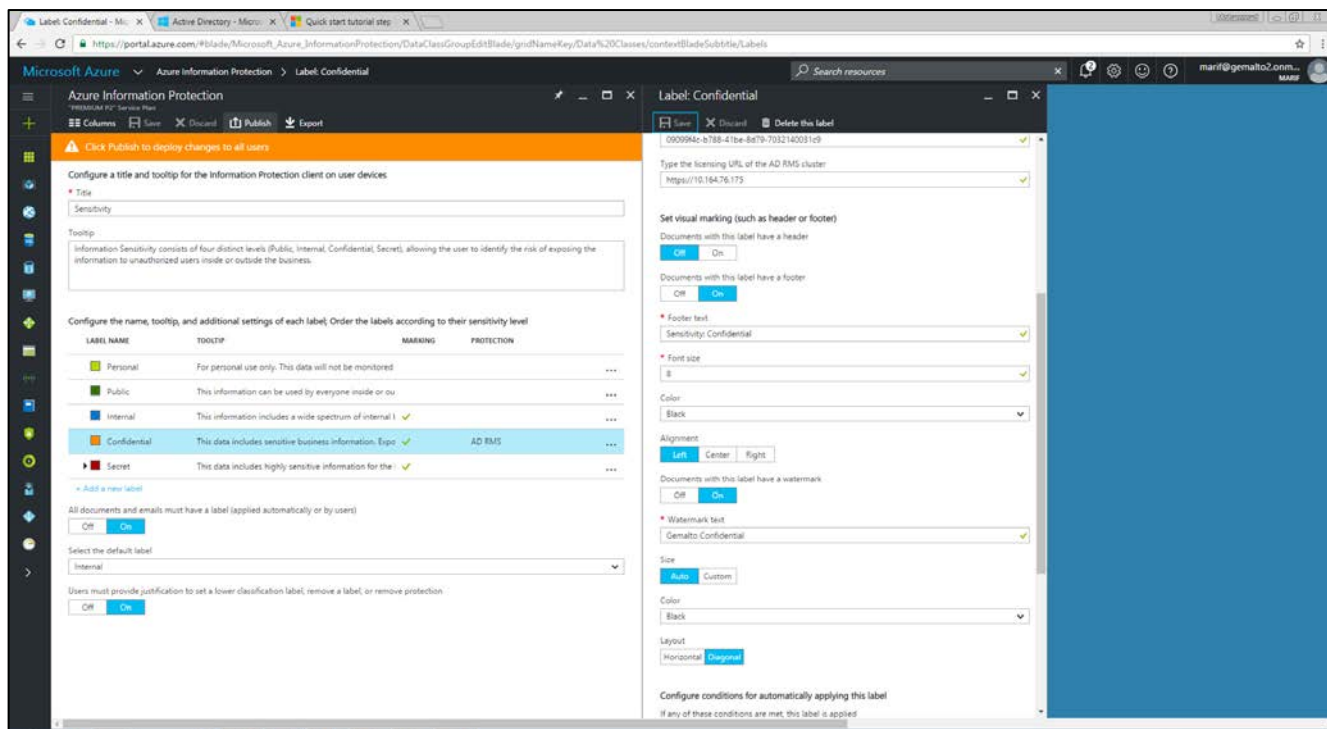
Now, you need to change the settings of one of the labels, **Confidential**:

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.



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



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.

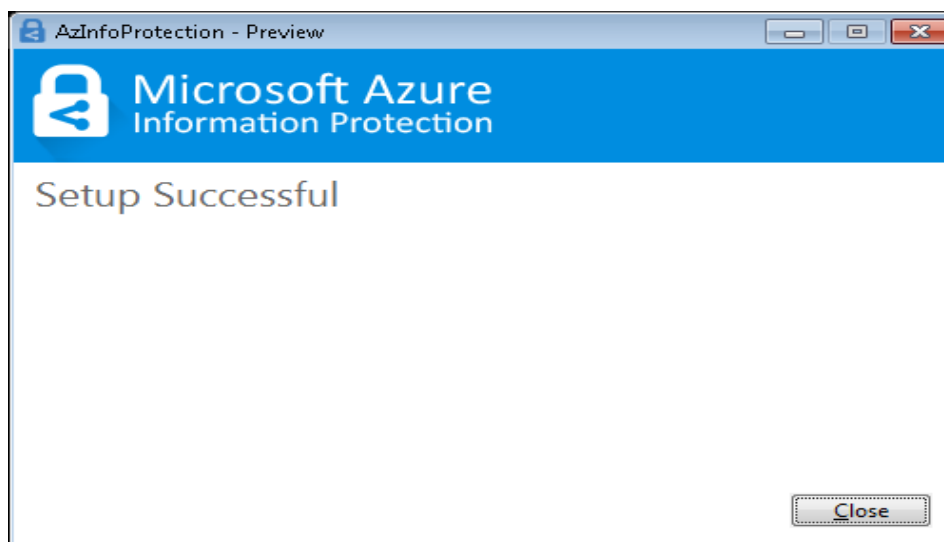
Above updates are needed to install the Azure Information Protection Client. You can download the Azure Information Protection Client from Microsoft download center.

<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**.



3. Click **Close** when installation finish.



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

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

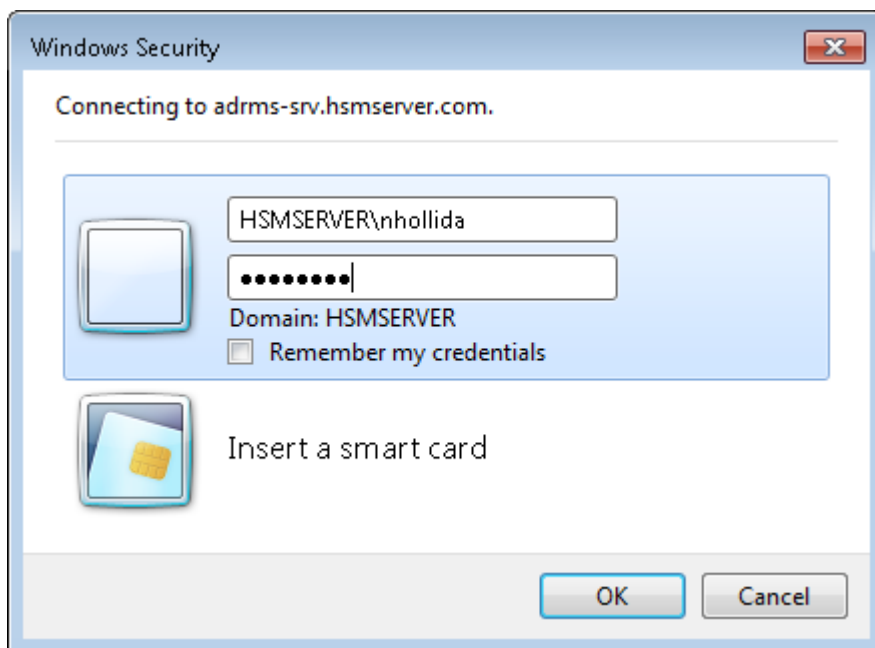


NOTE: If AD RMS setup is done as per the AD RMS Integration Guide then all these users would be there.

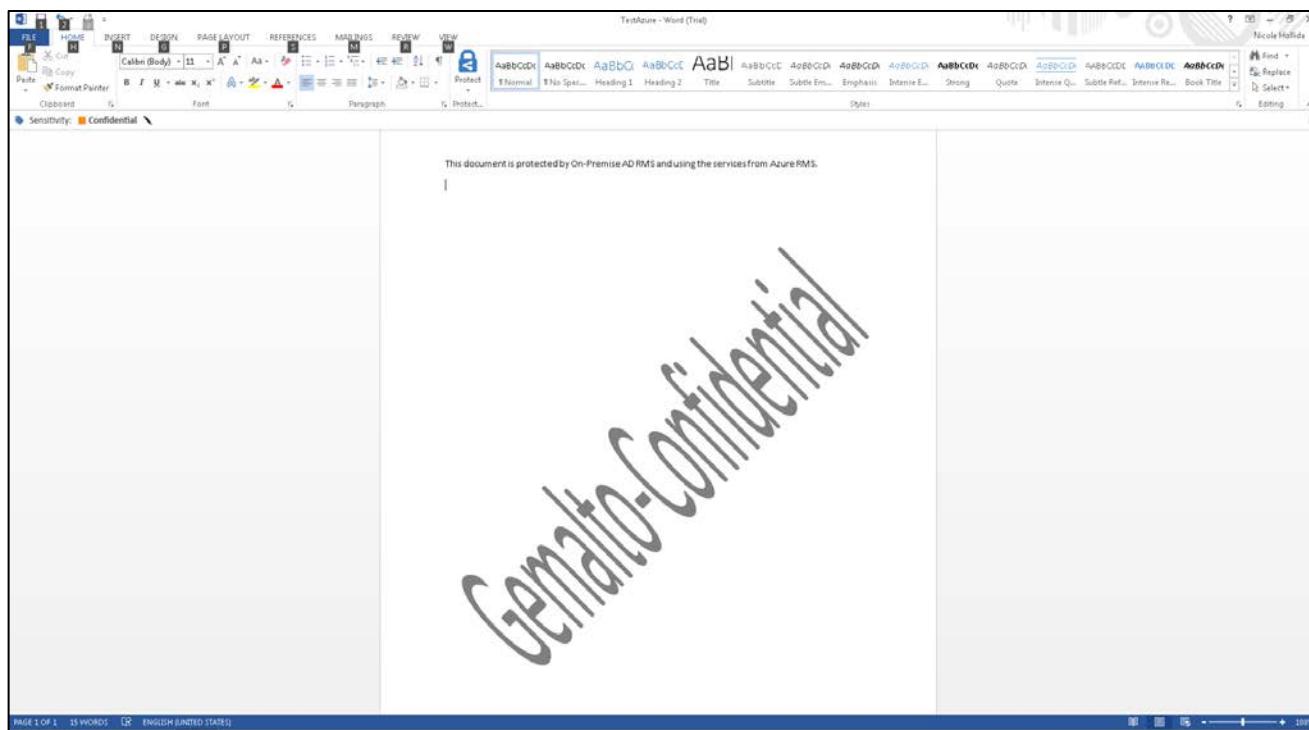
6. Create a new word document and write something in the document. You can see the Azure Information Protection labels in the document.
7. Click on the **Confidential** that you configured for **AD RMS (PREVIEW)** in Azure Portal.
8. A security alert message will display as you are using the self-signed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



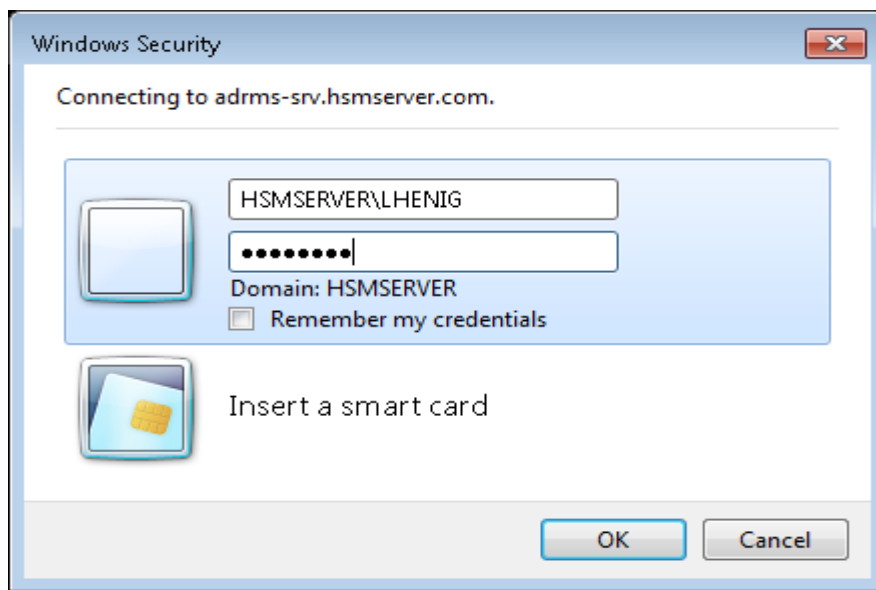
9. A security window will pop up that requires the username and password to connect with On Premise AD RMS Server. Provide the credentials. Click **OK**.



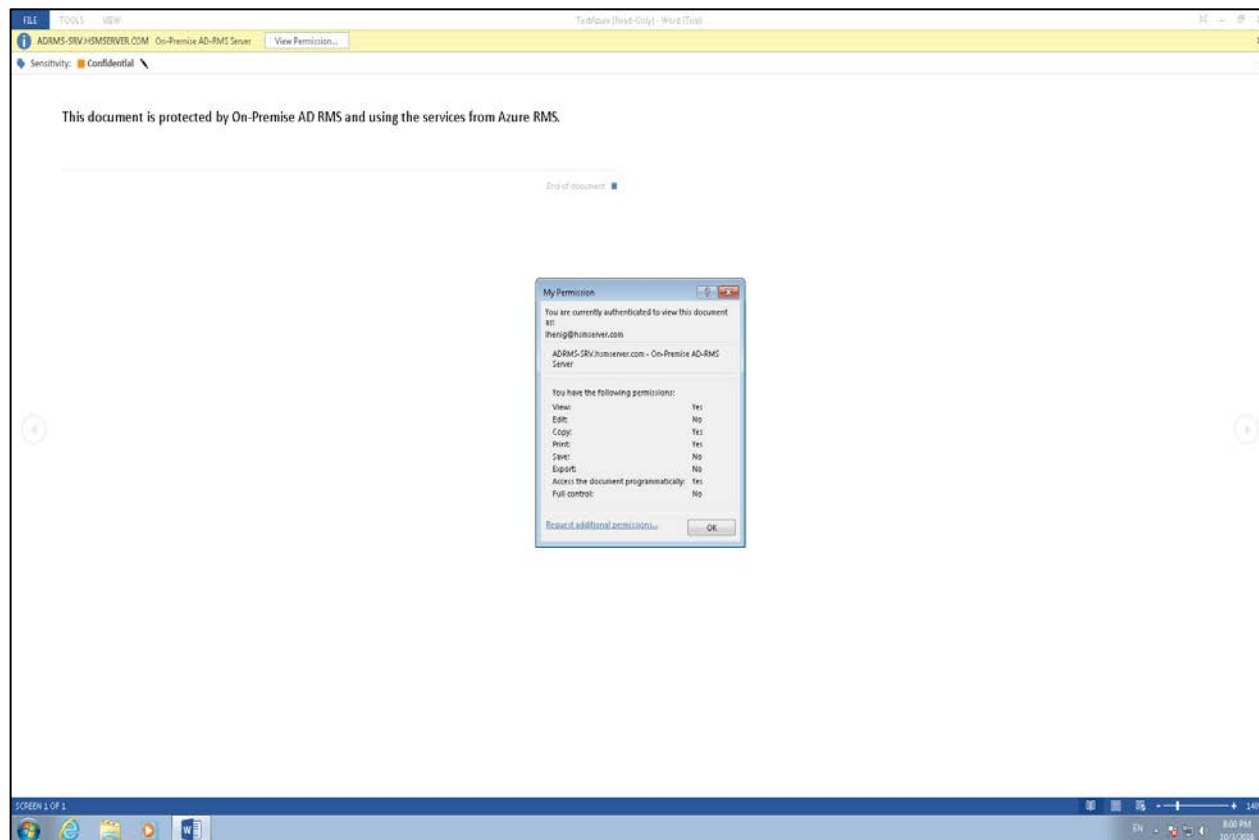
10. After verifying the credentials it will apply the label Confidential on the opened doc. It shows that it uses the Azure RMS label defined for AD RMS that uses On Premise AD RMS Server for verification of user account and licensing information.



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 **AD RMS-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**.



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



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.

