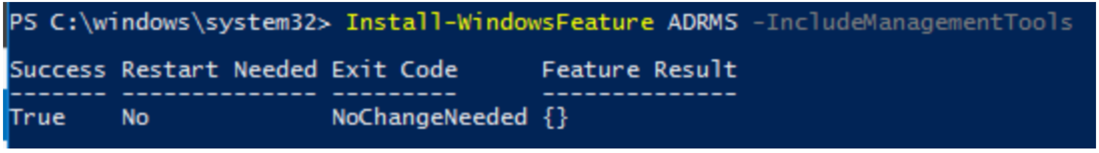
ADRMS
=======

1. Install AD RMS role and related management tool

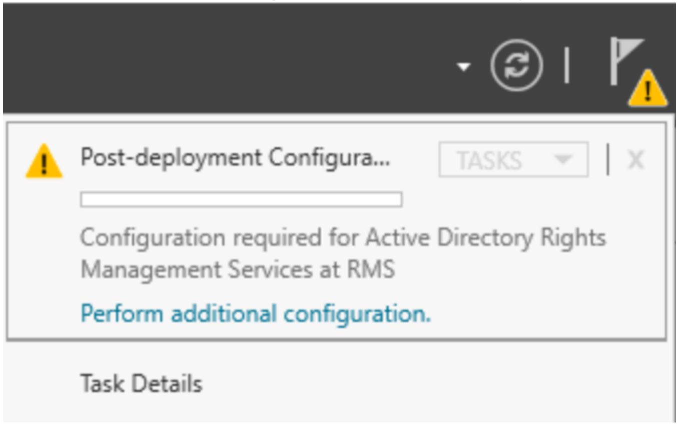
   Install-WindowsFeature ADRMS -IncludeManagementTools



```
PS C:\windows\system32> Install-WindowsFeature ADRMS -IncludeManagementTools

Success Restart Needed Exit Code      Feature Result
------- -------------- ---------      --------------
True    No             NoChangeNeeded {}
```

2. Launch server manager -> notification -> perform additional configuration

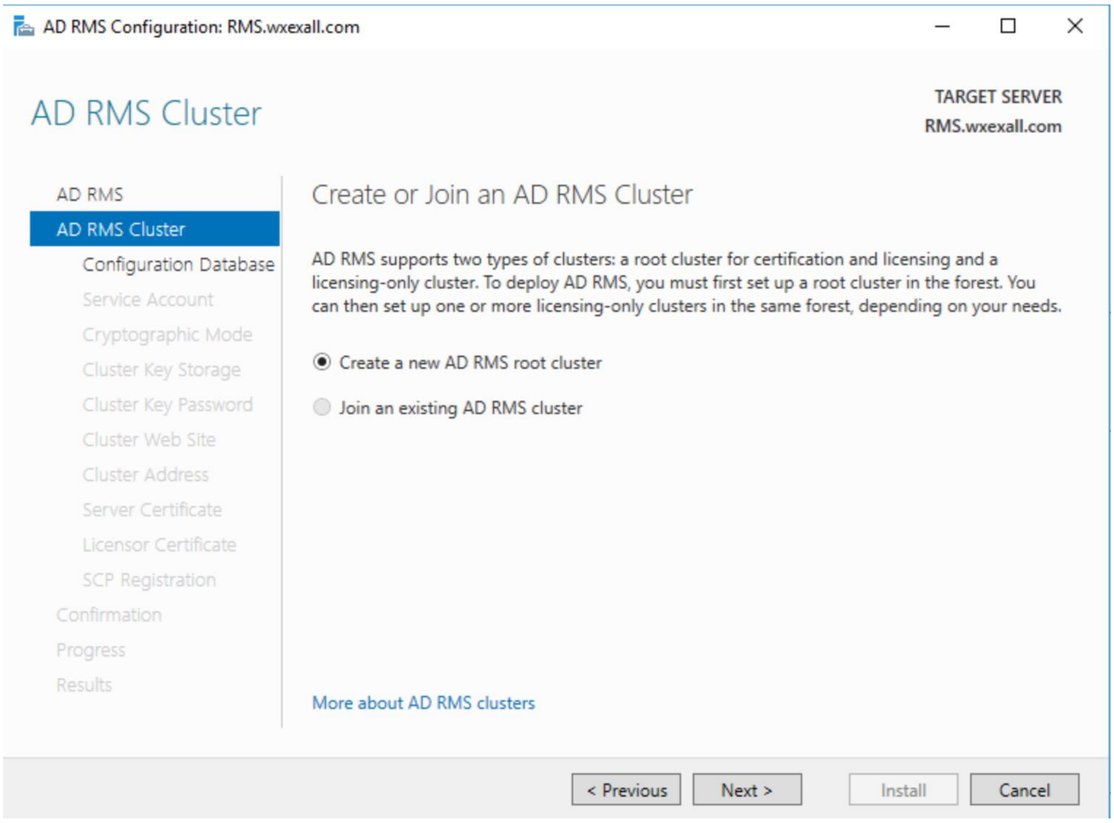


Post-deployment Configura...

Configuration required for Active Directory Rights Management Services at RMS

Perform additional configuration.

3. Choose "create a new AD RMS root cluster"



AD RMS Configuration: RMS.wxexall.com

AD RMS Cluster

TARGET SERVER
RMS.wxexall.com

Create or Join an AD RMS Cluster

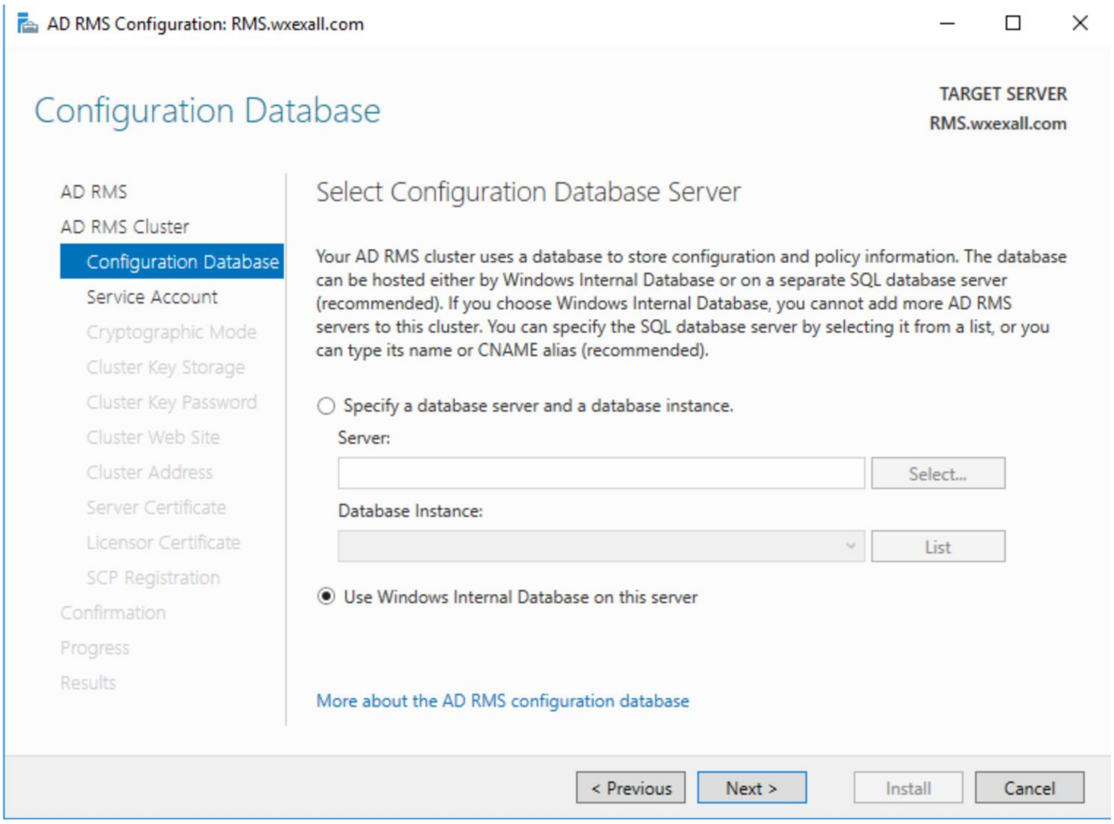
AD RMS supports two types of clusters: a root cluster for certification and licensing and a licensing-only cluster. To deploy AD RMS, you must first set up a root cluster in the forest. You can then set up one or more licensing-only clusters in the same forest, depending on your needs.

● Create a new AD RMS root cluster

○ Join an existing AD RMS cluster

More about AD RMS clusters

4. Choose "use windows internal database on this server" since we don't have SQL server database here



AD RMS Configuration: RMS.wxexall.com

Configuration Database

TARGET SERVER
RMS.wxexall.com

Select Configuration Database Server

Your AD RMS cluster uses a database to store configuration and policy information. The database can be hosted either by Windows Internal Database or on a separate SQL database server (recommended). If you choose Windows Internal Database, you cannot add more AD RMS servers to this cluster. You can specify the SQL database server by selecting it from a list, or you can type its name or CNAME alias (recommended).

○ Specify a database server and a database instance.

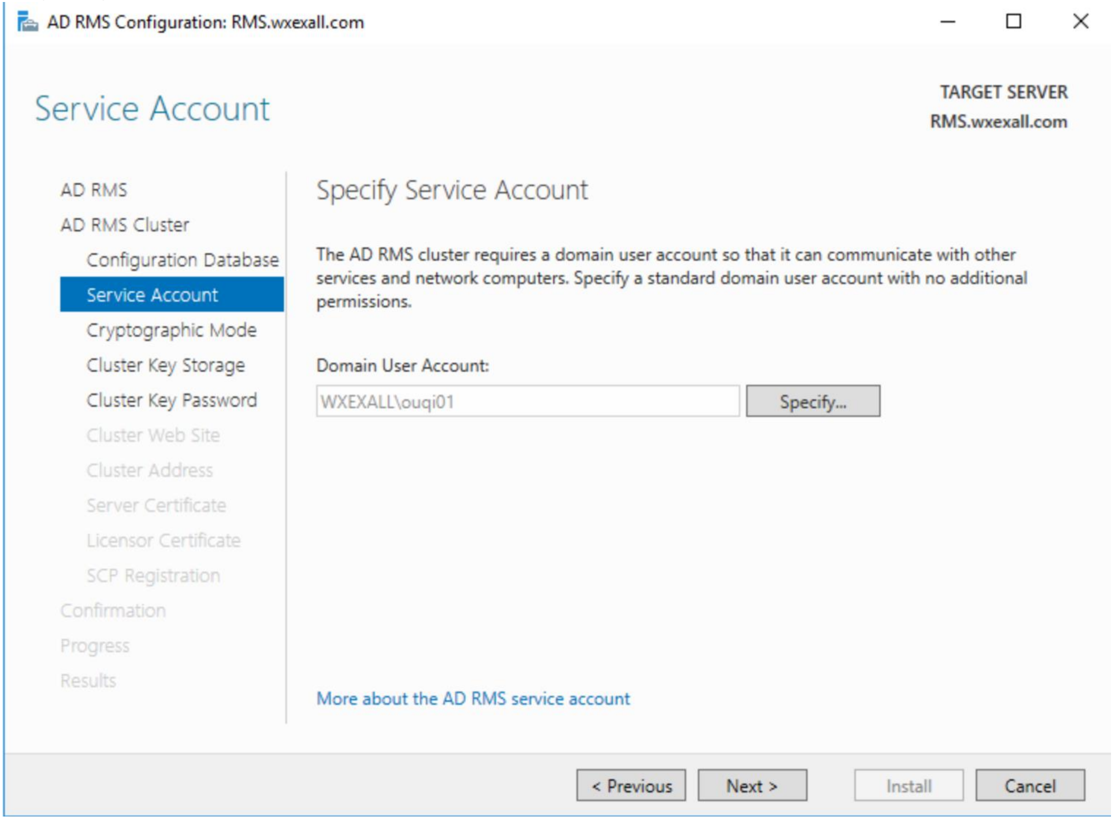
Server:

Database Instance:

● Use Windows Internal Database on this server

More about the AD RMS configuration database

5. Specify a service account



AD RMS Configuration: RMS.wxexall.com

Service Account

TARGET SERVER
RMS.wxexall.com

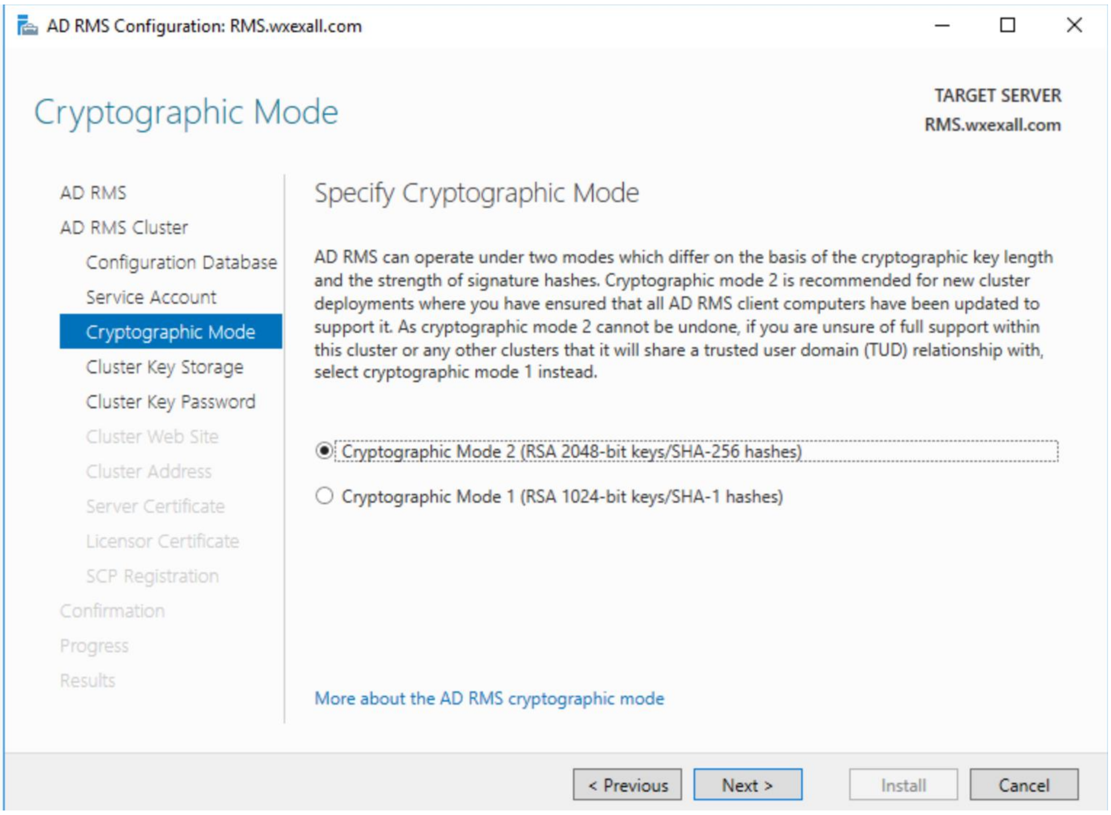
Specify Service Account

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

Domain User Account: WXEXALL\ouqi01

More about the AD RMS service account

6. Select Cryptographic mode 2



AD RMS Configuration: RMS.wxexall.com

Cryptographic Mode

TARGET SERVER
RMS.wxexall.com

Specify Cryptographic Mode

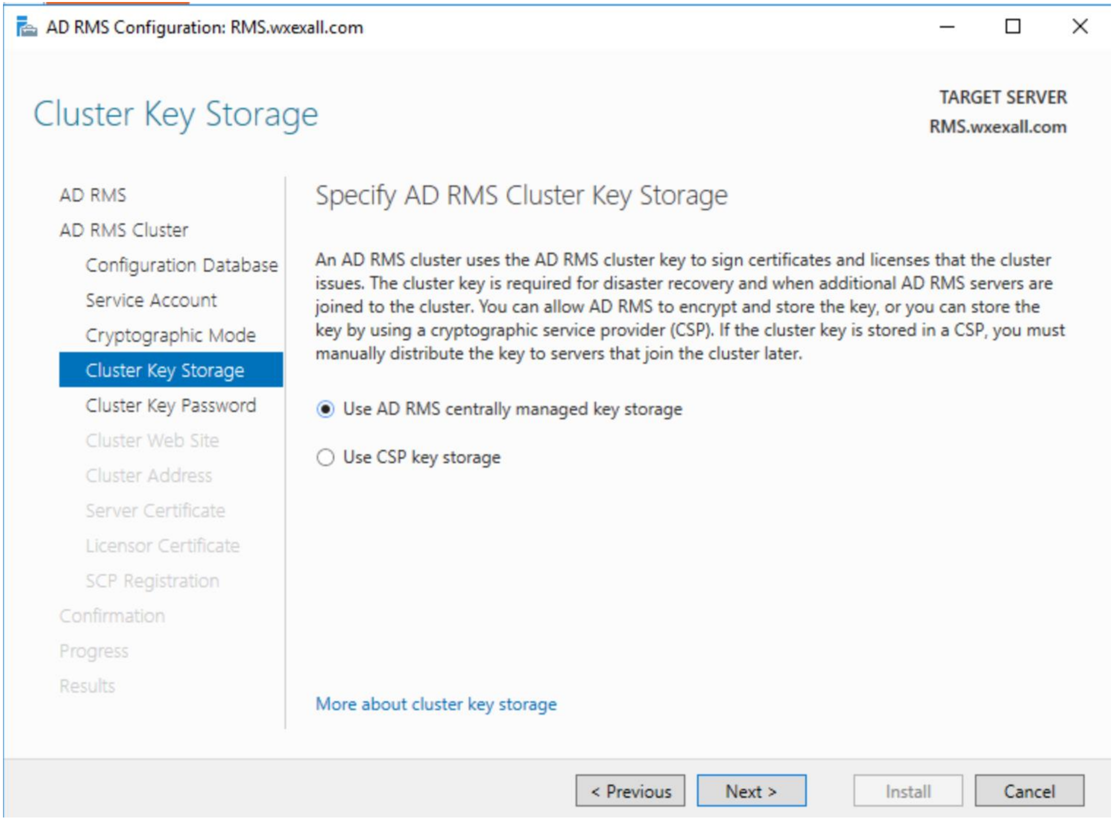
AD RMS can operate under two modes which differ on the basis of the cryptographic key length and the strength of signature hashes. Cryptographic mode 2 is recommended for new cluster deployments where you have ensured that all AD RMS client computers have been updated to support it. As cryptographic 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.

● Cryptographic Mode 2 (RSA 2048-bit keys/SHA-256 hashes)

○ Cryptographic Mode 1 (RSA 1024-bit keys/SHA-1 hashes)

More about the AD RMS cryptographic mode

7. Select "use AD RMS centrally managed key storage" here



AD RMS Configuration: RMS.wxexall.com

Cluster Key Storage

TARGET SERVER
RMS.wxexall.com

Specify AD RMS Cluster Key Storage

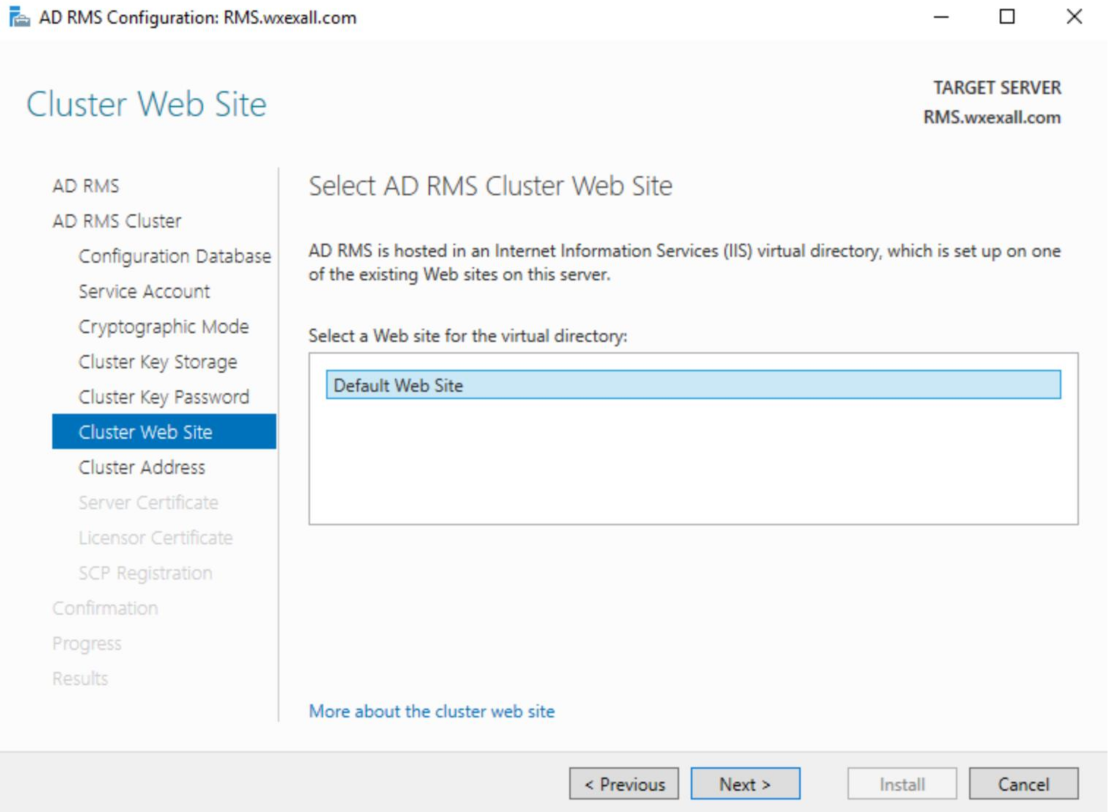
An AD RMS cluster uses the AD RMS cluster key to sign certificates and licenses that the cluster issues. The cluster key is required for disaster recovery and when additional AD RMS servers are joined to the cluster. You can allow AD RMS to encrypt and store the key, or you can store the key by using a cryptographic service provider (CSP). If the cluster key is stored in a CSP, you must manually distribute the key to servers that join the cluster later.

● Use AD RMS centrally managed key storage

○ Use CSP key storage

More about cluster key storage

8. Select the web site



Cluster Web Site

TARGET SERVER
RMS.wxexall.com

Select AD RMS Cluster Web Site

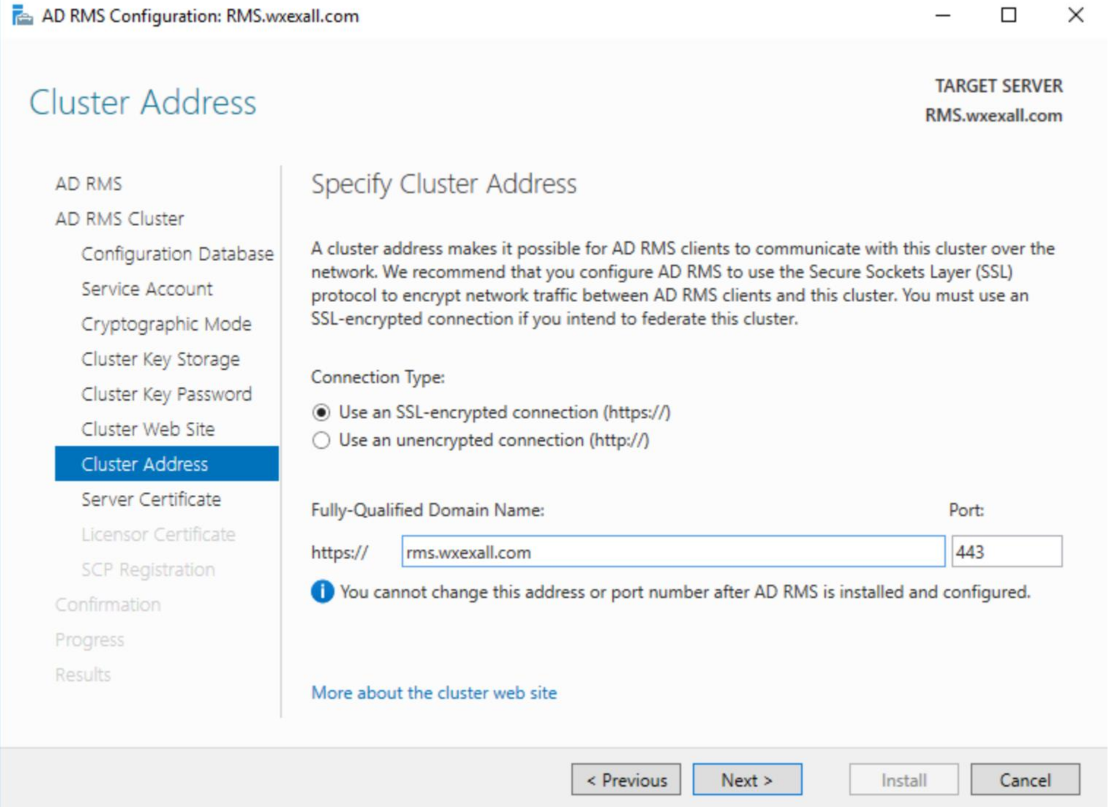
AD RMS is hosted in an Internet Information Services (IIS) virtual directory, which is set up on one of the existing Web sites on this server.

Select a Web site for the virtual directory:

Default Web Site

More about the cluster web site

9. Enter the address



Cluster Address

TARGET SERVER
RMS.wxexall.com

Specify Cluster Address

A cluster address makes it possible for AD RMS clients to communicate with this cluster over the network. We recommend that you configure AD RMS to use the Secure Sockets Layer (SSL) protocol to encrypt network traffic between AD RMS clients and this cluster. You must use an SSL-encrypted connection if you intend to federate this cluster.

Connection Type:

● Use an SSL-encrypted connection (https://)
○ Use an unencrypted connection (http://)

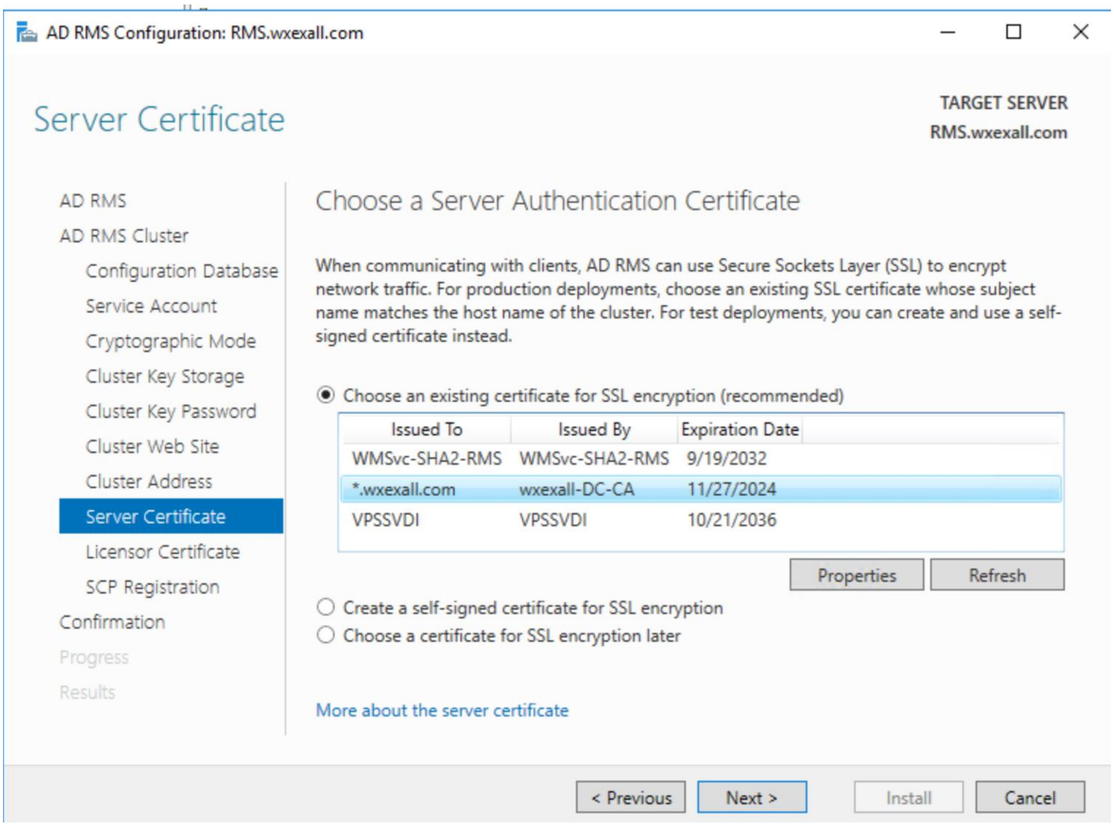
Fully-Qualified Domain Name: https:// rms.wxexall.com

Port: 443

You cannot change this address or port number after AD RMS is installed and configured.

More about the cluster web site

10. Select the certificate



AD RMS Configuration: RMS.wxexall.com

Server Certificate

TARGET SERVER
RMS.wxexall.com

Choose a Server Authentication Certificate

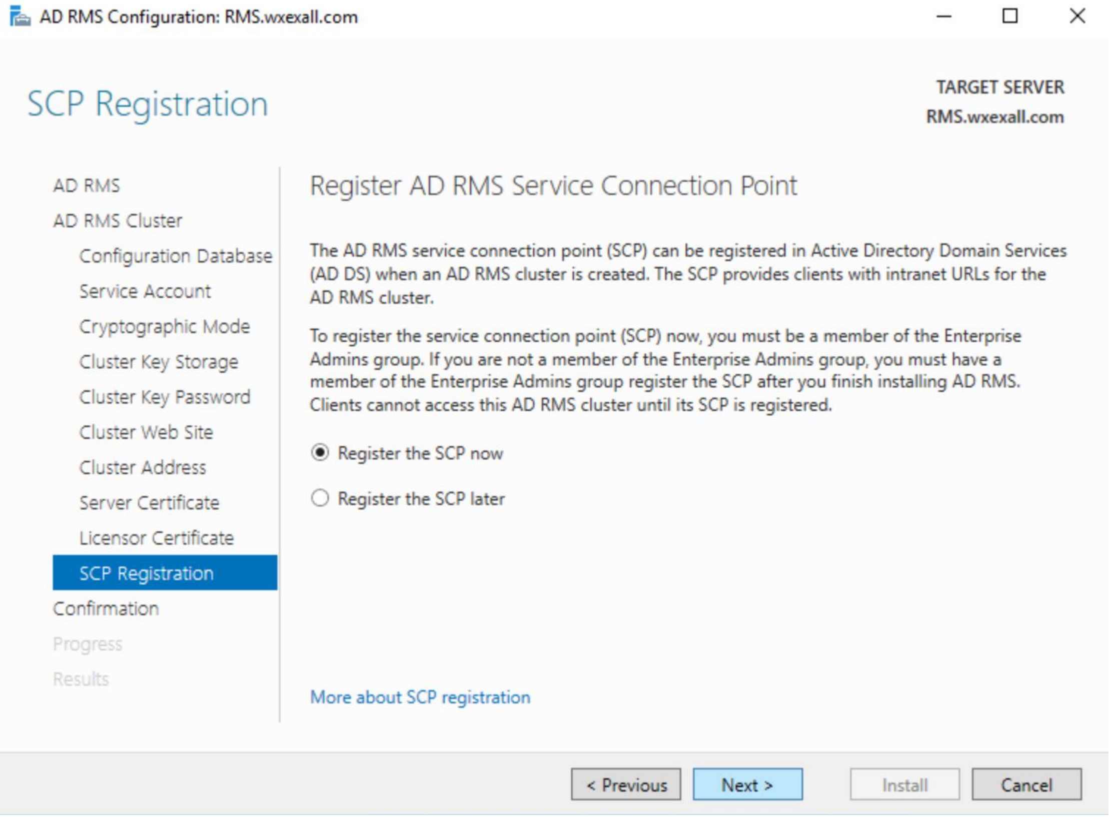
When communicating with clients, AD RMS can use Secure Sockets Layer (SSL) to encrypt network traffic. For production deployments, choose an existing SSL certificate whose subject name matches the host name of the cluster. For test deployments, you can create and use a self-signed certificate instead.

● Choose an existing certificate for SSL encryption (recommended)

Issued To	Issued By	Expiration Date
WMSvc-SHA2-RMS	WMSvc-SHA2-RMS	9/19/2032
*.wxexall.com	wxexall-DC-CA	11/27/2024
VPSSVDI	VPSSVDI	10/21/2036

○ Create a self-signed certificate for SSL encryption
○ Choose a certificate for SSL encryption later

11. Register SCP now



AD RMS Configuration: RMS.wxexall.com

SCP Registration

TARGET SERVER
RMS.wxexall.com

Register AD RMS Service Connection Point

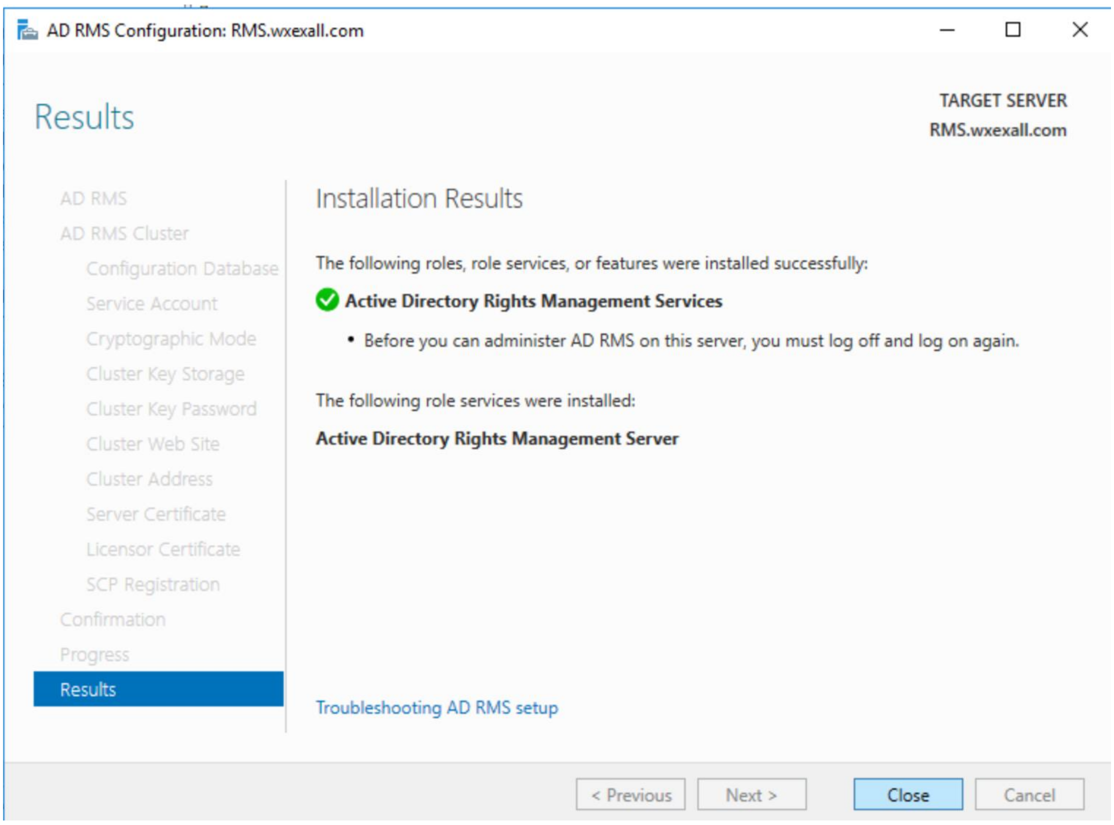
The AD RMS service connection point (SCP) can be registered in Active Directory Domain Services (AD DS) when an AD RMS cluster is created. The SCP provides clients with intranet URLs for the AD RMS cluster.

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.

● Register the SCP now

○ Register the SCP later

12. Install the RMS service



Installation Results

The following roles, role services, or features were installed successfully:

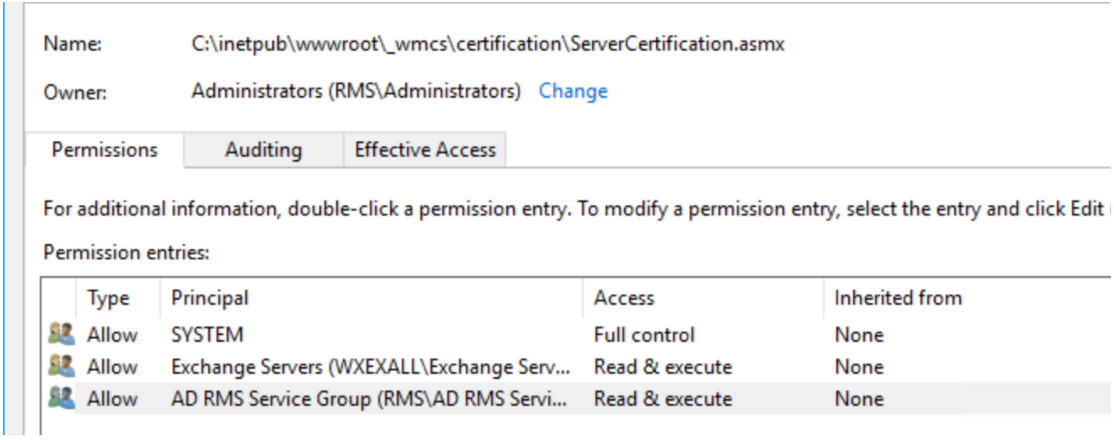
✓ **Active Directory Rights Management Services**

- Before you can administer AD RMS on this server, you must log off and log on again.

The following role services were installed:

Active Directory Rights Management Server

13. Confirm exchange servers group and AD RMS service group have read/read&execute permission on servercertificateion.asmx, publish.asmx



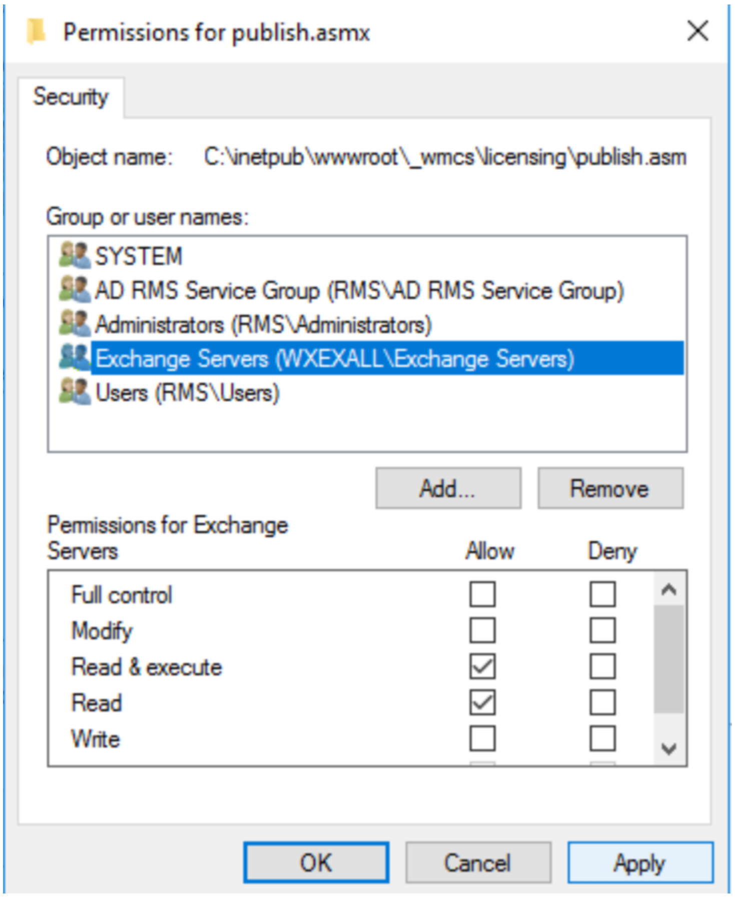
Name: C:\inetpub\wwwroot_wmcs\certification\ServerCertification.asmx

Owner: Administrators (RMS\Administrators) Change

For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit

Permission entries:

Type	Principal	Access	Inherited from
Allow	SYSTEM	Full control	None
Allow	Exchange Servers (WXEXALL\Exchange Serv...	Read & execute	None
Allow	AD RMS Service Group (RMS\AD RMS Servi...	Read & execute	None



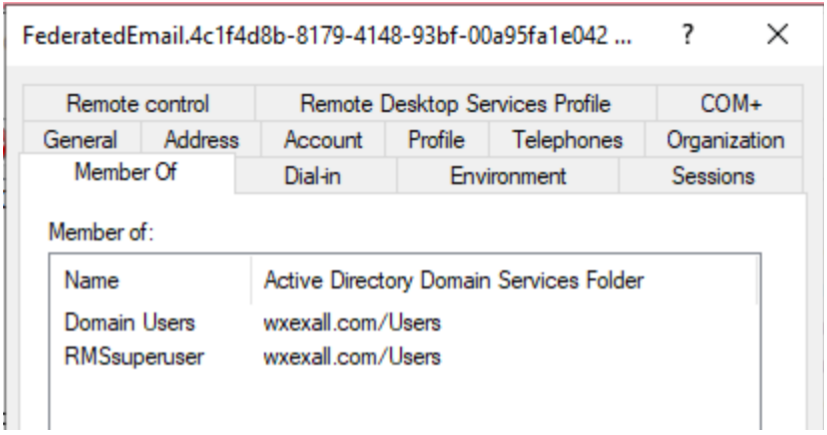
Object name: C:\inetpub\wwwroot_wmcs\licensing\publish.asm

Group or user names:

- SYSTEM
- AD RMS Service Group (RMS\AD RMS Service Group)
- Administrators (RMS\Administrators)
- Exchange Servers (WXEXALL\Exchange Servers)
- Users (RMS\Users)

Permissions for Exchange Servers	Allow	Deny
Full control	□	□
Modify	□	□
Read & execute	☑	□
Read	☑	□
Write	□	□

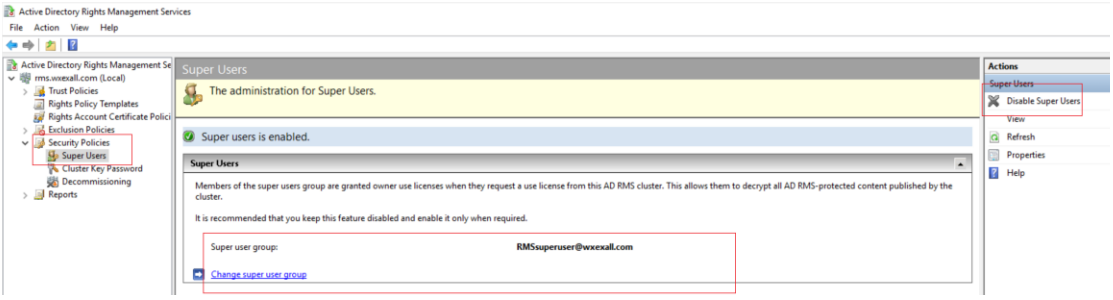
14. Log off rms server and log on again.
15. Create a RMS super user group, and add FederatedEmail.4c1f4d8b-8179-4148-93bf-00a95fa1e042 to the group



Member of:

Name	Active Directory Domain Services Folder
Domain Users	wxexall.com/Users
RMSsuperuser	wxexall.com/Users

16. Open active directory rights management service -> security policies -> super user -> enable super users -> change super user group -> choose the rms super user group



The administration for Super Users.

Super users is enabled.

Super Users

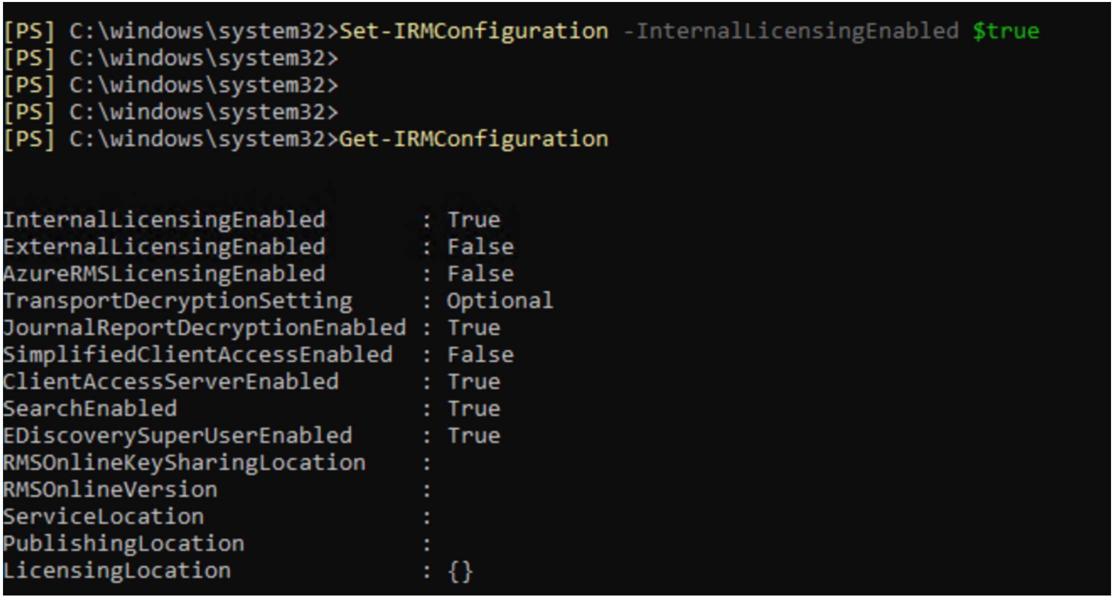
Members of the super users group are granted owner use licenses when they request a use license from this AD RMS cluster. This allows them to decrypt all AD RMS-protected content published by the cluster.

It is recommended that you keep this feature disabled and enable it only when required.

Super user group: RMSsuperuser@wxexall.com

Change super user group

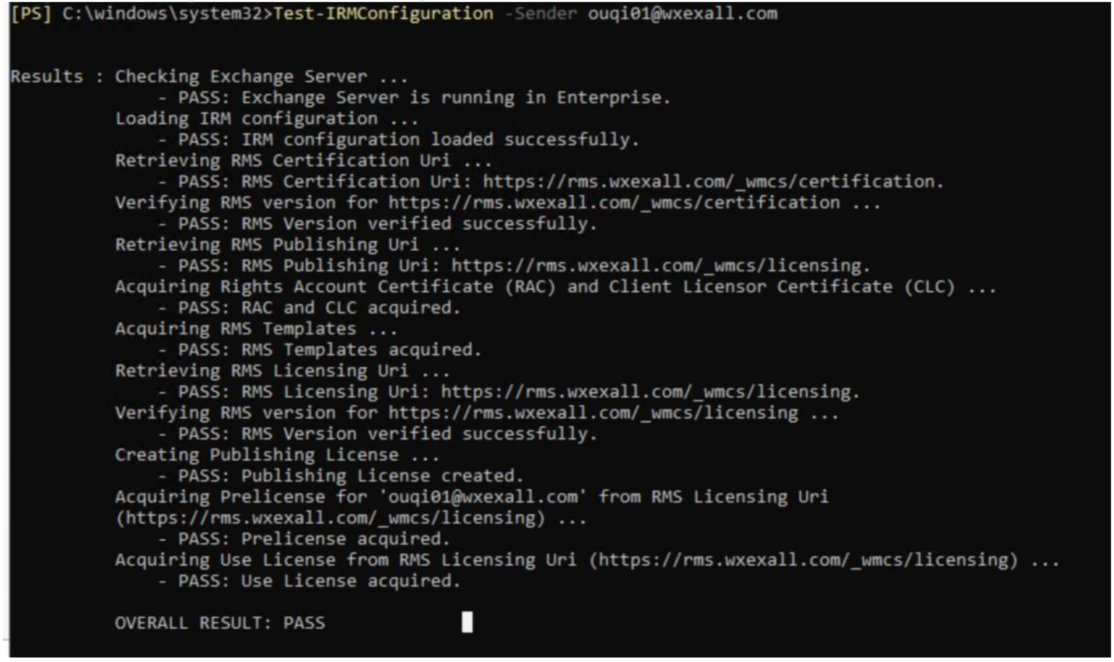
17. Set-IRMConfiguration -InternalLicensingEnabled $true and reset IIS



```
[PS] C:\windows\system32>Set-IRMConfiguration -InternalLicensingEnabled $true
[PS] C:\windows\system32>
[PS] C:\windows\system32>
[PS] C:\windows\system32>
[PS] C:\windows\system32>Get-IRMConfiguration


InternalLicensingEnabled        : True
ExternalLicensingEnabled        : False
AzureRMSLicensingEnabled        : False
TransportDecryptionSetting      : Optional
JournalReportDecryptionEnabled  : True
SimplifiedClientAccessEnabled   : False
ClientAccessServerEnabled       : True
SearchEnabled                   : True
EDiscoverySuperUserEnabled      : True
RMSOnlineKeySharingLocation     :
RMSOnlineVersion                :
ServiceLocation                 :
PublishingLocation              :
LicensingLocation               : {}
```

18. Test-irmconfiguration, confirming the result is pass

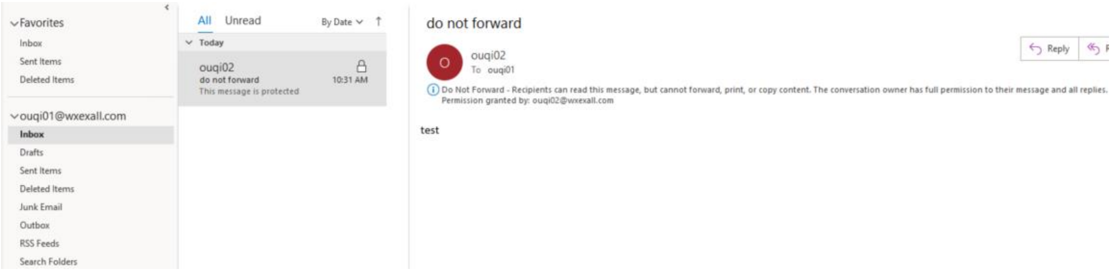


```
[PS] C:\windows\system32>Test-IRMConfiguration -Sender ouqi01@wxexall.com


Results : Checking Exchange Server ...
              - PASS: Exchange Server is running in Enterprise.
          Loading IRM configuration ...
              - PASS: IRM configuration loaded successfully.
          Retrieving RMS Certification Uri ...
              - PASS: RMS Certification Uri: https://rms.wxexall.com/_wmcs/certification.
          Verifying RMS version for https://rms.wxexall.com/_wmcs/certification ...
              - PASS: RMS Version verified successfully.
          Retrieving RMS Publishing Uri ...
              - PASS: RMS Publishing Uri: https://rms.wxexall.com/_wmcs/licensing.
          Acquiring Rights Account Certificate (RAC) and Client Licensor Certificate (CLC) ...
              - PASS: RAC and CLC acquired.
          Acquiring RMS Templates ...
              - PASS: RMS Templates acquired.
          Retrieving RMS Licensing Uri ...
              - PASS: RMS Licensing Uri: https://rms.wxexall.com/_wmcs/licensing.
          Verifying RMS version for https://rms.wxexall.com/_wmcs/licensing ...
              - PASS: RMS Version verified successfully.
          Creating Publishing License ...
              - PASS: Publishing License created.
          Acquiring Prelicense for 'ouqi01@wxexall.com' from RMS Licensing Uri
          (https://rms.wxexall.com/_wmcs/licensing) ...
              - PASS: Prelicense acquired.
          Acquiring Use License from RMS Licensing Uri (https://rms.wxexall.com/_wmcs/licensing) ...
              - PASS: Use License acquired.

          OVERALL RESULT: PASS
```

Also, the encrypted message can be successfully opened in outlook



ouqi02
do not forward
This message is protected
10:31 AM

do not forward

O ouqi02
To ouqi01

Do Not Forward - Recipients can read this message, but cannot forward, print, or copy content. The conversation owner has full permission to their message and all replies.
Permission granted by: ouqi02@wxexall.com

test