Protecting files in the cloud with Azure Information Protection

We're a cloud-first organization, so most applications at Microsoft are in the cloud, including SharePoint, email and productivity applications, and personal file storage. To better protect data where it resides, Core Services Engineering and Operations (CSEO) has migrated from Active Directory Rights Management Services (AD RMS) to Azure Information Protection (AIP)—which includes the protection capabilities formerly known as Azure RMS.

Azure Information Protection, part of the Enterprise Mobility + Security suite, is a cloud-based service that helps you discover, classify, label, and protect sensitive data both in the cloud and on-premises. Azure Information Protection uses encryption, identity, and authorization policies to help secure files and email across multiple devices, including phones, tablets, and PCs.

Azure Information Protection enables protected sharing in Microsoft Office and on a variety of platforms including Windows, Mac OS, iOS, Android. It supports mobility for employees who take advantage of our bring-your-own-device (BYOD) policy. Azure Information Protection helps protect data both inside and outside the organization because sensitivity labels and protection stay with the data—even when it leaves the corporate network boundaries.

Some of the benefits that we have realized include:

- Increased scalability. It runs as a cloud service, with the elasticity to scale up and out. We don't have to provision or deploy more on-premises servers.
- Improved manageability. It is easier to manage as a cloud service. It offers auditing and monitoring capabilities, allows us to create simple and flexible policy templates, and it supports on-premises and cloud services plus a broad range of applications.
- Cost effectiveness. We migrated with no hardware investment, and we don’t have to worry about maintaining servers or updating software.
- End-user experience. We gained the ability to better guide information workers on how to handle and protect sensitive data through recommended labeling and protection.

Migrating from AD RMS to Azure Information Protection paves the way for protecting sensitive data using additional capabilities.

Planning the move to the cloud

We have used AD RMS since its release in 2002. Many of our business apps depended on AD RMS encryption and information protection, and everyone with a Microsoft email address could use AD RMS templates for email protection. We used it to:

- Protect Microsoft Office documents from accidental disclosure and negligent sharing.
- Limit access to individuals or certain groups.
- Allow read-only or editing permissions.
- Allow only specific users to print or copy the content in sensitive documents.

When we started planning the move to Azure Information Protection, we needed to make sure that we offered a smooth transition with no downtime. We developed a strategy that would migrate users, templates, and applications in phases. Upon completion, we could then begin to use other capabilities in Azure Information Protection, including labeling and classification.
How Azure Information Protection protects data

Azure Information Protection makes the data in a document unreadable to anyone other than authorized users and services. It uses unique keys and certificates to manage encryption and decryption, and to authorize and enforce restrictions. Data is encrypted at the application level, which includes a policy that defines authorized use for a document. When a protected document is used by a legitimate user or it is processed by an authorized service, the data in the document is decrypted and the rights that are defined in the policy are enforced.

For more information about Azure Information Protection and how it works, go [here](#).

Configuring Azure Information Protection

At Microsoft, we have an Active Directory infrastructure with multiple forests and domains, and most of our client devices run RMS-enabled versions of Office 2013, Office 2016, or Office 365 Pro Plus. Azure Information Protection receives authentication and authorization information from Active Directory Federation Services (AD FS), Active Directory Domain Services, and Azure Active Directory (Azure AD).

We were able migrate to Azure Information Protection with no domain-level restructuring, architecture changes, or changes to existing services. Having multiple versions of Office did not affect our plans to migrate to Azure Information Protection, because the versions we run are compatible with both AD RMS and Azure Information Protection.

**NOTE: If you need to send protected emails or documents to external users, learn more [here](#).**

To configure the service at Microsoft, we had to migrate templates, install the Microsoft RMS Connector, migrate applications, and then migrate users and partners.

Migrating templates

We have several custom rights policy templates that we use to:

- Grant rights to a subset of users.
- Define a subset of users who can see and select a template (departmental template) from applications, rather than allow all users in the organization to see and select the template.
- Define custom rights for a template, such as View and Edit, but not Copy and Print.
- Configure more options in a template, including an expiration date and whether the content can be accessed without an Internet connection.

All our current templates within our configuration were migrated from AD RMS. We exported the templates from AD RMS to an XML file, and then uploaded that file to Azure Information Protection using a PowerShell cmdlet.

Creating and managing templates

An Azure global administrator can create and manage templates in the Azure classic portal. To minimize risk, we have only one Azure global administrator for the service. In addition to creating and managing templates from the Azure portal, we have a small group of administrators who can also create and manage templates using PowerShell.

For more information about managing and creating templates, read [Configuring and managing templates in the Azure Information Protection policy](#).

Installing the RMS connector

Microsoft RMS Connector is a small-footprint service that acts as a relay, allowing on-premises services to connect and consume Azure Information Protection. For fault tolerance and high availability, we [installed the RMS connector](#) on six virtual machines—the minimum requirement for the service is two.

[Source](microsoft.com/itshowcase)
Even though most people connect to online services, we use the RMS connector to support Microsoft Exchange and Microsoft SharePoint deployments that stay on-premises. For example, some employee mailboxes use Exchange Online and some use Exchange Server.

With the RMS connector installed, information protection now works seamlessly between our on-premises and cloud deployment configurations, as shown in Figure 1.

Figure 1. RMS connector service architecture

The Azure Information Protection global administrator authorized servers to use the RMS connector. We configured load balancing and high availability using Network Load Balancing on the Azure RMS virtual machine cluster.

**Migrating applications**

One of the more challenging tasks that we faced during this migration was making sure all the existing apps that had dependency on AD RMS pointed to Azure Information Protection. Using Group Policy, we ran a Microsoft Rights Management connector script, which we customized for our environment, on application servers. The script modified the registry to change the pointer to Azure Information Protection.

To track progress during the migration, we ran a different PowerShell script twice a month to parse IIS logs and check service and user accounts that were still using the AD RMS cluster. Once we identified which service accounts were still connecting for certificates and were accessing the licensing server, we worked with those app owners to make the changes that were necessary before the AD RMS service was shut down.

We created an internal website to communicate with app owners, which included a migration schedule, frequently asked questions about the service, and how to point their servers to Azure Information Protection. It helped reduce overall ambiguity about the migration and helped app owners understand what they needed to do.
Migrating users

We gradually added members from different domains until all client machines were moved. For domain-joined devices, we used Group Policy in the form of a user sign-in script. We added groups and people to the Azure Information Protection service and then pushed out a script to change configurations and update the pointers on client devices.

User migration went smoothly because we worked in phases and started with smaller pilot groups. The overall client deployment was partially managed by asking clients to install (at minimum) Windows 10 Anniversary Update, which would also install the Group Policy client script. Because the templates and applications were already moved, the environment looked the same to users. For non-domain-joined devices managed by Microsoft Intune, running Windows 10 Anniversary Update or later, we deployed a package that included a migration script through Intune.

Migrating partners

Microsoft shares protected information with partners, so we migrated partners to Azure Information Protection for protected sharing. Before migrating any partner companies, we needed all of them to create a Microsoft Online Services tenant and move their organization keys to the cloud.

Each of the partner companies that we share protected information with introduced configuration settings in their environment to redirect client applications to the right content protection infrastructure (on-premises or cloud) depending on the stage of the migration they were in. Partner migration involved the same steps, so our work consisted primarily of coordinating timing for the steps with the partner.

Migrating to Azure Key Vault

Azure Information Protection uses cryptographic controls, also called keys, to make sure that the security protection it offers is industry-standard. For each document or email that is protected by Azure Information Protection, Azure Information Protection creates a single Advanced Encryption Standard (AES) key, and that key is embedded in the document. The unique AES key, the organization’s tenant key, and the file’s policies are managed by Azure Information Protection.

Azure Key Vault offers a centralized key management solution for many cloud-based and on-premises services that use encryption. Some of the benefits of using Azure Key Vault for the Azure Information Protection tenant key include:

- Azure Key Vault supports several built-in interfaces for key management, including PowerShell, CLI, REST APIs, and the Azure portal.
- Azure Key Vault separates roles as a recognized security best practice.
- Azure Key Vault offers a high level of control for where the master key is stored because the service is available in many Azure regions.

In the first phases of the migration, due to the limitations of integrating Exchange Online and Bring your own Key (BYOK), we chose to migrate our keys into the Key Management Service that was part of Azure Information Protection without using BYOK. Once the restrictions in Exchange Online for BYOK were lifted, as part of an upgrade to that platform, we migrated the keys to Azure Key Vault.

Auditing and reporting

Although the RMS connector logs information, warning, and error messages to the event log, there isn’t a management pack that monitors for these events. We use System Center Configuration Manager to monitor those logs. To see a list of the events and their descriptions, along with more information, read Monitor the Azure RMS connector.
We’ve put a lot of effort into creating key performance indicators (KPIs) that measure template use. Those KPIs tell us what templates are used the most and which templates may be retired. This is particularly important to us as we are rolling out Azure Information Protection. With Azure Information Protection, we are changing the templates we want people to use and archiving older ones. It’s a gradual process, but having usage metrics makes it easy to see if new templates are being used, or if we need to engage with users to better prepare them for a template change. For more information about using logs to analyze usage data, read [Logging and analyzing usage of the Azure Rights Management service](https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/log-analysis).

**Best practices**

On our journey to Azure Information Protection, we learned some important lessons, including:

- Keep templates static during migration. To reduce complexity during the migration, we kept all our templates static until the migration was complete. If you change a template during migration, you will need to change it in multiple places, which increases the opportunity for errors. Now that we are done with the migration and we are moving on to other capabilities in Azure Information Protection, we are changing some template names to make them more relevant to users in different regions. We are also looking at template usage metrics to rationalize our published template portfolio, and we are replacing or archiving templates that aren’t being used.

- Understand and document your environment. Most of the migration challenges that we faced were related to incomplete or out-of-date documentation. When we were migrating applications, we had to rely on tracking the declining connection counts to the AD RMS cluster, via the collected IIS logs. Because not all app dependencies were documented, it needed a lot of up-front effort and created challenges when the listed application owners weren’t available. We had to continuously follow up with the owners to determine if they had migrated or not.

- Introduce Azure Information Protection to users as a transparent migration. We initially introduced the service to users as a transparent migration, with no obvious new features, to simplify the process. Then we started enabling and advertising the new Azure Information Protection features such as classification, tracking, and revocation.

- Protect accounts with elevated rights. Accounts with elevated rights, such as Azure global admin, can increase risk if a user’s primary corporate credentials are persistently elevated. There are a couple of ways to minimize that risk—you can either assign a secondary, privileged identity to use only when needed for admin tasks, or use a just-in-time elevated access tool such as Azure Privileged Identity Management. It elevates rights for a pre-defined duration, after which the rights expire.

**Conclusion**

We have completed our migration at scale. During each minute of the workday at Microsoft, 2,500 to 3,000 licensed users access the system to create new content, access existing encrypted content, or decrypt shared content. Azure Information Protection allowed for a seamless encryption/decryption service transition, and there was no discernable difference in the way the service works for users. For service managers, this service offers better logging and usage tracking than we had with AD RMS. Since the migration, we are saving costs because we don’t have a physical infrastructure to deploy, manage, update, or maintain—all those activities are part of the Azure subscription. Maintaining this service requires 66 percent less administrative resources than we needed for AD RMS.

Migrating to Azure Information Protection was the first step on our journey toward building a foundation for discovering, classifying, labeling, and protecting sensitive data at Microsoft using Azure Information Protection. For more information about starting your own migration, read [Migrating from AD RMS to Azure Information Protection](https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/migrate-from-ad-rms).

**For more information**

**Microsoft IT Showcase**

[microsoft.com/ITShowcase](https://microsoft.com/ITShowcase)

[Using Azure Information Protection to classify and label corporate data](https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/migrate-from-ad-rms)
Requirements for Azure Information Protection

What problems does Azure RMS solve?

Comparing Azure Information Protection and AD RMS

Microsoft Azure Key Vault helps protect keys, secrets, and certificates

© 2018 Microsoft Corporation. This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS SUMMARY. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.