Planning to Deploy the On-Premises RMS Connector

The Microsoft Rights Management (RMS) connector enables existing on-premises servers to use Information Rights Management (IRM) functionality with the cloud-based Azure Information Protection services (Azure RMS).

With this functionality you don't need an AD RMS infrastructure to use RMS features (IRM) with on-premises Exchange, SharePoint, and file servers with file classification infrastructure. They can directly utilize the Azure RMS functionalities with the RMS connector.

This topic examines the following information for deploying the RMS connector:

- Planning considerations when deploying the RMS connector
- Prerequisites for the RMS connector
- Credentials for the RMS connector
- Monitoring the RMS connector

Planning considerations when deploying the RMS connector

The RMS connector is delivered as an executable (.exe) and can be installed on any Windows server. When deciding for an RMS connector server, you should consider the following:

- Every on-premises IRM operation needs an RMS Connector being available, so you must plan one or multiple RMS connector servers to provide high availability.
- The RMS connector is installed with an IIS site available unencrypted (HTTP). You should consider this when planning a load balancer or deploy a certificate to use encryption (HTTPS).
- The server for RMS connector cannot host web services or be a Domain Controller.
- The RMS connector must not be installed on servers that are used for scanning such as file or SharePoint servers.
- The RMS connector can be installed on any physical or virtual machine, hosted on-premises or in Azure.
- The RMS connector needs access to the Internet via a firewall (or web proxy) that does not require authentication.
- Any RMS connector must be placed in the same AD domain as the on-premises service that will use them. Each domain in your forest that you plan to scan using RMS connector need its own RMS connector server.
- After setting up the RMS connectors, all servers that will use them have to be configured by a server and service administrator.
- There is no limit to the number of RMS connector servers that you can run for your organization.
- All connector servers installed share the same configuration, downloaded from the Azure tenant they are connected to.
- Provide the required credentials for the on-premises servers and Azure AD for your tenant.

Prerequisites for the RMS connector

Before you can install the RMS connector on a server, the machine must fulfill the following prerequisites.

Requirement	Description
Azure Information Protection is activated	The Azure RMS service must be activated in prior configuring the RMS connector.
Directory synchronization between on-premises Active Directory forests and Azure Active Directory	Azure Active Directory must be configured to work with the users and groups in your Active Directory database. Note: You must do this directory synchronization step for the RMS connector to work. Cloud-only Azure Active Directory Accounts with manual password synchronization are not sufficient.
Hardware requirements	Windows Server 2008 R2 / 2012 / 2012 R2 / 2016 in (x64) are supported At least 1 GB of RAM A minimum of 64 GB of disk space At least one network interface Access to the Internet via a firewall (or web proxy) that does not require authentication

Credentials for the RMS connector

You must provide two administrator identities for installing the RMS connector.

Identity	Access rights
On-premises credentials for installing the executable	• Local machine administrator
Azure AD admin account for accessing the AIP service	An identity with one of the following roles in the tenant: • Global administrator • Azure Rights Management global administrator • Azure Rights Management connector administrator

There are also additional requirements for the Azure AD admin account:

- This account must not require multi-factor authentication (MFA) because MFA is not supported.

- You cannot use a password that has any of the following characters:
    - Ampersand (&)
    - left angle bracket ([ )
    - right angle bracket ( ])
    - straight quotation (")
    - apostrophe (')
- Make sure the account you specify can use the AIP service and protect content.

Monitoring of the RMS connector

You can monitor the use and health of the RMS connector by using the tools identified in the following table.

Logging Tool	**Description**
Application event log entries	The RMS connector uses the Application event log to record entries for the 11 different applications actions.
Performance counters	When you install the RMS connector, it automatically creates "Microsoft Rights Management" connector performance counters.
RMS connector logging	Usage logging helps you identify when emails and documents are protected and consumed.

While the event logging is useful for the basic monitoring, the performance counters and usage logging are more useful for diagnosis purposes.

Additional reading: For more information, see the following article about the RMS connector installation process.