Operations Guide



Information Protection Using Azure Rights Management Services

Prepared for

[Customer Name]

June 20, 2014

Version

Prepared by

**Author**

Contributors

**Add Contributors to Doc Properties**

Revision and Signoff Sheet

Change Record

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Author | Version | Change Reference |
|  |  | 1.0 | Initial draft for review |
|  |  |  |  |
|  |  |  |  |

Reviewers

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Version Approved | Position | Date |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Table of Contents

[1 Introduction 6](#_Toc391033503)

[2 Operations 6](#_Toc391033504)

[2.1 Administrative Roles 6](#_Toc391033505)

[2.2 Administrative Tasks 7](#_Toc391033506)

[2.2.1 Viewing the Azure RMS Configuration 7](#_Toc391033507)

[2.2.2 Azure Rights Management Tenant Key 8](#_Toc391033508)

[2.2.3 Working with Rights Policy Templates 11](#_Toc391033509)

[2.2.4 Creating Rights Policy Templates 12](#_Toc391033510)

[2.3 Logging Maintenance Tasks 13](#_Toc391033511)

[2.3.1 Access RMS Logs 13](#_Toc391033512)

[2.3.2 Download Logs using PowerShell 14](#_Toc391033513)

[2.3.3 Suspend and Resume Logging 14](#_Toc391033514)

[2.3.4 Manage RMS Log Storage 14](#_Toc391033515)

[2.4 Recovery and e-Discovery of Azure RMS-protected Content 15](#_Toc391033516)

[2.5 Contingency Tasks 16](#_Toc391033517)

[2.5.1 Deactivate Azure Rights Management Service 16](#_Toc391033518)

[3 Appendix A: Interpreting Azure Logs 17](#_Toc391033519)

[3.1 Storage Account Format 17](#_Toc391033520)

[3.2 Log Sequence 18](#_Toc391033521)

[3.3 Blob Format 18](#_Toc391033522)

[3.3.1 User-id Exceptions 20](#_Toc391033523)

[3.4 Frequently Used Requests 20](#_Toc391033524)

**Spell/grammar check is turned ON within all SDM Word templates -** Remember to turn off spell/grammar check before sending out the document if you want to avoid showing spelling and grammar mark-ups in red. To turn this feature off, do the following:

1. Click **File**.
2. Click the **Options** on the left.
3. Click **Proofing**.
4. Scroll to bottom and check the two boxes shown below:



**To remove all the Visible Guidance (Hot Pink text with Grey Background) all at once:**

1. Click Ctrl + H to open the **Find and Replace** box
2. Make sure your cursor is in the **Find what** box.
3. Click the **More** button at the bottom left.
4. Click the **Format** button at the bottom left and select **Style**.
5. Scroll down, locate select the **Visible Guidance**.
6. Make sure the **Replace with** box is empty.
7. Click **Replace All**.
8. If not empty - click the format button in the lower left-hand corner. Scroll down and choose **(no style)**, then replace all.

**IMPORTANT – Finalize This Document**

**REMOVE** all pink text, guidance, comments, changes, and hidden text in this document before submitting it to the customer. You can do this in two ways:

* **Save as PDF** and send the PDF version to the customer.   
  ~ OR ~
* **Inspect document and remove comments, revisions, any document properties you do not want included, personal information, and hidden text.** For guidance on how to do this, see [Remove hidden data and personal information from Office documents](http://office.microsoft.com/client/helppreview.aspx?AssetID=HA100375931033&QueryID=ALdFua2no0&respos=6&rt=2&ns=WINWORD&lcid=1033&pid=CH100487501033#3).

1. Introduction

This document is designed to give detailed information on how to operate the Azure Rights Management Services solution in production, including the management and support tasks to keep the solution running correctly. The intended audience is <<Customer Name>>’s IT operations team.

1. Operations

This section covers the operation of the Microsoft Services Information Protection using Active Directory Rights Management Services solution after its initial configuration is complete.

* 1. Administrative Roles

There are several roles in the management of an Azure Rights Management Services (Azure RMS) deployment, each representing a particular set of capabilities with respect to the solution. By default, any user with global administrator permissions within the Office 365 tenant can administer Azure RMS. Permission to administer Azure RMS can also be delegated to specific users and groups.

The following table describes the capabilities of each administrative role defined for the Azure Rights Management Services platform.

|  |  |
| --- | --- |
| **Role Name** | **Description** |
| **Office 365 Global Administrator** | An administrative role within Office 365. Users with global administrator permissions have access to all administrative features, including those related to Azure RMS. The person who signs up to purchase Office 365 becomes a global administrator. Only global administrators can assign other administrator roles. There can be more than one global administrator at your company |
| **RMS Administrator** | A user or group that has been delegated permission to administer the Azure RMS service. This can be any Azure Active Directory user or group specified by another administrator. |
| **Superuser Group** | This sensitive group is used to grant access to RMS-protected documents, even though members of this group do not have explicit rights to the documents. This account is normally disabled. |
| **AD FS Admin Account** | Create a Dedicated User Account to administer Active Directory Federation Services component, if using AD FS. |

Table 1 Solution Administrative Roles

These security groups are used to describe the security requirements for the tasks listed in this guide. Each task description lists which security groups a person needs to be a member to complete the task.

* 1. Administrative Tasks

This section provides step-by-step instructions for performing the common administrative tasks required when operating the Azure RMS platform.

The table below lists all administrative tasks covered by the guide, the roles responsible for executing the task, and the frequency it should be executed.

|  |  |  |
| --- | --- | --- |
| **Task Name** | **Executed By** | **Frequency** |
| **Manage the RMS Key** | Office 365 Global Administrator  RMS Administrator | As required |
| **Working with Rights Policy Templates** | Office 365 Global Administrator  RMS Administrator | As required |
| **Creating Rights Policy Templates** | Office 365 Global Administrator  RMS Administrator | As required |
| **Logging Service maintenance** | Azure storage account name | As required |
| **Recovery and e-Discovery of RMS-protected content** | RMS SuperUsers | As required |
| **Contingency tasks** | Office 365 Global Administrator  RMS Administrator | As required |

Table 2 Common Administrative Tasks

* + 1. Viewing the Azure RMS Configuration

The following configuration of the Azure RMS subscription can be inspected using the Get-AadrmConfiguration command in Windows PowerShell:

* Intranet URL for licensing and publishing requests
* Extranet URL for licensing and publishing requests
* Certification URL for requests to the account certification services
* Connection URL for administration
* List of keys
* List of rights policy templates
* List and statue of the SuperUsers feature
* List of users with administrator permissions in Azure RMS
  + 1. Azure Rights Management Tenant Key

The Azure Rights Management Tenant Key is the root key of the information protection architecture. Depending on whether you choose to have Microsoft create and manage the tenant key or whether you created the tenant key and transferred to Microsoft datacenters using the Bring your own Key (ByoK) scenario, you will have different levels of control and responsibility for the tenant key. The following table identifies which operations you can do, depending on the topology that you’ve chosen for your Azure tenant key:

|  |  |  |
| --- | --- | --- |
| Lifecycle operation | Microsoft-managed (default) | Customer-managed (ByoK) |
| **Revoke your tenant key** | No (automatic) | No (automatic) |
| **Re-key your tenant key** | Yes | Yes |
| **Backup and recover your tenant key** | No | Yes |
| **Export your tenant key** | Yes | No |
| **Respond to a breach** | Yes | Yes |

The following sections outline how to perform the tasks listed above, depending on your key topology.

* + - 1. Microsoft-managed

**Revoke your tenant key**

When you deactivate Azure RMS and unsubscribe, Azure RMS automatically stops using your tenant key and no action is required.

**Re-key your tenant key**

Re-keying is also known as rolling your key. Do not re-key your tenant key unless it’s really necessary. Older clients, such as Office 2010, were not designed to handle key changes gracefully. In this scenario, you must clear the RMS state on computers by using Group Policy or an equivalent mechanism. However, there are some legitimate events that may force you to re-key your tenant key. For example:

* Your company has split into two or more companies. When you re-key your tenant key, the new company will not have access to new content that your employees publish. They can access the old content if they have a copy of the old tenant key.
* You believe the master copy of your tenant key (the copy in your possession) was compromised.

You can re-key your tenant key by calling CSS and proving that you are the tenant administrator.

When you re-key your tenant key, new content is protected by using the new tenant key. This happens in a phased manner, so for a period of time, some new content will continue to be protected with the old tenant key. Previously protected content stays protected to your old tenant key. To support this scenario, Azure RMS retains your old tenant key so that it can issue licenses for old content

**Backup and recover your tenant key**

Microsoft will perform the backup and recovery of your tenant key on your behalf. No further action is required.

**Export your tenant key**

You can export your tenant key and Azure RMS configuration. You may decide to export the tenant key in the event that you want to migrate from Azure RMS to AD RMS on-premises.

To export the tenant key, perform the following steps:

* Contact Microsoft Customer Service Support and verify that you are an administrator of the Azure RMS tenant.
* Microsoft will verify that your request is legitimate. Microsoft will notify your organization by mailing address and all administrators of the Azure RMS tenant via email. Microsoft will wait a minimum of five business days to receive a dissenting response.
* Once the request is verified, Microsoft Customer Support Services will send the Azure RMS configuration and tenant key in a password-protected file.
* Microsoft Customer Support Services will also send you a tool via email which is used to decrypt the tenant key.
* Run the tool from the command prompt using the **aadrmtpd.exe –createkey** command. This will generate an RSA key pair.
* Respond to the email from CSS and attach the file that starts with **PublicKey**. CSS will use this key to encrypt your tenant key.
* Once you receive the respond from CCS, run the tool from the command prompt using the **aadrmtpd.exe –decrypt yourtpdfile** command to decrypt the tenant key.

**Respond to a breach**

Microsoft has a dedicated team to respond to security incidents in its products and services. As soon as there is a credible report of an incident, this team engages to investigate the scope, root cause, and mitigations. If this incident affects your assets, then Microsoft will notify your Azure RMS tenant administrators by email by using the address that you supplied when you subscribed.

The corresponding response to the breach will depend on the scope of the breach. For example, if your tenant key is leaked, the most appropriate response might be to re-key your tenant key. Microsoft will work with you through this process to determine the most appropriate action to take.

* + - 1. Customer-managed (ByoK)

**Revoke your tenant key**

When you deactivate Azure RMS and unsubscribe, Azure RMS automatically stops using your tenant key and no action is required.

**Re-key your tenant key**

Re-keying is also known as rolling your key. Do not re-key your tenant key unless it’s really necessary. Older clients, such as Office 2010, were not designed to handle key changes gracefully. In this scenario, you must clear the RMS state on computers by using Group Policy or an equivalent mechanism. However, there are some legitimate events that may force you to re-key your tenant key. For example:

* Your company has split into two or more companies. When you re-key your tenant key, the new company will not have access to new content that your employees publish. They can access the old content if they have a copy of the old tenant key.
* You believe the master copy of your tenant key (the copy in your possession) was compromised.

When you re-key your tenant key, new content is protected by using the new tenant key. This happens in a phased manner, so for a period of time, some new content will continue to be protected with the old tenant key. Previously protected content stays protected to your old tenant key. To support this scenario, Azure RMS retains your old tenant key so that it can issue licenses for old content.

**Backup and recover your tenant key**

You are responsible for backing up the tenant key. To backup the tenant key, perform the procedures as documented by Thales.

**Export your tenant key**

Using the Bring your own Key scenario, the copy of the tenant key in the possession of Microsoft is not able to be exported, even by Microsoft datacenter administrators. This copy is non-recoverable.

**Respond to a breach**

Microsoft has a dedicated team to respond to security incidents in its products and services. As soon as there is a credible report of an incident, this team engages to investigate the scope, root cause, and mitigations. If this incident affects your assets, then Microsoft will notify your Azure RMS tenant administrators by email by using the address that you supplied when you subscribed.

The corresponding response to the breach will depend on the scope of the breach. For example, if your tenant key is leaked, the most appropriate response might be to re-key your tenant key. Microsoft will work with you through this process to determine the most appropriate action to take.

* + 1. Working with Rights Policy Templates

Azure RMS stores rights policy templates in Windows Azure. These templates are copies down to the local computer upon bootstrapping and are refreshed periodically.

* When a user attempts to consume protected content, the RMS-enabled application obtains the latest version of the rights policy template that was used to publish the content from the configuration database. The RMS-enabled application then applies its settings to the content.
* When the rights policy template is modified via the web interface, RMS updates the template accordingly in Windows Azure. If the template name or description has changed, the new information will appear to end users after the refresh interval has passed. Clients using Office 365 will see the templates automatically refreshed. Office 2013 users will see the templates refreshed on a schedule. By default, this interval is every 7 days, although this value can be modified. Clients using Office 2010 will see the template refreshed upon user log on.
* If a rights policy template is deleted, it is removed from the Azure RMS server and will removed from user computers after the end of the refresh interval. Note that if you delete a rights policy template, Azure RMS will no longer be able to issue use licenses for content protected by that template. We recommend that if you need to prevent users from using a specific rights policy template, you archive it rather than delete it. This will remove the template from the end user computers; however, it will still be available to Azure RMS to issue use licenses.

When working with rights policy templates:

* Create and edit rights policy templates. When creating a rights policy template, define the users and rights that apply. Also define how the rights policy template is to be applied to content. Edit the rights policy templates when they need to be updated. Create as many rights policy templates as are required to manage rights in the organization, but consider that some applications are limited in the number of templates that can be displayed in the application’s user interface. In addition, displaying more than a few templates in the application’s menus will create user confusion and increases the risk of usage of the wrong templates. If more than a few templates are created in a cluster, you might want to scope the different templates to different groups of users by applying Access Control Lists to the different templates in the export folder.
* Publish rights policy templates. For an author to apply a given rights policy template to content, a copy of the rights policy template must be visible from the author’s computer. Control which authors can apply which rights policy templates by managing template publication.
* Retire rights policy templates. When a template it is no longer appropriate, archive a rights policy template. Users attempting to consume content protected with the template will still be able to do so as the archived template is still accessible to the RMS servers issuing licenses.
* If it is desired that all documents protected with a template are no longer accessible to users, you can delete the template instead of archiving it. If users attempt to consume content that was published by using the deleted rights policy template, they will not be issued licenses.
  + 1. Creating Rights Policy Templates

To ease administration of the rights policy templates, rights policy templates can be created in a web console. To ease distribution of rights policy templates the RMS Client 2.x can automatically retrieve rights policy templates with Microsoft Office 2013 applications and the RMS App. No user or administrator action is required for these machines.

|  |  |
| --- | --- |
|  | **To create a new Azure Rights Management Services rights policy template** |
|  | * Access the ***Get started with Rights Management*** quick start page from the **Office 365 admin center** or from the **Azure Management Portal**. * Click **Create a new rights policy template** to start the **Rights Policy Template wizard**. * In the **Add a new rights policy template** window, choose the appropriate language for the rights policy template and enter a name and description for the template. You can assign name and description to a template in different languages, and to assure proper usage and non-deniability, you should do so for all the different languages in use in your organization. Click the Complete icon. * Click Manage your rights policy templates and select the newly created template. * Under Configure rights for users and groups click Get started. * Click Get started now. * In the Select users and groups window, locate and click the appropriate users or groups. Click the Next icon to continue. * Select the appropriate permission level and click the Complete icon. * Click Add and repeat the previous two steps to add additional users and groups with different permissions * Click the Configure tab. * If desired, add the template name and description in additional languages. * If desired, configure content expiration by date or number of days. * If desired, configure offline access. * To make the rights policy template available to end users, click the Publish icon. |

* 1. Logging Maintenance Tasks

The following sections detail common administrative tasks related to Azure RMS logging. These tasks assume that Azure RMS logging has previously been enabled. For more information about configuring Azure RMS logging, see the corresponding document Azure\_RMS\_05\_Build\_DELIVERY\_Step-by-Step-Installation-Procedures.

* + 1. Access RMS Logs

RMS logs are stored and accessed in Azure storage. It takes approximately 15 minutes for an action to be logged and accessible via Azure storage. These actions are written to Azure storage as a series of blobs where each blob contains one or more log records. Log records are stored in W3C extended log format and named in a number format, in the order in which they were created.

Logs can be viewed directly from Azure storage; however, to optimize performance and to help lower costs, we recommend that you download the logs from Azure storage to local storage on-premises. This enables you to retain logs for a longer period of time. There are two methods you can use to download your logs:

* **Use the Get-AadrmsUsageLog PowerShell cmdlet**: This cmdlet will download the logs to a file location that you specify. Each blob will be downloaded as a file
* **Create a custom application to download logs using the Azure Storage SDK**: You may decide to create a custom application to download the Azure RMS logs if you want increased flexibility. For example, if you would like to download logs in real time or if you would like to delegate the download of logs to a user who does not have RMS administrative credentials, you can create a custom application that will perform these functions. Creating a customer application for Azure storage is beyond the scope of this enagement. For more information about the Azure Storage SDK, see the [Microsoft Azure Storage SDK](http://azure.microsoft.com/en-us/develop/net/) article (http://azure.microsoft.com/en-us/develop/net/).
  + 1. Download Logs using PowerShell

The following steps describe how you can download your Azure RMS logs from Azure storage using Windows PowerShell:

* Log on to the computer on which you wish to download the Azure RMS storage logs.
* Start Windows PowerShell with the **Run as administrator** option.
* Enter the following command in Windows PowerShell: **Get-AadrmUsageLog –Path <***location***>**

You can also specify to only download a specific range of blobs using the **–FromCounter** and **–ToCounter** parameters. When you run these cmdlets, Windows PowerShell displays the name of the last blob that was downloaded. You can assign this name to a variable, which lets you run Get-AadrmUsageLog in a loop or a schedule job, downloading only the incremental logs each time.

Once the logs have been downloaded to local storage you can aggregate the log files into CSV format using the Microsoft Log Parser Tool. You can also use this tool to convert the log data to the SYSLOG format or to import it into a database. You can download the Log Parser tool from the [Microsoft Download Center](http://www.microsoft.com/en-us/download/details.aspx?id=24659) (<http://www.microsoft.com/en-us/download/details.aspx?id=24659>).

* + 1. Suspend and Resume Logging

You can choose to suspend logging of Azure RMS activity for a time. While RMS logging is suspending, RMS retains your storage account information so that you can easily resume logging again. You can suspend RMS logging using the following PowerShell cmdlet: Disable-AadrmsUsageLogFeature. You can resume RMS logging using the following PowerShell cmdlet: Enable-AadrmUsageLogFeature. To check the status of your RMS logging, using the following PowerShell cmdlet: Get-AadrmUsageLogFeature. A value of True indicates that logging is enabled while a value of False indicates that logging is currently disabled.

* + 1. Manage RMS Log Storage

Azure RMS provides no mechanism to automatically manage your RMS log files. By default, log files will remain in Azure storage until you take action to delete them. Note that you are charged for the storage space used to keep RMS logs. Therefore, to optimize performance and to reduce associated storage costs, we recommend that you periodically download the log files to local storage for long-term storage and analysis and periodically delete the files stored in Azure storage. However, when deleting files, take care not to delete the metadata file or its rms-metadata container file. These files are used to keep track of the last blob number used for your account.

For more information about using Azure storage, see the [Windows Azure Storage](http://azure.microsoft.com/en-us/documentation/services/storage/) documentation (<http://azure.microsoft.com/en-us/documentation/services/storage/>).

* 1. Recovery and e-Discovery of Azure RMS-protected Content

In any organization there’s often a need to identify content (typically in the form of documents or email) related to certain proceedings and grant access to those materials to specialized personnel. Another common situation involves the need for recovering information protected by employees without their cooperation, for example, because they no longer work for the company.

Azure RMS provides tools and capabilities to regain access to protected documents in different situations, in either an automated or systematic manner or as individual recovery or search operations.

Documents protected with Azure RMS can be stored in different locations, among them:

* A user’s workstation inside a personal folder
* A user workstation inside a .pst file connected to Outlook
* A file share
* A SharePoint library
* A user’s mailbox or in transit in an Exchange infrastructure
* An archival system

There are three common situations where access to protected information is needed:

1. The documents containing the information are already in the hands of the persons requiring access.
2. The documents are known to be located in a certain location but the particular documents containing the information in question are not identified.
3. There’s a need to proactively identify all documents pertaining to a certain matter and archive them in unprotected or accessible form.

In the first case, which is common when auditors have access to a user’s workstation and they want to read or unprotect a particular piece of information found in the user’s machine, access to the documents can be enabled by making that person, either temporarily or permanently, a member of the SuperUser’s group and enabling SuperUser functionality in Azure RMS.

When a user is a member of the Azure RMS superusers group that user is granted any license it requests, so the user can view, copy or unprotect the content at will. Obviously this functionality has to be managed in a very controlled way.

Another alternative for dealing with this case is to allow one person that is a member of the SuperUsers group to perform bulk unprotection of all documents in a certain location, and then handling the protected documents to the person requiring access. The information can then be indexed and searched using normal tools for the task.

Considering that the information is likely sensitive, a formal and secure process for dealing with these proceedings needs to be defined. The PowerShell and File API tools can be used for this task.

|  |  |  |  |
| --- | --- | --- | --- |
| **Scenario** | **Details** | **PowerShell** | **File API** |
| Bulk protection | Use RMS to selectively bulk protect items in certain locations | Can be used to select multiple files and pipeline the request to File API or a personalized application | Can protect multiple files on a directory or pipelined |
| Bulk un-protection | Use RMS to selectively bulk unprotect items in certain locations | Can be used to select multiple files and pipeline the request to File API or a personalized application | Can un-protect multiple files on a directory or pipelined |
| Manual protection | Use RMS to manually protect files or folders | Can be used to select a single or multiple files or a folder and pipeline the request to File API or a personalized application | Can protect single or multiple files on a directory |

Additionally, for this task, Microsoft has published a tool called the RMS Bulk Protection Tool which can be used to encrypt files through the command line or, more importantly in this case, unprotect them. The bulk protection tool can be combined with a script to search all protected files in a system and unprotect them, allowing someone performing discovery full access to all the files in the system.

The Bulk Protection Tool works not only on file shares, but also on emails and attachments stored in a .pst file. This way emails archived into a .pst file can also be unprotected in bulk, indexed, and searched as needed. Typically, the bulk protection tool will be combined with SuperUser privileges in order to access files or emails in a user’s workstation.

The Bulk Protection tool can be downloaded from <http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=f9fbe58f-c175-41d0-afdc-6f160ab809cd>.

When files are stored in a protected SharePoint library, they are stored in the database in an unprotected format, and they are only protected when downloaded through the SharePoint interfaces. So someone performing e-discovery only needs to be granted access rights over the SharePoint library in order to be able to perform searches or downloads of protected documents. Alternatively, by granting that person direct rights over the SQL Server database acting as the back-end of the SharePoint library the user will be able to extract the unprotected files directly from the database.

When information needs to be automatically and proactively decrypted for performing automated e-discovery or archival, similar solutions typically allow automating the task of unprotecting documents.

Since the Bulk Protection tool can also work with files stored in file shares, it can be also used combined with scripts and scheduled tasks, or with the File Server Resource Manager that’s part of Windows Server 2012 and later, to automatically create unprotected backups of protected files deposited in the file share. Once unprotected, files can be accessed and indexed as desired.

A common process associated to e-discovery is email journaling. In this situation, all emails with certain characteristics, such as all emails sent by or to a specific user, get archived in a special mailbox. If the message is processed by an Exchange 2010 or later server, the journaling system can be configured to automatically store both protected and unprotected copies of each journaled message, which greatly helps in e-discovery processes. It must be highlighted that while this functionality is only available in Exchange 2010 and later, only the Hub Transport servers performing the journaling need to be upgraded to this version, while the rest of the infrastructure can remain in previous versions of Exchange.

Exchange Server 2010 and later can also be configured to automatically unprotect certain messages in transit by using the Transport Decryption functionality. Typically this is used in conjunction with anti-malicious software (malware) solutions (so that the message can be scanned for malware even if protected) or for archival solutions that integrate with Exchange Server 2010 and later. Again, only the Hub Transport Server needs to be running this version of Exchange for this functionality to be available.

Finally, certain archival systems such as Symantec’s Enterprise Vault are commonly used to archive messages for e-discovery purposes. For many of these, either the ISVs providing these products or third parties working with them have developed Azure RMS integration capabilities so they can be configured to store protected or unprotected versions of the messages and index them as required.

If additional e-discovery capabilities are required, certain Microsoft partners provide capabilities such as enterprise-wide indexing, client-side action logging, and content tracking to fulfill specialized needs of auditing, legal, and other departments.

* 1. Contingency Tasks
     1. Deactivate Azure Rights Management Service

Deactivating the Azure Rights Management Service turns the feature off for the Microsoft cloud service subscription. Once the subscription is deactivated, users will no longer be able to acquire use licenses to content, even if they were granted permissions to it. Therefore, we recommend that you only deactivate rights management if you no longer need access to content that was previously rights-protected using Azure RMS.

Steps to deactivate the Azure Rights Management Service:

* + - 1. Enable the decommissioning service
* Sign in to the Office 365 admin center.
* Click **Service settings**.
* From the Service settings page, click **Rights management**.
* In the Protect your information section, click **Manage**.
* In the Rights management section, click **Deactivate**.
* Click **Deactivate** in the Do you want to deactivate Rights Management popup box.

1. Appendix A: Interpreting Azure Logs

The following sections detail the information stored in the Azure RMS logs and how to interpret that data.

* 1. Storage Account Format

Two containers are created the first time RMS writes logs ot the storage account:

* Rms-metadata: This is a reserved container for RMS that should not be deleted or modified in any way.
* Rms-logs-<guid>: RMS will create and store the logs in this container. Any files stored in this location can be deleted or moved.

The RMS service has the ability to create additional Rms-logs-<guid> containers. This can occur if the original Rms-metadata container is deleted or becomes corrupted; RMS will reset the Rms-metadata container and create a new Rms-logs-<guid> container. The logs stored in the old container will remain untouched, they will not be deleted.

* 1. Log Sequence

RMS will store the logs as a series of blobs. Each of these blobs will contain one or more log records and will be stored in the extended W3C log format. Each blob will be named as a number; the first blob in each container is named 000000001. Each following blob will be named numbered sequentially in the order they are created. Additionally, each blob will have a UTC time stamp, indicating when each request was served.

RMS logs are often created within 15 minutes of the RMS request and are not necessarily chronological. Therefore, administrators should add 15 minutes to obtained an accurate timestamp reading. Additionally, it is recommended to download and store the logs in a separate container where you can sort the logs based on the timestamp.

* 1. Blob Format

The Azure log blobs are recorded in the W3C extended format. The first two lines will display the following text:

**#Software: RMS**

**#Version: 1.0**

The first line identifies that this is an RMS log. The second displays the version specification that the blob will follow. It is recommended that any applications parsing the logs, verify these first two lines before parsing the rest of the blob.

The third line contains a list of field names separated by tabs:

**#Fields: date time row-id request-type user-id result correlation-id content-id c-info c-ip**

The next line contains all the log records and the values follow the above format. The following table describes the fields and provides an example value for each field.

| Field Name | W3C Data Type | Description | Example Value |
| --- | --- | --- | --- |
| date | Date | UTC date when the request was served.  The source is the local clock on the server that served the request. | 2014-06-01 |
| time | Time | UTC time in 24-hour format when the request was served.  The source is the local clock on the server that served the request. | 21:59:28 |
| row-id | Text | Unique GUID for this log record.  This value is useful when you aggregate logs or copy logs into another format. | 1c3fe7a9-d9e0-4654-97b7-14fafa72ea63 |
| request-type | Name | Name of the RMS API that was requested. | AcquireLicense |
| user-id | String | The user who made the request.  The value is enclosed in single quotation marks. Some request types are anonymous, in which case the value is ”. | ‘joe@contoso.com’ |
| result | String | ‘Success’ if the request was served successful.  The error type in single quotation marks if the request failed. | ‘Success’ |
| correlation-id | Text | GUID that is common between the RMS client log and server log for a given request.  This value can be useful to help troubleshooting client issues. | cab52088-8925-4371-be34-4b71a3112356 |
| content-id | Text | GUID, enclosed in curly braces that identifies the protected content (for example, a document).  This field has a value only if request-type is AcquireLicense and is blank for all other request types. | {bb4af47b-cfed-4719-831d-71b98191a4f2} |
| c-info | String | Information about the client platform that is making the request.  The specific string varies, depending on the application (for example, the operating system or the browser). | 'MSIPC;version=1.0.622.36;AppName=IPViewer.exe;AppVersion=1.0.1127.0;AppArch=x86;OSName=Windows;OSVersion=6.1.7601;OSArch=amd64’ |
| c-ip | Address | IP address of the client that makes the request. | 64.51.202.144 |

* + 1. User-id Exceptions

The user-id field will display the user who made the request, however, two exceptions can occur where the value will not map to a real user:

* The value **‘microsoftrmsonline@<YourTenantID>.rms.<region>.aadrm.com’**
  + This value indicates that an Office 365 service, like SharePoint Online or Exchange Online, is requesting the RMS service. The <YourTenantID> is the GUID vfor the tenant and <region> is the region where the tenant is registered: na is North America, eu is Europe, ap is Asia.
* If using the RMS Connector, requests will be logged with the service principal name that RMS has automatically generated upon installation of the RMS Connector.
  1. Frequently Used Requests

The following table describes the commonly used request types in Azure RMS:

| Request Type | Description |
| --- | --- |
| AcquireLicense | The client is requesting a license for a specific piece of content, from a Windows-based computer. |
| FECreateEndUserLicenseV1 | Similar to the AcquireLicense request but from mobile devices |
| Certify | The client is requesting a certificate (that is later used to get a license) from a Windows-based computer |
| GetClientLicensorCert | The client is requesting a publishing certificate (that is later used to protect content) from a Windows-based computer. |
| FECreatePublishingLicenseV1 | The same as Certify and GetClientLicensorCert combined, from mobile clients. |
| FindServiceLocationsForUser | Sometimes anonymous and sometimes with authentication. This request queries for the URLs to certify and acquire licenses. |
| Decrypt | Applicable only to bring your own key (ByoK) scenarios. RMS logs when your key is used for decryption and this is typically one time per AcquireLicence (or FECreateEndUserLicenseV1). |
| Sign | Applicable only to bring your own key (ByoK) scenarios. RMS logs when your key is used for signing and this is typically one time per AcquireLicence (or FECreateEndUserLicenseV1), Certify, and GetClientLicensorCert (or FECreatePublishingLicenseV1). |