

Contents

Azure Information Protection Documentation

Overview

[What is Azure Information Protection?](#)

[Azure Information Protection and AD RMS](#)

[Compare on premises and AD RMS](#)

[Manage Active Directory Mobile Device Extensions](#)

Requirements

[Overview](#)

[Azure Active Directory requirements](#)

[Client device support for protection](#)

[Application support for protection](#)

[On-premises server support for protection](#)

Quickstarts

[Get started in the Azure portal](#)

[Find what sensitive information you have](#)

[Configure a label to protect emails - classic client](#)

[Create a new label for specific users - classic client](#)

Tutorials

[Edit the policy and create a new label - classic client](#)

[Configure policy settings that work together - classic client](#)

[Configure client settings to control oversharing - classic client](#)

Concepts

[Overview of the Azure Information Protection policy](#)

[Rights Management protection](#)

[Overview](#)

[How does it work?](#)

[How applications support Azure Rights Management protection](#)

[Overview](#)

[Office applications and services](#)

File servers that run Windows Server and use File Classification Infrastructure

Other applications that support the RMS APIs

RMS for individuals and Azure Information Protection

Also known as ...

How-to guides

How-tos for common scenarios

Plan & prepare for the service

Deployment roadmap

Migrating from AD RMS

Overview

Preparation

Server-side configuration

Overview

Software key to software key

HSM key to HSM key

Software key to HSM key

Client-side configuration

Supporting services configuration

Post migration tasks

Planning and implementing your tenant key

Overview

BYOK details

Preparing users and groups

Configure & use the service

Activating protection

Overview

Microsoft 365 admin center

Azure portal

Configuring applications

Overview

Office 365 services

Office apps

- [Azure Information Protection client](#)
 - [Configuring usage rights](#)
 - [Configuring super users for discovery services or data recovery](#)
 - [Configuring the Azure Information Protection policy](#)
 - [Overview](#)
 - [The default policy](#)
 - [Configure the policy settings](#)
 - [Create a new label](#)
 - [Add or remove a label](#)
 - [Delete or reorder a label](#)
 - [Change a label](#)
 - [Configure protection](#)
 - [Overview](#)
 - [HYOK](#)
 - [Configure visual markings](#)
 - [Configure conditions](#)
 - [Configure scoped policies](#)
 - [Configure and manage templates](#)
 - [Overview](#)
 - [Refresh templates for users](#)
 - [PowerShell reference](#)
 - [Migrating from the Azure classic portal](#)
 - [Configure languages](#)
 - [Activate unified labels](#)
 - [Configure secure document collaboration](#)
 - [Configuring mail flow rules for Azure Information Protection labels](#)
 - [Azure Information Protection unified labeling scanner](#)
 - [Overview](#)
 - [Unified labeling scanner prerequisites](#)
 - [Configure and install the unified labeling scanner](#)
 - [Run the unified labeling scanner](#)
 - [Azure Information Protection classic scanner](#)

- [Overview](#)
- [Classic scanner prerequisites](#)
- [Configure and install the classic scanner](#)
- [Run the classic scanner](#)
- [Reporting for Azure Information Protection](#)
- [Deploying the RMS connector](#)
 - [Overview](#)
 - [Install and configure the connector](#)
 - [Configure servers](#)
 - [Overview](#)
 - [Registry settings](#)
 - [Monitor the connector](#)
- [Verifying the Azure Rights Management service](#)
- [Helping users to protect files](#)
- [Logging and analyzing usage](#)
- [Operations for your tenant key](#)
 - [Overview](#)
 - [Microsoft-managed](#)
 - [Customer-managed](#)
- [Manage personal data for Azure Information Protection](#)
- [Decommissioning and deactivating](#)
- [Administering with PowerShell](#)
 - [Overview](#)
 - [Installing the AIPService PowerShell module](#)
- [Deploy & use the client](#)
 - [Client deployment solutions](#)
 - [Overview](#)
 - [Azure Information Protection unified labeling client](#)
 - [Overview](#)
 - [Version history](#)
 - [Admin guide](#)
 - [Overview](#)

[Install the client for users](#)

[Customizations](#)

[Client files and usage logging](#)

[File types supported](#)

[PowerShell commands](#)

[User guide](#)

[Overview](#)

[Download and install the client](#)

[Classify a file or email](#)

[Classify and protect a file or email](#)

[Open files that have been protected](#)

[Remove labels and protection](#)

[Azure Information Protection client \(classic\)](#)

[Overview](#)

[Version history](#)

[Admin guide](#)

[Overview](#)

[Install the client for users](#)

[Customizations](#)

[Client files and usage logging](#)

[Document tracking](#)

[File types supported](#)

[PowerShell commands](#)

[User guide](#)

[Overview](#)

[Download and install the client](#)

[Classify a file or email](#)

[Classify and protect a file or email](#)

[Track and revoke your documents](#)

[Open files that have been protected](#)

[Remove labels and protection](#)

[Protection-only mode](#)

[Tasks that you used to do with the RMS sharing application](#)

[Azure Information Protection apps for iOS and Android](#)

[Overview](#)

[Start using the AIP mobile apps](#)

[Protected PDF readers](#)

[Overview](#)

[Windows](#)

[macOS](#)

[iOS](#)

[Android](#)

[RMS client deployment notes](#)

[RMS protection with Windows Server FCI](#)

[Overview](#)

[PowerShell script](#)

[Develop & customize apps](#)

[Developer's Guide](#)

[Microsoft Information Protection](#)

[Rights Management SDK 4.2](#)

[Deprecation notice](#)

[Overview](#)

[Get started](#)

[What's new](#)

[Setup Developer environment](#)

[Android setup](#)

[Linux setup](#)

[iOS and OS X setup](#)

[Windows Phone setup](#)

[Windows Store setup](#)

[Code examples](#)

[Android code examples](#)

[Linux code examples](#)

[iOS/OS X code examples](#)

[Community resources](#)

[Developer guidance](#)

[How to register and RMS enable your app with Azure AD](#)

[How to enable error and performance logging](#)

[How to use built-in rights](#)

[How to use document tracking](#)

[API reference](#)

[Android API Reference](#)

[Linux API reference](#)

[iOS / OS X API reference](#)

[Windows API Reference](#)

[Rights Management SDK 2.1](#)

[Overview](#)

[Client](#)

[Server](#)

[Get started](#)

[Release notes](#)

[Install the SDK](#)

[Configure Visual Studio](#)

[Developing your application](#)

[Testing your application](#)

[Deploy into production](#)

[Developer guidance](#)

[How-to use ADAL authentication](#)

[Configure Azure RMS for ADAL authentication](#)

[How to add explicit owner rights](#)

[How to debug a rights-enabled application](#)

[How to deploy an app](#)

[How to enable document tracking and revocation](#)

[How to enable email notification](#)

[How to enable your service application to work with cloud-based RMS](#)

[How to install and configure an RMS server](#)

- [How to set the API security mode](#)
- [How to work with encryption settings](#)
- [Application types](#)
- [File API configuration](#)
- [Security guide](#)
- [Supported file formats](#)
- [Supported platforms](#)
- [Understanding usage restrictions](#)

[API Reference](#)

- [Constants](#)
- [Data types](#)
- [Functions](#)
- [Structures](#)
- [Error codes](#)

[Terms](#)

[Resources](#)

[Frequently asked questions](#)

- [FAQs - general](#)
- [FAQs - classification & labeling](#)
- [FAQs - data protection](#)

[Information and support](#)

- [Compliance & supporting information](#)

- [PowerShell reference](#)

- [Audit log reference](#)

- [Terminology](#)

What is Azure Information Protection?

7/20/2020 • 7 minutes to read • [Edit Online](#)

Applies to: [Azure Information Protection](#)

Azure Information Protection (AIP) is a cloud-based solution that enables organizations to classify and protect documents and emails by applying labels. Labels can be applied automatically by administrators using rules and conditions, manually by users, or by a combination where administrators define the recommendations shown to users.

For example, your administrator might configure a label with rules that detect sensitive data, such as credit card information. In this case, any user who saves credit card information in a Word file might see a tooltip at the top of the document, recommending that they apply the label configured for this scenario.

Labels can both classify, and optionally protect, the document.

[Classifying](#) and [protecting](#) content enables you to track and control how it is used, analyze data flows to gain insight into your business, detect risky behaviors and take corrective measures, track document access, prevent data leakage or misuse, and more.

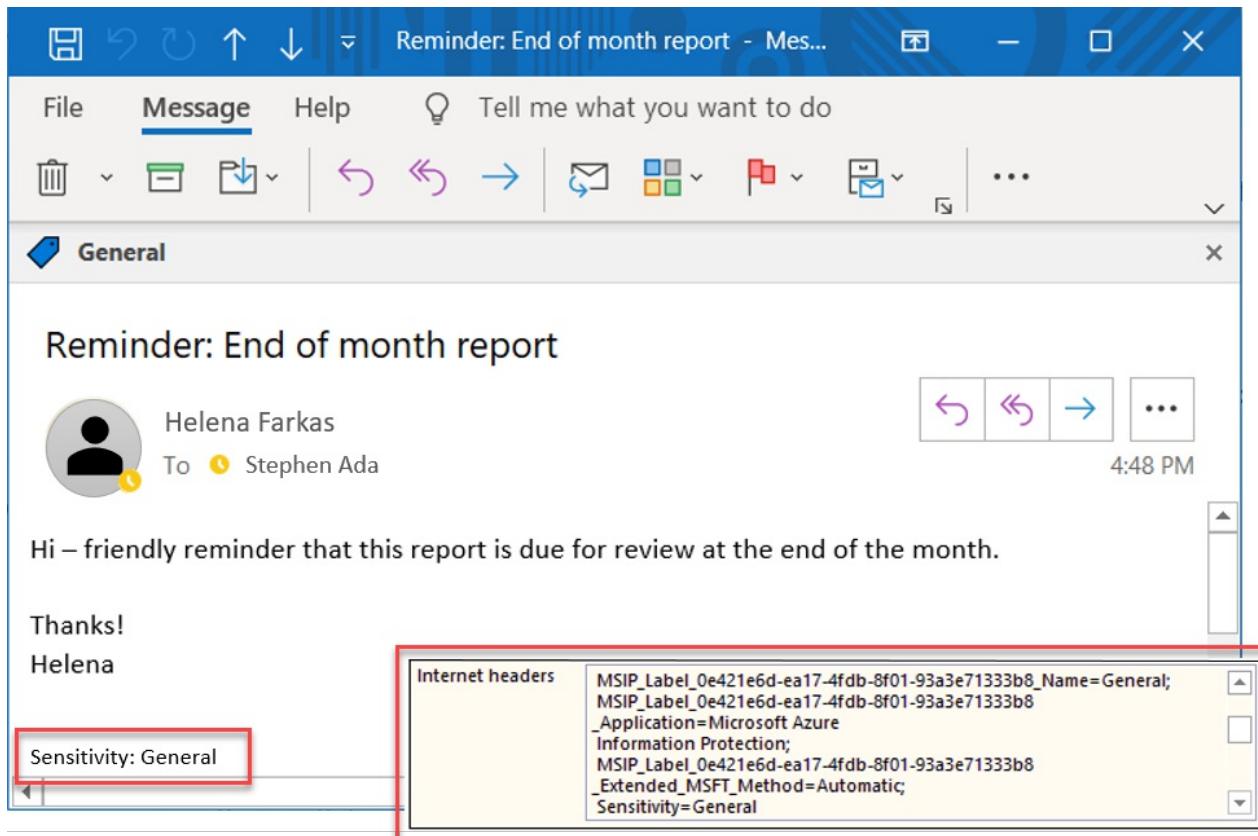
How labels apply classification

Use Azure Information Protection labels to apply classification to both documents and emails.

Labeling content includes:

- **Classification** that can be detected regardless of where the data is stored or with whom it's shared.
- **Visual markings**, such as headers, footers, or watermarks.
- **Metadata**, added to files and email headers in clear text. The clear text metadata ensures that other services can identify the classification and take appropriate action

For example, in the image below, labeling has classified an email message as *General*, using the [unified labeling client](#):



In this example, the label also:

- **Added a footer of *Sensitivity: General* to the email message.** This footer is a visual indicator for all recipients that it's intended for general business data that should not be sent outside of the organization.
- **Embedded metadata in the email headers.** Header data enables email services can inspect the label and theoretically create an audit entry or prevent it from being sent outside of the organization.

How data is protected

Azure Information Protection uses the *Azure Rights Management service* (Azure RMS) to protect your data. Azure RMS is integrated with other Microsoft cloud services and applications, such as Office 365 and Azure Active Directory, and can also be used with your own or third-party applications and information protection solutions. Azure RMS works with both on-premises and cloud solutions.

Azure RMS uses encryption, identity, and authorization policies. Similar to AIP labels, protection applied using Azure RMS stays with the documents and emails, regardless of the document or email's location, ensuring that you stay in control of your content even when it's shared with other people.

Protection settings can be part of your label configuration, so that users both classify and protect documents and emails simply by applying a label. Protection settings can also be used on their own, by applications and services that support protection but not labeling. For applications and services that support protection only, protection settings are used as [Rights Management templates](#).

For example, you may want to configure a report or sales forecast spreadsheet so that it can be accessed only by people in your organization. In this case, you'd apply protection settings to control whether that document can be edited, restrict it to read-only, or prevent it from being printed.

Emails can have similar protection settings to prevent them from being forwarded or from using the Reply All option.

Rights Management templates

As soon as the Azure Rights Management service is activated, two default templates are available for you that restrict data access to users within your organization. Use these templates immediately, or configure your own

protection settings to apply more restrictive controls in new templates.

Rights Management templates can be used with any applications or services that support Azure Rights Management.

The following image shows an example from the Exchange admin center, where you can configure Exchange Online mail flow rules to use RMS templates:

The screenshot shows the Exchange admin center interface. On the left, there's a configuration pane for a rule named 'Apply data protection'. It includes fields for 'The recipient is...' (set to "'New Launch Team'") and 'Do the following...' (with 'Apply rights protection to the message' selected). A 'select RMS template' dialog box is open over the main pane, listing several RMS templates: 'Sales and Marketing - Read and Print Only' (selected), 'Sales and Marketing - Read and Print Only', 'VanArsdel, Ltd - Confidential View Only', 'VanArsdel, Ltd - Confidential', and 'Do Not Forward'.

NOTE

Creating an AIP label that includes protection settings also creates a corresponding Rights Management template that can be used separately from the label.

For more information, see [What is Azure Rights Management?](#)

AIP and end-user integration for documents and emails

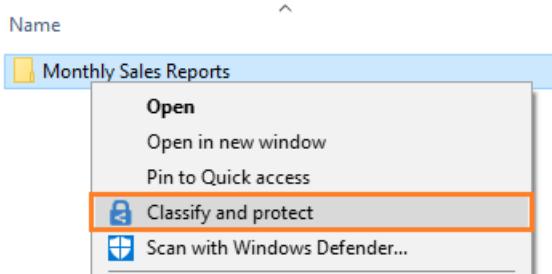
The AIP client installs the Information Protection bar to Office applications and enables end users to integrate AIP with their documents and emails.

For example, in Excel, using the [unified labeling client](#):

The screenshot shows an Excel spreadsheet titled 'Inventory list example'. The ribbon is visible at the top, and the 'Information Protection' tab is active. An orange box highlights the classification dropdown menu in the ribbon, which includes options like 'General', 'Personal', 'Public', 'Confidential', and 'Highly Confidential'. The main content area displays a table of inventory items with columns for 'For Reorder', 'Inventory ID', 'Name', 'Description', 'Unit Price', 'Quantity in Stock', 'Inventory Value', 'Reorder Level', and 'Reorder Time in Days'. The first row contains headers, and rows 4 through 7 contain data. Row 7 is highlighted in blue and labeled 'Inventory List'. The bottom status bar shows 'Ready'.

While labels can be applied automatically to documents and emails, removing guesswork for users or to comply with an organization's policies, the Information Protection bar enables end users to select labels and apply classification on their own.

Additionally, the AIP client enables users to classify and protect additional file types, or multiple files at once, using the right-click menu from Windows File Explorer. For example:



The **Classify and protect** menu option works similarly to the Information Protection bar in Office applications, enabling users to select a label or set custom permissions.

TIP

Power users or administrators might find that PowerShell commands are more efficient for managing and setting classification and protection for multiple files. [Relevant PowerShell commands](#) are included with the client, and can also be installed separately.

Users and administrators can use document tracking sites to monitor protected documents, watch who accesses them, and when. If they suspect misuse, they can also revoke access to these documents. For example:



Additional integration for email

Using AIP with Exchange Online provides the additional benefit of sending protected emails to any user, with the assurance that they can read it on any device.

For example, you may need to send sensitive information to personal email addresses that use a **Gmail**, **Hotmail**, or **Microsoft** account, or to users who don't have an account in Office 365 or Azure AD. These emails should be encrypted at rest and in transit, and be read only by the original recipients.

This scenario requires [Office 365 Message Encryption capabilities](#). If the recipients cannot open the protected email in their native email client, they can use a one-time passcode to read the sensitive information in a browser.

For example, a Gmail user might see the following prompt in an email message they receive:

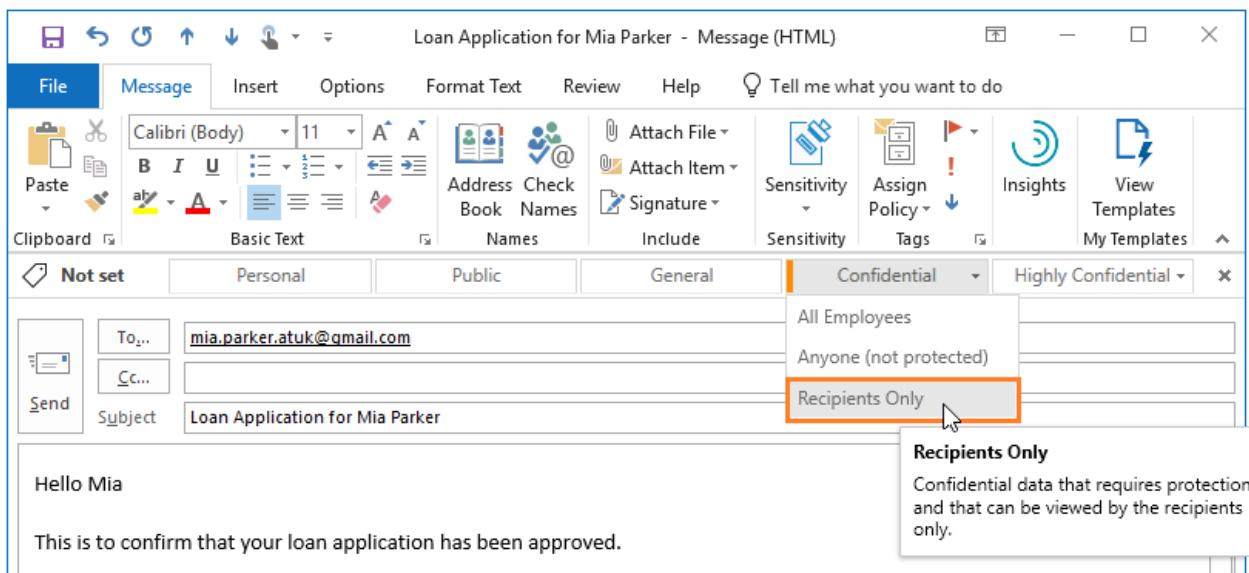
Sign in to view the message



Or, sign in with a one-time passcode

For the user sending the email, the actions required are the same as for sending a protected email to a user in their own organization. For example, select the **Do Not Forward** button that the AIP client can add to the Outlook ribbon.

Alternately, Do Not Forward functionality can be integrated into a label that users can select to apply both classification and protection to that email. For example, in the [unified labeling client](#):



Administrators can also automatically provide protection for users by configuring mail flow rules that apply rights protection.

Any Office documents attached to these emails are automatically protected as well.

Scanning for existing content to classify and protect

Ideally, you'll be labeling documents and emails as they're created. However, you likely have many existing documents, stored either on-premises or in the cloud, and want to classify and protect these documents as well.

Use one of the following methods to classify and protect existing content:

- **On-premises storage:** Use the [Azure Information Protection scanner](#) to discover, classify, and protect documents on network shares and Microsoft SharePoint Server sites and libraries.

The scanner runs as a service on Windows Server, and uses the same policy rules to detect sensitive information and apply specific labels to documents.

Alternately, use the scanner to apply a default label to all documents in a data repository without inspecting the file contents. Use the scanner in reporting mode only to discover sensitive information that you might not know you had.

- **Cloud data storage:** Use [Microsoft Cloud App Security](#) to apply your labels to documents in Box, SharePoint, and OneDrive. For a tutorial, see [Automatically apply Azure Information Protection classification labels](#)

Latest labeling updates for Microsoft 365

See the latest information about how Azure Information Protection helps you to discover, classify, protect, and monitor your sensitive information, wherever it lives, using Microsoft 365:

Additional Azure Information Protection resources

- Free trial: [Enterprise Mobility + Security E5](#)
- Subscription options and pricing: [Azure Information Protection Pricing](#)
- Download the client: [Azure Information Protection client](#)
- Download a customizable user guide: [Azure Information Protection End User Adoption Guide](#)

- FAQs: [Frequently asked questions for Azure Information Protection](#)
- Yammer: [Azure Information Protection](#)
- What's new in the documentation: [Azure Information Protection technical blog](#)

Additional resources: [Information and support for Azure Information Protection](#)

Microsoft Ignite

Microsoft Ignite 2019 in Orlando was a great success! There was lots of good information about Azure Information Protection with the latest updates and improvements. If you couldn't join us, sessions are recorded for viewing later.

See the following list for our top five sessions that we recommend:

- [BRK2119 - Secure your sensitive data! Understanding the latest Microsoft Information Protection capabilities](#)
- [THR3067 - Know your data: Top five tips and tricks to better understand your sensitive data landscape](#)
- [BRK3103 - Protecting sensitive files and data can be hard. Choose the right data protection options that balance security and worker productivity](#)
- [BRK2120 - Got Azure Information Protection? Navigating unified labeling, policy configuration, clients, and analytics](#)
- [BRK2121 - Extend the power of sensitivity labeling and protection to your own apps and ISV solutions with the Microsoft Information Protection SDK](#)

Latest blog post: [Understand where your sensitive data is located and intelligently protect it with Microsoft 365](#)

Next steps

Configure and see Azure Information Protection for yourself with our [quickstarts](#) and [tutorials](#). If you're ready to deploy this service for your organization, head over to the [how-to guides](#).

Comparing Azure Information Protection and AD RMS

7/20/2020 • 5 minutes to read • [Edit Online](#)

Applies to: Active Directory Rights Management Services, Azure Information Protection, Office 365

If you know or have previously deployed Active Directory Rights Management Services (AD RMS), you might be wondering how Azure Information Protection compares in terms of functionality and requirements as an information protection solution.

Some of the main differences for Azure Information Protection:

- **No server infrastructure required:** Azure Information Protection doesn't require the additional servers and PKI certificates that AD RMS needs, because Microsoft Azure takes care of those for you. That makes this cloud solution quicker to deploy and easier to maintain.
- **Cloud-based authentication:** Azure Information Protection uses Azure AD for authentication - for both internal users and users from other organizations. That means your users can be authenticated even when they are not connected to your internal network and it is easier to share protected content with users from other organizations. Many organizations already have user accounts in Azure AD because they are running Azure services or have Office 365. But if not, RMS for individuals lets users create a free account, or a Microsoft account can be used for [applications that support this authentication for Azure Information Protection](#). In comparison, to share AD RMS protected content with another organization, you must configure explicit trusts with each organization.
- **Built-in support for mobile devices:** No deployment changes are needed for Azure Information Protection to support mobile devices and Mac computers. To support these devices with AD RMS, you must install the mobile device extension, configure AD FS for federation, and create additional records for your public DNS service.
- **Default templates:** Azure Information Protection automatically creates default templates that restrict access of the content to your own organization. These templates make it easy to start protecting sensitive data immediately. There are no default templates for AD RMS.
- **Departmental templates:** Also known as scoped templates. Azure Information Protection supports departmental templates for additional templates that you create. This configuration lets you specify a subset of users to see specific templates in their client applications. Limiting the number of templates that users see makes it easier for them to select the correct policy that you define for different groups of users. AD RMS doesn't support departmental templates.
- **Document tracking and revocation:** Azure Information Protection supports these features with the Azure Information Protection client (classic), whereas AD RMS does not.
- **Classification and labeling:** Azure Information Protection supports labels that apply classification, and optionally, protection. These capabilities are provided with the [Azure Information Protection client \(classic\)](#) and the [Azure Information Protection unified labeling client](#). Using these clients, classification and labeling can be integrated with Office applications, File Explorer, PowerShell, and a scanner for on-premises data stores. AD RMS does not support these classification and labeling capabilities.

In addition, because Azure Information Protection is a cloud service, it can deliver new features and fixes more quickly than an on-premises server-based solution. There are no new features planned for AD RMS in Windows

Server.

For other differences, use the following table for a side-by-side comparison. If you have security-specific comparison questions, see the [Cryptographic controls for signing and encryption](#) section in this article.

AZURE INFORMATION PROTECTION	AD RMS
Supports information rights management (IRM) capabilities in both Microsoft Online services and on-premises Microsoft server products.	Supports information rights management (IRM) capabilities for on-premises Microsoft server products, and Exchange Online.
Automatically enables secure collaboration on documents with any organization that also uses Azure AD for authentication.	Secure collaboration on documents outside the organization requires authentication trusts to be explicitly defined in a direct point-to-point relationship between two organizations. You must configure either trusted user domains (TUDs) or federated trusts that you create by using Active Directory Federation Services (AD FS).
Send a protected email (optionally, with Office document attachments that are automatically protected) to users when no authentication trust relationship exists. This scenario is made possible by using federation with social providers or a one-time passcode and web browser for viewing.	Does not support sending protected email when no authentication trust relationship exists.
Supports the Azure Information Protection client (classic) and the Azure Information Protection unified labeling client for both protection and consumption activities.	Supports the Azure Information Protection client (classic) for protection and consumption activities. Supports the Azure Information Protection unified labeling client for consumption only, and you must install the Active Directory Rights Management Services Mobile Device Extension .
Supports multi-factor authentication (MFA) for computers and mobile devices. For more information, see the Multi-factor authentication (MFA) and Azure Information Protection .	Supports smart card authentication if IIS is configured to request certificates.
Supports Cryptographic Mode 2 by default to provide a recommended level of security for key lengths and encryption algorithms.	Supports Cryptographic Mode 1 by default and requires additional configuration to support Cryptographic Mode 2 for a recommended level of security. For more information, see AD RMS Cryptographic Modes .
Requires an Azure Information Protection license or Azure Rights Management license with Office 365 to protect content. No license is required to consume content that has been protected by Azure Information Protection (includes users from another organization). For more information about licensing, including the differences between a P1 and P2 license, see the feature list from the Azure Information Protection site.	Requires an RMS license to protect content, and to consume content that has been protected by AD RMS. For more information about licensing, see Client Access Licenses and Management Licenses for general information, but contact your Microsoft partner or Microsoft representative for specific information.

Cryptographic controls for signing and encryption

Azure Information Protection by default, uses RSA 2048 for all public key cryptography and SHA 256 for signing operations. In comparison, AD RMS supports RSA 1024 and RSA 2048, and SHA 1 or SHA 256 for signing

operations.

Both Azure Information Protection and AD RMS use AES 128 for symmetric encryption.

Azure Information Protection is compliant with FIPS 140-2 when your tenant key size is 2048 bits, which is the default when the Azure Rights Management service is activated.

For more information about the cryptographic controls, see [Cryptographic controls used by Azure RMS: Algorithms and key length](#).

Next steps

For more detailed requirements to use Azure Information Protection, such as device support and minimum versions, see [Requirements for Azure Information Protection](#).

If you are looking to migrate from AD RMS to Azure Information Protection, see [Migrating from AD RMS to Azure Information Protection](#).

Get started with [Active Directory Rights Management Services Mobile Device Extension](#).

You might be interested in the following FAQs:

- [What's the difference between Azure Information Protection and Microsoft Information Protection?](#)
- [What's the difference between Azure Information Protection and Azure Rights Management?](#)

Active Directory Rights Management Services Mobile Device Extension

7/20/2020 • 12 minutes to read • [Edit Online](#)

Applies To: Windows Server 2019, 2016, 2012 R2, and 2012

You can download the Active Directory Rights Management Services (AD RMS) mobile device extension from the [Microsoft Download Center](#) and install this extension on top of an existing AD RMS deployment. This lets users protect and consume sensitive data when their device supports the latest API-enlightened apps. For example, users can do the following:

- Use the Azure Information Protection app to consume protected text files in different formats (including .txt, .csv, and .xml).
- Use the Azure Information Protection app to consume protected image files (including .jpg, .gif, and .tif).
- Use the Azure Information Protection app to open any file that has been generically protected (.pfile format).
- Use the Azure Information Protection app to open an Office file (Word, Excel, PowerPoint) that is a PDF copy (.pdf and .ppdf format).
- Use the Azure Information Protection app to open protected email messages (.rpmsg) and protected PDF files on Microsoft SharePoint.
- Use an AIP-enlightened PDF viewer for cross-platform viewing or to open PDF files that were protected with any AIP-enlightened application.
- Use your internally developed AIP-enlightened apps that were written by using the [MIP SDK](#).

NOTE

You can download the Azure Information Protection app from the [Microsoft Rights Management](#) page of the Microsoft website. For information about other apps that are supported with the mobile device extension, see the table in the [Applications](#) page from this documentation. For more information about the different file types that RMS supports, see the [Supported file types and file name extensions](#) section from the Rights Management sharing application administrator guide.

IMPORTANT

Be sure to read and configure the prerequisites before you install the mobile device extension.

For additional information, download the "Microsoft Azure Information Protection" white paper and accompanying scripts from the [Microsoft Download Center](#).

Prerequisites for AD RMS mobile device extension

Before you install the AD RMS mobile device extension, make sure the following dependencies are in place.

Requirement	More Information
<p>An existing AD RMS deployment on Windows Server 2019, 2016, 2012 R2, or 2012, that includes the following:</p> <ul style="list-style-type: none"> - Your AD RMS cluster must be accessible from the Internet. - AD RMS must be using a full Microsoft SQL Server-based database on a separate server and not the Windows Internal Database that is often used for testing on the same server. - The account that you will use to install the mobile device extension must have sysadmin rights for the SQL Server instance that you're using for AD RMS. - The AD RMS servers must be configured to use SSL/TLS with a valid x.509 certificate that is trusted by the mobile device clients. - If the AD RMS servers are behind a firewall or published by using a reverse proxy, in addition to publishing the <code>/_wmcs</code> folder to the Internet, you must also publish the <code>/my</code> folder (for example: <code>https://RMSserver.contoso.com/my</code>). 	<p>For details about AD RMS prerequisites and deployment information, see the prerequisites section of this article.</p>
<p>AD FS deployed on your Windows Server:</p> <ul style="list-style-type: none"> - Your AD FS server farm must be accessible from the Internet (you have deployed federation server proxies). - Forms-based authentication is not supported; you must use Windows Integrated Authentication <p>Important: AD FS must be running a different computer from the computer running AD RMS and the mobile device extension.</p>	<p>For documentation about AD FS, see the Windows Server AD FS Deployment Guide in the Windows Server library.</p> <p>AD FS must be configured for the mobile device extension. For instructions, see the Configuring AD FS for the AD RMS mobile device extension section in this topic.</p>
<p>Mobile devices must trust the PKI certificates on the RMS server (or servers)</p>	<p>When you purchase your server certificates from a public CA, such as VeriSign or Comodo, it's likely that mobile devices will already trust the root CA for these certificates, so that these devices will trust the server certificates without additional configuration.</p> <p>However, if you use your own internal CA to deploy the server certificates for RMS, you must take additional steps to install the root CA certificate on the mobile devices. If don't do this, mobile devices will not be able to establish a successful connection with the RMS server.</p>

Requirement	More Information
SRV records in DNS	<p>Create one or more SRV records in your company domain or domains:</p> <p>1: Create a record for each email domain suffix that users will use</p> <p>2: Create a record for every FQDN used by your RMS clusters to protect content, not including the cluster name</p> <p>These records must be resolvable from any network that the connecting mobile devices use, which includes the intranet if your mobile devices connect via the intranet.</p> <p>When users supply their email address from their mobile device, the domain suffix is used to identify whether they should use an AD RMS infrastructure or Azure AIP. When the SRV record is found, clients are redirected to the AD RMS server that responds to that URL.</p> <p>When users consume protected content with a mobile device, the client application looks in DNS for a record that matches the FQDN in the URL of the cluster that protected the content (without the cluster name). The device is then directed to the AD RMS cluster specified in the DNS record and acquires a license to open the content. In most cases, the RMS cluster will be the same RMS cluster that protected the content.</p> <p>For information about how to specify the SRV records, see the Specifying the DNS SRV records for the AD RMS mobile device extension section in this topic.</p>
Supported clients using applications that are developed by using the MIP SDK for this platform.	Download the supported apps for the devices that you use by using the links on the Microsoft Azure Information Protection download page.

Configuring AD FS for the AD RMS mobile device extension

You must first configure AD FS, and then authorize the AIP app for the devices that you want to use.

Step 1: To configure AD FS

- You can either run a Windows PowerShell script to automatically configure AD FS to support the AD RMS mobile device extension, or you can manually specify the configuration options and values:
 - To automatically configure AD FS for the AD RMS mobile device extension, copy and paste the following into a Windows PowerShell script file, and then run it:

```

# This Script Configures the Microsoft Rights Management Mobile Device Extension and Claims used in the ADFS
Server

# Check if Microsoft Rights Management Mobile Device Extension is configured on the Server
$CheckifConfigured = Get-AdfsRelyingPartyTrust -Identifier "api.rms.rest.com"
if ($CheckifConfigured)
{
    Write-Host "api.rms.rest.com Identifier used for Microsoft Rights Management Mobile Device Extension is already
configured on this Server"
    Write-Host $CheckifConfigured
}
else
{
    Write-Host "Configuring Microsoft Rights Management Mobile Device Extension"

    # TransformRules used by Microsoft Rights Management Mobile Device Extension
    # Claims: E-mail, UPN and ProxyAddresses
    $TransformRules = @"
@RuleTemplate = "LdapClaims"
@RuleName = "Jwt Token"
c:[Type ==
"https://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname",
Issuer == "AD AUTHORITY"]
=> issue(store = "Active Directory", types =
("http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress",
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn",
"http://schemas.xmlsoap.org/claims/ProxyAddresses"), query =
";mail,userPrincipalName,proxyAddresses;{0}", param = c.Value);

@RuleTemplate = "PassThroughClaims"
@RuleName = "JWT pass through"
c:[Type == "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"]
=> issue(claim = c);

@RuleTemplate = "PassThroughClaims"
@RuleName = "JWT pass through"
c:[Type == "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn"]
=> issue(claim = c);

@RuleTemplate = "PassThroughClaims"
@RuleName = "JWT pass through Proxy addresses"
c:[Type == "http://schemas.xmlsoap.org/claims/ProxyAddresses"]
=> issue(claim = c);
"@

# AuthorizationRules used by Microsoft Rights Management Mobile Device Extension
# Allow All users
$AuthorizationRules = @"
@RuleTemplate = "AllowAllAuthzRule"
=> issue(Type = "https://schemas.microsoft.com/authorization/claims/permit",
Value = "true");
"@

# Add a Relying Part Truest with Name -"Microsoft Rights Management Mobile Device Extension" Identifier
"api.rms.rest.com"
Add-ADFSRelyingPartyTrust -Name "Microsoft Rights Management Mobile Device Extension" -Identifier
"api.rms.rest.com" -IssuanceTransformRules $TransformRules -IssuanceAuthorizationRules $AuthorizationRules

Write-Host "Microsoft Rights Management Mobile Device Extension Configured"
}

```

- To manually configure AD FS for the AD RMS mobile device extension, use these settings:

CONFIGURATION	VALUE
Relying Party Trust	_api.rms.rest.com
Claim rule	Attribute store: Active Directory E-mail addresses: E-mail-address User-Principal-Name: UPN Proxy-Address: _https://schemas.xmlsoap.org/claims/ProxyAddresses

TIP

For step-by-step instructions for an example deployment of AD RMS with AD FS, see [Deploying Active Directory Rights Management Services with Active Directory Federation Services](#).

Step 2: Authorize apps for your devices

- Run the following Windows PowerShell command after replacing the variables to add support for the **Azure Information Protection** app. Make sure to run both commands in the order shown:

```
Add-AdfsClient -Name "R<your application name>" -ClientId "<YOUR CLIENT ID >" -RedirectUri @("<YOUR REDIRECT URI >")
```

```
Grant-AdfsApplicationPermission -ClientRoleIdentifier '<YOUR CLIENT ID>' -ServerRoleIdentifier api.rms.rest.com -ScopeNames "openid"
```

Powershell Example

```
Add-AdfsClient -Name "Fabrikam application for MIP" -ClientId "96731E97-2204-4D74-BE5-75DCA53566C3" -RedirectUri @("com.fabrikam.MIPAPP://authorize")
```

```
Grant-AdfsApplicationPermission -ClientRoleIdentifier '96731E97-2204-4D74-BE5-75DCA53566C3' -ServerRoleIdentifier api.rms.rest.com -ScopeNames "openid"
```

- For the **Azure Information Protection unified labeling client**, run the following Windows PowerShell command to add support for the Azure Information Protection client on your devices:

```
Add-AdfsClient -Name "Azure Information Protection Client" -ClientId "c00e9d32-3c8d-4a7d-832b-029040e7db99" -RedirectUri @("com.microsoft.azip://authorize")
Grant-AdfsApplicationPermission -ClientRoleIdentifier "c00e9d32-3c8d-4a7d-832b-029040e7db99" -ServerRoleIdentifier api.rms.rest.com -ScopeName "openid"
```

- To support **ADFS on Windows 2016 and 2019** and **ADRMS MDE** for third party products, run the following Windows PowerShell command:

```
Add-AdfsClient -Name "YOUR APP" -ClientId 'YOUR CLIENT ID' -RedirectUri @("YOUR REDIRECT")
Grant-AdfsApplicationPermission -ClientRoleIdentifier 'YOUR CLIENT ID' -ServerRoleIdentifier api.rms.rest.com -ScopeNames "openid"
```

To configure the AIP client on **Windows, Mac, mobile and Office Mobile** for consuming HYOK or AD RMS protected content with AD FS on Windows Server 2012 R2 and newer, use the following:

- For Mac devices (using the RMS sharing app), make sure to run both commands in the order shown:

```
Add-AdfsClient -Name "RMS Sharing App for macOS" -ClientId "96731E97-2204-4D74-BEA5-75DCA53566C3" -RedirectUri @("com.microsoft.rms-sharing-for-osx://authorize")
```

```
Grant-AdfsApplicationPermission -ClientRoleIdentifier '96731E97-2204-4D74-BEA5-75DCA53566C3' -ServerRoleIdentifier api.rms.rest.com -ScopeNames "openid"
```

- For iOS devices (using the Azure Information Protection app), make sure to run both commands in the order shown:

```
Add-AdfsClient -Name "Azure Information Protection app for iOS" -ClientId "9D7590FB-9536-4D87-B5AA-FAA863DCC3AB" -RedirectUri @("com.microsoft.rms-sharing-for-ios://authorize")
```

```
Grant-AdfsApplicationPermission -ClientRoleIdentifier '9D7590FB-9536-4D87-B5AA-FAA863DCC3AB' -ServerRoleIdentifier api.rms.rest.com -ScopeNames "openid"
```

- For Android devices (using the Azure Information Protection app), make sure to run both commands in the order shown:

```
Add-AdfsClient -Name "Azure Information Protection app for Android" -ClientId "ECAD3080-3AE9-4782-B763-2DF1B1373B3A" -RedirectUri @("com.microsoft.rms-sharing-for-android://authorize")
```

```
Grant-AdfsApplicationPermission -ClientRoleIdentifier 'ECAD3080-3AE9-4782-B763-2DF1B1373B3A' -ServerRoleIdentifier api.rms.rest.com -ScopeNames "openid"
```

Run the following PowerShell commands to add support for Microsoft Office apps on your devices:

- For Mac, iOS, Android devices (make sure to run both commands in the order shown):

```
Add-AdfsClient -Name "Office for Mac and Office Mobile" -ClientId "d3590ed6-52b3-4102-aeff-aad2292ab01c" -RedirectUri @("urn:ietf:wg:oauth:2.0:oob")
```

```
Set-AdfsClient -TargetClientId d3590ed6-52b3-4102-aeff-aad2292ab01c -RedirectUri "urn:ietf:wg:oauth:2.0:oob","launch-word://com.microsoft.Office.Word","launch-excel://com.microsoft.Office.Excel","launch-ppt://com.microsoft.Office.Powerpoint"
```

Specifying the DNS SRV records for the AD RMS mobile device extension

You must create DNS SRV records for each email domain that your users use. If all your users use child domains from a single parent domain, and all users from this contiguous namespace use the same RMS cluster, you can use just one SRV record in the parent domain, and RMS will find the appropriate DNS records. The SRV records have the following format: _rmsdisco._http._tcp. <emailsuffix><portnumber><RMSClusterFQDN>

NOTE

Specify 443 for the <portnumber>. Although you can specify a different port number in DNS, devices using the mobile device extension will always use 443.

For example, if your organization has users with the following email addresses:

- _user@contoso.com
- _user@sales.contoso.com
- _user@fabrikam.com If there are no other child domains for _contoso.com that use a different RMS cluster than the one named _rmsserver.contoso.com, create two DNS SRV records that have these values:
 - _rmsdisco._http._tcp.contoso.com 443 _rmsserver.contoso.com
 - _rmsdisco._http._tcp.fabrikam.com 443 _rmsserver.contoso.com

If you use the DNS Server role on Windows Server, use the following tables as a guide for the SRV record properties in the DNS Manager console:

FIELD	VALUE
Domain	_tcp.contoso.com
Service	_rmsdisco
Protocol	_http
Priority	0
Weight	0
Port number	443
Host offering this service	_rmsserver.contoso.com

FIELD	VALUE
Domain	_tcp.fabrikam.com
Service	_rmsdisco
Protocol	_http
Priority	0
Weight	0
Port number	443
Host offering this service	_rmsserver.contoso.com

In addition to these DNS SRV records for your email domain, you must create another DNS SRV record in the RMS cluster domain. This record must specify the FQDNs of your RMS cluster that protects content. Every file that is protected by RMS includes a URL to the cluster that protected that file. Mobile devices use the DNS SRV record and

the URL FQDN specified in the record to find the corresponding RMS cluster that can support mobile devices.

For example, if your RMS cluster is `_rmsserver.contoso.com`, create a DNS SRV record that has the following values: `_rmsdisco._http._tcp.contoso.com 443 _rmsserver.contoso.com`

If you use the DNS Server role on Windows Server, use the following table as a guide for the SRV record properties in the DNS Manager console:

FIELD	VALUE
Domain	<code>_tcp.contoso.com</code>
Service	<code>_rmsdisco</code>
Protocol	<code>_http</code>
Priority	0
Weight	0
Port number	443
Host offering this service	<code>_rmsserver.contoso.com</code>

Deploying the AD RMS mobile device extension

Before you install the AD RMS mobile device extension, make sure that the prerequisites from the preceding section are in place, and that you know the URL of your AD FS server. Then do the following:

1. Download the AD RMS mobile device extension (`ADRMS.MobileDeviceExtension.exe`) from the Microsoft Download Center.
2. Run `ADRMS.MobileDeviceExtension.exe` to start the Active Directory Rights Management Services Mobile Device Extension Setup Wizard. When prompted, enter the URL of the AD FS server that you configured previously.
3. Complete the wizard.

Run this wizard on all the nodes in your RMS cluster.

If you have a proxy server between the AD RMS cluster and the AD FS servers, by default, your AD RMS cluster will not be able to contact the federated service. When this happens, AD RMS will be unable to verify the token that is received from the mobile client and will reject the request. If you have proxy server that blocks this communication, you must update the web.config file from the AD RMS mobile device extension website, so that AD RMS can bypass the proxy server when it needs to contact the AD FS servers.

Updating proxy settings for the AD RMS mobile device extension

1. Open the web.config file that is located in `\Program Files\Active Directory Rights Management Services Mobile Device Extension\Web Service`.
2. Add the following node to the file:

```
<system.net>
  <defaultProxy>
    <proxy proxyaddress="http://<proxy server>:<port>" bypassonlocal="true"
    />
    <bypasslist>
      <add address="<AD FS URL>" />
    </bypasslist>
  </defaultProxy>
</system.net>
```

1. Make the following changes, and then save the file:

- Replace <proxy-server> with the name or address of your proxy server.
- Replace <port> with the port number that the proxy server is configured to use.
- Replace <AD FS URL> with the URL of the federation service. Do not include the HTTP prefix.

NOTE

To learn more about overriding the proxy settings, see [Proxy Configuration](#) documentation.

1. Reset IIS, for example, by running **iisreset** as an administrator from a command prompt.

Repeat this procedure on all the nodes in your RMS cluster.

See Also

Find out more about Azure Information Protection, make contact with other AIP customers, and with AIP product managers using the [AIP yammer group](#).

"

Azure Information Protection requirements

7/20/2020 • 7 minutes to read • [Edit Online](#)

Applies to: [Azure Information Protection](#), [Office 365](#)

Before deploying Azure Information Protection, ensure that your system meets the following prerequisites:

- [Subscription for Azure Information Protection](#)
- [Azure Active Directory](#)
- [Client devices](#)
- [Applications](#)
- [Firewalls and network infrastructure](#)

Subscription for Azure Information Protection

You must have one of the following, depending on the Azure Information Protection features you'll be using:

- An [Azure Information Protection plan](#). Required for classification, labeling, and protection by using the Azure Information Protection scanner or client (classic, or unified labeling)
- An [Office 365 plan that includes Azure Information Protection](#). Required for protection only.

To verify that your subscription includes the Azure Information Protection features you want to use, check the feature list at [Azure Information Protection pricing](#).

If you have questions about licensing, read through the [frequently asked questions](#) for licensing.

TIP

Looking to see if your Office 365 plan or Exchange Online standalone plan supports the [new capabilities from Office 365 Message Encryption](#), to send protected emails to personal email addresses? For example, Gmail, Yahoo, and Microsoft. Check the following resources:

- [Exchange Online Service Description](#)
- [Office 365 Education](#)
- [Office 365 US Government](#)

If you have questions about subscriptions or licensing, do not post them on this page. Instead, see if they are answered in the [frequently asked questions](#) for licensing. If your question is not answered there, contact your Microsoft Account Manager or [Microsoft Support](#).

Azure Active Directory

To support authentication and authorization for Azure Information Protection, you must have an Azure Active Directory (AD). To use user accounts from your on-premises director (AD DS), you must also configure directory integration.

- **Single sign-on (SSO)** is supported for Azure Information Protection so that users are not repeatedly prompted for their credentials. If you use another vendor solution for federation, check with that vendor for how to configure it for Azure AD. WS-Trust is a common requirement for these solutions to support

single sign-on.

- **Multi-factor authentication (MFA)** is supported with Azure Information Protection when you have the required client software and have correctly configured the MFA-supporting infrastructure.

Conditional access is supported in preview for documents protected by Azure Information Protection. For more details see: [I see Azure Information Protection is listed as an available cloud app for conditional access—how does this work?](#)

For more details, see:

- [Azure Active Directory requirements for Azure Information Protection](#)
- [Preparing users and groups for Azure Information Protection](#)

Client devices

Users computers or mobile devices must run on an operating system that supports Azure Information Protections.

Supported operating systems for client devices

The following operating systems support both the Azure Information Protection unified labeling and the Azure Information Protection clients:

- **Windows 10** (x86, x64). Handwriting is not supported in the Windows 10 RS4 build and later.
- **Windows 8.1** (x86, x64)
- **Windows 8** (x86, x64)
- **Windows Server 2019**
- **Windows Server 2016**
- **Windows Server 2012 R2 and Windows Server 2012**

[Both clients](#) let users classify and label their documents and emails.

For details about support in earlier versions of Windows, contact your Microsoft account or support representative.

NOTE

When the Azure Information Protection clients protect the data by using the Azure Rights Management service, the data can be consumed by the [same devices](#) that support the Azure Rights Management service.

Virtual machines

If you're working with virtual machines, check whether the software vendor for your virtual desktop solution as additional configurations required for running the Azure Information Protection unified labeling or the Azure Information Protection client.

For example, for Citrix solutions, you might need to [disable Citrix Application Programming Interface \(API\) hooks](#) for Office, the Azure Information Protection unified labeling client, or the Azure Information Protection client.

These applications use the following files, respectively: **winword.exe**, **excel.exe**, **outlook.exe**, **powerpnt.exe**, **msip.app.exe**, **msip.viewer.exe**

Server support

For each of the server versions listed above, Azure Information Protection clients are supported for Remote Desktop Services.

If you delete user profiles when you use the Azure Information Protection clients with Remote Desktop Services, do not delete the %Appdata%\Microsoft\Protect folder.

Additionally, Server Core and Nano Server are not supported.

Additional requirements per client

Each Azure Information Protection client has additional prerequisites. For details, see:

- [Azure Information Protection unified labeling client prerequisites](#)
- [Azure Information Protection client prerequisites](#)

Applications

The Azure Information Protection clients can label and protect documents and emails by using Microsoft Word, Excel, PowerPoint, and Outlook from any of the following Office editions:

- **Office apps minimum version 1805**, build 9330.2078 from Office 365 Business or Microsoft 365 Business.

This edition is supported only when the user is assigned a license for Azure Rights Management, also known as Azure Information Protection for Office 365.

- **Office 365 ProPlus**
- **Office Professional Plus 2019**
- **Office Professional Plus 2016**
- **Office Professional Plus 2013 with Service Pack 1**
- **Office Professional Plus 2010 with Service Pack 2**

Other editions of Office cannot protect documents and emails by using a Rights Management service. For these editions, Azure Information Protection is supported for classification only, and labels that apply protection are not displayed for users.

These labels would have otherwise been displayed on the Azure Information Protection bar or in the unified labeling client on the Office ribbon (from the **Protect** button in the classic client or the **Sensitivity** button in the unified labeling client).

For more details, see [Applications that support Azure Rights Management data protection](#).

Office features and capabilities not supported

- The Azure Information Protection clients, including both classic and unified labeling, do not support multiple versions of Office on the same computer, or switching user accounts in Office.
- The Office [mail merge](#) feature is not supported with any Azure Information Protection feature.

Firewalls and network infrastructure

If you have a firewalls or similar intervening network devices that are configured to allow specific connections, the network connectivity requirements are listed in this Office article: [Office 365 URLs and IP address ranges > Microsoft 365 Common and Office Online](#).

Azure Information Protection has the following additional requirements:

- **Unified labeling client.** To download labels and label policies, allow the following URL over HTTPS:
*.protection.outlook.com
- **Web proxies.** If you use a web proxy that requires authentication, you must configure the proxy to use integrated Windows authentication with the user's Active Directory logon credentials.
- **TLS client-to-service connections.** Do not terminate any TLS client-to-service connections, for example to perform packet-level inspection, to the aadrm.com URL. Doing so breaks the certificate pinning that RMS clients use with Microsoft-managed CAs to help secure their communication with the Azure Rights Management service.

To determine whether your client connection is terminated before it reaches the Azure Rights Management service, use the following PowerShell commands:

```
$request = [System.Net.HttpWebRequest]::Create("https://admin.na.aadrm.com/admin/admin.svc")
$request.GetResponse()
$request.ServicePoint.Certificate.Issuer
```

The result should show that the issuing CA is from a Microsoft CA, for example:

```
CN=Microsoft Secure Server CA 2011, O=Microsoft Corporation, L=Redmond, S=Washington, C=US .
```

If you see an issuing CA name that is not from Microsoft, it is very likely that your secure client-to-service connection is being terminated and needs reconfiguration on your firewall.

- **TLS version 1.2 or higher** (unified labeling client only). The unified labeling client requires a TLS version of 1.2 or higher to ensure the use of cryptographically secure protocols and align with Microsoft security guidelines.

On-premises servers

The following on-premises servers are supported with the Azure Rights Management service from Azure Information Protection:

- Exchange Server
- SharePoint Server
- Windows Server file servers that support File Classification Infrastructure

For information about the additional requirements for this scenario, see [On-premises servers that support Azure Rights Management data protection](#).

Coexistence of AD RMS with Azure RMS

Using AD RMS and Azure RMS side-by-side, in the same organization, to protect content by the same user in the same organization, is **only** supported in AD RMS for [HYOK \(hold your own key\) protection](#) with Azure Information Protection.

This scenario is *not* supported during [migration](#). Supported migration paths include:

- [From AD RMS to Azure Information Protection](#)
- [From Azure Information Protection to AD RMS](#)

TIP

If you deploy Azure Information Protection and then decide that you no longer want to use this cloud service, see [Decommissioning and deactivating Azure Information Protection](#).

For other, non-migration scenarios, where both services are active in the same organization, both services must be configured so that only one of them allows any given user to protect content. This can be configured as follows:

- Use redirections for an [AD RMS to Azure RMS migration](#)
- If both services must be active for different users at the same time, use service-side configurations to enforce exclusivity. Use the Azure RMS onboarding controls in the cloud service, and an ACL on the Publish URL to set **Read-Only** mode for AD RMS.

Service Tags

Make sure to allow access to all ports for the following Service Tags:

- **AzureInformationProtection**
- **AzureActiveDirectory**
- **AzureFrontDoor.FrontEnd**

The Azure Information Protection service also depends on two specific IP addresses:

- 13.107.6.181
- 13.107.9.181

Make sure to create rules to allow outbound access to these specific IP addresses.

Azure Active Directory requirements for Azure Information Protection

7/20/2020 • 3 minutes to read • [Edit Online](#)

Applies to: [Azure Information Protection](#), [Office 365](#)

You must have an Azure AD directory to use Azure Information Protection. You use an account from this directory to sign in to the Azure portal, where, for example, you can configure and manage Azure Information Protection labels and Azure Rights Management templates.

If you have a subscription that includes Azure Information Protection or Azure Rights Management, your Azure AD directory is automatically created for you if needed.

For more information about Azure AD, see [What is Azure AD Directory?](#)

To integrate your Azure AD directory with your on-premises AD forests, see [Integrate on-premises Active Directory domains with Azure Active Directory](#).

Scenarios that have specific requirements

Computers running Office 2010:

- These computers require the [Azure Information Protection unified labeling client](#) or [Azure Information Protection client](#) to authenticate to Azure Information Protection and its data protection service, Azure Rights Management.
- If your user accounts are federated (for example, you use AD FS), they must use Windows Integrated Authentication. Forms-based authentication in this scenario fails to authenticate users for Azure Information Protection.

Support for certificate-based authentication (CBA):

- The Azure Information Protection apps for iOS and Android support certificate-based authentication. For instructions to configure certificate-based authentication, see [Get started with certificate-based authentication in Azure Active Directory](#).

Users' UPN value doesn't match their email address:

- This is not a recommended configuration and doesn't support single sign-on for Azure Information Protection. If you cannot change the UPN value, configure alternate login ID for users, and instruct them how to sign in to Office by using this alternate login. For more information, see [Configuring Alternate Login ID](#) and [Office applications periodically prompt for credentials to SharePoint, OneDrive, and Lync Online](#).

When the domain name in the UPN value is a domain that is verified for your tenant, add the user's UPN value as another email address to the Azure AD proxyAddresses attribute. This lets the user be authorized for Azure Rights Management if their UPN value is specified at the time the usage rights are granted. For more information about this and how user accounts are authorized, see [Preparing users and groups for Azure Information Protection](#).

Mobile devices or Mac computers that authenticate on-premises by using AD FS or an equivalent authentication provider:

- You must use AD FS on the minimum server version of [Windows Server 2012 R2](#), or an alternative authentication provider that supports the OAuth 2.0 protocol.

Multi-factor authentication (MFA) and Azure Information Protection

To use multi-factor authentication (MFA) with Azure Information Protection requires at least one of the following:

- Office 2013 (minimum version):
 - If you have Office 2013, you might need to install an additional update to support Active Directory Authentication Library (ADAL). For example, the [June 9, 2015, update for Office 2013 \(KB3054853\)](#). For more information about this update and how modern authentication brings Active Directory Authentication Library (ADAL)-based sign-in to Office 2013, see [Office 2013 modern authentication public preview announced](#) on the Office blog.
- Azure Information Protection client:
 - The Azure Information Protection clients for Windows and the viewer app for iOS and Android has always supported MFA; no minimum version is required.
- Rights Management sharing app for Mac computers:
 - MFA support went into the September 2015 release of the RMS sharing app.

Then, configure your MFA solution:

- For Microsoft-managed tenants (you have Azure Active Directory or Office 365):
 - Configure Azure MFA to enforce MFA for users. For instructions, see [Getting started with Azure Multi-Factor Authentication in the cloud](#) from the Multi-factor Authentication documentation.
For more information about Azure MFA, see [What is Azure Multi-Factor Authentication?](#)
- For federated tenants (you operate federation servers on-premises):
 - Configure your federation servers for Azure Active Directory or Office 365. For example, if you are using AD FS, see [Configure Additional Authentication Methods for AD FS](#).
For more information about this scenario, see [The Works with Office 365 – Identity program now streamlined](#) on the Office blog.

The Rights Management connector and the Azure Information Protection scanner do not support MFA. If you deploy the connector or scanner, the following accounts must not require MFA:

- The account that installs and configures the connector.
- The service principal account in Azure AD, **Aadrm_S-1-7-0**, that the connector creates.
- The service account that runs the scanner.

Next steps

To check for other requirements, see [Requirements for Azure Information Protection](#).

Client devices that support Azure Rights Management data protection

1/13/2020 • 2 minutes to read • [Edit Online](#)

Applies to: [Azure Information Protection](#), [Office 365](#)

Use the following sections to identify which devices support the Azure Rights Management service. This service provides data protection for Azure Information Protection.

Computers

The following computer operating systems support the Azure Rights Management service:

- **Windows 7** (x86, x64)
- **Windows 8** (x86, x64)
- **Windows 8.1** (x86, x64)
- **Windows 10** (x86, x64)
- **macOS**: Minimum version of macOS 10.8 (Mountain Lion)

Mobile devices

The following mobile device operating systems support the Azure Rights Management service:

- **Android phones and tablets**: Minimum version of Android 6.0
- **iPhone and iPad**: Minimum version of iOS 11.0
- **Windows phones and tablets**: Windows 10 Mobile

Next steps

To check for other requirements, see [Requirements for Azure Information Protection](#).

Applications that support Azure Rights Management data protection

7/20/2020 • 8 minutes to read • [Edit Online](#)

Applies to: [Azure Information Protection](#), [Office 365](#)

Use the following information to identify the applications and solutions that natively support the Azure Rights Management service (Azure RMS), which provides the data protection for Azure Information Protection.

For these applications and solutions, Rights Management support is tightly integrated by using the Rights Management APIs to support [usage restrictions](#). These applications and solutions are also known as "RMS-enlightened."

Unless stated otherwise, the supported capabilities apply to both Azure RMS and AD RMS. In addition, AD RMS support on iOS, Android, macOS, and Windows Phone 8.1 requires [Active Directory Rights Management Services Mobile Device Extension](#).

RMS-enlightened applications

The following table displays RMS-enlightened client applications from Microsoft and software vendors.

For information about viewing protected PDF documents, see [Protected PDF readers for Microsoft Information Protection](#).

Information about the table columns:

- **Email:** The email clients that are listed can protect the email message itself, which automatically protects any attached Office files that are not already protected. In this scenario, the client's preview feature can display the protected content (message and attachment) to authorized recipients. However, if an email message itself is not protected but the attachment is protected, the client's preview feature cannot display the protected attachment to authorized recipients.

Tip: For email clients that don't support protecting emails, consider using [Exchange Online mail flow rules to apply this protection](#).

- **Other file types:** Text and image files include files that have a file name extension such as .txt, .xml, jpg, and .jpeg. These files change their file name extension after they are natively protected by Rights Management, and become read-only. Files that cannot be natively protected have a .pfile file name extension after they are generically protected by Rights Management. For more information, see the [File types supported](#) from the Azure Information Protection client admin guide.

DEVICE OPERATING SYSTEM	WORD, EXCEL, POWERPOINT	EMAIL	OTHER FILE TYPES
-------------------------	----------------------------	-------	------------------

DEVICE OPERATING SYSTEM	WORD, EXCEL, POWERPOINT	EMAIL	OTHER FILE TYPES
Windows	<p>Office 365 apps [1]</p> <p>Office 2010</p> <p>Office 2013</p> <p>Office 2016</p> <p>Office 2019</p> <p>Office for the web (viewing protected documents) [2]</p> <p>Web browser [3]</p>	<p>Outlook 2010</p> <p>Outlook 2013</p> <p>Outlook 2016</p> <p>Outlook 2019</p> <p>Outlook from Office 365 ProPlus</p> <p>Web browser [4]</p> <p>Windows Mail [5]</p>	<p>Visio from Office 365 apps, Office 2019, and Office 2016: .vsdm, .vsdx, .vssm, .vstm, .vssx, .vstx</p> <p>Azure Information Protection client for Windows: Text, images, pfile</p> <p>SealPath RMS plugin for AutoCAD: .dwg</p>
iOS	<p>GigaTrust</p> <p>Office Mobile</p> <p>Office for the web [2]</p> <p>TITUS Docs</p> <p>Web browser [3]</p>	<p>Azure Information Protection app (viewing protected email)</p> <p>BlackBerry Work</p> <p>Citrix WorxMail</p> <p>NitroDesk [5]</p> <p>Outlook for iPad and iPhone [5]</p> <p>TITUS Mail</p> <p>Web browser [4]</p>	<p>Azure Information Protection app (viewing protecting text and images)</p> <p>TITUS Docs: Pfile</p>
Android	<p>GigaTrust App for Android</p> <p>Office for the web [2]</p> <p>Office Mobile (unless using sensitivity labels, limited to viewing and editing protected documents)</p> <p>Web browser [3]</p>	<p>9Folders [5]</p> <p>Azure Information Protection app (viewing protected emails)</p> <p>BlackBerry Work</p> <p>GigaTrust App for Android [5]</p> <p>Citrix WorxMail</p> <p>NitroDesk [5]</p> <p>Outlook for Android [5]</p> <p>Samsung Email (S3 and later) [5]</p> <p>TITUS Classification for Mobile</p> <p>Web browser [4]</p>	<p>Azure Information Protection app (viewing protected text and images)</p>

DEVICE OPERATING SYSTEM	WORD, EXCEL, POWERPOINT	EMAIL	OTHER FILE TYPES
macOS	Office 365 apps Office 2019 for Mac Office 2016 for Mac Office for the web [2] Web browser [3]	Outlook 2019 for Mac Outlook 2016 for Mac Web browser [4]	RMS sharing app (viewing protected text, images, generically protected files)
Windows 10 Mobile	Office Mobile apps (viewing protected documents using Azure RMS) Web browser [3]	Citrix WorxMail Outlook Mail (viewing protected emails) Web browser [4]	Not supported
Blackberry 10	Web browser [3]	Blackberry email [5] Web browser [4]	Not supported

Footnote 1

Includes:

- Office apps minimum version 1805, build 9330.2078 from Office 365 Business or Microsoft 365 Business when the user is assigned a license for Azure Rights Management (also known as Azure Information Protection for Office 365)
- Office 365 ProPlus apps

Footnote 2

Supported only with Microsoft SharePoint and OneDrive, and the documents are unprotected before they are uploaded to a protected library.

Footnote 3

For [Office attachments](#) that are protected by using [Office 365 Message Encryption with the new capabilities](#).

Footnote 4

If the sender and the recipient are part of the same organization. Or either of the following conditions:

- The sender or the recipient are using Exchange Online.
- The sender is using Exchange on-premises in a hybrid configuration.

Footnote 5

Uses Exchange ActiveSync IRM, which must be enabled by the Exchange administrator. Users can view, reply, and reply all for protected email messages but users cannot protect new email messages.

If the email application cannot render the message because the Exchange ActiveSync IRM is not enabled, the recipient can view the email in a web browser when the sender uses Exchange Online, or Exchange on-premises in a hybrid configuration.

More information about Azure RMS support for Office

Azure RMS is tightly integrated into the Word, Excel, PowerPoint, and Outlook apps, where this functionality is often referred to as Information Rights Management (IRM).

See also: [Office Applications Service Description](#)

Windows computers for Information Rights Management (IRM)

The following Office client suites support protecting files and emails on Windows computers by using the Azure Rights Management service:

- Office apps minimum version 1805, build 9330.2078 from Office 365 Business or Microsoft 365 Business when the user is assigned a license for Azure Rights Management (also known as Azure Information Protection for Office 365)
- Office 365 ProPlus

These editions of Office are included with most but not all Office 365 subscriptions that include data protection from Azure Information Protection. Check your subscription information to see if Office 365 ProPlus is included. You'll also find this information in the [Azure Information Protection datasheet](#).

- Office Professional Plus 2019
- Office Professional Plus 2016
- Office Professional Plus 2013
- Office Professional Plus 2010 with Service Pack 2

All editions of Office (with the exception of Office 2007) support consuming protected content.

When you use the Azure Rights Management service with Office Professional Plus 2010 and Service Pack 2 or Office Professional 2010 with Service Pack 2:

- Requires the Azure Information Protection client for Windows.
- Not supported on Windows 10.
- Does not support forms-based authentication for federated user accounts. These accounts must use Windows Integrated Authentication.
- Does not support overriding template protection with custom permissions that a user selects with the Azure Information Protection client. In this scenario, the original protection must first be removed before custom permissions can be applied.

Mac computers for Information Rights Management (IRM)

The following Office client suites support protecting files and emails on macOS by using Azure RMS:

- Office 365 ProPlus
- Office Standard 2019 for Mac
- Office Standard 2016 for Mac

All editions of Office for Mac 2019 and Office for Mac 2016 support consuming protected content.

Tip: To get started with protecting documents by using Office for Mac, you might find the following FAQ useful: [How do I configure a Mac computer to protect and track documents?](#)

More information about the Azure Information Protection app for iOS and Android

The Azure Information Protection app for iOS and Android provides a viewer for rights-protected email messages (.rpmsg files) when these mobile devices don't have an email app that can open protected emails. This app can also open rights-protected PDF files, and pictures and text files that are rights-protected.

If your iOS and Android devices are enrolled by Microsoft Intune, users can install the app from the Company Portal and you can manage the app by using Intune's [app protection policies](#).

For more information about how to use app, see the [FAQ for Microsoft Azure Information Protection app for iOS and Android](#).

More information about the Azure Information Protection client for Windows

For more information, see the following resources:

- Azure Information Protection client administrator guides:
 - [Unified labeling client](#)
 - [Classic client](#)
- Azure Information Protection client user guides:
 - [Unified labeling client](#)
 - [Classic client](#)
- [FAQs for Azure Information Protection app for iOS and Android](#)

Download the relevant app by using the links on the [Microsoft Azure Information Protection page](#).

More information about the Rights Management sharing app

For Mac computers, the Rights Management sharing app offers a viewer for protected PDF files (.ppdf), protected text images, and generically protected files. It can also protect image files, but not other files. To protect Office files on these computers, use Office for Mac or Office 365 ProPlus.

For more information, see the following resources:

- [FAQ for Microsoft Rights Management Sharing Application for Mobile Platforms](#)

Download the Rights Management sharing app for Mac computers by using the link on the [Microsoft Azure Information Protection page](#).

More information about other applications that support Azure Information Protection

In addition to the applications in the table, any application that supports the APIs for the Azure Rights Management service can be integrated with Azure Information Protection, which includes:

- Line-of-business applications that are written in-house by using the RMS SDKs
- Applications from software vendors that are written by using the RMS SDKs.

For more information, see the [Azure Information Protection Developer's Guide](#).

Applications that are not supported by Azure RMS

The following applications that are not currently supported by Azure RMS include the following:

- Microsoft OneDrive for SharePoint Server 2013
- XPS Viewer

In addition, the Azure Information Protection client has the following restrictions:

- For Windows computers: Requires a minimum version of Windows 7 Service Pack 1

RMS-enlightened solutions

For the latest information about solutions that support the Azure Rights Management service and Azure Information Protection, see the blog post, [Microsoft Ignite 2019 – Microsoft Information Protection solutions Partner ecosystem showcase](#).

Next steps

To check for other requirements, see [Requirements for Azure Information Protection](#).

For more information about how the most commonly used applications support the Azure Rights Management service, see [How applications support the Azure Rights Management service](#).

For information about how to configure the most commonly used applications for the Azure Rights Management

service, see [Configuring applications for Azure Rights Management](#).

On-premises servers that support Azure Rights Management data protection

7/20/2020 • 2 minutes to read • [Edit Online](#)

Applies to: [Azure Information Protection](#), [Office 365](#)

The following on-premises server products are supported with Azure Information Protection when you use the Azure Rights Management connector. This connector acts as a communications interface (a relay) between the on-premises servers and the Azure Rights Management service that is used by Azure Information Protection to protect Office documents and emails.

To use this connector, you must configure directory synchronization between your Active Directory forests and Azure Active Directory.

- **Exchange Server:**

- Exchange Server 2016
 - Exchange Server 2013
 - Exchange Server 2010

- **Office SharePoint Server:**

- Office SharePoint Server 2016
 - Office SharePoint Server 2013
 - Office SharePoint Server 2010

- **File servers that run Windows Server and use File Classification Infrastructure (FCI):**

- Windows Server 2016
 - Windows Server 2012 R2
 - Windows Server 2012

You can also use these cmdlets with servers running later versions of Windows Server, with the benefit that these cmdlets can protect all file types. The RMS connector protects Office files only. For how-to instructions, see [RMS Protection with Windows Server File Classification Infrastructure \(FCI\)](#).

The Rights Management connector is supported on Windows Server 2016, Windows Server 2012 R2, Windows Server 2012.

For more information about how to configure the Rights Management connector for these on-premises servers, see [Deploying the Azure Rights Management connector](#).

Next steps

To check for other requirements, see [Requirements for Azure Information Protection](#).

Quickstart: Get started with Azure Information Protection in the Azure portal

7/20/2020 • 5 minutes to read • [Edit Online](#)

Applies to: [Azure Information Protection](#)

In this quickstart, you'll add Azure Information Protection to the Azure portal, confirm the protection service is activated, create default labels if you don't already have labels, and view the policy settings for the Azure Information Protection client (classic).

You can finish this quickstart in less than 10 minutes.

Prerequisites

To complete this quickstart, you need:

- A subscription that includes Azure Information Protection Plan 1 or Plan 2.

If you don't have one of these subscriptions, you can create a [free](#) account for your organization.

For a full list of prerequisites to use Azure Information Protection, see [Requirements for Azure Information Protection](#).

Add Azure Information Protection to the Azure portal

Azure Information Protection isn't automatically available in the Azure portal. You must add it.

1. Sign in to the [Azure portal](#) by using the global admin account for your tenant.

If you are not the global admin, use the following link for alternative roles: [Signing in to the Azure portal](#)

2. Select **+ Create a resource**, and then, from the search box for the Marketplace, type **Azure Information Protection**.
3. From the results list, select **Azure Information Protection**. Then on the **Azure Information Protection** pane, click **Create**.

TIP

Optionally, 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** again.

Confirm the protection service is activated

The protection service is now automatically activated for new customers, but it's a good idea to confirm it doesn't need manually activating.

1. On the **Azure Information Protection** pane, select **Manage > Protection activation**.
2. Confirm whether protection is activated for your tenant:

- If protection is activated, you see the following confirmation:

Deactivate

Protection activation status

The protection status is **activated**.

Protection must be activated to configure labels that set permissions or to enable Office Information Rights Management (IRM) protection for Exchange or SharePoint.

You can use "Deactivate" to stop using this protection capability. Deactivating the protection could result in protected documents and emails that can't be opened. To prevent this happening, read through and follow the instructions in [Decommissioning and deactivating protection](#).

- If protection is not activated, you see this reflected in the status information, and the option to activate:

Activate

Protection activation status

The protection status is **not activated**.

Protection must be activated to configure labels that set permissions or to enable Office Information Rights Management (IRM) protection for Exchange or SharePoint.

Select "Activate" to enable protection.

Important! If you have AD RMS, don't activate protection at this time. [More Information](#)

- If protection isn't activated, select **Activate**.

When activation is complete, the information bar displays **Activation finished successfully**.

Create and publish labels

Your organization might already have labels because they were automatically created for your tenant, or because you have sensitivity labels in the Office 365 Security & Compliance center, the Microsoft security center, or the Microsoft compliance center. Let's take a look:

- Select **Classifications > Labels**:

If you see the option **Generate default labels**, you don't yet have any labels:

The screenshot shows the Azure Information Protection - Labels interface. On the left, there's a navigation sidebar with options like General, Quick start, Analytics, Usage report (Preview), Activity logs (Preview), Data discovery (Preview), Recommendations (Preview), Classifications, Labels (which is selected and highlighted in blue), and Policies. The main area has a search bar, column headers (Label Display Name, Policy, Marking, Protection), and a 'Generate default labels' button. Below these are sections for 'Protection templates' and '+ Add a new label'.

If you don't see this option to generate default labels, you might already have labels, perhaps similar to those in the following picture, which are the default labels for Azure Information Protection:

Azure Information Protection - Labels

LABEL DISPLAY NAME	POLICY	MARKING	PROTECTION
Personal	Global		...
Public	Global		...
General	Global		...
▶ Confidential	Global		...
▶ Highly Confidential	Global		...
▶ Protection templates			...

+ Add a new label

If you don't see this option to generate default labels and you also don't see any labels, go to **Manage > Unified labeling**, and view the status of **Unified labeling**. If you see **Not activated**, select **Activate** and then return to the **Classifications > Labels** pane.

2. If you don't yet have labels, select that option to **Generate default labels**.

3. To publish the labels for all users, from **Classifications > Policies > Global**:

a. Select **Add or remove labels**.

b. From the **Policy: Add or remove labels** pane, select all the labels, and then select **OK**.

c. Back on the **Policy: Global** pane, select **Save**.

Publishing the labels in the Azure portal makes them available for the Azure Information Protection client (classic).

View your labels

Select **Classifications > Labels**, and spend a few minutes familiarizing yourself with the labels that are displayed on the **Azure Information Protection - Labels** pane.

If they don't look similar to the labels in the picture from the previous section, you aren't using default labels from Azure Information Protection but labels that might have been created from the Office 365 Security & Compliance Center, the Microsoft 365 Security center, or the Microsoft 365 Compliance center.

TIP

If you don't want to use your custom labels, but instead, use default labels from Azure Information Protection:

- Delete the custom labels and you then see the option to generate default labels in the **Labels** pane, as described in the previous section.

From the **Azure Information Protection - Labels** pane:

- The default labels for classification are **Personal**, **Public**, **General**, **Confidential**, and **Highly Confidential**. The last two labels expand to show sublabels, which provide examples of how a classification can have subcategories.
- From the **MARKING** and **PROTECTION** columns, you can see that some labels have visual markings configured. The visual markers are a footer, header, and watermark. Some labels might also have protection set.

For example:

LABEL DISPLAY NAME	POLICY	MARKING	PROTECTION
Personal	Global		...
Public	Global		...
General	Global		...
▼ Confidential	Global		...
All Employees	Global	✓	✓
Anyone (not protected)	Global	✓	...
Recipients Only	Global	✓	✓
▶ Highly Confidential	Global		...
▶ Protection templates			...
+ Add a new label			

If you select a label, you see details for that label configuration on a new pane.

View your policy settings

The first time you connect to the Azure Information Protection service by using the Azure portal, default policy settings are always created for you that are used by the Azure Information Protection client (classic). For the classic client, policy settings and the labels we viewed are downloaded to the client in the Azure Information Protection policy.

If you are using the Azure Information Protection unified labeling client, this client does not use these policy settings. Instead, this client downloads the same labels but different policy settings from the Office 365 Compliance & Security Center, the Microsoft 365 Compliance center, or the Microsoft 365 Security center. Use those admin centers to edit your labels and label policies instead of the Azure portal.

To view the default Azure Information Protection policy settings for the classic client:

1. Select **Classifications > Policies > Global** to display the default Azure Information Protection policy settings that are created for your tenant.
2. After the labels, in the **Configure settings to display and apply on Information Protection end users** section, you see the policy settings. For example, there is no default label set, documents and emails are not required to have a label, and users do not have to provide justification when they change labels:

Configure settings to display and apply on Information Protection end users

* Title

Sensitivity

Tooltip

The current label for this content. This setting identifies the risk to the business if this content is shared with unauthorized people inside or outside the organization.

Select the default label

None

Send audit data to Azure Information Protection analytics 

Off Not configured

All documents and emails must have a label (applied automatically or by users)

Off On

Users must provide justification to set a lower classification label, remove a label, or remove protection

Off On

For email messages with attachments, apply a label that matches the highest classification of those attachments

Off Automatic Recommended

Display the Information Protection bar in Office apps

Off On

Add the Do Not Forward button to the Outlook ribbon

Off On

Make the custom permissions option available for users

Off On

Provide a custom URL for the Azure Information Protection client "Tell me more" web page (optional; otherwise keep blank)

Enter a custom URL or keep blank

3. You can now close any panes in the portal that you have opened.

Next steps

If you are using the classic client:

- You might find the following tutorial helpful as your next step: [Edit the policy and create a new label for Azure Information Protection](#).
- Alternatively, for detailed instructions for configuring all aspects of the Azure Information Protection policy, see [Configuring the Azure Information Protection policy](#).

If you are using the unified labeling client:

- See [Learn about sensitivity labels](#) from the Microsoft 365 Compliance documentation.

Not sure of the difference between these clients? See this [FAQ](#).

Quickstart: Find what sensitive information you have in files stored on-premises

7/20/2020 • 7 minutes to read • [Edit Online](#)

Applies to: [Azure Information Protection](#)

In this quickstart, you'll permission SharePoint to allow scanning, and install and configure the Azure Information Protection scanner to find what sensitive information you have in files that are stored in an on-premises data store, such as a network share or a SharePoint Server.

NOTE

You can use this quickstart with the current general availability version of the Azure Information Protection client (classic), or the current general availability version of the Azure Information Protection unified labeling client that includes the scanner.

Not sure of the difference between these clients? See this [FAQ](#).

You can finish this configuration in less than 15 minutes.

Prerequisites

To complete this quickstart, you need:

1. A subscription that includes Azure Information Protection Plan 1 or Plan 2.

If you don't have one of these subscriptions, you can create a [free](#) account for your organization.

2. One of the following Azure Information Protection clients is installed on your computer:

- The classic client: To install this client, go to the [Microsoft download center](#) and download **AzInfoProtection.exe** from the Azure Information Protection page.
- The unified labeling client: To install this client, go the [Microsoft download center](#) and download **AzInfoProtection_UL.exe** from the Azure Information Protection page.

3. SQL Server Express is also installed on your computer.

If this SQL Server edition isn't already installed, you can download it from the [Microsoft Download Center](#) and select a Basic installation.

4. Your domain account is synchronized to Azure AD.

For a full list of prerequisites to use Azure Information Protection, see [Requirements for Azure Information Protection](#).

5. SharePoint policy permissions access if you choose to permissions a SharePoint scan.

Prepare a test folder and file

For an initial test to confirm that the scanner is working:

1. Create a new folder on an accessible network share. For example, name this folder **TestScanner**.

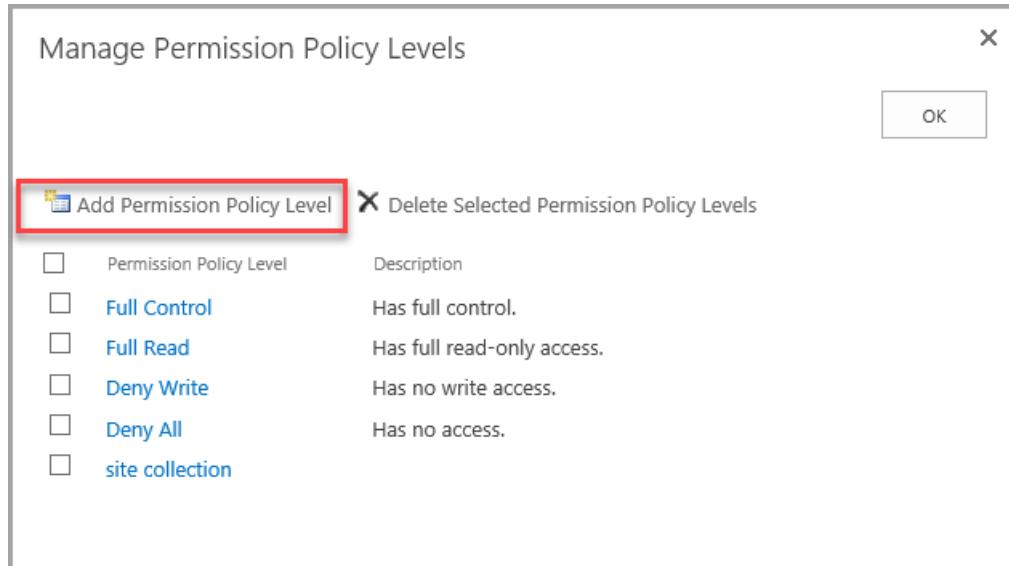
2. Create and save a Word document in that folder, which has the text **Credit card: 4242-4242-4242-4242**.

Permission users to scan SharePoint repositories

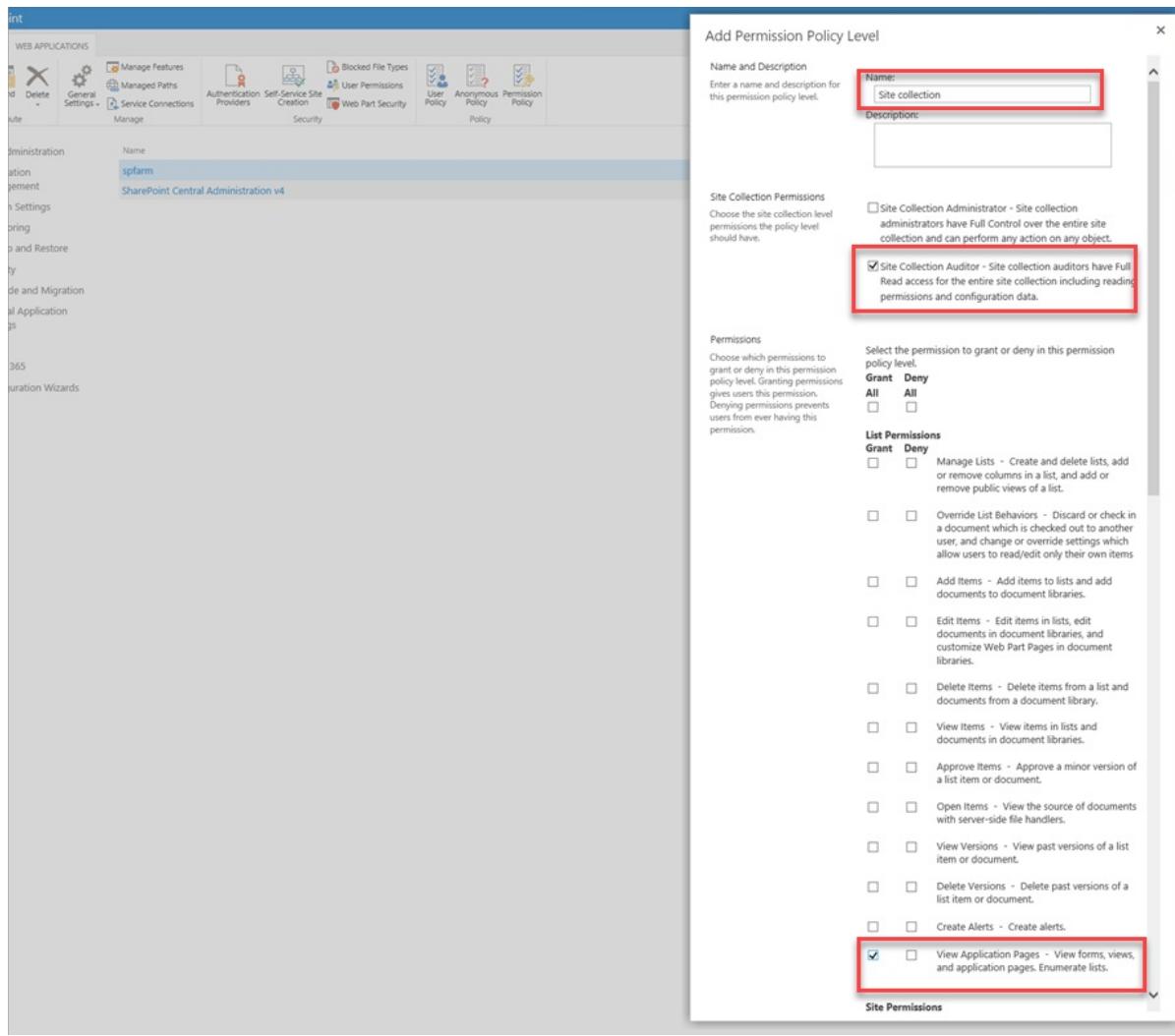
You can use the scanner across SharePoint repositories by specifying the site url and Azure Information Protection will discover all sites under that url and scan them.

To enable scans across repositories, add the following SharePoint permissions for the user you intend to use to scan:

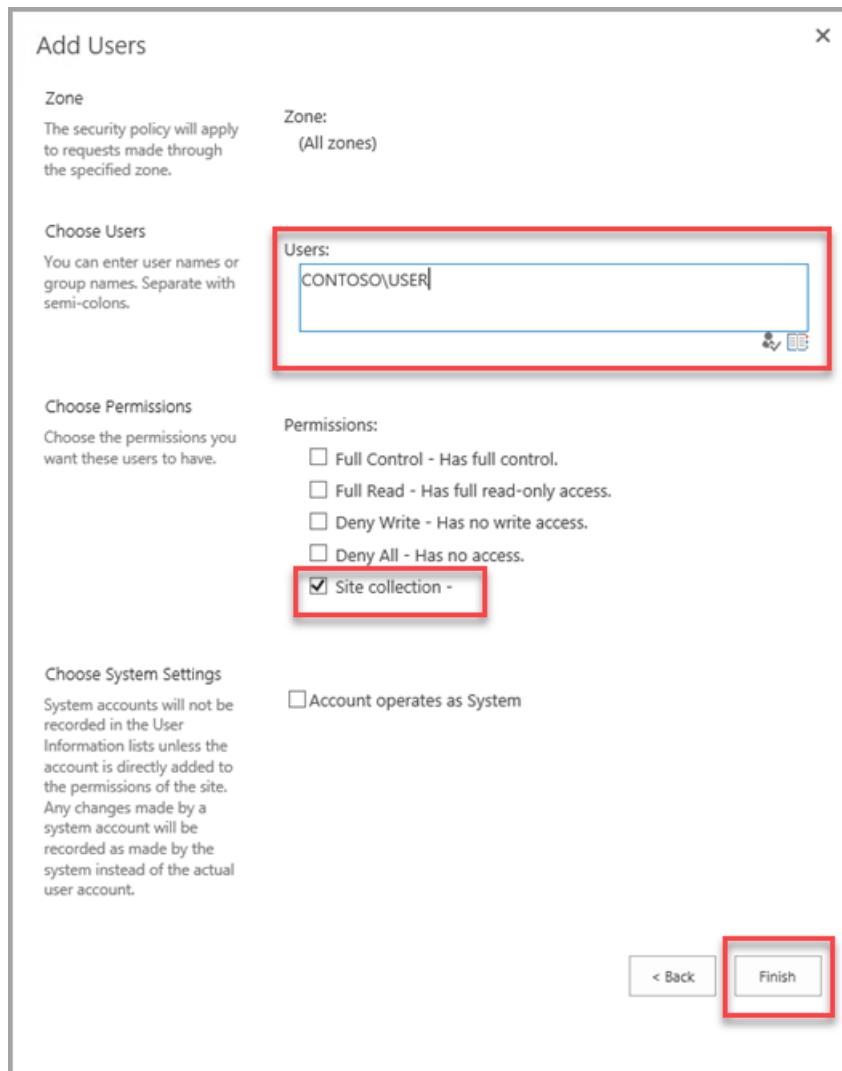
1. Open SharePoint, and select **Permission Policy** and select **Add Permission Policy Level**.



2. Under **Site Collection Permissions** select the **Site Collector Auditor** option.
3. Under **Permissions**, select **Grant** for the **View Application Pages** option and **Save** your changes.



4. After confirming your changes, click **OK** in the **Policy for Web Application** notice that opens,
5. In the **Add Users** page, add the user you intend to use for scanning in the **Choose users** field. Under **Choose Permissions**, select the **site collection** option and then click **Finish** to apply the permissions you created to the user you added or selected.



Configure a profile for the scanner

Before you install the scanner, create a profile for it in the Azure portal. This profile contains scanner settings and locations of the data repositories to scan.

1. Open a new browser window and [sign in to the Azure portal](#). Then navigate to the **Azure Information Protection** pane.

For example, in the search box for resources, services, and docs: Start typing **Information** and select **Azure Information Protection**.

2. Locate the **Scanner** options from the left pane, and select **Profiles**.
3. On the **Azure Information Protection - Profiles** pane, select **Add**:

The screenshot shows the 'Azure Information Protection - Profiles' pane. At the top, there is a toolbar with buttons for 'Add' (highlighted with a red box), 'Refresh', 'Export', 'Delete', 'Scan now', and 'Rescan all files'. Below the toolbar is a search bar with the placeholder 'Search to filter items...'. Underneath the search bar is a table header with columns: NAME, SCHED..., ENFORCE, REPOSIT..., NODES, LAST SC..., LAST SC..., and CURREN... . The table body is empty and displays the message 'No Scanner Profiles'.

4. On the **Add a new profile** pane, specify a name for the scanner that is used to identify its configuration settings and data repositories to scan. For example, for this quickstart, you might specify **Quickstart**. When you later install the scanner, you will need to specify the same profile name.

Optionally, specify a description for administrative purposes, to help you identify the scanner's profile name.

5. Locate the **Policy enforcement** section, where for this quickstart, select just one setting: For **Enforce**, select **Off**. Then select **Save** but do not close the pane.

The settings configure the scanner to do a one-time discovery of all files in your specified data repositories. This scan looks for all known sensitive information types, and doesn't require you to first configure your Azure Information Protection labels or policy settings.

6. Now that the profile is created and saved, you're ready to return to the **Configure repositories** option to specify your network folder as the data store to be scanned.

Still on the **Add a new profile** pane, select **Configure repositories** to open the **Repositories** pane:

The screenshot shows the 'Profile settings' section with 'Schedule' set to 'Manual'. Below it, 'Info types to be discovered' is set to 'Policy only'. A large orange box highlights the 'Configure repositories' section, which shows '0 repositories configured'.

7. On the **Repositories** pane, select **Add**:

The screenshot shows the 'Repositories' pane with a table header: PATH, DEFAULT LABEL, and ENFORCE. A blue box highlights the '+ Add' button in the top-left corner.

8. On the **Repository** pane, specify the folder that you created in the very first step. For example:

\server\TestScanner

For the remaining settings on this pane, do not change them but keep them as **Profile default**. This means that the data repository inherits the settings from the scanner profile.

Select **Save**.

9. Back on the **Azure Information Protection - Profiles** pane, you now see your profile listed, together with the **SCHEDULE** column showing **Manual** and the **ENFORCE** column is blank.

The **NODES** column shows **0** because you haven't yet installed the scanner for this profile.

You're now ready to install the scanner with the scanner profile that you've just created.

Install the scanner

1. Open a PowerShell session with the **Run as an administrator** option.
2. Use the following command to install the scanner, specifying the name of your network share and the profile name that you saved in the Azure portal:

```
Install-AIPScanner -SqlServerInstance <your network share name>\SQLEXPRESS -Profile <profile name>
```

When you're prompted, provide your own credentials for the scanner by using the <domain\user name> format, and then your password.

Start the scan and confirm it finished

1. Back in the Azure portal, refresh the **Azure Information Protection - Profiles** pane, and you should see the **NODES** column now display 1.
2. Select your profile name, and then the **Scan now** option:



If this option is not available after selecting your profile, the scanner is not connected to Azure Information Protection. Review your configuration and internet connectivity.

3. There's only one small file to inspect, so this initial test scan will be very quick:

Wait until you see values displayed for the **LAST SCAN RESULTS** and **LAST SCAN (END TIME)** columns.

Alternatively, for the scanner from the classic client only: Check the local Windows **Applications and Services** event log, **Azure Information Protection**. Confirm the informational event ID 911 for the **MSIP.Scanner** process. The event log entry also has a summary of results from the scan.

See detailed results

Using File Explorer, locate the scanner reports in `%localappdata%\Microsoft\MSIP\Scanner\Reports`. Open the detailed report file that has a .csv file format.

In Excel, the first two columns display your data store repository and file name. As you look through the columns, you'll see one named **Information Type Name**, which is the column you're most interested in. For our initial test, it displays **Credit Card Number**, one of many sensitive information types that the scanner can find.

Scan your own data

1. Edit your scanner profile and add a new data repository, this time specifying your own on-premises data store that you want to scan for sensitive information.

You can specify a network share (UNC path) or a SharePoint Server URL for a SharePoint site or library.

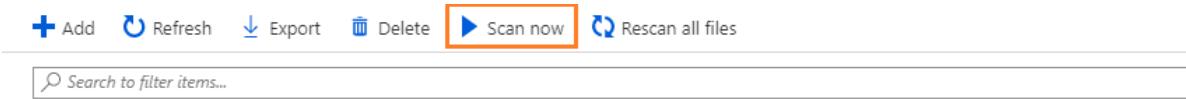
- Example for a network share

`\\\NAS\HR`

- Example for a SharePoint folder

`http://sp2016/Shared Documents`

2. Restart the scanner again: From the **Azure Information Protection - Profiles** pane, make sure your profile is selected, and then select the **Scan now** option:



3. View the new results when the scan is complete.

How long this scan takes depends on how many files there are in your data store, how large those files are, and the type of file.

Clean up resources

In a production environment, you would run the scanner on a Windows Server, using a service account that silently authenticates to the Azure Information Protection service. You would also use an enterprise-grade version of SQL Server, and likely specify several data repositories.

To clean up resources, ready for that production deployment, in your PowerShell session, run the following command to uninstall the scanner:

```
Uninstall-AIPScanner
```

Then restart your computer.

This command doesn't remove the following items and you must manually remove them if you don't want them after this quickstart:

- The SQL Server database that was created by running the `Install-AIPScanner` cmdlet when the Azure Information Protection scanner was installed:
 - For the classic client: `AIPScanner_<profile>`
 - For the unified labeling client: `AIPScannerUL_<profile_name>`
- The scanner reports located in `%localappdata%\Microsoft\MSIP\Scanner\Reports`.
- The **Log on as a service** user right assignment that your domain account was granted for your local computer.

Next steps

This quickstart includes the minimum configuration so that you can quickly see how the scanner can find sensitive information in on-premises data stores. If you're ready to install the scanner in a production environment, see [Deploying the Azure Information Protection scanner to automatically classify and protect files](#).

If you want to classify and protect the files that contain sensitive information, you must configure labels for automatic classification and protection:

- For the classic client:
 - [How to configure conditions for automatic and recommended classification for Azure Information Protection](#)
 - [How to configure a label for Rights Management protection](#)
- For the unified labeling client:
 - [Apply a sensitivity label to content automatically](#)
 - [Restrict access to content by using encryption in sensitivity labels](#)

Quickstart: Configure a label for users to easily protect emails that contain sensitive information

7/20/2020 • 4 minutes to read • [Edit Online](#)

Applies to: [Azure Information Protection](#)

Instructions for: [Azure Information Protection client for Windows](#)

NOTE

To provide a unified and streamlined customer experience, **Azure Information Protection client (classic)** and **Label Management** in the Azure Portal are being **deprecated** as of March 31, 2021. This time-frame allows all current Azure Information Protection customers to transition to our unified labeling solution using the Microsoft Information Protection Unified Labeling platform. Learn more in the official [deprecation notice](#).

In this quickstart, you'll configure an existing Azure Information Protection label to automatically apply the Do Not Forward protection setting.

The current Azure Information Protection policy already contains two labels that have this configuration:

- Confidential \ Recipients Only
- Highly Confidential \ Recipients Only

However, if your policy is older, or if protection wasn't activated at the time your organization's policy was created, you won't have these labels.

You can finish this configuration in 5 minutes.

Prerequisites

To complete this quickstart, you need:

1. A subscription that includes Azure Information Protection Plan 1 or Plan 2.

If you don't have one of these subscriptions, you can create a [free account](#) for your organization.

2. You've added the Azure Information Protection pane to the Azure portal, and confirmed that the protection service is activated.

If you need help with these actions, see [Quickstart: Get started in the Azure portal](#).

3. An existing Azure Information Protection label to configure.

You can use one of the default labels, or a label that you've created. If you need help with creating a new label, see [Quickstart: Create a new Azure Information Protection label for specific users](#).

4. To test the new label: The Azure Information Protection client (classic) must be installed on a Windows computer.

You can install the classic client by going to the [Microsoft download center](#) and download **AzInfoProtection.exe** from the Azure Information Protection page.

If you are using a different labeling client to the classic client, see the Microsoft 365 Compliance documentation

for equivalent instructions to this tutorial. For example, [Learn about sensitivity labels](#).

5. To test the new label: A computer running Windows (minimum of Windows 7 with Service Pack 1), and on this computer, you're signed in to Office apps from one of the following categories:
 - Office apps minimum version 1805, build 9330.2078 from Office 365 Business or Microsoft 365 Business when you are assigned a license for Azure Rights Management (also known as Azure Information Protection for Office 365).
 - Office 365 ProPlus.
 - Office Professional Plus 2019.
 - Office Professional Plus 2016.
 - Office Professional Plus 2013 with Service Pack 1.
 - Office Professional Plus 2010 with Service Pack 2.

For a full list of prerequisites to use Azure Information Protection, see [Requirements for Azure Information Protection](#).

Configure an existing label to apply the Do Not Forward protection

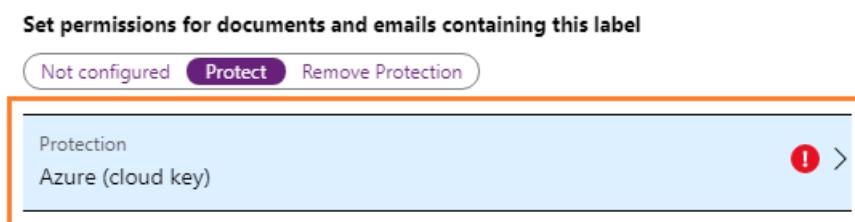
1. Open a new browser window and sign in to the [Azure portal](#) as a global admin. Then navigate to [Azure Information Protection](#).

For example, in the search box for resources, services, and docs: Start typing **Information** and select **Azure Information Protection**.

If you are not the global admin, use the following link for alternative roles: [Signing in to the Azure portal](#)

2. From the **Classifications > Labels** menu option: On the **Azure Information Protection - Labels** pane, select the label you want to configure to apply the protection.
3. On the **Label** pane, locate **Set permissions for documents and emails containing this label**. Select **Protect**, and the **Protection** pane automatically opens if **Not configured** or **Remove Protection** was previously selected.

If the **Protection** pane does not automatically open, select **Protection**:



4. On the **Protection** pane, make sure that **Azure (cloud key)** is selected.
5. Select **Set user-defined permissions (Preview)**.
6. Make sure that the following option is selected: **In Outlook apply Do Not Forward**.
7. If selected, clear the following option: **In Word, Excel, PowerPoint and File Explorer prompt user for custom permissions**.
8. Click **OK** on the **Protection** pane, and then click **Save** on the **Label** pane.

Your label is now configured to display in Outlook only, and apply the Do Not Forward protection to emails.

Test your new label

Your configured label displays only in Outlook and is suitable for emails sent to any recipient outside your organization when Exchange Online is configured for the [new capabilities in Office 365 Message Encryption](#).

1. On your computer, open Outlook and create a new email message. If Outlook is already open, restart it to force a policy refresh.
2. Specify the recipients, some text for the email message, and then apply the label that you just created.

The email message is classified according to the label name, and protected with the Do Not Forward restriction.

3. Send the email.

The result is that recipients cannot forward the email, or print it, copy from it, or save attachments, or save the email as a different name. The protected email message can be read by any user, on any device.

Clean up resources

Do the following if you do not want to keep this configuration and return your label such that it doesn't apply protection:

1. From the **Classifications > Labels** menu option: On the **Azure Information Protection - Labels** pane, select the label you configured.
2. On the **Label** pane, locate **Set permissions for documents and emails containing this label**, select **Not configured**, and select **Save**.

Next steps

This quickstart includes the minimum options so that you can quickly configure a label that makes it easy for users to protect their emails. However, if the configuration is too restrictive, or not restrictive enough, see the other example configurations:

- [Label for protected email that supports less restrictive permissions than Do Not Forward](#)
- [Label that encrypts content but doesn't restrict who can access it](#)

For full instructions how to configure a label that applies protection, see [How to configure a label for Rights Management protection](#).

Quickstart: Create a new Azure Information Protection label for specific users

7/20/2020 • 4 minutes to read • [Edit Online](#)

Applies to: [Azure Information Protection](#)

Instructions for: [Azure Information Protection client for Windows](#)

NOTE

To provide a unified and streamlined customer experience, **Azure Information Protection client (classic)** and **Label Management** in the Azure Portal are being **deprecated** as of **March 31, 2021**. This time-frame allows all current Azure Information Protection customers to transition to our unified labeling solution using the Microsoft Information Protection Unified Labeling platform. Learn more in the official [deprecation notice](#).

In this quickstart, you'll create a new Azure Information Protection label that only specific users can see and apply to classify and protect their documents and emails.

This configuration uses a scoped policy.

You can finish this configuration in less than 10 minutes.

Prerequisites

To complete this quickstart, you need:

1. A subscription that includes Azure Information Protection Plan 1 or Plan 2.

If you don't have one of these subscriptions, you can create a [free](#) account for your organization.

2. You've added the Azure Information Protection pane to the Azure portal, and confirmed that the protection service is activated.

If you need help with these actions, see [Quickstart: Get started in the Azure portal](#).

3. An emailed-enabled group in Azure AD that contains the users who will see and apply the new label.

If you don't have a suitable group, create one named **Sales Team** and add at least one user.

4. To test the new label: The Azure Information Protection client (classic) must be installed on a Windows computer.

You can install the classic client by going to the [Microsoft download center](#) and download **AzInfoProtection.exe** from the Azure Information Protection page.

If you are using a different labeling client to the classic client, see the Microsoft 365 Compliance documentation for equivalent instructions to this tutorial. For example, [Learn about sensitivity labels](#).

For a full list of prerequisites to use Azure Information Protection, see [Requirements for Azure Information Protection](#).

Create a new label

First, create your new label.

1. If you haven't already done so, open a new browser window and sign in to the [Azure portal](#). Then navigate to the **Azure Information Protection** pane.

For example, in the search box for resources, services, and docs: Start typing **Information** and select **Azure Information Protection**.

If you are not the global admin, use the following link for alternative roles: [Signing in to the Azure portal](#)

2. From the **Classifications > Labels** menu option: On the **Azure Information Protection - Labels** pane, click **Add a new label**.
3. On the **Label** pane, specify at least the following:

- **Label display name:** A name for the new label that users will see, and that identifies the classification for the content. For example: **Sales - Restricted**.
- **Description:** A tooltip to help users identify when to select this new label. For example:
Business data that is restricted to the Sales Team.

4. Make sure that **Enabled** is set to **On** (the default), and select **Save**.

Add the label to a new scoped policy

Now, add your newly created label to a new scoped policy.

1. From the **Classifications > Policies** menu option: On the **Azure Information Protection - Policies** pane, select **Add a new policy**.
2. On the **Policy** pane, for the **Policy name** box, enter a name that identifies the group of users who will see your new created label. For example, **Sales**.
3. Select the option **Select which users or groups get this policy**.
4. On the **AAD users and Groups** pane, select **Users/Groups**. Then on the new **Users/Groups** pane, search for and select the group that you identified in the prerequisites. For example, **Sales Team**. Click **Select** on that pane, and then **OK**.
5. Back on the **Policy** pane, select **Add or remove labels**.
6. On the **Policy: Add or remove labels** pane, select the label that you created, for example, **Sales - Restricted**, and then select **OK**.
7. Back on the **Policy** pane, select **Save**.

Your new label is now published just to the members of the group that you specified.

Test your new label

To test this label, you need a minimum of two computers because the Azure Information Protection client does not support multiple users on the same computer:

- On your first computer, sign in as a member of the Sales Team group. Open Word and confirm that you can see the new label. If Word is already open, restart it to force a policy refresh.
- On your second computer, sign in as a user who isn't a member of the Sales Team group. Open Word and confirm that you can't see the new label. As before, if Word is already open, restart it.

Clean up resources

Do the following if you do not want to keep this label and scoped policy:

1. From the **Classifications > Policies** menu option: On the **Azure Information Protection - Policies** pane, select the context menu (...) for the scoped policy you just created. For example, **Sales**.
2. Select **Delete policy** and if you're asked to confirm, select **OK**.
3. From the **Classifications > Label** menu option: On the **Azure Information Protection - Label** pane, select the context menu (...) for the label you just created. For example, **Sales - Restricted**.
4. Select **Delete this label** and if you're asked to confirm, select **OK**.

Next steps

This quickstart includes the minimum options so that you can quickly create a new label for specific users. For full instructions, see the following articles:

- [How to create a new label](#)
- [How to configure the policy for specific users by using scoped policies](#)

In addition, if you want the label to protect the content such that only members of the Sales Team could open it, you will need to configure the label to apply protection. For instructions, see [How to configure a label for Rights Management protection](#).

Tutorial: Configure Azure Information Protection policy settings and create a new label

7/20/2020 • 11 minutes to read • [Edit Online](#)

Applies to: [Azure Information Protection](#)

Instructions for: [Azure Information Protection client for Windows](#)

NOTE

To provide a unified and streamlined customer experience, **Azure Information Protection client (classic)** and **Label Management** in the Azure Portal are being **deprecated** as of **March 31, 2021**. This time-frame allows all current Azure Information Protection customers to transition to our unified labeling solution using the Microsoft Information Protection Unified Labeling platform. Learn more in the official [deprecation notice](#).

In this tutorial, you learn how to:

- Configure policy settings
- Create a new label
- Configure the label for visual markings, recommended classification, and protection
- See your settings and labels in action

As a result of this configuration, users see a default label applied when they create a new document or email. However, they are prompted to apply the new label when credit card information is detected. When the new label is applied, the content is reclassified and protected, with a corresponding footer and watermark.

You can finish this tutorial in about 15 minutes.

Prerequisites

To complete this tutorial, you need:

1. A subscription that includes Azure Information Protection Plan 2.

If you don't have a subscription that includes Azure Information Protection Plan 2, you can create a [free](#) account for your organization.

2. The Azure Information Protection pane is added to the Azure portal, the protection service is activated, and you have one or more labels published in the Azure Information Protection global policy.

These steps are covered in the [Quickstart: Add Azure Information Protection to the Azure portal and view the policy](#).

3. The Azure Information Protection client (classic) is installed on your Windows computer (minimum of Windows 7 with Service Pack 1).

You can install the classic client by going to the [Microsoft download center](#) and download **AzInfoProtection.exe** from the Azure Information Protection page. If you are using a different labeling client to the classic client, see the [Microsoft 365 Compliance documentation](#) for equivalent instructions to this tutorial.

4. You're signed in to Office apps from one of the following categories:

- Office apps minimum version 1805, build 9330.2078 from Office 365 Business or Microsoft 365 Business when you are assigned a license for Azure Rights Management (also known as Azure Information Protection for Office 365).
- Office 365 ProPlus.
- Office Professional Plus 2019.
- Office Professional Plus 2016.
- Office Professional Plus 2013 with Service Pack 1.
- Office Professional Plus 2010 with Service Pack 2.

For a full list of prerequisites to use Azure Information Protection, see [Requirements for Azure Information Protection](#).

Let's get started.

Edit the Azure Information Protection policy

Using the Azure portal, we'll first change a couple of policy settings, and then create a new label.

Edit the policy settings

1. Open a new browser window and sign in to the [Azure portal](#) as a global admin. Then navigate to **Azure Information Protection**.

For example, in the search box for resources, services, and docs: Start typing **Information** and select **Azure Information Protection**.

If you are not the global admin, use the following link for alternative roles: [Signing in to the Azure portal](#)

2. Select **Classifications > Policies > Global** to open the **Policy: Global** pane.
3. Locate the policy settings after the labels, in the **Configure settings to display and apply on Information Protection end users** section.

Make a note of how the settings are currently configured. Specifically, the settings **Select the default label** and **Users must provide justification to set a lower classification label, remove a label, or remove protection**. For example:

Configure settings to display and apply on Information Protection end users

Title	Sensitivity
Tooltip	The current label for this content. This setting identifies the risk to the business if this content is shared with unauthorized people inside or outside the organization.
Select the default label	None
Send audit data to Azure Information Protection analytics	Off Not configured
All documents and emails must have a label (applied automatically or by users)	Off On
Users must provide justification to set a lower classification label, remove a label, or remove protection	Off On

We'll use these policy settings later in the tutorial when you will see them in action.

4. For **Select the default label**, select one of the labels, such as **General**.

The **General** label is one of the default labels that Azure Information Protection can create for you. This step is covered in the [Create and publish labels](#) section from the quickstart to add Azure Information Protection to the Azure portal.

5. For **Users must provide justification to set a lower classification label, remove a label, or remove protection**, set this option to **On** if it is not already.

6. In addition, make sure that **Display the Information Protection bar in Office apps** is set to **On**.

7. Select **Save** on this **Policy: Global** pane, and if you're prompted to confirm your action, select **OK**. Close this pane.

Create a new label for protection, visual markers, and a condition to prompt for classification

We'll now create a new sublabel for **Confidential**.

1. From the **Classifications > Labels** menu option: Right-click the **Confidential** label, and select **Add a sub-label**.

If you don't have a label named **Confidential**, you can select another label or you can create a new label instead and still follow the tutorial with minor differences.

2. On the **Sub-label** pane, specify the label name of **Finance** and add the following description: **Confidential data that contains financial information that is restricted to employees only.**

This text describes how the selected label is intended to be used and it's visible to users as a tooltip, to help them decide which label to select.

3. For **Set permissions for documents and emails containing this label**, select **Protect**, which automatically opens the **Protection** pane by selecting the **Protection** option for you:

Set permissions for documents and emails containing this label

[Not configured](#) **Protect** [Remove Protection](#)



4. On the **Protection** pane, make sure that **Azure (cloud key)** is selected. This option uses the Azure Rights Management service to protect documents and emails. Also make sure that the **Set Permissions** option is selected. Then select **Add permissions**.

5. On the **Add permissions** pane, select **Add <organization name> - All members**. For example, if your organization name is VanArsdel Ltd, you see the following option to select:

Specify users and groups

[Select from the list](#) [Enter details](#)

+ Add VanArsdel, Ltd - All members

+ Add any authenticated users

+ Browse directory

This option automatically selects all the users in your organization who can be granted permissions. However, you can see from the other options that you could browse and search for groups or users from

your tenant. Or, when you select the **Enter details** option, you can specify individual email addresses or even all users from another organization.

6. For the permissions, select **Reviewer** from the preset options. You see how this permission level automatically grants some permissions listed but not all permissions:

Choose permissions from preset or set custom ?

Co-Owner Co-Author **Reviewer** Viewer Custom

PERMISSIONS

View, Open, Read (VIEW)
 View Rights (VIEWRIGHTSDATA)
 Edit Content, Edit (DOCEDIT)
 Save (EDIT)

Print (PRINT)

Copy (EXTRACT)

Reply (REPLY) **
 Reply All (REPLY ALL) **
 Forward (FORWARD) **

Change Rights (EDITRIGHTSDATA)

Save As, Export (EXPORT)

Allow Macros (OBJMODEL) *

Full Control (OWNER)

You can select different permission levels or specify individual usage rights by using the **Custom** option. But for this tutorial, keep the **Reviewer** option. You can experiment with different permissions later and read how they restrict what the specified users can do with the protected document or email.

7. Click **OK** to close this **Add permissions** pane, and you see how the **Protection** pane is updated to reflect your configuration. For example:

USERS	PERMISSIONS	...
vanarsdelltd.onmicrosoft.com	Reviewer	...
+ Add permissions		

If you select **Add permissions**, this action opens the **Add permissions** pane again, so that you can add more users and grant them different permissions. For example, grant just view access for a specific group. But for this tutorial, we'll keep with one set of permissions for all users.

8. Review and keep the defaults for content expiration and offline access, and then click **OK** to save and close this **Protection** pane.
9. Back on the Sub-label pane, locate the **Set visual marking** section:

For the **Documents with this label have a footer** setting, click **On**, and then for the **Text** box, type **Classified as Confidential**.

For the **Documents with this label have a watermark** setting, click **On**, and then for the **Text** box, type

your organization name. For example, **VanArsdel, Ltd**

Although you can change the appearance for these visual markers, we'll leave these settings at the defaults for now.

10. Locate the section **Configure conditions for automatically applying this label**:

Click **Add a new condition** and then, on the **Condition** pane, select the following:

- a. **Choose the type of condition:** Keep the default of **Information Types**.
- b. For **Choose an industry:** Keep the default of **All**.
- c. In the **Select information types** search box: Type **credit card number**. Then, from the search results, select **Credit Card Number**.
- d. **Minimum number of occurrences:** Keep the default of **1**.
- e. **Count occurrences with unique values only:** Keep the default of **Off**.

The screenshot shows the 'Condition' pane with the following settings:

- Choose the type of condition:** Information Types (selected)
- Choose an industry:** All (selected)
- Select information types:** credit card number (searched)
- NAME:** Credit Card Number (checkbox checked)
- * Minimum number of occurrences:** 1
- Count occurrences with unique values only:** Off (selected)

Click **Save** to return to the **Sub-label** pane.

11. On the **Sub-label** pane, you see that **Credit Card Number** is displayed as the **CONDITION NAME**, with **1 OCCURRENCES**:

Configure conditions for automatically applying this label ⓘ

If any of these conditions are met, this label is applied

CONDITION NAME	OCCURRENCES
Credit Card Number	1
+ Add a new condition	

12. For **Select how this label is applied:** Keep the default of **Recommended**, and don't change the default policy tip.

13. In the **Add notes for administrator use** box, type **For testing purposes only**.

14. Click **Save** on this **Sub-label** pane. If you're prompted to confirm, click **OK**. The new label is created and saved, but not yet added to a policy.

15. From the **Classifications > Policies** menu option: Select **Global** again, and then select the **Add or remove labels** link after the labels.

- From the **Policy: Add or remove labels** pane, select the label that you've just created, the sublabel named **Finance**, and click **OK**.
- On the **Policy: Global** pane, you now see your new sublabel in your global policy, which is configured for visual markings and protection. For example:

LABEL DISPLAY NAME	POLICY	MARKING	PROTECTION
Personal	Global		
Public	Global		
General	Global		
▼ Confidential	Global		
All Employees	Global	✓	✓
Anyone (not protected)	Global	✓	
Recipients Only	Global	✓	✓
Finance	Global	✓	✓
► ■ Highly Confidential	Global		
Add or remove labels			

You also see that the settings are configured for the default label and justification:

Select the default label
General

Send audit data to Azure Information Protection analytics ⓘ
Off Not configured

All documents and emails must have a label (applied automatically or by users)
Off On

Users must provide justification to set a lower classification label, remove a label, or remove protection
Off On

- Click **Save** on this **Policy: Global** pane. If you're prompted to confirm this action, click **OK**.

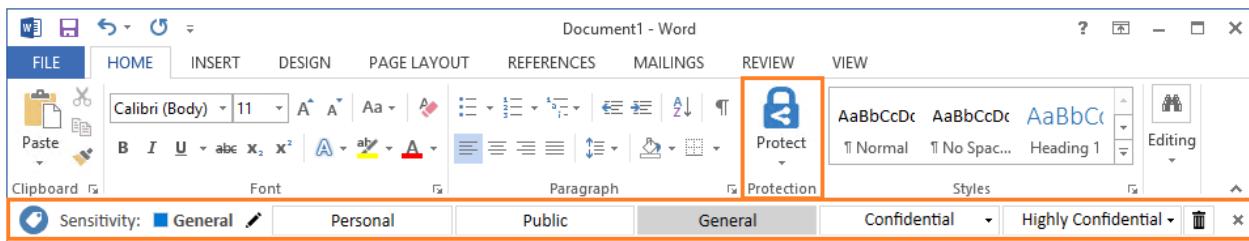
You can either close the Azure portal, or leave it open to try additional configuration options after you've finished this tutorial.

You're ready to try out the results of your changes.

See classification, labeling, and protection in action

The policy changes you made and the new label you created applies to Word, Excel, PowerPoint, and Outlook. But for this tutorial, we'll use Word to see them in action.

Open a new document in Word. Because the Azure Information Protection client is installed, you see the following:



- On the **Home** tab, a **Protection** group, with a button named **Protect**.

Click Protect > Help and Feedback, and in the Microsoft Azure Information Protection dialog box, confirm your client status. It should display **Connected as** and your user name. In addition, you should also see a recent time and date for the last connection and when the Information Protection policy was downloaded. Verify that your displayed user name is correct for your tenant.

- A new bar under the ribbon; the Information Protection bar. It displays the title of **Sensitivity**, and the labels that we saw in the Azure portal.

To manually change our default label

1. On the Information Protection bar, select the last label and you see how sublabels display:



2. Select one of these sublabels, and you see how the other labels no longer display on the bar now that you've selected a label for this document. The **Sensitivity** value changes to show the label and sublabel name, with a corresponding change in label color. For example:

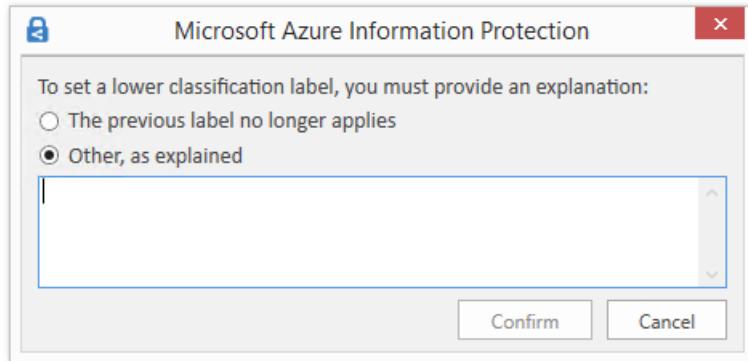


3. On the Information Protection bar, click the **Edit Label** icon next to the currently selected label value:



This action displays the available labels again.

4. Now select the first label, **Personal**. Because you've selected a label that's a lower classification than the previously selected label for this document, you're prompted to justify why you're lowering the classification level:



Select **The previous label no longer applies**, and click **Confirm**. The **Sensitivity** value changes to **Personal** and the other labels are hidden again.

To remove the classification completely

1. On the Information Protection bar, click the **Edit Label** icon again. But instead of choosing one of the labels, click the **Delete Label** icon:

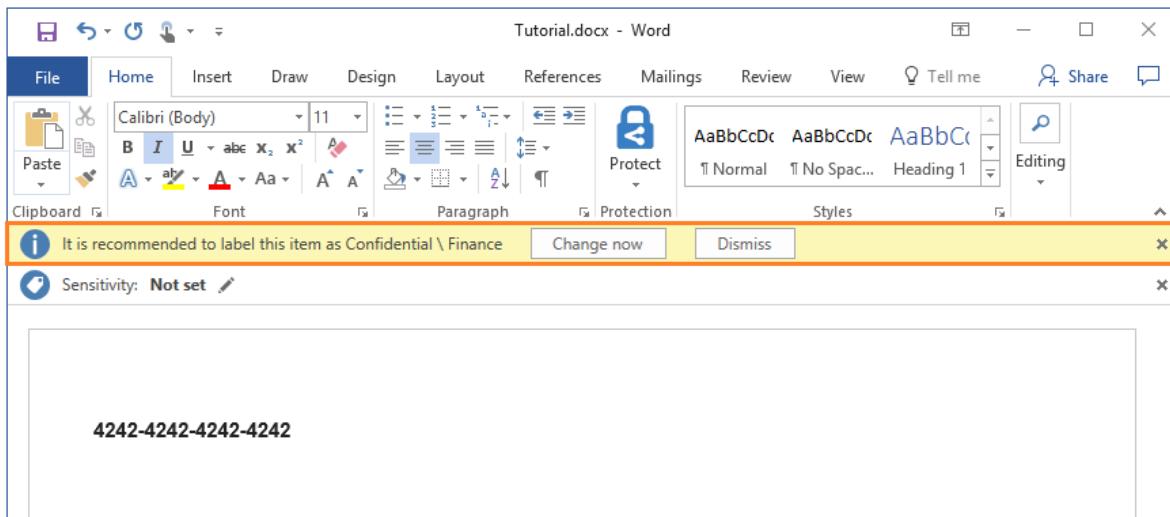


2. This time when you're prompted, type "This document doesn't need classifying", and click **Confirm**.

You see the **Sensitivity** value display **Not set**, which is what users see initially for new documents if you don't set a default label as a policy setting.

To see a recommendation prompt for labeling and automatic protection

1. In the Word document, type a valid credit card number, for example: 4242-4242-4242-4242.
2. Save the document locally, with any file name.
3. You now see a prompt to apply the label that you configured for protection when credit card numbers are detected. If we didn't agree with the recommendation, our policy setting lets us reject it, by selecting **Dismiss**. Giving a recommendation but letting a user override it helps to reduce false positives when you're using automatic classification. For this tutorial, click **Change now**.



In addition to the document now showing that our configured label is applied (for example, **Confidential \ Finance**), you immediately see the watermark of your organization name across the page, and the footer of **Classified as Confidential** is also applied.

The document is also protected with the permissions that you specified for this label. You can confirm that the document is protected by clicking the **File** tab and view the information for **Protect Document**. You see that the document is protected by **Confidential \ Finance** and the label description.

Because of the protection configuration of the label, only employees can open the document and some actions are restricted for them. For example, because they don't have the Print and the Copy and extract content permissions, they can't print the document or copy from it. Such restrictions help to prevent data loss. As the owner of the document, you can print it and copy from it. However, if you email the document to another user in your organization, they cannot do these actions.

4. You can now close this document.

Clean up resources

Do the following if you don't want to keep the changes that you made in this tutorial:

1. Select **Classifications > Policies > Global** to open the **Policy: Global** pane.
2. Return the policy settings to their original values that you took a note of, and then select **Save**.
3. From the **Classifications > Label** menu option: On the **Azure Information Protection - Label** pane, select the context menu (...) for the **Finance** label you created.
4. Select **Delete this label** and if you're asked to confirm, select **OK**.

Restart Word to download these changes.

Next steps

For more information about editing the Azure Information Protection policy, see [Configuring Azure Information](#)

Protection policy

For more information about where the labeling activity is logged, see [Usage logging for the Azure Information Protection client](#).

Tutorial: Configure Azure Information Protection policy settings that work together

7/20/2020 • 8 minutes to read • [Edit Online](#)

Applies to: [Azure Information Protection](#)

Instructions for: [Azure Information Protection client for Windows](#)

NOTE

To provide a unified and streamlined customer experience, **Azure Information Protection client (classic)** and **Label Management** in the Azure Portal are being **deprecated** as of **March 31, 2021**. This time-frame allows all current Azure Information Protection customers to transition to our unified labeling solution using the Microsoft Information Protection Unified Labeling platform. Learn more in the official [deprecation notice](#).

In this tutorial, you learn how to:

- Configure policy settings that work together
- See your settings in action

Rather than relying on users to manually label their documents and emails, you can use Azure Information Protection policy settings to:

- Ensure a base level of classification for new and edited content
- Educate users about labels and make it easy for them to apply the correct label

You can finish this tutorial in about 15 minutes.

Prerequisites

To complete this tutorial, you need:

1. A subscription that includes Azure Information Protection Plan 1 or Plan 2.

If you don't have a subscription that includes this plan, you can create a [free](#) account for your organization.

2. The Azure Information Protection pane is added to the Azure portal and you have one or more labels published in the Azure Information Protection global policy.

These steps are covered in the [Quickstart: Add Azure Information Protection to the Azure portal and view the policy](#).

3. The Azure Information Protection client (classic) is installed on your Windows computer (minimum of Windows 7 with Service Pack 1).

You can install the classic client by going to the [Microsoft download center](#) and download **AzInfoProtection.exe** from the Azure Information Protection page.

If you are using a different labeling client to the classic client, see the Microsoft 365 Compliance documentation for information about policy settings for sensitivity labels. For example, [Learn about sensitivity labels](#).

4. You are signed in to Office apps from one of the following categories:

- Office apps minimum version 1805, build 9330.2078 from Office 365 Business or Microsoft 365 Business when you are assigned a license for Azure Rights Management (also known as Azure Information Protection for Office 365).
- Office 365 ProPlus.
- Office Professional Plus 2019.
- Office Professional Plus 2016.
- Office Professional Plus 2013 with Service Pack 1.
- Office Professional Plus 2010 with Service Pack 2.

For a full list of prerequisites to use Azure Information Protection, see [Requirements for Azure Information Protection](#).

Let's get started.

Edit the Azure Information Protection policy

Rather than relying on users to manually label their documents and emails, you can use some of the policy settings to ensure a base level of classification.

Using the Azure portal, we'll edit the global policy to change policy settings for all users.

1. Open a new browser window and sign in to the [Azure portal](#) as a global admin. Then navigate to **Azure Information Protection**.

For example, in the search box for resources, services, and docs: Start typing **Information** and select **Azure Information Protection**.

If you are not the global admin, use the following link for alternative roles: [Signing in to the Azure portal](#)

2. Select **Classifications > Policies > Global** to open the **Policy: Global** pane.
3. Locate the policy settings after the labels, in the **Configure settings to display and apply on Information Protection end users** section. Your settings might have different values to ones shown:

Configure settings to display and apply on Information Protection end users

* Title

Sensitivity

Tooltip

The current label for this content. This setting identifies the risk to the business if this content is shared with unauthorized people inside or outside the organization.

Select the default label

None

Send audit data to Azure Information Protection analytics ⓘ

Off Not configured

All documents and emails must have a label (applied automatically or by users)

Off On

Users must provide justification to set a lower classification label, remove a label, or remove protection

Off On

For email messages with attachments, apply a label that matches the highest classification of those attachments

Off Automatic Recommended

Display the Information Protection bar in Office apps

Off On

Add the Do Not Forward button to the Outlook ribbon

Off On

Make the custom permissions option available for users

Off On

Provide a custom URL for the Azure Information Protection client "Tell me more" web page (optional; otherwise keep blank)

Enter a custom URL or keep blank

4. Change your settings to match the value in the following table. Make a note of the settings that you change in case you want to change them back again when you have finished this tutorial.

SETTING	VALUE	INFORMATION
Select the default label	General	The General label is one of the default labels that Azure Information Protection can create for you. This step is covered in the Create and publish labels quickstart. If you don't have a label named General , select another label from the dropdown list. Unlabeled documents and emails will have this label applied automatically as a base classification. However, users can change your selected label to a different one.
All documents and emails must have a label	On	This setting is often referred to as mandatory labeling because it prevents users from saving documents or sending emails that are unlabeled. Together with the default label, documents and emails will have either the default label that you set, or a label that they choose.

SETTING	VALUE	INFORMATION
For email messages with attachments, apply a label that matches the highest classification of those attachments	Recommended	This setting prompts users to select a higher classification label for their emails when they attach documents that have a higher classification than your selected default label.
Display the Information Protection bar in Office apps	On	Displaying the Information Protection bar makes it easier for users to see and change the default label.

The settings should now look like this:

Select the default label
General

Send audit data to Azure Information Protection analytics ⓘ
Off Not configured

All documents and emails must have a label (applied automatically or by users)
Off On

Users must provide justification to set a lower classification label, remove a label, or remove protection
Off On

For email messages with attachments, apply a label that matches the highest classification of those attachments
Off Automatic Recommended

Add policy tip describing to users the reasons for applying this label
It is recommended to label this email as \${Attachment.Label} ✓

Display the Information Protection bar in Office apps
Off On

Add the Do Not Forward button to the Outlook ribbon
Off On

Make the custom permissions option available for users
Off On

5. Select **Save** on this **Policy: Global** pane, and if you're prompted to confirm your action, select **OK**.

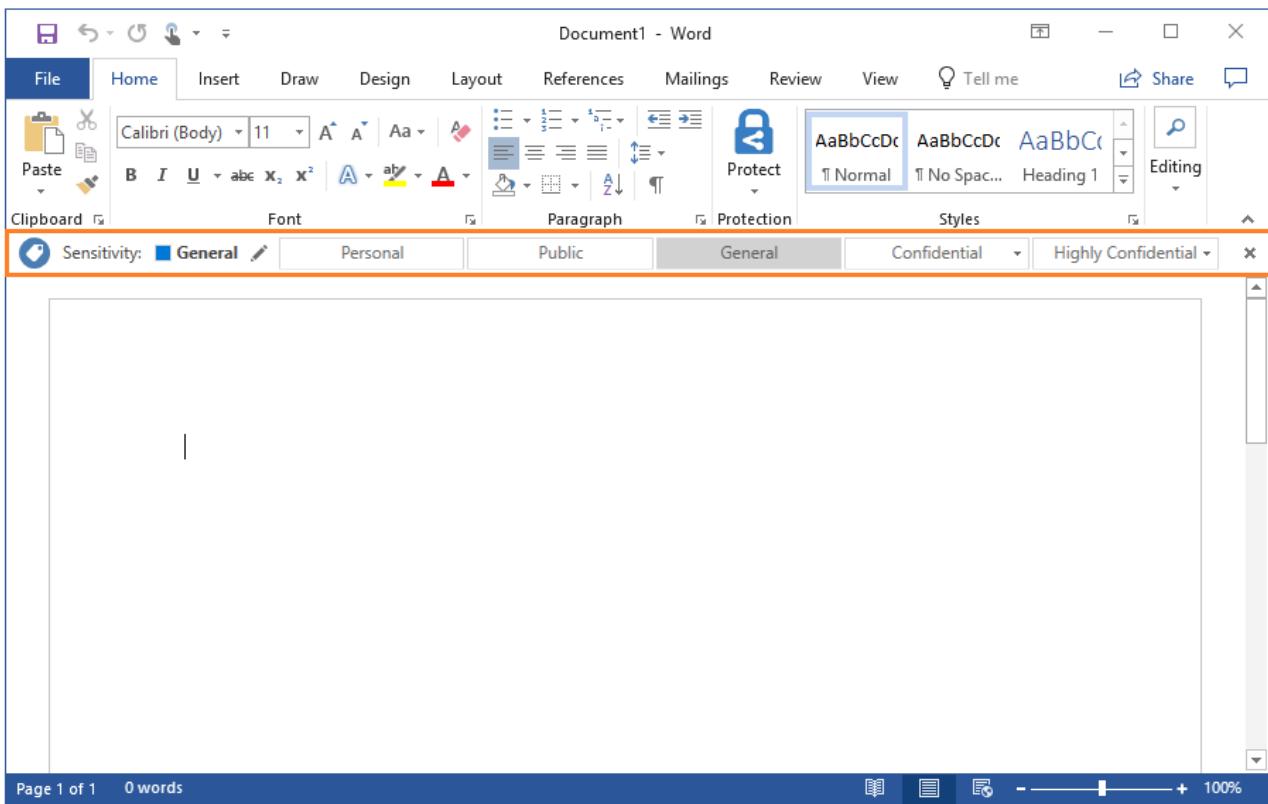
See your policy settings in action

For this tutorial, we'll use Word and Outlook to see your policy changes in action. If these apps were already loaded before you changed the policy settings, restart them to download the changes.

Default label and the Information Protection bar

Open a new document in Word. You see the document is automatically labeled as **General** rather than relying on users to select a label.

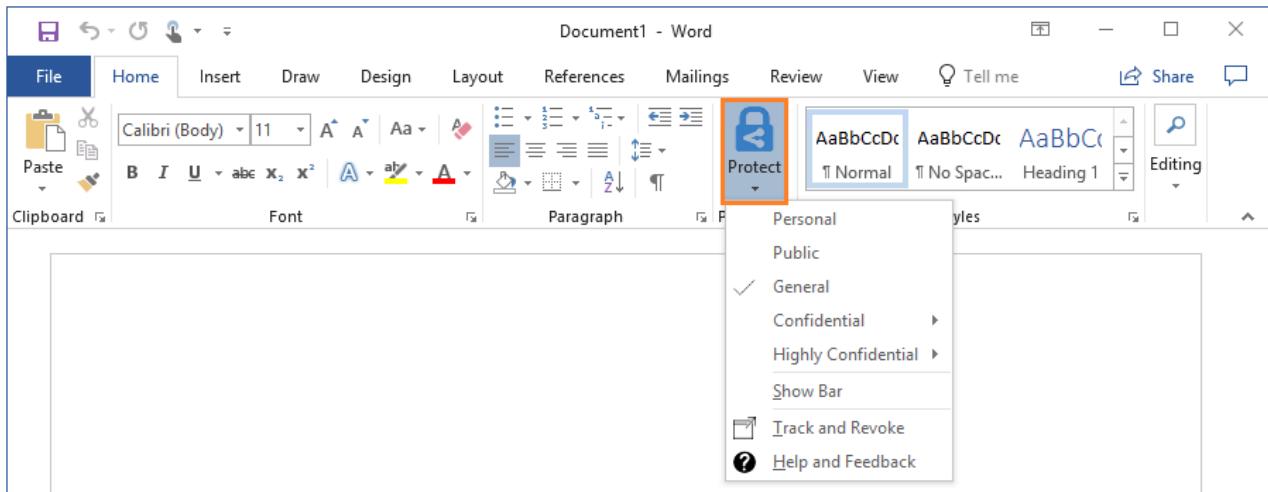
With the Information Protection bar displayed and showing the available labels, it's easy for users to see the currently selected label, and change it if the default label isn't appropriate:



Instead of changing the label, close the Information Protection bar to compare the experience if the bar is not shown:



The **General** label is still selected, but it's much less obvious. It's also less obvious how to select a different label. To do that, users must select the **Protect** button:



Now, from the pull-down menu, you see that the **General** label is selected because it has a check mark next to it. To change the currently selected label, users can select a different label from the list. When users are new to labeling, they probably won't remember to select the **Protect** button each time. They also might not realize that they can select another label.

To display the Information Protection bar again, select **Show Bar** from the pull-down menu.

TIP

You can select a different default label for Outlook, by configuring an [advanced client setting](#).

Mandatory labeling

You can change the currently selected **General** label to a different label, but you cannot remove it. Because we changed the **All documents and emails must have a label** setting to **On**, the **Delete Label** icon is not available on the Information Protection bar.

If we hadn't changed that setting, the Information Protection bar shows this icon:



Together with a default label, mandatory labeling ensures that new and edited documents (and emails) have a base classification of your choosing.

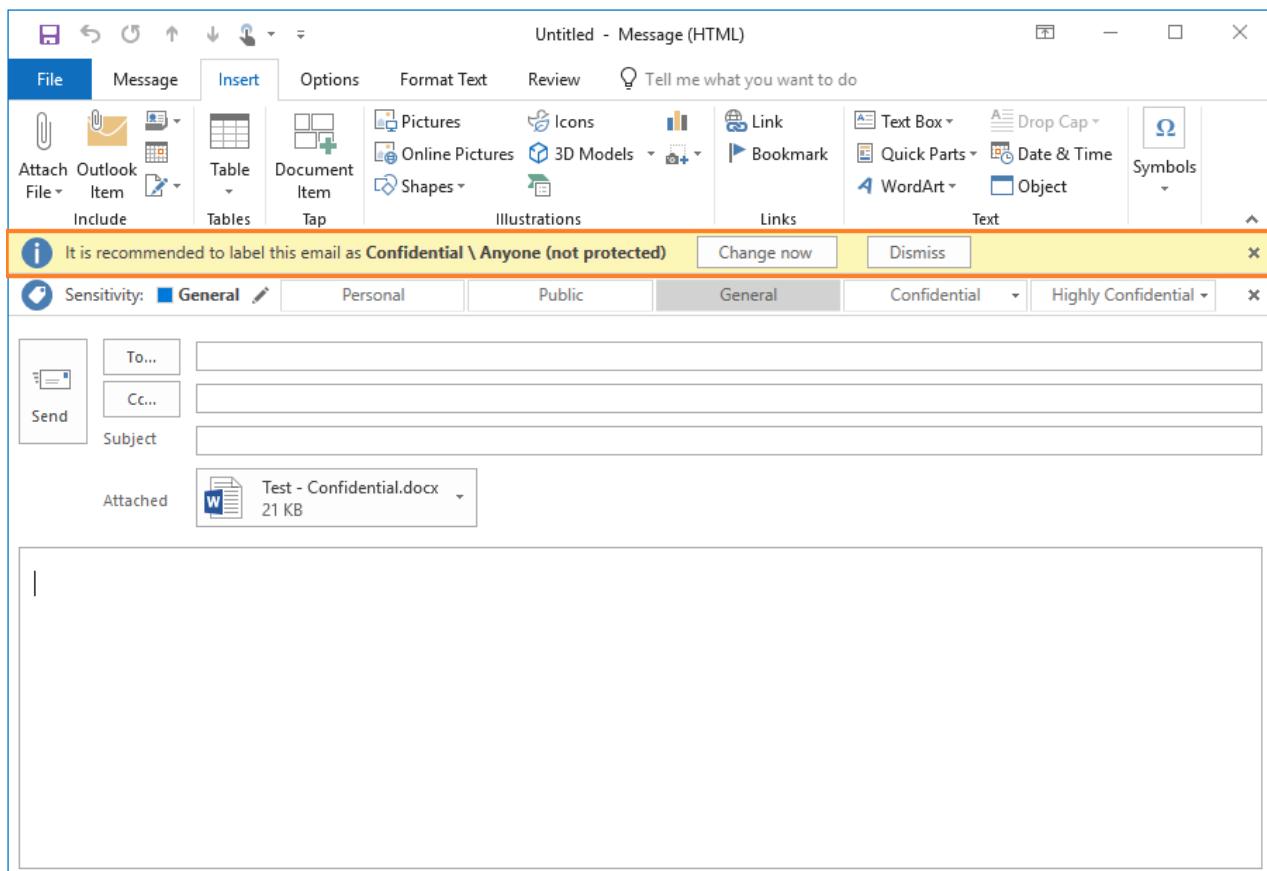
If we hadn't set a default label with the mandatory labeling setting, users are always prompted to select a label when they save an unlabeled document or send an unlabeled email. For many users, these continual prompts can be frustrating and also result in less accurate labeling. For them to be prompted to select a label when they've finished working on a document or email interrupts their workflows, and there's then a temptation for them to select any label at random so they can move onto the next thing they need to do.

Recommendations for emails with attachments

For the open Word document, choose a label that has a higher classification than **General**. For example, one of the sublabels under **Confidential**, such as **Confidential - Anyone (not protected)**. Save the document locally and give it any name.

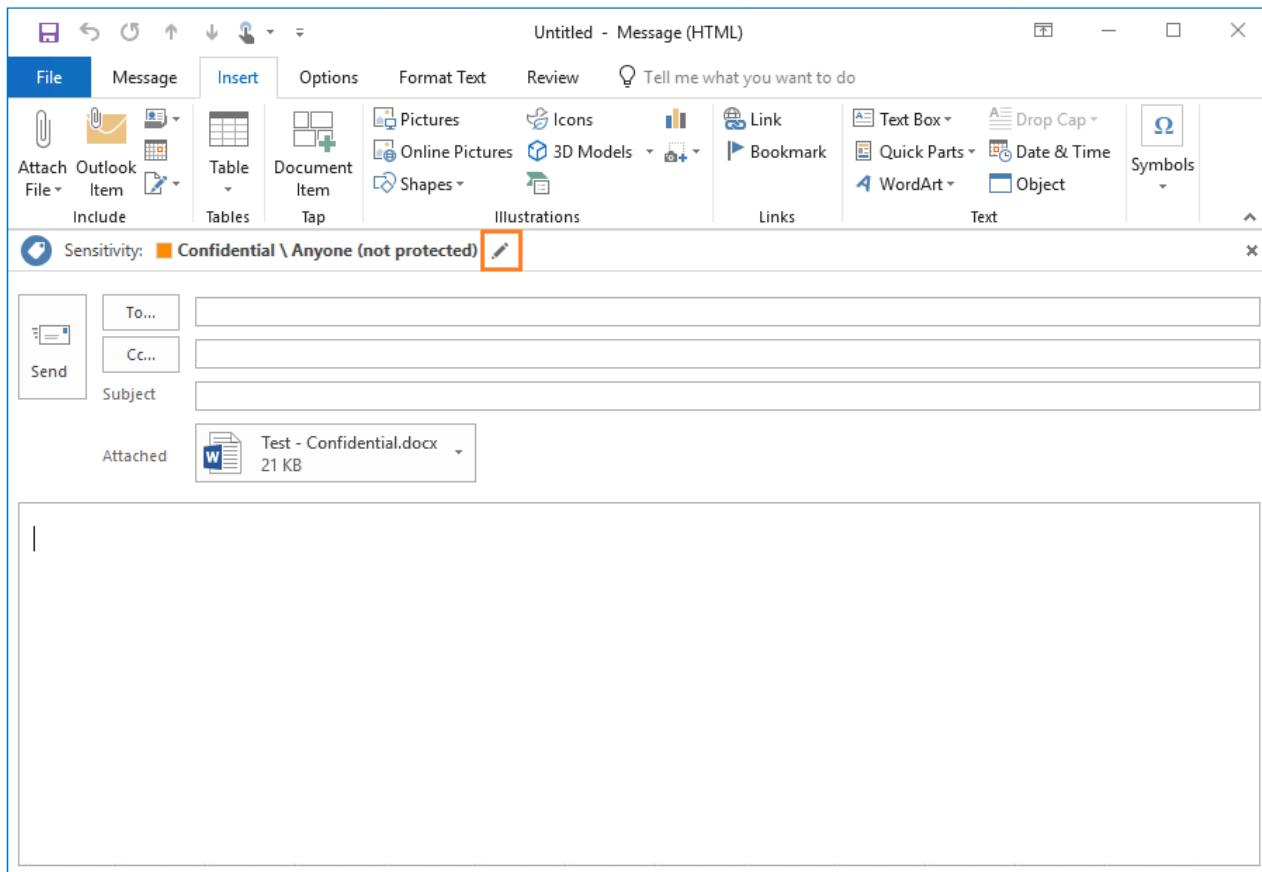
Start Outlook and create a new email message. Just as we saw with Word, the new email message is automatically labeled as **General** and the Information Protection bar is displayed.

Add the Word document you just labeled as an attachment to the email message. You see a prompt to change the email label to the **Confidential** label that matches the Word attachment. You can accept the recommendation or dismiss it:



If you click **Dismiss**, the new label is not applied but you see how the email is still labeled with the default label that we configured, **General**. The available labels are still visible to select as an alternative.

If you select **Change now**, the email is relabeled to the **Confidential** sublabel. However, users can still change the label before sending the email, by selecting the **Edit Label** icon:



The Information Protection bar then displays again, for users to select an alternative label.

Because the label is selected before sending the email, there's no need to actually send the email to see how this policy setting works. You can close the email without sending or saving it.

However, you might want to try repeating this exercise but also attach another document that has a higher classification (a sublabel from the **Highly Confidential** label). Then, you'll see how the prompt changes to apply the higher classification label. If you test multiple attachments with sublabels that have same parent label, you must configure [an advanced client setting](#) to support their ordering in the Azure portal.

Clean up resources

Do the following if you don't want to keep the changes that you made in this tutorial:

1. Select **Classifications > Policies > Global** to open the **Policy: Global** pane.
2. Return the policy settings to their original values that you took a note of, and then select **Save**.

Restart your Word and Outlook apps to download these changes.

Next steps

For more information about editing the Azure Information Protection policy settings, see [How to configure the policy settings for Azure Information Protection](#).

The policy settings that we changed helped to ensure a base level of classification, as well as encourage users to select an appropriate label. The next step is to augment this strategy by inspecting the contents of documents and emails, and then recommending or automatically applying an appropriate label. You do this by configuring labels for conditions. To learn more, see [How to configure conditions for automatic and recommended classification for Azure Information Protection](#).

Tutorial: Configure Azure Information Protection to control oversharing of information using Outlook

7/20/2020 • 16 minutes to read • [Edit Online](#)

Applies to: [Azure Information Protection](#)

Instructions for: [Azure Information Protection client for Windows](#)

NOTE

To provide a unified and streamlined customer experience, **Azure Information Protection client (classic)** and **Label Management** in the Azure Portal are being **deprecated** as of **March 31, 2021**. This time-frame allows all current Azure Information Protection customers to transition to our unified labeling solution using the Microsoft Information Protection Unified Labeling platform. Learn more in the official [deprecation notice](#).

In this tutorial, you learn how to:

- Configure settings that implement warn, justify, or block popup messages in Outlook
- See your settings in action
- Review the logged user messages and actions in the Event Log

Email is one of the most common methods by which users inappropriately share information—whether it's in the email message itself or in attachments. You might use data loss prevention (DLP) solutions that can identify known sensitive information and help prevent it from leaving your organization boundaries. However, you can also use the Azure Information Protection client with some advanced client settings to help prevent oversharing and also educate your users with interactive messages that provide feedback in real time.

This tutorial steps you through a basic configuration that uses just one label to illustrate the warn, justify, and block messages that users can see and respond to.

You can finish this tutorial in about 15 minutes.

Prerequisites

To complete this tutorial, you need:

1. A subscription that includes Azure Information Protection Plan 2.

If you don't have a subscription that includes this plan, you can create a [free](#) account for your organization.

2. The Azure Information Protection pane is added to the Azure portal and you have at least one label published in the Azure Information Protection global policy.

Although this tutorial uses the default label, **General**, you can substitute this label for another one if you prefer. If you need help adding the Azure Information Protection pane, or don't yet have any labels published to the global policy, see [Quickstart: Add Azure Information Protection to the Azure portal and view the policy](#).

3. A computer running Windows (minimum of Windows 7 with Service Pack 1), and on this computer, you can sign in to Outlook. Be prepared to restart Outlook multiple times during this tutorial.
4. The Azure Information Protection client (classic) is installed on your Windows computer.

You can install the classic client by going to the [Microsoft download center](#) and download **AzInfoProtection.exe** from the Azure Information Protection page.

If you are using the unified labeling client instead of the classic client, see the following instructions that explain how to use PowerShell advanced settings for the equivalent configurations in this tutorial:

- Admin guide instructions: [Implement pop-up messages in Outlook that warn, justify, or block emails being sent](#)
- Video: [Azure Information Protection Outlook Popup Configuration](#)

For a full list of prerequisites to use Azure Information Protection, see [Requirements for Azure Information Protection](#).

Let's get started.

Identify a label ID for testing

For this tutorial, we'll use just one label to see the resulting behavior for users. You can use any label, but a good example for testing is the default label named **General**, which is typically suitable for business data that is not intended for public consumption, and does not apply protection.

To specify your chosen label, you must know its ID, which you identify from the Azure portal:

1. Open a new browser window and sign in to the [Azure portal](#) as a global admin. Then navigate to [Azure Information Protection](#).

For example, in the search box for resources, services, and docs: Start typing **Information** and select **Azure Information Protection**.

If you are not the global admin, use the following link for alternative roles: [Signing in to the Azure portal](#)

2. Select **Classifications > Labels** and then select the **General** label to open the **Label: General** pane.
3. Locate the label ID at the bottom of the pane:

The screenshot shows the 'Label: General' configuration page. At the top, there are buttons for Save, Discard, and Delete this label. Below that, two toggle switches are shown: 'Documents with this label have a footer' (set to On) and 'Documents with this label have a watermark' (set to Off). A section titled 'Configure conditions for automatically applying this label' follows, with a note that if any conditions are met, the label is applied. It lists a single condition: 'no condition set'. There is a '+ Add a new condition' link. Below this is a section for 'Add notes for administrator use' with a text input field. At the bottom, the 'Label ID' is displayed as 'Label ID - 0e421e6d-ea17-4fdb-8f01-93a3e71333b8', which is highlighted with an orange border.

4. Copy and paste the label ID value into a temporary file so that this value can be easily copied for a later step.
In our example, this label ID value is **0e421e6d-ea17-4fdb-8f01-93a3e71333b8**.
5. Close the **Label: General** pane, but do not close the Azure portal.

Create a scoped policy to test the new advanced client settings

We'll create a new scoped policy so that the new advanced client settings will apply to just you, for testing.

1. On the **Azure Information Protection - Policies** pane, select **Add a new policy**. You then see the **Policy** pane that displays labels and settings from your existing global policy.
2. Specify the policy name of **Oversharing tutorial** and optionally, a description of **Advanced client settings to control oversharing using Outlook**.
3. Select **Specify which users/groups get this policy**, and using the subsequent panes, specify your own user account.
4. With your account name now displayed on the **Policy** pane, select **Save** without making additional changes to the labels or settings on this pane. You might be prompted to confirm your choice.

This scoped policy is now ready to add advanced client settings. Close the **Policy: Oversharing tutorial** pane, but do not close the Azure portal.

Configure and test advanced client settings to warn, prompt for justification, or block emails that have the General label

For this step of the tutorial, we'll specify the following advanced client settings, and test each in turn:

- **OutlookWarnUntrustedCollaborationLabel**
- **OutlookJustifyUntrustedCollaborationLabel**

- **OutlookBlockUntrustedCollaborationLabel**

Create the advanced client setting to warn users if an email or attachment has the General label

Using the newly created scoped policy, we'll add a new advanced client setting named

OutlookWarnUntrustedCollaborationLabel with the ID of your **General** label:

1. Back on the **Azure Information Protection - Policies** pane, select the context menu (...) next to **Oversharing tutorial**. Then select **Advanced settings**.
2. On the **Advanced settings** pane, type the advanced setting name, **OutlookWarnUntrustedCollaborationLabel**, and paste your own label ID for the value. Using our example label ID:

NAME	VALUE	...
OutlookWarnUntrustedCollaborationLabel	0e421e6d-ea17-4fdb-8f01-93a3e71333b8	...
DisableDNF	true	...
EnableAudit	true	...
EnableCustomPermissions	false	...
HideBarByDefault	true	...

3. Select **Save and close**.

Do not close the **Policies** pane, or the Azure portal.

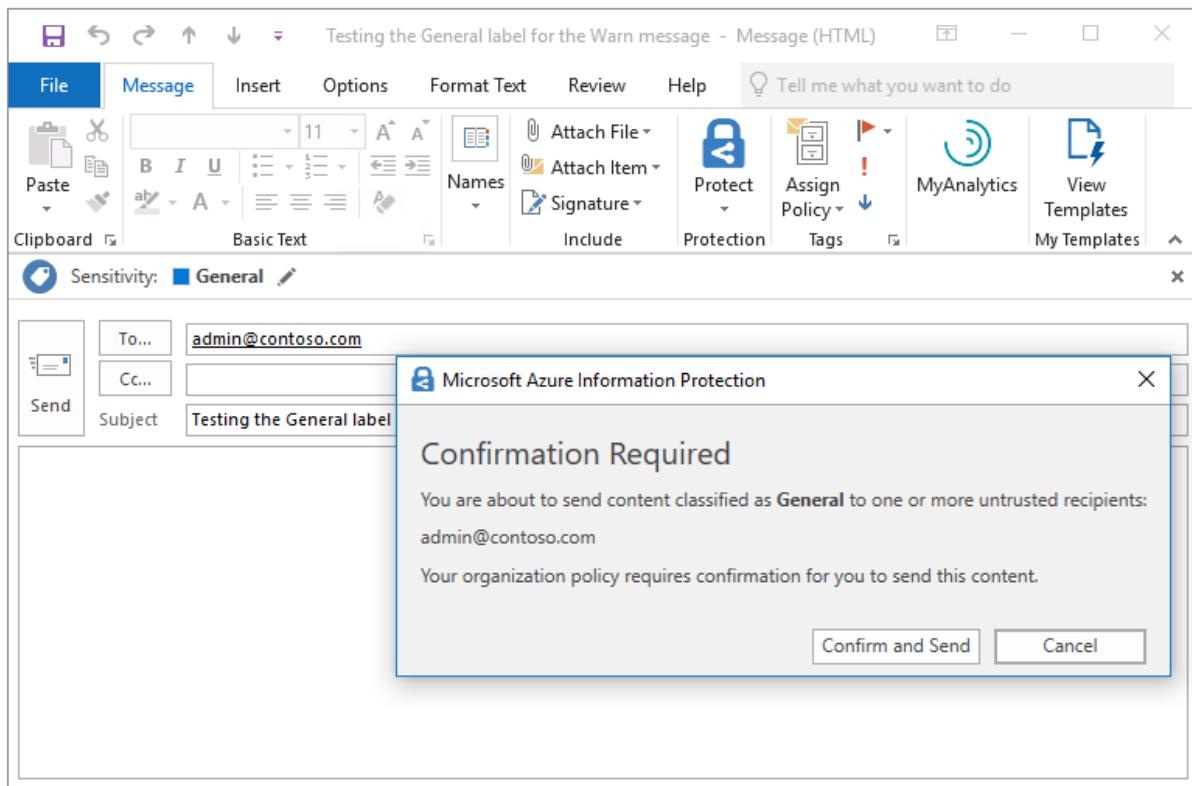
Test the advanced client setting to warn users if an email or attachment has the General label

On your client computer, we'll now see the results of configuring this advanced client setting.

1. On your client computer, open Outlook.

If Outlook is already open, restart it. The restart is needed to download the change we just made.

2. Create a new email message, and apply the **General** label. For example, from the **File** tab, select the **Protect** button, and then select **General**.
3. Specify your own email address for the **To** field, and for the subject, type **Testing the General label for the Warn message**. Then send the email.
4. As a result of the advanced client setting, you see the following warning, asking you to confirm before sending the email. For example:



5. As if you are a user who has mistakenly tried to email something that was labeled **General**, select **Cancel**. You see that the email is not sent but the email message remains so you can make changes, such as change the content or the label.
6. Without making any changes, select **Send** again. This time, as if you are a user who acknowledges that the content is appropriate for sending, select **Confirm and Send**. The email is sent.

Change the advanced client setting to prompt users to justify if an email has the General label

We'll edit the existing advanced client setting to keep your **General** label ID, but change the name to **OutlookJustifyUntrustedCollaborationLabel**:

1. On the **Azure Information Protection - Policies** pane, select the context menu (...) next to **Oversharing tutorial**. Then select **Advanced settings**.
2. On the **Advanced settings** pane, replace the previous advanced setting name you created, **OutlookWarnUntrustedCollaborationLabel**, with the new name of **OutlookJustifyUntrustedCollaborationLabel**:

Advanced settings □ X

Configure advanced client settings for this policy

NAME	VALUE
DisableDNF	true
EnableAudit	true
EnableCustomPermissions	false
HideBarByDefault	true
OutlookJustifyUntrustedCollaborationLabel	0e421e6d-ea17-4fdb-8f01-93a3e71333b8

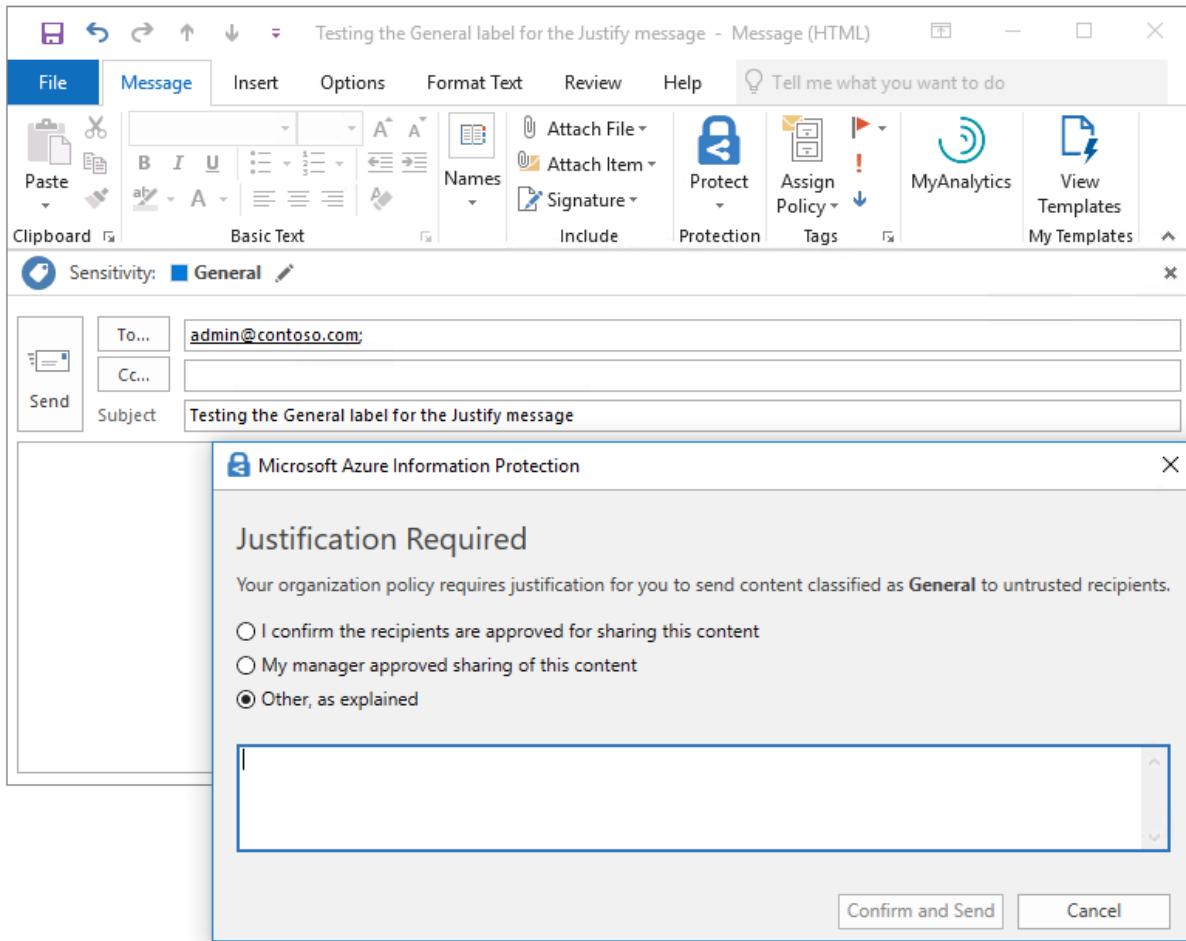
3. Select **Save and close**.

Do not close the Policies pane, or the Azure portal.

Test the advanced client setting to prompt users to justify if an email has the General label

On your client computer, we'll now see the results of this new advanced client setting.

1. On your client computer, restart Outlook to download the change we just made.
2. Create a new email message, and as before, apply the **General** label. For example, from the **File** tab, select the **Protect** button, and then select **General**.
3. Specify your own email address for the **To** field, and for the subject, type **Testing the General label for the Justify message**. Then send the email.
4. This time, you see the following message, asking you to provide justification before sending the email. For example:



5. As if you are a user who has mistakenly tried to email something that was labeled as **General**, select **Cancel**. You see that the email is not sent but the email message itself remains so you can make changes, such as change the content or the label.
6. Without making any changes, select **Send** again. This time, select one of the justification options, such as **I confirm the recipients are approved for sharing this content**, and then select **Confirm and Send**. The email is sent.

Change the advanced client setting to block users from sending an email that has the General label

We'll edit the existing advanced client setting one more time, to keep your **General** label ID, but change the name to **OutlookBlockUntrustedCollaborationLabel**:

1. In the Azure portal, on the **Azure Information Protection - Policies** pane, select the context menu (...) next to **Oversharing tutorial**. Then select **Advanced settings**.

2. On the **Advanced settings** pane, replace the previous advanced setting name you created, **OutlookJustifyUntrustedCollaborationLabel**, with the new name of **OutlookBlockUntrustedCollaborationLabel**:

NAME	VALUE	...
DisableDNF	true	...
EnableAudit	true	...
EnableCustomPermissions	false	...
HideBarByDefault	true	...
OutlookBlockUntrustedCollaborationLabel	0e421e6d-ea17-4fdb-8f01-93a3e71333b8	...

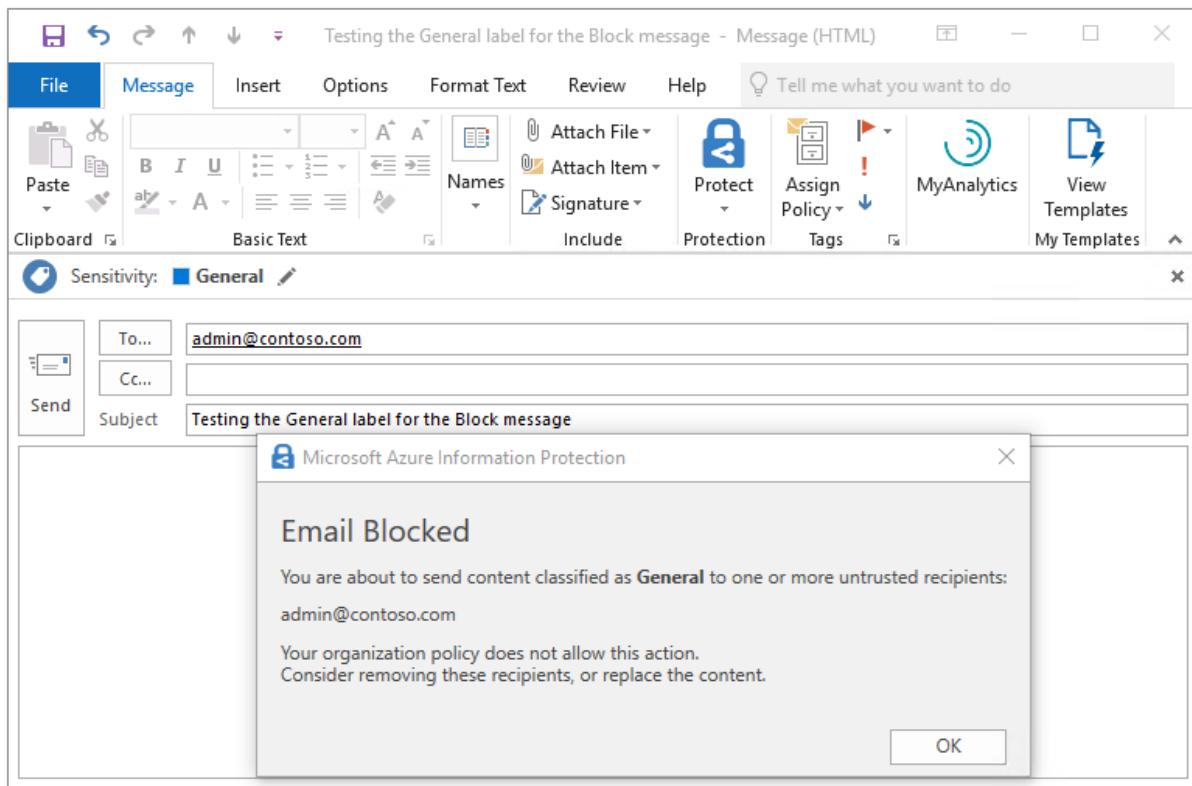
3. Select **Save and close**.

Do not close the **Policies** pane, or the Azure portal.

Test the advanced client setting to block users from sending an email that has the General label

On your client computer, we'll now see the results of this new advanced client setting.

1. On your client computer, restart Outlook to download the change we just made.
2. Create a new email message, and as before, apply the **General** label. For example, from the **File** tab, select the **Protect** button, and then select **General**.
3. Specify your own email address for the **To** field, and for the subject, type **Testing the General label for the Block message**. Then send the email.
4. This time, you see the following message that prevents the email from being sent. For example:



5. Acting as your user, you see the only option available is **OK**, which takes you back to the email message where you can make changes. Select **OK**, and cancel this email message.

Use Event Log to identify the messages and user actions for the General label

Before we move on to the next scenario for when an email or attachment doesn't have a label, start Event Viewer and navigate to Applications and Services Logs > Azure Information Protection.

For each of the tests that you did, information events are created to record both the message and the user response:

- Warn messages: Information ID 301
- Justify messages: Information ID 302
- Block messages: Information ID 303

For example, the first test was to warn the user, and you selected **Cancel**, so the **User Response** displays **Dismissed** in the first Event 301. For example:

```

Client Version: 1.53.10.0
Client Policy ID: e5287fe6-f82c-447e-bf44-6fa8ff146ef4
Item Full Path: Testing the General label for the Warn message.msg
Item Name: Testing the General label for the Warn message
Process Name: OUTLOOK
Action: Warn
Label After Action: General
Label ID After Action: 0e421e6d-ea17-4fdb-8f01-93a3e71333b8
Action Source:
User Response: Dismissed

```

However, you then selected **Confirm and Send**, which is reflected in the next Event 301, where the **User Response** displays **Confirmed**:

```
Client Version: 1.53.10.0
Client Policy ID: e5287fe6-f82c-447e-bf44-6fa8ff146ef4
Item Full Path: Testing the General label for the Warn message.msg
Item Name: Testing the General label for the Warn message
Process Name: OUTLOOK
Action: Warn
Label After Action: General
Label ID After Action: 0e421e6d-ea17-4fdb-8f01-93a3e71333b8
Action Source:
User Response: Confirmed
```

The same pattern is repeated for the justify message, which has an Event 302. The first event has a **User Response** of **Dismissed**, and the second shows the justification that was selected. For example:

```
Client Version: 1.53.10.0
Client Policy ID: e5287fe6-f82c-447e-bf44-6fa8ff146ef4
Item Full Path: Testing the General label for the Justify message.msg
Item Name: Testing the General label for the Justify message
Process Name: OUTLOOK
Action: Justify
Label After Action: General
Label ID After Action: 0e421e6d-ea17-4fdb-8f01-93a3e71333b8
User Justification: I confirm the recipients are approved for sharing this content
Action Source:
User Response: Confirmed
```

At the top of the event log, you see the block message logged, which has an Event 303. For example:

```
Client Version: 1.53.10.0
Client Policy ID: e5287fe6-f82c-447e-bf44-6fa8ff146ef4
Item Full Path: Testing the General label for the Block message.msg
Item Name: Testing the General label for the Block message
Process Name: OUTLOOK
Action: Block
Label After Action: General
Label ID After Action: 0e421e6d-ea17-4fdb-8f01-93a3e71333b8
Action Source:
```

Optional: Create an additional advanced client setting to exempt these messages for internal recipients

You tested your warn, justify, and block messages by using your own email address as the recipient. In a production environment, you might choose to display these messages for your specified labels only if recipients are external to your organization. You might extend that exemption to partners that your organization regularly works with.

To illustrate how this works, we'll create an additional advanced client setting named **OutlookBlockTrustedDomains** and specify your own domain name from your email address. This will prevent the block message you saw previously from displaying for recipients that share your domain name in their email address, but will still be shown for other recipients. You can similarly create additional advanced client settings for **OutlookWarnTrustedDomains** and **OutlookJustifyTrustedDomains**.

1. In the Azure portal, on the **Azure Information Protection - Policies** pane, select the context menu (...) next to **Oversharing tutorial**. Then select **Advanced settings**.
2. On the **Advanced settings** pane, type the advanced setting name, **OutlookBlockTrustedDomains**, and paste your domain name from your email address for the value. For example:

Advanced settings

Configure advanced client settings for this policy



NAME	VALUE	...
OutlookBlockTrustedDomains	contoso.com	...
DisableDNF	true	...
EnableAudit	true	...
EnableCustomPermissions	false	...
HideBarByDefault	true	...
OutlookJustifyUntrustedCollaborationLabel	0e421e6d-ea17-4fdb-8f01-93a3e71333b8	...
OutlookUnlabeledCollaborationAction	Block	...

3. Select **Save and close**. Do not close the **Policies** pane, or the Azure portal.
4. Now repeat the [previous test to block users from sending an email that has the General label](#), and you no longer see the block message when you use your own email address. The email is sent without interruption.

To confirm that the block message is still shown for external recipients, repeat the test one more time but specify a recipient from outside your organization. This time, you see the block message again, listing the new recipient address as untrusted.

Configure and test an advanced client setting to warn, prompt for justification, or block emails that don't have a label

For this step of the tutorial, we'll specify a new advanced client setting with different values, and test each in turn:

- **OutlookUnlabeledCollaborationAction**

Create the advanced client setting to warn users if an email doesn't have a label

This new advanced client setting named **OutlookUnlabeledCollaborationAction** doesn't need a label ID but specifies the action to take for unlabeled content:

1. In the Azure portal, back on the **Azure Information Protection - Policies** pane, select the context menu (...) next to **Oversharing tutorial**. Then select **Advanced settings**.
2. On the **Advanced settings** pane, type the advanced setting name, **OutlookUnlabeledCollaborationAction**, and for the value, specify **Warn**:

Advanced settings

Configure advanced client settings for this policy

NAME	VALUE	...
OutlookUnlabeledCollaborationAction	Warn	...
DisableDNF	true	...
EnableAudit	true	...
EnableCustomPermissions	false	...
HideBarByDefault	true	...
OutlookBlockUntrustedCollaborationLabel	0e421e6d-ea17-4fdb-8f01-93a3e71333b8	...

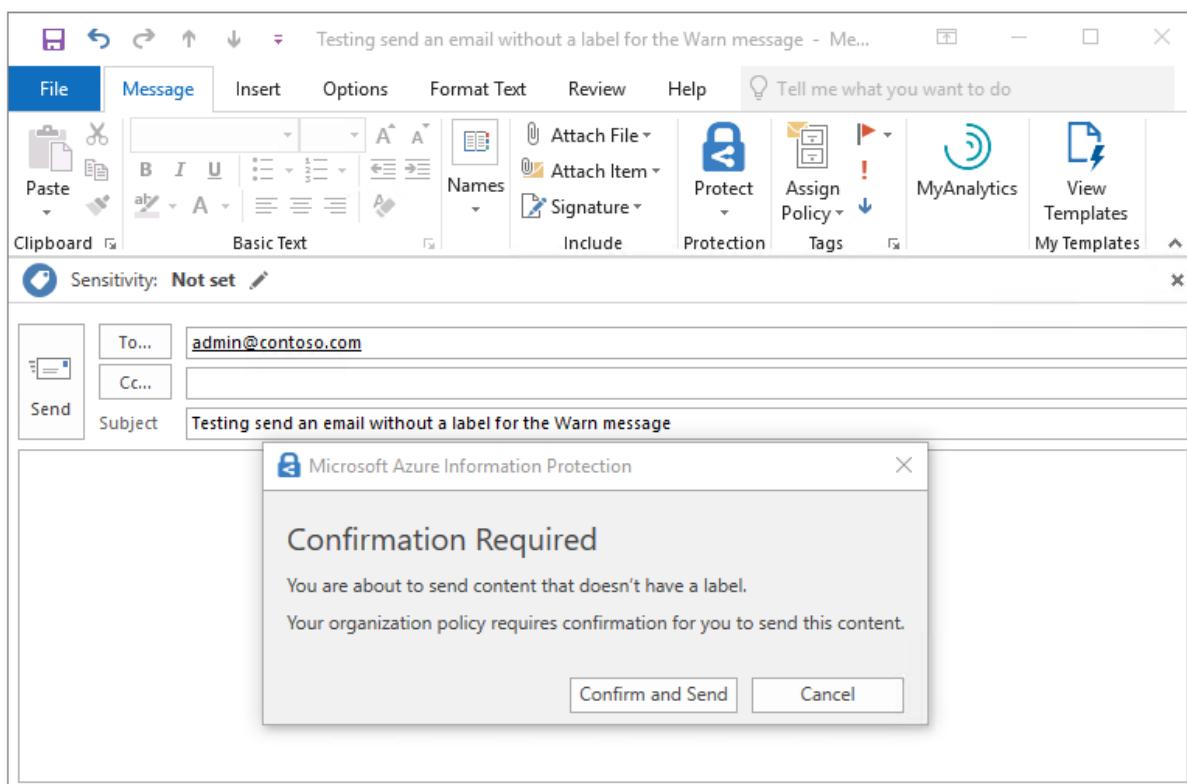
3. Select **Save and close**.

Do not close the Policies pane, or the Azure portal.

Test the advanced client setting to warn users if an email doesn't have a label

On your client computer, we'll now see the results of configuring this new advanced client setting for when content doesn't have a label:

1. On your client computer, restart Outlook to download the change we just made.
2. Create a new email message, and this time, do not apply a label.
3. Specify your own email address for the To field, and for the subject, type **Testing send an email without a label for the Warn message**. Then send the email.
4. This time, you see a **Confirmation Required** message that you can **Confirm and Send** or **Cancel**:



5. Select **Confirm and Send**.

Change the advanced client setting to prompt users to justify if an email is unlabeled

We'll edit the existing advanced client setting to keep the name of **OutlookUnlabeledCollaborationAction**, but change the value to **Justify**:

1. On the **Azure Information Protection - Policies** pane, select the context menu (...) next to **Oversharing tutorial**. Then select **Advanced settings**.
2. On the **Advanced settings** pane, locate the **OutlookUnlabeledCollaborationAction** setting and replace the previous value of **Warn** with new value **Justify**:

The screenshot shows the 'Advanced settings' pane with the following table:

NAME	VALUE	...
DisableDNF	true	...
EnableAudit	true	...
EnableCustomPermissions	false	...
HideBarByDefault	true	...
OutlookJustifyUntrustedCollaborationLabel	0e421e6d-ea17-4fdb-8f01-93a3e71333b8	...
OutlookUnlabeledCollaborationAction	Justify	...

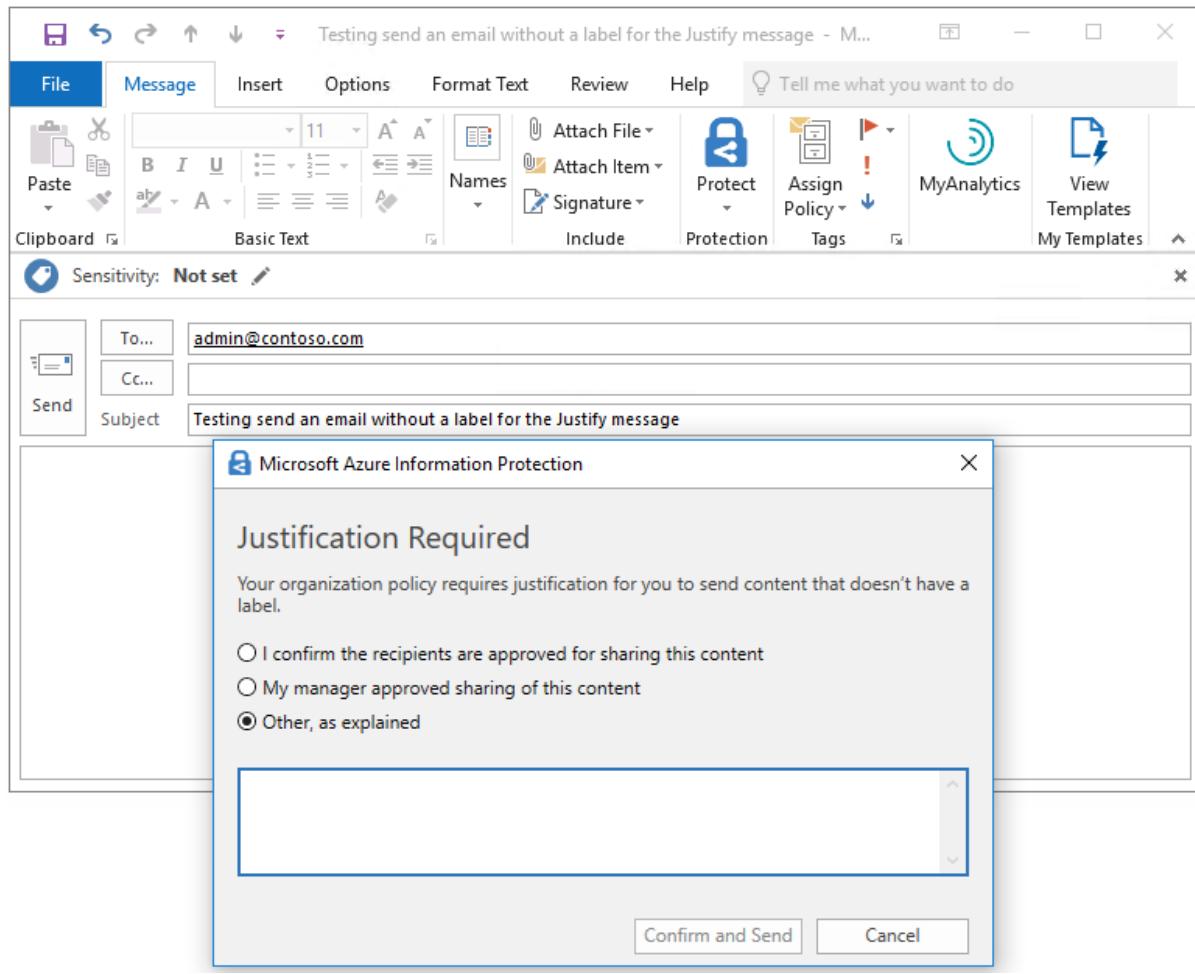
3. Select **Save and close**.

Do not close the **Policies** pane, or the Azure portal.

Test the advanced client setting to prompt users to justify if an email isn't labeled

On your client computer, we'll now see the results of changing the value for this advanced client setting.

1. On your client computer, restart Outlook to download the change we just made.
2. Create a new email message, and as before, do not apply a label.
3. Specify your own email address for the **To** field, and for the subject, type **Testing send an email without a label for the Justify message**. Then send the email.
4. This time, you see a **Justification Required** message with different options:



5. Select an option, such as **My manager approved sharing of this content**. Then select **Confirm and Send**.

Change the advanced client setting to block users from sending an email that isn't labeled

As before, we'll edit the existing advanced client setting to keep the name of **OutlookUnlabeledCollaborationAction**, but change the value to **Block**:

1. On the **Azure Information Protection - Policies** pane, select the context menu (...) next to **Oversharing tutorial**. Then select **Advanced settings**.
2. On the **Advanced settings** pane, locate the **OutlookUnlabeledCollaborationAction** setting and replace the previous value of **Justify** with the new value of **Block**:

Advanced settings	
Configure advanced client settings for this policy	
NAME	VALUE
DisableDNF	true
EnableAudit	true
EnableCustomPermissions	false
HideBarByDefault	true
OutlookJustifyUntrustedCollaborationLabel	0e421e6d-ea17-4fdb-8f01-93a3e71333b8
OutlookUnlabeledCollaborationAction	Block

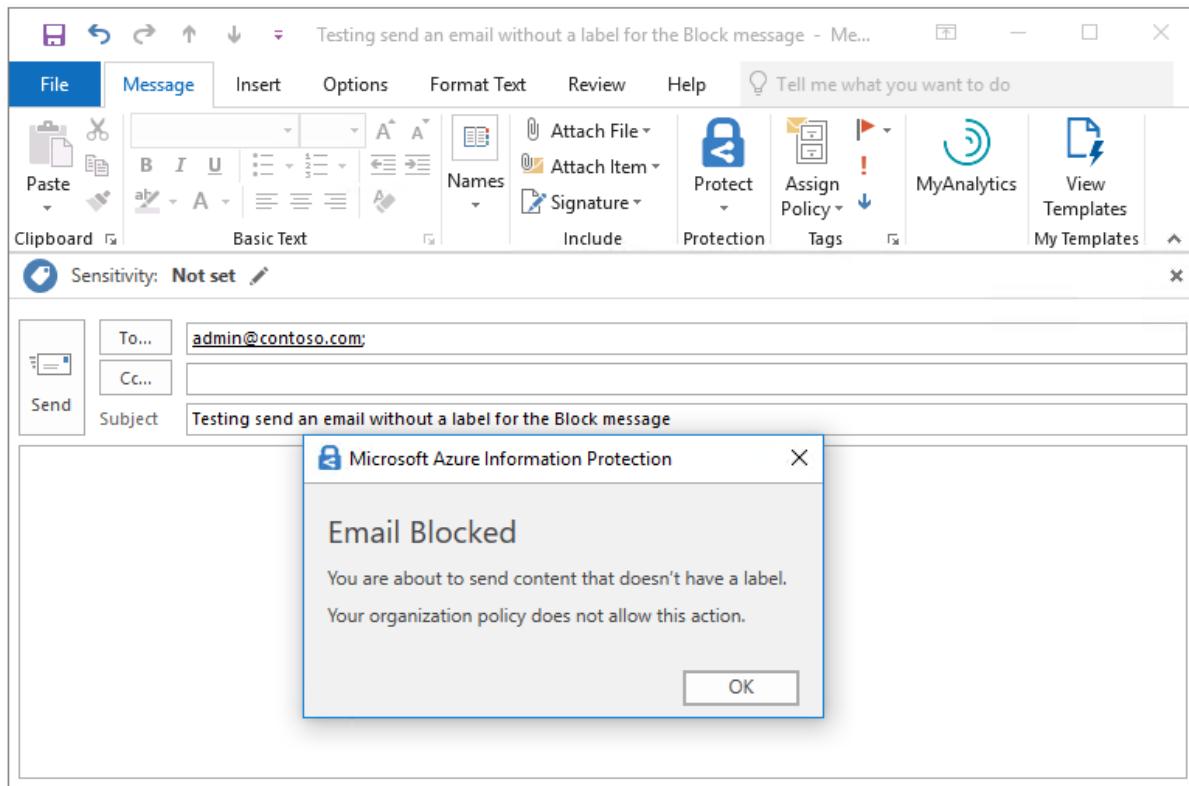
3. Select **Save and close**.

Do not close the Policies pane, or the Azure portal.

Test the advanced client setting to block users from sending an email that isn't labeled

On your client computer, we'll now see the results of changing the value of this advanced client setting.

1. On your client computer, restart Outlook to download the change we just made.
2. Create a new email message, and as before, do not apply a label.
3. Specify your own email address for the To field, and for the subject, type **Testing send an email without a label for the Block message**. Then send the email.
4. This time, you see the following message that prevents the email from being sent, with an explanation for the user. For example:



5. Acting as your user, you see the only option available is **OK**, which takes you back to the email message where you can select a label.

Select **OK**, and cancel this email message.

Use Event Log to identify the messages and user actions for the unlabeled email

As before, the messages and user responses are logged in Event Viewer, **Applications and Services Logs > Azure Information Protection**, with the same event IDs.

- Warn messages: Information ID 301
- Justify messages: Information ID 302
- Block messages: Information ID 303

For example, the results of our justification prompt when the email didn't have a label:

```
Client Version: 1.53.10.0
Client Policy ID: e5287fe6-f82c-447e-bf44-6fa8ff146ef4
Item Full Path: Testing send an email without a label for the Justify message.msg
Item Name: Testing send an email without a label for the Justify message
Process Name: OUTLOOK
Action: Justify
User Justification: My manager approved sharing of this content
Action Source:
User Response: Confirmed
```

Clean up resources

Do the following if you don't want to keep the changes that you made in this tutorial:

1. In the Azure portal, on the **Azure Information Protection - Policies** pane, select the context menu (...) next to **Oversharing tutorial**. Then select **Delete policy**.
2. If you are prompted to confirm, select **OK**.

Restart Outlook so it's no longer configured for the settings we configured for this tutorial.

Next steps

For quicker testing, this tutorial used an email message to a single recipient, and without attachments. But you can apply the same method with multiple recipients, multiple labels, and also apply the same logic to email attachments whose labeling status is often less obvious to users. For example, the email message itself is labeled Public but the PowerPoint presentation attached is labeled General. For more information about the configuration options, see the following section from the admin guide: [Implement pop-up messages in Outlook that warn, justify, or block emails being sent](#)

The admin guide also contains information about other advanced client settings that you can use to customize the behavior of the client. For a full list, see [Available advanced client settings](#).

Overview of the Azure Information Protection policy

7/20/2020 • 2 minutes to read • [Edit Online](#)

Applies to: [Azure Information Protection](#)

Instructions for: [Azure Information Protection client for Windows](#)

NOTE

The Azure Information Protection policy applies to the Azure Information Protection client (classic) and not the Azure Information Protection unified labeling client. Not sure of the difference between these clients? See this [FAQ](#).

If you are looking for information about sensitivity labels, see the Microsoft 365 Compliance documentation. For example, [Learn about sensitivity labels](#).

An Azure Information Protection policy contains the following elements that you can configure:

- Which labels are included that let administrators and users classify (and optionally, protect) documents and emails.
- Title and tooltip for the Information Protection bar that users see in their Office applications.
- The option to set a default label as a starting point for classifying documents and emails.
- The option to enforce classification when users save documents and send emails.
- The option to prompt users to provide a reason when they select a label that has a lower sensitivity level than the original.
- The option to automatically label an email message, based on its attachments.
- The option to control whether the Information Protection bar is displayed in Office applications.
- The option to control whether the Do Not Forward button is displayed in Outlook.
- The option to let users specify their own permissions for documents.
- The option to provide a custom help link for users.

Azure Information Protection comes with a [default policy](#), which contains five main labels. Two of these labels contain sublabels to provide subcategories, when needed.

When a label is configured for sublabels, users cannot select the main label but must select one of the sublabels. In this scenario, the main label is supported as a display container only for the name and color.

The Azure Information Protection labels can be used with the full range of data that an organization typically creates and stores, from the lowest classification of personal data, to the highest classification of highly confidential data.

You can use the default labels without changes, or you can customize them, or you can delete them, and you can create new labels. For full instructions, see [Configuring the Azure Information Protection policy](#).

Next steps

For examples of how to customize the Azure Information Protection policy, and see the resulting behavior for users,

try the following tutorials:

- [Edit the Azure Information Protection policy and create a new label and create a new label](#)
- [Configure Azure Information Protection policy settings that work together](#)

What is Azure Rights Management?

7/20/2020 • 7 minutes to read • [Edit Online](#)

Applies to: [Azure Information Protection](#), [Office 365](#)

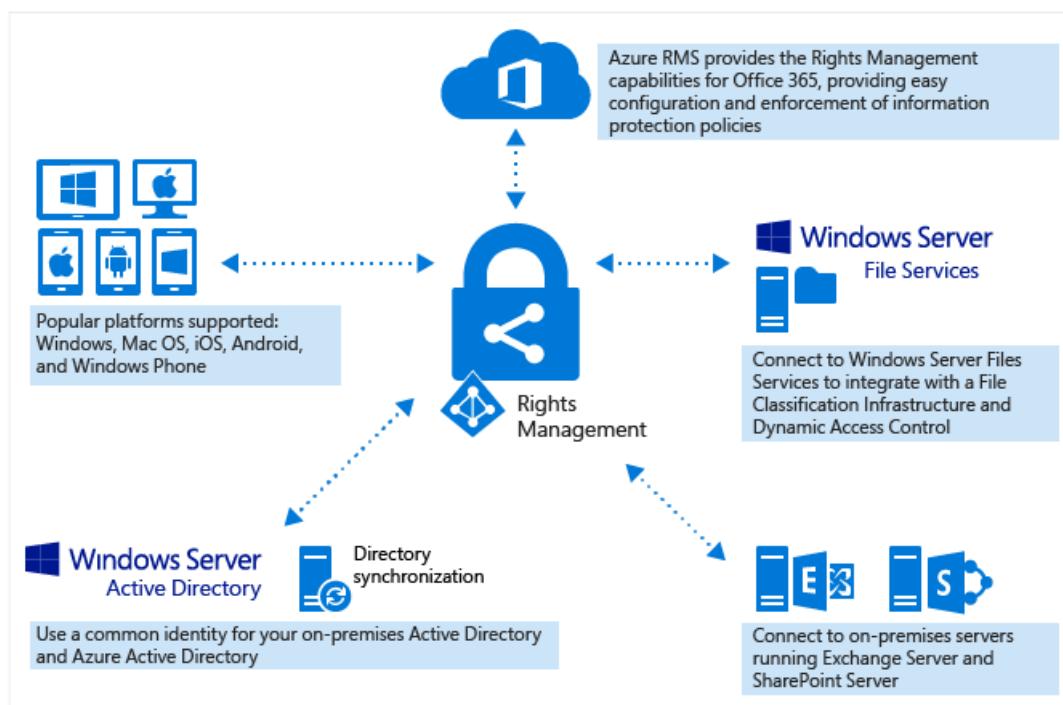
Azure Rights Management (often abbreviated to Azure RMS) is the protection technology used by [Azure Information Protection](#).

This cloud-based protection service uses encryption, identity, and authorization policies to help secure your files and email, and it works across multiple devices—phones, tablets, and PCs. Information can be protected both within your organization and outside your organization because that protection remains with the data, even when it leaves your organization's boundaries.

As an example, employees might email a document to a partner company, or save a document to their cloud drive. The persistent protection that Azure RMS provides not only helps to secure your company data, but might also be legally mandated for compliance, legal discovery requirements, or simply for good information management practices.

But importantly, authorized people and services (such as search and indexing) can continue to read and inspect the protected data. This capability is not easily accomplished with other information protection solutions that use peer-to-peer encryption. You might have heard this capability referred to as "reasoning over data" and it is a crucial element in maintaining control of your organization's data.

The following picture shows how this service offers a protection solution for Office 365, as well as for on-premises servers and services. You also see that protection is supported by the popular end-user devices that run Windows, macOS, iOS, and Android.



You can use this protection with Office 365 subscriptions as well as with subscriptions for Azure Information Protection. You can find more information about the available subscriptions and which features they support on the [Azure Information Protection](#) site.

Business problems solved by Azure Rights Management

Use the following table to identify business requirements or problems that your organization might have for protecting documents and emails, and how the Azure Rights Management technology can address these.

Requirement or Problem	Solved by Azure RMS
Protect multiple file types	Ã¢ In early implementations of Rights Management, only Office files could be protected, using native Rights Management protection. Now, generic protection that was first offered by the Rights Management sharing application and now by the Azure Information Protection client means that more file types are supported.
Protect files anywhere	Ã¢ When a file is protected , the protection stays with the file, even if it is saved or copied to storage that is not under the control of IT, such as a cloud storage service.
Safely share information	Ã¢ When a file is protected , it is safe to share with others. For example, an attachment to an email or a link to a SharePoint site. If the sensitive information is within an email message, you can protect the email or simply use the Do Not Forward option from Outlook. The benefit of attaching a protected file rather than protecting the whole email message is that the email text is not encrypted, so you can include instructions for first-time use if the email is being sent outside your organization. Anybody can read the instructions but because the attached document is protected, only authorized users will be able to open the document, even if the email or document is forwarded to other people.
Auditing and monitoring	Ã¢ You can audit and monitor usage of your protected files, even after these files leave your organization's boundaries. For example, you work for Contoso, Ltd. You are working on a joint project with three people from Fabrikam, Inc. You email these three people a document that you protect and restrict to read-only. Azure Rights Management auditing can provide the following information: <ul style="list-style-type: none">- Whether the people you specified in Fabrikam opened the document, and when.- Whether other people that you didn't specify attempted (and failed) to open the document—perhaps because it was forwarded or saved to a shared location that others could access.- Whether any of the specified people tried (and failed) to print or change the document. In addition, the document tracking site lets users and administrators track, and if necessary, revoke access to protected documents.

Requirement or Problem	Solved by Azure RMS
Support for commonly used devices, not just Windows computers	<p>Ã Supported devices include:</p> <ul style="list-style-type: none"> - Windows computers and phones - Mac computers - iOS tablets and phones - Android tablets and phones
Support for business-to-business collaboration	<p>Ã Because Azure Rights Management is a cloud service, there's no need to explicitly configure trusts with other organizations before you can share protected content with them. If they already have an Office 365 or an Azure AD directory, collaboration across organizations is automatically supported. If they do not, users can sign up for the free RMS for individuals subscription, or use a Microsoft account for applications that support this authentication for Azure Information Protection.</p>
Support for on-premises services, as well as Office 365	<p>Ã In addition to working seamlessly with Office 365, you can also use Azure Rights Management with the following on-premises services when you deploy the RMS connector:</p> <ul style="list-style-type: none"> - Exchange Server - SharePoint Server - Windows Server running File Classification Infrastructure
Easy activation	<p>Ã For new subscriptions, activation is automatic. For existing subscriptions, activating the Rights Management service requires just a couple of clicks in your management portal. Or, if you prefer command-line control, just two PowerShell commands.</p>
Ability to scale across your organization, as needed	<p>Ã Because Azure Rights Management runs as a cloud service with the Azure elasticity to scale up and out, you don't have to provision or deploy additional on-premises servers.</p>
Ability to create simple and flexible policies	<p>Ã Customized protection templates provide a quick and easy solution for administrators to apply policies, and for users to apply the correct level of protection for each document and restrict access to people inside your organization.</p> <p>For example, for a company-wide strategy paper to be shared with all employees, you could apply a read-only policy to all internal employees. Then, for a more sensitive document, such as a financial report, you could restrict access to executives only.</p>

Requirement or problem	Solved by Azure RMS
Broad application support	<ul style="list-style-type: none"> Ã Azure Rights Management has tight integration with Microsoft Office applications and services, and extends support for other applications by using the Azure Information Protection client. Ã The Azure Information Protection SDKs provide your internal developers and software vendors with APIs to write custom applications that support Azure Information Protection. <p>For more information, see Other applications that support the Rights Management APIs.</p>
IT must maintain control of data	<ul style="list-style-type: none"> Ã Organizations can choose to manage their own tenant key and use the "Bring Your Own Key" (BYOK) solution and store their tenant key in Hardware Security Modules (HSMs). Ã Support for auditing and usage logging so that you can analyze for business insights, monitor for abuse, and (if you have an information leak) perform forensic analysis. Ã Delegated access by using the super user feature ensures that IT can always access protected content, even if a document was protected by an employee who then leaves the organization. In comparison, peer-to-peer encryption solutions risk losing access to company data. Ã Synchronize just the directory attributes that Azure RMS needs to support a common identity for your on-premises Active Directory accounts, by using a hybrid identity solution, such as Azure AD Connect. Ã Enable single-sign on without replicating passwords to the cloud, by using AD FS. Ã Organizations always have the choice to stop using the Azure Rights Management service without losing access to content that was previously protected by Azure Rights Management. For information about decommissioning options, see Decommissioning and deactivating Azure Rights Management. In addition, organizations who have deployed Active Directory Rights Management Services (AD RMS) can migrate to the Azure Rights Management service without losing access to data that was previously protected by AD RMS.

TIP

If you are familiar with the on-premises version of Rights Management, Active Directory Rights Management Services (AD RMS), you might be interested in the comparison table from [Comparing Azure Rights Management and AD RMS](#).

Security, compliance, and regulatory requirements

Azure Rights Management supports the following security, compliance, and regulatory requirements:

- Ã Use of industry-standard cryptography and supports FIPS 140-2. For more information, see the [Cryptographic controls used by Azure RMS: Algorithms and key lengths](#) information.

Ã Support for nCipher nShield hardware security module (HSM) to store your tenant key in Microsoft Azure data centers. Azure Rights Management uses separate security worlds for its data centers in North America, EMEA (Europe, Middle East and Africa), and Asia, so your keys can be used only in your region.

Ã Certified for the following:

- ISO/IEC 27001:2013 (./includes [ISO/IEC 27018](#))
- SOC 2 SSAE 16/ISAE 3402 attestations
- HIPAA BAA
- EU Model Clause
- FedRAMP as part of Azure Active Directory in Office 365 certification, issued FedRAMP Agency Authority to Operate by HHS
- PCI DSS Level 1

For more information about these external certifications, see the [Azure Trust Center](#).

Next steps

For more technical information about how the Azure Rights Management service works, see [How does Azure RMS work?](#)

How does Azure RMS work? Under the hood

7/20/2020 • 11 minutes to read • [Edit Online](#)

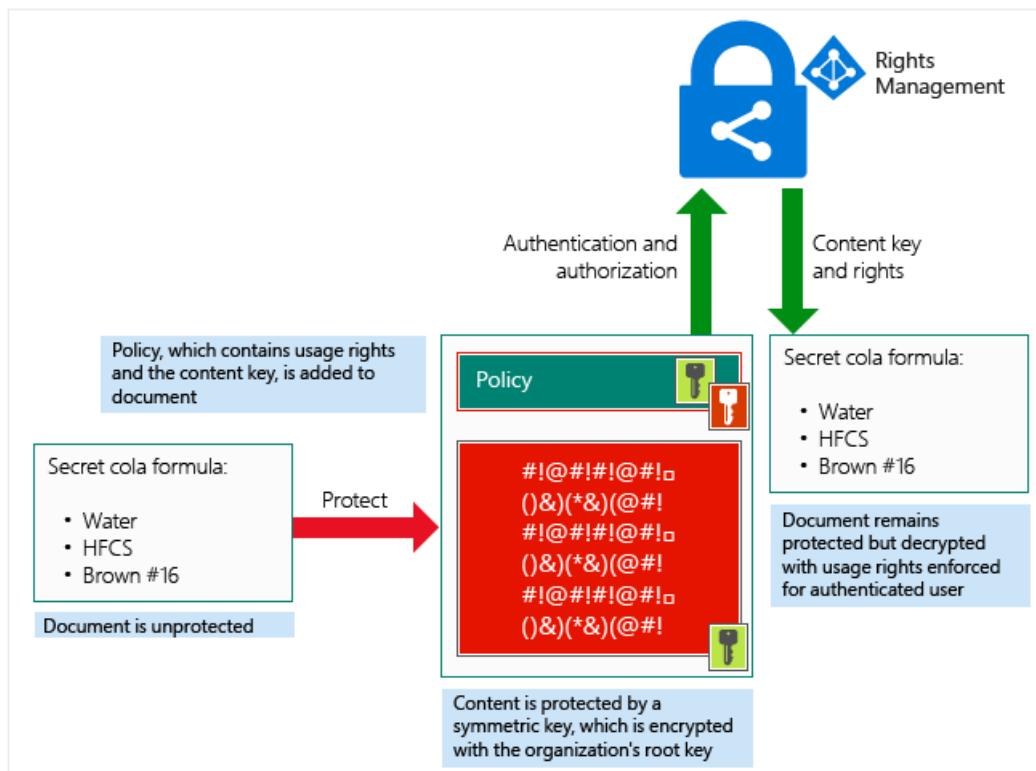
Applies to: [Azure Information Protection](#), [Office 365](#)

An important thing to understand about how Azure RMS works, is that this data protection service from Azure Information Protection, does not see or store your data as part of the protection process. Information that you protect is never sent to or stored in Azure, unless you explicitly store it in Azure or use another cloud service that stores it in Azure. Azure RMS simply makes the data in a document unreadable to anyone other than authorized users and services:

- The data is encrypted at the application level and includes a policy that defines the authorized use for that 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.

At a high level, you can see how this process works in the following picture. A document containing the secret formula is protected, and then successfully opened by an authorized user or service. The document is protected by a content key (the green key in this picture). It is unique for each document and is placed in the file header where it is protected by your Azure Information Protection tenant root key (the red key in this picture). Your tenant key can be generated and managed by Microsoft, or you can generate and manage your own tenant key.

Throughout the protection process when Azure RMS is encrypting and decrypting, authorizing, and enforcing restrictions, the secret formula is never sent to Azure.



For a detailed description of what's happening, see the [Walkthrough of how Azure RMS works: First use, content protection, content consumption](#) section in this article.

For technical details about the algorithms and key lengths that Azure RMS uses, see the next section.

Cryptographic controls used by Azure RMS: Algorithms and key lengths

Even if you don't need to know in detail how this technology works, you might be asked about the cryptographic controls that it uses. For example, to confirm that the security protection is industry-standard.

CRYPTOGRAPHIC CONTROLS	USE IN AZURE RMS
Algorithm: AES Key length: 128 bits and 256 bits [1]	Content protection
Algorithm: RSA Key length: 2048 bits [2]	Key protection
SHA-256	Certificate signing

Footnote 1

256 bits is used by the Azure Information Protection client in the following scenarios:

- Generic protection (.pfile).
- Native protection for PDF documents when the document has been protected with the ISO standard for PDF encryption, or the resulting protected document has a .ppdf file name extension.
- Native protection for text or image files (such as .ptxt or .pjjpg).

Footnote 2

2048 bits is the key length when the Azure Rights Management service is activated. 1024 bits is supported for the following optional scenarios:

- During a migration from on-premises if the AD RMS cluster is running in Cryptographic Mode 1.
- For archived keys that were created on-premises before the migration, so that content that was previously protected by AD RMS can continue to be opened by the Azure Rights Management service post migration.

How the Azure RMS cryptographic keys are stored and secured

For each document or email that is protected by Azure RMS, Azure RMS creates a single AES key (the "content key"), and that key is embedded to the document, and persists through editions of the document.

The content key is protected with the organization's RSA key (the "Azure Information Protection tenant key") as part of the policy in the document, and the policy is also signed by the author of the document. This tenant key is common to all documents and emails that are protected by the Azure Rights Management service for the organization and this key can only be changed by an Azure Information Protection administrator if the organization is using a tenant key that is customer-managed (known as "bring your own key", or BYOK).

This tenant key is protected in Microsoft's online services, in a highly controlled environment and under close monitoring. When you use a customer-managed tenant key (BYOK), this security is enhanced by the use of an array of high-end hardware security modules (HSMs) in each Azure region, without the ability for the keys to be extracted, exported, or shared under any circumstances. For more information about the tenant key and BYOK, see [Planning and implementing your Azure Information Protection tenant key](#).

Licenses and certificates that are sent to a Windows device are protected with the client's device private key, which is created the first time a user on the device uses Azure RMS. This private key, in turn, is protected with DPAPI on the client, which protects these secrets by using a key derived from the user's password. On mobile devices, the keys are used only one time, so because they are not stored on the clients, these keys don't need to be protected on the device.

Walkthrough of how Azure RMS works: First use, content protection, content consumption

To understand in more detail how Azure RMS works, let's walk through a typical flow after the [Azure Rights Management service is activated](#) and when a user first uses the Rights Management service on their Windows computer (a process sometimes known as **initializing the user environment** or bootstrapping), **protects content** (a document or email), and then **consumes** (opens and uses) content that has been protected by somebody else.

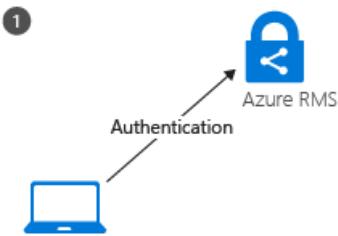
After the user environment is initialized, that user can then protect documents or consume protected documents on that computer.

NOTE

If this user moves to another Windows computer, or another user uses this same Windows computer, the initialization process is repeated.

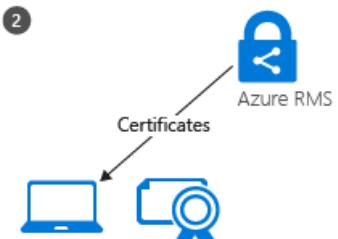
Initializing the user environment

Before a user can protect content or consume protected content on a Windows computer, the user environment must be prepared on the device. This is a one-time process and happens automatically without user intervention when a user tries to protect or consume protected content:



What's happening in step 1: The RMS client on the computer first connects to the Azure Rights Management service, and authenticates the user by using their Azure Active Directory account.

When the user's account is federated with Azure Active Directory, this authentication is automatic and the user is not prompted for credentials.



What's happening in step 2: After the user is authenticated, the connection is automatically redirected to the organization's Azure Information Protection tenant, which issues certificates that let the user authenticate to the Azure Rights Management service in order to consume protected content and to protect content offline.

One of these certificates is the rights account certificate, often abbreviated to RAC. This certificate authenticates the user to Azure Active Directory and is valid for 31 days. The certificate is automatically renewed by the RMS client, providing the user account is still in Azure Active Directory and the account is enabled. This certificate is not configurable by an administrator.

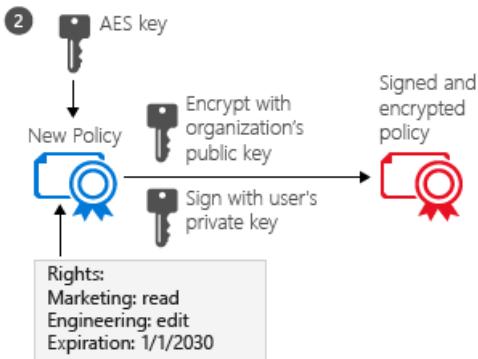
A copy of this certificate is stored in Azure so that if the user moves to another device, the certificates are created by using the same keys.

Content protection

When a user protects a document, the RMS client takes the following actions on an unprotected document:



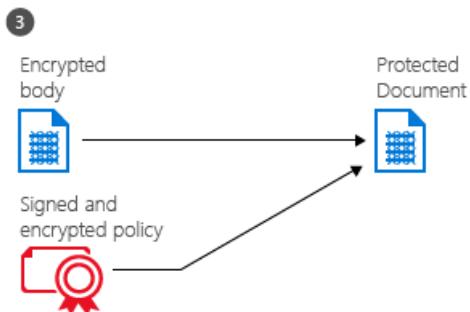
What's happening in step 1: The RMS client creates a random key (the content key) and encrypts the document using this key with the AES symmetric encryption algorithm.



What's happening in step 2: The RMS client then creates a certificate that includes a policy for the document that includes the [usage rights](#) for users or groups, and other restrictions, such as an expiration date. These settings can be defined in a template that an administrator previously configured, or specified at the time the content is protected (sometimes referred to as an "ad hoc policy").

The main Azure AD attribute used to identify the selected users and groups is the Azure AD ProxyAddresses attribute, which stores all the email addresses for a user or group. However, if a user account doesn't have any values in the AD ProxyAddresses attribute, the user's UserPrincipalName value is used instead.

The RMS client then uses the organization's key that was obtained when the user environment was initialized and uses this key to encrypt the policy and the symmetric content key. The RMS client also signs the policy with the user's certificate that was obtained when the user environment was initialized.

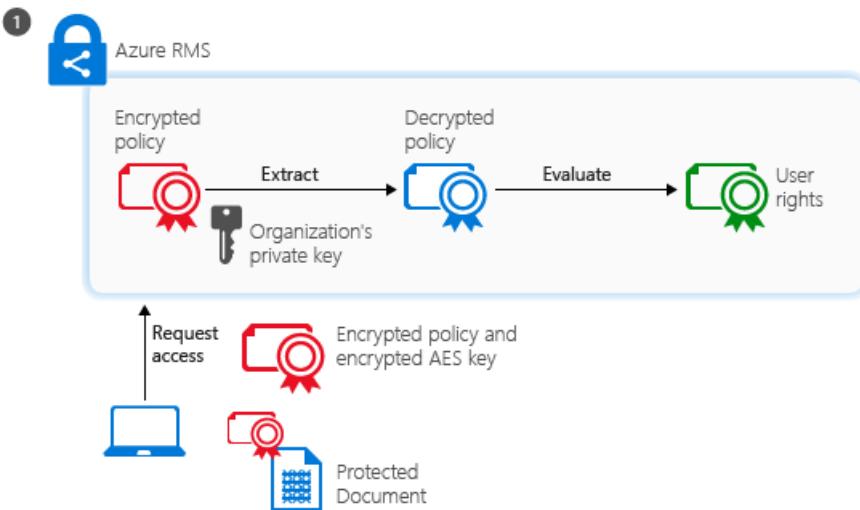


What's happening in step 3: Finally, the RMS client embeds the policy into a file with the body of the document encrypted previously, which together comprise a protected document.

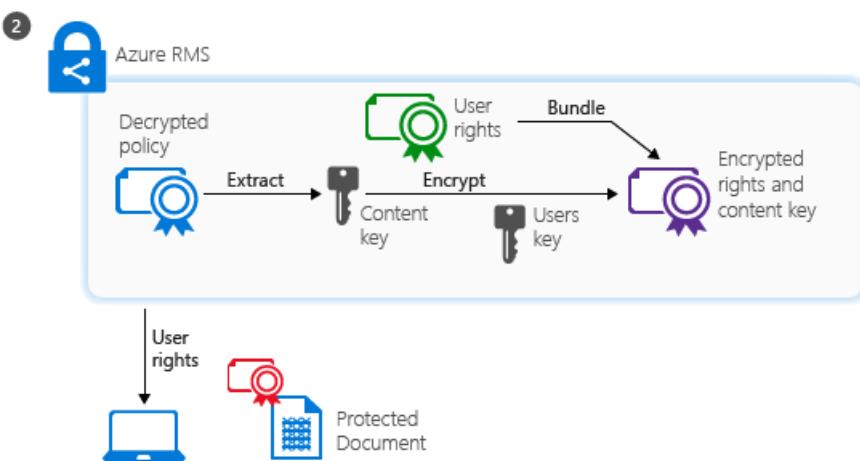
This document can be stored anywhere or shared by using any method, and the policy always stays with the encrypted document.

Content consumption

When a user wants to consume a protected document, the RMS client starts by requesting access to the Azure Rights Management service:

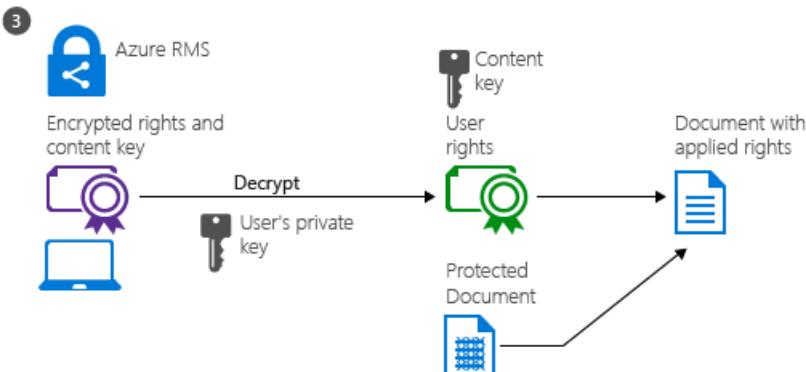


What's happening in step 1: The authenticated user sends the document policy and the user's certificates to the Azure Rights Management service. The service decrypts and evaluates the policy, and builds a list of rights (if any) the user has for the document. To identify the user, the Azure AD ProxyAddresses attribute is used for the user's account and groups to which the user is a member. For performance reasons, group membership is [cached](#). If the user account has no values for the Azure AD ProxyAddresses attribute, the value in the Azure AD UserPrincipalName is used instead.



What's happening in step 2: The service then extracts the AES content key from the decrypted policy. This key is then encrypted with the user's public RSA key that was obtained with the request.

The re-encrypted content key is then embedded into an encrypted use license with the list of user rights, which is then returned to the RMS client.



What's happening in step 3: Finally, the RMS client takes the encrypted use license and decrypts it with its own user private key. This lets the RMS client decrypt the document's body as it is needed and render it on the screen.

The client also decrypts the rights list and passes them to the application, which enforces those rights in the application's user interface.

NOTE

When users who are external to your organization consume content that you've protected, the consumption flow is the same. What changes for this scenario, is how the user is authenticated. For more information, see [When I share a protected document with somebody outside my company, how does that user get authenticated?](#)

Variations

The preceding walkthroughs cover the standard scenarios but there are some variations:

- **Email protection:** When Exchange Online and Office 365 Message Encryption with new capabilities is used to protect email messages, authentication for consumption can also use federation with a social identity provider or by using a one-time passcode. Then, the process flows are very similar, except that content consumption happens service-side in a web browser session over a temporarily cached copy of the outbound email.
- **Mobile devices:** When mobile devices protect or consume files with the Azure Rights Management service, the process flows are much simpler. Mobile devices don't first go through the user initialization process because instead, each transaction (to protect or consume content) is independent. As with Windows computers, mobile devices connect to the Azure Rights Management service and authenticate. To protect content, mobile devices submit a policy and the Azure Rights Management service sends them a publishing license and symmetric key to protect the document. To consume content, when mobile devices connect to the Azure Rights Management service and authenticate, they send the document policy to the Azure Rights Management service and request a use license to consume the document. In response, the Azure Rights Management service sends the necessary keys and restrictions to the mobile devices. Both processes use TLS to protect the key exchange and other communications.
- **RMS connector:** When the Azure Rights Management service is used with the RMS connector, the process flows remain the same. The only difference is that the connector acts as a relay between the on-premises services (such as Exchange Server and SharePoint Server) and the Azure Rights Management service. The connector itself does not perform any operations, such as the initialization of the user environment, or encryption or decryption. It simply relays the communication that would usually go to an AD RMS server, handling the translation between the protocols that are used on each side. This scenario lets you use the Azure Rights Management service with on-premises services.
- **Generic protection (.pfile):** When the Azure Rights Management service generically protects a file, the flow is basically the same for content protection except that the RMS client creates a policy that grants all rights. When the file is consumed, it is decrypted before it is passed to the target application. This scenario lets you protect all files, even if they don't natively support RMS.
- **Microsoft accounts:** Azure Information Protection can authorize email addresses for consumption when they are authenticated with a Microsoft account. However, not all applications can open protected content when a Microsoft account is used for authentication. [More information](#).

Next steps

To learn more about the Azure Rights Management service, use the other articles in the **Understand & Explore** section, such as [How applications support the Azure Rights Management service](#) to learn how your existing applications can integrate with Azure Rights Management to provide an information protection solution.

Review [Terminology for Azure Information Protection](#) so that you're familiar with the terms that you might come across as you're configuring and using the Azure Rights Management service, and be sure to also check [Requirements for Azure Information Protection](#) before you start your deployment. If you want to dive right in and

try it out for yourself, use the [Edit the policy and create a new label](#) tutorial.

If you're ready to start deploying data protection for your organization, use the [Azure Information Protection deployment roadmap](#) for your deployment steps and links for how-to instructions.

TIP

For additional information and help, use the resources and links in [Information and support for Azure Information Protection](#).

How applications support the Azure Rights Management service

5/21/2020 • 2 minutes to read • [Edit Online](#)

Applies to: [Azure Information Protection](#), [Office 365](#)

Use the following information to help you understand how the most commonly used end-user applications and services can use the Azure Rights Management service from Azure Information Protection to help protect your organization's documents and emails. These applications include Word, Excel, PowerPoint, and Outlook. The services include Exchange and Microsoft SharePoint.

NOTE

To verify the applications and versions that the Azure Rights Management service supports, see [Applications that support Azure Rights Management data protection](#).

In some cases, the Azure Rights Management service automatically applies protection, according to policies that administrators configure. For example, this is the case with SharePoint libraries and Exchange transport rules. In other cases, end users must apply the protection themselves from their applications. For example, users select a classification label that is configured to apply protection, or they select a template, or select specific options. Protection that is applied by users is typical when users protect a file to share and they also restrict access or usage to selected users or to users outside the organization.

Templates make it easier for users (and administrators who configure policies) to apply the correct level of protection and restrict access to people inside your organization. Although the Azure Rights Management service comes with two default templates, you probably want to create custom templates to reduce the times when users and administrators have to specify individual options. For more information about templates, see [Configuring and managing templates for Azure Information Protection](#).

For the cases where users must apply the protection themselves, be sure to provide them with instructions and guidance how and when to do this. Make the instructions specific for the application and versions that they use and how they use them. Also provide guidance for when and how users should apply the protection that is appropriate for your business. For more information, see [Helping users to protect files by using the Azure Rights Management service](#).

For information about how to configure these applications for the Azure Rights Management service from Azure Information Protection, see [Configuring applications for Azure Rights Management](#).

Search services can integrate with Rights Management in different ways. For example:

- Exchange Online and Exchange Server use service-side indexing so that a user's protected emails are automatically displayed in their search results.
- SharePoint in Microsoft 365 and SharePoint Server apply Rights Management protection to files only on download. This implementation means that indexing and search results on SharePoint are not affected by this document protection solution. However, if you have a document that you want to store in SharePoint and this document should not be returned in search results, protect the document before uploading it to SharePoint.
- Windows desktop search uses a shared index between different users of the device, so to keep the data in

the protected documents secure, it does not index protected files. This means that although your search results don't include files that you have protected, you can be assured that your files that contain sensitive data are not displayed in search results for other users who might sign in to your PC, or connect to your PC.

Next steps

Learn more about how each of the following applications and services supports the Azure Rights Management service:

- [Office applications and services](#)
- [File servers that run Windows Server and use File Classification Infrastructure \(FCI\)](#)
- [Other applications that support the RMS APIs](#)

How Office applications and services support Azure Rights Management

7/20/2020 • 8 minutes to read • [Edit Online](#)

Applies to: [Azure Information Protection](#), [Office 365](#)

End-user Office applications and Office services can use the Azure Rights Management service from Azure Information Protection to help protect your organization's data. These Office applications are Word, Excel, PowerPoint, and Outlook. The Office services are Exchange and Microsoft SharePoint. The Office configurations that support the Azure Rights Management service often use the term **information rights management (IRM)**.

Office applications: Word, Excel, PowerPoint, Outlook

These applications natively support Azure Rights Management and let users apply protection to a saved document or to an email message to be sent. Users can apply [templates](#) to apply the protection. Or, for Word, Excel, and PowerPoint, users can choose customized settings for access, rights, and usage restrictions.

For example, users can configure a Word document so that it can be accessed only by people in your organization. Or, control whether an Excel spreadsheet can be edited, or restricted to read-only, or prevent it from being printed. For time-sensitive files, an expiration time can be configured for when the file can no longer be accessed. This configuration can be made directly by users or by applying a protection template. For Outlook, users can also choose the **Do Not Forward** option to help prevent data leakage.

If you are ready to configure Office apps see [Office apps: Configuration for clients](#).

NOTE

Due to a limitation in recent Windows updates, files that are attached to emails may be currently be locked after opening the file.

Exchange Online and Exchange Server

When you use Exchange Online or Exchange Server, you can configure options for Azure Information Protection. This configuration lets Exchange provide the following protection solutions:

- **Exchange ActiveSync IRM** so that mobile devices can protect and consume protected email messages.
- Email protection support for **Outlook on the web**, which is implemented similarly to the Outlook client. This configuration lets users protect email messages by using protection templates or options. Users can read and use protected email messages that are sent to them.
- **Protection rules** for Outlook clients that an administrator configures to automatically apply protection templates and options to email messages for specified recipients. For example, when internal emails are sent to your legal department, they can only be read by members of the legal department and cannot be forwarded. Users see the protection applied to the email message before sending it, and by default, they can remove this protection if they decide it is not necessary. Emails are encrypted before they are sent. For more information, see [Outlook Protection Rules](#) and [Create an Outlook Protection Rule](#) in the Exchange library.
- **Mail flow rules** that an administrator configures to automatically apply protection templates or options to

email messages. These rules are based on properties such as sender, recipient, message subject, and content. These rules are similar in concept to protection rules but don't allow users to remove the protection because the protection is set by the Exchange service rather than by the client. Because protection is set by the service, it doesn't matter what device or what operating system the users have. For more information, see [Mail flow rules \(transport rules\) in Exchange Online](#) and [Create a Transport Protection Rule for Exchange on-premises](#).

- **Data loss prevention (DLP) policies** that contain sets of conditions to filter email messages and take actions, to help prevent data loss for confidential or sensitive content. One of the actions that you can specify is to apply encryption as protection, by specifying one of the protection templates or options. Policy Tips can be used when sensitive data is detected, to alert users that they might need to apply protection. For more information, see [Data loss prevention](#) in the Exchange Online documentation.
- **Office 365 Message Encryption** that supports sending a protected email message and protected Office documents as attachments to any email address on any device. For user accounts that don't use Azure AD, a web experience supports social identity providers or a one-time passcode. For more information, see [Set up new Office 365 Message Encryption capabilities built on top of Azure Information Protection](#) from the Office 365 documentation. To help you find additional information that is related to this configuration, see [Office 365 Message Encryption](#).

If you use Exchange on-premises, you can use the IRM features with the Azure Rights Management service by deploying the Azure Rights Management connector. This connector acts as a relay between your on-premises servers and the Azure Rights Management service.

For more information about the protection templates, see [Configuring and managing templates for Azure Information Protection](#).

For more information about the email options that you can use to protect emails, see [Do Not Forward option for emails](#) and [Encrypt-Only option for emails](#).

If you're ready to configure Exchange to protect emails:

- For Exchange Online, see [Exchange Online: IRM Configuration](#).
- For Exchange on-premises, see [Deploying the Azure Rights Management connector](#).

SharePoint in Microsoft 365 and SharePoint Server

When you use SharePoint in Microsoft 365 or SharePoint Server, you can protect documents by using the SharePoint information rights management (IRM) feature. This feature lets administrators protect lists or libraries so that when a user checks out a document, the downloaded file is protected so that only authorized people can view and use the file according to the information protection policies that you specify. For example, the file might be read-only, disable the copying of text, prevent saving a local copy, and prevent printing the file.

Word, PowerPoint, Excel, and PDF documents support this SharePoint IRM protection. By default, the protection is restricted to the person who downloads the document. You can change this default with a configuration option named **Allow group protection**, which extends the protection to a group that you specify. For example, you could specify a group that has permission to edit documents in the library so that the same group of users can edit the document outside SharePoint, regardless of which user downloaded the document. Or, you could specify a group that isn't granted permissions in SharePoint but users in this group need to access the document outside SharePoint. For SharePoint lists and libraries, this protection is always configured by an administrator, never an end user. You set the permissions at the site level, and these permissions, by default, are inherited by any list or library in that site. If you use SharePoint in Microsoft 365, users can also configure their Microsoft OneDrive library for IRM protection.

For more fine-grained control, you can configure a list or library in the site to stop inheriting permissions from its parent. You can then configure IRM permissions at that level (list or library) and they are then referred to as

"unique permissions." However, permissions are always set at the container level; you cannot set permissions on individual files.

The IRM service must first be enabled for SharePoint. Then, you specify IRM permissions for a library. For SharePoint and OneDrive, users can also specify IRM permissions for their OneDrive library. SharePoint does not use rights policy templates, although there are SharePoint configuration settings that you can select that match some settings that you can specify in the templates.

If you use SharePoint Server, you can use this IRM protection by deploying the Azure Rights Management connector. This connector acts as a relay between your on-premises servers and the Rights Management cloud service. For more information, see [Deploying the Azure Rights Management connector](#).

NOTE

There are some limitations when you use SharePoint IRM:

- You cannot use the default or custom protection templates that you manage in the Azure portal.
- Files that have a .ppdf file name extension for protected PDF files are not supported. For more information about viewing protected PDF documents, see [Protected PDF readers for Microsoft Information Protection](#).
- Coauthoring, when more than one person edits a document at the same time, is not supported. To edit a document in an IRM-protected library, you must first check out the document and download it, and then edit it in your Office application. Consequently, only one person can edit the document at a time.

For libraries that are not IRM-protected, if you apply protection-only to a file that you then upload to SharePoint or OneDrive, the following do not work with this file: Co-authoring, Office for the web, search, document preview, thumbnail, eDiscovery, and data loss prevention (DLP).

IMPORTANT

SharePoint IRM can be used in combination with sensitivity labels that apply protection. When you use both features together, the behavior changes for protected files. For more information, see [Enable sensitivity labels for Office files in SharePoint and OneDrive](#).

When you use SharePoint IRM protection, the Azure Rights Management service applies usage restrictions and data encryption for documents when they are downloaded from SharePoint, and not when the document is first created in SharePoint or uploaded to the library. For information about how documents are protected before they are downloaded, see [Data Encryption in OneDrive and SharePoint](#) from the SharePoint documentation.

Although no longer new, the following post from the Office 365 blog has some additional information that you might find useful: [What's New with Information Rights Management in SharePoint](#)

For changes that are coming, see [Updates to SharePoint security, administration, and migration](#).

If you are ready to configure SharePoint for IRM:

- For SharePoint in Microsoft 365, see [SharePoint in Microsoft 365 and OneDrive: IRM Configuration](#).
- For Sharepoint Server, see [Deploying the Azure Rights Management connector](#).

Next steps

If you have Office 365, you might be interested in reviewing [File Protection Solutions in Office 365](#), which provides recommended capabilities for protecting files in Office 365.

To see how other applications and services support the Azure Rights Management service from Azure Information

Protection, see [How applications support the Azure Rights Management service](#).

If you are ready to start deployment, which includes configuring these applications and services, see the [Azure Information Protection deployment roadmap](#).

How Windows file servers that use FCI support Azure Rights Management

7/20/2020 • 2 minutes to read • [Edit Online](#)

Applies to: [Azure Information Protection](#), [Office 365](#)

When you configure Windows Server to use File Classification Infrastructure, this File Server Resource Manager feature can scan local files and determine whether they contain sensitive data. For files that meet this criteria, they are tagged with classification properties that an administrator defines. The File Classification Infrastructure can then take automatic action, according to the classification. One of these actions includes applying information protection by using Azure Rights Management and the deployment of the Rights Management connector (also known as the RMS connector). Office files are then automatically protected by Azure RMS.

To protect all file types, do not use the RMS connector, but instead, run a Windows PowerShell script that uses cmdlets from the [Azure Information Protection module](#).

The classification policies are fully configurable and highly extensible so that you can prevent potential data leakage from unauthorized and authorized users. It can even help to reduce the risk of data leakage by network administrators because you can configure policies that don't require these administrators to have access to the files.

For instructions to deploy and configure the RMS connector for Office files, see [Deploying the Azure Rights Management connector](#).

For instructions to use the Windows PowerShell script for all file types, see [RMS Protection with Windows Server File Classification Infrastructure \(FCI\)](#).

Next steps

Now that you understand how applications and services support Azure RMS, you might be interested in comparing Azure RMS with the on-premises version of Rights Management, Active Directory Rights Management Services (AD RMS). For a comparison of features, requirements, and security controls, see [Comparing Azure Rights Management and AD RMS](#).

Other applications that support the Rights Management APIs

4/28/2020 • 2 minutes to read • [Edit Online](#)

Applies to: [Azure Information Protection](#), [Office 365](#)

Use the following information to help you understand how the Azure Rights Management service from Azure Information Protection can support other applications to protect your organization's data.

By using the Azure Information Protection SDKs, your internal developers can write line-of-business applications to natively support the Azure Rights Management service. How information protection is integrated with these applications depends on how they are written. For example, the integration might be automatically applied with minimal user interaction required, or for a more customized experience, users might be prompted to configure settings to apply information protection to files. For more information, see the [Developer's Guide](#).

Similarly, many software vendors provide applications to provide information protection solutions, also known as enterprise rights management (ERM) products. A popular example is a PDF reader that supports the Azure Rights Management service for specific platforms. You can use the table in [Applications that support Azure Rights Management data protection](#) to identify applications that support Rights Management (RMS-enlightened applications), and then use a web search to purchase or download the application.

Next steps

To see how other applications and services support the Azure Rights Management service, see [How Applications Support the Azure Rights Management service](#).

RMS for individuals and Azure Information Protection

7/20/2020 • 3 minutes to read • [Edit Online](#)

Applies to: [Azure Information Protection](#)

RMS for individuals is a free self-service subscription for users who need to open files that have been protected by Azure Information Protection. If these users cannot be authenticated by Azure Active Directory, this free sign-up service can create an account in Azure Active Directory for a user. As a result, these users can now authenticate by using their company email address and then read the protected files on computers or mobile devices.

RMS for individuals uses Azure Active Directory self-service signup. If users have created accounts for your organization by using this subscription, as an administrator for your organization, you can claim ownership and [take control of their accounts](#).

NOTE

This free subscription is one option to help ensure that authorized people outside your organization can always read files that your organization protects. Another option is to email documents by using [Office 365 Message Encryption with new capabilities](#). This email solution works for all email addresses on all devices and is the recommended way to safely share information and view Office documents in a browser with people outside your organization.

Another option is to use Microsoft accounts. However, not all applications can open protected content when a Microsoft account is used for authentication. [More information](#)

To sign up for this free account, users go to the [Microsoft Azure Information Protection page](#), and provide their work email address. They receive an email in response from Microsoft, and they can then complete the sign-up process by entering details to create their account.

When the account is created, the final page displays links to download the Azure Information Protection client or viewer for different devices, a link to the user guide, and a link for a current list of applications that natively support Rights Management protection.

To sign up for RMS for individuals

1. Using a Windows or Mac computer, or a mobile device, go to the [Microsoft Azure Information Protection page](#).
2. Type the email address that was used to protect the document you need to open.
3. Click **Sign up**.

Microsoft uses your email address to check whether your organization already has a [subscription for Azure Information Protection Premium](#) or an [Office 365 subscription that includes data protection by using Azure Information Protection](#). If either of these subscriptions are found, you don't need RMS for individuals. You are signed in immediately and the self-service sign up for RMS for individuals is canceled. If one of these subscriptions isn't found, you continue to the next step.

4. Wait for a confirmation email message to be sent to the address that you supplied. It will be from the Office 365 Team (support@email.microsoftonline.com) and has the subject **Finish signing up for Microsoft Azure Information Protection**.

5. When you receive the email, click **Yes, that's me** to verify your email address and complete the sign-up process.
6. You now see a **One last thing ...** page for you to supply details for your account. Type in your first name, your last name, enter and confirm a password of your choice, and then click **Start**.
7. When your account is created, you see a new Microsoft Azure Information Protection page where you can download and install the Azure Information Protection client, or click the [User guide](#) link for how-to instructions for Windows computers.

Now your account is created, if you're prompted to sign in to read protected files, enter the same email address and password that you used to create the account for RMS for the individuals.

IMPORTANT

Although you can now also protect files with this account, do not do so until your organization has a [trial or paid subscription](#) for Azure Information Protection. If you protect files and emails by using this free subscription and then your organization takes control of your account, previously protected content might become inaccessible.

Next steps

RMS for individuals is an example of using the self-service signup feature that is supported by Azure Active Directory. For more information about how this feature works, see [What is Self-Service Signup for Azure Active Directory?](#) in the Azure Active Directory documentation.

Azure Information Protection - also known as ...

4/28/2020 • 2 minutes to read • [Edit Online](#)

Applies to: [Azure Information Protection](#), [Office 365](#)

Azure Information Protection (sometimes abbreviated to AIP) has evolved from a long history of established technologies from Microsoft that implement rights management protection. Because of this evolution, you might know this solution by one of its previous names. Or you might see references to these names in documentation, the UI, and log files.

The following sections list some of these names.

TIP

You'll find many of these product and service names, and their related terms in [Terminology for Azure Information Protection](#).

Cloud-based solutions

- **Azure Rights Management** or **Azure Rights Management service**—frequently abbreviated to *Azure RMS*
- **Azure Active Directory Rights Management**—occasionally abbreviated to *AADRM*
- **Windows Azure Active Directory Rights Management**—often abbreviated to *Windows Azure AD Rights Management*

On-premises solutions

- **Active Directory Rights Management Services**—frequently abbreviated to *AD RMS*
- **Windows Rights Management Services**—often abbreviated to *Windows RMS*

Other names

- **Microsoft Rights Management** or **Microsoft Rights Management services**

The collective name that includes the current on-premises version (AD RMS) and the cloud-based version (Azure RMS).

- **"The NEW Microsoft RMS"**

A popular label that was sometimes used when the cloud-based version was officially released, to emphasize the new ease of deployment in comparison to its on-premises predecessors.

- **Information Rights Management**—often abbreviated to */IRM*

The Office implementation of the technology that supports the current on-premises version (AD RMS) and the cloud-based version (Azure RMS).

- **Rights Management Online** or **RMS Online**

This was a proposed early name for the cloud-based version of AD RMS, and included here because you might see this name in log files and error messages.

Note that you might see or hear references to this technology as **DRM**, which is a well-known abbreviation for digital rights management. DRM solutions typically protect against illegal distribution of digital software, which is very different from this enterprise information protection solution.

Does "Azure Information Protection" now replace all these names?

As the cloud-based solution that you purchase, yes. Azure Information Protection offers the new capabilities of classification and labeling for an organization's documents and emails, which in turn can apply Rights Management protection.

However, Azure Rights Management is still used as the protection technology for Azure Information Protection, and for Office 365 services that use this cloud-based Rights Management protection. So in the context of the protection technology that is used by Azure Information Protection, "Azure Rights Management" (Azure RMS) remains a current name.

Similarly, "Active Directory Rights Management Services" (AD RMS) remains a current name for the Windows Server server role, which provides on-premises Rights Management protection. This protection technology can be used with Azure Information Protection and might be suitable for a very small percentage of documents and emails that must be protected by an on-premises key. In this scenario, AD RMS is often referred to as the "hold your own key" or HYOK solution.

How to evaluate or purchase the latest version

For more information about how you can purchase or evaluate Azure Information Protection, and the different features that are available for the subscription plans, see the [Azure Information Protection](#) site.

How-to guides for common scenarios that use Azure Information Protection

7/20/2020 • 2 minutes to read • [Edit Online](#)

Applies to: [Azure Information Protection](#)

Instructions for: [Azure Information Protection client for Windows](#)

There are many ways in which you can use Azure Information Protection to classify and optionally, protect your organization's documents and emails.

The most successful deployments are those that identify specific use cases that provide the most business benefit to the organization. Use the following list of common scenarios and instructions to get your deployment off the ground.

Common scenarios

SCENARIO: I WANT TO ...	INSTRUCTIONS
Find what sensitive information my organization stores on-premises	Quickstart: Find what sensitive information you have in files stored on-premises
Make it easy for users to protect their emails that contain sensitive information	Quickstart: Configure a label for users to easily protect emails that contain sensitive information
Make it easy for users to classify data as it's created or edited, and protect it if it contains sensitive information	Tutorial: Edit the policy and create a new label
Make it easy for users to collaborate on a protected document	Configuring secure document collaboration by using Azure Information Protection
Automatically protect users' emails that are sent outside the organization	Configuring mail flow rules for Azure Information Protection labels
Automatically classify and protect existing data in my on-premises data stores	Deploying the Azure Information Protection scanner
Use my own key to protect my organization's data	Planning and implementing your tenant key
Migrate from AD RMS	Migrating from AD RMS to Azure Information Protection

Additional deployment instructions

Our [Azure Information Protection technical blog](#) includes additional guidance from the trenches.

For example, a methodology with best practices for business decision makers and IT implementers:

- [Azure Information Protection Deployment Acceleration Guide](#)

Step-by-step instructions:

- [How to Build a Custom AIP Tracking Portal](#)
- [Create richer reports with Microsoft Information Protection and Azure AD login data](#)
- [Leverage Microsoft Cloud App Security to apply Azure Information Protection labels in the cloud](#)
- [How to prepare an Azure Information Protection "Cloud Exit" plan](#)
- [Cross-Tenant Label Visualization](#)
- [Using Azure Information Protection to protect PDF's and Adobe Acrobat Reader to view them](#)
- [Cataloging your Sensitive Data with AIP, Even Before Configuring Labels!](#)
- [Azure Information Protection Scanner Express Installation](#)
- [Discovery of Sensitive Data Using the AIP Scanner \(AIP Premium P1\)](#)

Next steps

Don't see your scenario listed? Check the [Deployment roadmap](#) for a full list of planning and deployment steps.

If you're new to Azure Information Protection, review [What is Azure Information Protection?](#) for a quick introduction to the service before you begin your deployment.

Azure Information Protection deployment roadmap

7/20/2020 • 12 minutes to read • [Edit Online](#)

Applies to: [Azure Information Protection](#), [Office 365](#)

NOTE

To provide a unified and streamlined customer experience, **Azure Information Protection client (classic)** and **Label Management** in the Azure Portal are being **deprecated** as of **March 31, 2021**. This time-frame allows all current Azure Information Protection customers to transition to our unified labeling solution using the Microsoft Information Protection Unified Labeling platform. Learn more in the official [deprecation notice](#).

Use the following steps as recommendations to help you prepare for, implement, and manage Azure Information Protection for your organization.

Alternatively:

- Looking for scenario-based instruction for Azure Information Protection? See [How-to guides for common scenarios that use Azure Information Protection](#).
- Looking for the Azure Information Protection release roadmap? See [Information about new releases and updates](#).

Identify your deployment roadmap

Before you implement any of the following steps to deploy Azure Information Protection, make sure that you have reviewed [Requirements for Azure Information Protection](#).

Then choose the deployment roadmap that's applicable for your organization and that matches the [subscription functionality and features](#) that you need:

- [Use classification, labeling, and protection](#)

The recommended path when you have a supporting subscription because the additional capabilities support discovering sensitive information, and labeling documents and emails for classification. The labels can also apply protection, abstracting this complexity from users.

The deployment steps are suitable for Azure Information Protection labels, and sensitivity labels that use the [unified labeling platform](#).

- [Use data protection only](#)

The path to use when you don't have a subscription that supports classification and labels, but does support protection without labels.

Deployment roadmap for classification, labeling, and protection

NOTE

Already using the protection functionality from Azure Information Protection? You can skip many of these steps and focus on steps 3 and 5.1.

Step 1: Confirm your subscription and assign user licenses

Review the subscription information and feature list from the [Azure Information Protection Pricing](#) page to confirm that your organization has a subscription that includes the functionality and features that you expect. Then, assign licenses from this subscription to each user in your organization who will classify, label, and protect documents and emails.

Note: Do not manually assign user licenses from the free RMS for individuals subscription and do not use this license to administer the Azure Rights Management service for your organization. These licenses display as **Rights Management Adhoc** in the Microsoft 365 admin center, and **RIGHTSMANAGEMENT_ADHOC** when you run the Azure AD PowerShell cmdlet, [Get-MsolAccountSku](#). For more information about how the RMS for individuals subscription is automatically granted and assigned to users, see [RMS for individuals and Azure Information Protection](#).

Step 2: Prepare your tenant to use Azure Information Protection

Before you begin using Azure Information Protection, make sure that you have user accounts and groups in Office 365 or Azure Active Directory. These user accounts and groups will be used by Azure Information Protection to authenticate and authorize users from your organization. If necessary, create these account and groups, or synchronize them from your on-premises directory.

For more information, see [Preparing users and groups for Azure Information Protection](#).

Step 3: Configure and deploy classification and labeling

Before you configure labels and policy settings, decide which Azure Information Protection client you're going to use: The classic client or the unified labeling client. Or you might need both clients. This client decision is needed now, so you know which management portal to use to configure labels and policy settings. For more information and to help you with this decision, see [Choose which Azure Information Protection client to use](#).

TIP

Optional but recommended: Consider using the [scanner quickstart](#) to discover what sensitive information you have on your local data stores. The information that the scanner finds can help you with your classification taxonomy, provide valuable information about what labels you need, and which files need protecting.

Because the scanner discovery mode doesn't require you to configure labels or even have your classification taxonomy defined, running the scanner in this way is suitable for this very early stage of your deployment. You can also use this configuration of the scanner in parallel with the following deployment steps, until you configure recommended or automatic labeling.

If you don't already have a classification strategy, review the [default Azure Information Protection policy](#) and use this as the basis for deciding what classification labels to assign to your organization data. You can customize these to meet your business requirements.

Reconfigure your labels to make any changes you need to support your classification decisions. Configure the policy for manual labeling by users, and write user guidance that explains which label to apply and when. If your default policy was created with labels that automatically apply protection, temporarily remove the protection settings or disable the label. For more information about how to configure the labels and policy settings, see the following documentation:

- Azure Information Protection labels for the classic client: [Configuring Azure Information Protection policy](#)
- Sensitivity labels for the unified labeling client: [Learn about sensitivity labels](#)

Then deploy the Azure Information Protection client (classic) or the Azure Information Protection unified labeling client for users. Provide user training and specific instructions when to select the labels. For more information about installing and supporting the clients, see the admin guides:

- [Azure Information Protection client administrator guide](#)

- [Azure Information Protection unified labeling client administrator guide](#)

After a period of time, when users are comfortable labeling their documents and emails, introduce more advanced configurations. These might include the following:

- Apply a default label
- Prompt users for justification if they chose a label with a lower classification level or remove a label
- Mandate that all documents and emails have a label
- Customized headers, footers, or watermarks
- Recommended and automatic labeling

At this stage, do not select the option to protect documents and emails. However, after you have configured labels for automatic labeling, run the [Azure Information Protection scanner](#) on your local data stores in discovery mode and to match your policy. Running the scanner with this configuration tells you which labels would be applied to files. This information helps you fine-tune your label configuration and prepares you for classifying and protecting files in bulk.

Step 4: Prepare for data protection

When users are comfortable labeling documents and emails, you're ready to start introducing data protection for your most sensitive data. This stage requires the following preparation:

1. Decide whether you want Microsoft to manage your tenant key (the default), or generate and manage your tenant key yourself (known as bring your own key, or BYOK). For more information, see [Planning and implementing your Azure Information Protection tenant key](#).
2. Install the PowerShell module for AIPService on at least one computer that has internet access. You can do this step now, or later. For more information, see [Installing the AIPService PowerShell module](#).
3. If you are currently using AD RMS: Perform a migration to move the keys, templates, and URLs to the cloud. For more information, see [Migrating from AD RMS to Information Protection](#).
4. Make sure that the protection service is activated so that you can begin to protect documents and emails. If a phased deployment is required, configure user onboarding controls to restrict users' ability to apply protection. For more information, see [Activating the protection service from Azure Information Protection](#).

Optionally, consider configuring the following:

- Usage logging so that you can monitor how your organization is using the protection service. You can do this step now, or later. For more information, see [Logging and analyzing the protection usage from Azure Information Protection](#).

Step 5: Configure labels and settings, applications, and services for data protection

1. Update your labels to apply protection

For the Azure Information Protection client (classic), see [How to configure a label for Rights Management protection](#).

For the Azure Information Protection unified labeling client, see [Restrict access to content by using encryption in sensitivity labels](#).

Note that users can apply labels in Outlook that apply Rights Management protection even if Exchange is not configured for information rights management (IRM). However, until Exchange is configured for IRM or [Office 365 Message Encryption with new capabilities](#), your organization will not get the full functionality of using Azure Rights Management protection with Exchange. This additional configuration is included in the following list (2 for Exchange Online, and 5 for Exchange on-premises).

2. Configure Office applications and services

Configure Office applications and services for the information rights management (IRM) features in Microsoft SharePoint or Exchange Online. For more information, see [Configuring applications for Azure Rights Management](#).

3. Configure the super user feature for data recovery

If you have existing IT services that need to inspect files that Azure Information Protection will protect—such as data leak prevention (DLP) solutions, content encryption gateways (CEG), and anti-malware products—configure the service accounts to be super users for Azure Rights Management. For more information, see [Configuring super users for Azure Information Protection and discovery services or data recovery](#).

4. Classify and protect existing files in bulk

For your on-premises data stores, now run the [Azure Information Protection scanner](#) in enforcement mode so that files are automatically labeled. For cloud-based data stores, use [Azure Cloud App Security](#).

For files on PCs, you can use PowerShell cmdlets to classify and protect files. For more information, see the following admin guides:

- Azure Information Protection client (classic): [Using PowerShell with the Azure Information Protection client](#)
- Azure Information Protection unified labeling client: [Using PowerShell with the Azure Information Protection unified labeling client](#)

5. Deploy the connector for IRM-protected libraries on SharePoint Server, and IRM-protected emails for Exchange on-premises

If you have SharePoint and Exchange on-premises and want to use their information rights management (IRM) features, install and configure the Rights Management connector. For more information, see [Deploying the Azure Rights Management connector](#).

Step 6: Use and monitor your data protection solutions

You're now ready to monitor how your organization is using the labels that you've configured and confirm that you're protecting sensitive information. For addition information to support this deployment phase, see the following:

- [Central reporting for Azure Information Protection](#) - currently in preview
- [Local usage logging with Windows event monitor](#) for the Azure Information Protection client (classic)
- [Logging and analyzing the protection usage from Azure Information Protection](#)

Step 7: Administer the protection service for your tenant account as needed

As you begin to use the protection service, you might find PowerShell useful to help script or automate administrative changes. PowerShell might also be needed for some of the advanced configurations.

For more information, see [Administering protection from Azure Information Protection by using PowerShell](#).

Deployment roadmap for data protection only

Step 1: Confirm that you have a subscription that includes the protection service from Azure Information Protection

Review the subscription information and feature list from the [Azure Information Protection Pricing](#) page to confirm that your organization has a subscription that includes the functionality and features that you expect. Then, assign a license from this subscription to each user in your organization who will protect documents and

emails.

Note: Do not manually assign user licenses from the free RMS for individuals subscription and do not use this license to administer the Azure Rights Management service for your organization. These licenses display as **Rights Management Adhoc** in the Microsoft 365 admin center, and **RIGHTSMANAGEMENT_ADHOC** when you run the Azure AD PowerShell cmdlet, [Get-MsolAccountSku](#). For more information about how the RMS for individuals subscription is automatically granted and assigned to users, see [RMS for individuals and Azure Information Protection](#).

Step 2: Prepare your tenant to use Azure Information Protection

Before you begin using the protection service from Azure Information Protection, do the following preparation:

1. Make sure that your Office 365 tenant contains the user accounts and groups that will be used by Azure Information Protection to authenticate and authorize users from your organization. If necessary, create these account and groups, or synchronize them from your on-premises directory. For more information, see [Preparing users and groups for Azure Information Protection](#).
2. Decide whether you want Microsoft to manage your tenant key (the default), or generate and manage your tenant key yourself (known as bring your own key, or BYOK). For more information, see [Planning and implementing your Azure Information Protection tenant key](#).
3. Install the PowerShell module for AIPService on at least one computer that has internet access. You can do this step now, or later. For more information, see [Installing the AIPService PowerShell module](#).
4. If you are currently using AD RMS: Perform a migration to move the keys, templates, and URLs to the cloud. For more information, see [Migrating from AD RMS to Azure Information Protection](#).
5. Make sure that the protection service is activated so that you can begin to protect documents and emails. If a phased deployment is required, configure user onboarding controls to restrict users' ability to apply protection. For more information, see [Activating the protection service from Azure Information Protection](#).

Optionally, consider configuring the following:

- Custom templates for protection settings if the default templates are not sufficient for your organization. You can do this step now, or later. For more information, see [Configuring and managing templates for Azure Information Protection](#).
- Usage logging so that you can monitor how your organization is using the protection service. You can do this step now, or later. For more information, see [Logging and analyzing the protection usage from Azure Information Protection](#).

Step 3: Install the Azure Information Protection client (classic) and configure applications and services for Rights Management

1. Deploy the Azure Information Protection client (classic)

Install the classic client for users to support Office 2010, to protect files other than Office documents and emails, and to track protected documents. Provide user training for this client. For more information, see [Azure Information Protection client for Windows](#).

2. Configure Office applications and services

Configure Office applications and services for the information rights management (IRM) features in SharePoint or Exchange Online. For more information, see [Configuring applications for Azure Rights Management](#).

3. Configure the super user feature for data recovery

If you have existing IT services that need to inspect files that Azure Information Protection will protect—such as data leak prevention (DLP) solutions, content encryption gateways (CEG), and anti-malware

products—configure the service accounts to be super users for Azure Rights Management. For more information, see [Configuring super users for Azure Information Protection and discovery services or data recovery](#).

4. Protect existing files in bulk

You can use PowerShell cmdlets to bulk-protect or bulk-unprotect multiple file types. For more information, see [Using PowerShell with the Azure Information Protection client](#) from the admin guide.

For files on Windows-based file servers, you can use these cmdlets with a script and Windows Server File Classification Infrastructure. For more information, see [RMS protection with Windows Server File Classification Infrastructure \(FCI\)](#).

5. Deploy the connector for on-premises servers

If you have on-premises services that you want to use with the protection service, install and configure the Rights Management connector. For more information, see [Deploying the Azure Rights Management connector](#).

Step 4: Use and monitor your data protection solutions

You're now ready to protect your data, and log how your company is using the protection service. For additional information to support this deployment phase, see [Helping users to protect files by using the Azure Rights Management service](#) and [Logging and analyzing the protection usage from Azure Information Protection](#).

Step 5: Administer the protection service for your tenant account as needed

As you begin to use the protection service, you might find PowerShell useful to help script or automate administrative changes. PowerShell might also be needed for some of the advanced configurations.

For more information, see [Administering protection from Azure Information Protection by using PowerShell](#).

Next steps

As you deploy Azure Information Protection, you might find it helpful to check the [frequently asked questions](#), and the [information and support](#) page for additional resources.

Migrating from AD RMS to Azure Information Protection

7/20/2020 • 11 minutes to read • [Edit Online](#)

Applies to: Active Directory Rights Management Services, Azure Information Protection, Office 365

Use the following set of instructions to migrate your Active Directory Rights Management Services (AD RMS) deployment to Azure Information Protection.

After the migration, your AD RMS servers are no longer in use but users still have access to documents and email messages that your organization protected by using AD RMS. Newly protected content will use the Azure Rights Management service (Azure RMS) from Azure Information Protection.

Not sure whether this AD RMS migration is right for your organization?

- For an introduction to Azure Information Protection, see [What is Azure Information Protection?](#)
- For a comparison of Azure Information Protection with AD RMS, see [Comparing Azure Information Protection and AD RMS](#).

Recommended reading before you migrate to Azure Information Protection

Although not required, you might find it useful to read the following documentation before you start the migration. This knowledge provides you with a better understanding of how the technology works when it is relevant to your migration step.

- [Planning and implementing your Azure Information Protection tenant key](#): Understand the key management options that you have for your Azure Information Protection tenant where your SLC key equivalent in the cloud is either managed by Microsoft (the default) or managed by you (the "bring your own key", or BYOK configuration).
- [RMS service discovery](#): This section of the RMS client deployment notes explains that the order for service discovery is **registry**, then **service connection point (SCP)**, then **cloud**. During the migration process when the SCP is still installed, you configure clients with registry settings for your Azure Information Protection tenant so that they do not use the AD RMS cluster returned from the SCP.
- [Overview of the Microsoft Rights Management connector](#): This section from the RMS connector documentation explains how your on-premises servers can connect to the Azure Rights Management service to protect documents and emails.

In addition, if you are not familiar with how AD RMS works, you might find it useful to read [How does Azure RMS work? Under the hood](#) to help you identify which technology processes are the same or different for the cloud version.

Prerequisites for migrating AD RMS to Azure Information Protection

Before you start the migration to Azure Information Protection, make sure that the following prerequisites are in place and that you understand any limitations.

- **A supported RMS deployment:**

- The following releases of AD RMS support a migration to Azure Information Protection:

- Windows Server 2012 (x64)
- Windows Server 2012 R2 (x64)
- Windows Server 2016 (x64)
- All valid AD RMS topologies are supported:
 - Single forest, single RMS cluster
 - Single forest, multiple licensing-only RMS clusters
 - Multiple forests, multiple RMS clusters

Note: By default, multiple AD RMS clusters migrate to a single tenant for Azure Information Protection. If you want separate tenants for Azure Information Protection, you must treat them as different migrations. A key from one RMS cluster cannot be imported to more than one tenant.

- **All requirements to run Azure Information Protection, including a subscription for Azure Information Protection (the Azure Rights Management service is not activated):**

See [Requirements for Azure Information Protection](#).

Note that if you have computers that run Office 2010, you must install the [Azure Information Protection client](#) or the [Azure Information Protection unified labeling client for users](#), because these clients provide the ability to authenticate users to cloud services. For later versions of Office, these clients are required for classification and labeling, and the Azure Information Protection client is optional but recommended if you want to only protect data. For more information, see the admin guides for the [Azure Information Protection client](#) and the [Azure Information Protection unified labeling client](#).

Although you must have a subscription for Azure Information Protection before you can migrate from AD RMS, we recommend that the Rights Management service for your tenant is not activated before you start the migration. The migration process includes this activation step after you have exported keys and templates from AD RMS and imported them to your tenant for Azure Information Protection. However, if the Rights Management service is already activated, you can still migrate from AD RMS with some additional steps.

- **Preparation for Azure Information Protection:**

- Directory synchronization between your on-premises directory and Azure Active Directory
- Mail-enabled groups in Azure Active Directory

See [Preparing users and groups for Azure Information Protection](#).

- **If you have used the Information Rights Management (IRM) functionality of Exchange Server (for example, transport rules and Outlook Web Access) or SharePoint Server with AD RMS:**

- Plan for a short period of time when IRM will not be available on these servers

You can continue to use IRM on these servers after the migration. However, one of the migration steps is to temporarily disable the IRM service, install and configure a connector, reconfigure the servers, and then re-enable IRM.

This is the only interruption to service during the migration process.

- **If you want to manage your own Azure Information Protection tenant key by using an HSM-protected key:**

- This optional configuration requires Azure Key Vault and an Azure subscription that supports Key

Vault with HSM-protected keys. For more information, see the [Azure Key Vault Pricing page](#).

Cryptographic mode considerations

If your AD RMS cluster is currently in Cryptographic Mode 1, do not upgrade the cluster to Cryptographic Mode 2 before you start the migration. Instead, migrate using Cryptographic Mode 1 and you can rekey your tenant key at the end of the migration, as one of the post migration tasks.

To confirm the AD RMS cryptographic mode:

- For Windows Server 2012 R2 and Windows 2012: AD RMS cluster properties > **General** tab.

Migration limitations

- If you have software and clients that are not supported by the Rights Management service that is used by Azure Information Protection, they will not be able to protect or consume content that is protected by Azure Rights Management. Be sure to check the supported applications and clients sections from [Requirements for Azure Information Protection](#).
- If your AD RMS deployment is configured to collaborate with external partners (for example, by using trusted user domains or federation), they must also migrate to Azure Information Protection either at the same time as your migration, or as soon as possible afterwards. To continue to access content that your organization previously protected by using Azure Information Protection, they must make client configuration changes that are similar to those that you make, and included in this document.

Because of the possible configuration variations that your partners might have, exact instructions for this reconfiguration are out of scope for this document. However, see the next section for planning guidance and for additional help, [contact Microsoft Support](#).

Migration planning if you collaborate with external partners

Include your AD RMS partners in your planning phase for migration because they must also migrate to Azure Information Protection. Before you do any of the following migration steps, make sure that the following is in place:

- They have an Azure Active Directory tenant that supports the Azure Rights Management service.
For example, they have an Office 365 E3 or E5 subscription, or an Enterprise Mobility + Security subscription, or a standalone subscription for Azure Information Protection.
- Their Azure Rights Management service is not yet activated but they know their Azure Rights Management service URL.
They can get this information by installing the Azure Rights Management Tool, connecting to the service ([Connect-AipService](#)), and then viewing their tenant information for the Azure Rights Management service ([Get-AipServiceConfiguration](#)).
- They provide you with the URLs for their AD RMS cluster and their Azure Rights Management service URL, so that you can configure your migrated clients to redirect requests for their AD RMS protected content to their tenant's Azure Rights Management service. Instructions for configuring client redirection are in step 7.
- They import their AD RMS cluster root keys (SLC) into their tenant before you start to migrate your users. Similarly, you must import your AD RMS cluster root keys before they start to migrate their users. Instructions for importing the key are covered in this migration process, [Step 4. Export configuration data from AD RMS and import it to Azure Information Protection](#).

Overview of the steps for migrating AD RMS to Azure Information

Protection

The migration steps can be divided into five phases that can be done at different times, and by different administrators.

PHASE 1: MIGRATION PREPARATION

- **Step 1: Install the AIPService PowerShell module and identify your tenant URL**

The migration process requires you to run one or more of the PowerShell cmdlets from the AIPService module. You will need to know your tenant's Azure Rights Management service URL to complete many of the migration steps, and you can identify this value by using PowerShell.

- **Step 2. Prepare for client migration**

If you cannot migrate all clients at once and will migrate them in batches, use onboarding controls and deploy a pre-migration script. However, if you will migrate everything at the same time rather than do a phased migration, you can skip this step.

- **Step 3: Prepare your Exchange deployment for migration**

This step is required if you currently use the IRM feature of Exchange Online or Exchange on-premises to protect emails. However, if you will migrate everything at the same time rather than do a phased migration, you can skip this step.

PHASE 2: SERVER-SIDE CONFIGURATION FOR AD RMS

- **Step 4. Export configuration data from AD RMS and import it to Azure Information Protection**

You export the configuration data (keys, templates, URLs) from AD RMS to an XML file, and then upload that file to the Azure Rights Management service from Azure Information Protection, by using the Import-AipServiceTpd PowerShell cmdlet. Then, identify which imported Server Licenser Certificate (SLC) key to use as your tenant key for the Azure Rights Management service. Additional steps might be needed, depending on your AD RMS key configuration:

- **Software-protected key to software-protected key migration:**

Centrally managed, password-based keys in AD RMS to Microsoft-managed Azure Information Protection tenant key. This is the simplest migration path and no additional steps are required.

- **HSM-protected key to HSM-protected key migration:**

Keys that are stored by an HSM for AD RMS to customer-managed Azure Information Protection tenant key (the "bring your own key" or BYOK scenario). This requires additional steps to transfer the key from your on-premises nCipher HSM to Azure Key Vault and authorize the Azure Rights Management service to use this key. Your existing HSM-protected key must be module-protected; OCS-protected keys are not supported by Rights Management services.

- **Software-protected key to HSM-protected key migration:**

Centrally managed, password-based keys in AD RMS to customer-managed Azure Information Protection tenant key (the "bring your own key" or BYOK scenario). This requires the most configuration because you must first extract your software key and import it to an on-premises HSM, and then do the additional steps to transfer the key from your on-premises nCipher HSM to an Azure Key Vault HSM and authorize the Azure Rights Management service to use the key vault that stores the key.

- **Step 5. Activate the Azure Rights Management service**

If possible, do this step after the import process and not before. Additional steps are required if the service was activated before the import.

- **Step 6: Configure imported templates**

When you import your rights policy templates, their status is archived. If you want users to be able to see and use them, you must change the template status to be published in the Azure classic portal.

PHASE 3: CLIENT-SIDE CONFIGURATION

- **Step 7: Reconfigure Windows computers to use Azure Information Protection**

Existing Windows computers must be reconfigured to use the Azure Rights Management service instead of AD RMS. This step applies to computers in your organization, and to computers in partner organizations if you have collaborated with them while you were running AD RMS.

PHASE 4: SUPPORTING SERVICES CONFIGURATION

- **Step 8: Configure IRM integration for Exchange Online**

This step completes the AD RMS migration for Exchange Online to now use the Azure Rights Management service.

- **Step 9: Configure IRM integration for Exchange Server and SharePoint Server**

This step completes the AD RMS migration for Exchange or SharePoint on-premises to now use the Azure Rights Management service, which requires deploying the Rights Management connector.

PHASE 5: POST MIGRATION TASKS

- **Step 10: Deprovision AD RMS**

When you have confirmed that all Windows computers are using the Azure Rights Management service and are no longer accessing your AD RMS servers, you can deprovision your AD RMS deployment.

- **Step 11: Complete client migration tasks**

If you have deployed the [mobile device extension](#) to support mobile devices such as iOS phones and iPads, Android phones and tablets, Windows phones and tablets, and Mac computers, you must remove the SRV records in DNS that redirected these clients to use AD RMS.

The onboarding controls that you configured during the preparation phase are no longer needed. However, if you did not use onboarding controls because you chose to migrate everything at the same time rather than do a phased migration, you can skip the instructions to remove the onboarding controls.

If your Windows computers are running Office 2010, check whether you need to disable the **AD RMS Rights Policy Template Management (Automated)** task.

- **Step 12: Rekey your Azure Information Protection tenant key**

This step is recommended if you were not running in Cryptographic Mode 2 before the migration.

Next steps

To start the migration, go to [Phase 1 - preparation](#).

Migration phase 1 - preparation

7/20/2020 • 5 minutes to read • [Edit Online](#)

Applies to: Active Directory Rights Management Services, Azure Information Protection, Office 365

Use the following information for Phase 1 of migrating from AD RMS to Azure Information Protection. These procedures cover steps 1 through 3 from [Migrating from AD RMS to Azure Information Protection](#) and prepare your environment for migration without any impact to your users.

Step 1: Install the AIPService PowerShell module and identify your tenant URL

Install the AIPService module so that you can configure and manage the service that provides the data protection for Azure Information Protection.

For instructions, see [Installing the AIPService PowerShell module](#).

To complete some of the migration instructions, you will need to know the Azure Rights Management service URL for your tenant so that you can substitute it for when you see references to <Your Tenant URL>. Your Azure Rights Management service URL has the following format: {GUID}.rms.[Region].aadrm.com.

For example: 5c6bb73b-1038-4eec-863d-49bded473437.rms.na.aadrm.com

To identify your Azure Rights Management service URL

1. Connect to the Azure Rights Management service and when prompted, enter the credentials for your tenant's global administrator:

```
Connect-AipService
```

2. Get your tenant's configuration:

```
Get-AipServiceConfiguration
```

3. Copy the value displayed for **LicensingIntranetDistributionPointUrl**, and from this string, remove

```
/_wmcs\licensing .
```

What remains is your Azure Rights Management service URL for your Azure Information Protection tenant. This value is often shortened to *Your tenant URL* in the following migration instructions.

You can verify that you have the correct value by running the following PowerShell command:

```
(Get-AipServiceConfiguration).LicensingIntranetDistributionPointUrl -match "https://[0-9A-Za-z\.-]*"  
| Out-Null; $matches[0]
```

Step 2. Prepare for client migration

For most migrations, it is not practical to migrate all clients at once, so you will likely migrate clients in batches. This means that for a period of time, some clients will be using Azure Information Protection and some will still be using AD RMS. To support both pre-migrated and migrated users, use onboarding controls and deploy a pre-

migration script. This step is required during the migration process so that users who have not yet migrated can consume content that has been protected by migrated users who are now using Azure Rights Management.

1. Create a group, for example, named **AIPMigrated**. This group can be created in Active Directory and synchronized to the cloud, or it can be created in Office 365 or Azure Active Directory. Do not assign any users to this group at this time. At a later step, when users are migrated, you will add them to the group.

Make a note of this group's object ID. To do this, you can use Azure AD PowerShell—for example, for version 1.0 of the module, use the [Get-MsolGroup](#) command. Or you can copy the object ID of the group from the Azure portal.

2. Configure this group for onboarding controls to allow only people in this group to use Azure Rights Management to protect content. To do this, in a PowerShell session, connect to the Azure Rights Management service and when prompted, specify your global admin credentials:

```
Connect-AipService
```

Then configure this group for onboarding controls, substituting your group object ID for the one in this example, and enter Y to confirm when you are prompted:

```
Set-AipServiceOnboardingControlPolicy -UseRmsUserLicense $False -SecurityGroupObjectId "fba99fed-32a0-44e0-b032-37b419009501" -Scope WindowsApp
```

3. [Download the following file](#) that contains client migration scripts:

Migration-Scripts.zip

4. Extract the files and follow the instructions in **Prepare-Client.cmd** so that it contains the server name for your AD RMS cluster extranet licensing URL.

To locate this name: From the Active Directory Rights Management Services console, click the cluster name. From the **Cluster Details** information, copy the server name from the **Licensing** value from the extranet cluster URLs section. For example: **rmscluster.contoso.com**.

IMPORTANT

The instructions include replacing example addresses of **adrms.contoso.com** with your AD RMS server addresses. When you do this, be careful that there are no additional spaces before or after your addresses, which will break the migration script and is very hard to identify as the root cause of the problem. Some editing tools automatically add a space after pasting text.

5. Deploy this script to all Windows computers to ensure that when you start to migrate clients, clients yet to be migrated continue to communicate with AD RMS even if they consume content that is protected by migrated clients that are now using the Azure Rights Management service.

You can use Group Policy or another software deployment mechanism to deploy this script.

Step 3. Prepare your Exchange deployment for migration

If you are using Exchange on-premises or Exchange online, you might have previously integrated Exchange with your AD RMS deployment. In this step you will configure them to use the existing AD RMS configuration to support content protected by Azure RMS.

Make sure that you have your [Azure Rights Management service URL for your tenant](#) so that you can substitute this value for <YourTenantURL> in the following commands.

If you have integrated Exchange Online with AD RMS: Open an Exchange Online PowerShell session and run the following PowerShell commands either one by one, or in a script:

```
$irmConfig = Get-IRMConfiguration  
$list = $irmConfig.LicensingLocation  
$list += "<YourTenantURL>/_wmcs/licensing"  
Set-IRMConfiguration -LicensingLocation $list  
Set-IRMConfiguration -internallicensingenabled $false  
Set-IRMConfiguration -internallicensingenabled $true
```

If you have integrated Exchange on-premises with AD RMS: For each Exchange organization, first add registry values on each Exchange server, and then run PowerShell commands:

Registry values for Exchange 2013 and Exchange 2016:

Registry path:

HKLM\SOFTWARE\Microsoft\ExchangeServer\v15\IRM\LicenseServerRedirection

Type: Reg_SZ

Value: https://<Your Tenant URL>/_wmcs/licensing

Data: https://<AD RMS Extranet Licensing URL>/_wmcs/licensing

Registry values For Exchange 2010:

Registry path:

HKLM\SOFTWARE\Microsoft\ExchangeServer\v14\IRM\LicenseServerRedirection

Type: Reg_SZ

Value: https://<Your Tenant URL>/_wmcs/licensing

Data: https://<AD RMS Extranet Licensing URL>/_wmcs/licensing

PowerShell commands to run either one by one, or in a script

```
$irmConfig = Get-IRMConfiguration  
$list = $irmConfig.LicensingLocation  
$list += "<YourTenantURL>/_wmcs/licensing"  
Set-IRMConfiguration -LicensingLocation $list  
Set-IRMConfiguration -internallicensingenabled $false  
Set-IRMConfiguration -RefreshServerCertificates  
Set-IRMConfiguration -internallicensingenabled $true  
IISReset
```

After running these commands for Exchange Online or Exchange on-premises, if your Exchange deployment was configured to support content that was protected by AD RMS, it will also support content protected by Azure RMS after the migration. Your Exchange deployment will continue to use AD RMS to support protected content until a later step in the migration.

Next steps

Go to [phase 2 - server-side configuration](#).

Migration phase 2 - server-side configuration for AD RMS

7/20/2020 • 9 minutes to read • [Edit Online](#)

Applies to: Active Directory Rights Management Services, Azure Information Protection, Office 365

Use the following information for Phase 2 of migrating from AD RMS to Azure Information Protection. These procedures cover steps 4 through 6 from [Migrating from AD RMS to Azure Information Protection](#).

Step 4. Export configuration data from AD RMS and import it to Azure Information Protection

This step is a two-part process:

1. Export the configuration data from AD RMS by exporting the trusted publishing domains (TPDs) to an .xml file. This process is the same for all migrations.
2. Import the configuration data to Azure Information Protection. There are different processes for this step, depending on your current AD RMS deployment configuration and your preferred topology for your Azure RMS tenant key.

Export the configuration data from AD RMS

Do the following procedure on all AD RMS clusters, for all trusted publishing domains that have protected content for your organization. You do not need to run this procedure on licensing-only clusters.

To export the configuration data (trusted publishing domain information)

1. Log on the AD RMS cluster as a user with AD RMS administration permissions.
2. From the AD RMS management console (**Active Directory Rights Management Services**), expand the AD RMS cluster name, expand **Trust Policies**, and then click **Trusted Publishing Domains**.
3. In the results pane, select the trusted publishing domain, and then, from the Actions pane, click **Export Trusted Publishing Domain**.
4. In the **Export Trusted Publishing Domain** dialog box:
 - Click **Save As** and save to path and a file name of your choice. Make sure to specify **.xml** as the file name extension (this is not appended automatically).
 - Specify and confirm a strong password. Remember this password, because you will need it later, when you import the configuration data to Azure Information Protection.
 - Do not select the checkbox to save the trusted domain file in RMS version 1.0.

When you have exported all the trusted publishing domains, you're ready to start the procedure to import this data to Azure Information Protection.

Note that the trusted publishing domains include the Server Licensor Certificate (SLC) keys to decrypt previously protected files, so it's important that you export (and later import into Azure) all the trusted publishing domains and not just the currently active one.

For example, you will have multiple trusted publishing domains if you upgraded your AD RMS servers from Cryptographic Mode 1 to Cryptographic Mode 2. If you do not export and import the trusted publishing domain

that contains your archived key that used Cryptographic Mode 1, at the end of the migration, users will not be able to open content that was protected with the Cryptographic Mode 1 key.

Import the configuration data to Azure Information Protection

The exact procedures for this step depend on your current AD RMS deployment configuration, and your preferred topology for your Azure Information Protection tenant key.

Your current AD RMS deployment is using one of the following configurations for your server licenser certificate (SLC) key:

- Password protection in the AD RMS database. This is the default configuration.
- HSM protection by using a nCipher hardware security module (HSM).
- HSM protection by using a hardware security module (HSM) from a supplier other than nCipher.
- Password protected by using an external cryptographic provider.

NOTE

For more information about using hardware security modules with AD RMS, see [Using AD RMS with Hardware Security Modules](#).

The two Azure Information Protection tenant key topology options are: Microsoft manages your tenant key (**Microsoft-managed**) or you manage your tenant key (**customer-managed**) in Azure Key Vault. When you manage your own Azure Information Protection tenant key, it's sometimes referred to as "bring your own key" (BYOK). For more information, see [Planning and implementing your Azure Information Protection tenant key](#) article.

Use the following table to identify which procedure to use for your migration.

CURRENT AD RMS DEPLOYMENT	CHOSEN AZURE INFORMATION PROTECTION TENANT KEY TOPOLOGY	MIGRATION INSTRUCTIONS
Password protection in the AD RMS database	Microsoft-managed	<p>See the Software-protected key to software-protected key migration procedure after this table.</p> <p>This is the simplest migration path and requires only that you transfer your configuration data to Azure Information Protection.</p>
HSM protection by using a nCipher nShield hardware security module (HSM)	Customer-managed (BYOK)	<p>See the HSM-protected key to HSM-protected key migration procedure after this table.</p> <p>This requires the Azure Key Vault BYOK toolset and three sets of steps to first transfer the key from your on-premises HSM to the Azure Key Vault HSMs, then authorize the Azure Rights Management service from Azure Information Protection to use your tenant key, and finally to transfer your configuration data to Azure Information Protection.</p>

CURRENT AD RMS DEPLOYMENT	CHOSEN AZURE INFORMATION PROTECTION TENANT KEY TOPOLOGY	MIGRATION INSTRUCTIONS
Password protection in the AD RMS database	Customer-managed (BYOK)	<p>See the Software-protected key to HSM-protected key migration procedure after this table.</p> <p>This requires the Azure Key Vault BYOK toolset and four sets of steps to first extract your software key and import it to an on-premises HSM, then transfer the key from your on-premises HSM to the Azure Information Protection HSMs, next transfer your Key Vault data to Azure Information Protection, and finally to transfer your configuration data to Azure Information Protection.</p>
HSM protection by using a hardware security module (HSM) from a supplier other than nCipher	Customer-managed (BYOK)	Contact the supplier for your HSM for instructions how to transfer your key from this HSM to a nCipher nShield hardware security module (HSM). Then follow the instructions for the HSM-protected key to HSM-protected key migration procedure after this table.
Password protected by using an external cryptographic provider	Customer-managed (BYOK)	Contact the supplier for your cryptographic provider for instructions how to transfer your key to a nCipher nShield hardware security module (HSM). Then follow the instructions for the HSM-protected key to HSM-protected key migration procedure after this table.

If you have an HSM-protected key that you cannot export, you can still migrate to Azure Information Protection by configuring your AD RMS cluster for a read-only mode. In this mode, previously protected content can still be opened but newly protected content uses a new tenant key that is managed by you (BYOK) or managed by Microsoft. For more information, see [An update is available for Office to support migrations from AD RMS to Azure RMS](#).

Before you start these key migration procedures, make sure that you can access the .xml files that you created earlier when you exported the trusted publishing domains. For example, these might be saved to a USB thumb drive that you move from the AD RMS server to the internet-connected workstation.

NOTE

However you store these files, use security best practices to protect them because this data includes your private key.

To complete Step 4, choose and select the instructions for your migration path:

- [Software-protected key to software-protected key](#)
- [HSM-protected key to HSM-protected key](#)
- [Software-protected key to HSM-protected key](#)

Step 5. Activate the Azure Rights Management service

Open a PowerShell session and run the following commands:

1. Connect to the Azure Rights Management service and when prompted, specify your global admin credentials:

```
Connect-AipService
```

2. Activate the Azure Rights Management service:

```
Enable-AipService
```

What if your Azure Information Protection tenant is already activated? If the Azure Rights Management service is already activated for your organization, and you have created custom templates that you want to use after the migration, you must export and import these templates. This procedure is covered in the next step.

Step 6. Configure imported templates

Because the templates that you imported have a default state of **Archived**, you must change this state to be **Published** if you want users to be able to use these templates with the Azure Rights Management service.

Templates that you import from AD RMS look and behave just like custom templates that you can create in the Azure portal. To change imported templates to be published so that users can see them and select them from applications, see [Configuring and managing templates for Azure Information Protection](#).

In addition to publishing your newly imported templates, there are just two important changes for the templates that you might need to make before you continue with the migration. For a more consistent experience for users during the migration process, do not make additional changes to the imported templates and do not publish the two default templates that come with Azure Information Protection, or create new templates at this time. Instead, wait until the migration process is complete and you have deprovisioned the AD RMS servers.

The template changes that you might need to make for this step:

- If you created Azure Information Protection custom templates before the migration, you must manually export and import them.
- If your templates in AD RMS used the **ANYONE** group, you might need to manually add users or groups.

In AD RMS, the **ANYONE** group granted rights to all users authenticated by your on-premises Active Directory, and this group is not supported by Azure Information Protection. The closest equivalent is a group that's automatically created for all users in your Azure AD tenant. If you were using the **ANYONE** group for your AD RMS templates, you might need to add users and the rights that you want to grant them.

Procedure if you created custom templates before the migration

If you created custom templates before the migration, either before or after activating the Azure Rights Management service, templates will not be available to users after the migration, even if they were set to **Published**. To make them available to users, you must first do the following:

1. Identify these templates and make a note of their template ID, by running the [Get-AipServiceTemplate](#).
2. Export the templates by using the Azure RMS PowerShell cmdlet, [Export-AipServiceTemplate](#).
3. Import the templates by using the Azure RMS PowerShell cmdlet, [Import-AipServiceTemplate](#).

You can then publish or archive these templates as you would any other template that you create after the migration.

Procedure if your templates in AD RMS used the ANYONE group

If your templates in AD RMS used the ANYONE group, the closest equivalent group in Azure Information Protection is named **AllStaff-7184AB3F-CCD1-46F3-8233-3E09E9CF0E66@<tenant_name>.onmicrosoft.com**. For example, this group might look like the following for Contoso: **AllStaff-7184AB3F-CCD1-46F3-8233-3E09E9CF0E66@contoso.onmicrosoft.com**. This group contains all users from your Azure AD tenant.

When you manage templates and labels in the Azure portal, this group displays as your tenant's domain name in Azure AD. For example, this group might look like the following for Contoso: **contoso.onmicrosoft.com**. To add this group, the option displays **Add <organization name> - All members**.

If you're not sure whether your AD RMS templates include the ANYONE group, you can use the following sample Windows PowerShell script to identify these templates. For more information about using Windows PowerShell with AD RMS, see [Using Windows PowerShell to Administer AD RMS](#).

You can easily add external users to templates when you convert these templates to labels in the Azure portal. Then, on the **Add permissions** pane, choose **Enter details** to manually specify the email addresses for these users.

For more information about this configuration, see [How to configure a label for Rights Management protection](#).

Sample Windows PowerShell script to identify AD RMS templates that include the ANYONE group

This section contains the sample script to help you identify any AD RMS templates that have the ANYONE group defined, as described in the preceding section.

Disclaimer: This sample script is not supported under any Microsoft standard support program or service. This sample script is provided AS IS without warranty of any kind.

```
import-module adrmsadmin

New-PSDrive -Name MyRmsAdmin -PsProvider AdRmsAdmin -Root https://localhost -Force

$ListofTemplates=dir MyRmsAdmin:\RightsPolicyTemplate

foreach($Template in $ListofTemplates)
{
    $templateID=$Template.id

    $rights = dir MyRmsAdmin:\RightsPolicyTemplate\$Templateid\userright

    $templateName=$Template.DefaultDisplayName

    if ($rights.usergroupname -eq "anyone")

    {
        $templateName = $Template.defaultdisplayname

        write-host "Template " -NoNewline

        write-host -NoNewline $templateName -ForegroundColor Red

        write-host " contains rights for " -NoNewline

        write-host ANYONE -ForegroundColor Red
    }
}

Remove-PSDrive MyRmsAdmin -force
```

Next steps

Go to [phase 3 - client-side configuration](#).

Step 2: Software-protected key to software-protected key migration

7/20/2020 • 2 minutes to read • [Edit Online](#)

Applies to: Active Directory Rights Management Services, Azure Information Protection, Office 365

These instructions are part of the [migration path from AD RMS to Azure Information Protection](#), and are applicable only if your AD RMS key is software-protected and you want to migrate to Azure Information Protection with a software-protected tenant key.

If this is not your chosen configuration scenario, go back to [Step 4. Export configuration data from AD RMS and import it to Azure RMS](#) and choose a different configuration.

Use the following procedure to import the AD RMS configuration to Azure Information Protection, to result in your Azure Information Protection tenant key that is managed by Microsoft.

To import the configuration data to Azure Information Protection

1. On an internet-connected workstation, use the [Connect-AipService](#) cmdlet to connect to the Azure Rights Management service:

```
Connect-AipService
```

When prompted, enter your Azure Rights Management tenant administrator credentials (typically, you will use an account that is a global administrator for Azure Active Directory or Office 365).

2. Use the [Import-AipServiceTpd](#) cmdlet to upload each exported trusted publishing domain (.xml) file. For example, you should have at least one additional file to import if you upgraded your AD RMS cluster for Cryptographic Mode 2.

To run this cmdlet, you will need the password that you specified earlier for each configuration data file.

For example, first run the following to store the password:

```
$TPD_Password = Read-Host -AsSecureString
```

Enter the password that you specified to export the first configuration data file. Then, using E:\contosokey1.xml as an example for that configuration file, run the following command and confirm that you want to perform this action:

```
Import-AipServiceTpd -TpDFile E:\contosokey1.xml -ProtectionPassword $TPD_Password -Verbose
```

3. When you have uploaded each file, run [Set-AipServiceKeyProperties](#) to identify the imported key that matches the currently active SLC key in AD RMS. This key will become the active tenant key for your Azure Rights Management service.
4. Use the [Disconnect-AipServiceService](#) cmdlet to disconnect from the Azure Rights Management service:

```
Disconnect-AipServiceService
```

You're now ready to go to [Step 5. Activate the Azure Rights Management service.](#)

Step 2: HSM-protected key to HSM-protected key migration

7/20/2020 • 4 minutes to read • [Edit Online](#)

Applies to: Active Directory Rights Management Services, Azure Information Protection

These instructions are part of the [migration path from AD RMS to Azure Information Protection](#), and are applicable only if your AD RMS key is HSM-protected and you want to migrate to Azure Information Protection with a HSM-protected tenant key in Azure Key Vault.

If this is not your chosen configuration scenario, go back to [Step 4. Export configuration data from AD RMS and import it to Azure RMS](#) and choose a different configuration.

NOTE

These instructions assume your AD RMS key is module-protected. This is the most typical case.

It's a two-part procedure to import your HSM key and AD RMS configuration to Azure Information Protection, to result in your Azure Information Protection tenant key that is managed by you (BYOK).

Because your Azure Information Protection tenant key will be stored and managed by Azure Key Vault, this part of the migration requires administration in Azure Key Vault, in addition to Azure Information Protection. If Azure Key Vault is managed by a different administrator than you for your organization, you must co-ordinate and work with that administrator to complete these procedures.

Before you begin, make sure that your organization has a key vault that has been created in Azure Key Vault, and that it supports HSM-protected keys. Although it's not required, we recommend that you have a dedicated key vault for Azure Information Protection. This key vault will be configured to allow the Azure Rights Management service to access it, so the keys that this key vault stores should be limited to Azure Information Protection keys only.

TIP

If you are doing the configuration steps for Azure Key Vault and you are not familiar with this Azure service, you might find it useful to first review [Get started with Azure Key Vault](#).

Part 1: Transfer your HSM key to Azure Key Vault

These procedures are done by the administrator for Azure Key Vault.

- For each exported SLC key that you want to store in Azure Key Vault, follow the instructions from the Azure Key Vault documentation, using [Implementing bring your own key \(BYOK\) for Azure Key Vault](#) with the following exception:
 - Do not do the steps for **Generate your tenant key**, because you already have the equivalent from your AD RMS deployment. Instead, identify the keys used by your AD RMS server from the nCipher installation and prepare these keys for transfer, and then transfer them to Azure Key Vault.Encrypted key files for nCipher are named **key_<keyAppName>_<keyIdentifier>** locally on the server. For example,

```
C:\Users\All Users\nCipher\Key Management  
Data\local\key_msapi_f829e3d888f6908521fe3d91de51c25d27116a54
```

. You will need the **msapi** value as the keyAppName, and your own value for the key identifier when you run the KeyTransferRemote command to create a copy of the key with reduced permissions.

When the key uploads to Azure Key Vault, you see the properties of the key displayed, which includes the key ID. It will look similar to <https://contosorms-kv.vault.azure.net/keys/contosorms-byok/aaaabbbbcccc111122223333>. Make a note of this URL because the Azure Information Protection administrator needs it to tell the Azure Rights Management service to use this key for its tenant key.

2. On the internet-connected workstation, in a PowerShell session, use the [Set-AzKeyVaultAccessPolicy](#) cmdlet to authorize the Azure Rights Management service principal to access the key vault that will store the Azure Information Protection tenant key. The permissions required are decrypt, encrypt, unwrapkey, wrapkey, verify, and sign.

For example, if the key vault that you have created for Azure Information Protection is named contoso-byok-ky, and your resource group is named contoso-byok-rg, run the following command:

```
Set-AzKeyVaultAccessPolicy -VaultName "contoso-byok-kv" -ResourceGroupName "contoso-byok-rg" -  
ServicePrincipalName 00000012-0000-0000-c000-000000000000 -PermissionsToKeys decrypt,sign,get
```

Now that you've prepared your HSM key in Azure Key Vault for the Azure Rights Management service from Azure Information Protection, you're ready to import your AD RMS configuration data.

Part 2: Import the configuration data to Azure Information Protection

These procedures are done by the administrator for Azure Information Protection.

1. On the internet-connect workstation and in the PowerShell session, connect to the Azure Rights Management service by using the [Connect-AipService](#) cmdlet.

Then upload each trusted publishing domain (.xml) file, by using the [Import-AipServiceTpd](#) cmdlet. For example, you should have at least one additional file to import if you upgraded your AD RMS cluster for Cryptographic Mode 2.

To run this cmdlet, you need the password that you specified earlier for each configuration data file, and the URL for the key that was identified in the previous step.

For example, using a configuration data file of C:\contoso-tpd1.xml and our key URL value from the previous step, first run the following to store the password:

```
$TPD_Password = Read-Host -AsSecureString
```

Enter the password that you specified to export the configuration data file. Then, run the following command and confirm that you want to perform this action:

```
Import-AipServiceTpd -TpdFile "C:\contoso-tpd1.xml" -ProtectionPassword $TPD_Password -KeyVaultKeyUrl  
https://contoso-byok-kv.vault.azure.net/keys/contosorms-byok/aaaabbbbcccc111122223333 -Verbose
```

As part of this import, the SLC key is imported and automatically set as archived.

2. When you have uploaded each file, run [Set-AipServiceKeyProperties](#) to specify which imported key matches the currently active SLC key in your AD RMS cluster. This key becomes the active tenant key for your Azure Rights Management service.

3. Use the [Disconnect-AipServiceService](#) cmdlet to disconnect from the Azure Rights Management service:

```
Disconnect-AipServiceService
```

If you later need to confirm which key your Azure Information Protection tenant key is using in Azure Key Vault, use the [Get-AipServiceKeys](#) Azure RMS cmdlet.

You're now ready to go to [Step 5. Activate the Azure Rights Management service.](#)

Step 2: Software-protected key to HSM-protected key migration

7/20/2020 • 7 minutes to read • [Edit Online](#)

Applies to: Active Directory Rights Management Services, Azure Information Protection

These instructions are part of the [migration path from AD RMS to Azure Information Protection](#), and are applicable only if your AD RMS key is software-protected and you want to migrate to Azure Information Protection with a HSM-protected tenant key in Azure Key Vault.

If this is not your chosen configuration scenario, go back to [Step 4. Export configuration data from AD RMS and import it to Azure RMS](#) and choose a different configuration.

It's a four-part procedure to import the AD RMS configuration to Azure Information Protection, to result in your Azure Information Protection tenant key that is managed by you (BYOK) in Azure Key Vault.

You must first extract your server licensor certificate (SLC) key from the AD RMS configuration data and transfer the key to an on-premises nCipher HSM, next package and transfer your HSM key to Azure Key Vault, then authorize the Azure Rights Management service from Azure Information Protection to access your key vault, and then import the configuration data.

Because your Azure Information Protection tenant key will be stored and managed by Azure Key Vault, this part of the migration requires administration in Azure Key Vault, in addition to Azure Information Protection. If Azure Key Vault is managed by a different administrator than you for your organization, you must co-ordinate and work with that administrator to complete these procedures.

Before you begin, make sure that your organization has a key vault that has been created in Azure Key Vault, and that it supports HSM-protected keys. Although it's not required, we recommend that you have a dedicated key vault for Azure Information Protection. This key vault will be configured to allow the Azure Rights Management service from Azure Information Protection to access it, so the keys that this key vault stores should be limited to Azure Information Protection keys only.

TIP

If you are doing the configuration steps for Azure Key Vault and you are not familiar with this Azure service, you might find it useful to first review [Get started with Azure Key Vault](#).

Part 1: Extract your SLC key from the configuration data and import the key to your on-premises HSM

1. Azure Key Vault administrator: For each exported SLC key that you want to store in Azure Key Vault, use the following steps in the [Implementing bring your own key \(BYOK\) for Azure Key Vault](#) section of the Azure Key Vault documentation:
 - **Generate and transfer your key to Azure Key Vault HSM:** [Step 1: Prepare your internet-connected workstation](#)
 - **Generate and transfer your tenant key – over the internet:** [Step 2: Prepare your disconnected workstation](#)

Do not follow the steps to generate your tenant key, because you already have the equivalent in the exported configuration data (.xml) file. Instead, you will run a tool to extract this key from the file and import it to your on-premises HSM. The tool creates two files when you run it:

- A new configuration data file without the key, which is then ready to be imported to your Azure Information Protection tenant.
 - A PEM file (key container) with the key, which is then ready to be imported to your on-premises HSM.
2. Azure Information Protection administrator or Azure Key Vault administrator: On the disconnected workstation, run the TpdUtil tool from the [Azure RMS migration toolkit](#). For example, if the tool is installed on your E drive where you copy your configuration data file named ContosoTPD.xml:
- ```
E:\TpdUtil.exe /tpd:ContosoTPD.xml /otpd:ContosoTPD.xml /opem:ContosoTPD.pem
```
- If you have more than one RMS configuration data files, run this tool for the remainder of these files.
- To see Help for this tool, which includes a description, usage, and examples, run TpdUtil.exe with no parameters
- Additional information for this command:
- The **/tpd:** specifies the full path and name of the exported AD RMS configuration data file. The full parameter name is **TpdFilePath**.
  - The **/otpd:** specifies the output file name for the configuration data file without the key. The full parameter name is **OutPfxFile**. If you do not specify this parameter, the output file defaults to the original file name with the suffix **\_keyless**, and it is stored in the current folder.
  - The **/opem:** specifies the output file name for the PEM file, which contains the extracted key. The full parameter name is **OutPemFile**. If you do not specify this parameter, the output file defaults to the original file name with the suffix **\_key**, and it is stored in the current folder.
  - If you don't specify the password when you run this command (by using the **TpdPassword** full parameter name or **pwd** short parameter name), you are prompted to specify it.
3. On the same disconnected workstation, attach and configure your nCipher HSM, according to your nCipher documentation. You can now import your key into your attached nCipher HSM by using the following command where you need to substitute your own file name for ContosoTPD.pem:

```
generatekey --import simple pemreadfile=e:\ContosoTPD.pem plainname=ContosoBYOK protect=module ident=contosobyok type=RSA
```

#### NOTE

If you have more than one file, choose the file that corresponds to the HSM key you want to use in Azure RMS to protect content after the migration.

This generates an output display similar to the following:

key generation parameters:

|             |                                      |        |
|-------------|--------------------------------------|--------|
| operation   | Operation to perform                 | import |
| application | Application                          | simple |
| verify      | Verify security of configuration key | yes    |

|                    |                                    |                   |
|--------------------|------------------------------------|-------------------|
| <b>type</b>        | <b>Key type</b>                    | RSA               |
| <b>pemreadfile</b> | <b>PEM file containing RSA key</b> | e:\ContosoTPD.pem |
| <b>ident</b>       | <b>Key identifier</b>              | contosobyok       |
| <b>plainname</b>   | <b>Key name</b>                    | ContosoBYOK       |

Key successfully imported.

Path to key: C:\ProgramData\nCipher\Key Management Data\local\key\_simple\_contosobyok

This output confirms that the private key is now migrated to your on-premises nCipher HSM device with an encrypted copy that is saved to a key (in our example, "key\_simple\_contosobyok").

Now that your SLC key has been extracted and imported to your on-premises HSM, you're ready to package the HSM-protected key and transfer it to Azure Key Vault.

#### IMPORTANT

When you have completed this step, securely erase these PEM files from the disconnected workstation to ensure that they cannot be accessed by unauthorized people. For example, run "cipher /w: E" to securely delete all files from the E: drive.

## Part 2: Package and transfer your HSM key to Azure Key Vault

Azure Key Vault administrator: For each exported SLC key that you want to store in Azure Key vault, use the following steps from the [Implementing bring your own key \(BYOK\) for Azure Key Vault](#) section of the Azure Key Vault documentation:

- [Step 4: Prepare your key for transfer](#)
- [Step 5: Transfer your key to Azure Key Vault](#)

Do not follow the steps to generate your key pair, because you already have the key. Instead, you will run a command to transfer this key (in our example, our KeyIdentifier parameter uses "contosobyok") from your on-premises HSM.

Before you transfer your key to Azure Key Vault, make sure that the KeyTransferRemote.exe utility returns **Result: SUCCESS** when you create a copy of your key with reduced permissions (step 4.1) and when you encrypt your key (step 4.3).

When the key uploads to Azure Key Vault, you see the properties of the key displayed, which includes the key ID. It will look similar to <https://contosorms-kv.vault.azure.net/keys/contosorms-byok/aaaabbbbcccc111122223333>. Make a note of this URL because the Azure Information Protection administrator will need it to tell the Azure Rights Management service from Azure Information Protection to use this key for its tenant key.

Then use the [Set-AzKeyVaultAccessPolicy](#) cmdlet to authorize the Azure Rights Management service principal to access the key vault. The permissions required are decrypt, encrypt, unwrapkey, wrapkey, verify, and sign.

For example, if the key vault that you have created for Azure Information Protection is named contosorms-byok-kv, and your resource group is named contosorms-byok-rg, run the following command:

```
Set-AzKeyVaultAccessPolicy -VaultName "contosorms-byok-kv" -ResourceGroupName "contosorms-byok-rg" -ServicePrincipalName 00000012-0000-0000-c000-000000000000 -PermissionsToKeys decrypt,encrypt,unwrapkey,wrapkey,verify,sign,get
```

Now that you've transferred your HSM key to Azure Key Vault, you're ready to import your AD RMS configuration

data.

## Part 3: Import the configuration data to Azure Information Protection

1. Azure Information Protection administrator: On the internet-connected workstation and in the PowerShell session, copy over your new configuration data files (.xml) that have the SLC key removed after running the TpdUtil tool.
2. Upload each .xml file, by using the [Import-AipServiceTpd](#) cmdlet. For example, you should have at least one additional file to import if you upgraded your AD RMS cluster for Cryptographic Mode 2.

To run this cmdlet, you need the password that you specified earlier for the configuration data file, and the URL for the key that was identified in the previous step.

For example, using a configuration data file of C:\contoso\_keyless.xml and our key URL value from the previous step, first run the following to store the password:

```
$TPD_Password = Read-Host -AsSecureString
```

Enter the password that you specified to export the configuration data file. Then, run the following command and confirm that you want to perform this action:

```
Import-AipServiceTpd -TpDFile "C:\contoso_keyless.xml" -ProtectionPassword $TPD_Password -
KeyVaultStringUrl https://contoso-byok-kv.vault.azure.net/keys/contosorms-byok/aaaabbbbcccc111122223333
-Verbose
```

As part of this import, the SLC key is imported and automatically set as archived.

3. When you have uploaded each file, run [Set-AipServiceKeyProperties](#) to specify which imported key matches the currently active SLC key in your AD RMS cluster.
4. Use the [Disconnect-AipServiceService](#) cmdlet to disconnect from the Azure Rights Management service:

```
Disconnect-AipServiceService
```

If you later need to confirm which key your Azure Information Protection tenant key is using in Azure Key Vault, use the [Get-AipServiceKeys](#) Azure RMS cmdlet.

You're now ready to go to [Step 5. Activate the Azure Rights Management service](#).

# Migration phase 3 - client-side configuration

7/20/2020 • 6 minutes to read • [Edit Online](#)

Applies to: Active Directory Rights Management Services, Azure Information Protection, Office 365

Use the following information for Phase 3 of migrating from AD RMS to Azure Information Protection. These procedures cover step 7 from [Migrating from AD RMS to Azure Information Protection](#).

## Step 7. Reconfigure Windows computers to use Azure Information Protection

For Windows computers that use Office 365 apps, Office 2019, or Office 2016 click-to-run desktop apps:

- You can reconfigure these clients to use Azure Information Protection by using DNS redirection. This is the preferred method for client migration because it is the simplest. However, this method is restricted to Office 2016 (or later) click-to-run desktop apps for Windows computers.

This method requires you to create a new SRV record, and set an NTFS deny permission for users on the AD RMS publishing endpoint.

- For Windows computers that don't use Office 2019 or Office 2016 click-to-run:

You cannot use DNS redirection and instead, must use registry edits. If you have a mix of Office versions that can and cannot use DNS redirection, you can use this single method for all Windows computers, or a combination of DNS redirection and editing the registry.

The registry changes are made easier for you by editing and deploying scripts that you can download.

See the following sections for more information about how to reconfigure Windows clients.

### Client reconfiguration by using DNS redirection

This method is suitable only for Windows clients that run Office 365 apps and Office 2016 (or later) click-to-run desktop apps.

1. Create a DNS SRV record using the following format:

```
_rmsredir._http._tcp.<AD RMS cluster>. <TTL> IN SRV <priority> <weight> <port> <your tenant URL>.
```

For *<AD RMS cluster>*, specify the FQDN of your AD RMS cluster. For example, **rmscluster.contoso.com**.

Alternatively, if you have just one AD RMS cluster in that domain, you can specify just the domain name of the AD RMS cluster. In our example, that would be **contoso.com**. When you specify the domain name in this record, the redirection applies to any and all AD RMS clusters in that domain.

The *<port>* number is ignored.

For *<your tenant URL>*, specify your own [Azure Rights Management service URL for your tenant](#).

If you use the DNS Server role on Windows Server, you can use the following table as an example how to specify the SRV record properties in the DNS Manager console.

| FIELD                      | VALUE                                                 |
|----------------------------|-------------------------------------------------------|
| Domain                     | _tcp.rmscluster.contoso.com                           |
| Service                    | _rmsredir                                             |
| Protocol                   | _http                                                 |
| Priority                   | 0                                                     |
| Weight                     | 0                                                     |
| Port number                | 80                                                    |
| Host offering this service | 5c6bb73b-1038-4eec-863d-49bded473437.rms.na.aadrm.com |

2. Set a deny permission on the AD RMS publishing endpoint for users running Office 365 apps or Office 2016 (or later):
  - a. On one of your AD RMS servers in the cluster, start the Internet Information Services (IIS) Manager console.
  - b. Navigate to Default Web Site and expand \_wmcs.
  - c. Right-click licensing and select Switch to Content View.
  - d. In the details pane, right-click license.asmx > Properties > Edit
  - e. In the Permissions for license.asmx dialog box, either select Users if you want to set redirection for all users, or click Add and then specify a group that contains the users that you want to redirect.

Even if all your users are using a version of Office that supports DNS redirection, you might prefer to initially specify a subset of users for a phased migration.

  - f. For your selected group, select Deny for the Read & Execute and the Read permission, and then click OK twice.
  - g. To confirm this configuration is working as expected, try to connect to the licensing.asmx file directly from a browser. You should see the following error message, which triggers the client running Office 365 apps or Office 2019 or Office 2016 to look for the SRV record:

**Error message 401.3: You do not have permissions to view this directory or page using the credentials you supplied (access denied due to Access Control Lists).**

## Client reconfiguration by using registry edits

This method is suitable for all Windows clients and should be used if they do not run Office 365 apps, or Office 2016 (or later). This method uses two migration scripts to reconfigure AD RMS clients:

- Migrate-Client.cmd
- Migrate-User.cmd

The client configuration script (Migrate-Client.cmd) configures computer-level settings in the registry, which means that it must run in a security context that can make those changes. This typically means one of the following methods:

- Use group policy to run the script as a computer startup script.
- Use group policy software installation to assign the script to the computer.
- Use a software deployment solution to deploy the script to the computers. For example, use System Center Configuration Manager [packages and programs](#). In the properties of the package and program, under **Run mode**, specify that the script runs with administrative permissions on the device.
- Use a logon script if the user has local administrator privileges.

The user configuration script (Migrate-User.cmd) configures user-level settings and cleans up the client license store. This means that this script must run in the context of the actual user. For example:

- Use a logon script.
- Use group policy software installation to publish the script for the user to run.
- Use a software deployment solution to deploy the script to the users. For example, use System Center Configuration Manager [packages and programs](#). In the properties of the package and program, under **Run mode**, specify that the script runs with the permissions of the user.
- Ask the user to run the script when they are signed in to their computer.

The two scripts include a version number and do not rerun until this version number is changed. This means that you can leave the scripts in place until the migration is complete. However, if you do make changes to the scripts that you want computers and users to rerun on their Windows computers, update the following line in both scripts to a higher value:

```
SET Version=20170427
```

The user configuration script is designed to run after the client configuration script, and uses the version number in this check. It stops if the client configuration script with the same version has not run. This check ensures that the two scripts run in the right sequence.

When you cannot migrate all your Windows clients at once, run the following procedures for batches of clients. For each user who has a Windows computer that you want to migrate in your batch, add the user to the **AIPMigrated** group that you created earlier.

### **Modifying the scripts for registry edits**

1. Return to the migration scripts, **Migrate-Client.cmd** and **Migrate-User.cmd**, which you extracted previously when you downloaded these scripts in the [preparation phase](#).
2. Follow the instructions in **Migrate-Client.cmd** to modify the script so that it contains your tenant's Azure Rights Management service URL, and also your server names for your AD RMS cluster extranet licensing URL and intranet licensing URL. Then, increment the script version, which was previously explained. A good practice for tracking script versions is to use today's date in the following format: YYYYMMDD

#### **IMPORTANT**

As before, be careful not to introduce additional spaces before or after your addresses.

In addition, if your AD RMS servers use SSL/TLS server certificates, check whether the licensing URL values include the port number 443 in the string. For example: [https://rms.treyresearch.net:443/\\_wmcs/licensing](https://rms.treyresearch.net:443/_wmcs/licensing). You can find this information in the Active Directory Rights Management Services console when you click the cluster name and view the **Cluster Details** information. If you see the port number 443 included in the URL, include this value when you modify the script. For example, <https://rms.treyresearch.net:443>.

If you need to retrieve your Azure Rights Management service URL for <YourTenantURL>, refer back to [To identify your Azure Rights Management service URL](#).

3. Using the instructions at the beginning of this step, configure your script deployment methods to run **Migrate-Client.cmd** and **Migrate-User.cmd** on the Windows client computers that are used by the members of the AIPMigrated group.

## Next steps

To continue the migration, go to [phase 4 -supporting services configuration](#).

# Migration phase 4 - supporting services configuration

7/20/2020 • 6 minutes to read • [Edit Online](#)

*Applies to: Active Directory Rights Management Services, Azure Information Protection, Office 365*

Use the following information for Phase 4 of migrating from AD RMS to Azure Information Protection. These procedures cover steps 8 through 9 from [Migrating from AD RMS to Azure Information Protection](#).

## Step 8. Configure IRM integration for Exchange Online

### IMPORTANT

Because you cannot control which recipients migrated users might select for protected emails, make sure that all users and mail-enabled groups in your organization have an account in Azure AD that can be used with Azure Information Protection.

[More information](#)

Independently from the Azure Information Protection tenant key topology that you chose, do the following:

1. For Exchange Online to be able to decrypt emails that are protected by AD RMS, it needs to know that the AD RMS URL for your cluster corresponds to the key that's available in your tenant. This is done with the DNS SRV record for your AD RMS cluster that is also used to reconfigure Office clients to use Azure Information Protection. If you did not create the DNS SRV record for client reconfiguration in step 7, create this record now to support Exchange Online. [Instructions](#)

When this DNS record is in place, users using Outlook on the web and mobile email clients will be able to view AD RMS protected emails in those apps, and Exchange will be able to use the key you imported from AD RMS to decrypt, index, journal, and protect content that has been protected by AD RMS.

2. Run the Exchange Online [Get-IRMConfiguration](#) command. If you need help running this command, see the step-by-step instructions from [Exchange Online: IRM Configuration](#).

From the output, check whether **AzureRMSLicensingEnabled** is set to **True**:

- If **AzureRMSLicensingEnabled** is set to **True**, no further configuration is needed for this step.
- If **AzureRMSLicensingEnabled** is set **False**, run `Set-IRMConfiguration -AzureRMSLicensingEnabled $true` and then use the verification steps from [Set up new Office 365 Message Encryption capabilities built on top of Azure Information Protection](#) to confirm that Exchange Online is now ready to use the Azure Rights Management service.

## Step 9. Configure IRM integration for Exchange Server and SharePoint Server

If you have used the Information Rights Management (IRM) functionality of Exchange Server or SharePoint Server with AD RMS, you will need to deploy the Rights Management (RMS) connector, which acts as a communications interface (a relay) between your on-premises servers and the protection service for Azure Information Protection.

This step covers installing and configuring the connector, disabling IRM for Exchange and SharePoint, and configuring these servers to use the connector. Finally, if you have imported AD RMS data configuration files (.xml)

into Azure Information Protection that were used to protect email messages, you must manually edit the registry on the Exchange Server computers to redirect all trusted publishing domain URLs to the RMS connector.

**NOTE**

Before you start, check the versions of the on-premises servers that the Azure Rights Management service supports, from [On-premises servers that support Azure RMS](#).

## Install and configure the RMS connector

Use the instructions in the [Deploying the Azure Rights Management connector](#) article, and do steps 1 though 4. Do not start step 5 yet from the connector instructions.

## Disable IRM on Exchange Servers and remove AD RMS configuration

**IMPORTANT**

If you haven't yet configured IRM on any of your Exchange servers, do just steps 2 and 6.

Do all these steps if all the licensing URLs of all your AD RMS clusters are not displayed in the *LicensingLocation* parameter when you run [Get-IRMConfiguration](#).

1. On each Exchange server, locate the following folder and delete all the entries in that folder:  
`\ProgramData\Microsoft\DRM\Server\S-1-5-18`
2. From one of the Exchange servers, run the following PowerShell commands to ensure that users will be able to read emails that are protected by using Azure Rights Management.

Before you run these commands, substitute your own Azure Rights Management service URL for *<Your Tenant URL>*.

```
$irmConfig = Get-IRMConfiguration
$list = $irmConfig.LicensingLocation
$list += "<Your Tenant URL>/_wmcs/licensing"
Set-IRMConfiguration -LicensingLocation $list
```

Now when you run [Get-IRMConfiguration](#), you should see all your AD RMS cluster licensing URLs and your Azure Rights Management service URL displayed for the *LicensingLocation* parameter.

3. Now disable IRM features for messages that are sent to internal recipients:

```
Set-IRMConfiguration -InternalLicensingEnabled $false
```

4. Then use the same cmdlet to disable IRM in Microsoft Office Outlook Web App and in Microsoft Exchange ActiveSync:

```
Set-IRMConfiguration -ClientAccessServerEnabled $false
```

5. Finally, use the same cmdlet to clear any cached certificates:

```
Set-IRMConfiguration -RefreshServerCertificates
```

6. On each Exchange Server, now reset IIS, for example, by running a command prompt as an administrator and typing `iisreset`.

## **Disable IRM on SharePoint Servers and remove AD RMS configuration**

1. Make sure that there are no documents checked out from RMS-protected libraries. If there are, they will become inaccessible at the end of this procedure.
2. On the SharePoint Central Administration Web site, in the **Quick Launch** section, click **Security**.
3. On the **Security** page, in the **Information Policy** section, click **Configure information rights management**.
4. On the **Information Rights Management** page, in the **Information Rights Management** section, select **Do not use IRM on this server**, then click **OK**.
5. On each of the SharePoint Server computers, delete the contents of the folder `\ProgramData\Microsoft\MSIPC\Server\<SID of the account running SharePoint Server>`.

## **Configure Exchange and SharePoint to use the connector**

1. Return to the instructions for deploying the RMS connector: [Step 5: Configuring servers to use the RMS connector](#)

If you have SharePoint Server only, go straight to [Next steps](#) to continue the migration.

2. On each Exchange Server, manually add the registry keys in the next section for each configuration data file (.xml) that you imported, to redirect the trusted publishing domain URLs to the RMS connector. These registry entries are specific to migration and are not added by the server configuration tool for Microsoft RMS connector.

When you make these registry edits, use the following instructions:

- Replace *connector FQDN* with the name that you defined in DNS for the connector. For example, `rmsconnector.contoso.com`.
- Use the HTTP or HTTPS prefix for the connector URL, depending on whether you have configured the connector to use HTTP or HTTPS to communicate with your on-premises servers.

### **Registry edits for Exchange**

For all Exchange servers, add the following registry values to LicenseServerRedirection, depending on your versions of Exchange:

---

For Exchange 2013 and Exchange 2016 - registry edit 1:

**Registry path:**

`HKLM\SOFTWARE\Microsoft\ExchangeServer\v15\IRM\LicenseServerRedirection`

**Type:** Reg\_SZ

**Value:** `https://<AD RMS Intranet Licensing URL>/_wmcs/licensing`

**Data:**

One of the following, depending on whether you are using HTTP or HTTPS from your Exchange server to the RMS connector:

- `http://<connector FQDN>/_wmcs/licensing`
- `https://<connector FQDN>/_wmcs/licensing`

---

Exchange 2013 - registry edit 2:

**Registry path:**

HKLM\SOFTWARE\Microsoft\ExchangeServer\v15\IRM\LicenseServerRedirection

**Type:** Reg\_SZ

**Value:** https://<AD RMS Extranet Licensing URL>/\_wmcs/licensing

**Data:**

One of the following, depending on whether you are using HTTP or HTTPS from your Exchange server to the RMS connector:

- http://<connector FQDN>/\_wmcs/licensing
- https://<connector FQDN>/\_wmcs/licensing

---

For Exchange 2010 - registry edit 1:

**Registry path:**

HKLM\SOFTWARE\Microsoft\ExchangeServer\v14\IRM\LicenseServerRedirection

**Type:** Reg\_SZ

**Value:** https://<AD RMS Intranet Licensing URL>/\_wmcs/licensing

**Data:**

One of the following, depending on whether you are using HTTP or HTTPS from your Exchange server to the RMS connector:

- http://<connector FQDN>/\_wmcs/licensing
- https://<connector Name>/\_wmcs/licensing

---

For Exchange 2010 - registry edit 2:

**Registry path:**

HKLM\SOFTWARE\Microsoft\ExchangeServer\v14\IRM\LicenseServerRedirection

**Type:** Reg\_SZ

**Value:** https://<AD RMS Extranet Licensing URL>/\_wmcs/licensing

**Data:**

One of the following, depending on whether you are using HTTP or HTTPS from your Exchange server to the RMS connector:

- http://<connector FQDN>/\_wmcs/licensing
- https://<connector FQDN>/\_wmcs/licensing

---

## Next steps

To continue the migration, go to [phase 5 -post migration tasks](#).

# Migration phase 5 - post migration tasks

7/20/2020 • 6 minutes to read • [Edit Online](#)

*Applies to: Active Directory Rights Management Services, Azure Information Protection, Office 365*

Use the following information for Phase 5 of migrating from AD RMS to Azure Information Protection. These procedures cover steps 10 through 12 from [Migrating from AD RMS to Azure Information Protection](#).

## Step 10. Deprovision AD RMS

Remove the Service Connection Point (SCP) from Active Directory to prevent computers from discovering your on-premises Rights Management infrastructure. This is optional for the existing clients that you migrated because of the redirection that you configured in the registry (for example, by running the migration script). However, removing the SCP prevents new clients and potentially RMS-related services and tools from finding the SCP when the migration is complete. At this point, all computer connections should go to the Azure Rights Management service.

To remove the SCP, make sure that you are logged in as a domain enterprise administrator, and then use the following procedure:

1. In the Active Directory Rights Management Services console, right-click the AD RMS cluster, and then click **Properties**.
2. Click the **SCP** tab.
3. Select the **Change SCP** check box.
4. Select **Remove Current SCP**, and then click **OK**.

Now monitor your AD RMS servers for activity. For example, check the [requests in the System Health report](#), the [ServiceRequest table](#) or [audit user access to protected content](#).

When you have confirmed that RMS clients are no longer communicating with these servers and that clients are successfully using Azure Information Protection, you can remove the AD RMS server role from these servers. If you're using dedicated servers, you might prefer the cautionary step of first shutting down the servers for a period of time. This gives you time to make sure that there are no reported problems that might require you to restart these servers for service continuity while you investigate why clients are not using Azure Information Protection.

After you have deprovisioned your AD RMS servers, you might want to take the opportunity to review your templates in the Azure portal. For example, convert them to labels, consolidate them so that users have fewer to choose between, or reconfigure them. This would be also a good time to publish the default templates. For more information, see [Configuring and managing templates for Azure Information Protection](#).

### IMPORTANT

At the end of this migration, your AD RMS cluster cannot be used with Azure Information Protection and the hold your own key (HYOK) option. If you decide to use HYOK for an Azure Information Protection label, because of the redirections that are now in place, the AD RMS cluster that you use must have different licensing URLs to the ones in the clusters that you migrated.

### Addition configuration for computers that run Office 2010

If migrated clients run Office 2010, users might experience delays in opening protected content after our AD RMS

servers are deprovisioned. Or, users might see messages that they don't have credentials to open protected content. To resolve these problems, create a network redirection for these computers, which redirects the AD RMS URL FQDN to the local IP address of the computer (127.0.0.1). You can do this by configuring the local hosts file on each computer, or by using DNS.

Redirection via local hosts file:

- Add the following line in the local hosts file, replacing <AD RMS URL FQDN> with the value for your AD RMS cluster, without prefixes or web pages:

```
127.0.0.1 <AD RMS URL FQDN>
```

Redirection via DNS:

- Create a new host (A) record for your AD RMS URL FQDN, which has the IP address of 127.0.0.1.

## Step 11. Complete client migration tasks

For mobile device clients and Mac computers: Remove the DNS SRV records that you created when you deployed the [AD RMS mobile device extension](#).

When these DNS changes have propagated, these clients will automatically discover and start to use the Azure Rights Management service. However, Mac computers that run Office Mac cache the information from AD RMS. For these computers, this process can take up to 30 days.

To force Mac computers to run the discovery process immediately, in the keychain, search for "adal" and delete all ADAL entries. Then, run the following commands on these computers:

```
rm -r ~/Library/Cache/MSRightsManagement
rm -r ~/Library/Caches/com.microsoft.RMS-XPCService
rm -r ~/Library/Caches/Microsoft\ Rights\ Management\ Services
rm -r ~/Library/Containers/com.microsoft.RMS-XPCService
rm -r ~/Library/Containers/com.microsoft.RMSTestApp
rm ~/Library/Group\ Containers/UBF8T346G9.Office/DRM.plist
killall cfprefsd
```

When all your existing Windows computers have migrated to Azure Information Protection, there's no reason to continue to use onboarding controls and maintain the **AIPMigrated** group that you created for the migration process.

Remove the onboarding controls first, and then you can delete the **AIPMigrated** group and any software deployment method that you created to deploy the migration scripts.

To remove the onboarding controls:

1. In a PowerShell session, connect to the Azure Rights Management service and when prompted, specify your global admin credentials:

```
Connect-AipService
```

- Run the following command, and enter Y to confirm:

```
Set-AipServiceOnboardingControlPolicy -UseRmsUserLicense $False
```

Note that this command removes any license enforcement for the Azure Rights Management protection service, so that all computers can protect documents and emails.

- Confirm that onboarding controls are no longer set:

```
Get-AipServiceOnboardingControlPolicy
```

In the output, **License** should show **False**, and there is no GUID displayed for the **SecurityGroupId**.

Finally, if you are using Office 2010 and you have enabled the **AD RMS Rights Policy Template Management (Automated)** task in the Windows Task Scheduler library, disable this task because it is not used by the Azure Information Protection client. This task is typically enabled by using group policy and supports an AD RMS deployment. You can find this task in the following location: **Microsoft > Windows > Active Directory Rights Management Services Client**

## Step 12. Rekey your Azure Information Protection tenant key

This step is required when migration is complete if your AD RMS deployment was using RMS Cryptographic Mode 1 because this mode uses a 1024-bit key and SHA-1. This configuration is considered to offer an inadequate level of protection. Microsoft doesn't endorse the use of lower key lengths such as 1024-bit RSA keys and the associated use of protocols that offer inadequate levels of protection, such as SHA-1.

Rekeying results in protection that uses RMS Cryptographic Mode 2, which results in a 2048-bit key and SHA-256.

Even if your AD RMS deployment was using Cryptographic Mode 2, we still recommend you do this step because a new key helps to protect your tenant from potential security breaches to your AD RMS key.

When you rekey your Azure Information Protection tenant key (also known as "rolling your key"), the currently active key is archived and Azure Information Protection starts to use a different key that you specify. This different key could be a new key that you create in Azure Key Vault, or the default key that was automatically created for your tenant.

Moving from one key to another doesn't happen immediately but over a few weeks. Because it's not immediate, do not wait until you suspect a breach to your original key but do this step as soon as the migration is complete.

To rekey your Azure Information Protection tenant key:

- If your tenant key is managed by Microsoft: Run the PowerShell cmdlet [Set-AipServiceKeyProperties](#) and specify the key identifier for the key that was automatically created for your tenant. You can identify the value to specify by running the [Get-AipServiceKeys](#) cmdlet. The key that was automatically created for your tenant has the oldest creation date, so you can identify it by using the following command:

```
(Get-AipServiceKeys) | Sort-Object CreationTime | Select-Object -First 1
```

- If your tenant key is managed by you (BYOK): In Azure Key Vault, repeat your key creation process for your Azure Information Protection tenant, and then run the [Use-AipServiceKeyVaultKey](#) cmdlet again to specify the URL for this new key.

For more information about managing your Azure Information Protection tenant key, see [Operations for your Azure Information Protection tenant key](#).

## Next steps

Now that you have completed the migration, review the [deployment roadmap](#) to identify any other deployment tasks that you might need to do.

# Planning and implementing your Azure Information Protection tenant key

7/20/2020 • 13 minutes to read • [Edit Online](#)

Applies to: [Azure Information Protection](#), [Office 365](#)

Use the information in this article to help you plan for and manage your Azure Information Protection tenant key. For example, instead of Microsoft managing your tenant key (the default), you might want to manage your own tenant key to comply with specific regulations that apply to your organization. Managing your own tenant key is also referred to as bring your own key, or BYOK.

What is the Azure Information Protection tenant key?

- The Azure Information Protection tenant key is a root key for your organization. Other keys can be derived from this root key, such as user keys, computer keys, and document encryption keys. Whenever Azure Information Protection uses these keys for your organization, they cryptographically chain to your Azure Information Protection tenant key.
- The Azure Information Protection tenant key is the online equivalent of the Server Licensor Certificate (SLC) key from Active Directory Rights Management Services (AD RMS).

**At a glance:** Use the following table as a quick guide to your recommended tenant key topology. Then, use the additional documentation for more information.

| BUSINESS REQUIREMENT                                                                                                                                                                                                                                   | RECOMMENDED TENANT KEY TOPOLOGY |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------|
| Deploy Azure Information Protection quickly and without special hardware, additional software, or an Azure subscription.<br><br>For example: Testing environments and when your organization does not have regulatory requirements for key management. | Managed by Microsoft            |
| Compliance regulations and control over all life cycle operations.<br><br>For example: Your key must be protected by a hardware security module (HSM).                                                                                                 | BYOK                            |

If required, you can change your tenant key topology after deployment, by using the [Set-AipServiceKeyProperties](#) cmdlet.

## Choose your tenant key topology: Managed by Microsoft (the default) or managed by you (BYOK)

Decide which tenant key topology is best for your organization:

- **Managed by Microsoft:** Microsoft automatically generates a tenant key for your organization and this key is used exclusively for Azure Information Protection. By default, Microsoft uses this key for your tenant and manages most aspects of your tenant key life cycle.

This is the simplest option with the lowest administrative overheads. In most cases, you do not even need to know that you have a tenant key. You just sign up for Azure Information Protection and the rest of the key management process is handled by Microsoft.

- **Managed by you (BYOK):** For complete control over your tenant key, use [Azure Key Vault](#) with Azure Information Protection. For this tenant key topology, you create the key, either directly in Key Vault, or create it on-premises. If you create it on-premises, you next transfer or import this key into Key Vault. You then configure Azure Information Protection to use this key, and you manage it in Azure Key Vault.

## More information about BYOK

To create your own key, you have the following options:

- **A key that you create on-premises and transfer or import to Key Vault:**
  - An HSM-protected key that you create on-premises and transfer to Key Vault as an HSM-protected key.
  - A software-protected key that you create on-premises, convert, and then transfer to Key Vault as an HSM-protected key. This option is supported only when you [migrate from Active Directory Rights Management Services \(AD RMS\)](#).
  - A software-protected key that you create on-premises and import to Key Vault as a software-protected key. This option requires a .PFX certificate file.
- **A key that you create in Key Vault:**
  - An HSM-protected key that you create in Key Vault.
  - A software-protected key that you create in Key Vault.

Of these BYOK options, the most typical is an HSM-protected key that you create on-premises and transfer to Key Vault as an HSM-protected key. Although this option has the greatest administrative overheads, it might be required for your organization to comply with specific regulations. The HSMs that are used by Azure Key Vault are FIPS 140-2 Level 2 validated.

With this option, the following happens:

1. You generate your tenant key on your premises, in line with your IT policies and security policies. This key is the master copy. It remains on-premises and you are responsible for backing it up.
2. You create a copy of this key, and securely transfer this copy from your HSM to Azure Key Vault. Throughout this process, the master copy of this key never leaves the hardware protection boundary.
3. The copy of the key is protected by Azure Key Vault.

### NOTE

As an additional protection measure, Azure Key Vault uses separate security domains for its data centers in regions such as North America, EMEA (Europe, Middle East and Africa), and Asia. Azure Key Vault also uses different instances of Azure, such as Microsoft Azure Germany, and Azure Government.

Although it's optional, you will also probably want to use the near real-time usage logs from Azure Information Protection to see exactly how and when your tenant key is being used.

When you use BYOK for your Azure Information Protection tenant key, you can't export your trusted publishing domain (TPD). The TPD is needed if you decide to no longer use Azure Information Protection but must still be able to decrypt content that was protected by Azure Information Protection. To prepare for this scenario by creating a suitable TPD ahead of time, see the following instructions [How to prepare an Azure Information](#)

Protection "Cloud Exit" plan.

## When you have decided your tenant key topology

If you decide to let Microsoft manage your tenant key:

- Unless you are migrating from AD RMS, no further action is required for you to generate the key for your tenant and you can go straight to [Next steps](#).
- If you currently have AD RMS and want to migrate to Azure Information Protection, use the migration instructions: [Migrating from AD RMS to Azure Information Protection](#).

If you decide to manage your tenant key yourself, read the following sections for more information.

## Implementing BYOK for your Azure Information Protection tenant key

Use the information and procedures in this section if you have decided to generate and manage your tenant key; the bring your own key (BYOK) scenario:

### NOTE

If you have started to use Azure Information Protection with a tenant key that is managed by Microsoft and you now want to manage your tenant key (move to BYOK), your previously protected documents and emails will remain accessible by using an archived key.

### Prerequisites for BYOK

See the following table for a list of prerequisites for bring your own key (BYOK).

| REQUIREMENT                                                                                                                                                                                                                                              | MORE INFORMATION                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Your Azure Information Protection tenant must have an Azure subscription. If you do not have one, you can sign up for a <a href="#">free account</a>.</p> <p>To use an HSM-protected key, you must have the Azure Key Vault Premium service tier.</p> | <p>The free Azure subscription that provides access to configure Azure Active Directory and configuration of Azure Rights Management custom templates (<a href="#">Access to Azure Active Directory</a>) is not sufficient to use Azure Key Vault. To confirm that you have an Azure subscription that you can use for BYOK, use <a href="#">Azure PowerShell</a> cmdlets:</p> <ol style="list-style-type: none"><li>Start an Azure PowerShell session with the <b>Run as administrator</b> option, and sign in as a global admin for your Azure Information Protection tenant by using <code>Connect-AzAccount</code> and then copy and paste the resulting token string into <code>https://microsoft.com/devicelogin</code> by using a browser.<br/>For more information, see <a href="#">Sign in with Azure PowerShell</a>.</li><li>Type the following and confirm that you see values displayed for your subscription name and ID, your Azure Information Protection tenant ID, and that the state is enabled: <code>Get-AzSubscription</code><br/>If no values are displayed and you are just returned to the prompt, you do not have an Azure subscription that can be used for BYOK.</li></ol> <p><b>Note:</b> In addition to the BYOK prerequisites, if you are migrating from AD RMS to Azure Information Protection by using software key to hardware key, you must have a minimum version of 11.62 if you are using Thales firmware for your HSM.</p> |

| Requirement                                                                                                                                                                | More Information                                                                                                                                                                                                                                                                                                                              |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| To use an HSM-protected key that you create on-premises:<br><br>- All the prerequisites listed for Key Vault BYOK.                                                         | See <a href="#">Prerequisites for BYOK</a> from the Azure Key Vault documentation.<br><br><b>Note:</b> In addition to the BYOK prerequisites, if you are migrating from AD RMS to Azure Information Protection by using software key to hardware key, you must have a minimum version of 11.62 if you are using Thales firmware for your HSM. |
| If the key vault to contain your tenant key uses Virtual Network Service Endpoints for Azure Key Vault:<br><br>- Allow trusted Microsoft services to bypass this firewall. | For more information, see <a href="#">Virtual Network Service Endpoints for Azure Key Vault</a> .                                                                                                                                                                                                                                             |
| The AIPService PowerShell module for Azure Information Protection.                                                                                                         | For installation instructions, see <a href="#">Installing the AIPService PowerShell module</a> .                                                                                                                                                                                                                                              |

For more information about nCipher nShield hardware security module (HSM) and how they are used with Azure Key Vault, see the [nCipher website](#).

### Choosing your key vault location

When you create a key vault to contain the key to be used as your tenant key for Azure Information, you must specify a location. This location is an Azure region, or Azure instance.

Make your choice first for compliance, and then to minimize network latency:

- If you have chosen the BYOK key topology for compliance reasons, those compliance requirements might mandate the Azure region or Azure instance that stores your Azure Information Protection tenant key.
- Because all cryptographic calls for protection chain to your Azure Information Protection tenant key, you want to minimize the network latency that these calls incur. To do that, create your key vault in the same Azure region or instance as your Azure Information Protection tenant.

To identify the location of your Azure Information Protection tenant, use the [Get-AipServiceConfiguration](#) PowerShell cmdlet and identify the region from the URLs. For example:

```
LicensingIntranetDistributionPointUrl : https://5c6bb73b-1038-4eec-863d-49bded473437.rms.na.aadrm.com/_wmcs/licensing
```

The region is identifiable from [rms.na.aadrm.com](https://rms.na.aadrm.com), and for this example, it is in North America.

Use the following table to identify which Azure region or instance is recommended to minimize network latency.

| Azure Region or Instance | Recommended Location for Your Key Vault |
|--------------------------|-----------------------------------------|
| rms.na.aadrm.com         | North Central US or East US             |
| rms.eu.aadrm.com         | North Europe or West Europe             |
| rms.ap.aadrm.com         | East Asia or Southeast Asia             |
| rms.sa.aadrm.com         | West US or East US                      |
| rms.govus.aadrm.com      | Central US or East US 2                 |

| AZURE REGION OR INSTANCE | RECOMMENDED LOCATION FOR YOUR KEY VAULT |
|--------------------------|-----------------------------------------|
| rms.aadrm.us             | US Gov Virginia or US Gov Arizona       |
| rms.aadrm.cn             | China East 2 or China North 2           |

## Instructions for BYOK

Use the Azure Key Vault documentation to create a key vault and the key that you want to use for Azure Information Protection. For example, see [Get started with Azure Key Vault](#).

Make sure that the key length is 2048 bits (recommended) or 1024 bits. Other key lengths are not supported by Azure Information Protection.

Don't use a 1024-bit key as your active tenant key because it is considered to offer an inadequate level of protection. Microsoft doesn't endorse the use of lower key lengths such as 1024-bit RSA keys and the associated use of protocols that offer inadequate levels of protection, such as SHA-1. We recommend moving to a higher key length.

To create an HSM-protected key on-premises and transfer it to your key vault as an HSM-protected key, follow the procedures in [How to generate and transfer HSM-protected keys for Azure Key Vault](#).

For Azure Information Protection to use the key, all Key Vault operations must be permitted for the key. This is the default configuration and the operations are encrypt, decrypt, wrapKey, unwrapKey, sign, and verify. You can check the permitted operations of a key by using the following PowerShell command:

```
(Get-AzKeyVaultKey -VaultName <key vault name> -Name <key name>).Attributes.KeyOps
```

If necessary, add permitted operations by using [Update-AzKeyVaultKey](#) and the *KeyOps* parameter.

A key that is stored in Key Vault has a key ID. This key ID is a URL that contains the name of the key vault, the keys container, the name of the key, and the key version. For example: <https://contosorms-kv.vault.azure.net/keys/contosorms-byok/aaaabbccccc111122223333>. You must configure Azure Information Protection to use this key, by specifying its key vault URL.

Before Azure Information Protection can use the key, the Azure Rights Management service must be authorized to use the key in your organization's key vault. To do this, the Azure Key Vault administrator can use the Azure portal, or Azure PowerShell:

Configuration by using the Azure portal:

1. Navigate to **Key vaults** > <*your key vault name*> > **Access policies** > **Add new**.
2. From the **Add access policy** pane, select **Azure Information Protection BYOK** from the **Configure from template (optional)** list box, and click **OK**.

The selected template has the following configuration:

- **Microsoft Rights Management Services** is automatically assigned for **Select principal**.
- **Get, Decrypt, and Sign** is automatically selected for the key permissions.

Configuration by using PowerShell:

- Run the Key Vault PowerShell cmdlet, [Set-AzKeyVaultAccessPolicy](#), and grant permissions to the Azure Rights Management service principal, by using the GUID 00000012-0000-0000-c000-000000000000. For example:

```
Set-AzKeyVaultAccessPolicy -VaultName 'ContosoRMS-kv' -ResourceGroupName 'ContosoRMS-byok-rg' -ServicePrincipalName 00000012-0000-0000-c000-000000000000 -PermissionsToKeys decrypt,sign,get
```

You're now ready to configure Azure Information Protection to use this key as your organization's Azure Information Protection tenant key. Using Azure RMS cmdlets, first connect to the Azure Rights Management service and sign in:

```
Connect-AipService
```

Then run the [Use-AipServiceKeyVaultKey cmdlet](#), specifying the key URL. For example:

```
Use-AipServiceKeyVaultKey -KeyVaultKeyId "https://contosorms-kv.vault.azure.net/keys/contosorms-byok/aaaabbbbcccc111122223333"
```

#### IMPORTANT

In this example, "aaaabbbbcccc111122223333" is the version of the key to use. If you do not specify the version, the current version of the key is used without warning and the command appears to work. However, if your key in Key Vault is later updated (renewed), the Azure Rights Management service will stop working for your tenant, even if you run the Use-AipServiceKeyVaultKey command again.

Make sure that you specify the key version, in addition to the key name when you run this command. You can use the Azure Key Vault cmd, [Get-AzKeyVaultKey](#), to get the version number of the current key. For example:

```
Get-AzKeyVaultKey -VaultName 'contosorms-kv' -KeyName 'contosorms-byok'
```

If you need to confirm that the key URL is set correctly for Azure Information Protection: In Azure Key Vault, run [Get-AzKeyVaultKey](#) to see the key URL.

Finally, if the Azure Rights Management service is already activated, run [Set-AipServiceKeyProperties](#) to tell Azure Information Protection to use this key as the active tenant key for the Azure Rights Management service. If you do not do this step, Azure Information Protection will continue to use the default Microsoft-managed key that was automatically created for your tenant.

## Next steps

Now that you've planned for and if necessary, created and configured your tenant key, do the following:

1. Start to use your tenant key:

- If the protection service isn't already activated, you must now activate the Rights Management service so that your organization can start to use Azure Information Protection. Users immediately start to use your tenant key (managed by Microsoft, or managed by you in Azure Key Vault).

For more information about activation, see [Activating the protection service from Azure Information Protection](#).

- If the Rights Management service was already activated and then you decided to manage your own tenant key, users gradually transition from the old tenant key to the new tenant key. This staggered transition can take a few weeks to complete. Documents and files that were protected with the old tenant key remains accessible to authorized users.

2. Consider using usage logging, which logs every transaction that the Azure Rights Management service performs.

If you decided to manage your own tenant key, logging includes information about using your tenant key. See the following snippet from a log file displayed in Excel where the **KeyVaultDecryptRequest** and **KeyVaultSignRequest** request types show that the tenant key is being used.

| date      | time     | row-id      | request-type           | user-id                | result    | correlation-id    |
|-----------|----------|-------------|------------------------|------------------------|-----------|-------------------|
| 7/18/2016 | 17:41:39 | -           | KeyVaultDecryptRequest | "                      | 'Success' | b9e063ac-6208-4d2 |
| 7/17/2016 | 02:22:51 | 76445a86-3d | AcquireTemplates       | -                      | 'Success' | b01bc442-cde2-41e |
| 7/18/2016 | 17:41:40 | -           | KeyVaultSignRequest    | "                      | 'Success' | b9e063ac-6208-4d2 |
| 7/18/2016 | 17:41:40 | -           | KeyVaultDecryptRequest | "                      | 'Success' | b9e063ac-6208-4d2 |
| 7/17/2016 | 01:40:33 | a5b1172b-c6 | GetClientLicensorCert  | 'RmsTenantUser@db8048l | 'Success' | d6670bb5-4da7-4e1 |
| 7/17/2016 | 01:40:59 | 9d93a998-8c | Certify                | 'RmsTenantUser@db8048l | 'Success' | 928a5df6-ccab-414 |
| 7/17/2016 | 01:35:50 | d5da5952-0t | AcquireLicense         | 'RmsTenantConsumer@dl  | 'Success' | ae695fd1-a4e1-44e |

For more information about usage logging, see [Logging and analyzing the protection usage from Azure Information Protection](#).

### 3. Manage your tenant key.

For more information about the life cycle operations for your tenant key, see [Operations for your Azure Information Protection tenant key](#).

# Bring your own key (BYOK) details for Azure Information Protection

5/21/2020 • 4 minutes to read • [Edit Online](#)

Applies to: [Azure Information Protection](#), [Office 365](#)

Organizations that have a subscription that includes Azure Information Protection can configure their Azure Information Protection tenant to use a customer-managed key and [log its usage](#). The customer-managed key configuration is often referred to as "bring you own key", or BYOK.

This customer-managed key must be stored in Azure Key Vault, which requires an Azure subscription. To use an HSM-protected key, you must use the Azure Key Vault Premium service tier. Using a key in Azure Key Vault incurs a monthly charge. For more information, see the [Azure Key Vault Pricing page](#).

When you use Azure Key Vault for your Azure Information Protection tenant key, we recommend that you use a dedicated key vault for this key to help ensure that it's used by only the Azure Rights Management service. This configuration ensures that calls by other services do not result in exceeding the [service limits](#) for the key vault, which could throttle the response times for the Azure Rights Management service.

In addition, because each service that uses Azure Key Vault typically has different key management requirements, we recommend a separate Azure subscription for this key vault to help safeguard against misconfiguration.

However, if you want to share an Azure subscription with other services that use Azure Key Vault, make sure that the subscription shares a common set of administrators. This precaution means that the administrators who use that subscription have a good understanding of all the keys that they have access to, so that they are less likely to misconfigure them.

For example, a shared Azure subscription if the administrators for your Azure Information Protection tenant key are the same people who administer keys for Office 365 Customer Key and CRM Online.

Alternatively, if the administrators who manage the keys for Customer Key or CRM Online are not the same people who administer your Azure Information Protection tenant key, then we recommend you do not share your Azure subscription for Azure Information Protection.

## Benefits of using Azure Key Vault

For additional assurance, you can cross-reference your Azure Information Protection usage logging with [Azure Key Vault logging](#). The Key Vault logs provide you with a method to independently monitor that only the Azure Rights Management service is using your key. If necessary, you can immediately revoke access to the key by removing the permissions on the key vault.

Other benefits of using Azure Key Vault for your Azure Information Protection tenant key include:

- Azure Key Vault provides a centralized key management solution that offers a consistent management solution for many cloud-based and even on-premises services that use encryption.
- Azure Key Vault supports a number of built-in interfaces for key management, including PowerShell, CLI, REST APIs, and the Azure portal. Other services and tools have integrated with Key Vault, to provide capabilities that are optimized for specific tasks, such as monitoring. For example, you can analyze your key usage logs via Log analytics from the Operations Management Suite, set alerts when specified criteria are met, and so on.

- Azure Key Vault provides role separation, as a recognized security best practice. Azure Information Protection administrators can focus on managing data classification and protection, and Azure Key Vault administrators can focus on managing encryption keys and any special policies that they might require for security or compliance.
- Some organizations have restrictions where their master key must live. Azure Key Vault provides a high level of control where to store the master key because the service is available in many Azure regions. You can choose from a number of Azure regions and you can expect this number to increase. For more information, see the [Products available by region](#) page on the Azure site.

In addition to managing keys, Azure Key Vault offers your security administrators the same management experience to store, access, and manage certificates and secrets (such as passwords) for other services and applications that use encryption.

For more information about Azure Key Vault, see [What is Azure Key Vault?](#) and visit the [Azure Key Vault team blog](#) for the latest information and to learn how other services use this technology.

## BYOK support for services and clients

BYOK and [usage logging](#) work seamlessly with every application that integrates with the Azure Rights Management service that is used by Azure Information Protection to protect data. This includes cloud services such as Microsoft SharePoint, on-premises servers that run Exchange and SharePoint that use the Azure Rights Management service by using the RMS connector, and client applications such as Office 2019, Office 2016, and Office 2013.

You get key usage logs whatever application makes requests to the Azure Rights Management service.

## Next steps

If you've made the decision to manage your own key, go to [Implementing your Azure Information Protection tenant key](#).

If you've decided to stay with the default configuration where Microsoft manages your tenant key, see the [Next steps](#) section of the Planning and implementing your Azure Information Protection tenant key article.

# Preparing users and groups for Azure Information Protection

7/20/2020 • 11 minutes to read • [Edit Online](#)

*Applies to:* [Azure Information Protection](#), [Office 365](#)

Before you deploy Azure Information Protection for your organization, make sure that you have accounts for users and groups in Azure AD for your organization's tenant.

There are different ways to create these accounts for users and groups, which include:

- You create the users in the Microsoft 365 admin center, and the groups in the Exchange Online admin center.
- You create the users and groups in the Azure portal.
- You create the users and group by using Azure AD PowerShell and Exchange Online cmdlets.
- You create the users and groups in your on-premises Active Directory and synchronize them to Azure AD.
- You create the users and groups in another directory and synchronize them to Azure AD.

When you create users and groups by using the first three methods from this list, with one exception, they are automatically created in Azure AD, and Azure Information Protection can use these accounts directly. However, many enterprise networks use an on-premises directory to create and manage users and groups. Azure Information Protection cannot use these accounts directly; you must synchronize them to Azure AD.

The exception referred to in the previous paragraph is dynamic distribution lists that you can create for Exchange Online. Unlike static distribution lists, these groups are not replicated to Azure AD and so cannot be used by Azure Information Protection.

## How users and groups are used by Azure Information Protection

There are three scenarios for using users and groups with Azure Information Protection:

**For assigning labels to users** when you configure the Azure Information Protection policy so that labels can be applied to documents and emails. Only administrators can select these users and groups:

- The default Azure Information Protection policy is automatically assigned to all users in your tenant's Azure AD. However, you can also assign additional labels to specified users or groups by using scoped policies.

**For assigning usage rights and access controls** when you use the Azure Rights Management service to protect documents and emails. Administrators and users can select these users and groups:

- Usage rights determine whether a user can open a document or email and how they can use it. For example, whether they can only read it, or read and print it, or read and edit it.
- Access controls include an expiry date and whether a connection to the internet is required for access.

**For configuring the Azure Rights Management service** to support specific scenarios, and therefore only administrators select these groups. Examples include configuring the following:

- Super users, so that designated services or people can open encrypted content if required for eDiscovery or data recovery.

- Delegated administration of the Azure Rights Management service.
- Onboarding controls to support a phased deployment.

## Azure Information Protection requirements for user accounts

For assigning labels:

- All user accounts in Azure AD can be used to configure scoped policies that assign additional labels to users.

For assigning usage rights and access controls, and configuring the Azure Rights Management service:

- To authorize users, two attributes in Azure AD are used: **proxyAddresses** and **userPrincipalName**.
- The **Azure AD proxyAddresses** attribute stores all email addresses for an account and can be populated in different ways. For example, a user in Office 365 that has an Exchange Online mailbox automatically has an email address that is stored in this attribute. If you assign an alternative email address for an Office 365 user, it is also saved in this attribute. It can also be populated by the email addresses that are synchronized from on-premises accounts.

Azure Information Protection can use any value in this Azure AD proxyAddresses attribute, providing the domain has been added to your tenant (a "verified domain"). For more information about verifying domains:

- For Azure AD: [Add a custom domain name to Azure Active Directory](#)
- For Office 365: [Add a domain to Office 365](#)
- The **Azure AD userPrincipalName** attribute is used only when an account in your tenant doesn't have values in the Azure AD proxyAddresses attribute. For example, you create a user in the Azure portal, or create a user for Office 365 that doesn't have a mailbox.

### Assigning usage rights and access controls to external users

In addition to using the Azure AD proxyAddresses and Azure AD userPrincipalName for users in your tenant, Azure Information Protection also uses these attributes in the same way to authorize users from another tenant.

Other authorization methods:

- For email addresses that are not in Azure AD, Azure Information Protection can authorize these when they are authenticated with a Microsoft account. However, not all applications can open protected content when a Microsoft account is used for authentication. [More information](#)
- When an email is sent by using Office 365 Message Encryption with new capabilities to a user who doesn't have an account in Azure AD, the user is first authenticated by using federation with a social identity provider or by using a one-time passcode. Then the email address specified in the protected email is used to authorize the user.

## Azure Information Protection requirements for group accounts

For assigning labels:

- To configure scoped policies that assign additional labels to group members, you can use any type of group in Azure AD that has an email address that contains a verified domain for the user's tenant. A group that has an email address is often referred to as a mail-enabled group.

For example, you can use a mail-enabled security group, a static distribution group, and an Office 365 group. You cannot use a security group (dynamic or static) because this group type doesn't have an email address. You also cannot use a dynamic distribution list from Exchange Online because this group isn't replicated to Azure AD.

For assigning usage rights and access controls:

- You can use any type of group in Azure AD that has an email address that contains a verified domain for the user's tenant. A group that has an email address is often referred to as a mail-enabled group.

For configuring the Azure Rights Management service:

- You can use any type of group in Azure AD that has an email address from a verified domain in your tenant, with one exception. That exception is when you configure onboarding controls to use a group, which must be a security group in Azure AD for your tenant.
- You can use any group in Azure AD (with or without an email address) from a verified domain in your tenant for delegated administration of the Azure Rights Management service.

### Assigning usage rights and access controls to external groups

In addition to using the Azure AD proxyAddresses for groups in your tenant, Azure Information Protection also uses this attribute in the same way to authorize groups from another tenant.

## Using accounts from Active Directory on-premises for Azure Information Protection

If you have accounts that are managed on-premises that you want to use with Azure Information Protection, you must synchronize these to Azure AD. For ease of deployment, we recommend that you use [Azure AD Connect](#). However, you can use any directory synchronization method that achieves the same result.

When you synchronize your accounts, you do not need to synchronize all attributes. For a list of the attributes that must be synchronized, see the [Azure RMS section](#) from the Azure Active Directory documentation.

From the attributes list for Azure Rights Management, you see that for users, the on-premises AD attributes of **mail**, **proxyAddresses**, and **userPrincipalName** are required for synchronization. Values for **mail** and **proxyAddresses** are synchronized to the Azure AD proxyAddresses attribute. For more information, see [How the proxyAddresses attribute is populated in Azure AD](#)

## Confirming your users and groups are prepared for Azure Information Protection

You can use Azure AD PowerShell to confirm that users and groups can be used with Azure Information Protection. You can also use PowerShell to confirm the values that can be used to authorize them.

For example, using the V1 PowerShell module for Azure Active Directory, [MSOnline](#), in a PowerShell session, first connect to the service and supply your global admin credentials:

```
Connect-MsolService
```

Note: If this command doesn't work, you can run `Install-Module MSOnline` to install the MSOnline module.

Next, configure your PowerShell session so that it doesn't truncate the values:

```
$FormatEnumerationLimit = 1
```

### Confirm user accounts are ready for Azure Information Protection

To confirm the user accounts, run the following command:

```
Get-MsolUser | select DisplayName, UserPrincipalName, ProxyAddresses
```

Your first check is to make sure that the users you want to use with Azure Information Protection are displayed.

Then check whether the **ProxyAddresses** column is populated. If it is, the email values in this column can be used to authorize the user for Azure Information Protection.

If the **ProxyAddresses** column is not populated, the value in the **UserPrincipalName** is used to authorize the user for the Azure Rights Management service.

For example:

| DISPLAY NAME    | USERPRINCIPALNAME          | PROXYADDRESSES                                                       |
|-----------------|----------------------------|----------------------------------------------------------------------|
| Jagannath Reddy | jagannathreddy@contoso.com | {}                                                                   |
| Ankur Roy       | ankurroy@contoso.com       | {SMTP:ankur.roy@contoso.com, smtp:ankur.roy@onmicrosoft.contoso.com} |

In this example:

- The user account for Jagannath Reddy will be authorized by **jagannathreddy@contoso.com**.
- The user account for Ankur Roy can be authorized by using **ankur.roy@contoso.com** and **ankur.roy@onmicrosoft.contoso.com**, but not **ankurroy@contoso.com**.

In most cases, the value for UserPrincipalName matches one of the values in the ProxyAddresses field. This is the recommended configuration but if you cannot change your UPN to match the email address, you must take the following steps:

1. If the domain name in the UPN value is a verified domain for your Azure AD tenant, add the UPN value as another email address in Azure AD so that the UPN value can now be used to authorize the user account for Azure Information Protection.

If the domain name in the UPN value is not a verified domain for your tenant, it cannot be used with Azure Information Protection. However, the user can still be authorized as a member of a group when the group email address uses a verified domain name.

2. If the UPN is not routable (for example, **ankurroy@contoso.local**), configure alternate login ID for users and instruct them how to sign in to Office by using this alternate login. You must also set a registry key for Office.

For more information, see [Configuring Alternate Login ID](#) and [Office applications periodically prompt for credentials to SharePoint, OneDrive, and Lync Online](#).

#### TIP

You can use the Export-Csv cmdlet to export the results to a spreadsheet for easier management, such as searching and bulk-editing for import.

```
For example: Get-MsolGroup | select DisplayName, ProxyAddresses | Export-Csv -Path UserAccounts.csv
```

#### Confirm group accounts are ready for Azure Information Protection

To confirm group accounts, use the following command:

```
Get-MsolGroup | select DisplayName, ProxyAddresses
```

Make sure that the groups you want to use with Azure Information Protection are displayed. For the groups displayed, the email addresses in the **ProxyAddresses** column can be used to authorize the group members for the Azure Rights Management service.

Then check that the groups contain the users (or other groups) that you want to use for Azure Information Protection. You can use PowerShell to do this (for example, [Get-MsolGroupMember](#)), or use your management portal.

For the two Azure Rights Management service configuration scenarios that use security groups, you can use the following PowerShell command to find the object ID and display name that can be used to identify these groups. You can also use the Azure portal to find these groups and copy the values for the object ID and the display name:

```
Get-MsolGroup | where {$_ .GroupType -eq "Security"}
```

## Considerations for Azure Information Protection if email addresses change

If you change the email address of a user or group, we recommend that you add the old email address as a second email address (also known as a proxy address, alias, or alternate email address) to the user or group. When you do this, the old email address is added to the Azure AD proxyAddresses attribute. This account administration ensures business continuity for any usage rights or other configurations there were saved when the old email address was in use.

If you cannot do this, the user or group with the new email address risks being denied access to documents and emails that were previously protected with the old email address. In this case, you must repeat the protection configuration to save the new email address. For example, if the user or group was granted usage rights in templates or labels, edit those templates or labels and specify the new email address with same usage rights as you granted to the old email address.

Note that it's rare for a group to change its email address and if you assign usage rights to a group rather than individual users, it doesn't matter if the user's email address changes. In this scenario, the usage rights are assigned to the group email address and not individual user email addresses. This is the most likely (and recommended) method for an administrator to configure usage rights that protect documents and emails. However, users might more typically assign custom permissions for individual users. Because you cannot always know whether a user account or group has been used to grant access, it's safest to always add the old email address as a second email address.

## Group membership caching by Azure Information Protection

For performance reasons, Azure Information Protection caches group membership. This means that any changes to group membership in Azure AD can take up to three hours to take effect when these groups are used by Azure Information Protection and this time period is subject to change.

Remember to factor this delay into any changes or testing that you do when you use groups for granting usage rights or configuring the Azure Rights Management service, or when you configure scoped policies.

## Next steps

When you have confirmed that your users and groups can be used with Azure Information Protection and you are ready to start protecting documents and emails, check whether you need to activate the Azure Rights Management service. This service must be activated before you can protect your organization's documents and

emails:

- Beginning with February 2018: If your subscription that includes Azure Rights Management or Azure Information Protection was obtained during or after this month, the service is automatically activated for you.
- If your subscription was obtained before February 2018: You must activate the service yourself.

For more information, which includes checking the activation status, see [Activating the protection service from Azure Information Protection](#).

# Activating the protection service from Azure Information Protection

5/21/2020 • 5 minutes to read • [Edit Online](#)

Applies to: [Azure Information Protection](#), [Office 365](#)

## NOTE

This configuration information is for administrators who are responsible for a service that applies to all users in an organization. If you are looking for user help and information to use the Rights Management functionality for a specific application or how to open a file or email that is rights-protected, use the help and guidance that accompanies your application.

For example, for Office applications, click the Help icon and enter search terms such as **Rights Management** or **IRM**. For the Azure Information Protection client for Windows, see the [Azure Information Protection client user guide](#).

For technical support and other questions about the service, see the [Support options and community resources](#) information.

When the protection service for Azure Information Protection is activated for your organization, administrators and users can start to protect important data by using applications and services that support this information protection solution. Administrators can also manage and monitor protected documents and emails that your organization owns.

## Do you need to activate the protection service, Azure Rights Management?

When you have a service plan that includes Azure Rights Management, you might not have to activate the service:

- **If your subscription that includes Azure Rights Management or Azure Information Protection was obtained towards the end of February 2018 or later:** The service is automatically activated for you. You do not have to activate the service unless you or another global administrator for your organization deactivated Azure Rights Management.
- **If your subscription that includes Azure Rights Management or Azure Information Protection was obtained before or during February 2018:** Microsoft is starting to activate the Azure Rights Management service for these subscriptions if your tenant is using Exchange Online. For these subscriptions, automatic activation is starting to roll out August 1, 2018 when the service will be activated for you unless you see **AutomaticServiceUpdateEnabled** is set to **false** when you run [Get-IRMConfiguration](#).

If neither of the subsequent scenarios apply to you, you must manually activate the protection service.

When the service is activated, all users in your organization can apply information protection to their documents and emails, and all users can open (consume) documents and emails that have been protected by the Azure Rights Management service. However, if you prefer, you can restrict who can apply information protection, by using onboarding controls for a phased deployment. For more information, see the [Configuring onboarding controls for a phased deployment](#) section in this article.

# How to activate or confirm the status of the protection service

## IMPORTANT

Do not activate the protection service if you have Active Directory Rights Management Services (AD RMS) deployed for your organization. [More information](#)

To use this data protection solution, your organization must have a service plan that includes the Azure Rights Management service from Azure Information Protection. Without this, the protection service cannot be activated. You must have one of the following:

- An [Azure Information Protection plan](#)
- An [Office 365 plan that includes Rights Management](#).

When the protection service is activated, all users in your organization can apply information protection to their documents and emails, and all users can open (consume) documents and emails that have been protected by this service. However, if you prefer, you can restrict who can apply information protection, by using onboarding controls for a phased deployment. For more information, see the [Configuring onboarding controls for a phased deployment](#) section in this article.

## Choosing your activation method

For instructions how to activate the protection service from your management portal, select whether to use the Microsoft 365 admin center or the Azure portal:

- [Microsoft 365 admin center](#) - requires Global Administrator account
- [Azure portal](#) - does not require Global Administrator account

Alternatively, you can use the following PowerShell commands:

1. Install the AIPService module, to configure and manage the protection service. For instructions, see [Installing the AIPService PowerShell module](#).
2. From a PowerShell session, run [Connect-AipService](#), and when prompted, provide the Global Administrator account details for your Azure Information Protection tenant.
3. Run [Get-AipService](#) to confirm whether the protection service is activated. A status of **Enabled** confirms activation; **Disabled** indicates that the service is deactivated.
4. To activate the service, run [Enable-AipService](#).

## Configuring onboarding controls for a phased deployment

If you don't want all users to be able to protect documents and emails immediately by using Azure Information Protection, you can configure user onboarding controls by using the [Set-AipServiceOnboardingControlPolicy](#) PowerShell command. You can run this command before or after you activate the Azure Rights Management service.

For example, if you initially want only administrators in the "IT department" group (that has an object ID of fbb99ded-32a0-45f1-b038-38b519009503) to be able to protect content for testing purposes, use the following command:

```
Set-AipServiceOnboardingControlPolicy -UseRmsUserLicense $False -SecurityGroupObjectId "fbb99ded-32a0-45f1-b038-38b519009503"
```

Note that for this configuration option, you must specify a group; you cannot specify individual users. To obtain the object ID for the group, you can use Azure AD PowerShell—for example, for version 1.0 of the module, use the [Get-MsolGroup](#) command. Or, you can copy the **Object ID** value of the group from the Azure portal.

Alternatively, if you want to ensure that only users who are correctly licensed to use Azure Information Protection can protect content:

```
Set-AipServiceOnboardingControlPolicy -UseRmsUserLicense $True
```

When you no longer need to use onboarding controls, whether you used the group or licensing option, run:

```
Set-AipServiceOnboardingControlPolicy -UseRmsUserLicense $False
```

For more information about this cmdlet and additional examples, see the [Set-AipServiceOnboardingControlPolicy](#) help.

When you use these onboarding controls, all users in the organization can always consume protected content that has been protected by your subset of users, but they won't be able to apply information protection themselves from client applications. For example, they won't see in their Office apps the default protection templates that are automatically published when the protection service is activated, or custom templates that you might configure. Server-side applications, such as Exchange, can implement their own per-user controls to achieve the same result. For example, to prevent users from protecting emails in Outlook on the web, use [Set-OwaMailboxPolicy](#) to set the *IRMEnabled* parameter to *\$false*.

## Next steps

When the protection service is activated for your organization, use the [Azure Information Protection deployment roadmap](#) to check whether there are other configuration steps that you might need to do before you roll out Azure Information Protection to users and administrators.

For example, you might want to use [templates](#) to make it easier for users to apply protection to files, connect your on-premises servers to use the protection service by installing the [Rights Management connector](#), and deploy the [Azure Information Protection client](#) that supports protecting all file types on all devices.

Office services, such as Exchange Online and Microsoft SharePoint require additional configuration before you can use their Information Rights Management (IRM) features. For information about how your applications work with the protection service, Azure Rights Management, see [How applications support the Azure Rights Management service](#).

# How to activate Rights Management protection from the Microsoft 365 admin center

5/5/2020 • 2 minutes to read • [Edit Online](#)

Applies to: [Azure Information Protection](#), [Office 365](#)

Use these instructions if you have access to the Azure Rights Management service from the Microsoft 365 admin center and you are a global administrator.

To activate the Azure Rights Management service, you must have either an [Azure Information Protection Premium plan](#) or an [Office 365 plan that includes Rights Management](#). For example, your organization has a plan for Office 365 E3 or Office 365 E5.

If you have questions about the subscription requirements, or you need help activating the service, [contact Microsoft Support](#) or use your standard support channels.

1. When you have confirmed that your organization has a plan that includes Azure Rights Management, go to the [Rights Management page](#) in the Microsoft 365 admin center.

If you are prompted to sign in, use an account that is a global administrator for Office 365.

## TIP

For admin center help, see [About the Microsoft 365 admin center](#).

If you prefer to navigate to the **rights management** page from the admin center: **Settings > Services & add-ins > Microsoft Azure Information Protection > Manage Microsoft Azure Information Protection settings**

2. On the **rights management** page, click **activate**.
3. When you see the message **Do you want to activate Rights Management?**, click **activate**.

You should now see **Rights management is activated** and the option to deactivate.

## Next steps

Resume reading [Activating the protection service from Azure Information Protection](#).

# How to activate the Rights Management protection service from the Azure portal

3/16/2020 • 2 minutes to read • [Edit Online](#)

Applies to: [Azure Information Protection](#)

## NOTE

To provide a unified and streamlined customer experience, **Azure Information Protection client (classic)** and **Label Management** in the Azure Portal are being **deprecated** as of **March 31, 2021**. This time-frame allows all current Azure Information Protection customers to transition to our unified labeling solution using the Microsoft Information Protection Unified Labeling platform. Learn more in the official [deprecation notice](#).

Use these instructions if you want to activate the Rights Management protection service (Azure RMS) from Azure Information Protection, by using the Azure portal.

1. If you haven't already done so, open a new browser window and [sign in to the Azure portal](#). Then navigate to the **Azure Information Protection** pane.

For example, in the search box for resources, services, and docs: Start typing **Information** and select **Azure Information Protection**.

If you haven't accessed the Azure Information Protection pane before, see the one-time [additional steps](#) to add this pane to the portal.

To open the Azure Information Protection pane, you must have either an [Azure Information Protection Premium plan](#) or an [Office 365 plan that includes Rights Management](#). If you have one of these subscriptions but see a message that a valid subscription cannot be found, [contact Microsoft Support](#) or use your standard support channels.

2. Locate the **Manage** menu options, and select **Protection activation**.

Click **Activate**, and then confirm your action.

When activation is complete, the information bar displays **Activation finished successfully**.

## Next steps

Resume reading [Activating the protection service from Azure Information Protection](#).

# Configuring applications for Azure Rights Management

5/21/2020 • 2 minutes to read • [Edit Online](#)

Applies to: [Azure Information Protection](#), [Office 365](#)

## NOTE

This information is for IT administrators and consultants who have deployed Azure Information Protection. If you are looking for user help and information about how to use the Rights Management functionality for a specific application or how to open a file that is rights-protected, use the help and guidance that accompanies your application.

For example, for Office applications, click the Help icon and enter search terms such as **Rights Management** or **IRM**. For the Azure Information Protection client for Windows, see the [Azure Information Protection client user guide](#).

After you have deployed Azure Information Protection for your organization, use the following information to configure applications, the Azure Information Protection client, and services. For example, Office applications such as Word 2019, Word 2016, and Word 2013. Also services such as Exchange Online (transport rules, data loss prevention, do not forward, and message encryption) and Microsoft SharePoint (protected libraries). For information about how these applications and services support the data protection service from Azure Information Protection, see [How applications support the Azure Rights Management service](#).

## IMPORTANT

For information about supported versions and other requirements, see [Requirements for Azure Information Protection](#).

- [Office 365: Configuration for online services](#)
  - [Exchange Online: IRM Configuration](#)
  - [SharePoint in Microsoft 365 and OneDrive: IRM Configuration](#)
- [Office applications: Configuration for clients](#)
  - [Office 365 apps, Office 2019, Office 2016, and Office 2013](#)
  - [Office 2010](#)
- [Azure Information Protection client: Installation and configuration for clients](#)

To configure on-premises servers such as Exchange Server and SharePoint Server, see [Deploying the Azure Rights Management connector](#).

In addition to these applications and services, there are other applications that support the Rights Management APIs. This category includes line-of-business applications that are written in-house by using the Rights Management SDK, and applications from software vendors that are written by using the Rights Management SDK. For these applications, follow the instructions that are provided with the application.

## Next steps

After you've configured your applications to support the Azure Rights Management service, use the [Azure](#)

[Information Protection deployment roadmap](#) to check whether there are other configuration steps that you might want to do before you roll out Azure Information Protection to users and administrators. If not, you might find the following operational information useful:

- [Verifying the Azure Rights Management service](#)
- [Helping users to protect files by using the Azure Rights Management service](#)
- [Logging and analyzing the Azure Rights Management service](#)
- [Operations for your Azure Information Protection tenant key](#)

# Office 365: Configuration for online services to use the Azure Rights Management service

7/20/2020 • 21 minutes to read • [Edit Online](#)

Applies to: [Azure Information Protection](#), [Office 365](#)

Use the following sections to help you configure Exchange Online, Microsoft SharePoint, and Microsoft OneDrive to use the Azure Rights Management service from Azure Information Protection.

## Exchange Online: IRM Configuration

For information about how Exchange Online works with the Azure Rights Management service, see the [Exchange Online and Exchange Server](#) section from [How Office applications and services support Azure Rights Management](#).

Exchange Online might already be enabled to use the Azure Rights Management service. To check, run the following commands:

1. If this is the first time that you have used Windows PowerShell for Exchange Online on your computer, you must configure Windows PowerShell to run signed scripts. Start your Windows PowerShell session by using the **Run as administrator** option, and then type:

```
Set-ExecutionPolicy RemoteSigned
```

Press Y to confirm.

2. In your Windows PowerShell session, sign in to Exchange Online by using an account that is enabled for remote Shell access. By default, all accounts that are created in Exchange Online are enabled for remote Shell access but this can be disabled (and enabled) by using the [Set-User <UserIdentity> -RemotePowerShellEnabled](#) command.

To sign in, first type:

```
$Cred = Get-Credential
```

Then, in the **Windows PowerShell credential request** dialog box, supply your Office 365 user name and password.

3. Connect to the Exchange Online service by first setting a variable:

```
$Session = New-PSSession -ConfigurationName Microsoft.Exchange -ConnectionUri https://ps.outlook.com/powershell/ -Credential $Cred -Authentication Basic -AllowRedirection
```

Then run the following command:

```
Import-PSSession $Session
```

4. Run the [Get-IRMConfiguration](#) command to view your Exchange Online configuration for the protection service:

#### Get-IRMConfiguration

From the output, locate the **AzureRMSLicensingEnabled** value:

- If AzureRMSLicensingEnabled is set to **True**, Exchange Online is already enabled for the Azure Rights Management service.
- If AzureRMSLicensingEnabled is set **False**, run the follow command to enable Exchange Online for the Azure Rights Management service: `Set-IRMConfiguration -AzureRMSLicensingEnabled $true`

5. To test that Exchange Online is configured successfully, run the following command:

```
Test-IRMConfiguration -Sender <user email address>
```

For example: \*\*Test-IRMConfiguration -Sender adams@contoso.com\*\*

This command runs a series of checks that includes verifying connectivity to the service, retrieving the configuration, retrieving URIs, licenses, and any templates. In the Windows PowerShell session, you will see the results of each and at the end, if everything passes these checks: **OVERALL RESULT: PASS**

When Exchange Online is enabled to use the Azure Rights Management service, you can configure features that apply information protection automatically, such as [mail flow rules](#), [data loss prevention \(DLP\) policies](#), and [protected voice mail](#) (Unified Messaging).

## SharePoint in Microsoft 365 and OneDrive: IRM Configuration

For information about how SharePoint IRM works with the Azure Rights Management service, see [SharePoint in Microsoft 365 and SharePoint Server from the Rights Management protection](#) section of this documentation.

To configure SharePoint in Microsoft 365 and OneDrive to support the Azure Rights Management service, you must first enable the information rights management (IRM) service for SharePoint by using the SharePoint admin center. Then, site owners can IRM-protect their SharePoint lists and document libraries, and users can IRM-protect their OneDrive library so that documents that are saved there, and shared with others, are automatically protected by the Azure Rights Management service.

#### NOTE

IRM-protected libraries for SharePoint in Microsoft 365 and OneDrive require the latest version of the new OneDrive sync client (OneDrive.exe), and the version of the [RMS client from the Microsoft Download Center](#). Install this version of the RMS client even if you have installed the Azure Information Protection client. For more information about this deployment scenario, see [Deploy the new OneDrive sync client in an enterprise environment](#).

To enable the information rights management (IRM) service for SharePoint, see the following instructions from the Office documentation:

- [Set up Information Rights Management \(IRM\) in the SharePoint admin center](#)

This configuration is done by the Office 365 administrator.

#### Configuring IRM for libraries and lists

After you have enabled the IRM service for SharePoint, site owners can IRM-protect their SharePoint document libraries and lists. For instructions, see the following from the Office website:

- [Apply Information Rights Management to a list or library](#)

This configuration is done by the SharePoint site administrator.

## Configuring IRM for OneDrive

After you have enabled the IRM service for SharePoint, users' OneDrive document library or individual folders can then be configured for Rights Management protection. Users can configure this for themselves by using their OneDrive website. Although administrators cannot configure this protection for them by using the SharePoint admin center, you can do this by using Windows PowerShell.

### NOTE

For more information about configuring OneDrive, see the Office documentation, [Set up OneDrive in Office 365](#).

### Configuration for users

Give users the following instructions so that they can configure their OneDrive to protect their business files.

1. Sign in to Office 365 with your work or school account and go to the [OneDrive website](#).
2. In the navigation pane, at the bottom, select **Return to classic OneDrive**.
3. Select the **Settings** icon. In the **Settings** pane, if the **Ribbon** is set to **Off**, select this setting to turn the ribbon on.
4. To configure all OneDrive files to be protected, select the **LIBRARY** tab from the ribbon, and then select **Library Settings**.
5. On the **Documents > Settings** page, in the **Permissions and Management** section, select **Information Rights Management**.
6. On the **Information Rights Management Settings** page, select **Restrict permissions on this library on download** check box. Specify your choice of name and a description for the permissions, and optionally, click **SHOW OPTIONS** to configure optional configurations, and then click **OK**.

For more information about the configuration options, see the instructions in [Apply Information Rights Management to a list or library](#) from the Office documentation.

Because this configuration relies on users rather than an administrator to IRM-protect their OneDrive files, educate users about the benefits of protecting their files and how to do this. For example, explain that when they share a document from OneDrive, only people they authorize can access it with any restrictions that they configure, even if the file is renamed and copied somewhere else.

### Configuration for administrators

Although you cannot configure IRM for users' OneDrive by using the SharePoint admin center, you can do this by using Windows PowerShell. To enable IRM for these libraries, follow these steps:

1. Download and install the [SharePoint Client Components SDK](#).
2. Download and install the [SharePoint Management Shell](#).
3. Copy the contents of the following script and name the file Set-IRMOnOneDriveForBusiness.ps1 on your computer.

**\*\*Disclaimer\*\*.** This sample script is not supported under any Microsoft standard support program or service. This sample script is provided AS IS without warranty of any kind.

```
Requires Windows PowerShell version 3

<#
 Description:
#>
```

Configures IRM policy settings for OneDrive and can also be used for SharePoint libraries and lists

Script Installation Requirements:

SharePoint Client Components SDK  
<https://www.microsoft.com/download/details.aspx?id=42038>

SharePoint Management Shell  
<https://www.microsoft.com/download/details.aspx?id=35588>

=====

#>

```
URL will be in the format https://<tenant-name>-admin.sharepoint.com
$sharepointAdminCenterUrl = "https://contoso-admin.sharepoint.com"
```

```
$tenantAdmin = "admin@contoso.com"
```

```
$webUrls = @("https://contoso-my.sharepoint.com/personal/user1_contoso_com",
 "https://contoso-my.sharepoint.com/personal/user2_contoso_com",
 "https://contoso-my.sharepoint.com/personal/user3_contoso_com")
```

```
<# As an alternative to specifying the URLs as an array, you can import them from a CSV file (no header,
single value per row).
```

```
Then, use: $webUrls = Get-Content -Path "File_path_and_name.csv"
```

#>

```
$listTitle = "Documents"
```

```
function Load-SharePointOnlineClientComponentAssemblies
```

```
{
```

```
 [cmdletbinding()]
 param()
```

```
 process
```

```
 {
```

```
 # assembly location: C:\Program Files\Common Files\microsoft shared\Web Server
Extensions\16\ISAPI
 try
 {
 Write-Verbose "Loading Assembly: Microsoft.Office.Client.Policy, Version=16.0.0.0,
Culture=neutral, PublicKeyToken=71e9bce111e9429c"
 [System.Reflection.Assembly]::Load("Microsoft.Office.Client.Policy, Version=16.0.0.0,
Culture=neutral, PublicKeyToken=71e9bce111e9429c") | Out-Null
```

```
 Write-Verbose "Loading Assembly: Microsoft.Office.Client.TranslationServices,
Version=16.0.0.0, Culture=neutral, PublicKeyToken=71e9bce111e9429c"
 [System.Reflection.Assembly]::Load("Microsoft.Office.Client.TranslationServices,
Version=16.0.0.0, Culture=neutral, PublicKeyToken=71e9bce111e9429c") | Out-Null
```

```
 Write-Verbose "Loading Assembly: Microsoft.SharePoint.Client, Version=16.0.0.0,
Culture=neutral, PublicKeyToken=71e9bce111e9429c"
 [System.Reflection.Assembly]::Load("Microsoft.SharePoint.Client, Version=16.0.0.0,
Culture=neutral, PublicKeyToken=71e9bce111e9429c") | Out-Null
```

```
 Write-Verbose "Loading Assembly: Microsoft.SharePoint.Client.DocumentManagement,
Version=16.0.0.0, Culture=neutral, PublicKeyToken=71e9bce111e9429c"
 [System.Reflection.Assembly]::Load("Microsoft.SharePoint.Client.DocumentManagement,
Version=16.0.0.0, Culture=neutral, PublicKeyToken=71e9bce111e9429c") | Out-Null
```

```
 Write-Verbose "Loading Assembly: Microsoft.SharePoint.Client.Publishing, Version=16.0.0.0,
Culture=neutral, PublicKeyToken=71e9bce111e9429c"
 [System.Reflection.Assembly]::Load("Microsoft.SharePoint.Client.Publishing,
Version=16.0.0.0, Culture=neutral, PublicKeyToken=71e9bce111e9429c") | Out-Null
```

```
 Write-Verbose "Loading Assembly: Microsoft.SharePoint.Client.Runtime, Version=16.0.0.0,
Culture=neutral, PublicKeyToken=71e9bce111e9429c"
 [System.Reflection.Assembly]::Load("Microsoft.SharePoint.Client.Runtime, Version=16.0.0.0,
```

```

Culture=neutral, PublicKeyToken=71e9bce111e9429c") | Out-Null

 Write-Verbose "Loading Assembly: Microsoft.SharePoint.Client.Search.Applications,
Version=16.0.0.0, Culture=neutral, PublicKeyToken=71e9bce111e9429c"
 [System.Reflection.Assembly]::Load("Microsoft.SharePoint.Client.Search.Applications,
Version=16.0.0.0, Culture=neutral, PublicKeyToken=71e9bce111e9429c") | Out-Null

 Write-Verbose "Loading Assembly: Microsoft.SharePoint.Client.Search, Version=16.0.0.0,
Culture=neutral, PublicKeyToken=71e9bce111e9429c"
 [System.Reflection.Assembly]::Load("Microsoft.SharePoint.Client.Search, Version=16.0.0.0,
Culture=neutral, PublicKeyToken=71e9bce111e9429c") | Out-Null

 Write-Verbose "Loading Assembly: Microsoft.SharePoint.Client.Taxonomy, Version=16.0.0.0,
Culture=neutral, PublicKeyToken=71e9bce111e9429c"
 [System.Reflection.Assembly]::Load("Microsoft.SharePoint.Client.Taxonomy, Version=16.0.0.0,
Culture=neutral, PublicKeyToken=71e9bce111e9429c") | Out-Null

 Write-Verbose "Loading Assembly: Microsoft.SharePoint.Client.UserProfiles, Version=16.0.0.0,
Culture=neutral, PublicKeyToken=71e9bce111e9429c"
 [System.Reflection.Assembly]::Load("Microsoft.SharePoint.Client.UserProfiles,
Version=16.0.0.0, Culture=neutral, PublicKeyToken=71e9bce111e9429c") | Out-Null

 return $true
 }
 catch
 {
 if($_.Exception.Message -match "Could not load file or assembly")
 {
 Write-Error -Message "Unable to load the SharePoint Server 2013 Client
Components.\`nDownload Location: https://www.microsoft.com/download/details.aspx?id=42038"
 }
 else
 {
 Write-Error -Exception $_.Exception
 }
 return $false
 }
}
}

function Load-SharePointOnlineModule
{
 [cmdletbinding()]
 param()

 process
 {
 do
 {
 # Installation location: C:\Program Files\SharePoint Online Management
 Shell\Microsoft.Online.SharePoint.PowerShell
 $spoModule = Get-Module -Name Microsoft.Online.SharePoint.PowerShell -ErrorAction
 SilentlyContinue

 if(-not $spoModule)
 {
 try
 {
 Import-Module Microsoft.Online.SharePoint.PowerShell -DisableNameChecking
 return $true
 }
 catch
 {
 if($_.Exception.Message -match "Could not load file or assembly")
 {
 Write-Error -Message "Unable to load the SharePoint Online Management
 Shell.\`nDownload Location: https://www.microsoft.com/download/details.aspx?id=35588"
 }
 else
 }
 }
 }
 }
}

```

```

 {
 Write-Error -Exception $_.Exception
 }
 return $false
 }
}
else
{
 return $true
}
}
while(-not $spoModule)
}
}

function Set-IrmConfiguration
{
 [cmdletbinding()]
 param(
 [parameter(Mandatory=$true)][Microsoft.SharePoint.Client.List]$List,
 [parameter(Mandatory=$true)][string]$PolicyTitle,
 [parameter(Mandatory=$true)][string]$PolicyDescription,
 [parameter(Mandatory=$false)][switch]$IrmReject,
 [parameter(Mandatory=$false)][DateTime]$ProtectionExpirationDate,
 [parameter(Mandatory=$false)][switch]$DisableDocumentBrowserView,
 [parameter(Mandatory=$false)][switch]$AllowPrint,
 [parameter(Mandatory=$false)][switch]$AllowScript,
 [parameter(Mandatory=$false)][switch]$AllowWriteCopy,
 [parameter(Mandatory=$false)][int]$DocumentAccessExpireDays,
 [parameter(Mandatory=$false)][int]$LicenseCacheExpireDays,
 [parameter(Mandatory=$false)][string]$GroupName
)
}

process
{
 Write-Verbose "Applying IRM Configuration on '$($List.Title)'

 # reset the value to the default settings
 $list.InformationRightsManagementSettings.Reset()

 $list.IrmEnabled = $true

 # IRM Policy title and description

 $list.InformationRightsManagementSettings.PolicyTitle = $PolicyTitle
 $list.InformationRightsManagementSettings.PolicyDescription = $PolicyDescription

 # Set additional IRM library settings

 # Do not allow users to upload documents that do not support IRM
 $list.IrmReject = $IrmReject.isPresent

 $parsedDate = Get-Date
 if([DateTime]::.TryParse($ProtectionExpirationDate, [ref]$parsedDate))
 {
 # Stop restricting access to the library at <date>
 $list.IrmExpire = $true
 $list.InformationRightsManagementSettings.DocumentLibraryProtectionExpireDate =
$ProtectionExpirationDate
 }

 # Prevent opening documents in the browser for this Document Library
 $list.InformationRightsManagementSettings.DisableDocumentBrowserView =
$DisableDocumentBrowserView.isPresent

 # Configure document access rights

 # Allow viewers to print
 $list.InformationRightsManagementSettings.AllowPrint = $AllowPrint.isPresent
}

```

```

Allow viewers to run script and screen reader to function on downloaded documents
$list.InformationRightsManagementSettings.AllowScript = $AllowScript.isPresent

Allow viewers to write on a copy of the downloaded document
$list.InformationRightsManagementSettings.AllowWriteCopy = $AllowWriteCopy.isPresent

if($DocumentAccessExpireDays)
{
 # After download, document access rights will expire after these number of days (1-365)
 $list.InformationRightsManagementSettings.EnableDocumentAccessExpire = $true
 $list.InformationRightsManagementSettings.DocumentAccessExpireDays =
$DocumentAccessExpireDays
}

Set group protection and credentials interval

if($LicenseCacheExpireDays)
{
 # Users must verify their credentials using this interval (days)
 $list.InformationRightsManagementSettings.EnableLicenseCacheExpire = $true
 $list.InformationRightsManagementSettings.LicenseCacheExpireDays =
$LicenseCacheExpireDays
}

if($GroupName)
{
 # Allow group protection. Default group:
 $list.InformationRightsManagementSettings.EnableGroupProtection = $true
 $list.InformationRightsManagementSettings.GroupName = $GroupName
}

}
end
{
if($list)
{
 Write-Verbose "Committing IRM configuration settings on '$($list.Title)'"
 $list.InformationRightsManagementSettings.Update()
 $list.Update()
 $script:clientContext.Load($list)
 $script:clientContext.ExecuteQuery()
}
}

function Get-CredentialFromCredentialCache
{
[cmdletbinding()]
param([string]$CredentialName)

#if(Test-Path variable:\global:CredentialCache)
if(Get-Variable 0365TenantAdminCredentialCache -Scope Global -ErrorAction SilentlyContinue)
{
 if($global:0365TenantAdminCredentialCache.ContainsKey($CredentialName))
 {
 Write-Verbose "Credential Cache Hit: $CredentialName"
 return $global:0365TenantAdminCredentialCache[$CredentialName]
 }
}
Write-Verbose "Credential Cache Miss: $CredentialName"
return $null
}

function Add-CredentialToCredentialCache
{
[cmdletbinding()]
param([System.Management.Automation.PSCredential]$Credential)

if(-not (Get-Variable CredentialCache -Scope Global -ErrorAction SilentlyContinue))

```

```

if(-not ($global:0365TenantAdminCredentialCache -Scope Global -ErrorAction SilentlyContinue))
{
 Write-Verbose "Initializing the Credential Cache"
 $global:0365TenantAdminCredentialCache = @{}
}

Write-Verbose "Adding Credential to the Credential Cache"
$global:0365TenantAdminCredentialCache[$Credential.UserName] = $Credential
}

load the required assemblies and Windows PowerShell modules

if(-not ((Load-SharePointOnlineClientComponentAssemblies) -and (Load-SharePointOnlineModule))) {
return }

Add the credentials to the client context and SharePoint service connection

check for cached credentials to use
$o365TenantAdminCredential = Get-CredentialFromCredentialCache -CredentialName $tenantAdmin

if(-not $o365TenantAdminCredential)
{
 # when credentials are not cached, prompt for the tenant admin credentials
 $o365TenantAdminCredential = Get-Credential -UserName $tenantAdmin -Message "Enter the password
for the Office 365 admin"

 if(-not $o365TenantAdminCredential -or -not $o365TenantAdminCredential.UserName -or
$o365TenantAdminCredential.Password.Length -eq 0)
 {
 Write-Error -Message "Could not validate the supplied tenant admin credentials"
 return
 }

 # add the credentials to the cache
 Add-CredentialToCredentialCache -Credential $o365TenantAdminCredential
}

connect to Office365 first, required for SharePoint cmdlets to run

Connect-SPOService -Url $sharepointAdminCenterUrl -Credential $o365TenantAdminCredential

enumerate each of the specified site URLs

foreach($webUrl in $webUrls)
{
 $grantedSiteCollectionAdmin = $false

 try
 {
 # establish the client context and set the credentials to connect to the site
 $script:clientContext = New-Object Microsoft.SharePoint.Client.ClientContext($webUrl)
 $script:clientContext.Credentials = New-Object
Microsoft.SharePoint.Client.SharePointOnlineCredentials($o365TenantAdminCredential.UserName,
$o365TenantAdminCredential.Password)

 # initialize the site and web context
 $script:clientContext.Load($script:clientContext.Site)
 $script:clientContext.Load($script:clientContext.Web)
 $script:clientContext.ExecuteQuery()

 # load and ensure the tenant admin user account if present on the target SharePoint site
 $tenantAdminUser = $script:clientContext.Web.EnsureUser($o365TenantAdminCredential.UserName)
 $script:clientContext.Load($tenantAdminUser)
 $script:clientContext.ExecuteQuery()

 # check if the tenant admin is a site admin
 if(-not $tenantAdminUser.IsSiteAdmin)
 {
 try
 {
 $script:clientContext.Load($tenantAdminUser)
 $script:clientContext.ExecuteQuery()
 }
 catch
 {
 Write-Error "An error occurred while trying to verify if the tenant admin is a site
admin. Please ensure the provided credentials are valid and the user has site collection
administrator privileges." -ErrorAction Stop
 }
 }
 }
 catch
 {
 Write-Error "An error occurred while connecting to the SharePoint site at $webUrl. Please
check the URL and credentials." -ErrorAction Stop
 }
}
}

```

```

 {
 # grant the tenant admin temporary admin rights to the site collection
 Set-SPOUser -Site $script:clientContext.Site.Url -LoginName
 $o365TenantAdminCredential.UserName -IsSiteCollectionAdmin $true | Out-Null
 $grantedSiteCollectionAdmin = $true
 }
 catch
 {
 Write-Error $_.Exception
 return
 }
}

try
{
 # load the list orlibrary using CSOM

 $list = $null
 $list = $script:clientContext.Web.Lists.GetByTitle($listTitle)
 $script:clientContext.Load($list)
 $script:clientContext.ExecuteQuery()

 # ***** ADMIN INSTRUCTIONS *****
 # If necessary, modify the following Set-IrmConfiguration parameters to match your
 required values
 # The supplied options and values are for example only
 # Example that shows the Set-IrmConfiguration command with all parameters: Set-
 IrmConfiguration -List $list -PolicyTitle "Protected Files" -PolicyDescription "This policy restricts
 access to authorized users" -IrmReject -ProtectionExpirationDate $(Get-Date).AddDays(180) -
 DisableDocumentBrowserView -AllowPrint -AllowScript -AllowWriteCopy -LicenseCacheExpireDays 25 -
 DocumentAccessExpireDays 90

 Set-IrmConfiguration -List $list -PolicyTitle "Protected Files" -PolicyDescription "This
 policy restricts access to authorized users"
}
catch
{
 Write-Error -Message "Error setting IRM configuration on site: $webUrl.\`nError Details:
 $($_.Exception.ToString())"
}
finally
{
 if($grantedSiteCollectionAdmin)
 {
 # remove the temporary admin rights to the site collection
 Set-SPOUser -Site $script:clientContext.Site.Url -LoginName
 $o365TenantAdminCredential.UserName -IsSiteCollectionAdmin $false | Out-Null
 }
}
}

Disconnect-SPOSERVICE -ErrorAction SilentlyContinue

```

4. Review the script and make the following changes:

- Search for `$sharepointAdminCenterUrl` and replace the example value with your own SharePoint admin center URL.

You'll find this value as the base URL when you go into the SharePoint admin center, and it has the following format: `https://<tenant_name>-admin.sharepoint.com`

For example, if the tenant name is "contoso", then you would specify: <https://contoso-admin.sharepoint.com>

- Search for `$tenantAdmin` and replace the example value with your own fully qualified global

administrator account for Office 365.

This value is the same as the one you use to sign in to the Microsoft 365 admin center as the global administrator and has the following format: `user_name@<tenant domain name>.com`

For example, if the Office 365 global administrator user name is "admin" for the "contoso.com" tenant domain, you would specify: `**admin@contoso.com**`

- c. Search for `$webUrls` and replace the example values with your users' OneDrive web URLs, adding or deleting as many entries as you need.

Alternatively, see the comments in the script about how to replace this array by importing a .CSV file that contains all the URLs you need to configure. We've provided another sample script to automatically search for and extract the URLs to populate this .CSV file. When you're ready to do this, use the [Additional script to output all OneDrive URLs to a .CSV file](#) section immediately after these steps.

The web URL for the user's OneDrive is in the following format: `https://<tenant name>-my.sharepoint.com/personal/<user_name>_<tenant name>.com`

For example, if the user in the contoso tenant has a user name of "rsimone", you would specify:  
[https://contoso-my.sharepoint.com/personal/rsimone\\_contoso\\_com](https://contoso-my.sharepoint.com/personal/rsimone_contoso_com)

- d. Because we are using the script to configure OneDrive, do not change the value of **Documents** for the `$listTitle` variable.
  - e. Search for `ADMIN INSTRUCTIONS`. If you make no changes to this section, the user's OneDrive will be configured for IRM with the policy title of "Protected Files" and the description of "This policy restricts access to authorized users". No other IRM options will be set, which is probably appropriate for most environments. However, you can change the suggested policy title and description, and also add any other IRM options that are appropriate for your environment. See the commented example in the script to help you construct your own set of parameters for the `Set-IrmConfiguration` command.
5. Save the script and sign it. If you do not sign the script (more secure), Windows PowerShell must be configured on your computer to run unsigned scripts. To do this, run a Windows PowerShell session with the **Run as Administrator** option, and type: **Set-ExecutionPolicy Unrestricted**. However, this configuration lets all unsigned scripts run (less secure).

For more information about signing Windows PowerShell scripts, see [about\\_Signing](#) in the PowerShell documentation library.

6. Run the script and if prompted, supply the password for the Office 365 admin account. If you modify the script and run it in the same Windows PowerShell session, you won't be prompted for credentials.

#### TIP

You can also use this script to configure IRM for a SharePoint library. For this configuration, you will likely want to enable the additional option **Do not allow users to upload documents that do not support IRM**, to ensure that the library contains only protected documents. To do that, add the `-IrmReject` parameter to the `Set-IrmConfiguration` command in the script.

You would also need to modify the `$webUrls` variable (for example, <https://contoso.sharepoint.com>) and `$listTitle` variable (for example, `$Reports`).

If you need to disable IRM for user's OneDrive libraries, see the [Script to disable IRM for OneDrive](#) section.

[Additional script to output all OneDrive URLs to a .CSV file](#)

For step 4c above, you can use the following Windows PowerShell script to extract the URLs for all users' OneDrive

libraries, which you can then check, edit if necessary, and then import into the main script.

This script also requires the [SharePoint Client Components SDK](#) and the [SharePoint Management Shell](#). Follow the same instructions to copy and paste it, save the file locally (for example, "ReportOneDriveForBusinessSiteInfo.ps1"), modify the `$sharepointAdminCenterUrl` and `$tenantAdmin` values as before, and then run the script.

**\*\*Disclaimer\*\*:** This sample script is not supported under any Microsoft standard support program or service. This sample script is provided AS IS without warranty of any kind.

```
Requires Windows PowerShell version 3

<#
Description:

 Queries the search service of an Office 365 tenant to retrieve all OneDrive sites.
 Details of the discovered sites are written to a .CSV file (by
 default, "OneDriveForBusinessSiteInfo_<date>.csv").

Script Installation Requirements:

 SharePoint Client Components SDK
 https://www.microsoft.com/download/details.aspx?id=42038

 SharePoint Management Shell
 https://www.microsoft.com/download/details.aspx?id=35588

=====

#>

URL will be in the format https://<tenant-name>-admin.sharepoint.com
$sharepointAdminCenterUrl = "https://contoso-admin.sharepoint.com"

$tenantAdmin = "admin@contoso.onmicrosoft.com"

$reportName = "OneDriveForBusinessSiteInfo_$((Get-Date).ToString("yyyy-MM-dd_hh.mm.ss")).csv"

$oneDriveForBusinessSiteUrls= @()
$resultsProcessed = 0

function Load-SharePointOnlineClientComponentAssemblies
{
 [cmdletbinding()]
 param()

 process
 {
 # assembly location: C:\Program Files\Common Files\microsoft shared\Web Server Extensions\16\ISAPI
 try
 {
 Write-Verbose "Loading Assembly: Microsoft.Office.Client.Policy, Version=16.0.0.0,
Culture=neutral, PublicKeyToken=71e9bce111e9429c"
 [System.Reflection.Assembly]::Load("Microsoft.Office.Client.Policy, Version=16.0.0.0,
Culture=neutral, PublicKeyToken=71e9bce111e9429c") | Out-Null

 Write-Verbose "Loading Assembly: Microsoft.Office.Client.TranslationServices, Version=16.0.0.0,
Culture=neutral, PublicKeyToken=71e9bce111e9429c"
 [System.Reflection.Assembly]::Load("Microsoft.Office.Client.TranslationServices, Version=16.0.0.0,
Culture=neutral, PublicKeyToken=71e9bce111e9429c") | Out-Null

 Write-Verbose "Loading Assembly: Microsoft.SharePoint.Client, Version=16.0.0.0, Culture=neutral,
PublicKeyToken=71e9bce111e9429c"
 [System.Reflection.Assembly]::Load("Microsoft.SharePoint.Client, Version=16.0.0.0,
Culture=neutral, PublicKeyToken=71e9bce111e9429c") | Out-Null

 Write-Verbose "Loading Assembly: Microsoft.SharePoint.Client.DocumentManagement, Version=16.0.0.0,
Culture=neutral, PublicKeyToken=71e9bce111e9429c"
 [System.Reflection.Assembly]::Load("Microsoft.SharePoint.Client.DocumentManagement, Version=16.0.0.0,
Culture=neutral, PublicKeyToken=71e9bce111e9429c") | Out-Null
 }
 }
}
```

```

Culture=neutral, PublicKeyToken=71e9bce111e9429c"
[System.Reflection.Assembly]::Load("Microsoft.SharePoint.Client.DocumentManagement,
Version=16.0.0.0, Culture=neutral, PublicKeyToken=71e9bce111e9429c") | Out-Null

 Write-Verbose "Loading Assembly: Microsoft.SharePoint.Client.Publishing, Version=16.0.0.0,
Culture=neutral, PublicKeyToken=71e9bce111e9429c"
 [System.Reflection.Assembly]::Load("Microsoft.SharePoint.Client.Publishing, Version=16.0.0.0,
Culture=neutral, PublicKeyToken=71e9bce111e9429c") | Out-Null

 Write-Verbose "Loading Assembly: Microsoft.SharePoint.Client.Runtime, Version=16.0.0.0,
Culture=neutral, PublicKeyToken=71e9bce111e9429c"
 [System.Reflection.Assembly]::Load("Microsoft.SharePoint.Client.Runtime, Version=16.0.0.0,
Culture=neutral, PublicKeyToken=71e9bce111e9429c") | Out-Null

 Write-Verbose "Loading Assembly: Microsoft.SharePoint.Client.Search.Applications,
Version=16.0.0.0, Culture=neutral, PublicKeyToken=71e9bce111e9429c"
 [System.Reflection.Assembly]::Load("Microsoft.SharePoint.Client.Search.Applications,
Version=16.0.0.0, Culture=neutral, PublicKeyToken=71e9bce111e9429c") | Out-Null

 Write-Verbose "Loading Assembly: Microsoft.SharePoint.Client.Search, Version=16.0.0.0,
Culture=neutral, PublicKeyToken=71e9bce111e9429c"
 [System.Reflection.Assembly]::Load("Microsoft.SharePoint.Client.Search, Version=16.0.0.0,
Culture=neutral, PublicKeyToken=71e9bce111e9429c") | Out-Null

 Write-Verbose "Loading Assembly: Microsoft.SharePoint.Client.Taxonomy, Version=16.0.0.0,
Culture=neutral, PublicKeyToken=71e9bce111e9429c"
 [System.Reflection.Assembly]::Load("Microsoft.SharePoint.Client.Taxonomy, Version=16.0.0.0,
Culture=neutral, PublicKeyToken=71e9bce111e9429c") | Out-Null

 Write-Verbose "Loading Assembly: Microsoft.SharePoint.Client.UserProfiles, Version=16.0.0.0,
Culture=neutral, PublicKeyToken=71e9bce111e9429c"
 [System.Reflection.Assembly]::Load("Microsoft.SharePoint.Client.UserProfiles, Version=16.0.0.0,
Culture=neutral, PublicKeyToken=71e9bce111e9429c") | Out-Null

 return $true
 }
 catch
 {
 if($_.Exception.Message -match "Could not load file or assembly")
 {
 Write-Error -Message "Unable to load the SharePoint Server 2013 Client Components.\`nDownload
Location: https://www.microsoft.com/download/details.aspx?id=42038"
 }
 else
 {
 Write-Error -Exception $_.Exception
 }
 return $false
 }
}
}

function Load-SharePointOnlineModule
{
 [cmdletbinding()]
 param()

 process
 {
 do
 {
 # Installation location: C:\Program Files\SharePoint Online Management
 Shell\Microsoft.Online.SharePoint.PowerShell
 $spoModule = Get-Module -Name Microsoft.Online.SharePoint.PowerShell -ErrorAction SilentlyContinue

 if(-not $spoModule)
 {
 try
 {

```

```

 Import-Module Microsoft.Online.SharePoint.PowerShell -DisableNameChecking
 return $true
 }
 catch
 {
 if($_.Exception.Message -match "Could not load file or assembly")
 {
 Write-Error -Message "Unable to load the SharePoint Online Management Shell.\nDownload Location: https://www.microsoft.com/download/details.aspx?id=35588"
 }
 else
 {
 Write-Error -Exception $_.Exception
 }
 return $false
 }
}
else
{
 return $true
}
}

while(-not $spoModule)
{
}

function Get-CredentialFromCredentialCache
{
 [cmdletbinding()]
 param([string]$CredentialName)

 #if(Test-Path variable:\global:CredentialCache)
 if(Get-Variable O365TenantAdminCredentialCache -Scope Global -ErrorAction SilentlyContinue)
 {
 if($global:O365TenantAdminCredentialCache.ContainsKey($CredentialName))
 {
 Write-Verbose "Credential Cache Hit: $CredentialName"
 return $global:O365TenantAdminCredentialCache[$CredentialName]
 }
 }
 Write-Verbose "Credential Cache Miss: $CredentialName"
 return $null
}

function Add-CredentialToCredentialCache
{
 [cmdletbinding()]
 param([System.Management.Automation.PSCredential]$Credential)

 if(-not (Get-Variable CredentialCache -Scope Global -ErrorAction SilentlyContinue))
 {
 Write-Verbose "Initializing the Credential Cache"
 $global:O365TenantAdminCredentialCache = @{}
 }

 Write-Verbose "Adding Credential to the Credential Cache"
 $global:O365TenantAdminCredentialCache[$Credential.UserName] = $Credential
}

load the required assemblies and Windows PowerShell modules

if(-not ((Load-SharePointOnlineClientComponentAssemblies) -and (Load-SharePointOnlineModule))) { return }

Add the credentials to the client context and SharePoint service connection

check for cached credentials to use
$o365TenantAdminCredential = Get-CredentialFromCredentialCache -CredentialName $tenantAdmin

if(-not $o365TenantAdminCredential)

```

```

{
 # when credentials are not cached, prompt for the tenant admin credentials
 $o365TenantAdminCredential = Get-Credential -UserName $tenantAdmin -Message "Enter the password for
the Office 365 admin"

 if(-not $o365TenantAdminCredential -or -not $o365TenantAdminCredential.UserName -or
$o365TenantAdminCredential.Password.Length -eq 0)
 {
 Write-Error -Message "Could not validate the supplied tenant admin credentials"
 return
 }

 # add the credentials to the cache
 Add-CredentialToCredentialCache -Credential $o365TenantAdminCredential
}

establish the client context and set the credentials to connect to the site

$clientContext = New-Object Microsoft.SharePoint.Client.ClientContext($sharepointAdminCenterUrl)
$clientContext.Credentials = New-Object
Microsoft.SharePoint.Client.SharePointOnlineCredentials($o365TenantAdminCredential.UserName,
$o365TenantAdminCredential.Password)

run a query against the Office 365 tenant search service to retrieve all OneDrive URLs

do
{
 # build the query object
 $query = New-Object Microsoft.SharePoint.Client.Search.Query.KeywordQuery($clientContext)
 $query.TrimDuplicates = $false
 $query.RowLimit = 500
 $query.QueryText = "SPSiteUrl:'/personal/' AND contentclass:STS_Site"
 $query.StartRow = $resultsProcessed
 $query.TotalRowsExactMinimum = 500000

 # run the query
 $searchExecutor = New-Object Microsoft.SharePoint.Client.Search.Query.SearchExecutor($clientContext)
 $queryResults = $searchExecutor.ExecuteQuery($query)
 $clientContext.ExecuteQuery()

 # enumerate the search results and store the site URLs
 $queryResults.Value[0].ResultRows | % {
 $oneDriveForBusinessSiteUrls += $_.Path
 $resultsProcessed++
 }
}
while($resultsProcessed -lt $queryResults.Value.TotalRows)

$oneDriveForBusinessSiteUrls | Out-File -FilePath $reportName

```

#### Script to disable IRM for OneDrive

Use the following sample script if you need to disable IRM for users' OneDrive.

This script also requires the [SharePoint Client Components SDK](#) and the [SharePoint Management Shell](#). Copy and paste the contents, save the file locally (for example, "Disable-IRMOnOneDriveForBusiness.ps1"), and modify the `$sharepointAdminCenterUrl` and `$tenantAdmin` values. Manually specify the OneDrive URLs or use the script in the previous section so that you can import these, and then run the script.

**\*\*Disclaimer\*\*:** This sample script is not supported under any Microsoft standard support program or service. This sample script is provided AS IS without warranty of any kind.

```

Requires Windows PowerShell version 3

<#
Description:

```

Disables IRM for OneDrive and can also be used for SharePoint libraries and lists

Script Installation Requirements:

SharePoint Client Components SDK  
<https://www.microsoft.com/download/details.aspx?id=42038>

SharePoint Management Shell  
<https://www.microsoft.com/download/details.aspx?id=35588>

=====

#>

```
$sharepointAdminCenterUrl = "https://contoso-admin.sharepoint.com"
```

```
$tenantAdmin = "admin@contoso.com"
```

```
$webUrls = @("https://contoso-my.sharepoint.com/personal/user1_contoso_com",
 "https://contoso-my.sharepoint.com/personal/user2_contoso_com",
 "https://contoso-my.sharepoint.com/personal/person3_contoso_com")
```

<# As an alternative to specifying the URLs as an array, you can import them from a CSV file (no header, single value per row).

Then, use: \$webUrls = Get-Content -Path "File\_path\_and\_name.csv"

#>

```
$listTitle = "Documents"
```

```
function Load-SharePointOnlineClientComponentAssemblies
{
 [cmdletbinding()]
 param()

 process
 {
 # assembly location: C:\Program Files\Common Files\microsoft shared\Web Server Extensions\16\ISAPI
 try
 {
 Write-Verbose "Loading Assembly: Microsoft.Office.Client.Policy, Version=16.0.0.0,
Culture=neutral, PublicKeyToken=71e9bce111e9429c"
 [System.Reflection.Assembly]::Load("Microsoft.Office.Client.Policy, Version=16.0.0.0,
Culture=neutral, PublicKeyToken=71e9bce111e9429c") | Out-Null

 Write-Verbose "Loading Assembly: Microsoft.Office.Client.TranslationServices, Version=16.0.0.0,
Culture=neutral, PublicKeyToken=71e9bce111e9429c"
 [System.Reflection.Assembly]::Load("Microsoft.Office.Client.TranslationServices, Version=16.0.0.0,
Culture=neutral, PublicKeyToken=71e9bce111e9429c") | Out-Null

 Write-Verbose "Loading Assembly: Microsoft.SharePoint.Client, Version=16.0.0.0, Culture=neutral,
PublicKeyToken=71e9bce111e9429c"
 [System.Reflection.Assembly]::Load("Microsoft.SharePoint.Client, Version=16.0.0.0,
Culture=neutral, PublicKeyToken=71e9bce111e9429c") | Out-Null

 Write-Verbose "Loading Assembly: Microsoft.SharePoint.Client.DocumentManagement, Version=16.0.0.0,
Culture=neutral, PublicKeyToken=71e9bce111e9429c"
 [System.Reflection.Assembly]::Load("Microsoft.SharePoint.Client.DocumentManagement,
Version=16.0.0.0, Culture=neutral, PublicKeyToken=71e9bce111e9429c") | Out-Null

 Write-Verbose "Loading Assembly: Microsoft.SharePoint.Client.Publishing, Version=16.0.0.0,
Culture=neutral, PublicKeyToken=71e9bce111e9429c"
 [System.Reflection.Assembly]::Load("Microsoft.SharePoint.Client.Publishing, Version=16.0.0.0,
Culture=neutral, PublicKeyToken=71e9bce111e9429c") | Out-Null

 Write-Verbose "Loading Assembly: Microsoft.SharePoint.Client.Runtime, Version=16.0.0.0,
Culture=neutral, PublicKeyToken=71e9bce111e9429c"
 [System.Reflection.Assembly]::Load("Microsoft.SharePoint.Client.Runtime, Version=16.0.0.0,
Culture=neutral, PublicKeyToken=71e9bce111e9429c") | Out-Null
 }
 }
}
```

```

 Write-Verbose "Loading Assembly: Microsoft.SharePoint.Client.Search.Applications,
Version=16.0.0.0, Culture=neutral, PublicKeyToken=71e9bce111e9429c"
 [System.Reflection.Assembly]::Load("Microsoft.SharePoint.Client.Search.Applications,
Version=16.0.0.0, Culture=neutral, PublicKeyToken=71e9bce111e9429c") | Out-Null

 Write-Verbose "Loading Assembly: Microsoft.SharePoint.Client.Search, Version=16.0.0.0,
Culture=neutral, PublicKeyToken=71e9bce111e9429c"
 [System.Reflection.Assembly]::Load("Microsoft.SharePoint.Client.Search, Version=16.0.0.0,
Culture=neutral, PublicKeyToken=71e9bce111e9429c") | Out-Null

 Write-Verbose "Loading Assembly: Microsoft.SharePoint.Client.Taxonomy, Version=16.0.0.0,
Culture=neutral, PublicKeyToken=71e9bce111e9429c"
 [System.Reflection.Assembly]::Load("Microsoft.SharePoint.Client.Taxonomy, Version=16.0.0.0,
Culture=neutral, PublicKeyToken=71e9bce111e9429c") | Out-Null

 Write-Verbose "Loading Assembly: Microsoft.SharePoint.Client.UserProfiles, Version=16.0.0.0,
Culture=neutral, PublicKeyToken=71e9bce111e9429c"
 [System.Reflection.Assembly]::Load("Microsoft.SharePoint.Client.UserProfiles, Version=16.0.0.0,
Culture=neutral, PublicKeyToken=71e9bce111e9429c") | Out-Null

 return $true
 }
 catch
 {
 if($_.Exception.Message -match "Could not load file or assembly")
 {
 Write-Error -Message "Unable to load the SharePoint Server 2013 Client Components. `nDownload
Location: https://www.microsoft.com/download/details.aspx?id=42038"
 }
 else
 {
 Write-Error -Exception $_.Exception
 }
 return $false
 }
}
}

function Load-SharePointOnlineModule
{
 [cmdletbinding()]
 param()

 process
 {
 do
 {
 # Installation location: C:\Program Files\SharePoint Online Management
 Shell\Microsoft.Online.SharePoint.PowerShell
 $spoModule = Get-Module -Name Microsoft.Online.SharePoint.PowerShell -ErrorAction SilentlyContinue

 if(-not $spoModule)
 {
 try
 {
 Import-Module Microsoft.Online.SharePoint.PowerShell -DisableNameChecking
 return $true
 }
 catch
 {
 if($_.Exception.Message -match "Could not load file or assembly")
 {
 Write-Error -Message "Unable to load the SharePoint Online Management Shell. `nDownload
Location: https://www.microsoft.com/download/details.aspx?id=35588"
 }
 else
 {
 Write-Error -Exception $_.Exception
 }
 }
 }
 }
 }
}

```

```

 }
 return $false
 }
}
else
{
 return $true
}
}
while(-not $spoModule)
}
}

function Remove-IrmConfiguration
{
[cmdletbinding()]
param(
 [parameter(Mandatory=$true)][Microsoft.SharePoint.Client.List]$List
)

process
{
 Write-Verbose "Disabling IRM Configuration on '$($List.Title)'

 $List.IrmEnabled = $false
 $List.IrmExpire = $false
 $List.IrmReject = $false
 $List.InformationRightsManagementSettings.Reset()
}
end
{
 if($List)
 {
 Write-Verbose "Committing IRM configuration settings on '$($list.Title)'"
 $list.InformationRightsManagementSettings.Update()
 $list.Update()
 $script:clientContext.Load($list)
 $script:clientContext.ExecuteQuery()
 }
}
}

function Get-CredentialFromCredentialCache
{
[cmdletbinding()]
param([string]$CredentialName)

#if(Test-Path variable:\global:CredentialCache)
if(Get-Variable 0365TenantAdminCredentialCache -Scope Global -ErrorAction SilentlyContinue)
{
 if($global:0365TenantAdminCredentialCache.ContainsKey($CredentialName))
 {
 Write-Verbose "Credential Cache Hit: $CredentialName"
 return $global:0365TenantAdminCredentialCache[$CredentialName]
 }
}
Write-Verbose "Credential Cache Miss: $CredentialName"
return $null
}

function Add-CredentialToCredentialCache
{
[cmdletbinding()]
param([System.Management.Automation.PSCredential]$Credential)

if(-not (Get-Variable CredentialCache -Scope Global -ErrorAction SilentlyContinue))
{
 Write-Verbose "Initializing the Credential Cache"
 $global:0365TenantAdminCredentialCache = @{}
}

```

```

}

Write-Verbose "Adding Credential to the Credential Cache"
$global:O365TenantAdminCredentialCache[$Credential.UserName] = $Credential
}

load the required assemblies and Windows PowerShell modules

if(-not ((Load-SharePointOnlineClientComponentAssemblies) -and (Load-SharePointOnlineModule))) { return }

Add the credentials to the client context and SharePoint service connection

check for cached credentials to use
$o365TenantAdminCredential = Get-CredentialFromCredentialCache -CredentialName $tenantAdmin

if(-not $o365TenantAdminCredential)
{
 # when credentials are not cached, prompt for the tenant admin credentials
 $o365TenantAdminCredential = Get-Credential -UserName $tenantAdmin -Message "Enter the password for
the Office 365 admin"

 if(-not $o365TenantAdminCredential -or -not $o365TenantAdminCredential.UserName -or
$o365TenantAdminCredential.Password.Length -eq 0)
 {
 Write-Error -Message "Could not validate the supplied tenant admin credentials"
 return
 }

 # add the credentials to the cache
 Add-CredentialToCredentialCache -Credential $o365TenantAdminCredential
}

connect to Office365 first, required for SharePoint cmdlets to run

Connect-SPOService -Url $sharepointAdminCenterUrl -Credential $o365TenantAdminCredential

enumerate each of the specified site URLs

foreach($webUrl in $webUrls)
{
 $grantedSiteCollectionAdmin = $false

 try
 {
 # establish the client context and set the credentials to connect to the site
 $script:clientContext = New-Object Microsoft.SharePoint.Client.ClientContext($webUrl)
 $script:clientContext.Credentials = New-Object
Microsoft.SharePoint.Client.SharePointOnlineCredentials($o365TenantAdminCredential.UserName,
$o365TenantAdminCredential.Password)

 # initialize the site and web context
 $script:clientContext.Load($script:clientContext.Site)
 $script:clientContext.Load($script:clientContext.Web)
 $script:clientContext.ExecuteQuery()

 # load and ensure the tenant admin user account if present on the target SharePoint site
 $tenantAdminUser = $script:clientContext.Web.EnsureUser($o365TenantAdminCredential.UserName)
 $script:clientContext.Load($tenantAdminUser)
 $script:clientContext.ExecuteQuery()

 # check if the tenant admin is a site admin
 if(-not $tenantAdminUser.IsSiteAdmin)
 {
 try
 {
 # grant the tenant admin temporary admin rights to the site collection
 Set-SPOUser -Site $script:clientContext.Site.Url -LoginName
$o365TenantAdminCredential.UserName -IsSiteCollectionAdmin $true | Out-Null
 $grantedSiteCollectionAdmin = $true
 }
 }
 }
}

```

```

 }
 catch
 {
 Write-Error $_.Exception
 return
 }
}

try
{
 # load the list orlibrary using CSOM

 $list = $null
 $list = $script:clientContext.Web.Lists.GetByTitle($listTitle)
 $script:clientContext.Load($list)
 $script:clientContext.ExecuteQuery()

 Remove-IrmConfiguration -List $list
}
catch
{
 Write-Error -Message "Error setting IRM configuration on site: $webUrl.\nError Details:
$($_.Exception.ToString())"
}
}
finally
{
 if($grantedSiteCollectionAdmin)
 {
 # remove the temporary admin rights to the site collection
 Set-SPOUser -Site $script:clientContext.Site.Url -LoginName
 $o365TenantAdminCredential.UserName -IsSiteCollectionAdmin $false | Out-Null
 }
}
}

Disconnect-SPOSERVICE -ErrorAction SilentlyContinue

```

# Office apps: Configuration for clients to use the Azure Rights Management service

7/20/2020 • 2 minutes to read • [Edit Online](#)

Applies to: [Azure Information Protection](#), [Office 365](#)

Use this information to determine what you need to do so that Office apps work with the Azure Rights Management service from Azure Information Protection.

## Office 365 apps, Office 2019, Office 2016, and Office 2013

Because these later versions of Office natively support the Azure Rights Management service, no client computer configuration is required to support the information rights management (IRM) features for applications such as Word, Excel, PowerPoint, Outlook, and Outlook on the web. All users have to do for these apps on Windows, is sign in to their Office applications with their Office 365 credentials. They can then protect files and emails, and use files and emails that have been protected by others.

### User instructions for Office for Mac

Users who have Office for Mac must first verify their credentials before they can protect content. For example:

1. Open Outlook and create a profile by using your Office 365 work or school account.
2. Create a new message and on the **Options** tab, select **Permissions**, and then select **Verify Credentials**. When prompted, specify your Office 365 work or school account details again, and select **Sign in**.

This action downloads the Azure Rights Management templates and **Verify Credentials** is now replaced with options that include **No Restrictions**, **Do Not Forward**, and any Azure Rights Management templates that are published for your tenant.

3. You can now cancel this new message.
4. To protect an email message or a document: On the **Options** tab, select **Permissions** and choose an option or template that protects your email or document.

## Office 2010

For client computers to use the Azure Rights Management service with Office 2010, they must have the Azure Information Protection client (classic). No further configuration is required other than users must sign in with their Office 365 credentials and they can then protect files and use files that have been protected by others.

For more information about the Azure Information Protection client (classic), see [Azure Information Protection client: Installation and configuration for clients](#).

# Azure Information Protection client: Installation and configuration for clients

7/20/2020 • 2 minutes to read • [Edit Online](#)

Applies to: [Azure Information Protection](#), [Office 365](#)

## NOTE

To provide a unified and streamlined customer experience, **Azure Information Protection client (classic)** and **Label Management** in the Azure Portal are being **deprecated** as of March 31, 2021. This time-frame allows all current Azure Information Protection customers to transition to our unified labeling solution using the Microsoft Information Protection Unified Labeling platform. Learn more in the official [deprecation notice](#).

Computers running Office 2010 require either the Azure Information Protection client (classic) or the Azure Information Protection unified labeling client to authenticate to the Azure Information Protection service.

Not sure of the difference between these two clients? See [What's the difference between the Azure Information Protection client and the Azure Information Protection unified labeling client?](#)

These clients are also recommended for all Windows computers because they install an Office add-in so that users can easily label and protect documents and emails directly from the Office ribbon. These clients also offer labeling and protection for file types that are not natively supported by the protection service (Azure Rights Management), and a viewer for protected files that can't be opened by Office apps. There's a similar viewer for iOS and Android.

The classic client also supports a document tracking site for users to track and revoke files that they have protected.

## The Azure Information Protection client for Windows: Installation and configuration

For an enterprise installation and configuration of the client for Windows, see the following admin guides:

- Unified labeling client: [Azure Information Protection unified labeling client administrator guide](#)(./rms-client/client-admin-guide.md)
- Classic client: [Azure Information Protection client administrator guide](#)

However, if you want to quickly install and test these clients for a single computer, see the following instructions from the user guides:

- Unified labeling client: [Download and install the Azure Information Protection unified labeling client](#)
- Classic client: [Download and install the Azure Information Protection client from the Azure Information Protection client user guide.](#)

## The Azure Information Protection app for iOS and Android: Installation and management

To install the Azure Information Protection app viewer for iOS and Android, use the links on the [Microsoft Azure Information Protection page](#). No configuration is required.

## NOTE

For Mac computers, links from this page download the RMS sharing app. These computers do not support the Azure Information Protection client.

## Integration with Intune

Because the Azure Information Protection viewer app uses the Microsoft Intune App Software Development Kit, when iOS and Android devices are enrolled by Intune, you can deploy and manage the Azure Information Protection viewer app for these devices:

1. [Add the Azure Information Protection app to Intune](#)

2. Do one or both of the following actions:

- Deploy the app by [assigning it to users](#)
- Manage the app by using [app protection policies](#)

Additional information for when you add the Azure Information Protection app to Intune:

- For iOS: Search for and add the app from Intune.
- For Android: When you add the app, use the following **Appstore URL**:

```
https://play.google.com/store/apps/details?id=com.microsoft.ipviewer
```

When the Azure Information Protection app is configured for an app protection policy for Android devices, in addition to opening protected text, images, and PDF documents, this app can also open audio and video files. For more information, see [View media files with the Azure Information Protection app](#).

## Next steps

After you have installed and configured Azure Information Protection clients, you might need to learn more about how the client interprets the different usage rights that can be used to protect documents and emails. For more information, see [Configuring usage rights for Azure Information Management](#).

# Configuring usage rights for Azure Information Protection

7/20/2020 • 21 minutes to read • [Edit Online](#)

Applies to: [Azure Information Protection](#), [Office 365](#)

When you configure sensitivity labels or protection templates for encryption, you select the usage rights that will then be automatically applied when the label or template is selected by users, administrators, or configured services. For example, in the Azure portal you can select roles that configure a logical grouping of usage rights, or you can configure the individual rights. Alternatively users might select and apply the usage rights themselves.

Use this article to help you configure the usage rights you want for the application you're using and understand how these rights are designed to be interpreted by applications. However, applications might vary in how they implement the rights so always consult their documentation and do your own testing with the applications that users use to check the behavior before you deploy in production.

## NOTE

For completeness, this article includes values from the Azure classic portal, which was retired January 08, 2018.

## Usage rights and descriptions

The following table lists and describes the usage rights that Rights Management supports, and how they are used and interpreted. They are listed by their **common name**, which is typically how you might see the usage right displayed or referenced, as a more friendly version of the single-word value that is used in the code (the **Encoding in policy** value).

In this table:

- The **API Constant or Value** is the SDK name for an MSIPC API call, used when you write an application that checks for a usage right, or adds a usage right to a policy.
- The **labeling admin center** refers to where you configure sensitivity labels and can be either the Microsoft 365 compliance center, the Microsoft 365 security center, or the Office 365 Security & Compliance Center.

| USAGE RIGHT | DESCRIPTION | IMPLEMENTATION |
|-------------|-------------|----------------|
|-------------|-------------|----------------|

| Usage right                                                                                    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Implementation                                                                                                                                                                                                                                                                                                                                                                           |
|------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Common name: <b>Edit Content</b>, <b>Edit</b></p> <p>Encoding in policy: <b>DOCEDIT</b></p> | <p>Allows the user to modify, rearrange, format, or sort the content inside the application. It does not grant the right to save the edited copy.</p> <p>In Word, unless you have Office 365 ProPlus with a minimum version of <b>1807</b>, this right isn't sufficient to turn on or turn off <b>Track Changes</b>, or to use all the track changes features as a reviewer. Instead, to use all the track changes options requires the following right: <b>Full Control</b>.</p>                                          | <p>Office custom rights: As part of the <b>Change</b> and <b>Full Control</b> options.</p> <p>Name in the Azure classic portal: <b>Edit Content</b></p> <p>Name in the labeling admin center and Azure portal: <b>Edit Content</b>, <b>Edit (DOCEDIT)</b></p> <p>Name in AD RMS templates: <b>Edit</b></p> <p>API constant or value: Not applicable.</p>                                 |
| <p>Common name: <b>Save</b></p> <p>Encoding in policy: <b>EDIT</b></p>                         | <p>Allows the user to save the document to the current location.</p> <p>In Office applications, this right also allows the user to modify the document and save it to a new location and a new name if the selected file format natively supports Rights Management protection. The file format restriction ensures that the original protection cannot be removed from the file.</p>                                                                                                                                      | <p>Office custom rights: As part of the <b>Change</b> and <b>Full Control</b> options.</p> <p>Name in the Azure classic portal: <b>Save File</b></p> <p>Name in the labeling admin center and Azure portal: <b>Save (EDIT)</b></p> <p>Name in AD RMS templates: <b>Save</b></p> <p>API constant or value:<br/> <code>IPC_GENERIC_WRITE L"EDIT"</code></p>                                |
| <p>Common name: <b>Comment</b></p> <p>Encoding in policy: <b>COMMENT</b></p>                   | <p>Enables the option to add annotations or comments to the content.</p> <p>This right is available in the SDK, is available as an ad-hoc policy in the AzureInformationProtection and RMS Protection module for Windows PowerShell, and has been implemented in some software vendor applications. However, it is not widely used and is not supported by Office applications.</p>                                                                                                                                        | <p>Office custom rights: Not implemented.</p> <p>Name in the Azure classic portal: Not implemented.</p> <p>Name in the labeling admin center and Azure portal: Not implemented.</p> <p>Name in AD RMS templates: Not implemented.</p> <p>API constant or value:<br/> <code>IPC_GENERIC_COMMENT L"COMMENT"</code></p>                                                                     |
| <p>Common name: <b>Save As</b>, <b>Export</b></p> <p>Encoding in policy: <b>EXPORT</b></p>     | <p>Enables the option to save the content to a different file name (Save As).</p> <p>For the Azure Information Protection client, the file can be saved without protection, and also reprotected with new settings and permissions. These permitted actions mean that a user who has this right can change or remove an Azure Information Protection label from a protected document or email.</p> <p>This right also allows the user to perform other export options in applications, such as <b>Send to OneNote</b>.</p> | <p>Office custom rights: As part of the <b>Full Control</b> option.</p> <p>Name in the Azure classic portal: <b>Export Content (Save As)</b></p> <p>Name in the labeling admin center and Azure portal: <b>Save As</b>, <b>Export (EXPORT)</b></p> <p>Name in AD RMS templates: <b>Export (Save As)</b></p> <p>API constant or value:<br/> <code>IPC_GENERIC_EXPORT L"EXPORT"</code></p> |

| Usage right                                                                     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Implementation                                                                                                                                                                                                                                                                                                                                                                     |
|---------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Common name: <b>Forward</b></p> <p>Encoding in policy: <b>FORWARD</b></p>    | <p>Enables the option to forward an email message and to add recipients to the <b>To</b> and <b>Cc</b> lines. This right does not apply to documents; only email messages.</p> <p>Does not allow the forwarder to grant rights to other users as part of the forward action.</p> <p>When you grant this right, also grant the <b>Edit Content</b>, <b>Edit</b> right (common name), and additionally grant the <b>Save</b> right (common name) to ensure that the protected email message is not delivered as an attachment. Also specify these rights when you send an email to another organization that uses the Outlook client or Outlook web app. Or, for users in your organization that are exempt from using Rights Management protection because you have implemented <a href="#">onboarding controls</a>.</p> | <p>Office custom rights: Denied when using the <b>Do Not Forward</b> standard policy.</p> <p>Name in the Azure classic portal: <b>Forward</b></p> <p>Name in the labeling admin center and Azure portal: <b>Forward (FORWARD)</b></p> <p>Name in AD RMS templates: <b>Forward</b></p> <p>API constant or value:<br/> <code>IPC_EMAIL_FORWARD L"FORWARD"</code></p>                 |
| <p>Common name: <b>Full Control</b></p> <p>Encoding in policy: <b>OWNER</b></p> | <p>Grants all rights to the document and all available actions can be performed.</p> <p>Includes the ability to remove protection and reprotect a document.</p> <p>Note that this usage right is not the same as the <a href="#">Rights Management owner</a>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | <p>Office custom rights: As the <b>Full Control</b> custom option.</p> <p>Name in the Azure classic portal: <b>Full Control</b></p> <p>Name in the labeling admin center and Azure portal: <b>Full Control (OWNER)</b></p> <p>Name in AD RMS templates: <b>Full Control</b></p> <p>API constant or value:<br/> <code>IPC_GENERIC_ALL L"OWNER"</code></p>                           |
| <p>Common name: <b>Print</b></p> <p>Encoding in policy: <b>PRINT</b></p>        | <p>Enables the options to print the content.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | <p>Office custom rights: As the <b>Print Content</b> option in custom permissions. Not a per-recipient setting.</p> <p>Name in the Azure classic portal: <b>Print</b></p> <p>Name in the labeling admin center and Azure portal: <b>Print (PRINT)</b></p> <p>Name in AD RMS templates: <b>Print</b></p> <p>API constant or value:<br/> <code>IPC_GENERIC_PRINT L"PRINT"</code></p> |

| Usage right                                                                        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Implementation                                                                                                                                                                                                                                                                                                                                                                                         |
|------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Common name: <b>Reply</b></p> <p>Encoding in policy: <b>REPLY</b></p>           | <p>Enables the <b>Reply</b> option in an email client, without allowing changes in the <b>To</b> or <b>Cc</b> lines.</p> <p>When you grant this right, also grant the <b>Edit Content</b>, <b>Edit</b> right (common name), and additionally grant the <b>Save</b> right (common name) to ensure that the protected email message is not delivered as an attachment. Also specify these rights when you send an email to another organization that uses the Outlook client or Outlook web app. Or, for users in your organization that are exempt from using Rights Management protection because you have implemented <a href="#">onboarding controls</a>.</p>                         | <p>Office custom rights: Not applicable.</p> <p>Name in the Azure classic portal: <b>Reply</b></p> <p>Name in the Azure classic portal: <b>Reply (REPLY)</b></p> <p>Name in AD RMS templates: <b>Reply</b></p> <p>API constant or value:<br/> <span style="border: 1px solid black; padding: 2px;">IPC_EMAIL_REPLY</span></p>                                                                          |
| <p>Common name: <b>Reply All</b></p> <p>Encoding in policy: <b>REPLYALL</b></p>    | <p>Enables the <b>Reply All</b> option in an email client, but doesn't allow the user to add recipients to the <b>To</b> or <b>Cc</b> lines.</p> <p>When you grant this right, also grant the <b>Edit Content</b>, <b>Edit</b> right (common name), and additionally grant the <b>Save</b> right (common name) to ensure that the protected email message is not delivered as an attachment. Also specify these rights when you send an email to another organization that uses the Outlook client or Outlook web app. Or, for users in your organization that are exempt from using Rights Management protection because you have implemented <a href="#">onboarding controls</a>.</p> | <p>Office custom rights: Not applicable.</p> <p>Name in the Azure classic portal: <b>Reply All</b></p> <p>Name in the labeling admin center and Azure portal: <b>Reply All (REPLY ALL)</b></p> <p>Name in AD RMS templates: <b>Reply All</b></p> <p>API constant or value:<br/> <span style="border: 1px solid black; padding: 2px;">IPC_EMAIL_REPLYALL L"REPLYALL"</span></p>                         |
| <p>Common name: <b>View, Open, Read</b></p> <p>Encoding in policy: <b>VIEW</b></p> | <p>Allows the user to open the document and see the content.</p> <p>In Excel, this right isn't sufficient to sort data, which requires the following right: <b>Edit Content</b>, <b>Edit</b>. To filter data in Excel, you need the following two rights: <b>Edit Content</b>, <b>Edit</b> and <b>Copy</b>.</p>                                                                                                                                                                                                                                                                                                                                                                         | <p>Office custom rights: As the <b>Read</b> custom policy, <b>View</b> option.</p> <p>Name in the Azure classic portal: <b>View</b></p> <p>Name in the labeling admin center and Azure portal: <b>View, Open, Read (VIEW)</b></p> <p>Name in AD RMS templates: <b>Read</b></p> <p>API constant or value:<br/> <span style="border: 1px solid black; padding: 2px;">IPC_GENERIC_READ L"VIEW"</span></p> |

| Usage Right                                                                               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Implementation                                                                                                                                                                                                                                                                                                                                                                                         |
|-------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Common name: <b>Copy</b></p> <p>Encoding in policy: <b>EXTRACT</b></p>                 | <p>Enables options to copy data (including screen captures) from the document into the same or another document.</p> <p>In some applications, it also allows the whole document to be saved in unprotected form.</p> <p>In Skype for Business and similar screen-sharing applications, the presenter must have this right to successfully present a protected document. If the presenter does not have this right, the attendees cannot view the document and it displays as blacked out to them.</p> | <p>Office custom rights: As the <b>Allow users with Read access to copy content</b> custom policy option.</p> <p>Name in the Azure classic portal: <b>Copy and Extract content</b></p> <p>Name in the labeling admin center and Azure portal: <b>Copy (EXTRACT)</b></p> <p>Name in AD RMS templates: <b>Extract</b></p> <p>API constant or value:<br/> <code>IPC_GENERIC_EXTRACT L"EXTRACT"</code></p> |
| <p>Common name: <b>View Rights</b></p> <p>Encoding in policy: <b>VIEWRIGHTSDATA</b></p>   | <p>Allows the user to see the policy that is applied to the document.</p> <p>Not supported by Office apps or Azure Information Protection clients.</p>                                                                                                                                                                                                                                                                                                                                                | <p>Office custom rights: Not implemented.</p> <p>Name in the Azure classic portal: <b>View Assigned Rights</b></p> <p>Name in the labeling admin center and Azure portal: <b>View Rights (VIEWRIGHTSDATA)</b>.</p> <p>Name in AD RMS templates: <b>View Rights</b></p> <p>API constant or value:<br/> <code>IPC_READ_RIGHTS L"VIEWRIGHTSDATA"</code></p>                                               |
| <p>Common name: <b>Change Rights</b></p> <p>Encoding in policy: <b>EDITRIGHTSDATA</b></p> | <p>Allows the user to change the policy that is applied to the document.</p> <p>Includes including removing protection.</p> <p>Not supported by Office apps or Azure Information Protection clients.</p>                                                                                                                                                                                                                                                                                              | <p>Office custom rights: Not implemented.</p> <p>Name in the Azure classic portal: <b>Change Rights</b></p> <p>Name in the labeling admin center and Azure portal: <b>Edit Rights (EDITRIGHTSDATA)</b>.</p> <p>Name in AD RMS templates: <b>Edit Rights</b></p> <p>API constant or value:<br/> <code>PC_WRITE_RIGHTS L"EDITRIGHTSDATA"</code></p>                                                      |

| USAGE RIGHT                                                                 | DESCRIPTION                                                                                                   | IMPLEMENTATION                                                                                                                                                                                                                                                                                                                                                              |
|-----------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Common name: <b>Allow Macros</b><br><br>Encoding in policy: <b>OBJMODEL</b> | Enables the option to run macros or perform other programmatic or remote access to the content in a document. | Office custom rights: As the <b>Allow Programmatic Access</b> custom policy option. Not a per-recipient setting.<br><br>Name in the Azure classic portal: <b>Allow Macros</b><br><br>Name in the labeling admin center and Azure portal: <b>Allow Macros (OBJMODEL)</b><br><br>Name in AD RMS templates: <b>Allow Macros</b><br><br>API constant or value: Not implemented. |

## Rights included in permissions levels

Some applications group usage rights together into permissions levels, to make it easier to select usage rights that are typically used together. These permissions levels help to abstract a level of complexity from users, so they can choose options that are role-based. For example, **Reviewer** and **Co-Author**. Although these options often show users a summary of the rights, they might not include every right that is listed in the previous table.

Use the following table for a list of these permissions levels and a complete list of the usage rights that they contain. The usage rights are listed by their [common name](#).

| PERMISSIONS LEVEL | APPLICATIONS                                                                                    | USAGE RIGHTS INCLUDED                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-------------------|-------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Viewer            | Azure classic portal<br><br>Azure portal<br><br>Azure Information Protection client for Windows | View, Open, Read; View Rights; Reply [1]; Reply All [1]; Allow Macros [2]<br><br>Note: For emails, use Reviewer rather than this permission level to ensure that an email reply is received as an email message rather than an attachment. Reviewer is also required when you send an email to another organization that uses the Outlook client or Outlook web app. Or, for users in your organization that are exempt from using the Azure Rights Management service because you have implemented <a href="#">onboarding controls</a> . |
| Reviewer          | Azure classic portal<br><br>Azure portal<br><br>Azure Information Protection client for Windows | View, Open, Read; Save; Edit Content, Edit; View Rights; Reply: Reply All [3]; Forward [3]; Allow Macros [2]                                                                                                                                                                                                                                                                                                                                                                                                                              |

| PERMISSIONS LEVEL | APPLICATIONS                                    | USAGE RIGHTS INCLUDED                                                                                                                                                   |
|-------------------|-------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Co-Author         | Azure classic portal                            | View, Open, Read; Save; Edit Content, Edit; Copy; View Rights; Allow Macros; Save As, Export [4]; Print; Reply [3]; Reply All [3]; Forward [3]                          |
|                   | Azure portal                                    |                                                                                                                                                                         |
|                   | Azure Information Protection client for Windows |                                                                                                                                                                         |
| Co-Owner          | Azure classic portal                            | View, Open, Read; Save; Edit Content, Edit; Copy; View Rights; Change Rights; Allow Macros; Save As, Export; Print; Reply [3]; Reply All [3]; Forward [3]; Full Control |
|                   | Azure portal                                    |                                                                                                                                                                         |
|                   | Azure Information Protection client for Windows |                                                                                                                                                                         |

Footnote 1

Not included in the labeling admin center or Azure portal.

Footnote 2

For the Azure Information Protection client for Windows, this right is required for the Information Protection bar in Office apps.

Footnote 3

Not applicable to the Azure Information Protection client for Windows.

Footnote 4

Not included in the labeling admin center, the Azure portal, or the Azure Information Protection client for Windows.

## Rights included in the default templates

The following table lists the usage rights that are included when the default templates are created. The usage rights are listed by their [common name](#).

These default templates are created when your subscription was purchased, and the names and usage rights can be [changed](#) in the Azure portal and with [PowerShell](#).

| DISPLAY NAME OF TEMPLATE                                                                                             | USAGE RIGHTS OCTOBER 6, 2017 TO CURRENT DATE                                                                                                                | USAGE RIGHTS BEFORE OCTOBER 6, 2017                                                                         |
|----------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------|
| < <i>organization name</i> > - Confidential<br>View Only<br><br>or<br><br><i>Highly Confidential \ All Employees</i> | View, Open, Read; Copy; View Rights; Allow Macros; Print; Forward; Reply; Reply All; Save; Edit Content, Edit                                               | View, Open, Read                                                                                            |
| < <i>organization name</i> >- Confidential<br><br>or<br><br><i>Confidential \ All Employees</i>                      | View, Open, Read; Save As, Export; Copy; View Rights; Change Rights; Allow Macros; Print; Forward; Reply; Reply All; Save; Edit Content, Edit; Full Control | View, Open, Read; Save As, Export; Edit Content, Edit; View Rights; Allow Macros; Forward; Reply; Reply All |

## Do Not Forward option for emails

Exchange clients and services (for example, the Outlook client, Outlook on the web, Exchange mail flow rules, and DLP actions for Exchange) have an additional information rights protection option for emails: **Do Not Forward**.

Although this option appears to users (and Exchange administrators) as if it's a default Rights Management template that they can select, **Do Not Forward** is not a template. That explains why you cannot see it in the Azure portal when you view and manage protection templates. Instead, the **Do Not Forward** option is a set of usage rights that is dynamically applied by users to their email recipients.

When the **Do Not Forward** option is applied to an email, the email is encrypted and recipients must be authenticated. Then, the recipients cannot forward it, print it, or copy from it. For example, in the Outlook client, the **Forward** button is not available, the **Save As** and **Print** menu options are not available, and you cannot add or change recipients in the **To**, **Cc**, or **Bcc** boxes.

Unprotected [Office documents](#) that are attached to the email automatically inherit the same restrictions. The usage rights applied to these documents are **Edit Content**, **Edit; Save; View, Open, Read**; and **Allow Macros**. If you want different usage rights for an attachment, or your attachment is not an Office document that supports this inherited protection, protect the file before you attach it to the email. You can then assign the specific usage rights that you need for the file.

#### Difference between Do Not Forward and not granting the Forward usage right

There's an important distinction between applying the **Do Not Forward** option and applying a template that doesn't grant the **Forward** usage right to an email: The **Do Not Forward** option uses a dynamic list of authorized users that is based on the user's chosen recipients of the original email; whereas the rights in the template have a static list of authorized users that the administrator has previously specified. What's the difference? Let's take an example:

A user wants to email some information to specific people in the Marketing department that shouldn't be shared with anybody else. Should she protect the email with a template that restricts rights (viewing, replying, and saving) to the Marketing department? Or should she choose the **Do Not Forward** option? Both choices would result in the recipients not able to forward the email.

- If she applied the template, the recipients could still share the information with others in the marketing department. For example, a recipient could use Explorer to drag and drop the email to a shared location or a USB drive. Now, anybody from the marketing department (and the email owner) who has access to this location can view the information in the email.
- If she applied the **Do Not Forward** option, the recipients will not be able to share the information with anybody else in the marketing department by moving the email to another location. In this scenario, only the original recipients (and the email owner) will be able to view the information in the email.

#### NOTE

Use **Do Not Forward** when it's important that only the recipients that the sender chooses should see the information in the email. Use a template for emails to restrict rights to a group of people that the administrator specifies in advance, independently from the sender's chosen recipients.

## Encrypt-Only option for emails

When Exchange Online uses the new capabilities for Office 365 Message Encryption, a new email option becomes available: **Encrypt-Only**.

This option is available to tenants who use Exchange Online and can be selected in Outlook on the web, as another rights protection option for a mail flow rule, as an Office 365 DLP action, and from Outlook (minimum version of [1804](#) for Office 365 ProPlus, and minimum version of 1805 when you have [Office 365 apps that support Azure RMS](#)). For more information about the Encrypt-Only option, see the following blog post announcement from the Office team: [Encrypt only rolling out in Office 365 Message Encryption](#).

When this option is selected, the email is encrypted and recipients must be authenticated. Then, the recipients

have all usage rights except **Save As**, **Export** and **Full Control**. This combination of usage rights means that the recipients have no restrictions except that they cannot remove the protection. For example, a recipient can copy from the email, print it, and forward it.

Similarly, by default, unprotected [Office documents](#) that are attached to the email inherit the same permissions. These documents are automatically protected and when they are downloaded, they can be saved, edited, copied, and printed from Office applications by the recipients. When the document is saved by a recipient, it can be saved to a new name and even a different format. However, only file formats that support protection are available so that the document cannot be saved without the original protection. If you want different usage rights for an attachment, or your attachment is not an Office document that supports this inherited protection, protect the file before you attach it to the email. You can then assign the specific usage rights that you need for the file.

Alternatively, you can change this protection inheritance of documents by specifying

```
Set-IRMConfiguration -DecryptAttachmentForEncryptOnly $true
```

 with [Exchange Online PowerShell](#). Use this configuration when you don't need to retain the original protection for the document after the user is authenticated. When recipients open the email message, the document is not protected.

If you do need an attached document to retain the original protection, see [Secure document collaboration by using Azure Information Protection](#).

Note: If you see references to **DecryptAttachmentFromPortal**, this parameter is now deprecated for [Set-IRMConfiguration](#). Unless you have previously set this parameter, it is not available.

## Automatically encrypt PDF documents with Exchange Online

When Exchange Online uses the new capabilities for Office 365 Message Encryption, you can automatically encrypt unprotected PDF documents when they are attached to an encrypted email. The document inherits the same permissions as those for the email message. To enable this configuration, set **EnablePdfEncryption** **\$True** with [Set-IRMConfiguration](#).

Recipients who don't already have a reader installed that supports the ISO standard for PDF encryption can install one of the readers listed in [PDF readers that support Microsoft Information Protection](#). Alternatively, recipients can read the protected PDF document in the OME portal.

## Rights Management issuer and Rights Management owner

When a document or email is protected by using the Azure Rights Management service, the account that protects that content automatically becomes the Rights Management issuer for that content. This account is logged as the **issuer** field in the [usage logs](#).

The Rights Management issuer is always granted the Full Control usage right for the document or email, and in addition:

- If the protection settings include an expiry date, the Rights Management issuer can still open and edit the document or email after that date.
- The Rights Management issuer can always access the document or email offline.
- The Rights Management issuer can still open a document after it is revoked.

By default, this account is also the **Rights Management owner** for that content, which is the case when a user who created the document or email initiates the protection. But there are some scenarios where an administrator or service can protect content on behalf of users. For example:

- An administrator bulk-protects files on a file share: The administrator account in Azure AD protects the documents for the users.

- The Rights Management connector protects Office documents on a Windows Server folder: The service principal account in Azure AD that is created for the RMS connector protects the documents for the users.

In these scenarios, the Rights Management issuer can assign the Rights Management owner to another account by using the Azure Information Protection SDKs or PowerShell. For example, when you use the [Protect-RMSFile](#) PowerShell cmdlet with the Azure Information Protection client, you can specify the `OwnerEmail` parameter to assign the Rights Management owner to another account.

When the Rights Management issuer protects on behalf of users, assigning the Rights Management owner ensures that the original document or email owner has the same level of control for their protected content as if they initiated the protection themselves.

For example, the user who created the document can print it, even though it's now protected with a template that doesn't include the Print usage right. The same user can always access their document, regardless of the offline access setting or expiry date that might have been configured in that template. In addition, because the Rights Management owner has the Full Control usage right, this user can also reprotect the document to grant additional users access (at which point the user then becomes the Rights Management issuer as well as the Rights Management owner), and this user can even remove the protection. However, only the Rights Management issuer can track and revoke a document.

The Rights Management owner for a document or email is logged as the `owner-email` field in the [usage logs](#).

Note that the Rights Management owner is independent from the Windows file system Owner. They are often the same but can be different, even if you don't use the SDKs or PowerShell.

## Rights Management use license

When a user opens a document or email that has been protected by Azure Rights Management, a Rights Management use license for that content is granted to the user. This use license is a certificate that contains the user's usage rights for the document or email message, and the encryption key that was used to encrypt the content. The use license also contains an expiry date if this has been set, and how long the use license is valid.

A user must have a valid use license to open the content in addition to their rights account certificate (RAC), which is a certificate that's granted when the [user environment is initialized](#) and then renewed every 31 days.

For the duration of the use license, the user is not reauthenticated or reauthorized for the content. This lets the user continue to open the protected document or email without an internet connection. When the use license validity period expires, the next time the user accesses the protected document or email, the user must be reauthenticated and reauthorized.

When documents and email messages are protected by using a label or a template that defines the protection settings, you can change these settings in your label or template without having to reprotect the content. If the user has already accessed the content, the changes take effect after their use license has expired. However, when users apply custom permissions (also known as an ad-hoc rights policy) and these permissions need to change after the document or email is protected, that content must be protected again with the new permissions.

Custom permissions for an email message are implemented with the Do Not Forward option.

The default use license validity period for a tenant is 30 days and you can configure this value by using the PowerShell cmdlet, [Set-AipServiceMaxUseLicenseValidityTime](#). You can configure a more restrictive setting for when protection is applied by using a label or template:

- When you configure a label or template in the Azure portal, the use license validity period takes its value from the **Allow offline access setting**.

For more information and guidance to configure this setting in the Azure portal, see the [Information about the protection settings](#) table from the instructions how to configure a label for Rights Management protection.

- When you configure a template by using PowerShell, the use license validity period takes its value from the *LicenseValidityDuration* parameter in the [Set-AipServiceTemplateProperty](#) and [Add-AipServiceTemplate](#) cmdlets.

For more information and guidance to configure this setting by using PowerShell, see the help for each cmdlet.

## See Also

[Configuring and managing templates for Azure Information Protection](#)

[Configuring super users for Azure Information Protection and discovery services or data recovery](#)

# Configuring super users for Azure Information Protection and discovery services or data recovery

7/20/2020 • 5 minutes to read • [Edit Online](#)

*Applies to:* [Azure Information Protection](#), [Office 365](#)

The super user feature of the Azure Rights Management service from Azure Information Protection ensures that authorized people and services can always read and inspect the data that Azure Rights Management protects for your organization. If necessary, the protection can then be removed or changed.

A super user always has the Rights Management Full Control [usage right](#) for documents and emails that have been protected by your organization's Azure Information Protection tenant. This ability is sometimes referred to as "reasoning over data" and is a crucial element in maintaining control of your organization's data. For example, you would use this feature for any of the following scenarios:

- An employee leaves the organization and you need to read the files that they protected.
- An IT administrator needs to remove the current protection policy that was configured for files and apply a new protection policy.
- Exchange Server needs to index mailboxes for search operations.
- You have existing IT services for data loss prevention (DLP) solutions, content encryption gateways (CEG), and anti-malware products that need to inspect files that are already protected.
- You need to bulk decrypt files for auditing, legal, or other compliance reasons.

## Configuration for the super user feature

By default, the super user feature is not enabled, and no users are assigned this role. It is enabled for you automatically if you configure the Rights Management connector for Exchange, and it is not required for standard services that run Exchange Online, Microsoft Sharepoint Server, or SharePoint in Microsoft 365.

If you need to manually enable the super user feature, use the PowerShell cmdlet [Enable-AipServiceSuperUserFeature](#), and then assign users (or service accounts) as needed by using the [Add-AipServiceSuperUser](#) cmdlet or the [Set-AipServiceSuperUserGroup](#) cmdlet and add users (or other groups) as needed to this group.

Although using a group for your super users is easier to manage, be aware that for performance reasons, Azure Rights Management [caches the group membership](#). So if you need to assign a new user to be a super user to decrypt content immediately, add that user by using Add-AipServiceSuperUser, rather than adding the user to an existing group that you have configured by using Set-AipServiceSuperUserGroup.

### NOTE

If you have not yet installed the Windows PowerShell module for Azure Rights Management, see [Installing the AIPService PowerShell module](#).

It doesn't matter when you enable the super user feature or when you add users as super users. For example, if you enable the feature on Thursday and then add a user on Friday, that user can immediately open content that was protected at the very beginning of the week.

# Security best practices for the super user feature

- Restrict and monitor the administrators who are assigned a global administrator for your Office 365 or Azure Information Protection tenant, or who are assigned the GlobalAdministrator role by using the [Add-AipServiceRoleBasedAdministrator](#) cmdlet. These users can enable the super user feature and assign users (and themselves) as super users, and potentially decrypt all files that your organization protects.
- To see which users and service accounts are individually assigned as super users, use the [Get-AipServiceSuperUser](#) cmdlet. To see whether a super user group is configured, use the [Get-AipServiceSuperUserGroup](#) cmdlet and your standard user management tools to check which users are a member of this group. Like all administration actions, enabling or disabling the super feature, and adding or removing super users are logged and can be audited by using the [Get-AipServiceAdminLog](#) command. See the next section for an example. When super users decrypt files, this action is logged and can be audited with [usage logging](#).
- If you do not need the super user feature for everyday services, enable the feature only when you need it, and disable it again by using the [Disable-AipServiceSuperUserFeature](#) cmdlet.

## Example auditing for the super user feature

The following log extract shows some example entries from using the [Get-AipServiceAdminLog](#) cmdlet.

In this example, the administrator for Contoso Ltd confirms that the super user feature is disabled, adds Richard Simone as a super user, checks that Richard is the only super user configured for the Azure Rights Management service, and then enables the super user feature so that Richard can now decrypt some files that were protected by an employee who has now left the company.

```
2015-08-01T18:58:20 admin@contoso.com GetSuperUserFeatureState Passed Disabled
```

```
2015-08-01T18:59:44 admin@contoso.com AddSuperUser -id rsimone@contoso.com Passed True
```

```
2015-08-01T19:00:51 admin@contoso.com GetSuperUser Passed rsimone@contoso.com
```

```
2015-08-01T19:01:45 admin@contoso.com SetSuperUserFeatureState -state Enabled Passed True
```

## Scripting options for super users

Often, somebody who is assigned a super user for Azure Rights Management will need to remove protection from multiple files, in multiple locations. While it's possible to do this manually, it's more efficient (and often more reliable) to script this. To do so, you can use the [Unprotect-RMSFile](#) cmdlet, and [Protect-RMSFile](#) cmdlet as required.

If you are using classification and protection, you can also use the [Set-AIPFileLabel](#) to apply a new label that doesn't apply protection, or remove the label that applied protection.

For more information about these cmdlets, see [Using PowerShell with the Azure Information Protection client](#) from the Azure Information Protection client admin guide.

### NOTE

The AzureInformationProtection module is different from and supplements the [AIPService PowerShell module](#) that manages the Azure Rights Management service for Azure Information Protection.

## Guidance for using Unprotect-RMSFile for eDiscovery

Although you can use the Unprotect-RMSFile cmdlet to decrypt protected content in PST files, use this cmdlet strategically as part of your eDiscovery process. Running Unprotect-RMSFile on large files on a computer is a

resource-intensive (memory and disk space) and the maximum file size supported for this cmdlet is 5 GB.

Ideally, use [Office 365 eDiscovery](#) to search and extract protected emails and protected attachment in emails. The super user ability is automatically integrated with Exchange Online so that eDiscovery in the Office 365 Security & Compliance Center or Microsoft 365 compliance center can search for encrypted items prior to export, or decrypt encrypted email on export.

If you cannot use Office 365 eDiscovery, you might have another eDiscovery solution that integrates with the Azure Rights Management service to similarly reason over data. Or, if your eDiscovery solution cannot automatically read and decrypt protected content, you can still use this solution in a multi-step process that lets you run Unprotect-RMSFile more efficiently:

1. Export the email in question to a PST file from Exchange Online or Exchange Server, or from the workstation where the user stored their email.
2. Import the PST file into your eDiscovery tool. Because the tool cannot read protected content, it's expected that these items will generate errors.
3. From all the items that the tool couldn't open, generate a new PST file that this time, contains just protected items. This second PST file will likely be much smaller than the original PST file.
4. Run Unprotect-RMSFile on this second PST file to decrypt the contents of this much smaller file. From the output, import the now-decrypted PST file into your discovery tool.

For more detailed information and guidance for performing eDiscovery across mailboxes and PST files, see the following blog post: [Azure Information Protection and eDiscovery Processes](#).

# Configuring the Azure Information Protection policy

7/20/2020 • 7 minutes to read • [Edit Online](#)

Applies to: [Azure Information Protection](#)

Instructions for: [Azure Information Protection client for Windows](#)

## NOTE

The Azure Information Protection policy applies to the Azure Information Protection client (classic) and not the Azure Information Protection unified labeling client. Not sure of the difference between these clients? See this [FAQ](#).

If you are looking for information to configure sensitivity labels and policy settings for the unified labeling client, see [Learn about sensitivity labels](#) from the Microsoft 365 Compliance documentation.

To configure classification, labeling, and protection for the classic client, you must configure the Azure Information Protection policy. This policy is then downloaded to computers that have installed the [Azure Information Protection client](#).

The policy contains labels and settings:

- Labels apply a classification value to documents and emails, and can optionally protect this content. The Azure Information Protection client displays these labels for your users in Office apps and when users right-click from File Explorer. These labels can also be applied by using PowerShell and the Azure Information Protection scanner.
- The settings change the default behavior of the Azure Information Protection client. For example, you can select a default label, whether all documents and emails must have a label, and whether the Azure Information Protection bar is displayed in Office apps.

## Subscription support

Azure Information Protection supports different levels of subscriptions:

- Azure Information Protection P2: Support for all classification, labeling, and protection features.
- Azure Information Protection P1: Support for most classification, labeling, and protection features, but not automatic classification or HYOK.
- Office 365 that includes the Azure Rights Management service: Support for protection but not classification and labeling.

Options that require an Azure Information Protection P2 subscription are identified in the portal.

If your organization has a mix of subscriptions, it is your responsibility to make sure that users do not use features that their account is not licensed to use. The Azure Information Protection client does not do license checking and enforcement. When you configure options that not all users have a license for, use scoped policies or a registry setting to ensure that your organization stays in compliance with your licenses:

- When your organization has a mix of Azure Information Protection P1 and Azure Information Protection P2 licenses:** For users who have a P2 license, create and use one or more [scoped policies](#) when you configure options that require an Azure Information Protection P2 license. Make sure that your global policy does not contain options that require an Azure Information Protection P2 license.

- When your organization has a subscription for Azure Information Protection but some users have only a license for Office 365 that includes the Azure Rights Management service: For the users who do not have a license for Azure Information Protection, edit the registry on their computers so they do not download the Azure Information Protection policy. For instructions, see the admin guide for the following customization: [Enforce protection-only mode when your organization has a mix of licenses](#).

For more information about the subscriptions, see [What subscription do I need for Azure Information Protection and what features are included?](#)

## Signing in to the Azure portal

To sign in to the Azure portal, to configure and manage Azure Information Protection:

- Use the following link: <https://portal.azure.com>
  - Use an Azure AD account that has one of the following [administrator roles](#):
    - Azure Information Protection administrator
    - Compliance administrator
    - Compliance data administrator
    - Security administrator
- Security reader** - Azure Information Protection analytics only
- Global reader** - Azure Information Protection analytics only
- Global administrator

### NOTE

If your tenant is on the [unified labeling platform](#), the Azure Information Protection administrator role (formerly "Information Protection administrator") is not supported for the Azure portal. [More information](#)

Microsoft accounts cannot manage Azure Information Protection.

## To access the Azure Information Protection pane for the first time

- Sign in to the Azure portal.
- Select + **Create a resource**, and then, from the search box for the Marketplace, type **Azure Information Protection**.
- From the results list, select **Azure Information Protection**. On the **Azure Information Protection** pane, click **Create**.

### TIP

Optionally, 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** again.

- You see the **Quick start** page that automatically opens the first time you connect to the service. Browse the suggested resources, or use the other menu options. To configure the labels that users can select, use the following procedure.

Next time you access the Azure Information Protection pane, it automatically selects the **Labels** option so that you can view and configure labels for all users. You can return to the **Quick start** page by selecting it from the **General** menu.

## How to configure the Azure Information Protection policy

1. Make sure that you are signed in to the Azure portal by using one of these administrative roles: Azure Information Protection administrator, Security administrator, or Global administration. See the [preceding section](#) for more information about these administrative roles.
2. If necessary, navigate to the **Azure Information Protection** pane: For example, on the hub menu, click **All services** and start typing **Information Protection** in the Filter box. From the results, select **Azure Information Protection**.

The **Azure Information Protection - Labels** pane automatically opens for you to view and edit the available labels. The labels can be made available to all users, selected users, or no users by adding or removing them from a policy.

3. To view and edit the policies, select **Policies** from the menu options. To view and edit the policy that all users get, select the **Global** policy. To create a custom policy for selected users, select **Add a new policy**.

### Making changes to the policy

You can create any number of labels. However, when they start to get too many for users to easily see and select the right label, create scoped policies so that users see only the labels that are relevant to them. There is an upper limit for labels that apply protection, which is 500.

When you make any changes on an Azure Information Protection pane, click **Save** to save the changes, or click **Discard** to revert to the last saved settings. When you save changes in a policy, or make changes to labels that are added to policies, those changes are automatically published. There's no separate publish option.

The Azure Information Protection client checks for any changes whenever a supported Office application starts, and downloads the changes as its latest Azure Information Protection policy. Additional triggers that refresh the policy on the client:

- Right-click to classify and protect a file or folder.
- Running the [PowerShell cmdlets](#) for labeling and protection (Get-AIPFileStatus, Set-AIPFileClassification, and Set-AIPFileLabel).
- Every 24 hours.
- For the [Azure Information Protection Scanner](#): When the service starts (if the policy is older than an hour), and every hour during operation.

#### NOTE

When the client downloads the policy, be prepared to wait a few minutes before it's fully operational. The actual time varies, according to factors such as the size and complexity of the policy configuration, and the network connectivity. If the resulting action of your labels does not match your latest changes, allow up to 15 minutes and then try again.

### Configuring your organization's policy

Use the following information to help you configure the Azure Information Protection policy:

- [The default Information Protection policy](#)
- [How to configure the policy settings](#)

- [How to create a new label](#)
- [How to add or remove a label](#)
- [How to delete or reorder a label](#)
- [How to change or customize an existing label](#)
- [How to configure a label for protection](#)
- [How to configure a label to apply visual markings](#)
- [How to configure conditions for automatic and recommended classification](#)
- [How to configure the policy for specific users by using scoped policies](#)
- [How to configure and manage templates](#)
- [How to configure labels for different languages](#)
- [How to migrate Azure Information Protection labels to Office 365](#)

## Label information stored in emails and documents

When a label is applied to a document or email, under the covers, the label is stored in metadata so that applications and services can read the label:

- In emails, this information is stored in the x-header: **msip\_labels**:  
**MSIP\_Label\_<GUID>\_Enabled=True**
- For Word documents (.doc and .docx), Excel spreadsheets (.xls and .xlsx), PowerPoint presentations (.ppt and .pptx), and PDF documents, this metadata is stored in the following custom property:  
**MSIP\_Label\_<GUID>\_Enabled=True**

For emails, the label information is stored when the email is sent. For documents, the label information is stored when the file is saved.

To identify the GUID for a label, locate the Label ID value on the **Label** pane in the Azure portal, when you view or configure the Azure Information Protection policy. For files that have labels applied, you can also run the [Get-AIPFileStatus](#) PowerShell cmdlet to identify the GUID (MainLabelId or SubLabelId). When a label has sublabels, always specify the GUID of just a sublabel and not the parent label.

## Next steps

For examples of how to customize the Azure Information Protection policy, and see the resulting behavior for users, try the following tutorials:

- [Edit the Azure Information Protection policy and create a new label](#)
- [Configure Azure Information Protection policy settings that work together](#)

To see how your policy is performing, see [Central reporting for Azure Information Protection](#).

# The default Azure Information Protection policy

7/20/2020 • 11 minutes to read • [Edit Online](#)

Applies to: [Azure Information Protection](#)

Instructions for: [Azure Information Protection client for Windows](#)

## NOTE

To provide a unified and streamlined customer experience, **Azure Information Protection client (classic)** and **Label Management** in the Azure Portal are being **deprecated** as of **March 31, 2021**. This time-frame allows all current Azure Information Protection customers to transition to our unified labeling solution using the Microsoft Information Protection Unified Labeling platform. Learn more in the official [deprecation notice](#).

## NOTE

The Azure Information Protection policy applies to the Azure Information Protection client (classic) and not the Azure Information Protection unified labeling client. Not sure of the difference between these clients? See this [FAQ](#).

If you are looking for information to configure sensitivity labels and policy settings for the unified labeling client, see [Learn about sensitivity labels](#) from the Microsoft 365 Compliance documentation.

Use the following information to understand how the default policy for Azure Information Protection is configured.

When an administrator first connects to the Azure Information Protection service by using the Azure portal, the Azure Information Protection default policy for that tenant is created. Occasionally, Microsoft might make changes to this default policy but if you were already using the service before the default policy was revised, your earlier version of the Azure Information Protection default policy is not updated because you might have configured it and deployed into production.

You can reference the following values to return your Azure Information Protection policy to the defaults, or update your Azure Information Protection policy to the latest values.

## IMPORTANT

Starting April 2019, the default labels are not automatically created for new customers. These tenants are automatically provisioned for the unified labeling platform, so there is no need to migrate labels after you have configured them in the Azure portal.

For these tenants, if there aren't any sensitivity labels already created in the Office 365 Security & Compliance Center, the Microsoft 365 Security center, or the Microsoft 365 compliance center, you can create the default labels from the current default policy for Azure Information Protection. To do this, select **Generate default labels** from the **Labels** pane, and add the labels to the global policy. If you don't see the option to generate default labels, you might need to first activate unified labeling from the **Manage > Unified labeling** pane. For detailed instructions, see the [Get started with Azure Information Protection in the Azure portal](#) quickstart.

## Current default policy

This version of the Azure Information Protection default policy is from July 31, 2017.

This Azure Information Protection default policy is created when the Azure Rights Management service is activated, which is the case for new tenants starting February 2018. For more information, see the blog post announcement [Improvements to the protection stack in Azure Information Protection](#).

This Azure Information Protection default policy is also created if you have manually [activated the service](#) before the Azure Information Protection policy was created.

If the service was not activated, the Azure Information Protection default policy does not configure protection for the following sublabels:

- Confidential \ All Employees
- Confidential \ Recipients Only
- Highly Confidential \ All Employees
- Highly Confidential \ Recipients Only

When these sublabels are not automatically configured for protection, the Azure Information Protection default policy remains the same as the [previous default policy](#).

When protection is applied to the **All Employees** sublabels, the protection is configured by using the default templates that are automatically converted to labels in the Azure portal. For more information about these templates, see [Configuring and managing templates for Azure Information Protection](#).

Starting August 30, 2017, this version of the Azure Information Protection default policy includes multi-language versions of the label names and descriptions.

#### **More information about the Recipients Only sublabel**

Users see this label in Outlook only. They do not see this label in Word, Excel, PowerPoint, or from File Explorer.

When users select this label, the Outlook Do Not Forward option is automatically applied to the email. The recipients that the users specify cannot forward the email and cannot copy or print the contents, or save any attachments.

#### **Labels**

| LABEL    | TOOLTIP                                                                          | SETTINGS                                                                                                                             |
|----------|----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|
| Personal | Non-business data, for personal use only.                                        | <b>Enabled:</b> On<br><b>Color:</b> Light green<br><b>Visual markings:</b> Off<br><b>Conditions:</b> None<br><b>Protection:</b> None |
| Public   | Business data that is specifically prepared and approved for public consumption. | <b>Enabled:</b> On<br><b>Color:</b> Green<br><b>Visual markings:</b> Off<br><b>Conditions:</b> None<br><b>Protection:</b> None       |

| LABEL               | TOOLTIP                                                                                                                                                                                                                                                          | SETTINGS                                                                                                                        |
|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| General             | Business data that is not intended for public consumption. However, this can be shared with external partners, as required. Examples include a company internal telephone directory, organizational charts, internal standards, and most internal communication. | <b>Enabled:</b> On<br><b>Color:</b> Blue<br><b>Visual markings:</b> Off<br><b>Conditions:</b> None<br><b>Protection:</b> None   |
| Confidential        | Sensitive business data that could cause damage to the business if shared with unauthorized people. Examples include contracts, security reports, forecast summaries, and sales account data.                                                                    | <b>Enabled:</b> On<br><b>Color:</b> Orange<br><b>Visual markings:</b> Off<br><b>Conditions:</b> None<br><b>Protection:</b> None |
| Highly Confidential | Very sensitive business data that would cause damage to the business if it was shared with unauthorized people. Examples include employee and customer information, passwords, source code, and pre-announced financial reports.                                 | <b>Enabled:</b> On<br><b>Color:</b> Red<br><b>Visual markings:</b> Off<br><b>Conditions:</b> None<br><b>Protection:</b> None    |

## Sublabels

| LABEL                                 | TOOLTIP                                                                                                                            | SETTINGS                                                                                                                                                                       |
|---------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Confidential \ All Employees          | Confidential data that requires protection, which allows all employees full permissions. Data owners can track and revoke content. | <b>Enabled:</b> On<br><b>Visual markings:</b> Footer (document and email)<br>Classified as Confidential<br><b>Conditions:</b> None<br><b>Protection:</b> Azure (cloud key) [1] |
| Confidential \ Anyone (not protected) | Data that does not require protection. Use this option with care and with appropriate business justification.                      | <b>Enabled:</b> On<br><b>Visual markings:</b> Footer (document and email)<br>Classified as Confidential<br><b>Conditions:</b> None<br><b>Protection:</b> None                  |

| LABEL                                        | TOOLTIP                                                                                                                                         | SETTINGS                                                                                                                                                                                                                               |
|----------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Confidential \ Recipients Only               | Confidential data that requires protection and that can be viewed by the recipients only.                                                       | <b>Enabled:</b> On<br><b>Visual markings:</b> Footer (email)<br><br>Classified as Confidential<br><br><b>Conditions:</b> None<br><br><b>Protection:</b> Set user defined permissions (Preview), In Outlook apply Do Not Forward        |
| Highly Confidential \ All Employees          | Highly confidential data that allows all employees view, edit, and reply permissions to this content. Data owners can track and revoke content. | <b>Enabled:</b> On<br><b>Visual markings:</b> Footer (document and email)<br><br>Classified as Highly Confidential<br><br><b>Conditions:</b> None<br><br><b>Protection:</b> Azure (cloud key) [2]                                      |
| Highly Confidential \ Anyone (not protected) | Data that does not require protection. Use this option with care and with appropriate business justification.                                   | <b>Enabled:</b> On<br><b>Visual markings:</b> Footer (document and email)<br><br>Classified as Highly Confidential<br><br><b>Conditions:</b> None<br><br><b>Protection:</b> None                                                       |
| Highly Confidential \ Recipients Only        | Highly confidential data that requires protection and that can be viewed by the recipients only.                                                | <b>Enabled:</b> On<br><b>Visual markings:</b> Footer (email)<br><br>Classified as Highly Confidential<br><br><b>Conditions:</b> None<br><br><b>Protection:</b> Set user defined permissions (Preview), In Outlook apply Do Not Forward |

Footnote 1

The protection permissions match those in the [default template](#), Confidential \ All Employees.

Footnote 2

The protection permissions match those in the [default template](#), Highly Confidential \ All Employees.

## Information Protection bar

| SETTING | VALUE       |
|---------|-------------|
| Title   | Sensitivity |

| SETTING | VALUE                                                                                                                                                                       |
|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Tooltip | The current label for this content. This setting identifies the risk to the business if this content is shared with unauthorized people inside or outside the organization. |

## Settings

Some of the settings were added after July 31, 2017.

| SETTING                                                                                                         | VALUE |
|-----------------------------------------------------------------------------------------------------------------|-------|
| Select the default label                                                                                        | None  |
| Send audit data to Azure Information Protection analytics                                                       | Off   |
| All documents and emails must have a label (applied automatically or by users)                                  | Off   |
| Users must provide justification to set a lower classification label, remove a label, or remove protection      | Off   |
| For email messages with attachments, apply a label that matches the highest classification of those attachments | Off   |
| Display the Information Protection bar in Office apps                                                           | Off   |
| Add the Do Not Forward button to the Outlook ribbon                                                             | Off   |
| Make the custom permissions option available for users                                                          | Off   |
| Provide a custom URL for the Azure Information Protection client "Tell me more" web page                        | Blank |

## Default policy before July 31, 2017

Note that descriptions in this policy refer to data that requires protection, and also to data tracking and revoking. The policy does not configure this protection for these labels, so you must take additional steps to fulfill this description. For example, configure the label to apply protection or use a data loss prevention (DLP) solution. Before you can track and revoke a document by using the document tracking site, the document must be protected by the Azure Rights Management service and tracked by the person who protected the document.

### Labels

| LABEL    | TOOLTIP                                   | SETTINGS                                                                                                                             |
|----------|-------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|
| Personal | Non-business data, for personal use only. | <b>Enabled:</b> On<br><b>Color:</b> Light green<br><b>Visual markings:</b> Off<br><b>Conditions:</b> None<br><b>Protection:</b> None |

| LABEL               | TOOLTIP                                                                                                                                                                                                                                                          | SETTINGS                                                                                                                        |
|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| Public              | Business data that is specifically prepared and approved for public consumption.                                                                                                                                                                                 | <b>Enabled:</b> On<br><b>Color:</b> Green<br><b>Visual markings:</b> Off<br><b>Conditions:</b> None<br><b>Protection:</b> None  |
| General             | Business data that is not intended for public consumption. However, this can be shared with external partners, as required. Examples include a company internal telephone directory, organizational charts, internal standards, and most internal communication. | <b>Enabled:</b> On<br><b>Color:</b> Blue<br><b>Visual markings:</b> Off<br><b>Conditions:</b> None<br><b>Protection:</b> None   |
| Confidential        | Sensitive business data that could cause damage to the business if shared with unauthorized people. Examples include contracts, security reports, forecast summaries, and sales account data.                                                                    | <b>Enabled:</b> On<br><b>Color:</b> Orange<br><b>Visual markings:</b> Off<br><b>Conditions:</b> None<br><b>Protection:</b> None |
| Highly Confidential | Very sensitive business data that would cause damage to the business if it was shared with unauthorized people. Examples include employee and customer information, passwords, source code, and pre-announced financial reports.                                 | <b>Enabled:</b> On<br><b>Color:</b> Red<br><b>Visual markings:</b> Off<br><b>Conditions:</b> None<br><b>Protection:</b> None    |

## Sublabels

| LABEL                        | TOOLTIP                                                                                                                            | SETTINGS                                                                                                                                                      |
|------------------------------|------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Confidential \ All Employees | Confidential data that requires protection, which allows all employees full permissions. Data owners can track and revoke content. | <b>Enabled:</b> On<br><b>Visual markings:</b> Footer (document and email)<br>Classified as Confidential<br><b>Conditions:</b> None<br><b>Protection:</b> None |

| LABEL                                        | TOOLTIP                                                                                                                                         | SETTINGS                                                                                                                                                             |
|----------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Confidential \ Anyone (not protected)        | Data that does not require protection. Use this option with care and with appropriate business justification.                                   | <b>Enabled:</b> On<br><b>Visual markings:</b> Footer (document and email)<br>Classified as Confidential<br><b>Conditions:</b> None<br><b>Protection:</b> None        |
| Highly Confidential \ All Employees          | Highly confidential data that allows all employees view, edit, and reply permissions to this content. Data owners can track and revoke content. | <b>Enabled:</b> On<br><b>Visual markings:</b> Footer (document and email)<br>Classified as Highly Confidential<br><b>Conditions:</b> None<br><b>Protection:</b> None |
| Highly Confidential \ Anyone (not protected) | Data that does not require protection. Use this option with care and with appropriate business justification.                                   | <b>Enabled:</b> On<br><b>Visual markings:</b> Footer (document and email)<br>Classified as Highly Confidential<br><b>Conditions:</b> None<br><b>Protection:</b> None |

## Information Protection bar

| SETTING | VALUE                                                                                                                                                                       |
|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Title   | Sensitivity                                                                                                                                                                 |
| Tooltip | The current label for this content. This setting identifies the risk to the business if this content is shared with unauthorized people inside or outside the organization. |

## Settings

| SETTING                                                                                                    | VALUE |
|------------------------------------------------------------------------------------------------------------|-------|
| All documents and emails must have a label (applied automatically or by users)                             | Off   |
| Select the default label                                                                                   | None  |
| Users must provide justification to set a lower classification label, remove a label, or remove protection | Off   |

| Setting                                                                                                         | Value |
|-----------------------------------------------------------------------------------------------------------------|-------|
| For email messages with attachments, apply a label that matches the highest classification of those attachments | Off   |
| Provide a custom URL for the Azure Information Protection client "Tell me more" web page                        | Blank |

## Default policy before March 21, 2017

### Labels

| Label        | Tooltip                                                                                                                                                                                                                                                              | Settings                                                                                                                                                                              |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Personal     | For personal use only. This data will not be monitored by the organization. Personal information must not include any business-related data.                                                                                                                         | <b>Enabled:</b> On<br><b>Color:</b> Light green<br><b>Visual markings:</b> Off<br><b>Conditions:</b> None<br><b>Protection:</b> None                                                  |
| Public       | This information is internal and can be used by everyone inside or outside the business.                                                                                                                                                                             | <b>Enabled:</b> On<br><b>Color:</b> Green<br><b>Visual markings:</b> Off<br><b>Conditions:</b> None<br><b>Protection:</b> None                                                        |
| Internal     | This information includes a wide spectrum of internal business data that can be used by all employees and can be shared with authorized customers and business partners. Examples for internal information are company policies and most internal communications.    | <b>Enabled:</b> On<br><b>Color:</b> Blue<br><b>Visual markings:</b> Footer (document and email):<br>Sensitivity: Internal<br><b>Conditions:</b> None<br><b>Protection:</b> None       |
| Confidential | This data includes sensitive business information. Exposing this data to unauthorized users may cause damage to the organization. Examples for Confidential information are employee information, individual customer projects or contracts, and sales account data. | <b>Enabled:</b> On<br><b>Color:</b> Orange<br><b>Visual markings:</b> Footer (document and email):<br>Sensitivity: Confidential<br><b>Conditions:</b> None<br><b>Protection:</b> None |

| LABEL  | TOOLTIP                                                                                                                                                                                                                                                                                                                        | SETTINGS                                                                                                                                                                            |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Secret | This data includes highly sensitive information for the business that must be protected. Exposing Secret data to unauthorized users may cause serious damage to the organization. Examples for Secret information are personal identification information, customer records, source code, and pre-announced financial reports. | <b>Enabled:</b> On<br><b>Color:</b> Red<br><b>Visual markings:</b> Footer (document and email):<br><b>Sensitivity:</b> Secret<br><b>Conditions:</b> None<br><b>Protection:</b> None |

## Sublabels

| LABEL                | TOOLTIP                                                                                  | SETTINGS                                                                                                |
|----------------------|------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------|
| Secret \ All Company | This data includes sensitive business information - permitted for all company employees. | <b>Enabled:</b> On<br><b>Visual markings:</b> Off<br><b>Conditions:</b> None<br><b>Protection:</b> None |
| Secret \ My Group    | This data includes sensitive business information - permitted for employee groups only.  | <b>Enabled:</b> On<br><b>Visual markings:</b> Off<br><b>Conditions:</b> None<br><b>Protection:</b> None |

## Information Protection bar

| SETTING | VALUE                                                                                                                                                                                                                       |
|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Title   | Sensitivity                                                                                                                                                                                                                 |
| Tooltip | Information Sensitivity consists of four distinct levels (Public, Internal, Confidential, Secret), allowing the user to identify the risk of exposing the information to unauthorized users inside or outside the business. |

## Settings

| SETTING                                                                                                    | VALUE |
|------------------------------------------------------------------------------------------------------------|-------|
| All documents and emails must have a label (applied automatically or by users)                             | Off   |
| Select the default label                                                                                   | None  |
| Users must provide justification to set a lower classification label, remove a label, or remove protection | Off   |

| SETTING                                                                                  | VALUE |
|------------------------------------------------------------------------------------------|-------|
| Provide a custom URL for the Azure Information Protection client "Tell me more" web page | Blank |

## Next steps

For more information about configuring your Azure Information Protection policy, use the links in the [Configuring your organization's policy](#) section.

# How to configure the policy settings for Azure Information Protection

7/20/2020 • 7 minutes to read • [Edit Online](#)

*Applies to:* [Azure Information Protection](#)

*Instructions for:* [Azure Information Protection client for Windows](#)

## NOTE

To provide a unified and streamlined customer experience, **Azure Information Protection client (classic)** and **Label Management** in the Azure Portal are being **deprecated** as of **March 31, 2021**. This time-frame allows all current Azure Information Protection customers to transition to our unified labeling solution using the Microsoft Information Protection Unified Labeling platform. Learn more in the official [deprecation notice](#).

## NOTE

These instructions apply to the Azure Information Protection client (classic) and not the Azure Information Protection unified labeling client. Not sure of the difference between these clients? See this [FAQ](#).

If you are looking for information to configure policy settings for the unified labeling client, see the Microsoft 365 Compliance documentation. For example, [Learn about sensitivity labels](#).

In addition to the Information Protection bar title and tooltip, there are some settings in the Azure Information Protection policy that you can configure independently from the labels:

#### Configure settings to display and apply on Information Protection end users

\* Title

Sensitivity

Tooltip

The current label for this content. This setting identifies the risk to the business if this content is shared with unauthorized people inside or outside the organization.

Select the default label

None



Send audit data to Azure Information Protection analytics ⓘ

Off Not configured

All documents and emails must have a label (applied automatically or by users)

Off On

Users must provide justification to set a lower classification label, remove a label, or remove protection

Off On

For email messages with attachments, apply a label that matches the highest classification of those attachments

Off Automatic Recommended

Display the Information Protection bar in Office apps

Off On

Add the Do Not Forward button to the Outlook ribbon

Off On

Make the custom permissions option available for users

Off On

Provide a custom URL for the Azure Information Protection client "Tell me more" web page (optional; otherwise keep blank)

Enter a custom URL or keep blank

Note that your policy settings might have different default values, depending on when you purchased your subscription for Azure Information Protection. Some settings might also be set by a [custom client setting](#).

## To configure the policy settings

1. If you haven't already done so, open a new browser window and [sign in to the Azure portal](#). Then navigate to the **Azure Information Protection** pane.

For example, in the search box for resources, services, and docs: Start typing **Information** and select **Azure Information Protection**.

2. From the **Classifications > Policies** menu option: On the **Azure Information Protection - Policies** pane, select **Global** if the settings that you want to configure will apply to all users.

If the settings that you want to configure are in a [scoped policy](#) so that they apply to selected users only, select your scoped policy instead.

3. On the **Policy** pane, configure the settings:

- **Select the default label:** When you set this option, select the label to assign to documents and emails that do not have a label. You cannot set a label as the default if it has sublabels.

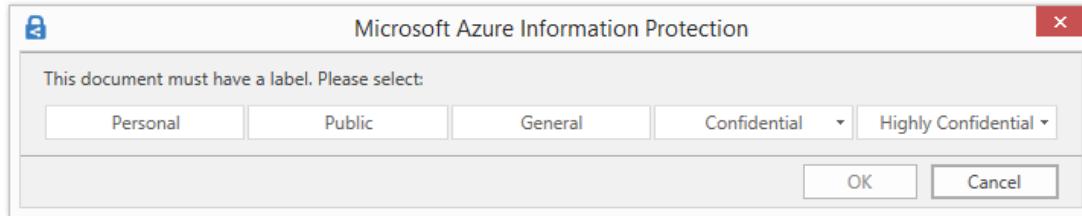
This setting applies to Office apps and the scanner. It does not apply to File Explorer, or PowerShell.

- **Send audit data to Azure Information Protection analytics:** Before you create an Azure Log Analytics workspace for [Azure Information analytics](#), the values for this setting display **Off** and **Not configured**. When you create the workspace, the values change to **Off** and **On**.

When the setting is **On**, clients that support central reporting send data to the Azure Information Protection service. This information includes what labels are applied and when a user selects a label with a lower classification, or removes a label. For more information about what information is sent and stored, see the [Information collected and sent to Microsoft](#) section in the central reporting documentation. Set this policy setting to **Off** to prevent this data from being sent.

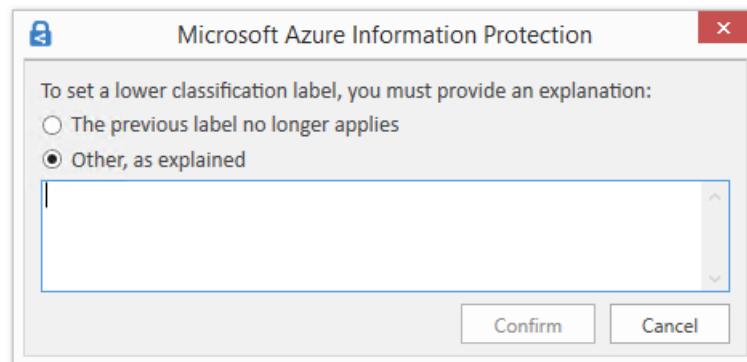
- **All documents and emails must have a label:** When you set this option to **On**, all saved documents and sent emails must have a label applied. The labeling might be manually assigned by a user, automatically as a result of a [condition](#), or be assigned by default (by setting the [Select the default label](#) option).

If a label is not assigned when users save a document or send an email, they are prompted to select a label. For example:



This option does not apply when you remove a label by using the [Set-AIPFileLabel](#) PowerShell cmdlet with the *RemoveLabel* parameter.

- **Users must provide justification to set a lower classification label, remove a label, or remove protection:** When you set this option to **On** and a user does any of these actions (for example, change the **Public** label to **Personal**), the user is prompted to provide an explanation for this action. For example, the user might explain that the document no longer contains sensitive information. The action and its justification reason are logged in their local Windows event log: **Applications and Services Logs > Azure Information Protection**.



This option is not applicable for lowering the classification of sublabels under the same parent label.

- **For email messages with attachments, apply a label that matches the highest classification of those attachments:** When you set this option to **Recommended**, users are prompted to apply a label to their email message. The label is dynamically chosen, based on the classification labels that are applied to the attachments, and the highest classification label is selected. The attachment must be a physical file, and cannot be a link to a file (for example, a link to a file on Microsoft SharePoint or OneDrive). Users can accept the recommendation or dismiss it. When you set this option to **Automatic**, the label is automatically applied but users can remove the label or select a different label before sending the email.

To take the ordering of sublabels into consideration when you use this policy setting, you must [configure an advanced client setting](#).

When the attachment with the highest classification label is configured for protection with the preview setting of user-defined permissions: - When the label's user-defined permissions include Outlook (Do Not Forward), that label is applied and Do Not Forward protection is applied to the email. When the label's user-defined permissions are just for Word, Excel, PowerPoint, and File Explorer, that label is not applied to the email, and neither is protection.

- **Display the Information Protection bar in Office apps:** When this setting is off, users cannot select labels from a bar in Word, Excel, PowerPoint, and Outlook. Instead, users must select labels from the **Protect** button on the ribbon. When this setting is on, users can select labels from either the bar or the button.

When this setting is on, it can be used in conjunction with an advanced client setting so that users can [permanently hide the Azure Information Protection bar](#) if they choose not to show the bar. They can do this by clearing the **Show Bar** option from the **Protect** button.

- **Add the Do Not Forward button to the Outlook ribbon:** When this setting is on, users can select this button from the **Protection** group on the Outlook ribbon in addition to selecting the **Do Not Forward** option from Outlook menus. To help ensure that users classify their emails as well as protect them, you might prefer to not add this button but instead, [configure a label for protection](#) and a user-defined permission for Outlook. This protection setting is functionally the same as selecting the **Do Not Forward** button, but when this functionality is included with a label, emails are classified as well as protected.

This policy setting can also be configured with an advanced client setting as a [client customization](#).

- **Make the custom permissions option available to users:** When this setting is on, users see options to set their own protection settings that can override any protection settings that you might have included with a label configuration. Users can also see an option to remove protection. When this setting is off, users do not see these options.

Note that this policy setting has no effect on custom permissions that users can configure from Office menu options. However, it can also be configured with an advanced client setting as a [client customization](#).

The custom permissions options are located in the following places:

- In Office applications: From the ribbon, **Home** tab > **Protection** group > **Protect** > **Custom Permissions**
- From File Explorer: Right-click > **Classify and protect** > **Custom permissions**
- **Provide a custom URL for the Azure Information Protection client "Tell me more" web page:** Users see this link in the **Microsoft Azure Information Protection** dialog box, **Help and Feedback** section, when they select **Protect** > **Help and feedback** from the **Home** tab in their Office applications. By default, this link goes to the [Azure Information Protection](#) website. You can enter an HTTP or HTTPS (recommended) URL if you want this link to go to an alternative web page. No check is made to verify that the custom URL entered is accessible or displays correctly on all devices.

As an example, for your help desk, you might enter the Microsoft documentation page that includes information about installing and using the client:

<https://docs.microsoft.com/information-protection/rms-client/info-protect-client>. Or release version information:

<https://docs.microsoft.com/information-protection/rms-client/client-version-release-history>.

Alternatively, you might publish your own webpage that includes information for users to contact your help desk, or a video that steps users through how to use the labels that you have configured.

4. To save your changes and make them available to users, click **Save**.

When you click **Save**, your changes are automatically available to users and services. There's no longer a separate publish option.

## Next steps

To see how some of these policy settings can work together, try the [Configure Azure Information Protection policy settings that work together](#) tutorial.

For more information about configuring your Azure Information Protection policy, use the links in the [Configuring your organization's policy](#) section.

# How to create a new label for Azure Information Protection

7/20/2020 • 3 minutes to read • [Edit Online](#)

Applies to: [Azure Information Protection](#)

Instructions for: [Azure Information Protection client for Windows](#)

## NOTE

To provide a unified and streamlined customer experience, **Azure Information Protection client (classic)** and **Label Management** in the Azure Portal are being **deprecated** as of **March 31, 2021**. This time-frame allows all current Azure Information Protection customers to transition to our unified labeling solution using the Microsoft Information Protection Unified Labeling platform. Learn more in the official [deprecation notice](#).

Although Azure Information Protection comes with default labels that you can customize, you can also create your own labels.

You can add a new label, or add a new sublabel to an existing label when you need a further level of classification. For example, the last label in the [default policy](#), contains sublabels.

When you create the first sublabel for a label, users can no longer select the original, parent label. If necessary, create a new sublabel to recreate the parent label settings so that users can apply the same settings.

Use the following instructions to add a new label that can then be added to an Azure Information Protection policy.

## To create a new label

1. If you haven't already done so, open a new browser window and [sign in to the Azure portal](#). Then navigate to the **Azure Information Protection** pane.

For example, in the search box for resources, services, and docs: Start typing **Information** and select **Azure Information Protection**.

2. From the **Classifications > Labels** menu option: On the **Azure Information Protection - Labels** pane, do one of the following actions:
  - To create a new label: Click **Add a new label**.
  - To create a new sublabel: Right-click or select the context menu (...) for the label that you want to create a sublabel for, and then click **Add a sub-label**.
3. On the **Label** or **Sub-label** pane, select the options that you want for this new label, and then click **Save**.

When you specify a display name, you are prevented from specifying some characters (such as a backslash and ampersand) because not all services and applications that use Azure Information Protection can support these characters. In addition to the characters that are blocked, do not specify the # character.

Note that new labels are automatically assigned the color black. Choose a distinguishing color from the list of colors, or enter a hex triplet code for the red, green, and blue (RGB) components of the color. For example, #DAA520. If you need a reference for these codes, you'll find a helpful table from the [<color>](#) page from the MSDN web docs. You also find these codes in many applications that let you edit pictures. For example,

Microsoft Paint lets you choose a custom color from a palette and the RGB values are automatically displayed, which you can then copy.

4. To make your new label available to users: From the **Classifications > Policies** menu option, select the policy to contain the new label. Select **Add or remove labels**. Select the label from the **Policy: Add or remove labels** pane, select **OK**, and then select **Save**.

**TIP**

For new labels, consider adding them first to a scoped policy that you use for testing. When you are satisfied with the results, remove the label from this testing scope, and then add the label to a policy that you use in production.

For more information about adding labels, see [How to add or remove a label](#).

Your changes are automatically available to users and services. There's no longer a separate publish option.

5. If you want this new label name and description to display in different languages for users: Follow the procedures in [How to configure labels for different languages](#).

## Next steps

For more information about configuring your Azure Information Protection policy, use the links in the [Configuring your organization's policy](#) section.

# Add or remove a label to or from an Azure Information Protection policy

7/20/2020 • 2 minutes to read • [Edit Online](#)

*Applies to:* [Azure Information Protection](#)

*Instructions for:* [Azure Information Protection client for Windows](#)

## NOTE

To provide a unified and streamlined customer experience, **Azure Information Protection client (classic)** and **Label Management** in the Azure Portal are being **deprecated** as of **March 31, 2021**. This time-frame allows all current Azure Information Protection customers to transition to our unified labeling solution using the Microsoft Information Protection Unified Labeling platform. Learn more in the official [deprecation notice](#).

After you create an Azure Information Protection label, you can then add it to a policy so that it is available for users. If the label is for all users, add the label to the global policy. If the label is for a subset of users, add the label to a scoped policy. A label can be added to only one policy.

To add a sublabel, its parent label must be in the same policy, or in the global policy. When you add a sublabel, settings from the main label are not inherited. For users who are assigned the sublabel in their policy, the main label is supported only as a display container for the name and color. In this scenario, other configuration settings in the main label are not supported for visual markings, protection, and conditions. Although you can still configure them, those settings in the main label are supported only for users who have the main label in their policy without the sublabel.

For labels that are already in a policy, you can remove them from the policy. This action does not delete the label. It remains available to be used in another policy.

If you haven't yet created the label, see [How to create a new label for Azure Information Protection](#).

If you need to create a scoped policy so that the label applies to a subset of users, see [How to configure the Azure Information Protection policy for specific users by using scoped policies](#).

## To add or remove a label to or from a policy

1. If you haven't already done so, open a new browser window and [sign in to the Azure portal](#). Then navigate to the **Azure Information Protection** pane.

For example, in the search box for resources, services, and docs: Start typing **Information** and select **Azure Information Protection**.

2. From the **Classifications > Policies** menu option: On the **Azure Information Protection - Policies** pane, select **Global** if the label to add or remove applies to all users.

If the label to add or remove applies to a subset of users, select your scoped policy instead.

3. On the **Policy** pane, select **Add or remove labels**.

4. On the **Policy: Add or remove labels** pane, you see all your labels with a checkbox selected if they are already in a policy, and the corresponding policy name in the **POLICY** column.

Sublabels display as indented. In a scoped policy, labels that are inherited from the global policy display as unavailable.

Do one or more of the following actions, and then click **OK**:

- To add a label, select it, which adds a selected checkbox.
- To remove a label, clear its checkbox.

5. To save your changes, click **Save**.

Your changes are automatically available to users and services. There's no longer a separate publish option.

## Next steps

For more information about configuring your Azure Information Protection policy, use the links in the [Configuring your organization's policy](#) section.

# How to delete or reorder a label for Azure Information Protection

7/20/2020 • 3 minutes to read • [Edit Online](#)

Applies to: [Azure Information Protection](#)

Instructions for: [Azure Information Protection client for Windows](#)

## NOTE

To provide a unified and streamlined customer experience, **Azure Information Protection client (classic)** and **Label Management** in the Azure Portal are being **deprecated** as of **March 31, 2021**. This time-frame allows all current Azure Information Protection customers to transition to our unified labeling solution using the Microsoft Information Protection Unified Labeling platform. Learn more in the official [deprecation notice](#).

You can delete or reorder the Azure Information Protection labels that users see in their Office applications by selecting these actions for the labels.

| LABEL NAME   | TOOLTIP                                                                                                                                                            | MARKING           | PROTECTION |
|--------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------|------------|
| Personal     | For personal use only. This data will not be monitored by the business. Personal info.                                                                             |                   | ...        |
| Public       | This information is internal and can be used by everyone inside or outside the organization.                                                                       | Add a sub-label   | ...        |
| Internal     | This information includes a wide spectrum of internal business data that can be used by anyone inside the organization.                                            | Delete this label | ...        |
| Confidential | This data includes sensitive business information. Exposing this data to unauthorized users could result in significant legal, financial, and reputational damage. | Move up           | ...        |
| Secret       | This data includes highly sensitive information for the business. It is recommended that you do not share this data with anyone outside the organization.          | Move down         | ...        |

When you delete a label that has been applied to documents and emails, users see **Not set** for the label status when these documents and emails are next opened by the Azure Information Protection client. However, the label information remains in the metadata and it can still be read by services that look for this label information.

In addition, if the deleted label applied protection, that protection is not removed. The protection settings from the label remain and display in the **Protection templates** section. This template can now be converted to a new label. While this template remains, you cannot create a new label with the same name as the label that you deleted. If you want to do that, you have the following options:

- Convert the template to a label.

This action is recommended because if required, you can then change the name of the template and modify the protection settings.

- Use PowerShell to rename the template or delete it.

Before you do these actions, consider whether other admins or services are using the template, or have used it in the past. You can identify the template by its template ID that doesn't change, or its name (which can be changed). As a best practice, delete a template only if you are sure that users will not have to open documents or emails that were protected by the template.

For more information about managing protection templates, see [Configuring and managing templates for Azure Information Protection](#).

Before you delete a label, instead, consider disabling it or removing it from the policy:

- When you disable a label that has been applied to documents and emails, the applied label is not removed from these documents and emails. The label remains in the policy but no longer displays as a label that users can select on the Information Protection bar. Disabling a label lets you keep the original configuration for when you might want users in the same policy to select the label at a later time, when you simply re-enable the label.
- When you remove a label from a policy, the applied label is also not removed from these documents and emails. But when you remove the label from the policy, it becomes available for you to add this label to another policy. For more information, see [Add or remove a label to or from an Azure Information Protection policy](#).

Order the labels so that users see them in a logical progression in the Information Protection bar. For example, order the labels in increasing sensitivity so that users see the least sensitive label first and the most sensitive label last. The [default policy](#) uses this configuration and reflects the increasing sensitivity in the label names.

**IMPORTANT**

If you configure [conditions](#) for your labels that might apply to more than one label, you must order the labels from least sensitive to most sensitive. This ordering ensures that the most sensitive label is applied when the conditions are evaluated.

Use the following instructions to make these changes.

1. If you haven't already done so, open a new browser window and [sign in to the Azure portal](#). Then navigate to the **Azure Information Protection** pane.

For example, in the search box for resources, services, and docs: Start typing **Information** and select **Azure Information Protection**.

2. From the **Classifications > Labels** menu option: On the **Azure Information Protection - Labels** pane, do one or more of the following actions:

- To delete a label: Right-click or select the context menu (...) for the label that you want to delete, click **Delete this label**, and click **OK** to confirm.
- To disable a label: Select the label that you want to disable. On the **Label** pane, for **Enabled**, select **Off**, and then click **Save**.
- To reorder a label: Right-click or select the context menu (...) for the label that you want to reorder, click **Move up** or **Move down** until the label is in the order that you want.

## Next steps

For more information about configuring your Azure Information Protection policy, use the links in the [Configuring your organization's policy](#) section.

# How to change or customize an existing label for Azure Information Protection

7/20/2020 • 2 minutes to read • [Edit Online](#)

Applies to: [Azure Information Protection](#)

Instructions for: [Azure Information Protection client for Windows](#)

## NOTE

To provide a unified and streamlined customer experience, **Azure Information Protection client (classic)** and **Label Management** in the Azure Portal are being **deprecated** as of **March 31, 2021**. This time-frame allows all current Azure Information Protection customers to transition to our unified labeling solution using the Microsoft Information Protection Unified Labeling platform. Learn more in the official [deprecation notice](#).

You can change or refine any of the labels that users see on the Information Protection bar or from the **Protect** button on the Office ribbon, by configuring the labels in the Azure portal.

For example, you can change a label or sublabel name, tooltip, color, and order. You can change whether the label applies visual markings such as a footer or watermark. You can also change whether the label applies protection, and recommended or automatic classification.

To change a label, use the following instructions:

1. If you haven't already done so, open a new browser window and [sign in to the Azure portal](#). Then navigate to the **Azure Information Protection** pane.

For example, in the search box for resources, services, and docs: Start typing **Information** and select **Azure Information Protection**.

2. From the **Classifications > Labels** menu option: On the **Azure Information Protection - Labels** pane, select the label you want to change.

The exception is if you want to reorder a label: Instead of selecting the label, either right-click the label or select the context menu for the label. Then, select the **Move up** or **Move down** options.

3. Whenever you make changes on a new pane, click **Save** on that pane if you want to keep your changes.

When you click **Save**, your changes are automatically available to users and services. There's no longer a separate publish option.

4. If you changed the label display name or description and you have configured these for additional languages: Export your Azure Information Protection policy again, provide new translations, and import the changes. For more information, see [How to configure labels for different languages](#).

## TIP

If you want to return one of the default labels to the default values, use the information in [The default Information Protection policy](#).

## Next steps

For more information about configuring the options that you can make for a label, and other settings for your Azure Information Protection policy, use the links in the [Configuring your organization's policy](#) section.

# How to configure a label for Rights Management protection

7/20/2020 • 23 minutes to read • [Edit Online](#)

*Applies to:* [Azure Information Protection](#)

*Instructions for:* [Azure Information Protection client for Windows](#)

## NOTE

To provide a unified and streamlined customer experience, Azure Information Protection client (classic) and Label Management in the Azure Portal are being **deprecated** as of **March 31, 2021**. This time-frame allows all current Azure Information Protection customers to transition to our unified labeling solution using the Microsoft Information Protection Unified Labeling platform. Learn more in the official [deprecation notice](#).

## NOTE

These instructions apply to the Azure Information Protection client (classic) and not the Azure Information Protection unified labeling client. Not sure of the difference between these clients? See this [FAQ](#).

If you are looking for information to configure a sensitivity label to apply Rights Management protection, see the Microsoft 365 Compliance documentation. For example, [Restrict access to content by using encryption in sensitivity labels](#).

You can protect your most sensitive documents and emails by using a Rights Management service. This service uses encryption, identity, and authorization policies to help prevent data loss. The protection is applied with a label that is configured to use Rights Management protection for documents and emails, and users can also select the **Do not forward** button in Outlook.

When your label is configured with the protection setting of **Azure (cloud key)**, under the covers, this action creates and configures a protection template that can then be accessed by services and applications that integrate with Rights Management templates. For example, Exchange Online and mail flow rules, and Outlook on the web.

## How the protection works

When a document or email is protected by a Rights Management service, it is encrypted at rest and in transit. It can then be decrypted only by authorized users. This encryption stays with the document or email, even if it is renamed. In addition, you can configure usage rights and restrictions, such as the following examples:

- Only users within your organization can open the company-confidential document or email.
- Only users in the marketing department can edit and print the promotion announcement document or email, while all other users in your organization can only read this document or email.
- Users cannot forward an email or copy information from it that contains news about an internal reorganization.
- The current price list that is sent to business partners cannot be opened after a specified date.

For more information about the Azure Rights Management protection and how it works, see [What is Azure](#)

## Rights Management?

### IMPORTANT

To configure a label to apply this protection, the Azure Rights Management service must be activated for your organization. For more information, see [Activating the protection service from Azure Information Protection](#).

When the label applies protection, a protected document is not suitable to be saved on SharePoint or OneDrive. These locations do not support the following features for protected files: Co-authoring, Office for the web, search, document preview, thumbnail, eDiscovery, and data loss prevention (DLP).

### TIP

When you [migrate your labels](#) to unified sensitivity labels and publish them from one of the labeling admin centers such as the Microsoft 365 compliance center, labels that apply protection are then supported for these locations. For more information, see [Enable sensitivity labels for Office files in SharePoint and OneDrive \(public preview\)](#).

Exchange does not have to be configured for Azure Information Protection before users can apply labels in Outlook to protect their emails. However, until Exchange is configured for Azure Information Protection, you do not get the full functionality of using Azure Rights Management protection with Exchange. For example, users cannot view protected emails on mobile phones or with Outlook on the web, protected emails cannot be indexed for search, and you cannot configure Exchange Online DLP for Rights Management protection. To ensure that Exchange can support these additional scenarios, see the following resources:

- For Exchange Online, see the instructions for [Exchange Online: IRM Configuration](#).
- For Exchange on-premises, you must deploy the [RMS connector and configure your Exchange servers](#).

## To configure a label for protection settings

1. If you haven't already done so, open a new browser window and [sign in to the Azure portal](#). Then navigate to the **Azure Information Protection** pane.  
For example, in the search box for resources, services, and docs: Start typing **Information** and select **Azure Information Protection**.
2. From the **Classifications > Labels** menu option: On the **Azure Information Protection - Labels** pane, select the label you want to change.
3. On the **Label** pane, locate **Set permissions for documents and emails containing this label**, and select one of the following options:
  - **Not configured**: Select this option if the label is currently configured to apply protection and you no longer want the selected label to apply protection. Then go to step 11.

The previously configured protection settings are retained as an archived protection template, and will be displayed again if you change the option back to **Protect**. You do not see this template in the Azure portal but if necessary, you can still manage the template by using [PowerShell](#). This behavior means that content remains accessible if it has this label with the previously applied protection settings.

When a label with this **Not configured** protection setting is applied:

- If the content was previously protected without using a label, that protection is preserved.
- If the content was previously protected with a label, that protection is removed if the user

applying the label has permissions to remove Rights Management protection. This requirement means that the user must have the [Export or Full Control usage right](#). Or, be the Rights Management owner (which automatically grants the Full Control usage right), or a [super user for Azure Rights Management](#).

If the user doesn't have permissions to remove protection, the label cannot be applied and the following message is displayed: **Azure Information Protection cannot apply this label. If this problem persists, contact your administrator.**

- **Protect:** Select this option to apply protection, and then go to step 4.
- **Remove Protection:** Select this option to remove protection if a document or email is protected. Then go to step 11.

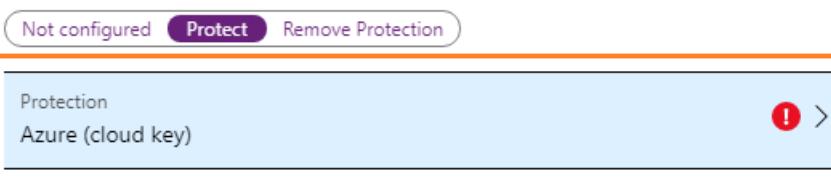
If the protection was applied with a label or protection template, the protection settings are retained as an archived protection template, and will be displayed again if you change the option back to **Protect**. You do not see this template in the Azure portal but if necessary, you can still manage the template by using [PowerShell](#). This behavior means that content remains accessible if it has this label with the previously applied protection settings.

Note that for a user to successfully apply a label that has this option, that user must have permissions to remove Rights Management protection. This requirement means that the user must have the [Export or Full Control usage right](#). Or, be the Rights Management owner (which automatically grants the Full Control usage right), or a [super user for Azure Rights Management](#).

If the user applying the label with this setting does not have permissions to remove Rights Management protection, the label cannot be applied and the following message is displayed: **Azure Information Protection cannot apply this label. If this problem persists, contact your administrator.**

4. If you selected **Protect**, the **Protection** pane automatically opens if one of the other options were previously selected. If this new pane does not automatically open, select **Protection**:

#### Set permissions for documents and emails containing this label



5. On the **Protection** pane, select **Azure (cloud key)** or **HYOK (AD RMS)**.

In most cases, select **Azure (cloud key)** for your permission settings. Do not select **HYOK (AD RMS)** unless you have read and understood the prerequisites and restrictions that accompany this "*hold your own key*" (HYOK) configuration. For more information, see [Hold your own key \(HYOK\) requirements and restrictions for AD RMS protection](#). To continue the configuration for HYOK (AD RMS), go to step 9.

6. Select one of the following options:

- **Set permissions:** To define new protection settings in this portal.
- **Set user-defined permissions (Preview):** To let users specify who should be granted permissions and what those permissions are. You can then refine this option and choose Outlook only, or Word, Excel, PowerPoint, and File Explorer. This option is not supported, and does not work, when a label is configured for [automatic classification](#).

If you choose the option for Outlook: The label is displayed in Outlook and the resulting behavior when users apply the label is the same as the [Do Not Forward](#) option.

If you choose the option for Word, Excel, PowerPoint, and File Explorer: When this option is set, the label is displayed in these applications. The resulting behavior when users apply the label is to display the dialog box for users to select custom permissions. In this dialog box, users choose one of the [predefined permissions levels](#), browse to or specify the users or groups, and optionally, set an expiry date. Make sure that users have instructions and guidance how to supply these values.

- **Select a predefined template:** To use one of the default templates or a custom template that you've configured. Note that this option does not display for new labels, or if you are editing a label that previously used the **Set permissions** option.

To select a predefined template, the template must be published (not archived) and must not be linked already to another label. When you select this option, you can use an **Edit Template** button to [convert the template into a label](#).

If you are used to creating and editing custom templates, you might find it useful to reference [Tasks that you used to do with the Azure classic portal](#).

7. If you selected **Set permissions for Azure (cloud key)**, this option lets you select users and usage rights.

If you don't select any users and select **OK** on this pane, followed by **Save** on the **Label** pane: The label is configured to apply protection such that only the person who applies the label can open the document or email with no restrictions. This configuration is sometimes referred to as "Just for me" and might be the required outcome, so that a user can save a file to any location and be assured that only they can open it. If this outcome matches your requirement and others are not required to collaborate on the protected content, do not select **Add permissions**. After saving the label, the next time you open this **Protection** pane, you see **IPC\_USER\_ID\_OWNER** displayed for **Users**, and **Co-Owner** displayed for **Permissions** to reflect this configuration.

To specify the users you want to be able to open protected documents and emails, select **Add permissions**. Then on the **Add permissions** pane, select the first set of users and groups who will have rights to use the content that will be protected by the selected label:

- Choose **Select from the list** where you can then add all users from your organization by selecting **Add <organization name> - All members**. This setting excludes guest accounts. Or, you can select **Add any authenticated users**, or browse the directory.

When you choose all members or browse the directory, the users or groups must have an email address. In a production environment, users and groups nearly always have an email address, but in a simple testing environment, you might need to add email addresses to user accounts or groups.

More information about [Add any authenticated users](#)

This setting doesn't restrict who can access the content that the label protects, while still encrypting the content and providing you with options to restrict how the content can be used (permissions), and accessed (expiry and offline access). However, the application opening the protected content must be able to support the authentication being used. For this reason, federated social providers such as Google, and onetime passcode authentication should be used for email only, and only when you use Exchange Online and the new capabilities from Office 365 Message Encryption. Microsoft accounts can be used with the Azure Information Protection viewer and Office 365 apps (Click-to-Run).

Some typical scenarios for the any authenticated users setting:

- You don't mind who views the content, but you want to restrict how it is used. For example, you do not want the content to be edited, copied, or printed.
- You don't need to restrict who accesses the content, but you want to be able to track who opens

- it and potentially, revoke it.
- You have a requirement that the content must be encrypted at rest and in transit, but it doesn't require access controls.
  - Choose **Enter details** to manually specify email addresses for individual users or groups (internal or external). Or, use this option to specify all users in another organization by entering any domain name from that organization. You can also use this option for social providers, by entering their domain name such as **gmail.com**, **hotmail.com**, or **outlook.com**.

**NOTE**

If an email address changes after you select the user or group, see the [Considerations if email addresses change](#) section from the planning documentation.

As a best practice, use groups rather than users. This strategy keeps your configuration simpler and makes it less likely that you have to update your label configuration later and then reprotect content. However, if you make changes to the group, keep in mind that for performance reasons, Azure Rights Management [caches the group membership](#).

When you have specified the first set of users and groups, select the permissions to grant these users and groups. For more information about the permissions that you can select, see [Configuring usage rights for Azure Information Protection](#). However, applications that support this protection might vary in how they implement these permissions. Consult their documentation and do your own testing with the applications that users use to check the behavior before you deploy the template for users.

If required, you can now add a second set of users and groups with usage rights. Repeat until you have specified all the users and groups with their respective permissions.

**TIP**

Consider adding the **Save As, Export (EXPORT)** custom permission and grant this permission to data recovery administrators or personnel in other roles that have responsibilities for information recovery. If needed, these users can then remove protection from files and emails that will be protected by using this label or template. This ability to remove protection at the permission level for a document or email provides more fine-grained control than the [super user feature](#).

For all the users and groups that you specified, on the **Protection** pane, now check whether you want to make any changes to the following settings. Note that these settings, as with the permissions, do not apply to the [Rights Management issuer](#) or [Rights Management owner](#), or any [super user](#) that you have assigned.

Information about the protection settings

| SETTING | MORE INFORMATION | RECOMMENDED SETTING |
|---------|------------------|---------------------|
|---------|------------------|---------------------|

| Setting                 | More Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Recommended Setting                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| File Content Expiration | <p>Define a date or number of days for when documents that are protected by these settings should not open for the selected users. For emails, expiration isn't always enforced because of caching mechanisms used by some email clients.</p> <p>You can specify a date or specify a number of days starting from the time that the protection is applied to the content.</p> <p>When you specify a date, it is effective midnight, in your current time zone.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | <b>Content never expires</b> unless the content has a specific time-bound requirement.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Allow offline access    | <p>Use this setting to balance any security requirements that you have (includes access after revocation) with the ability for the selected users to open protected content when they don't have an internet connection.</p> <p>If you specify that content is not available without an internet connection or that content is only available for a specified number of days, when that threshold is reached, these users must be reauthenticated and their access is logged. When this happens, if their credentials are not cached, the users are prompted to sign in before they can open the document or email.</p> <p>In addition to reauthentication, the policy and the user group membership is reevaluated. This means that users could experience different access results for the same document or email if there are changes in the policy or group membership from when they last accessed the content. That could include no access if the document has been <a href="#">revoked</a>.</p> | <p>Depending on how sensitive the content is:</p> <ul style="list-style-type: none"> <li>- <b>Number of days the content is available without an internet connection = 7</b> for sensitive business data that could cause damage to the business if shared with unauthorized people. This recommendation offers a balanced compromise between flexibility and security. Examples include contracts, security reports, forecast summaries, and sales account data.</li> <li>- <b>Never</b> for very sensitive business data that would cause damage to the business if it was shared with unauthorized people. This recommendation prioritizes security over flexibility, and ensures that if the document is revoked, all authorized users immediately cannot open the document. Examples include employee and customer information, passwords, source code, and pre-announced financial reports.</li> </ul> |

When you have finished configuring the permissions and settings, click **OK**.

This grouping of settings creates a custom template for the Azure Rights Management service. These templates can be used with applications and services that integrate with Azure Rights Management. For information about how computers and services download and refresh these templates, see [Refreshing templates for users and services](#).

8. If you selected **Select a predefined template** for Azure (cloud key), click the drop-down box and select the [template](#) that you want to use to protect documents and emails with this label. You do not see archived templates or templates that are already selected for another label.

If you select a **departmental template**, or if you have configured [onboarding controls](#):

- Users who are outside the configured scope of the template or who are excluded from applying Azure Rights Management protection still see the label but cannot apply it. If they select the label, they see the following message: **Azure Information Protection cannot apply this label. If this problem persists, contact your administrator.**

Note that all published templates are always shown, even if you are configuring a scoped policy. For example, you are configuring a scoped policy for the Marketing group. The templates that you can select are not restricted to templates that are scoped to the Marketing group and it's possible to select a departmental template that your selected users cannot use. For ease of configuration and to minimize troubleshooting, consider naming the departmental template to match the label in your scoped policy.

9. If you selected HYOK (AD RMS), select either **Set AD RMS templates details** or **Set user defined permissions (Preview)**. Then specify the licensing URL of your AD RMS cluster.

For instructions to specify a template GUID and your licensing URL, see [Locating the information to specify AD RMS protection with an Azure Information Protection label](#).

The user-defined permissions option lets users specify who should be granted permissions and what those permissions are. You can then refine this option and choose Outlook only (the default), or Word, Excel, PowerPoint, and File Explorer. This option is not supported, and does not work, when a label is configured for [automatic classification](#).

If you choose the option for Outlook: The label is displayed in Outlook and the resulting behavior when users apply the label is the same as the [Do Not Forward](#) option.

If you choose the option for Word, Excel, PowerPoint, and File Explorer: When this option is set, the label is displayed in these applications. The resulting behavior when users apply the label is to display the dialog box for users to select custom permissions. In this dialog box, users choose one of the [predefined permissions levels](#), browse to or specify the users or groups, and optionally, set an expiry date. Make sure that users have instructions and guidance how to supply these values.

10. Click **OK** to close the **Protection** pane and see your choice of **User defined** or your chosen template display for the **Protection** option in the **Label** pane.

11. On the **Label** pane, click **Save**.

12. On the **Azure Information Protection** pane, use the **PROTECTION** column to confirm that your label now displays the protection setting that you want:

- A check mark if you have configured protection.
- An x mark to denote cancellation if you have configured a label to remove protection.
- A blank field when protection is not set.

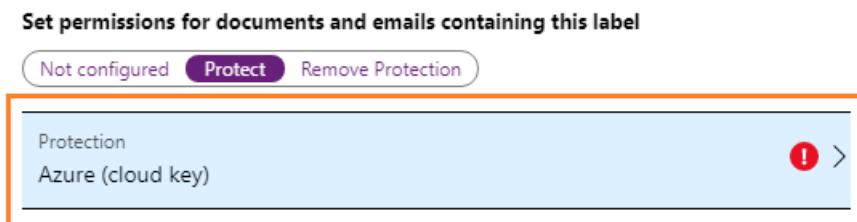
When you clicked **Save**, your changes are automatically available to users and services. There's no longer a separate publish option.

## Example configurations

The **All Employees and Recipients Only** sublabels from the **Confidential** and **High Confidential** labels from the [default policy](#) provide examples of how you can configure labels that apply protection. You can also use the following examples to help you configure protection for different scenarios.

For each example that follows, on your *<label name>* pane, select **Protect**. If the **Protection** pane doesn't automatically open, select **Protection** to open this pane that lets you select your protection configuration

options:



### Example 1: Label that applies Do Not Forward to send a protected email to a Gmail account

This label is available only in Outlook and is suitable when Exchange Online is configured for the [new capabilities in Office 365 Message Encryption](#). Instruct users to select this label when they need to send a protected email to people using a Gmail account (or any other email account outside your organization).

Your users type the Gmail email address in the **To** box. Then, they select the label and the Do Not Forward option is automatically added to the email. The result is that recipients cannot forward the email, or print it, copy from it, or save the email outside their mailbox by using the **Save As** option.

1. On the **Protection** pane, make sure that **Azure (cloud key)** is selected.
2. Select **Set user-defined permissions (Preview)**.
3. Make sure that the following option is selected: **In Outlook apply Do Not Forward**.
4. If selected, clear the following option: **In Word, Excel, PowerPoint and File Explorer prompt user for custom permissions**.
5. Click **OK** on the **Protection** pane, and then click **Save** on the **Label** pane.

### Example 2: Label that restricts read-only permission to all users in another organization, and that supports immediate revocation

This label is suitable for sharing (read-only) very sensitive documents that always require an internet connection to view it. If revoked, users will not be able to view the document the next time they try to open it.

This label is not suitable for emails.

1. On the **Protection** pane, make sure that **Azure (cloud key)** is selected.
2. Make sure that the **Set permissions** option is selected, and then select **Add permissions**.
3. On the **Add permissions** pane, select **Enter details**.
4. Enter the name of a domain from the other organization, for example, **fabrikam.com**. Then select **Add**.
5. From **Choose permissions from preset**, select **Viewer**, and then select **OK**.
6. Back on the **Protection** pane, for **Allow offline access setting**, select **Never**.
7. Click **OK** on the **Protection** pane, and then click **Save** on the **Label** pane.

### Example 3: Add external users to an existing label that protects content

The new users that you add will be able open documents and emails that have already been protected with this label. The permissions that you grant these users can be different from the permissions that the existing users have.

1. On the **Protection** pane, make sure **Azure (cloud key)** is selected.
2. Ensure that **Set permissions** is selected, and then select **Add permissions**.
3. On the **Add permissions** pane, select **Enter details**.

4. Enter the email address of the first user (or group) to add, and then select **Add**.
5. Select the permissions for this user (or group).
6. Repeat steps 4 and 5 for each user (or group) that you want to add to this label. Then click **OK**.
7. Click **OK** on the **Protection** pane, and then click **Save** on the **Label** pane.

#### **Example 4: Label for protected email that supports less restrictive permissions than Do Not Forward**

This label cannot be restricted to Outlook but does provide less restrictive controls than using Do Not Forward. For example, you want the recipients to be able to copy from the email or an attachment, or save and edit an attachment.

If you specify external users who do not have an account in Azure AD:

- The label is suitable for email when Exchange Online is using the [new capabilities in Office 365 Message Encryption](#).
- For Office attachments that are automatically protected, these documents are available to view in a browser. To edit these documents, download and edit them with Office 365 apps (Click-to-Run), and a Microsoft account that uses the same email address. [More information](#)

#### **NOTE**

Exchange Online is rolling out a new option, [Encrypt-Only](#). This option is not available for label configuration. However, when you know who the recipients will be, you can use this example to configure a label with the same set of usage rights.

When your users specify the email addresses in the **To** box, the addresses must be for the same users that you specify for this label configuration. Because users can belong to groups and have more than one email address, the email address that they specify does not have to match the email address that you specify for the permissions. However, specifying the same email address is the easiest way to ensure that the recipient will be successfully authorized. For more information about how users are authorized for permissions, see [Preparing users and groups for Azure Information Protection](#).

1. On the **Protection** pane, make sure that **Azure (cloud key)** is selected.
2. Make sure **Set permissions** is selected, and select **Add permissions**.
3. On the **Add permissions** pane: To grant permissions to users in your organization, select **Add <organization name> - All members** to select all users in your tenant. This setting excludes guest accounts. Or, select **Browse directory** to select a specific group. To grant permissions to external users or if you prefer to type the email address, select **Enter details** and type the email address of the user, or Azure AD group, or a domain name.

Repeat this step to specify additional users who should have the same permissions.

4. For **Choose permissions from preset**, select **Co-Owner**, **Co-Author**, **Reviewer**, or **Custom** to select the permissions that you want to grant.

Note: Do not select **Viewer** for emails and if you do select **Custom**, make sure that you include **Edit** and **Save**.

To select the same permissions that match the new **Encrypt-Only** option from Exchange Online, select **Custom**. Then select all permissions except **Save As**, **Export (EXPORT)** and **Full Control (OWNER)**.

5. To specify additional users who should have different permissions, repeat steps 3 and 4.
6. Click **OK** on the **Add permissions** pane.

7. Click **OK** on the **Protection** pane, and then click **Save** on the **Label** pane.

#### **Example 5: Label that encrypts content but doesn't restrict who can access it**

This configuration has the advantage that you don't need to specify users, groups, or domains to protect an email or document. The content will still be encrypted and you can still specify usage rights, an expiry date, and offline access. Use this configuration only when you do not need to restrict who can open the protected document or email. [More information about this setting](#)

1. On the **Protection** pane, make sure **Azure (cloud key)** is selected.
2. Make sure **Set permissions** is selected, and then select **Add permissions**.
3. On the **Add permissions** pane, on the **Select from the list** tab, select **Add any authenticated users**.
4. Select the permissions you want, and click **OK**.
5. Back on the **Protection** pane, configure settings for **File Content Expiration** and **Allow offline access**, if needed, and then click **OK**.
6. On the **Label** pane, select **Save**.

#### **Example 6: Label that applies "Just for me" protection**

This configuration offers the opposite of secure collaboration for documents: With the exception of a [super user](#), only the person who applies the label can open the protected content, without any restrictions. This configuration is often referred to as "Just for me" protection and is suitable when a user wants to save a file to any location and be assured that only they can open it.

The label configuration is deceptively simple:

1. On the **Protection** pane, make sure **Azure (cloud key)** is selected.
2. Select **OK** without selecting any users, or configuring any settings on this pane.

Although you can configure settings for **File Content Expiration** and **Allow offline access**, when you do not specify users and their permissions, these access settings are not applicable. That's because the person who applies the protection is the [Rights Management issuer](#) for the content, and this role is exempt from these access restrictions.

3. On the **Label** pane, select **Save**.

## **Next steps**

For more information about configuring your Azure Information Protection policy, use the links in the [Configuring your organization's policy](#) section.

Exchange mail flow rules can also apply protection, based on your labels. For more information and examples, see [Configuring Exchange Online mail flow rules for Azure Information Protection labels](#).

# Hold your own key (HYOK) protection for Azure Information Protection

7/20/2020 • 11 minutes to read • [Edit Online](#)

Applies to: [Azure Information Protection](#)

Instructions for: [Azure Information Protection client for Windows](#)

## NOTE

To provide a unified and streamlined customer experience, **Azure Information Protection client (classic)** and **Label Management** in the Azure Portal are being **deprecated** as of **March 31, 2021**. This time-frame allows all current Azure Information Protection customers to transition to our unified labeling solution using the Microsoft Information Protection Unified Labeling platform. Learn more in the official [deprecation notice](#).

Use the following information to understand what hold your own key (HYOK) protection is for Azure Information Protection, and how it is different from the default cloud-based protection. Before you use HYOK protection, make sure that you understand when it's appropriate, the supported scenarios, the limitations, and requirements.

## Cloud-based protection vs. HYOK

When you protect your most sensitive documents and emails by using Azure Information Protection, you typically do this by applying a cloud-based key that uses Azure Rights Management (Azure RMS) protection to benefit from the following:

- No server infrastructure required, which makes the solution quicker and more cost effective to deploy and maintain than an on-premises solution.
- Easier sharing with partners and users from other organizations by using cloud-based authentication.
- Tight integration with other Azure and Office 365 services, such as search, web viewers, pivoted views, anti-malware, eDiscovery, and Delve.
- Document tracking, revocation, and email notification for sensitive documents that you have shared.

A cloud-based key protects your organization's documents and emails by using a private key for the organization that is managed by Microsoft (the default), or managed by you (the "bring your own key" or BYOK scenario). For more information about the tenant key options, see [Planning and implementing your Azure Information Protection tenant key](#).

Documents and emails that you protect could be stored in the cloud or on-premises. For more information about how the protection process works for this cloud-based key, see [What is Azure Rights Management?](#)

Office 365 services and cloud-based applications for your tenant can integrate with Azure Information Protection so that important business functions, such as search, indexing, archiving, and anti-malware services continue to work seamlessly for content that's protected by Azure Information Protection. This ability to read the encrypted content for these scenarios is often referred to as "reasoning over data". For example, it's this ability that lets Exchange Online decrypt emails for malware scanning and to run data loss prevention (DLP) rules on encrypted emails.

However, for regulatory requirements, a few organizations might be required to encrypt content with a key that is

isolated from the cloud. This isolation means that the encrypted content can be read only by on-premises applications and on-premises services. This key management option is supported by Azure Information Protection, and it is referred to as "hold your own key" or HYOK. When you use Azure Information Protection with HYOK, your tenant has both a cloud-based key and an on-premises key.

## HYOK guidance and best practices

Use HYOK protection just for the documents and emails that require the encryption key to be isolated from the cloud. HYOK protection doesn't provide the listed benefits that you get when you use cloud-based key protection, and it often comes at the cost of "data opacity". This phrase means that only on-premises applications and services will be able to open HYOK-protected data; cloud-based services and applications cannot reason over HYOK-protected data.

Even for the organizations that use HYOK protection, it is typically suitable for a small number of documents that need to be protected. As guidance, use it only for documents and when they match all the following criteria:

- The content has the highest classification in your organization ("Top Secret") and access is restricted to just a few people
- The content is not shared outside the organization
- The content is only consumed on the internal network

Because HYOK protection is an administrator configuration option for a label, user workflows remain the same, irrespective of whether the protection uses a cloud-based key or HYOK.

[Scoped policies](#) are a good way to ensure that only the users who need to apply HYOK protection see labels that are configured for HYOK protection.

## Supported scenarios for HYOK

To apply HYOK protection, use Azure Information Protection labels.

The following table lists the supported scenarios for protecting content by using labels that are configured for HYOK, and opening (consuming) content that's protected by HYOK.

| PLATFORM | APPLICATION                                                                                                                      | SUPPORTED                                      |
|----------|----------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------|
| Windows  | Azure Information Protection client with Office 365 apps, Office 2019, Office 2016, and Office 2013<br>- Word, Excel, PowerPoint | Protection: Yes<br>Consumption: Yes            |
| Windows  | Azure Information Protection client with Office 365 apps, Office 2019, Office 2016, and Office 2013<br>- Outlook                 | Protection: Yes<br>Consumption: Yes            |
| Windows  | Azure Information Protection client with File Explorer                                                                           | Protection: Yes<br>Consumption: Yes            |
| Windows  | Azure Information Protection Viewer                                                                                              | Protection: Not applicable<br>Consumption: Yes |

| PLATFORM | APPLICATION                                                          | SUPPORTED                                      |
|----------|----------------------------------------------------------------------|------------------------------------------------|
| Windows  | Azure Information Protection client with PowerShell labeling cmdlets | Protection: Yes<br>Consumption: Yes            |
| Windows  | Azure Information Protection scanner                                 | Protection: Yes<br>Consumption: Yes            |
| Windows  | Rights Management sharing app                                        | Protection: No<br>Consumption: Yes             |
| MacOS    | Office for Mac<br>- Word, Excel, PowerPoint                          | Protection: No<br>Consumption: Yes             |
| MacOS    | Office for Mac<br>- Outlook                                          | Protection: No<br>Consumption: Yes             |
| MacOS    | Rights Management sharing app                                        | Protection: No<br>Consumption: Yes             |
| iOS      | Office Mobile<br>- Word, Excel, PowerPoint                           | Protection: No<br>Consumption: Yes             |
| iOS      | Office Mobile<br>-Outlook                                            | Protection: No<br>Consumption: No              |
| iOS      | Azure Information Protection Viewer                                  | Protection: Not applicable<br>Consumption: Yes |
| Android  | Office Mobile<br>- Word, Excel, PowerPoint                           | Protection: No<br>Consumption: Yes             |
| Android  | Office Mobile<br>- Outlook                                           | Protection: No<br>Consumption: No              |
| Android  | Azure Information Protection Viewer                                  | Protection: Not applicable<br>Consumption: Yes |
| Web      | Outlook on the web                                                   | Protection: No<br>Consumption: No              |
| Web      | Office for the web<br>- Word, Excel, PowerPoint                      | Protection: No<br>Consumption: No              |

| PLATFORM  | APPLICATION                                        | SUPPORTED                         |
|-----------|----------------------------------------------------|-----------------------------------|
| Universal | Office Universal apps<br>- Word, Excel, PowerPoint | Protection: No<br>Consumption: No |

## Additional limitations when using HYOK

Additionally, using HYOK protection with Azure Information Protection labels has the following limitations:

- Does not support versions of Office earlier than Office 2013.
- Office 365 services and other online services will not be able to decrypt HYOK-protected documents and emails to inspect the content and take action on them. This limitation extends to HYOK-protected documents and emails that have been protected with the Rights Management connector.

This loss of functionality for HYOK-protected email includes malware scanners, data loss prevention (DLP) solutions, mail routing rules, journaling, eDiscovery, archiving solutions, and Exchange ActiveSync. In addition, users won't understand why some devices cannot open their HYOK-protected emails, and this can result in calls to your help desk. Because of these many limitations, we do not recommend that you use HYOK protection for emails.

## Implementing HYOK

HYOK is supported by Azure Information Protection when you have a working Active Directory Rights Management Services (AD RMS) deployment with the requirements that are documented in the next section. In this scenario, the usage rights policies and the organization's private key that protects these policies are managed and kept on-premises, while the Azure Information Protection policy for labeling and classification remains managed and stored in Azure.

Do not confuse HYOK and Azure Information Protection with using a full deployment of AD RMS and Azure Information Protection, or as an alternative to migrating AD RMS to Azure Information Protection. HYOK is only supported by applying labels, does not offer feature parity with AD RMS, and does not support all AD RMS deployment configurations:

- For more information about the scenarios that HYOK supports for protecting content and consuming protected content, see the [Supported scenarios for HYOK](#) section.
- For migration instructions from AD RMS, see [Migrating from AD RMS to Azure Information Protection](#).
- For more information about the AD RMS deployment requirements, see the next section.

### Requirements for AD RMS to support HYOK

An AD RMS deployment must meet the following requirements to provide HYOK protection for Azure Information Protection labels.

- AD RMS configuration:
  - Minimal version of Windows Server 2012 R2: Required for production environments but for testing or evaluation purposes, you can use a minimal version of Windows Server 2008 R2 with Service Pack 1.
  - One of the following topologies:
    - Single forest with a single AD RMS root cluster.
    - Multiple forests with independent AD RMS root clusters and users don't have access to the content that's protected by the users in the other forests.

- Multiple forests with AD RMS clusters in each of them. Each AD RMS cluster shares a licensing URL that points to the same AD RMS cluster. On this AD RMS cluster, you must import all the trusted user domain (TUD) certificates from all the other AD RMS clusters. For more information about this topology, see [Trusted User Domain](#).

When you have multiple AD RMS clusters in separate forests, delete any labels in the global policy that apply HYOK (AD RMS) protection and configure a [scoped policy](#) for each cluster. Then, assign users for each cluster to their scoped policy, making sure that you do not use groups that would result in a user being assigned to more than one scoped policy. The result should be that each user has labels for one AD RMS cluster only.

- [Cryptographic Mode 2](#): You can confirm the mode by checking the AD RMS cluster properties, **General** tab.
- Each AD RMS server is configured for the certification URL. [Instructions](#)
- A service connection point (SCP) is not registered in Active Directory: An SCP is not used when you use AD RMS protection with Azure Information Protection.
  - If you have registered an SCP for your AD RMS deployment, you must remove it so that [service discovery](#) is successful for Azure Rights Management protection.
  - If you are installing a new AD RMS cluster for HYOK, skip the step to register the SCP during the configuration of the first node. For each additional node, make sure that the server is configured for the certification URL before you add the AD RMS role and join the existing cluster.
- The AD RMS servers are configured to use SSL/TLS with a valid x.509 certificate that is trusted by the connecting clients: Required for production environments but not required for testing or evaluation purposes.
- Configured rights templates.
- Not configured for Exchange IRM.
- For mobile devices and Mac computers: The [Active Directory Rights Management Services Mobile Device Extension](#) is installed and configured.
- Directory synchronization is configured between your on-premises Active Directory and Azure Active Directory, and users who will use HYOK protection are configured for single sign-on.
- If you share documents or emails that are protected by HYOK with others outside your organization: AD RMS is configured for explicitly defined trusts in a direct point-to-point relationship with the other organizations by using either trusted user domains (TUDs) or federated trusts that are created by using Active Directory Federation Services (AD FS).
- Users have a version of Office that supports Information Rights Management (IRM) and at least Office 2013 Professional Plus with Service Pack 1, running on Windows 7 Service Pack 1 or later. Note that Office 2010 and Office 2007 are not supported for this scenario.
  - For Office 2016, Microsoft Installer (.msi)-based edition: You have installed [update 4018295 for Microsoft Office 2016 that was released on March 6, 2018](#).

## **IMPORTANT**

To fulfill the high assurance that HYOK protection offers, we recommend that your AD RMS servers are not located in your DMZ, and that they are used by only managed devices.

We also recommend that your AD RMS cluster uses a hardware security module (HSM), so that the private key for your Server Licensor Certificate (SLC) cannot be exposed or stolen if your AD RMS deployment should ever be breached or compromised.

For deployment information and instructions for AD RMS, see [Active Directory Rights Management Services](#) in the Windows Server library.

### **Configuring AD RMS servers to locate the certification URL**

1. On each AD RMS server in the cluster, create the following registry entry:

```
Computer\HKEY_LOCAL_MACHINE\Software\Microsoft\DRMS\GICURL = "<string>"
```

For the <string value>, specify one of the following:

- For AD RMS clusters using SSL/TLS:

```
https://<cluster_name>/_wmcs/certification/certification.asmx
```

- For AD RMS clusters not using SSL/TLS (testing networks only):

```
http://<cluster_name>/_wmcs/certification/certification.asmx
```

2. Restart IIS.

### **Locating the information to specify AD RMS protection with an Azure Information Protection label**

When you configure a label for HYOK (AD RMS) protection, you must specify the licensing URL of your AD RMS cluster. In addition, you must specify either a template that you've configured for the permissions to grant users, or let users define the permissions and users.

You can find the template GUID and licensing URL values from the Active Directory Rights Management Services console:

- To locate a template GUID: Expand the cluster and click **Rights Policy Templates**. From the **Distributed Rights Policy Templates** information, you can then copy the GUID from the template you want to use. For example: 82bf3474-6efe-4fa1-8827-d1bd93339119
- To locate the licensing URL: Click the cluster name. From the **Cluster Details** information, copy the **Licensing** value minus the `_wmcs/licensing` string. For example: <https://rmscluster.contoso.com>

If you have an extranet licensing value as well as an intranet licensing value, and they are different: Specify the extranet value only if you will share protected documents or emails with partners that you have defined with explicit point-to-point trusts. Otherwise, use the intranet value and make sure that all your client computers that use AD RMS protection with Azure Information Protection connect by using an intranet connection (for example, remote computers use a VPN connection).

## **Next steps**

To configure a label for HYOK protection, see [How to configure a label for Rights Management protection](#).

# How to configure a label for visual markings for Azure Information Protection

7/20/2020 • 7 minutes to read • [Edit Online](#)

Applies to: [Azure Information Protection](#)

## NOTE

To provide a unified and streamlined customer experience, **Azure Information Protection client (classic)** and **Label Management** in the Azure Portal are being **deprecated** as of March 31, 2021. This time-frame allows all current Azure Information Protection customers to transition to our unified labeling solution using the Microsoft Information Protection Unified Labeling platform. Learn more in the official [deprecation notice](#).

When you assign a label to a document or email message, you can select several options to make the chosen classification easily visible. These visual markings are a header, a footer, and a watermark.

Additional information about these visual markings:

- Headers and footers apply to Word, Excel, PowerPoint, and Outlook.
- Watermarks apply to Word, Excel, and PowerPoint:
  - Excel: Watermarks are visible only in Page layout and Print preview modes, and when printed.
  - PowerPoint: Watermarks are applied to the master slide, as a background image. On the **View** tab, **Slide Master**, make sure that the **Hide Background Graphics** check box is not selected.
- Multiple lines are supported for watermarks, and for headers and footers in Word, Excel, and PowerPoint. If you specify multiple lines for a label's header or footer that is applied in Outlook, the lines are concatenated. In this scenario, consider using the configuration to [set different visual markings for Word, Excel, PowerPoint, and Outlook](#).
- Maximum string lengths:
  - The maximum string length that you can enter for headers and footers is 1024 characters. However, Excel has a total limit of 255 characters for headers and footers. This limit includes characters that aren't visible in Excel, such as formatting codes. If that limit is reached, the string you enter is not displayed in Excel.
  - The maximum string length for watermarks that you can enter is 255 characters.
- You can specify just a text string, or use [variables](#) to dynamically create the text string when the header, footer, or watermark is applied.
- Word, PowerPoint, Outlook, and now Excel support visual markings in different colors.
- Visual markings support one language only.

## When visual markings are applied

For email messages, the visual markings are applied when an email message is sent from Outlook. If that email message is forwarded or replied to with a change of label, the original visual markings are always retained.

For documents, the visual markings are applied as follows:

- In an Office app, the visual markings from a label are applied when the label is applied. Visual markings are also applied when a labeled document is opened and the document is first saved.
- When a document is labeled by using File Explorer, PowerShell, or the Azure Information Protection scanner: Visual markings are not immediately applied but are applied by the Azure Information Protection client when that document is opened in an Office app and the document is first saved.

The exception is when you use [AutoSave](#) with Office apps for files that are saved in Microsoft SharePoint, OneDrive for work or school, or OneDrive for home: When AutoSave is on, visual markings are not applied unless you configure the [advanced client setting](#) to turn on classification to run continuously in the background.

## To configure visual markings for a label

Use the following instructions to configure visual markings for a label.

1. If you haven't already done so, open a new browser window and [sign in to the Azure portal](#). Then navigate to the **Azure Information Protection** pane.

For example, in the search box for resources, services, and docs: Start typing **Information** and select **Azure Information Protection**.

2. From the **Classifications > Labels** menu option: On the **Azure Information Protection - Labels** pane, select the label that contains the visual markings you want to add or change.
3. On the **Label** pane, in the **Set visual marking (such as header or footer)** section, configure the settings for the visual markings that you want, and then click **Save**:
  - To configure a header: For **Documents with this label have a header**, select **On** if you want a header, and **Off** if you do not. If you select **On**, then specify the header text, size, [font](#), [color](#), and alignment for the header.
  - To configure a footer: For **Documents with this label have a footer**, select **On** if you want a footer, and **Off** if you do not. If you select **On**, then specify the footer text, size, [font](#), [color](#), and alignment for the footer.
  - To configure a watermark: For **Documents with this label have a watermark**, select **On** if you want a watermark, and **Off** if you do not. If you select **On**, then specify the watermark text, size, [font](#), [color](#), and alignment for the watermark.

When you click **Save**, your changes are automatically available to users and services. There's no longer a separate publish option.

## Using variables in the text string

The following variables are generally available when using Azure Information Protection classic client and are in public preview availability when using the Azure Information Protection unified labeling client.

You can use the following variables in the text string for your header, footer, or watermark:

- `${Item.Label}` for the selected label. For example: General
- `${Item.Name}` for the file name or email subject. For example: JulySales.docx
- `${Item.Location}` for the path and file name for documents, and the email subject for emails. For example: \\Sales\2016\Q3\JulyReport.docx

- `${User.Name}`  for the owner of the document or email, by the Windows signed in user name. For example: rsimone
- `${User.PrincipalName}`  for the owner of the document or email, by the Azure Information Protection client signed in email address (UPN). For example: rsimone@vanarsdelltd.com
- `${Event.DateTime}`  for the date and time when the selected label was set. For example: 8/16/2016 1:30 PM

#### **NOTE**

This syntax is case-sensitive. For example, if you specify the string

`Document: ${Item.Name} Classification: ${Item.Label}`  for the **General** label footer, the footer text applied to a document named project.docx will be **Document: project.docx Classification: General**.

#### **TIP**

You can also use a [field code to insert the label name](#) into a document or template.

## Setting different visual markings for Word, Excel, PowerPoint, and Outlook

By default, the visual markings that you specify are applied across Word, Excel, PowerPoint, and Outlook. However, you can specify visual markings per Office application type when you use an "If.App" variable statement in the text string, and identify the application type by using the values **Word**, **Excel**, **PowerPoint**, or **Outlook**. You can also abbreviate these values, which is necessary if you want to specify more than one in the same If.App statement.

Use the following syntax:

```
 ${If.App.<application type>}<your visual markings text> ${If.End}
```

#### **NOTE**

This syntax in this statement is case-sensitive.

Examples:

- Set header text for Word documents only:

```
 ${If.App.Word}This Word document is sensitive ${If.End}
```

In Word document headers only, the label applies the header text "This Word document is sensitive". No header text is applied to other Office applications.

- Set footer text for Word, Excel, and Outlook, and different footer text for PowerPoint:

```
 ${If.App.WXO}This content is confidential. ${If.End}${If.App.PowerPoint}This presentation is confidential. ${If.End}
```

In Word, Excel, and Outlook, the label applies the footer text "This content is confidential." In PowerPoint, the label applies the footer text "This presentation is confidential."

- Set specific watermark text for Word and PowerPoint, and then watermark text for Word, Excel, and PowerPoint:

```
 ${If.App.WP}This content is ${If.End}Confidential
```

In Word and PowerPoint, the label applies the watermark text "This content is Confidential". In Excel, the label applies the watermark text "Confidential". In Outlook, the label doesn't apply any watermark text because watermarks as visual markings are not supported for Outlook.

#### **NOTE**

When using the Azure Information Protection unified labeling client, setting values for **font name** is only possible by using the Azure Information Protection portal. When setting values for **font color** beyond one of the five default values, is also only possible by using the Azure Information Protection portal.

### **Setting the font name**

Calibri is the default font for headers, footers, and watermark text. If you specify an alternative font name, make sure that it is available on the client devices that will apply the visual markings. If the font specified is not available, the client falls back to using the Calibri font.

### **Setting the font color**

You can choose from the list of available colors or specify a custom color by entering a hex triplet code for the red, green, and blue (RGB) components of the color. For example, #40e0d0 is the RGB hex value for turquoise.

If you need a reference for these codes, you'll find a helpful table from the [<color>](#) page from the MSDN web docs. You also find these codes in many applications that let you edit pictures. For example, Microsoft Paint lets you choose a custom color from a palette and the RGB values are automatically displayed, which you can then copy.

## **Next steps**

For more information about configuring your Azure Information Protection policy, use the links in the [Configuring your organization's policy](#) section.

# How to configure conditions for automatic and recommended classification for Azure Information Protection

7/20/2020 • 7 minutes to read • [Edit Online](#)

*Applies to:* [Azure Information Protection](#)

*Instructions for:* [Azure Information Protection client for Windows](#)

## NOTE

To provide a unified and streamlined customer experience, **Azure Information Protection client (classic)** and **Label Management** in the Azure Portal are being **deprecated** as of **March 31, 2021**. This time-frame allows all current Azure Information Protection customers to transition to our unified labeling solution using the Microsoft Information Protection Unified Labeling platform. Learn more in the official [deprecation notice](#).

## NOTE

These instructions apply to the Azure Information Protection client (classic) and not the Azure Information Protection unified labeling client. Not sure of the difference between these clients? See this [FAQ](#).

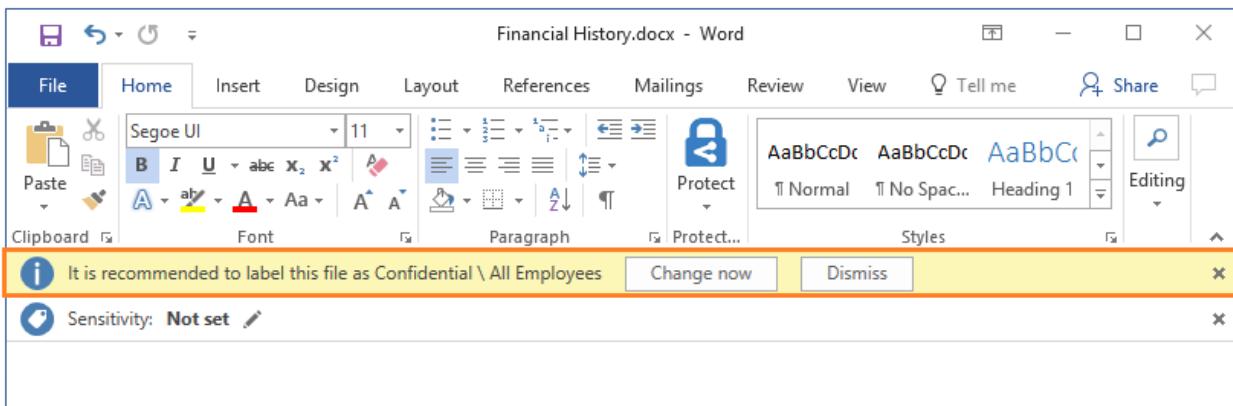
If you are looking for information to configure automatic and recommended classification for the unified labeling client, see the Microsoft 365 Compliance documentation. For example, [Apply a sensitivity label to content automatically](#).

When you configure conditions for a label, you can automatically assign a label to a document or email. Or, you can prompt users to select the label that you recommend.

When you configure these conditions, you can use predefined patterns, such as **Credit Card Number** or **USA Social Security Number (SSN)**. Or, you can define a custom string or pattern as a condition for automatic classification. These conditions apply to the body text in documents and emails, and to headers and footers. For more information about the conditions, see step 5 in the [following procedure](#).

For the best user experience and to ensure business continuity, we recommend that you start with user recommended classification, rather than automatic classification. This configuration lets your users accept the classification and any associated protection, or override these suggestions if they are not suitable for their document or email message.

An example prompt for when you configure a condition to apply a label as a recommended action, with a custom policy tip:



In this example, the user can click **Change now** to apply the recommended label, or override the recommendation by selecting **Dismiss**. If the user chooses to dismiss the recommendation and the condition still applies when the document is next opened, the label recommendation is displayed again.

If you configure automatic classification rather than recommended, the label is automatically applied and the user still sees a notification in Word, Excel, and PowerPoint. However, the **Change now** and **Dismiss** buttons are replaced with **OK**. In Outlook, there is no notification for automatic classification and the label is applied at the time the email is sent.

#### IMPORTANT

Do not configure a label for automatic classification and a user-defined permission. The user-defined permissions option is a [protection setting](#) that lets users specify who should be granted permissions.

When a label is configured for automatic classification and user-defined permissions, the content is checked for the conditions and the user-defined permission setting is not applied. You can use recommended classification and user-defined permissions.

## How automatic or recommended labels are applied

- Automatic classification applies to Word, Excel, and PowerPoint when you save documents, and apply to Outlook when you send emails.

You cannot use automatic classification for documents and emails that were previously manually labeled, or previously automatically labeled with a higher classification.

- Recommended classification applies to Word, Excel, and PowerPoint when you save documents. You cannot use recommended classification for Outlook unless you configure an [advanced client setting](#) that is currently in preview.

You cannot use recommended classification for documents that were previously labeled with a higher classification.

You can change this behavior so that the Azure Information Protection client periodically checks documents for the condition rules that you specify. For example, this would be appropriate if you're using [AutoSave](#) with Office apps that are automatically saved in Microsoft SharePoint, OneDrive for work or school, or OneDrive for home. To support this scenario, you can configure an [advanced client setting](#) that is currently in preview. The setting turns on classification to run continuously in the background.

## How multiple conditions are evaluated when they apply to more than one label

- The labels are ordered for evaluation, according to their position that you specify in the policy: The label positioned first has the lowest position (least sensitive) and the label positioned last has the highest position (most sensitive).

2. The most sensitive label is applied.

3. The last sublabel is applied.

## To configure recommended or automatic classification for a label

1. If you haven't already done so, open a new browser window and [sign in to the Azure portal](#). Then navigate to the **Azure Information Protection** pane.

For example, in the search box for resources, services, and docs: Start typing **Information** and select **Azure Information Protection**.

2. From the **Classifications > Labels** menu option: On the **Azure Information Protection - Labels** pane, select the label to configure.
3. On the **Label** pane, in the **Configure conditions for automatically applying this label** section, click **Add a new condition**.
4. On the **Condition** pane, select **Information Types** if you want to use a predefined condition, or **Custom** if you want to specify your own:

- For **Information Types**: Select from the list of available conditions, and then select the minimum number of occurrences and whether the occurrence should have a unique value to be included in the occurrence count.

The information types use the Office 365 data loss prevention (DLP) sensitivity information types and pattern detection. You can choose from many common sensitive information types, some of which are specific for different regions. For more information, see [What the sensitive information types look for](#) from the Office 365 documentation.

The list of information types that you can select from the Azure portal is periodically updated to include any new Office DLP additions. However, the list excludes any custom sensitive information types that you have defined and uploaded as a rule package to the Office 365 Security & Compliance Center.

### IMPORTANT

Some of the information types require a minimum version of the client. [More information](#)

When Azure Information Protection evaluates the information types that you select, it does not use the Office DLP confidence level setting but matches according to the lowest confidence.

- For **Custom**: Specify a name and phrase to match, which must exclude quotation marks and special characters. Then specify whether to match as a regular expression, use case sensitivity, and the minimum number of occurrences and whether the occurrence should have a unique value to be included in the occurrence count.

The regular expressions use the Office 365 regex patterns. To help you specify regular expressions for your custom conditions, see the following specific version of [Perl Regular Expression Syntax](#) from Boost.

5. Decide whether you need to change the **Minimum number of occurrences** and the **Count occurrence with unique value only**, and then select **Save**.

Example of the occurrences options: You select the information type for the social security number, set the minimum number of occurrences as 2, and a document has the same social security number listed twice: If you set the **Count occurrences with unique value only** to **On**, the condition is not met. If you set

this option to Off, the condition is met.

6. Back on the **Label** pane, configure the following, and then click **Save**:

- Choose automatic or recommended classification: For **Select how this label is applied: automatically or recommended to user**, select **Automatic or Recommended**.
- Specify the text for the user prompt or policy tip: Keep the default text or specify your own string.

When you click **Save**, your changes are automatically available to users and services. There's no longer a separate publish option.

### Sensitive information types that require a minimum version of the client

The following sensitive information types require a minimum version of 1.48.204.0 of the Azure Information Protection client:

- Azure Service Bus Connection String
- Azure IoT Connection String
- Azure Storage Account
- Azure IAAS Database Connection String and Azure SQL Connection String
- Azure Redis Cache Connection String
- Azure SAS
- SQL Server Connection String
- Azure DocumentDB Auth Key
- Azure Publish Setting Password
- Azure Storage Account Key (Generic)

For more information about these sensitive information types, see the following blog post: [Azure Information Protection helps you to be more secure by automatically discovering credentials](#)

Additionally, beginning with 1.48.204.0 of the Azure Information Protection client, the following sensitive information types are not supported and no longer display in the Azure portal. If you have labels that use these sensitive information types, we recommend that you remove them because we cannot ensure correct detection for them and any references to them in the scanner reports should be ignored:

- EU Phone Number
- EU GPS Coordinates

## Next steps

Consider deploying the [Azure Information Protection scanner](#), which can use your automatic classification rules to discover, classify, and protect files on network shares and on-premises file stores.

For more information about configuring your Azure Information Protection policy, use the links in the [Configuring your organization's policy](#) section.

# How to configure the Azure Information Protection policy for specific users by using scoped policies

7/20/2020 • 4 minutes to read • [Edit Online](#)

Applies to: [Azure Information Protection](#)

Instructions for: [Azure Information Protection client for Windows](#)

## NOTE

To provide a unified and streamlined customer experience, **Azure Information Protection client (classic)** and **Label Management** in the Azure Portal are being **deprecated** as of **March 31, 2021**. This time-frame allows all current Azure Information Protection customers to transition to our unified labeling solution using the Microsoft Information Protection Unified Labeling platform. Learn more in the official [deprecation notice](#).

When the Azure Information Protection policy downloads to computers that have installed the [Azure Information Protection client](#), all users get the settings and labels from the default policy or the changes that you configured for the global policy. If you want to supplement this configuration for specific users, by having different settings and labels, you must create a **scoped policy** that's configured for those users.

## How scoped policies work

For applications that support the Azure Information Protection client, all users receive the global policy, which contains the Information Protection bar title and tooltip, global settings, and global labels. If you have configured scoped policies for specific users, those users then receive those additional settings and labels.

Note that in addition to the Office desktop applications that support the Azure Information Protection client, labels are also supported with PowerShell, and the Azure Information Protection scanner. This means that you can create and configure scoped policies for accounts that run PowerShell commands, or the scanner.

Scoped policies, just like labels, are ordered in the Azure portal. If a user is configured for multiple scopes, an effective policy is computed for that user before it is downloaded. According to the order of the policies, the last policy setting is applied. The labels that the user sees are from the global policy and any additional labels from scoped policies that the user belongs to.

The exception is when a user from your tenant opens a labeled document or email and that user is not in the label's scope. In this scenario, the user sees the name of the label set but the label isn't displayed as available to select.

Because a scoped policy always inherits the labels and settings and from the global policy, the labels from the global policy are displayed when you create or edit a scoped policy. However, you cannot edit the labels from the global policy when you edit a scoped policy. You can however, add sublabels to these inherited labels.

For example, if you have a label named **Confidential** in the global policy, all users see this label. You cannot remove or reorder it with a scoped policy. But you might want to create a scoped policy for the Marketing department that adds a new sublabel to Confidential, so that these users see **Confidential \ Promotions**. You also create another scoped policy for the Sales department that adds a new sublabel to Confidential, so that these users see **Confidential \ Partners**. Each sublabel can then be configured for different settings and the sublabel is visible only to the users in the respective departments.

# Configure a scoped policy

1. If you haven't already done so, open a new browser window and [sign in to the Azure portal](#). Then navigate to the **Azure Information Protection** pane.  
For example, in the search box for resources, services, and docs: Start typing **Information** and select **Azure Information Protection**.
2. From the **Classifications > Policies** menu option: On the **Azure Information Protection - Policies** pane, select **Add a new policy**. You then see the **Policy** pane that displays your existing global policy, where you can now configure your new, scoped policy.
3. Specify a policy name and description that only administrators see in the Azure portal. The name must be unique to your tenant. Then select **Specify which users/groups get this policy**, and in the subsequent panes, you can search and select the users and groups for this policy. The labels and settings that you configure in this scoped policy will be applied to these users only.

For performance reasons, group membership for scoped policies is [cached](#).

## NOTE

Select up to 200 users or groups. If more than 200 users are needed to get the scoped policy, create a new group, add relevant users to the group, and then set the policy scope to the new group.

4. Now add new labels or configure the scoped policy settings. The global policy is always applied first, so you can supplement the global policy with new labels and you can override the global settings. For example, the global policy might have no default label specified and you configure a different default label in different scoped policies for specific departments.  
If you need help with configuring the labels or settings, use the links in the [Configuring your organization's policy](#) section.
5. Just as when you edit the global policy, when you make any changes on an Azure Information Protection pane, click **Save** to save the changes, or click **Discard** to revert to the last saved settings.
6. When you have finished making the changes that you want for this scoped policy, on the initial **Azure Information Protection - Policies** pane, make sure that this scoped policy is in the order that you want it applied. This is important when you have selected the same user for multiple scoped policies. To change the order, select the context menu (...) and select **Move up** or **Move down**.

The Azure Information Protection client checks for any changes whenever a supported Office application starts or File Explorer is opened. The client downloads any changes to the global policy or scoped policies that apply to that user.

## Next steps

For an example of how to customize the default policy, and see the resulting behavior in an Office application, try the [Edit the policy and create a new label](#) tutorial.

# Configuring and managing templates for Azure Information Protection

7/20/2020 • 11 minutes to read • [Edit Online](#)

*Applies to: Azure Information Protection, Office 365*

*Instructions for: Azure Information Protection client for Windows*

## NOTE

To provide a unified and streamlined customer experience, **Azure Information Protection client (classic)** and **Label Management** in the Azure Portal are being **deprecated** as of **March 31, 2021**. This time-frame allows all current Azure Information Protection customers to transition to our unified labeling solution using the Microsoft Information Protection Unified Labeling platform. Learn more in the official [deprecation notice](#).

Protection templates, also known as Rights Management templates, are a grouping of administrator-defined protection settings for Azure Information Protection. These settings include your chosen [usage rights](#) for authorized users, and access controls for expiry and offline access. These templates are integrated with the Azure Information Protection policy:

**When you have a subscription that includes classification, labeling, and protection (Azure Information Protection P1 or P2):**

- Templates that are not integrated with your labels for your tenant are displayed in the **Protection templates** section after your labels on the **Azure Information Protection - Labels** pane. To navigate to this pane, select the **Classifications > Labels** menu option. You can convert these templates to labels, or you can link to them when you configure protection for your labels.

**When you have a subscription that includes protection only (an Office 365 subscription that includes the Azure Rights Management service):**

- Templates for your tenant are displayed in the **Protection templates** section on the **Azure Information Protection - Labels** pane. To navigate to this pane, select the **Classifications > Labels** menu option. No labels are displayed. You also see configuration settings that are specific to classification and labeling, but these settings either have no effect on your templates or cannot be configured.

## NOTE

In some applications and services, you might see **Do Not Forward** and **Encrypt-Only** (or **Encrypt**) displayed as a template. These are not templates that you can edit or delete, but options that come by default with the Exchange service.

## Default templates

When you obtain your subscription for Azure Information Protection or for an Office 365 subscription that includes the Azure Rights Management service, two default templates are automatically created for your tenant. These templates restrict access to authorized users in your organization. When these templates are created, they have the permissions that are listed in the [Configuring usage rights for Azure Information Protection](#) documentation.

In addition, the templates are configured to allow offline access for seven days and do not have an expiration date.

#### NOTE

You can change these settings, and the names and descriptions of the default templates. This ability was not possible with the Azure classic portal and remains unsupported for PowerShell.

These default templates make it easy for you and others to immediately start protecting your organization's sensitive data. These templates can be used with Azure Information Protection labels, or by themselves with [applications and services](#) that can use Rights Management templates.

You can also create your own custom templates. Although you probably require only a few templates, you can have a maximum of 500 custom templates saved in Azure.

#### Default template names

If you recently obtained your subscription, your default templates are created with the following names:

- Confidential \ All Employees
- Highly Confidential \ All Employees

If you obtained your subscription some time ago, your default templates might be created with the following names:

- <organization name> - Confidential
- <organization name> - Confidential View Only

You can rename (and reconfigure) these default templates when you use the Azure portal.

#### NOTE

If you don't see your default templates in the **Azure Information Protection - Labels** pane, they are converted to labels, or linked to a label. They still exist as templates, but in the Azure portal, you see them as part of a label configuration that includes protection settings for a cloud key. You can always confirm what templates your tenant has, by running the [Get-AipServiceTemplate](#) from the [AIPService PowerShell module](#).

You can manually convert templates, as explained in the later section, [To convert templates to labels](#), and then rename them if you want. Or they are converted automatically for you if your default Azure Information Protection policy was recently created and the Azure Rights Management service for your tenant was activated at that time.

Templates that are archived display as unavailable in the **Azure Information Protection - Labels** pane. These templates cannot be selected for labels but they can be converted to labels.

## Considerations for templates in the Azure portal

Before you edit these templates or convert them to labels, make sure that you are aware of the following changes and considerations. Because of implementation changes, the following list is especially important if you previously managed templates in the Azure classic portal.

- After you edit or convert a template and save the Azure Information Protection policy, the following changes are made to the original [usage rights](#). If required, you can add or remove individual usage rights by using the Azure portal. Or, use PowerShell with the [New-AipServiceRightsDefinition](#) and [Set-AipServiceTemplateProperty](#) cmdlets.
  - **Allow Macros** (common name) is automatically added. This usage right is required for the Azure

Information Protection bar in Office apps.

- Published and Archived settings display as Enabled: On and Enabled: Off respectively on the Label pane. For templates that you want to retain but not be visible to users or services, set these templates to Enabled: Off.
- You cannot copy or delete a template in the Azure portal. When the template is converted to a label, you can configure the label to stop using the template by selecting Not configured for the Set permissions for documents and emails containing this label option. Or, you can delete the label. In both scenarios however, the template is not deleted and remains in an archived state.

You could now delete the template by using the PowerShell [Remove-AipServiceTemplate](#) cmdlet. You can also use this PowerShell cmdlet for templates that are not converted to labels. However, to ensure that previously protected content can be opened and used as intended, we usually advise against deleting templates. As a best practice, delete templates only if you are sure they were not used to protect documents or emails in production. As a precaution, you might want to consider first exporting the template as a backup, by using the [Export-AipServiceTemplate](#) cmdlet.

- Currently, if you edit and save a departmental template, it removes the scope configuration. The equivalent of a scoped template in the Azure Information Protection policy is a [scoped policy](#). If you convert the template to a label, you can select an existing scope.

In addition, you cannot set the application compatibility setting for a departmental template by using the Azure portal. If necessary, you can set this application compatibility setting by using the [Set-AipServiceTemplateProperty](#) cmdlet and the *EnableInLegacyApps* parameter.

- When you convert or link a template to a label, it can no longer be used by other labels. In addition, this template no longer displays in the **Protection templates** section.
- You do not create a new template from the **Protection templates** section. Instead, create a label that has the **Protect** setting, and configure the usage rights and settings from the **Protection** pane. For full instructions, see [To create a new template](#).

## To configure the templates in the Azure Information Protection policy

1. If you haven't already done so, open a new browser window and [sign in to the Azure portal](#). Then navigate to the **Azure Information Protection - Labels** pane.

For example, in the search box for resources, services, and docs: Start typing **Information** and select **Azure Information Protection**.

2. From the **Classifications > Labels** menu option: On the **Azure Information Protection - Labels** pane, expand **Protection templates**, and then locate the template that you want to configure.
3. Select the template, and on the **Label** pane, you can change the template name and description if required, by editing the **Label display name** and **Description**. Then, select **Protection** that has a value of **Azure (cloud key)**, to open the **Protection** pane.
4. On the **Protection** pane, you can change the permissions, content expiration, and offline access settings. For more information about configuring the protection settings, see [How to configure a label for Rights Management protection](#)

Click **OK** to keep your changes, and on the **Label** pane, click **Save**.

#### **NOTE**

You can also edit a template by using the **Edit Template** button on the **Protection** pane if you have configured a label to use a predefined template. Providing no other label also uses the selected template, this button converts the template into a label, and takes you to step 5. For more information about what happens when templates are converted to labels, see the next section.

## To convert templates to labels

When you have a subscription that includes classification, labeling, and protection, you can convert a template to a label. When you convert a template, the original template is retained but in the Azure portal, it now displays as included in a new label.

For example, if you convert a label named **Marketing** that grants usage rights to the marketing group, in the Azure portal it now displays as a label named **Marketing** that has the same protection settings. If you change the protection settings in this newly created label, you're changing them in the template and any user or service that uses this template will get the new protection settings with the next template refresh.

There is no requirement to convert all your templates to labels, but when you do, the protection settings are fully integrated with the full functionality of labels so that you do not have to maintain the settings separately.

To convert a template into a label, right-click the template, and select **Convert to label**. Alternatively, use the context-menu to select this option.

You can also convert a template to a label when you configure a label for protection and a predefined template, by using the **Edit Template** button.

When you convert a template to a label:

- The name of the template is converted to a new label name, and the template description is converted to the label tooltip.
- If the status of the template was published, this setting maps to **Enabled: On** for the label, which now displays as this label to users when you next publish the Azure Information Protection policy. If the status of the template was archived, this setting maps to **Enabled: Off** for the label and does not display as an available label to users.
- The protection settings are retained, and you can edit these if required, and also add other label settings such as visual markers and conditions.
- The original template is no longer displayed in **Protection templates** and cannot be selected as a predefined template when you configure protection for a label. To edit this template in the Azure portal, you now edit the label that was created when you converted the template. The template remains available for the Azure Rights Management service, and can still be managed by using [PowerShell commands](#).

## To create a new template

Templates can be created using the portal or using PowerShell.

### **Template creation using PowerShell**

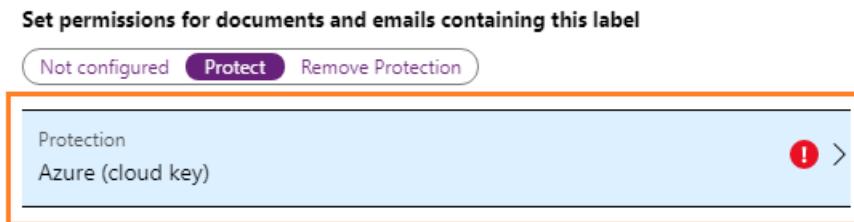
To create a new protection template using PowerShell with the specified name, description, policy, and desired status setting use the [Add-AipServiceTemplate](#) cmdlet.

### **Template creation using the portal**

When you create a new label using the portal with the protection setting of **Azure (cloud key)**, this action

creates a new custom template that can then be accessed by services and applications that integrate with Rights Management templates.

1. From the **Classifications > Labels** menu option: On the **Azure Information Protection - Labels** pane, select **Add a new label**.
2. On the **Label** pane, keep the default of **Enabled: On**, then enter a label name and description for the template name and description.
3. For **Set permissions for documents and emails containing this label**, select **Protect**, and then select **Protection**:



4. On the **Protection** pane, you can change the permissions, content expiration, and offline access settings. For more information about configuring these protection settings, see [How to configure a label for Rights Management protection](#)

Click **OK** to keep your changes, and on the **Label** pane, click **Save**.

On the **Azure Information Protection - Labels** pane, you now see your new label displayed with the **PROTECTION** column to indicate that it contains protection settings. These protection settings display as templates to applications and services that support the Azure Rights Management service.

Although the label is enabled, by default, the template is archived. So that applications and services can use the template to protect documents and emails, complete the final step to publish the template.

5. From the **Classifications > Policies** menu option, select the policy to contain the new protection settings. Then select **Add or remove labels**. From the **Policy: Add or remove labels** pane, select the newly created label that contains your protection settings, select **OK**, and then select **Save**.

## Next steps

It can take up to 15 minutes for a computer running the Azure Information Protection client to get these changed settings. For information about how computers and services download and refresh templates, see [Refreshing templates for users and services](#).

Everything that you can configure in the Azure portal to create and manage your templates, you can do by using PowerShell. In addition, PowerShell provides more options that are not available in the portal. For more information, see [PowerShell reference for protection templates](#).

For more information about configuring your Azure Information Protection policy, use the links in the [Configuring your organization's policy](#) section.

# Refreshing templates for users and services

7/20/2020 • 6 minutes to read • [Edit Online](#)

Applies to: [Azure Information Protection](#), [Office 365](#)

## NOTE

To provide a unified and streamlined customer experience, **Azure Information Protection client (classic)** and **Label Management** in the Azure Portal are being **deprecated** as of March 31, 2021. This time-frame allows all current Azure Information Protection customers to transition to our unified labeling solution using the Microsoft Information Protection Unified Labeling platform. Learn more in the official [deprecation notice](#).

When you use the Azure Rights Management service from Azure Information Protection, protection templates are automatically downloaded to client computers so that users can select them from their applications. However, you might need to take additional steps if you make changes to the templates:

| APPLICATION OR SERVICE                                                        | HOW TEMPLATES ARE REFRESHED AFTER CHANGES                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Exchange Online<br><br>Applicable for transport rules and the Outlook web app | Automatically refreshed within an hour - no additional steps required.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Azure Information Protection client                                           | Automatically refreshed whenever the Azure Information Protection policy is refreshed on the client: <ul style="list-style-type: none"><li>- When an Office application opens that supports the Azure Information Protection bar.</li><li>- When you right-click to classify and protect a file or folder.</li><li>- When you run the PowerShell cmdlets for labeling and protection (Get-AIPFileStatus and Set-AIPFileLabel).</li><li>- When the Azure Information Protection Scanner service starts and the local policy is older than one hour. In addition, the scanner service checks for changes every hour and uses these changes for the next scan cycle.</li><li>- Every 24 hours.</li></ul> <p>Additionally, because this client is tightly integrated with Office, any refreshed templates for Office 365 apps, Office 2019, Office 2016, or Office 2013 will also be refreshed for the Azure Information Protection client.</p> |

| APPLICATION OR SERVICE                                                                                                  | HOW TEMPLATES ARE REFRESHED AFTER CHANGES                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Azure Information Protection unified labeling client                                                                    | <p>For Office apps, the templates automatically refresh every time the app is opened.</p> <p>Additionally, because this client is tightly integrated with Office, any refreshed templates for Office 365 apps, Office 2019, Office 2016, or Office 2013 will also be refreshed for the Azure Information Protection unified labeling client.</p> <p>For File Explorer, PowerShell, and the scanner, the client doesn't download templates but accesses them online - no additional steps required.</p> |
| Office 365 apps, Office 2019, Office 2016, and Office 2013                                                              | <p>Automatically refreshed - on a schedule:</p> <ul style="list-style-type: none"> <li>- For these later versions of Office: The default refresh interval is every 7 days.</li> </ul> <p>To force a refresh sooner than the schedule, see the following section, <a href="#">Office 365 apps, Office 2019, Office 2016, and Office 2013: How to force a refresh for templates</a>.</p>                                                                                                                 |
| Office 2010                                                                                                             | Automatically refreshed when users sign out from Windows, sign back in, and wait up to 1 hour.                                                                                                                                                                                                                                                                                                                                                                                                         |
| Exchange on-premises with the Rights Management connector<br><br>Applicable for transport rules and the Outlook web app | Automatically refreshed - no additional steps required. However, the Outlook web app caches the UI for a day.                                                                                                                                                                                                                                                                                                                                                                                          |
| Office 2019 for Mac and Office 2016 for Mac                                                                             | Automatically refreshed when you open protected content. To force a refresh, see the following section, <a href="#">Office 2019 for Mac and Office 2016 for Mac: How to force a refresh for templates</a> .                                                                                                                                                                                                                                                                                            |
| RMS sharing app for Mac computers                                                                                       | Automatically refreshed - no additional steps required.                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Office 365 ProPlus apps with <a href="#">built-in labeling</a>                                                          | This built-in labeling client doesn't download templates but accesses them online - no additional steps required.                                                                                                                                                                                                                                                                                                                                                                                      |

When client applications need to download templates (initially or refreshed for changes), be prepared to wait up to 30 minutes before the download is complete and the new or updated templates are fully operational. The actual time will vary, according to factors such as the size and complexity of the template configuration, and the network connectivity.

## Office 365 apps, Office 2019, Office 2016, and Office 2013: How to force a refresh for templates

By editing the registry on the computers running Office 365 apps, Office 2019, Office 2016, or Office 2013, you can change the automatic schedule so that changed templates are refreshed on computers more frequently than their default value. You can also force an immediate refresh by deleting the existing data in a registry value.

## WARNING

If you use the Registry Editor incorrectly, you might cause serious problems that might require you to reinstall the operating system. Microsoft cannot guarantee that you can solve problems that result from using the Registry Editor incorrectly. Use the Registry Editor at your own risk.

### To change the automatic schedule

1. Using a registry editor, create and set one of the following registry values:

- To set an update frequency in days (minimum of 1 day): Create a new registry value named **TemplateUpdateFrequency** and define an integer value for the data, which specifies the frequency in days to download any changes to a downloaded template. Use the following information to locate the registry path to create this new registry value.

**Registry path:** HKEY\_CURRENT\_USER\Software\Classes\Local Settings\Software\Microsoft\MSIPC

**Type:** REG\_DWORD

**Value:** TemplateUpdateFrequency

- To set an update frequency in seconds (minimum of 1 second): Create a new registry value named **TemplateUpdateFrequencyInSeconds** and define an integer value for the data, which specifies the frequency in seconds to download any changes to a downloaded template. Use the following information to locate the registry path to create this new registry value.

**Registry path:** HKEY\_CURRENT\_USER\Software\Classes\Local Settings\Software\Microsoft\MSIPC

**Type:** REG\_DWORD

**Value:** TemplateUpdateFrequencyInSeconds

Make sure that you create and set one of these registry values, not both. If both are present, **TemplateUpdateFrequency** is ignored.

2. If you want to force an immediate refresh of the templates, go to the next procedure. Otherwise, restart your Office applications and instances of File Explorer now.

### To force an immediate refresh

1. Using a registry editor, delete the data for the **LastUpdatedTime** value. For example, the data might display **2015-04-20T15:52**; delete **2015-04-20T15:52** so that no data is displayed. Use the following information to locate the registry path to delete this registry value data.

**Registry path:** HKEY\_CURRENT\_USER\Software\Classes\Local Settings\Software\Microsoft\MSIPC\<MicrosoftRMS\_FQDN>\Template\<user\_alias>

**Type:** REG\_SZ

**Value:** LastUpdatedTime

**TIP**

In the registry path, <MicrosoftRMS\_FQDN> refers to your Microsoft RMS service FQDN. If you want to verify this value:

Run the [Get-AipServiceConfiguration](#) cmdlet for Azure Information Protection. If you haven't already installed the AIPService PowerShell module, see [Installing the AIPService PowerShell module](#).

From the output, identify the **LicensingIntranetDistributionPointUrl** value.

For example: **LicensingIntranetDistributionPointUrl** : [https://5c6bb73b-1038-4eec-863d-49bded473437.rms.na.aadrm.com/\\_wmcs/licensing](https://5c6bb73b-1038-4eec-863d-49bded473437.rms.na.aadrm.com/_wmcs/licensing)

From the value, remove **https://** and **\_wmcs/licensing** from this string. The remaining value is your Microsoft RMS service FQDN. In our example, the Microsoft RMS service FQDN would be the following value:

**5c6bb73b-1038-4eec-863d-49bded473437.rms.na.aadrm.com**

2. Delete the following folder and all files it contains: %localappdata%\Microsoft\MSIPC\Templates

3. Restart your Office applications and instances of File Explorer.

## Office 2019 for Mac and Office 2016 for Mac: How to force a refresh for templates

In these versions of Office for Mac, templates refresh when you open protected content or you protect content by using a sensitivity label that's newly configured to apply encryption. If you need to force a refresh of the templates, you can use the following instructions. However, the command in the instructions deletes the templates, the RMS token cache in the key chain, and local use licenses for any previously opened protected content. As a result, you will need to authenticate again and you must have an internet connection to open the previously opened protected content.

1. Open Terminal, and enter the following command:

```
defaults write
~/Library/Containers/com.microsoft.Outlook/Data/Library/Preferences/com.microsoft.Outlook ResetRMSCache
1
```

2. Restart Outlook for Mac.

3. Create a new email and select **Encrypt**, and then **Verify Credentials**.

## See Also

[Configuring and managing templates in the Azure Information Protection policy](#)

# PowerShell reference for protection templates

7/20/2020 • 2 minutes to read • [Edit Online](#)

*Applies to: Azure Information Protection, Office 365*

Protection settings for Azure Information Protection are saved in protection templates. Everything that you can do in the Azure portal to create and manage protection settings, you can do from the command line by using PowerShell.

In addition, you can export and import protection templates. These two actions let you copy protection templates between tenants or do bulk edits of complex properties, such as multilingual names and descriptions.

You can also use export and import to back up and restore your protection templates. As a best practice, regularly back up your templates. Then, if you make a change to the protection settings that wasn't intended, you can easily revert to a previous version.

For installation instructions, see [Installing the AIPService PowerShell module](#).

The cmdlets that support creating and managing protection templates:

- [Add-AipServiceTemplate](#)
- [Export-AipServiceTemplate](#)
- [Get-AipServiceTemplate](#)
- [Get-AipServiceTemplateProperty](#)
- [Import-AipServiceTemplate](#)
- [New-AipServiceRightsDefinition](#)
- [Remove-AipServiceTemplate](#)
- [Set-AipServiceTemplateProperty](#)

## See Also

[Configuring and managing templates for Azure Information Protection](#)

# Tasks that you used to do with the Azure classic portal

3/16/2020 • 4 minutes to read • [Edit Online](#)

Applies to: [Azure Information Protection](#), [Office 365](#)

## NOTE

To provide a unified and streamlined customer experience, **Azure Information Protection client (classic)** and **Label Management** in the Azure Portal are being **deprecated** as of **March 31, 2021**. This time-frame allows all current Azure Information Protection customers to transition to our unified labeling solution using the Microsoft Information Protection Unified Labeling platform. Learn more in the official [deprecation notice](#).

Used to the Azure classic portal for managing the Azure Rights Management service, and need some help transitioning to the Azure portal?

The Azure classic portal retired **January 08, 2018**. After this date, you will not be able to manage the Azure Rights Management service and custom templates from the classic portal. If you try to access the classic portal, you see a link that takes you to the new Azure portal.

For more information about the classic portal retirement, see the blog post announcement: [Marching into the future of the Azure AD admin experience: retiring the Azure classic portal](#). For the temporary extension to the original retirement date, see [Update on retirement of Azure AD classic portal experience and migration of conditional access policies](#).

## How to do your familiar admin tasks

Use the following information to help you quickly transition to the current portal.

| AZURE CLASSIC PORTAL                                 | HOW TO DO THIS TASK IN THE AZURE PORTAL                                                                                                                                                                                                                                                                                                                                                               |
|------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Access the configuration settings for the first time | <ol style="list-style-type: none"><li>1. <a href="#">Sign in to the Azure portal</a>.</li><li>2. Follow the instructions for <a href="#">To access the Azure Information Protection pane for the first time</a>.</li></ol>                                                                                                                                                                            |
| Create a new template                                | <p>Create a label that applies protection, and use <b>Set permissions</b> to define the permissions, expiration, and offline access.</p> <p>Under the covers, this configuration creates a new custom template that can then be accessed by services and applications that integrate with Rights Management templates.</p> <p>For more information, see <a href="#">To create a new template</a>.</p> |

| AZURE CLASSIC PORTAL                                                                                                                | HOW TO DO THIS TASK IN THE AZURE PORTAL                                                                                                                                                                                                                                                                                                                                                                                              |
|-------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Edit the template properties:<br>- Template name and description<br>- Usage rights, content expiration, and offline access settings | If you haven't already done so, <a href="#">convert the template to a label</a> , and then do the following<br><ol style="list-style-type: none"> <li>1. Change the label name and description</li> <li>2. Change the protection settings on the label to update the permissions, expiration, and offline access settings.</li> </ol> <p>For more information, see <a href="#">To configure a label for protection settings</a>.</p> |
| Archive a template                                                                                                                  | Set the label status to <b>Disabled</b> .                                                                                                                                                                                                                                                                                                                                                                                            |
| Create a scoped template                                                                                                            | Create a scoped policy and create a label in this scope that applies protection.<br><br>For more information, see <a href="#">How to configure the Azure Information Protection policy for specific users by using scoped policies</a> .                                                                                                                                                                                             |
| Copy a template                                                                                                                     | You can't copy a template in the Azure portal. If you want two labels to have the same protection settings, you must set the permissions on each label.<br><br>For more information, see <a href="#">To configure a label for protection settings</a> .                                                                                                                                                                              |
| Delete a template                                                                                                                   | Deleting templates can result in inaccessible data, so the Azure portal doesn't support this action. However, you can delete the label and then use the PowerShell <a href="#">Remove-AipServiceTemplate</a> cmdlet to remove the template.<br><br>For more information, see <a href="#">How to delete or reorder a label for Azure Information Protection</a> .                                                                     |
| Multi-language support                                                                                                              | From the <b>Manage</b> menu selection, select <b>Languages</b> to export the customizable fields that include the template name and description. Translate the strings, and then import these strings into the portal.<br><br>For more information, see <a href="#">How to configure labels and templates for different languages in Azure Information Protection</a> .                                                              |
| Rights Management web reports                                                                                                       | <a href="#">Centralized reporting for Azure Information Protection</a> is now in preview.<br><br>You can also use the PowerShell <a href="#">Get-AipServiceUsageLog</a> cmdlet to download usage logs for the Azure Rights Management service. You can then use this data to create customized reports. For more information, see <a href="#">Logging and analyzing the protection usage from Azure Information Protection</a> .     |

| AZURE CLASSIC PORTAL                                  | HOW TO DO THIS TASK IN THE AZURE PORTAL                                                                                                                                                                           |
|-------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Activate and deactivate the Rights Management service | <p>From the <b>Manage</b> menu options, select <b>Protection activation</b>.</p> <p>For more information, see <a href="#">How to activate the Rights Management protection service from the Azure portal</a>.</p> |

Before you edit your templates or convert them to labels in the Azure portal, see [Considerations for templates in the Azure portal](#).

## What else has changed

New functionality in the Azure portal:

- You can edit the [default templates](#) that are automatically created for your organization.
- You can convert templates to labels, so that you manage a single object rather than manage a template and label independently. For instructions, see [To convert templates to labels](#).
- Support for other admin roles: Whereas you had to sign in to the Azure classic portal as a Global administrator to configure Azure Rights Management, you can sign in to the Azure portal to manage Azure Information Protection by using many other administrative roles that include **Compliance administrator** and **Compliance data administrator**. The full list of roles supported are included in the [Signing in to the Azure portal](#) section.

The PowerShell cmdlets to create and manage templates, and to activate or deactivate the service, remain supported without changes.

## See also

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

# How to configure labels and templates for different languages in Azure Information Protection

7/20/2020 • 5 minutes to read • [Edit Online](#)

Applies to: [Azure Information Protection](#)

Instructions for: [Azure Information Protection client for Windows](#)

## NOTE

To provide a unified and streamlined customer experience, [Azure Information Protection client \(classic\)](#) and [Label Management](#) in the Azure Portal are being [deprecated](#) as of **March 31, 2021**. This time-frame allows all current Azure Information Protection customers to transition to our unified labeling solution using the Microsoft Information Protection Unified Labeling platform. Learn more in the official [deprecation notice](#).

## NOTE

These instructions apply to the Azure Information Protection client (classic) and not the Azure Information Protection unified labeling client. Not sure of the difference between these clients? See this [FAQ](#).

If you are looking for information to configure different languages for sensitivity labels, use Office 365 Security & Compliance PowerShell and the *LocaleSettings* parameter for [Set-Label](#).

Although the default labels for Azure Information Protection support multiple languages, you must configure support for label names and descriptions that you specify. This configuration requires you to do the following:

1. Select the languages that your users use.
2. Export your current label names and descriptions to a file.
3. Edit the file to supply your translations.
4. Import the file back into your Azure Information Protection policy.

You can also configure templates for different languages when either of the following conditions apply. This configuration is appropriate if users or administrators need to see the current template name and description in their localized language.

- The template was created in the Azure classic portal or by using PowerShell, and the template is not linked to a label by using the **Select a predefined template** protection setting.
- You do not have a subscription that supports labels, so you can only create and manage templates in the Azure portal.

Select the languages that match your users' language setting for Office and Windows. These label names and descriptions then display in the Azure Information Protection bar in Office apps, and in the **Classify and protect - Azure Information Protection** dialog box, respectively. For more information about which language is chosen, see the [How the Azure Information Protection client determines the language to display](#) section on this page.

## To configure labels and templates for different languages

1. If you haven't already done so, open a new browser window and [sign in to the Azure portal](#). Then navigate to the **Azure Information Protection** pane.

For example, in the search box for resources, services, and docs: Start typing **Information** and select **Azure Information Protection**.

2. From the **Manage > Languages** menu option: On the **Azure Information Protection - Languages** pane, select **Add a new language for translation**. Select the languages that you want to add and then select **OK**. You can either type the name of the language in the search box, or scroll through the list of available languages

3. Your selected languages now display on the **Azure Information Protection - Languages** pane:

- To add another language, select **Add a new language for translation** and repeat the previous step.

### NOTE

Be sure to select the languages that your users have for Office, and for Windows. In some cases, this might require two different selections per computer.

- If you change your mind about any language that you have added, select that entry from the list, and then click **Remove**.

4. When all the languages you want to support are listed, select the check box next to **LANGUAGE NAME** to select all the entries (or alternatively, select individual entries), and then click **Export** to save a local copy of the existing label names and descriptions to a file.

The downloaded file is named **exported localization.zip** and is saved in your local Downloads folder. It can also be accessed by selecting this file name on the status bar of the Azure portal.

5. Extract the files from **exported localization.zip** so that you have .xml files for each language that you selected for download.

6. Edit each .xml file: For each string within `<LocalizedText>` tags, provide the translations that you want for each chosen language.

7. When you have edited each .xml file, create a new compressed (zipped) folder that contains these files. The compressed folder can have any name, but must have a .zip extension.

Tip: You don't have to wait until you've edited each language file that you've downloaded. Instead, you could roll out different languages in a phased manner, by including in the .zip file a subset of the total files you downloaded. Then repeat steps 7 and 8 when you have completed the translations for more languages.

8. Return to the **Azure Information Protection - Languages** pane, and select **Import**. Note that if this option is unavailable, first clear the check box for **LANGUAGE NAME** or the check boxes for the individually selected languages.

When the import completes, the localized names and descriptions download to users.

You must repeat this procedure if you need to support a new language, create new labels, or you change the name or description of labels in the Azure portal.

## How the Azure Information Protection client determines the language to display

When users download an Azure Information Protection policy that supports different languages, the language that users see for their label names and tooltips is determined by the following logic:

**For the labels and tooltips that users see on the Azure Information Protection bar in Office apps:**

- When there is a direct match for the language of their Office app, label names and descriptions display in that language.
- When there is no match for the language of their Office app, label names and descriptions display in the language you specified by default for all users. This language is typically English, which is the language used in the default policy.

**For the labels and tooltips that users see when they use right-click to classify and protect files or folders:**

- When there is a direct match for the language of their operating system, label names and descriptions display in that language.
- When there is no match for the language of their operating system, label names and descriptions display in the language you specified by default for all users. This language is typically English, which is the language used in the default policy.

## When localized label names are not used

In the following scenarios, localized label (and sublabel) names are not used. For consistency across your tenant, the default language is always used for the following:

- Client usage logs
- PowerShell (output from Get-AIPFileStatus)
- Document metadata and email headers

## Next steps

For more information about configuring the options that you can make for a label, and other settings for your Azure Information Protection policies, use the links in the [Configuring your organization's policy](#) section.

# How to migrate Azure Information Protection labels to unified sensitivity labels

7/20/2020 • 17 minutes to read • [Edit Online](#)

Applies to: [Azure Information Protection](#), [Office 365](#)

Instructions for: [Azure Information Protection client for Windows](#)

## NOTE

To provide a unified and streamlined customer experience, [Azure Information Protection client \(classic\)](#) and [Label Management](#) in the Azure Portal are being [deprecated](#) as of **March 31, 2021**. This time-frame allows all current Azure Information Protection customers to transition to our unified labeling solution using the Microsoft Information Protection Unified Labeling platform. Learn more in the official [deprecation notice](#).

Migrate Azure Information Protection labels to the unified labeling platform so that you can use them as sensitivity labels by [clients and services that support unified labeling](#).

## NOTE

If your Azure Information Protection subscription is fairly new, you might not need to migrate labels because your tenant is already on the unified labeling platform. For more information, see [How can I determine if my tenant is on the unified labeling platform?](#)

After you migrate your labels, you won't see any difference with the Azure Information Protection client (classic) because this client continues to download the labels with the Azure Information Protection policy from the Azure portal. However, you can now use the labels with the Azure Information Protection unified labeling client and other clients and services that use sensitivity labels.

Before you read the instructions to migrate your labels, you might find the following frequently asked questions useful:

- [What's the difference between labels in Azure Information Protection and labels in Office 365?](#)
- [When is the right time to migrate my labels?](#)
- [After I've migrated my labels, which management portal do I use?](#)

## Administrative roles that support the unified labeling platform

If you use admin roles for delegated administration in your organization, you might need to do some changes for the unified labeling platform:

The [Azure AD role](#) of [Azure Information Protection administrator](#) (formerly [Information Protection administrator](#)) is not supported by the unified labeling platform. If this administrative role is used in your organization to manage Azure Information Protection, add the users who have this role to the Azure AD roles of [Compliance administrator](#), [Compliance data administrator](#), or [Security administrator](#). If you need help with this step, see [Give users access to the Office 365 Security & Compliance Center](#). You can also assign these roles in the Azure AD portal, the Microsoft 365 security center, and the Microsoft 365 compliance center.

Alternatively to using roles, in the admin centers, you can create a new role group for these users and add either

**Sensitivity Label Administrator** or **Organization Configuration** roles to this group.

If you do not give these users access to the admin centers by using one of these configurations, they won't be able to configure Azure Information Protection in the Azure portal after your labels are migrated.

Global administrators for your tenant can continue to manage labels and policies in both the Azure portal and the admin centers after your labels are migrated.

## Before you begin

Label migration has many benefits but is irreversible, so make sure that you are aware of the following changes and considerations:

- Make sure that you have [clients that support unified labels](#) and if necessary, be prepared for administration in both the Azure portal (for clients that don't support unified labels) and the admin centers (for client that do support unified labels).
- Policies, including policy settings and who has access to them (scoped policies), and all advanced client settings are not migrated. Your options to configure these settings after your label migration include the following:
  - Your admin center for sensitivity labels.
  - [Office 365 Security & Compliance PowerShell](#), which you must use to configure [advanced client settings](#).
- Not all settings from a migrated label are supported by the admin centers. Use the table in the [Label settings that are not supported in the admin centers](#) section to help you identify these settings and the recommended course of action.
- Protection templates:
  - Templates that use a cloud-based key and that are part of a label configuration are also migrated with the label. Other protection templates are not migrated.
  - If you have labels that are configured for a predefined template, edit these labels and select the **Set permissions** option to configure the same protection settings that you had in your template. Labels with predefined templates will not block label migration but this label configuration is not supported in the admin centers.

Tip: To help you reconfigure these labels, you might find it useful to have two browser windows: One window in which you select the **Edit Template** button for the label to view the protection settings, and the other window to configure the same settings when you select **Set permissions**.

- After a label with cloud-based protection settings has been migrated, the resulting scope of the protection template is the scoped that is defined in the Azure portal (or by using the AIPService PowerShell module) and the scope that is defined in the admin centers.
- For each label, the Azure portal displays only the label display name, which you can edit. Users see this label name in their apps. The admin centers show both this display name for a label, and the label name. The label name is the initial name that you specify when the label is first created and this property is used by the back-end service for identification purposes. When you migrate your labels, the display name remains the same and the label name is renamed to the label ID from the Azure portal.
- Any localized strings for the labels are not migrated. Define new localized strings for the migrated labels by using Office 365 Security & Compliance PowerShell and the *LocaleSettings* parameter for [Set-Label](#).
- After the migration, when you edit a migrated label in the Azure portal, the same change is automatically reflected in the admin centers. However, when you edit a migrated label in one of the admin centers, you must return to the Azure portal, **Azure Information Protection - Unified labeling** pane, and select

**Publish.** This additional action is needed for the Azure Information Protection clients (classic) to pick up the label changes.

#### Label settings that are not supported in the admin centers

Use the following table to identify which configuration settings of a migrated label are not supported by the Office 365 Security & Compliance Center, the Microsoft 365 security center, or the Microsoft compliance center. If you have labels with these settings, when the migration is complete, use the administration guidance in the final column before you publish your labels in one of the referenced admin centers.

If you are not sure how your labels are configured, view their settings in the Azure portal. If you need help with this step, see [Configuring the Azure Information Protection policy](#).

Azure Information Protection clients (classic) can use all label settings listed without any problems because they continue to download the labels from the Azure portal.

| LABEL CONFIGURATION                                                                       | SUPPORTED BY UNIFIED LABELING CLIENTS | GUIDANCE FOR THE ADMIN CENTERS                                                                                                                                                                                            |
|-------------------------------------------------------------------------------------------|---------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Status of enabled or disabled<br><br>This status is not synchronized to the admin centers | Not applicable                        | The equivalent is whether the label is published or not.                                                                                                                                                                  |
| Label color that you select from list or specify by using RGB code                        | Yes                                   | No configuration option for label colors. Instead, you can configure label colors in the Azure portal or use <a href="#">PowerShell</a> .                                                                                 |
| Cloud-based protection or HYOK-based protection using a predefined template               | No                                    | No configuration option for predefined templates. We do not recommend you publish a label with this configuration.                                                                                                        |
| Cloud-based protection using user-defined permissions for Word, Excel, and PowerPoint     | Yes                                   | The admin centers now have a configuration option for user-defined permissions.<br><br>If you publish a label with this configuration, check the results of applying the label from the <a href="#">following table</a> . |
| HYOK-based protection using user-defined permissions for Outlook (Do Not Forward)         | No                                    | No configuration option for HYOK. We do not recommend you publish a label with this configuration. If you do, the results of applying the label are listed in the <a href="#">following table</a> .                       |

| LABEL CONFIGURATION                                                                                       | SUPPORTED BY UNIFIED LABELING CLIENTS | GUIDANCE FOR THE ADMIN CENTERS                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-----------------------------------------------------------------------------------------------------------|---------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Custom font size and custom font color by RGB code for visual markings (header, footer, watermark)        | Yes                                   | <p>Configuration for visual markings is limited to a list of colors and font sizes. You can publish this label without changes although you cannot see the configured values in the admin centers.</p> <p>To change these options, you can use the Azure portal. However, for easier administration, consider changing the color to one of the listed options in the admin centers.</p> <p>Font type <b>custom</b> (Arial, Courier and others) is not supported by the unified labeling client</p>                                                                                                                |
| Variables in visual markings (header, footer)                                                             | Yes                                   | If you publish this label without changes, variables display as text on clients rather than display the dynamic values. Before you publish the label, edit the strings to remove the variables.                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Visual markings per app                                                                                   | Yes                                   | If you publish this label without changes, the app variables display as text on clients in all apps rather than display your text strings on chosen apps. Publish this label only if it is suitable for all apps, and edit the strings to remove the app variables.                                                                                                                                                                                                                                                                                                                                               |
| "Just for me" protection                                                                                  | Yes                                   | <p>The admin centers do not let you save encryption settings that you apply now, without specifying any users. In the Azure portal, this configuration results in a label that applies "<a href="#">"Just for me" protection</a>".</p> <p>As an alternative, create a label that applies encryption and specify a user with any permissions, and then edit the associated protection template by using PowerShell. First, use the <a href="#">New-AipServiceRightsDefinition</a> cmdlet (see Example 3), and then <a href="#">Set-AipServiceTemplateProperty</a> with the <i>RightsDefinitions</i> parameter.</p> |
| Conditions and associated settings<br><br>Includes automatic and recommended labeling, and their tooltips | Not applicable                        | Reconfigure your conditions by using auto labeling as a separate configuration from label settings.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

### Comparing the behavior of protection settings for a label

Use the following table to identify how the same protection setting for a label behaves differently, depending on whether it's used by the Azure Information Protection client (classic), the Azure Information Protection unified labeling client, or by Office apps that have labeling built in (also known as "native Office labeling"). The differences in label behavior might change your decision whether to publish the labels, especially when you have a mix of

clients in your organization.

If you are not sure how your protection settings are configured, view their settings in the **Protection** pane, in the Azure portal. If you need help with this step, see [To configure a label for protection settings](#).

Protection settings that behave the same way are not listed in the table, with the following exceptions:

- When you use Office apps with built-in labeling, labels are not visible in File Explorer unless you also install the Azure Information Protection unified labeling client.
- When you use Office apps with built-in labeling, if protection was previously applied independently from a label, that protection is preserved [1].

| PROTECTION SETTING FOR A LABEL                                                                  | AZURE INFORMATION PROTECTION CLIENT (CLASSIC)                                                                                                                                                                                                            | AZURE INFORMATION PROTECTION UNIFIED LABELING CLIENT                                                                                                                                                                                                                                                                                                                 | OFFICE APPS WITH BUILT-IN LABELING                                                                                                                                                                                                                                                                                                                        |
|-------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Azure (cloud key) with user-defined permissions for Word, Excel, PowerPoint, and File Explorer: | <p>Visible in Word, Excel, PowerPoint, and File Explorer</p> <p>When the label is applied:</p> <ul style="list-style-type: none"> <li>- Users are prompted for custom permissions that are then applied as protection using a cloud-based key</li> </ul> | <p>Visible in Word, Excel, PowerPoint, and File Explorer</p> <p>When the label is applied:</p> <ul style="list-style-type: none"> <li>- Users are prompted for custom permissions that are then applied as protection using a cloud-based key</li> </ul>                                                                                                             | <p>Visible in Word, Excel, PowerPoint, and Outlook:</p> <p>When the label is applied:</p> <ul style="list-style-type: none"> <li>- Users are not prompted for custom permissions and no protection is applied</li> <li>- If protection was previously applied independently from a label, that protection is preserved [1]</li> </ul>                     |
| HYOK (AD RMS) with a template:                                                                  | <p>Visible in Word, Excel, PowerPoint, Outlook, and File Explorer</p> <p>When this label is applied:</p> <ul style="list-style-type: none"> <li>- HYOK protection is applied to documents and emails</li> </ul>                                          | <p>Visible in Word, Excel, PowerPoint, Outlook, and File Explorer</p> <p>When this label is applied:</p> <ul style="list-style-type: none"> <li>- No protection is applied and protection is removed [2] if it was previously applied by a label</li> <li>- If protection was previously applied independently from a label, that protection is preserved</li> </ul> | <p>Visible in Word, Excel, PowerPoint, and Outlook</p> <p>When this label is applied:</p> <ul style="list-style-type: none"> <li>- No protection is applied and protection is removed [2] if it was previously applied by a label</li> <li>- If protection was previously applied independently from a label, that protection is preserved [1]</li> </ul> |
| HYOK (AD RMS) with user-defined permissions for Word, Excel, PowerPoint, and File Explorer:     | <p>Visible in Word, Excel, PowerPoint, and File Explorer</p> <p>When this label is applied:</p> <ul style="list-style-type: none"> <li>- HYOK protection is applied to documents and emails</li> </ul>                                                   | <p>Visible in Word, Excel, and PowerPoint</p> <p>When this label is applied:</p> <ul style="list-style-type: none"> <li>- Protection is not applied and protection is removed [2] if it was previously applied by a label</li> <li>- If protection was previously applied independently from a label, that protection is preserved</li> </ul>                        | <p>Visible in Word, Excel, and PowerPoint</p> <p>When this label is applied:</p> <ul style="list-style-type: none"> <li>- Protection is not applied and protection is removed [2] if it was previously applied by a label</li> <li>- If protection was previously applied independently from a label, that protection is preserved</li> </ul>             |

| PROTECTION SETTING FOR A LABEL                           | AZURE INFORMATION PROTECTION CLIENT (CLASSIC)                                                                                                                              | AZURE INFORMATION PROTECTION UNIFIED LABELING CLIENT                                                                                                                                                                                                                                                        | OFFICE APPS WITH BUILT-IN LABELING                                                                                                                                                                                                                                                                              |
|----------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| HYOK (AD RMS) with user-defined permissions for Outlook: | <p>Visible in Outlook</p> <p>When this label is applied:</p> <ul style="list-style-type: none"> <li>- Do Not Forward using HYOK protection is applied to emails</li> </ul> | <p>Visible in Outlook</p> <p>When this label is applied:</p> <ul style="list-style-type: none"> <li>- Protection is not applied and removed [2] if it was previously applied by a label</li> <li>- If protection was previously applied independently from a label, that protection is preserved</li> </ul> | <p>Visible in Outlook</p> <p>When this label is applied:</p> <ul style="list-style-type: none"> <li>- Protection is not applied and removed [2] if it was previously applied by a label</li> <li>- If protection was previously applied independently from a label, that protection is preserved [1]</li> </ul> |

Footnote 1

In Outlook, protection is preserved with one exception: When an email has been protected with the Encrypt-Only option, that protection is removed.

Footnote 2

Protection is removed if the user has a usage right or role that supports this action:

- The [usage right](#) Export or Full Control.
- The role of [Rights Management issuer](#) or [Rights Management owner](#), or [super user](#).

If the user doesn't have one of these usage rights or roles, the label is not applied and the original protection is preserved.

## To migrate Azure Information Protection labels

Use the following instructions to migrate your tenant and Azure Information Protection labels to use the unified labeling store.

You must be a Compliance administrator, Compliance data administrator, Security administrator, or Global administrator to migrate your labels.

1. If you haven't already done so, open a new browser window and [sign in to the Azure portal](#). Then navigate to the **Azure Information Protection** pane.

For example, in the search box for resources, services, and docs: Start typing **Information** and select **Azure Information Protection**.

2. From the **Manage** menu option, select **Unified labeling**.
3. On the **Azure Information Protection - Unified labeling** pane, select **Activate** and follow the online instructions.

If the option to activate is not available, check the **Unified labeling status**: If you see **Activated**, your tenant is already using the unified labeling store and there is no need to migrate your labels.

For the labels that successfully migrated, they can now be used by [clients and services that support unified labeling](#). However, you must first [publish these labels](#) in one of the admin centers: Office 365 Security & Compliance Center, Microsoft 365 security center, or Microsoft 365 compliance center.

## IMPORTANT

If you edit the labels outside the Azure portal, for Azure Information Protection clients (classic), return to this [Azure Information Protection - Unified labeling pane](#), and select **Publish**.

## Copy policies

### NOTE

This option is in preview and subject to change.

After you have migrated your labels, you can select an option to copy policies. If you select this option, a one-time copy of your policies with their [policy settings](#) and any [advanced client settings](#) is sent to the admin center where you manage your labels: Office 365 Security & Compliance Center, Microsoft 365 security center, Microsoft 365 compliance center.

Successfully copied policies with their settings and labels are then automatically published to the users and groups that were assigned to the policies in the Azure portal. Note that for the Global policy, this means all users. If you're not ready for the migrated labels in the copied policies to be published, after the policies are copied, you can remove the labels from the label policies in your admin labeling center.

Before you select the **Copy policies (preview)** option on the [Azure Information Protection - Unified labeling pane](#), be aware of the following:

- The **Copy policies (Preview)** option is not available until unified labeling is activated for your tenant.
- You cannot selectively choose policies and settings to copy. All policies (the **Global** policy and any scoped policies) are automatically selected to be copied, and all settings that are supported as label policy settings are copied. If you already have a label policy with the same name, it will be overwritten with the policy settings in the Azure portal.
- Some advanced client settings are not copied because for the Azure Information Protection unified labeling client, these are supported as *label advanced settings* rather than policy settings. You can configure these label advanced settings with [Office 365 Security & Compliance Center PowerShell](#). The advanced client settings that are not copied:
  - [LabelbyCustomProperty](#)
  - [LabelToSMIME](#)
- Unlike label migration where subsequent changes to labels are synchronized, the **Copy policies** action doesn't synchronize any subsequent changes to your policies or policy settings. You can repeat the copy policy action after making changes in the Azure portal, and any existing policies and their settings will be overwritten again. Or, use the Set-LabelPolicy or Set-Label cmdlets with the *AdvancedSettings* parameter from Office 365 Security & Compliance Center PowerShell.
- The **Copy policies** action verifies the following for each policy before it is copied:
  - Users and groups assigned to the policy are currently in Azure AD. If one or more account is missing, the policy is not copied. Group membership is not checked.
  - The Global policy contains at least one label. Because the admin labeling centers don't support label policies without labels, a Global policy without labels is not copied.
- If you copy policies and then delete them from your admin labeling center, wait at least two hours before you use the **Copy policies** action again to ensure sufficient time for the deletion to replicate.
- Policies copied from Azure Information Protection will not have the same name, they will instead be named

with a prefix of **AIP\_**. Policy names cannot be subsequently changed.

For more information about configuring the policy settings, advanced client settings, and label settings for the Azure Information Protection unified labeling client, see [Custom configurations for the Azure Information Protection unified labeling client](#) from the admin guide.

## Clients and services that support unified labeling

To confirm whether the clients and services you use support unified labeling, refer to their documentation to check whether they can use sensitivity labels that are published from one of the admin centers: Office 365 Security & Compliance Center, Microsoft 365 security center, or Microsoft 365 compliance center.

**Clients that currently support unified labeling include:**

- The [Azure Information Protection unified labeling client for Windows](#). For a comparison of this client with the Azure Information Protection client (classic), see [Compare the labeling clients for Windows computers](#).
- Apps from Office that are in different stages of availability. For more information, see [Support for sensitivity label capabilities in apps](#) from the Microsoft 365 Compliance documentation.
- Apps from software vendors and developers that use the [Microsoft Information Protection SDK](#).

**Services that currently support unified labeling include:**

- [Power BI \(in preview\)](#)
- Office Online (in preview) and Outlook on the web
- Microsoft SharePoint, OneDrive for work or school, OneDrive for home, Teams, and Office 365 groups (in preview)

For more information, see [Use sensitivity labels with Microsoft Teams, Office 365 groups, and SharePoint sites \(public preview\)](#) and [Enable sensitivity labels for Office files in SharePoint and OneDrive](#).

- Microsoft Defender Advanced Threat Protection
- Microsoft Cloud App Security

This service supports labels both before the migration to the unified labeling store, and after the migration, using the following logic:

- If the admin centers have sensitivity labels, these labels are retrieved from the admin centers. To select these labels in Cloud App Security, at least one label must be published to at least one user.
  - If the admin centers don't have sensitivity labels, Azure Information Protection labels are retrieved from the Azure portal.
- Services from software vendors and developers that use the [Microsoft Information Protection SDK](#).

## Next steps

For additional guidance and tips from our Customer Experience team, see the following resources:

- Blog post: [Understanding Unified Labeling Migration](#)
- Webinar: [Unified labeling recording, deck, and FAQs](#)

For more information about your migrated labels that can now be configured and published in one of the labeling admin centers, see [Learn about sensitivity labels](#) and [Create and configure sensitivity labels and their policies](#).

If you haven't already done so, install the Azure Information Protection unified labeling client. For release information, an admin guide, and user guide, see [Azure Information Protection unified labeling client for Windows](#).

# Configuring secure document collaboration by using Azure Information Protection

3/16/2020 • 7 minutes to read • [Edit Online](#)

Applies to: [Azure Information Protection](#), [Office 365](#)

## NOTE

To provide a unified and streamlined customer experience, **Azure Information Protection client (classic)** and **Label Management** in the Azure Portal are being **deprecated** as of March 31, 2021. This time-frame allows all current Azure Information Protection customers to transition to our unified labeling solution using the Microsoft Information Protection Unified Labeling platform. Learn more in the official [deprecation notice](#).

When you use Azure Information Protection, you can protect your documents without sacrificing collaboration for authorized users. The majority of documents that one user creates and then shares with others to view and edit will be Office documents from Word, Excel, and PowerPoint. These documents support native protection, which means that in addition to the protection features of authorization and encryption, they also support restricted permission for more fine-grained control.

These permissions are called usage rights, and include permissions such as view, edit, print. You can define individual usage rights when a document is protected, or you can define a grouping of usage rights, called permission levels. Permission levels make it easier to select usage rights that are typically used together, for example, Reviewer and Co-Author. For more information about usage rights and permission levels, see [Configuring usage rights for Azure Information Protection](#).

When you configure these permissions, you can specify which users they are for:

- **For users in your own organization or another organization that uses Azure Active Directory:** You can specify Azure AD user accounts, Azure AD groups, or all users in that organization.
- **For users who do not have an Azure Active Directory account:** Specify an email address that will be used with a Microsoft account. This account can already exist, or users can create it at the time they open the protected document.

To open documents with a Microsoft account, users must use Office 365 apps (Click-to-Run). Other Office editions and versions do not yet support opening Office protected documents with a Microsoft account.

- **For any authenticated user:** This option is suitable for when you don't need to control who accesses the protected document, providing the user can be authenticated. The authentication can be by Azure AD, by using a Microsoft account, or even a federated social provider or one-time passcode when the content is protected by the new capabilities of Office 365 Message Encryption.

As an administrator, you can configure an Azure Information Protection label to apply the permissions and authorized users. This configuration makes it very easy for users and other administrators to apply the correct protection settings, because they simply apply the label without having to specify any details. The following sections provide an example walk through to protect a document that supports secure collaboration with internal and external users.

## Example configuration for a label to apply protection to support

## internal and external collaboration

This example walks through configuring an existing label to apply protection so that users from your organization can collaborate on documents with all users from another organization that has Office 365 or Azure AD, a group from a different organization that has Office 365 or Azure AD, and a user who doesn't have an account in Azure AD and instead will use their Gmail email address.

Because the scenario restricts access to specific people, it does not include the setting for any authenticated users. For an example of how you can configure a label with this setting, see [Example 5: Label that encrypts content but doesn't restrict who can access it](#).

1. Select your label that's already in the global policy or a scoped policy. On the **Protection** pane, make sure **Azure (cloud key)** is selected.
2. Make sure **Set permissions** is selected, and select **Add permissions**.
3. On the **Add permissions** pane:
  - For your internal group: Select **Browse directory** to select the group, which must be email-enabled.
  - For all users in the first external organization: Select **Enter details** and type the name of a domain in the organization's tenant. For example, fabrikam.com.
  - For the group in the second external organization: Still on the **Enter details** tab, type the email address of the group in the organization's tenant. For example, sales@contoso.com.
  - For the user who doesn't have an Azure AD account: Still on the **Enter details** tab, type the user's email address. For example, bengi.turan@gmail.com.
4. To grant the same permissions to all these users: For **Choose permissions from preset**, select **Co-Owner, Co-Author, Reviewer, or Custom** to select the permissions that you want to grant.

For example, your configured permissions might look similar to the following:

**Protection settings** ⓘ

**Azure (cloud key)** **HYOK (AD RMS)**

Select the protection action type ⓘ

Set permissions  
 Set user-defined permissions (Preview)

| USERS                  | PERMISSIONS | ... |
|------------------------|-------------|-----|
| azureaip101@gmail.com  | Reviewer    | ... |
| fabrikam.com           | Reviewer    | ... |
| sales@contoso.com      | Reviewer    | ... |
| sales@vanarsdelltd.com | Reviewer    | ... |

[+ Add permissions](#)

5. Click **OK** on the **Add permissions** pane.
6. On the **Protection** pane, click **OK**.
7. On the **Label** pane, select **Save**.

## Applying the label that supports secure collaboration

Now that this label is configured, it can be applied to documents in a number of ways that include the following:

| DIFFERENT WAYS TO APPLY THE LABEL                                                                                                                                      | MORE INFORMATION                                                                                                                                                                                       |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| A user manually selects the label when the document is created in their Office application.                                                                            | Users select the label from the <b>Protect</b> button on the Office ribbon, or from the Azure Information Protection bar.                                                                              |
| Users are prompted to select a label when a new document is saved.                                                                                                     | You've configured the Azure Information Protection <a href="#">policy setting</a> named <b>All documents and emails must have a label</b> .                                                            |
| A user shares the document by email and manually selects the label in Outlook.                                                                                         | Users select the label from the <b>Protect</b> button on the Office ribbon, or from the Azure Information Protection bar, and the attached document is automatically protected with the same settings. |
| An administrator applies the label to the document by using PowerShell.                                                                                                | Use the <a href="#">Set-AIPFileLabel</a> cmdlet to apply the label to a specific document or all documents in a folder.                                                                                |
| You have additionally configured the label to apply automatic classification that can now be applied by using the Azure Information Protection scanner, or PowerShell. | See <a href="#">How to configure conditions for automatic and recommended classification for Azure Information Protection</a> .                                                                        |

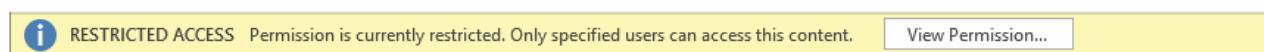
To complete this walkthrough, manually apply the label when you create the document in your Office application:

1. On a client computer, if you already have your Office application open, first close and reopen it to get the latest policy changes that include your newly configured label.
2. Apply the label to a document, and save it.

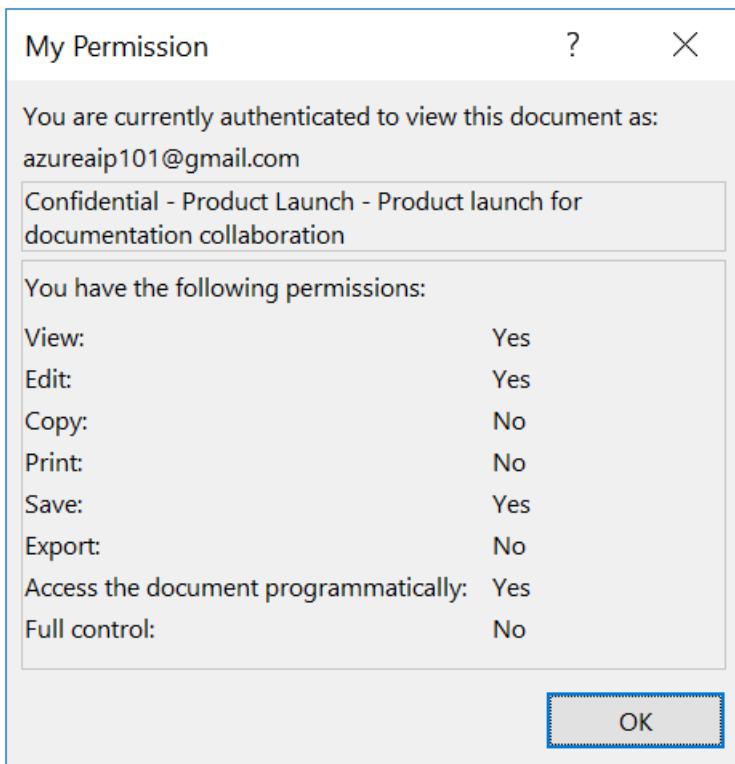
Share the protected document by attaching it to an email, and send it to the people you authorized to edit the document.

## Opening and editing the protected document

When users that you authorized open the document for editing, the document opens with an information banner that informs them that permissions are restricted. For example:



If they select the **View Permission** button, they see the permissions that they have. In the following example, the user can view and edit the document:



Note: If the document is opened by external users who are also using Azure Information Protection, the Office application does not display your classification label for the document, although any visual markings from the label remain. Instead, external users can apply their own label in line with their organization's classification taxonomy. If these external users then send back the edited document to you, Office displays your original classification label when you reopen the document.

Before the protected document opens, one of the following authentication flows happen:

- For the users who have an Azure AD account, they use their Azure AD credentials to be authenticated by Azure AD, and the document opens.
- For the user who doesn't have an Azure AD account, if they are not signed in to Office with an account that has permissions to open the document, they see the **Accounts** page.

On the **Accounts** page, select **Add Account**:

The screenshot shows the 'Accounts' page in Microsoft Office. At the top, there's a 'Switch Account' link and a 'Sign out' link. Below that, it says 'Current Account'. There's a placeholder card with a user icon and a blacked-out email address ending in '@.com'. At the bottom, there's a button labeled 'Add Account' with a plus sign, and a sub-instruction 'Click to sign in a new account into Office'.

On the **Sign in** page, select **Create one!** and follow the prompts to create a new Microsoft account with the email address that was used to grant the permissions:

The screenshot shows the Microsoft 'Sign in' page. It has the Microsoft logo, a 'Sign in' button, an input field for 'Email, phone, or Skype', and a 'Create one!' button which is highlighted with an orange border. At the bottom right is a 'Next' button, and at the bottom left is a copyright notice: '©2018 Microsoft Privacy statement'.

When the new Microsoft account is created, the local account switches to this new Microsoft account and the user can then open the document.

## Supported scenarios for opening protected documents

The following table summarizes the different authentication methods that are supported for viewing and editing protected documents.

In addition, the following scenarios support viewing documents:

- The Azure Information Protection viewer for Windows, and for iOS and Android can open files by using a Microsoft account.
- A browser can open protected attachments when social providers and one-time passcodes are used for authentication with Exchange Online and the new capabilities from Office 365 Message Encryption.

| PLATFORMS FOR VIEWING AND EDITING DOCUMENTS:<br>WORD, EXCEL, POWERPOINT | AUTHENTICATION METHOD:<br>AZURE AD | AUTHENTICATION METHOD:<br>MICROSOFT ACCOUNT |
|-------------------------------------------------------------------------|------------------------------------|---------------------------------------------|
| Windows                                                                 | Yes [1]                            | Yes [2]                                     |
| iOS                                                                     | Yes [1]                            | No                                          |
| Android                                                                 | Yes [1]                            | No                                          |
| MacOS                                                                   | Yes [1]                            | No                                          |

Footnote 1

Supports user accounts, email-enabled groups, all members. User accounts and email-enabled groups can include guest accounts. All members exclude guest accounts.

Footnote 2

Currently supported by Office 365 apps (Click-to-Run) only.

## Next steps

See other [example configurations](#) for labels to apply protection for common scenarios. This article also contains more details about the protection settings.

For more information about the other options and settings that you can configure for your label, see [Configuring Azure Information Protection policy](#).

The label that was configured in this article also creates a protection template by the same name. If you have applications and services that integrate with protection templates from Azure Information Protection, they can apply this template. For example, DLP solutions and mail flow rules. Outlook on the web automatically displays protection templates from the Azure Information Protection global policy.

# Configuring Exchange Online mail flow rules for Azure Information Protection labels

3/16/2020 • 4 minutes to read • [Edit Online](#)

Applies to: [Azure Information Protection](#), [Office 365](#)

## NOTE

To provide a unified and streamlined customer experience, **Azure Information Protection client (classic)** and **Label Management** in the Azure Portal are being **deprecated** as of March 31, 2021. This time-frame allows all current Azure Information Protection customers to transition to our unified labeling solution using the Microsoft Information Protection Unified Labeling platform. Learn more in the official [deprecation notice](#).

Use the following information to help you configure mail flow rules in Exchange Online to use Azure Information Protection labels, and to apply additional protection for specific scenarios. For example:

- Your default label is **General**, which does not apply protection. For emails with this label that are sent externally, apply the additional Do Not Forward protection action.
- If an attachment with a **Confidential \ Partners** label is emailed to people outside the organization and the email is not protected, apply the additional Encrypt-Only protection action.

Mail flow rules that apply protection as an action are ignored if the email is already protected. For example, an email message that has been protected by Do Not Forward cannot be changed by an Exchange mail flow rule to use the Encrypt-Only option.

You can extend these examples as well as modify them. For example, add more conditions. For more information about configuring mail flow rules, see [Mail flow rules \(transport rules\) in Exchange Online](#) from the Exchange Online documentation.

For more information about configuring mail flow rules to encrypt email messages, see [Define mail flow rules to encrypt email messages in Office 365](#) from the Office documentation.

## Prerequisite: Know your label GUID

Because an Azure Information Protection label is stored in metadata, mail flow rules in Exchange Online can read this information for messages and Office document attachments. Mail flow rules do not support inspecting the metadata for PDF documents.

Before you configure mail flow rules to identify messages and documents that are labeled, make sure that you know the GUID of the Azure Information Protection label that you want to use.

For more information about the metadata stored by a label and how to identify label GUIDs, see [Label information stored in emails and documents](#).

## Example configurations

For the following examples, create a new mail flow rule by using the following steps:

1. In a web browser, using a work or school account that has been granted global administrator permissions, sign in to Office 365.

2. Choose the **Admin** tile.
3. In the Microsoft 365 admin center, choose **Admin centers > Exchange**.
4. In the Exchange admin center: **mail flow > rules > + > Create a new rule**.

**TIP**

If you have problems with the user interface when you configure your rules, try a different browser, such as Internet Explorer.

The examples have a single condition that applies protection when an email is sent outside the organization. For more information about other conditions that you can select, see [Mail flow rule conditions and exceptions \(predicates\) in Exchange Online](#).

**Example 1: Rule that applies the Do Not Forward option to emails that are labeled General when they are sent outside the organization**

In this example, the **General** label has a GUID of 0e421e6d-ea17-4fdb-8f01-93a3e71333b8. Substitute your own label or sublabel GUID that you want to use with this rule.

In the Azure Information Protection policy, this label has been configured as the default label to classify emails as **General** and the label does not apply protection.

1. In **Name**, type a name for the rule, such as `Apply Do Not Forward for General emails sent externally`.

2. For **Apply this rule if:** Select **The recipient is located**, select **Outside the organization**, and then select **OK**.

3. Select **More options**, and then select **add condition**.

4. For **and**: Select **A message header**, and then select **includes any of these words**:

a. Select **Enter text**, and enter `msip_labels`.

b. Select **Enter words**, and enter `MSIP_Label_0e421e6d-ea17-4fdb-8f01-93a3e71333b8_Enabled=True`

c. Select **+**, and then select **OK**.

5. For **Do the following:** Select **Modify the message security > Apply Office 365 Message Encryption and rights protection > Do Not Forward**, and then select **OK**.

Your rule configuration should now look similar to the following:

The screenshot shows the 'Create a new rule' wizard. Under 'If...', there are two conditions: 'The recipient is located' set to 'Outside the organization' and 'A message header includes' set to '`msip_labels`' with the value '`MSIP_Label_0e421e6d-ea17-4fdb-8f01-93a3e71333b8_Enabled=True`'. Under 'Do the following...', there is one action: 'Apply Office 365 Message Encryption and rights protection to the message with...' set to 'Do Not Forward'.

6. Select **Save**

For more information about the Do Not Forward option, see [Do Not Forward option for emails](#).

**Example 2: Rule that applies the Encrypt-Only option to emails when they have attachments that are labeled Confidential \ Partners and these emails are sent outside the organization**

In this example, the **Confidential \ Partners** sublabel has a GUID of 0e421e6d-ea17-4fdb-8f01-93a3e71333b8. Substitute your own label or sublabel GUID that you want to use with this rule.

This label is used to classify and protect documents that you use for partner collaboration.

1. In **Name**, type a name for the rule, such as `Apply Encrypt to emails sent externally if protected attachments`.
2. For **Apply this rule if:** Select **The recipient is located**, select **Outside the organization**, and then select **OK**.
3. Select **More options**, and then select **add condition**.
4. For **and**: Select **Any attachment**, and then select **has these properties, including any of these words**:
  - a. Select + > **Specify a custom attachment property**.
  - b. For **Property**, enter `MSIP_Label_0e421e6d-ea17-4fdb-8f01-93a3e71333b8_Enabled`.
  - c. For **Value**, enter `True`
  - d. Select **Save**, and then select **OK**.
5. For **Do the following:** Select **Modify the message security** > **Apply Office 365 Message Encryption and rights protection** > **Encrypt**, and then select **OK**.

Your rule configuration should now look similar to the following:

The screenshot shows the Exchange Online mail flow rule configuration interface. It includes sections for 'Apply this rule if...' and 'Do the following...'. Under 'Apply this rule if...', there are two conditions: 'The recipient is located...' set to 'Outside the organization' and 'has these properties, including any of these words' set to 'MSIP\_Label\_0e421e6d-ea17-4fdb-8f01-93a3e71333b8\_Enabled:True'. An 'add condition' button is visible. Under 'Do the following...', there is one action: 'Apply Office 365 Message Encryption and rights protection to the message with...' set to 'Encrypt', with an 'add action' button below it.

6. Select **Save**

For more information about the **Encrypt** option, see [Encrypt-Only option for emails](#).

## Next steps

For information about creating and configuring the labels to use with Exchange Online mail flow rules, see [Configuring Azure Information Protection policy](#).

In addition, to help classify email messages that contain attachments, consider using the following Azure Information Protection **policy setting**: **For email messages with attachments, apply a label that matches the highest classification of those attachments**.

# What is the Azure Information Protection unified labeling scanner?

7/20/2020 • 5 minutes to read • [Edit Online](#)

*Applies to: Azure Information Protection, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2*

## NOTE

If you're using the classic scanner, see [What is the Azure Information Protection classic scanner?](#).

To scan and label files on cloud repositories, use [Cloud App Security](#) instead of the scanner.

Use the information in this section to learn about the Azure Information Protection unified labeling scanner, and then how to successfully install, configure, run and if necessary, troubleshoot it.

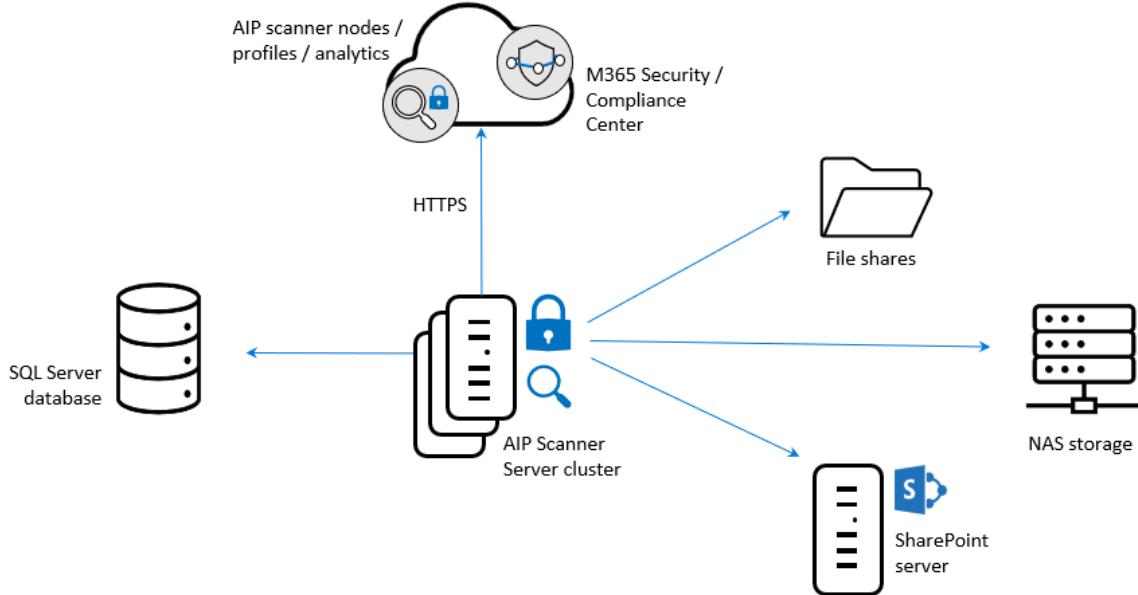
The AIP scanner runs as a service on Windows Server and lets you discover, classify, and protect files on the following data stores:

- **UNC paths** for network shares that use the Server Message Block (SMB) protocol.
- **SharePoint document libraries and folder** for SharePoint Server 2019 through SharePoint Server 2013. SharePoint 2010 is also supported for customers who have [extended support for this version of SharePoint](#).

## Azure Information Protection unified labeling scanner overview

The AIP scanner can inspect any files that Windows can index. If you've configured labels that apply automatic classification, the scanner can label discovered files to apply that classification, and optionally apply or remove protection.

The following image shows the AIP scanner architecture, where the scanner discovers files across your on-premises and SharePoint servers.



To inspect your files, the scanner uses IFilters installed on the computer. To determine whether the files need labeling, the scanner uses the Office 365 built-in data loss prevention (DLP) sensitivity information types and pattern detection, or Office 365 regex patterns.

The scanner uses the Azure Information Protection client, and can classify and protect the same types of files as the client. For more information, see [File types supported by the Azure Information Protection unified labeling client](#).

Do any of the following to configure your scans as needed:

- Run the scanner in **discovery mode only** to create reports that check to see what happens when your files are labeled.
- Run the scanner to discover files with **sensitive information**, without configuring labels that apply automatic classification.
- Run the scanner **automatically** to apply labels as configured.
- Define a **file types list** to specify specific files to scan or to exclude.

#### **NOTE**

The scanner does not discover and label in real time. It systematically crawls through files on data stores that you specify. Configure this cycle to run once, or repeatedly.

#### **TIP**

The unified labeling scanner supports scanner clusters with multiple nodes, enabling your organization to scale out, achieving faster scan times and broader scope.

Deploy multiple nodes right from the start, or start with a single-node cluster and add additional nodes later on as you grow. Deploy multiple nodes by using the same cluster name and database for the `Install-AIPScanner` cmdlet.

## AIP scanning process

When scanning files, the AIP scanner runs through the following steps:

1. Determine whether files are included or excluded for scanning

## 2. Inspect and label files

### 3. Label files that can't be inspected

For more information, see [Files not labeled by the scanner](#).

#### 1. Determine whether files are included or excluded for scanning

The scanner automatically skips files that are excluded from classification and protection, such as executable files and system files. For more information, see [File types that are excluded from classification and protection](#).

The scanner also considers any file lists explicitly defined to scan, or exclude from scanning. File lists apply for all data repositories by default, and can also be defined for specific repositories only.

To define file lists for scanning or exclusion, use the **File types to scan** setting in the content scan job. For example:

##### Configure file settings

Preserve "Date modified", "Last modified" and "Modified by" [i](#)

Off  On

File types to scan [i](#)

Include  Exclude

.lnk,.exe,.com,.cmd,.bat,.dll,.ini,.pst,.sca,.drm,.sys,.cpl,.inf,.drv,.dat,.tmp,.msp,.msi,.pdb,.jar,.ocx,.rtf,.rar,.msg

Default owner [i](#)

Scanner Account  Custom

For more information, see [Deploying the Azure Information Protection scanner to automatically classify and protect files](#).

## 2. Inspect and label files

After identifying excluded files, the scanner filters again to identify files supported for inspection.

These additional filters are the same ones used by the operating system for Windows Search and indexing, and require no additional configuration. Windows IFilter is also used to scan file types that are used by Word, Excel, and PowerPoint, and for PDF documents and text files.

For a full list of file types supported for inspection, and additional instructions for configuring filters to include .zip and .tiff files, see [File types supported for inspection](#).

After inspection, supported file types are labeled using the conditions specified for your labels. If you're using discovery mode, these files can either be reported to contain the conditions specified for your labels, or reported to contain any known sensitive information types.

### 3. Label files that can't be inspected

For any file types that can't be inspected, the AIP scanner applies the default label in the Azure Information Protection policy, or the default label configured for the scanner.

#### Files not labeled by the scanner

The AIP scanner cannot label files under the following circumstances:

- When the label applies classification, but not protection, and the file type does not support classification-only by the client. For more information, see [Unified labeling client file types](#).
- When the label applies classification and protection, but the scanner does not support the file type.

By default, the scanner protects only Office file types, and PDF files when they are protected by using the ISO standard for PDF encryption.

Other types of files can be added for protection when you [change the types of files to protect](#).

**Example:** After inspecting .txt files, the scanner can't apply a label that's configured for classification only, because the .txt file type doesn't support classification only.

However, if the label is configured for both classification and protection, and the .txt file type is included for the scanner to protect, the scanner can label the file.

## Next steps

For more information about deploying the scanner, see the following articles:

- [AIP scanner deployment prerequisites](#)
- [Configuring and installing the AIP scanner](#)
- [Running scans using the AIP scanner](#)

### More information:

- Interested in how the Core Services Engineering and Operations team in Microsoft implemented this scanner? Read the technical case study: [Automating data protection with Azure Information Protection scanner](#).
- You might be wondering: [What's the difference between Windows Server FCI and the Azure Information Protection scanner?](#)
- You can also use PowerShell to interactively classify and protect files from your desktop computer. For more information about this and other scenarios that use PowerShell, see [Using PowerShell with the Azure Information Protection unified labeling client](#).

# Prerequisites for installing and deploying the Azure Information Protection unified labeling scanner

7/20/2020 • 11 minutes to read • [Edit Online](#)

Applies to: [Azure Information Protection](#), Windows Server 2019, Windows Server 2016, Windows Server 2012 R2

## NOTE

If you're working with the classic scanner, see [Prerequisites for installing and deploying the Azure Information Protection classic scanner](#).

Before you install the Azure Information Protection scanner, make sure that your system complies with the following requirements:

- [Windows Server requirements](#)
- [Service account requirements](#)
- [SQL server requirements](#)
- [Azure Information Protection client requirements](#)
- [Label configuration requirements](#)
- [SharePoint requirements](#)
- [Microsoft Office requirements](#)
- [File path requirements](#)
- [Usage statistics requirements](#)

If you can't meet all the requirements in the table because they are prohibited by your organization policies, see the [alternative configurations](#) section.

When deploying the scanner in production or testing the performance for multiple scanners, see [Storage requirements and capacity planning for SQL Server](#).

When you're ready to start installing and deploying your scanner, continue with [Deploying the Azure Information Protection scanner to automatically classify and protect files](#).

## Windows Server requirements

You must have a Windows Server computer to run the scanner, which has the following system specifications:

| SPECIFICATION | DETAILS           |
|---------------|-------------------|
| Processor     | 4 core processors |
| RAM           | 8 GB              |

| SPECIFICATION        | DETAILS                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Disk space           | <p>10 GB free space (average) for temporary files. The scanner requires sufficient disk space to create temporary files for each file that it scans, four files per core.</p> <p>The recommended disk space of 10 GB allows for 4 core processors scanning 16 files that each have a file size of 625 MB.</p>                                                                                                                                                                                                                                                                                                                                                                                                          |
| Operating system     | <ul style="list-style-type: none"> <li>- Windows Server 2019</li> <li>- Windows Server 2016</li> <li>- Windows Server 2012 R2</li> </ul> <p><b>Note:</b> For testing or evaluation purposes in a non-production environment, you can also use any Windows operating system that is <a href="#">supported by the Azure Information Protection client</a>.</p>                                                                                                                                                                                                                                                                                                                                                           |
| Network connectivity | <p>Your scanner computer can be a physical or virtual computer with a fast and reliable network connection to the data stores to be scanned.</p> <p>If internet connectivity is not possible because of your organization policies, see <a href="#">Deploying the scanner with alternative configurations</a>.</p> <p>Otherwise, make sure that this computer has internet connectivity that allows the following URLs over HTTPS (port 443):</p> <ul style="list-style-type: none"> <li>- *.aadrm.com</li> <li>- *.azurerms.com</li> <li>- *.informationprotection.azure.com</li> <li>- informationprotection.hosting.portal.azure.net</li> <li>- *.aria.microsoft.com</li> <li>- *.protection.outlook.com</li> </ul> |
|                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

## Service account requirements

You must have a service account to run the scanner service on the Windows Server computer, as well as authenticate to Azure AD and download the Azure Information Protection Policy.

Your service account must be an Active Directory account and synchronized to Azure AD.

If you cannot synchronize this account because of your organization policies, see [Deploying the scanner with alternative configurations](#).

This service account has the following requirements:

| REQUIREMENT | DETAILS |
|-------------|---------|
|             |         |

| Requirement                                           | Details                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Log on locally</b> user right assignment           | <p>Required to install and configure the scanner, but not required to run scans.</p> <p>Once you've confirmed that the scanner can discover, classify, and protect files, you can remove this right from the service account.</p> <p>If granting this right even for a short period of time is not possible because of your organization policies, see <a href="#">Deploying the scanner with alternative configurations</a>.</p>                                                                                        |
| <b>Log on as a service</b> user right assignment.     | <p>This right is automatically granted to the service account during the scanner installation and this right is required for the installation, configuration, and operation of the scanner.</p>                                                                                                                                                                                                                                                                                                                          |
| <b>Permissions to the data repositories</b>           | <ul style="list-style-type: none"> <li>- <b>File shares or local files:</b> Grant <b>Read</b>, <b>Write</b>, and <b>Modify</b> permissions for scanning the files and then applying classification and protection as configured.</li> <li>- <b>SharePoint:</b> Grant <b>Full Control</b> permissions for scanning the files and then applying classification and protection as configured.</li> <li>- <b>Discovery mode:</b> To run the scanner in discovery mode only, <b>Read</b> permission is sufficient.</li> </ul> |
| <b>For labels that reprotect or remove protection</b> | <p>To ensure that the scanner always has access to protected files, make this account a <a href="#">super user</a> for Azure Information Protection, and ensure that the super user feature is enabled. Additionally, if you've implemented <a href="#">onboarding controls</a> for a phased deployment, make sure that the service account is included in the onboarding controls you've configured.</p>                                                                                                                |
|                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

## SQL server requirements

To store the scanner configuration data, use an SQL server with the following requirements:

- **A local or remote instance.**

We recommend hosting the SQL Server and scanner service on different machines, unless you're working with a small deployment.

SQL Server 2012 is the minimum version for the following editions:

- SQL Server Enterprise
- SQL Server Standard
- SQL Server Express (recommended for test environments only)

- **An account with Sysadmin role to install the scanner.**

This enables the installation process to automatically create the scanner configuration database and grant the required **db\_owner** role to the service account that runs the scanner.

If you cannot be granted the Sysadmin role or your organization policies require databases to be created and configured manually, see [Deploying the scanner with alternative configurations](#).

- **Capacity.** For capacity guidance, see [Storage requirements and capacity planning for SQL Server](#).

- [Case insensitive collation](#)

**NOTE**

Multiple configuration databases on the same SQL server are supported when you specify a custom cluster (profile) name for the scanner, or when you use the preview version of the scanner.

## Storage requirements and capacity planning for SQL Server

The amount of disk space required for the scanner's configuration database and the specification of the computer running SQL Server can vary for each environment, so we encourage you to do your own testing. Use the following guidance as a starting point.

For more information, see [Optimizing the performance of the scanner](#).

The disk size for the scanner configuration database will vary for each deployment. Use the following equation as guidance:

$$100 \text{ KB} + \langle \text{file count} \rangle * (1000 + 4 * \langle \text{average file name length} \rangle)$$

For example, to scan 1 million files that have an average file name length of 250 bytes, allocate 2 GB disk space.

For multiple scanners:

- **Up to 10 scanners**, use:
  - 4 core processors
  - 8 GB RAM recommended
- **More than 10 scanners** (maximum 40), use:
  - 8 core processes
  - 16 GB RAM recommended

## Azure Information Protection client requirements

You must have either the [current general availability version](#) of the Azure Information Protection client installed on the Windows Server computer.

For more information, see the [Unified labeling client admin guide](#).

**IMPORTANT**

You must install the full client for the scanner. Do not install the client with just the PowerShell module.

## Label configuration requirements

You must have labels configured that automatically apply classification, and optionally, protection.

If you don't have these labels configured, see [Deploying the scanner with alternative configurations](#).

For more information, see:

- [Apply a sensitivity label to content automatically](#)
- [Restrict access to content by using encryption in sensitivity labels](#)

## SharePoint requirements

To scan SharePoint document libraries and folders, ensure that your SharePoint server complies with the following requirements:

- **Supported versions.** Supported versions include: SharePoint 2019, SharePoint 2016, SharePoint 2013, and SharePoint 2010. Other versions of SharePoint are not supported for the scanner.
- **Versioning.** When you use [versioning](#), the scanner inspects and labels the last published version. If the scanner labels a file and [content approval](#) is required, that labeled file must be approved to be available for users.
- **Large SharePoint farms.** For large SharePoint farms, check whether you need to increase the list view threshold (by default, 5,000) for the scanner to access all files. For more information, see [Manage large lists and libraries in SharePoint](#).

## Microsoft Office requirements

To scan Office documents, your documents must be in one of the following formats:

- Microsoft Office 97-2003
- Office Open XML formats for Word, Excel, and PowerPoint

For more information, see [File types supported by the Azure Information Protection unified labeling client](#).

## File path requirements

To scan files, your file paths must have a maximum of 260 characters, unless the scanner is installed on Windows 2016 and the computer is configured to support long paths

Windows 10 and Windows Server 2016 support path lengths greater than 260 characters with the following [group policy setting](#): Local Computer Policy > Computer Configuration > Administrative Templates > All Settings > Enable Win32 long paths

For more information about supporting long file paths, see the [Maximum Path Length Limitation](#) section from the Windows 10 developer documentation.

## Usage statistics requirements

Disable usage statistics using one of the following methods:

- Setting the [AllowTelemetry](#) parameter to 0
- Ensure that the [Help improve Azure Information Protection by sending usage statistics to Microsoft](#) option remains unselected during the scanner installation process.

## Deploying the scanner with alternative configurations

The prerequisites listed above are the default requirements for the scanner deployment, and recommended because they support the simplest scanner configuration.

The default requirements should be suitable for initial testing, so that you can check the capabilities of the scanner.

However, in a production environment, your organization's policies may prohibit these default requirements. The scanner can accommodate the following restrictions with additional configuration:

- [The scanner server cannot have internet connectivity](#)
- [Restriction: The scanner service account cannot be synchronized to Azure Active Directory but the server has internet connectivity](#)

- **Restriction:** The service account for the scanner cannot be granted the **Log on locally** right
- **Restriction:** You cannot be granted Sysadmin or databases must be created and configured manually

#### **Restriction: The scanner server cannot have internet connectivity**

To support a disconnected computer, perform the following steps:

1. Configure labels in your policy, and then import the policy using the [Import-AIPScannerConfiguration](#) cmdlet. While the unified labeling client cannot apply protection without an internet connection, the scanner can still apply labels based on imported policies.
2. Configure the scanner in the Azure portal, by creating a scanner cluster. If you need help with this step, see [Configure the scanner in the Azure portal](#).
3. Export your content job from the **Azure Information Protection - Content scan jobs** pane using the **Export** option.
4. In a PowerShell session, run [Import-AIPScannerConfiguration](#) and specify the file that contains the exported settings.

#### **Restriction: You cannot be granted Sysadmin or databases must be created and configured manually**

If you can be granted the Sysadmin role *temporarily* to install the scanner, you can remove this role when the scanner installation is complete.

Do one of the following, depending on your organization's requirements:

- **You can have the Sysadmin role temporarily.** If you temporarily have the Sysadmin role, the database is automatically created for you and the service account for the scanner is automatically granted the required permissions.

However, the user account that configures the scanner still requires the **db\_owner** role for the scanner configuration database. If you only have the Sysadmin role until the scanner installation is complete, [grant the db\\_owner role to the user account manually](#).

- **You cannot have the Sysadmin role at all.** If you cannot be granted the Sysadmin role even temporarily, you must ask a user with Sysadmin rights to manually create a database before you install the scanner.

For this configuration, the **db\_owner** role must be assigned to the following accounts:

- Service account for the scanner
- User account for the scanner installation
- User account for scanner configuration

Typically, you will use the same user account to install and configure the scanner. If you use different accounts, they both require the **db\_owner** role for the scanner configuration database. Create this user and rights as needed. If you specify your own cluster (profile) name, the configuration database is named **AIPScannerUL\_<cluster\_name>**.

Additionally:

- You must be a local administrator on the server that will run the scanner
- The service account that will run the scanner must be granted Full Control permissions to the following registry keys:
  - **HKEY\_LOCAL\_MACHINE\SOFTWARE\WOW6432Node\Microsoft\MSIPC\Server**
  - **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\MSIPC\Server**

If, after configuring these permissions, you see an error when you install the scanner, the error can be ignored and

you can manually start the scanner service.

#### Populate the database manually

Populate the database using the following script:

```
if not exists(select * from master.sys.server_principals where sid = SUSER_SID('domain\user')) BEGIN declare
@T nvarchar(500) Set @T = 'CREATE LOGIN ' + quotename('domain\user') + ' FROM WINDOWS ' exec(@T) END
```

#### Create a user and grant db\_owner rights manually

To create a user and grant db\_owner rights on this database, ask the Sysadmin to do the following:

1. Create a DB for scanner:

```
CREATE DATABASE AIPScannerUL_[clustername]

ALTER DATABASE AIPScannerUL_[clustername] SET TRUSTWORTHY ON
```

2. Grant rights to the user that runs the install command and is used to run scanner management commands.

SQL script:

```
if not exists(select * from master.sys.server_principals where sid = SUSER_SID('domain\user')) BEGIN
declare @T nvarchar(500) Set @T = 'CREATE LOGIN ' + quotename('domain\user') + ' FROM WINDOWS '
exec(@T) END
USE DBName IF NOT EXISTS (select * from sys.database_principals where sid = SUSER_SID('domain\user'))
BEGIN declare @X nvarchar(500) Set @X = 'CREATE USER ' + quotename('domain\user') + ' FROM LOGIN ' +
quotename('domain\user'); exec sp_addrolemember 'db_owner', 'domain\user' exec(@X) END
```

3. Grant rights to scanner service account.

SQL script:

```
if not exists(select * from master.sys.server_principals where sid = SUSER_SID('domain\user')) BEGIN
declare @T nvarchar(500) Set @T = 'CREATE LOGIN ' + quotename('domain\user') + ' FROM WINDOWS '
exec(@T) END
```

#### Restriction: The service account for the scanner cannot be granted the Log on locally right

If your organization policies prohibit the **Log on locally** right for service accounts, but allows the **Log on as a batch job** right, use the *OnBehalfOf* parameter with Set-AIPAuthentication.

For more information, see [How to label files non-interactively for Azure Information Protection](#).

#### Restriction: The scanner service account cannot be synchronized to Azure Active Directory but the server has internet connectivity

You can have one account to run the scanner service and use another account to authenticate to Azure Active Directory:

- For the scanner service account, use a local Windows account or an Active Directory account.
- For the Azure Active Directory account, specify your local account for the *OnBehalfOf* parameter with Set-AIPAuthentication. For more information, see [How to label files non-interactively for Azure Information Protection](#).

## Next steps

Once you've confirmed that your system complies with the scanner prerequisites, continue with [Deploying the Azure Information Protection scanner to automatically classify and protect files](#).

For an overview about the scanner, see [Deploying the Azure Information Protection scanner to automatically classify and protect files](#).

**More information:**

- Interested in how the Core Services Engineering and Operations team in Microsoft implemented this scanner? Read the technical case study: [Automating data protection with Azure Information Protection scanner](#).
- You might be wondering: [What's the difference between Windows Server FCI and the Azure Information Protection scanner?](#)
- You can also use PowerShell to interactively classify and protect files from your desktop computer. For more information about this and other scenarios that use PowerShell, see [Using PowerShell with the Azure Information Protection unified labeling client](#).

# Configuring and installing the Azure Information Protection unified labeling scanner

7/20/2020 • 14 minutes to read • [Edit Online](#)

*Applies to:* [Azure Information Protection](#), Windows Server 2019, Windows Server 2016, Windows Server 2012 R2

## NOTE

If you're working with the AIP classic scanner, see [Installing and configuring the Azure Information Protection classic scanner](#).

Before you start configuring and installing the Azure Information Protection scanner, verify that your system complies with the [required prerequisites](#).

When you're ready, continue with the following steps:

1. [Configure the scanner in the Azure portal](#)
2. [Install the scanner](#)
3. [Get an Azure AD token for the scanner](#)
4. [Configure the scanner to apply classification and protection](#)

Perform the following additional configuration procedures as needed for your system:

| PROCEDURE                                                       | DESCRIPTION                                                                                                                                        |
|-----------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">Change which file types to protect</a>              | You may want to scan, classify, or protect different file types than the default. For more information, see <a href="#">AIP scanning process</a> . |
| <a href="#">Upgrading your scanner</a>                          | Upgrade your scanner to leverage the latest features and improvements.                                                                             |
| <a href="#">Editing data repository settings in bulk</a>        | Use import and export options to make changes in bulk for multiple data repositories.                                                              |
| <a href="#">Use the scanner with alternative configurations</a> | Use the scanner without configuring labels with any conditions                                                                                     |
| <a href="#">Optimize performance</a>                            | Guidance to optimize your scanner performance                                                                                                      |

For more information, see also [List of cmdlets for the scanner](#).

## Configure the scanner in the Azure portal

Before you install the scanner, or upgrade it from an older general availability version of the scanner, create a cluster and content scan job for the scanner in the Azure portal.

Then, configure the cluster and content scan job with scanner settings and the data repositories to scan.

To configure your scanner:

1. [Sign in to the Azure portal](#), and navigate to the **Azure Information Protection** pane.

For example, in the search box for resources, services, and docs: Start typing **Information** and select **Azure Information Protection**.

2. Locate the **Scanner** menu options, and select **Clusters**.

3. On the **Azure Information Protection - Clusters** pane, select **Add**:

The screenshot shows the 'Azure Information Protection - Clusters' pane. At the top, there are several buttons: '+ Add' (highlighted with a red box), 'Refresh', 'Export', 'Delete', 'Scan now', and 'Rescan all files'. Below these are filter and sorting options: 'NAME ↑↓', 'SCHED... ↑↓', 'ENFORCE ↑↓', 'REPOSIT... ↑↓', 'NODES ↑↓', 'LAST SC... ↑↓', 'LAST SC... ↑↓', and 'CURREN... ↑↓'. A search bar with placeholder text 'Search to filter items...' is positioned above the table. The main area displays the message 'No Scanner Profiles'.

4. On the **Add a new cluster** pane:

- a. Specify a meaningful name for the scanner. This name is used to identify the scanner's configuration settings and the data repositories to scan.

For example, you might specify **Europe** to identify the geographical location of the data repositories that your scanner will cover. When you later install or upgrade the scanner, you will need to specify the same cluster name.

- b. Optionally, specify a description for administrative purposes, to help you identify the scanner's cluster name.
- c. Select **Save**.

5. Locate the **Scanner** menu options, and select **Content scan jobs**.

6. On the **Azure Information Protection - Content scan jobs** pane, select **Add**.

7. For this initial configuration, configure the following settings, and then select **Save** but do not close the pane:

| SECTION                   | SETTINGS                                                                                                                                                                                                                                                                                                  |
|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Content scan job settings | <ul style="list-style-type: none"><li>- <b>Schedule:</b> Keep the default of <b>Manual</b></li><li>- <b>Info types to be discovered:</b> Change to <b>Policy only</b></li><li>- <b>Configure repositories:</b> Do not configure at this time because the content scan job must first be saved.</li></ul>  |
| Policy enforcement        | <ul style="list-style-type: none"><li>- <b>Enforce:</b> Select <b>Off</b></li><li>- <b>Label files based on content:</b> Keep the default of <b>On</b></li><li>- <b>Default label:</b> Keep the default of <b>Policy default</b></li><li>- <b>Relabel files:</b> Keep the default of <b>Off</b></li></ul> |

| SECTION                 | SETTINGS                                                                                                                                                                                                                                                                     |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Configure file settings | <ul style="list-style-type: none"> <li>- Preserve "Date modified", "Last modified" and "Modified by": Keep the default of On</li> <li>- File types to scan: Keep the default file types for Exclude</li> <li>- Default owner: Keep the default of Scanner Account</li> </ul> |
|                         |                                                                                                                                                                                                                                                                              |

8. Now that the content scan job is created and saved, you're ready to return to the **Configure repositories** option to specify the data stores to be scanned.

Specify UNC paths, and SharePoint Server URLs for SharePoint on-premises document libraries and folders.

**NOTE**

SharePoint Server 2019, SharePoint Server 2016, and SharePoint Server 2013 are supported for SharePoint. SharePoint Server 2010 is also supported when you have [extended support for this version of SharePoint](#).

To add your first data store, while on the **Add a new content scan job** pane, select **Configure repositories** to open the **Repositories** pane:

**Profile settings**

Schedule 

**Manual** **Always**

Info types to be discovered 

**Policy only** **All**

Configure repositories

0 repositories configured 

9. On the **Repositories** pane, select **Add**:

**Repositories**

**+ Add**  Export  Import 

 Search to filter items...

PATH

DEFAULT LABEL

ENFORCE

No Scanner Repositories

10. On the **Repository** pane, specify the path for the data repository, and then select **Save**.

For example:

- For a network share, use `\Server\Folder`.
- For a SharePoint library, use `http://sharepoint.contoso.com/Shared%20Documents/Folder`.

**NOTE**

Wildcards are not supported and WebDav locations are not supported.

Use the following syntax when adding SharePoint paths:

| PATH                                      | SYNTAX                                                                                                                                                                                                                                                                                                                                                                     |
|-------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Root path                                 | <pre>http://&lt;SharePoint server name&gt;</pre> <p>Scans all sites, including any site collections allowed for the scanner user.<br/>Requires <a href="#">additional permissions</a> to automatically discover root content</p>                                                                                                                                           |
| Specific SharePoint subsite or collection | <p>One of the following:</p> <ul style="list-style-type: none"> <li>- <pre>http://&lt;SharePoint server name&gt;/&lt;subsite name&gt;</pre></li> <li>- <pre>http://&lt;SharePoint server name&gt;/&lt;site collection name&gt;/&lt;site name&gt;</pre></li> </ul> <p>Requires <a href="#">additional permissions</a> to automatically discover site collection content</p> |
| Specific SharePoint library               | <p>One of the following:</p> <ul style="list-style-type: none"> <li>- <pre>http://&lt;SharePoint server name&gt;/&lt;library name&gt;</pre></li> <li>- <pre>http://&lt;SharePoint server name&gt;/.../&lt;library name&gt;</pre></li> </ul>                                                                                                                                |
| Specific SharePoint folder                | <pre>http://&lt;SharePoint server name&gt;/.../&lt;folder name&gt;</pre>                                                                                                                                                                                                                                                                                                   |
|                                           |                                                                                                                                                                                                                                                                                                                                                                            |

For the remaining settings on this pane, do not change them for this initial configuration, but keep them as **Content scan job default**. The default setting means that the data repository inherits the settings from the content scan job.

11. If you want to add another data repository, repeat steps 8 and 9.

12. Close the **Repositories** pane and the **content scan job** pane.

Back on the **Azure Information Protection - Content scan job** pane, your content scan name is displayed, together with the **SCHEDULE** column showing **Manual** and the **ENFORCE** column is blank.

You're now ready to install the scanner with the content scanner job that you've created. Continue with [Install the scanner](#).

## Install the scanner

After you've [configured the Azure Information Protection scanner in the Azure portal](#), perform the steps below to install the scanner:

1. Sign in to the Windows Server computer that will run the scanner. Use an account that has local administrator rights and that has permissions to write to the SQL Server master database.

### IMPORTANT

For more information, see [Prerequisites for installing and deploying the Azure Information Protection scanner](#).

2. Open a Windows PowerShell session with the **Run as an administrator** option.
3. Run the [Install-AIPScanner](#) cmdlet, specifying your SQL Server instance on which to create a database for the Azure Information Protection scanner, and the scanner cluster name that you specified in the preceding section:

```
Install-AIPScanner -SqlServerInstance <name> -Profile <cluster name>
```

Examples, using the profile name of **Europe**:

- For a default instance: `Install-AIPScanner -SqlServerInstance SQLSERVER1 -Profile Europe`

- For a named instance:

```
Install-AIPScanner -SqlServerInstance SQLSERVER1\AIPSCANNER -Profile Europe
```

- For SQL Server Express:

```
Install-AIPScanner -SqlServerInstance SQLSERVER1\SQLEXPRESS -Profile Europe
```

When you are prompted, provide the credentials for the scanner service account (<domain\user name>) and password.

#### 4. Verify that the service is now installed by using **Administrative Tools > Services**.

The installed service is named **Azure Information Protection Scanner** and is configured to run by using the scanner service account that you created.

Now that you have installed the scanner, you need to [get an Azure AD token for the scanner](#) service account to authenticate, so that the scanner can run unattended.

## Get an Azure AD token for the scanner

An Azure AD token allows the scanner to authenticate to the Azure Information Protection service.

To get an Azure AD token:

1. Return to the Azure portal to create an Azure AD application to specify an access token for authentication. This token lets the scanner run non-interactively. For more information, see [How to label files non-interactively for Azure Information Protection](#).
2. From the Windows Server computer, if your scanner service account has been granted the **Log on locally** right for the installation, sign in with this account and start a PowerShell session.

Run [Set-AIPAuthentication](#), specifying the values that you copied from the previous step:

```
Set-AIPAuthentication -AppId <ID of the registered app> -AppSecret <client secret string> -TenantId <your tenant ID> -DelegatedUser <Azure AD account>
```

For example:

```
$pscreds = Get-Credential CONTOSO\scanner
Set-AIPAuthentication -AppId "77c3c1c3-abf9-404e-8b2b-4652836c8c66" -AppSecret
"0Akk+rnuYc/u+Jah2kNxVbrDGbS47L4" -DelegatedUser scanner@contoso.com -TenantId "9c11c87a-ac8b-46a3-
8d5c-f4d0b72ee29a" -OnBehalfOf $pscreds
Acquired application access token on behalf of CONTOSO\scanner.
```

### TIP

If your scanner service account cannot be granted the **Log on locally** right for the installation, use the **OnBehalfOf** parameter with [Set-AIPAuthentication](#), as described in [How to label files non-interactively for Azure Information Protection](#).

The scanner now has a token to authenticate to Azure AD, which is valid for one year, two years, or never, according to your configuration of the **Web app /API client secret** in Azure AD.

When the token expires, you must repeat this procedure.

You're now ready to run your first scan in discovery mode. For more information, see [Run a discovery cycle and view reports for the scanner](#).

If you've already run a discovery scan, continue with [Configure the scanner to apply classification and protection](#).

## Configure the scanner to apply classification and protection

The default settings configure the scanner to run once, and in reporting-only mode.

To change these settings, edit the content scan job:

1. In the Azure portal, on the **Azure Information Protection - Content scan jobs** pane, select the cluster and content scan job to edit it.
2. On the Content scan job pane, change the following, and then select **Save**:
  - From the **Content scan job** section: Change the **Schedule** to **Always**
  - From the **Policy enforcement** section: Change **Enforce** to **On**

### TIP

You may want to change other settings on this pane, such as whether file attributes are changed and whether the scanner can relabel files. Use the information popup help to learn more information about each configuration setting.

3. Make a note of the current time and start the scanner again from the **Azure Information Protection - Content scan jobs** pane:



Alternatively, run the following command in your PowerShell session:

```
Start-AIPScan
```

The scanner is now scheduled to run continuously. When the scanner works its way through all configured files, it automatically starts a new cycle so that any new and changed files are discovered.

## Change which file types to protect

By default the AIP scanner protects Office file types and PDF files only.

Use PowerShell commands to change this behavior as needed, such as to configure the scanner to protect all file types, just as the client does, or to protect additional, specific file types.

For a label policy that applies to the user account downloading labels for the scanner, specify a PowerShell advanced setting named **PFileSupportedExtensions**.

For a scanner that has access to the internet, this user account is the account that you specify for the **DelegatedUser** parameter with the **Set-AIPAuthentication** command.

**Example 1:** PowerShell command for the scanner to protect all file types, where your label policy is named "Scanner":

```
Set-LabelPolicy -Identity Scanner -AdvancedSettings @{PFileSupportedExtensions="*"}
Set-LabelPolicy -Identity Scanner -AdvancedSettings @{}
PFileSupportedExtensions=ConvertTo-Json(".xml", ".tiff")
```

**Example 2:** PowerShell command for the scanner to protect .xml files and .tiff files in addition to Office files and PDF files, where your label policy is named "Scanner":

```
Set-LabelPolicy -Identity Scanner -AdvancedSettings @{}
PFileSupportedExtensions=ConvertTo-Json(".xml", ".tiff")
```

For more information, see [Change which file types to protect](#).

## Upgrading your scanner

If you have previously installed the scanner and want to upgrade, use the instructions described in [Upgrading the Azure Information Protection scanner](#).

Then, [configure](#) and [use your scanner](#) as usual, skipping the steps to install your scanner.

## Editing data repository settings in bulk

Use the **Export** and **Import** buttons to make changes for your scanner across several repositories.

This way, you don't need to make the same changes several times, manually, in the Azure portal.

For example, if you have a new file type on several SharePoint data repositories, you may want to update the settings for those repositories in bulk.

To make changes in bulk across repositories:

1. In the Azure portal on the **Repositories** pane, select the **Export** option. For example:

The screenshot shows the 'Repositories' pane in the Azure portal. At the top, there are four buttons: '+ Add', 'Export' (which is highlighted with a red box), 'Import', and 'Delete'. Below the buttons is a search bar with the placeholder 'Search to filter items...'. Underneath the search bar is a table with three columns: 'PATH', 'DEFAULT LABEL', and 'ENFORCE'. The table has a header row and several data rows. The 'EXPORT' button is located at the bottom right of the pane.

2. Manually edit the exported file to make your change.
3. Use the **Import** option on the same page to import the updates back across your repositories.

## Using the scanner with alternative configurations

The Azure Information Protection scanner usually looks for conditions specified for your labels in order to classify and protect your content as needed.

In the following scenarios, the Azure Information Protection scanner is also able to scan your content and manage labels, without any conditions configured:

- [Apply a default label to all files in a data repository](#)
- [Remove existing labels from all files in a data repository](#)
- [Identify all custom conditions and known sensitive information types](#)

### Apply a default label to all files in a data repository

In this configuration, all unlabeled files in the repository are labeled with the default label specified for the repository or the content scan job. Files are labeled without inspection.

Configure the following settings:

| SETTING                      | DESCRIPTION                                                                              |
|------------------------------|------------------------------------------------------------------------------------------|
| Label files based on content | Set to Off                                                                               |
| Default label                | Set to Custom, and then select the label to use                                          |
| Enforce default label        | Select to have the default label applied to all files, even if they are already labeled. |

### Remove existing labels from all files in a data repository

In this configuration, all existing labels are removed, including protection, if protection was applied with the label. Protection applied independently of a label is retained.

Configure the following settings:

| SETTING                      | DESCRIPTION                                                 |
|------------------------------|-------------------------------------------------------------|
| Label files based on content | Set to Off                                                  |
| Default label                | Set to None                                                 |
| Relabel files                | Set to On, with the Enforce default label checkbox selected |

### Identify all custom conditions and known sensitive information types

This configuration enables you to find sensitive information that you might not realize you had, at the expense of scanning rates for the scanner.

Set the Info types to be discovered to All.

To identify conditions and information types for labeling, the scanner uses any custom sensitive information types specified, and the list of built-in sensitive information types that are available to select, as defined in your labeling management center.

## Optimizing scanner performance

### NOTE

If you are looking to improve the responsiveness of the scanner computer rather than the scanner performance, use an advanced client setting to [limit the number of threads used by the scanner](#).

Use the following options and guidance to help you optimize scanner performance:

| OPTION | DESCRIPTION |
|--------|-------------|
|--------|-------------|

| OPTION                                                                                                    | DESCRIPTION                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-----------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Have a high speed and reliable network connection between the scanner computer and the scanned data store | <p>For example, place the scanner computer in the same LAN, or preferably, in the same network segment as the scanned data store.</p> <p>The quality of the network connection affects the scanner performance because, to inspect the files, the scanner transfers the contents of the files to the computer running the scanner service.</p> <p>Reducing or eliminating the network hops required for the data to travel also reduces the load on your network.</p> |
| Make sure the scanner computer has available processor resources                                          | <p>Inspecting the file contents and encrypting and decrypting files are processor-intensive actions.</p> <p>Monitor the typical scanning cycles for your specified data stores to identify whether a lack of processor resources is negatively affecting the scanner performance.</p>                                                                                                                                                                                 |
| Install multiple instances of the scanner                                                                 | <p>The Azure Information Protection scanner supports multiple configuration databases on the same SQL server instance when you specify a custom cluster (profile) name for the scanner.</p> <p>Multiple scanners can also share the same cluster (profile), resulting in quicker scanning times.</p>                                                                                                                                                                  |
| Check your alternative configuration usage                                                                | <p>The scanner runs more quickly when you use the <a href="#">alternative configuration</a> to apply a default label to all files because the scanner does not inspect the file contents.</p> <p>The scanner runs more slowly when you use the <a href="#">alternative configuration</a> to identify all custom conditions and known sensitive information types.</p>                                                                                                 |

## Additional factors that affect performance

Additional factors that affect the scanner performance include:

| FACTOR                             | DESCRIPTION                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Load/response times                | The current load and response times of the data stores that contain the files to scan will also affect scanner performance.                                                                                                                                                                                                                                                                                                                      |
| Scanner mode (Discovery / Enforce) | <p>Discovery mode typically has a higher scanning rate than enforce mode.</p> <p>Discovery requires a single file read action, whereas enforce mode requires read and write actions.</p>                                                                                                                                                                                                                                                         |
| Policy changes                     | <p>Your scanner performance may be affected if you've made changes to the autolabeling in the label policy.</p> <p>Your first scan cycle, when the scanner must inspect every file, will take longer than subsequent scan cycles that by default, inspect only new and changed files.</p> <p>If you change the conditions or autolabeling settings, all files are scanned again. For more information, see <a href="#">Rescanning files</a>.</p> |

| Factor              | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Regex constructions | <p>Scanner performance is affected by how your regex expressions for custom conditions are constructed. To avoid heavy memory consumption and the risk of timeouts (15 minutes per file), review your regex expressions for efficient pattern matching.</p> <p>For example:</p> <ul style="list-style-type: none"> <li>- Avoid <a href="#">greedy quantifiers</a></li> <li>- Use non-capturing groups such as <code>(?:expression)</code> instead of <code>(expression)</code></li> </ul> |
| Log level           | <p>Log level options include <b>Debug</b>, <b>Info</b>, <b>Error</b> and <b>Off</b> for the scanner reports.</p> <ul style="list-style-type: none"> <li>- <b>Off</b> results in the best performance</li> <li>- <b>Debug</b> considerably slows down the scanner and should be used only for troubleshooting.</li> </ul> <p>For more information, see the <i>ReportLevel</i>/parameter for the <a href="#">Set-AIPScannerConfiguration</a> cmdlet.</p>                                    |
| Files being scanned | <ul style="list-style-type: none"> <li>- With the exception of Excel files, Office files are more quickly scanned than PDF files.</li> <li>- Unprotected files are quicker to scan than protected files.</li> <li>- Large files obviously take longer to scan than small files.</li> </ul>                                                                                                                                                                                                |

## List of cmdlets for the scanner

This section lists PowerShell cmdlets supported for the Azure Information Protection scanner.

### NOTE

The Azure Information Protection scanner is configured from the Azure portal. Therefore, cmdlets used in previous versions to configure data repositories and the scanned file types list are now deprecated.

Supported cmdlets for the scanner include:

- [Get-AIPScannerConfiguration](#)
- [Get-AIPScannerStatus](#)
- [Export-AIPLogs](#)
- [Import-AIPScannerConfiguration](#)
- [Install-AIPScanner](#)
- [Set-AIPScanner](#)
- [Set-AIPScannerConfiguration](#)
- [Start-AIPScanDiagnostics](#)
- [Start-AIPScan](#)
- [Stop-AIPScan](#)
- [Uninstall-AIPScanner](#)

- [Update-AIPScanner](#)

## Next steps

Once you've installed and configured your scanner, start [scanning your files](#).

See also: [Deploying the Azure Information Protection scanner to automatically classify and protect files](#).

### More information:

- Interested in how the Core Services Engineering and Operations team in Microsoft implemented this scanner? Read the technical case study: [Automating data protection with Azure Information Protection scanner](#).
- You might be wondering: [What's the difference between Windows Server FCI and the Azure Information Protection scanner?](#)
- Use PowerShell to interactively classify and protect files from your desktop computer. For more information about this and other scenarios that use PowerShell, see [Using PowerShell with the Azure Information Protection unified labeling client](#).

# Running the Azure Information Protection scanner

7/20/2020 • 6 minutes to read • [Edit Online](#)

Applies to: [Azure Information Protection](#), Windows Server 2019, Windows Server 2016, Windows Server 2012 R2

## NOTE

If you're using the classic scanner, see [Installing and configuring the Azure Information Protection classic scanner](#).

Once you've confirmed your [system requirements](#) and [configured and installed your scanner](#), [run a discovery scan](#) to get started.

Use other steps detailed below to manage your scans moving forward.

- [Stop a scan](#)
- [Rescanning files](#)
- [Troubleshooting a stopped scan](#)
- [Troubleshooting using the scanner diagnostic tool](#)

For more information, see [Deploying the Azure Information Protection scanner to automatically classify and protect files](#).

## Run a discovery cycle and view reports for the scanner

Use the following procedure after you've [configured and installed your scanner](#) to get an initial understanding of your content.

Perform these steps again as needed when your content changes.

1. In the Azure portal, on the **Azure Information Protection - Content scan jobs** pane, select your content scan jobs, and then select the **Scan now** option:



Alternatively, in your PowerShell session, run the following command:

```
Start-AIPScan
```

2. Wait for the scanner to complete its cycle. The scan completes when the scanner has crawled through all the files in the specified data stores.

Do any of the following to monitor scanner progress:

- **Refresh the scan jobs.** On the **Azure Information Protection - Content scan jobs** pane, select Refresh.

Wait until you see values for the LAST SCAN RESULTS column and the LAST SCAN (END TIME) column.

- Use a PowerShell command. Run `Get-AIPScannerStatus` to monitor the status change.
3. When the scan is complete, review the reports stored in the `%localappdata%\Microsoft\MSIP\Scanner\Reports` directory.
- The .txt summary files include the time taken to scan, the number of scanned files, and how many files had a match for the information types.
  - The .csv files have more details for each file. This folder stores up to 60 reports for each scanning cycle and all but the latest report is compressed to help minimize the required disk space.

**Initial configurations** instruct you to set the **Info types to be discovered to Policy only**. This configuration means that only files that meet the conditions you've configured for automatic classification are included in the detailed reports.

If you don't see any labels applied, check that your label configuration includes automatic rather than recommended classification, or enable **Treat recommended labeling as automatic** (available in scanner version 2.7.x.x and above).

If the results are still not as you expect, you might need to reconfigure the conditions that you specified for your labels. If that's the case, reconfigure the conditions as needed, and repeat this procedure until you are satisfied with the results. Then, update your configuration automatically, and optionally protection.

### Viewing updates in the Azure portal

Scanners send this information to Azure Information Protection every five minutes, so that you can view the results in near real time from the Azure portal. For more information, see [Reporting for Azure Information Protection](#).

The Azure portal displays information about the last scan only. If you need to see the results of previous scans, return to the reports that are stored on the scanner computer, in the `%localappdata%\Microsoft\MSIP\Scanner\Reports` folder.

### Changing log levels or locations

Change the level of logging by using the *ReportLevel* parameter with [Set-AIPScannerConfiguration](#).

The report folder location or name cannot be changed. If you want to store reports in a different location, consider using a directory junction for the folder.

For example, use the [Mklink](#) command:

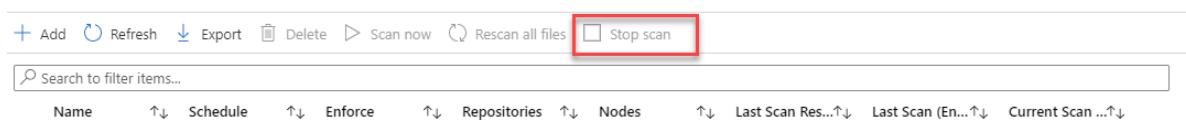
```
mklink /j D:\Scanner_reports C:\Users\aipscannersvc\AppData\Local\Microsoft\MSIP\Scanner\Reports
```

If you've performed these steps after an initial configuration and installation, continue with [Configure the scanner to apply classification and protection](#).

## Stopping a scan

To stop a currently running scan before it's complete, use one of the following methods:

- Azure portal. Select Stop scan:



- Run a PowerShell command. Run the following command:

```
Stop-AIPScan
```

# Rescanning files

For the [first scan cycle](#), the scanner inspects all files in the configured data stores. For subsequent scans, only new or modified files are inspected.

Inspecting all files again is typically useful when you want the reports to include all files, and when the scanner runs in discovery mode.

Run a new scan of all your files using one the following methods:

- [Manually run a full rescan](#)
- [Trigger a full rescan by refreshing the policy](#)

## Manually run a full rescan

Force the scanner to inspect all files again, as needed, from the **Azure Information Protection - Content scan jobs** pane in the Azure portal.

Select your content scan job from the list, and then select the **Rescan all files** option:



When a full scan is complete, the scan type automatically changes to incremental so that for subsequent scans, only new or modified files are scanned again.

## Trigger a full rescan by refreshing the policy

All files are also inspected whenever the scanner has new or changed settings for automatic and recommended labeling. The scanner automatically refreshes the policy every four hours.

To refresh the policy sooner, such as while testing, manually delete the contents of the `%LocalAppData%\Microsoft\MSIP\mip\<processname>\mip` directory and restart the Azure Information Protection service.

### NOTE

If you've also changed protection settings for your labels, wait an extra 15 minutes from when you saved the updated protection settings before restarting the Azure Information Protection service.

# Troubleshooting a stopped scan

If the scanner stops in the middle unexpectedly, and doesn't complete scanning a large number of files in a repository, you may need to modify one of the following settings:

- **Number of dynamic ports.** You may need to increase the number of dynamic ports for the operating system hosting the files. Server hardening for SharePoint can be one reason why the scanner exceeds the number of allowed network connections, and therefore stops.

To check whether this is the cause of the scanner stopping, look to see if the following error message is logged for the scanner in the `%localappdata%\Microsoft\MSIP\Logs\MSIPScanner.iplog` file.

**Unable to connect to the remote server ---> System.Net.Sockets.SocketException: Only one usage of each socket address (protocol/network address/port) is normally permitted IP:port**

**NOTE**

This file will be zipped if there are multiple logs.

For more information about how to view the current port range and increase the range, see [Settings that can be Modified to Improve Network Performance](#).

- **List view threshold.** For large SharePoint farms, you may need to increase the list view threshold. By default, the list view threshold is set to 5,000.

For more information, see [Manage large lists and libraries in SharePoint](#).

## Troubleshooting using the scanner diagnostic tool

If you're having issues with the Azure Information Scanner, verify whether your deployment is healthy using the following PowerShell command:

```
Start-AIPScannerDiagnostics
```

The diagnostics tool checks the following details and then exports a log file with the results:

- Whether the database is up to date
- Whether network URLs are accessible
- Whether there's a valid authentication token and the policy can be acquired
- Whether the profile is defined in the Azure portal
- Whether offline/online configuration exists and can be acquired
- Whether the rules configured are valid

**TIP**

If you are running the command under a user that is not the scanner user, be sure to add the **-OnBehalf** parameter.

**NOTE**

The **Start-AIPScannerDiagnostics** tool does not run a full prerequisites check. If you're having issues with the scanner, also ensure that your system complies with [scanner requirements](#), and that your [scanner configuration and installation](#) is complete.

## Next steps

- Interested in how the Core Services Engineering and Operations team in Microsoft implemented this scanner? Read the technical case study: [Automating data protection with Azure Information Protection scanner](#).
- You might be wondering: [What's the difference between Windows Server FCI and the Azure Information Protection scanner?](#)
- You can also use PowerShell to interactively classify and protect files from your desktop computer. For more information about this and other scenarios that use PowerShell, see [Using PowerShell with the Azure Information Protection unified labeling client](#).

# What is the Azure Information Protection classic scanner?

7/20/2020 • 5 minutes to read • [Edit Online](#)

Applies to: [Azure Information Protection](#), Windows Server 2019, Windows Server 2016, Windows Server 2012 R2

## NOTE

To provide a unified and streamlined customer experience, **Azure Information Protection client (classic)** and **Label Management** in the Azure Portal are being **deprecated** as of **March 31, 2021**. This time-frame allows all current Azure Information Protection customers to transition to our unified labeling solution using the Microsoft Information Protection Unified Labeling platform. Learn more in the official [deprecation notice](#).

If you're using the unified labeling client, see [What is the Azure Information Protection unified labeling scanner?](#).

Use the information in this section to learn about the Azure Information Protection scanner, and then how to successfully install, configure, run and if necessary, troubleshoot it.

The AIP scanner runs as a service on Windows Server and lets you discover, classify, and protect files on the following data stores:

- **UNC paths** for network shares that use the Server Message Block (SMB) protocol.
- **SharePoint document libraries and folder** for SharePoint Server 2019 through SharePoint Server 2013. SharePoint 2010 is also supported for customers who have [extended support for this version of SharePoint](#).

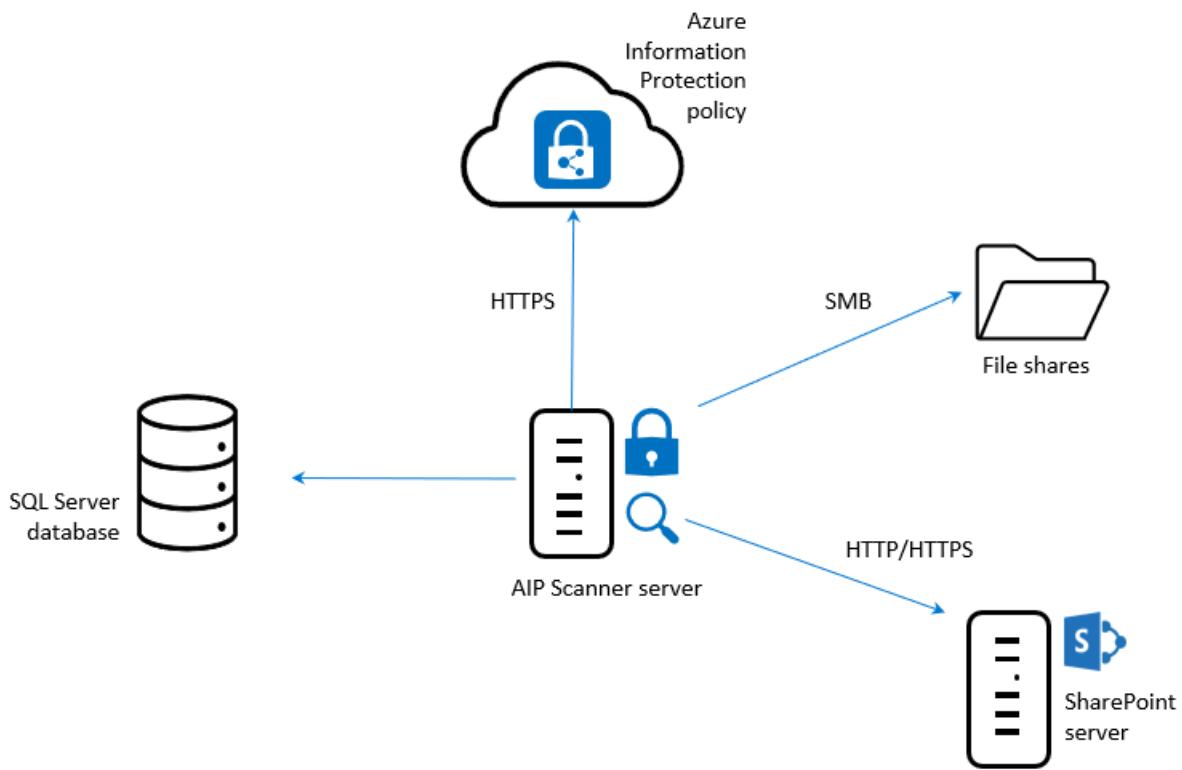
## NOTE

To scan and label files on cloud repositories, use [Cloud App Security](#) instead of the scanner.

## Azure Information Protection classic scanner overview

The AIP scanner can inspect any files that Windows can index. If you've configured labels that apply automatic classification, the scanner can label discovered files to apply that classification, and optionally apply or remove protection.

The following image shows the AIP scanner architecture, where the scanner discovers files across your on-premises and SharePoint servers.



To inspect your files, the scanner uses IFilters installed on the computer. To determine whether the files need labeling, the scanner uses the Office 365 built-in data loss prevention (DLP) sensitivity information types and pattern detection, or Office 365 regex patterns.

The scanner uses the Azure Information Protection client, and can classify and protect the same types of files as the client. For more information, see [File types supported by the Azure Information Protection client](#).

Do any of the following to configure your scans as needed:

- Run the scanner in **discovery mode only** to create reports that check to see what happens when your files are labeled.
- Run the scanner to discover files with sensitive information, without configuring labels that apply automatic classification.
- Run the scanner automatically to apply labels as configured.
- Define a **file types** list to specify specific files to scan or to exclude.

#### NOTE

The scanner does not discover and label in real time. It systematically crawls through files on data stores that you specify. Configure this cycle to run once, or repeatedly.

## AIP scanning process

When scanning files, the AIP scanner runs through the following steps:

1. Determine whether files are included or excluded for scanning
2. Inspect and label files
3. Label files that can't be inspected

#### **NOTE**

For more information, see [Files not labeled by the scanner](#).

## **1. Determine whether files are included or excluded for scanning**

The scanner automatically skips files that are excluded from classification and protection, such as executable files and system files. For more information, see [File types that are excluded from classification and protection](#).

The scanner also considers any file lists explicitly defined to scan, or exclude from scanning. File lists apply for all data repositories by default, and can also be defined for specific repositories only.

To define file lists for scanning or exclusion, use the **File types to scan** setting in the content scan job. For example:

#### **Configure file settings**

Preserve "Date modified", "Last modified" and "Modified by" [i](#)

Off  On

File types to scan [i](#)

Include  Exclude

.lnk,.exe,.com,.cmd,.bat,.dll,.ini,.pst,.sca,.drm,.sys,.cpl,.inf,.drv,.dat,.tmp,.msp,.msi,.pdb,.jar,.ocx,.rtf,.rar,.msg

Default owner [i](#)

Scanner Account  Custom

For more information, see [Deploying the Azure Information Protection scanner to automatically classify and protect files](#).

## **2. Inspect and label files**

After identifying excluded files, the scanner filters again to identify files supported for inspection.

These additional filters are the same ones used by the operating system for Windows Search and indexing, and require no additional configuration. Windows IFilter is also used to scan file types that are used by Word, Excel, and PowerPoint, and for PDF documents and text files.

For a full list of file types supported for inspection, and additional instructions for configuring filters to include .zip and .tiff files, see [File types supported for inspection](#).

After inspection, supported file types are labeled using the conditions specified for your labels. If you're using discovery mode, these files can either be reported to contain the conditions specified for your labels, or reported to contain any known sensitive information types.

## **3. Label files that can't be inspected**

For any file types that can't be inspected, the AIP scanner applies the default label in the Azure Information Protection policy, or the default label configured for the scanner.

#### **Files not labeled by the scanner**

The AIP scanner cannot label files under the following circumstances:

- When the label applies classification, but not protection, and the file type does not support classification-only by the client. For more information, see [Classic client file types](#).
- When the label applies classification and protection, but the scanner does not support the file type.

By default, the scanner protects only Office file types, and PDF files when they are protected by using the ISO standard for PDF encryption.

Other types of files can be added for protection when you [change the types of files to protect](#).

**Example:** After inspecting .txt files, the scanner can't apply a label that's configured for classification only, because the .txt file type doesn't support classification only.

However, if the label is configured for both classification and protection, and the .txt file type is included for the scanner to protect, the scanner can label the file.

## Next steps

For more information about deploying the scanner, see the following articles:

- [AIP scanner deployment prerequisites](#)
- [Configuring and installing the AIP scanner](#)
- [Running scans using the AIP scanner](#)

### More information:

- Interested in how the Core Services Engineering and Operations team in Microsoft implemented this scanner? Read the technical case study: [Automating data protection with Azure Information Protection scanner](#).
- You might be wondering: [What's the difference between Windows Server FCI and the Azure Information Protection scanner?](#)
- You can also use PowerShell to interactively classify and protect files from your desktop computer. For more information about this and other scenarios that use PowerShell, see [Using PowerShell with the Azure Information Protection client](#).

# Prerequisites for installing and deploying the Azure Information Protection classic scanner

7/20/2020 • 12 minutes to read • [Edit Online](#)

Applies to: [Azure Information Protection](#), Windows Server 2019, Windows Server 2016, Windows Server 2012 R2

## NOTE

To provide a unified and streamlined customer experience, **Azure Information Protection client (classic)** and **Label Management** in the Azure Portal are being **deprecated** as of **March 31, 2021**. This time-frame allows all current Azure Information Protection customers to transition to our unified labeling solution using the Microsoft Information Protection Unified Labeling platform. Learn more in the official [deprecation notice](#).

If you're working with the unified labeling scanner, see [Prerequisites for installing and deploying the Azure Information Protection unified labeling scanner](#).

Before you install the Azure Information Protection scanner, make sure that your system complies with the following requirements:

- [Windows Server requirements](#)
- [Service account requirements](#)
- [SQL server requirements](#)
- [Azure Information Protection client requirements](#)
- [Label configuration requirements](#)
- [SharePoint requirements](#)
- [Microsoft Office requirements](#)
- [File path requirements](#)
- [Usage statistics requirements](#)

If you can't meet all the requirements in the table because they are prohibited by your organization policies, see the [alternative configurations](#) section.

When deploying the scanner in production or testing the performance for multiple scanners, see [Storage requirements and capacity planning for SQL Server](#).

When you're ready to start installing and deploying your scanner, continue with [Deploying the Azure Information Protection scanner to automatically classify and protect files](#).

## Windows Server requirements

You must have a Windows Server computer to run the scanner, which has the following system specifications:

| SPECIFICATION | DETAILS           |
|---------------|-------------------|
| Processor     | 4 core processors |
| RAM           | 8 GB              |

| SPECIFICATION               | DETAILS                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Disk space</b>           | <p>10 GB free space (average) for temporary files.<br/>The scanner requires sufficient disk space to create temporary files for each file that it scans, four files per core.</p> <p>The recommended disk space of 10 GB allows for 4 core processors scanning 16 files that each have a file size of 625 MB.</p>                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Operating system</b>     | <ul style="list-style-type: none"> <li>- Windows Server 2019</li> <li>- Windows Server 2016</li> <li>- Windows Server 2012 R2</li> </ul> <p><b>Note:</b> For testing or evaluation purposes in a non-production environment, you can also use any Windows operating system that is <a href="#">supported by the Azure Information Protection client</a>.</p>                                                                                                                                                                                                                                                                                                                      |
| <b>Network connectivity</b> | <p>Your scanner computer can be a physical or virtual computer with a fast and reliable network connection to the data stores to be scanned.</p> <p>If internet connectivity is not possible because of your organization policies, see <a href="#">Deploying the scanner with alternative configurations</a>.</p> <p>Otherwise, make sure that this computer has internet connectivity that allows the following URLs over HTTPS (port 443):</p> <ul style="list-style-type: none"> <li>- *.aadrm.com</li> <li>- *.azurerm.com</li> <li>- *.informationprotection.azure.com</li> <li>- informationprotection.hosting.portal.azure.net</li> <li>- *.aria.microsoft.com</li> </ul> |

## Service account requirements

You must have a service account to run the scanner service on the Windows Server computer, as well as authenticate to Azure AD and download the Azure Information Protection Policy.

Your service account must be an Active Directory account and synchronized to Azure AD.

If you cannot synchronize this account because of your organization policies, see [Deploying the scanner with alternative configurations](#).

This service account has the following requirements:

| REQUIREMENT                                 | DETAILS                                                                                                                                                                                                                                                                                                                                                                                                                           |
|---------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Log on locally</b> user right assignment | <p>Required to install and configure the scanner, but not required to run scans.</p> <p>Once you've confirmed that the scanner can discover, classify, and protect files, you can remove this right from the service account.</p> <p>If granting this right even for a short period of time is not possible because of your organization policies, see <a href="#">Deploying the scanner with alternative configurations</a>.</p> |

| Requirement                                    | Details                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Log on as a service user right assignment.     | This right is automatically granted to the service account during the scanner installation and this right is required for the installation, configuration, and operation of the scanner.                                                                                                                                                                                                                                                                                                                                 |
| Permissions to the data repositories           | <ul style="list-style-type: none"> <li>- <b>File shares or local files:</b> Grant <b>Read</b>, <b>Write</b>, and <b>Modify</b> permissions for scanning the files and then applying classification and protection as configured.</li> <li>- <b>SharePoint:</b> Grant <b>Full Control</b> permissions for scanning the files and then applying classification and protection as configured.</li> <li>- <b>Discovery mode:</b> To run the scanner in discovery mode only, <b>Read</b> permission is sufficient.</li> </ul> |
| For labels that reprotect or remove protection | To ensure that the scanner always has access to protected files, make this account a <a href="#">super user</a> for Azure Information Protection, and ensure that the super user feature is enabled. Additionally, if you've implemented <a href="#">onboarding controls</a> for a phased deployment, make sure that the service account is included in the onboarding controls you've configured.                                                                                                                       |
|                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

## SQL server requirements

To store the scanner configuration data, use an SQL server with the following requirements:

- **A local or remote instance.**

We recommend hosting the SQL Server and scanner service on different machines, unless you're working with a small deployment.

SQL Server 2012 is the minimum version for the following editions:

- SQL Server Enterprise
- SQL Server Standard
- SQL Server Express (recommended for test environments only)

- **An account with Sysadmin role to install the scanner.**

This enables the installation process to automatically create the scanner configuration database and grant the required **db\_owner** role to the service account that runs the scanner.

If you cannot be granted the Sysadmin role or your organization policies require databases to be created and configured manually, see [Deploying the scanner with alternative configurations](#).

- **Capacity.** For capacity guidance, see [Storage requirements and capacity planning for SQL Server](#).
- **Case insensitive collation**

### NOTE

Multiple configuration databases on the same SQL server are supported when you specify a custom cluster (profile) name for the scanner.

## Storage requirements and capacity planning for SQL Server

The amount of disk space required for the scanner's configuration database and the specification of the computer running SQL Server can vary for each environment, so we encourage you to do your own testing. Use the following guidance as a starting point.

For more information, see [Optimizing the performance of the scanner](#).

The disk size for the configuration database will vary for each deployment. We recommend that you allocate 500 MB for every 1,000,000 files that you want to scan.

For each scanner, use:

- 4 core processors
- 8 GB RAM (4 GB minimum)

## Azure Information Protection client requirements

You must have the Azure Information Protection client installed on the Windows Server computer.

For more information, see the [Classic client admin guide](#).

### IMPORTANT

You must install the full client for the scanner. Do not install the client with just the PowerShell module.

## Label configuration requirements

You must have labels configured that automatically apply classification, and optionally, protection.

If you don't have these labels configured, see [Deploying the scanner with alternative configurations](#).

For more information, see:

- [How to configure conditions for automatic and recommended classification](#)
- [How to configure a label for Rights Management protection](#)

### TIP

Use the instructions from the [tutorial](#) to test the scanner with a label that looks for credit card numbers in a prepared Word document. However, you will need to change the label configuration so that the option **Select how this label is applied** is set to **Automatic**, rather than **Recommended** or **treat recommended labeling as automatic** (available in scanner version 2.7.x.x and above).

Then remove the label from the document (if it is applied) and copy the file to a data repository for the scanner.

## SharePoint requirements

To scan SharePoint document libraries and folders, ensure that your SharePoint server complies with the following requirements:

- **Supported versions.** Supported versions include: SharePoint 2019, SharePoint 2016, SharePoint 2013, and SharePoint 2010. Other versions of SharePoint are not supported for the scanner.
- **Versioning.** When you use [versioning](#), the scanner inspects and labels the last published version. If the scanner labels a file and [content approval](#) is required, that labeled file must be approved to be available for users.
- **Large SharePoint farms.** For large SharePoint farms, check whether you need to increase the list view

threshold (by default, 5,000) for the scanner to access all files. For more information, see [Manage large lists and libraries in SharePoint](#).

## Microsoft Office requirements

To scan Office documents, your documents must be in one of the following formats:

- Microsoft Office 97-2003
- Office Open XML formats for Word, Excel, and PowerPoint

For more information, see [File types supported by the Azure Information Protection client](#).

## File path requirements

To scan files, your file paths must have a maximum of 260 characters, unless the scanner is installed on Windows 2016 and the computer is configured to support long paths.

Windows 10 and Windows Server 2016 support path lengths greater than 260 characters with the following [group policy setting](#): Local Computer Policy > Computer Configuration > Administrative Templates > All Settings > Enable Win32 long paths

For more information about supporting long file paths, see the [Maximum Path Length Limitation](#) section from the Windows 10 developer documentation.

## Usage statistics requirements

Disable usage statistics using one of the following methods:

- Setting the [AllowTelemetry](#) parameter to 0
- Ensure that the [Help improve Azure Information Protection by sending usage statistics to Microsoft](#) option remains unselected during the scanner installation process.

## Deploying the scanner with alternative configurations

The prerequisites listed above are the default requirements for the scanner deployment, and recommended because they support the simplest scanner configuration.

The default requirements should be suitable for initial testing, so that you can check the capabilities of the scanner.

However, in a production environment, your organization's policies may prohibit these default requirements. The scanner can accommodate the following restrictions with additional configuration:

- [The scanner server cannot have internet connectivity](#)
- [Restriction: The scanner service account cannot be synchronized to Azure Active Directory but the server has internet connectivity](#)
- [Restriction: The service account for the scanner cannot be granted the Log on locally right](#)
- [Restriction: You cannot be granted Sysadmin or databases must be created and configured manually](#)

### **Restriction: The scanner server cannot have internet connectivity**

To support a disconnected computer, perform the following steps:

1. Configure your labels that apply classification only, or apply protection that uses [HYOK protection](#).

Without an internet connection, the scanner cannot apply protection, remove protection, or inspect protected files by using your organization's cloud-based key. Instead, the scanner is limited to using labels

that apply classification only, or apply protection that uses HYOK protection.

For more information, see [Support for disconnected computers](#).

2. Configure the scanner in the Azure portal, by creating a scanner cluster. If you need help with this step, see [Configure the scanner in the Azure portal](#).
3. Export your content job from the **Azure Information Protection - Content scan jobs** pane using the **Export** option.
4. In a PowerShell session, run [Import-AIPScannerConfiguration](#) and specify the file that contains the exported settings.

**Restriction: You cannot be granted Sysadmin or databases must be created and configured manually**

If you can be granted the Sysadmin role *temporarily* to install the scanner, you can remove this role when the scanner installation is complete.

Do one of the following, depending on your organization's requirements:

- **You can have the Sysadmin role temporarily.** If you temporarily have the Sysadmin role, the database is automatically created for you and the service account for the scanner is automatically granted the required permissions.

However, the user account that configures the scanner still requires the **db\_owner** role for the scanner configuration database. If you only have the Sysadmin role until the scanner installation is complete, [grant the db\\_owner role to the user account manually](#).

- **You cannot have the Sysadmin role at all.** If you cannot be granted the Sysadmin role even temporarily, you must ask a user with Sysadmin rights to manually create a database before you install the scanner.

For this configuration, the **db\_owner** role must be assigned to the following accounts:

- Service account for the scanner
- User account for the scanner installation
- User account for scanner configuration

Typically, you will use the same user account to install and configure the scanner. If you use different accounts, they both require the **db\_owner** role for the scanner configuration database. Create this user and rights as needed.

If you do not specify your own cluster (profile) name for the scanner, the configuration database is named **AIPScanner\_<computer\_name>**.

Continue with [creating a user and granting db\\_owner rights on the database](#).

Additionally:

- You must be a local administrator on the server that will run the scanner
- The service account that will run the scanner must be granted Full Control permissions to the following registry keys:
  - HKEY\_LOCAL\_MACHINE\SOFTWARE\WOW6432Node\Microsoft\MSIPC\Server
  - HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\MSIPC\Server

If, after configuring these permissions, you see an error when you install the scanner, the error can be ignored and you can manually start the scanner service.

**Populate the database manually**

Populate the database using the following script:

```
if not exists(select * from master.sys.server_principals where sid = SUSER_SID('domain\user')) BEGIN declare
@T nvarchar(500) Set @T = 'CREATE LOGIN ' + quotename('domain\user') + ' FROM WINDOWS ' exec(@T) END
```

#### Create a user and grant db\_owner rights manually

To create a user and grant db\_owner rights on this database, ask the Sysadmin to do the following:

1. Create a DB for scanner:

```
CREATE DATABASE AIPScannerUL_[clustername]

ALTER DATABASE AIPScannerUL_[clustername] SET TRUSTWORTHY ON
```

2. Grant rights to the user that runs the install command and is used to run scanner management commands.

SQL script:

```
if not exists(select * from master.sys.server_principals where sid = SUSER_SID('domain\user')) BEGIN
declare @T nvarchar(500) Set @T = 'CREATE LOGIN ' + quotename('domain\user') + ' FROM WINDOWS ' exec(@T)
END
USE DBName IF NOT EXISTS (select * from sys.database_principals where sid = SUSER_SID('domain\user'))
BEGIN declare @X nvarchar(500) Set @X = 'CREATE USER ' + quotename('domain\user') + ' FROM LOGIN ' +
quotename('domain\user'); exec sp_addrolemember 'db_owner', 'domain\user' exec(@X) END
```

3. Grant rights to scanner service account.

SQL script:

```
if not exists(select * from master.sys.server_principals where sid = SUSER_SID('domain\user')) BEGIN
declare @T nvarchar(500) Set @T = 'CREATE LOGIN ' + quotename('domain\user') + ' FROM WINDOWS ' exec(@T)
END
```

#### Restriction: The service account for the scanner cannot be granted the Log on locally right

If your organization policies prohibit the Log on locally right for service accounts, but allows the Log on as a batch job right, see [Specify and use the Token parameter for Set-AIPAuthentication](#).

#### Restriction: The scanner service account cannot be synchronized to Azure Active Directory but the server has internet connectivity

You can have one account to run the scanner service and use another account to authenticate to Azure Active Directory:

- For the scanner service account, use a local Windows account or an Active Directory account.
- For the Azure Active Directory account, specify and use the Token parameter for Set-AIPAuthentication.

## Next steps

Once you've confirmed that your system complies with the scanner prerequisites, continue with [Deploying the Azure Information Protection scanner to automatically classify and protect files](#).

For an overview about the scanner, see [Deploying the Azure Information Protection scanner to automatically classify and protect files](#).

#### More information:

Interested in how the Core Services Engineering and Operations team in Microsoft implemented this scanner? Read the technical case study: [Automating data protection with Azure Information Protection scanner](#).

You might be wondering: [What's the difference between Windows Server FCI and the Azure Information Protection scanner?](#)

You can also use PowerShell to interactively classify and protect files from your desktop computer. For more information about this and other scenarios that use PowerShell, see [Using PowerShell with the Azure Information Protection classic client](#)

# Configuring and installing the Azure Information Protection classic scanner

7/20/2020 • 15 minutes to read • [Edit Online](#)

Applies to: [Azure Information Protection](#), Windows Server 2019, Windows Server 2016, Windows Server 2012 R2

## NOTE

To provide a unified and streamlined customer experience, **Azure Information Protection client (classic)** and **Label Management** in the Azure Portal are being **deprecated** as of **March 31, 2021**. This time-frame allows all current Azure Information Protection customers to transition to our unified labeling solution using the Microsoft Information Protection Unified Labeling platform. Learn more in the official [deprecation notice](#).

If you're using the unified labeling scanner, see [Installing and configuring the Azure Information Protection unified labeling scanner](#).

Before you start configuring and installing the Azure Information Protection scanner, verify that your system complies with the [required prerequisites](#).

When you're ready, continue with the following steps:

1. [Configure the scanner in the Azure portal](#)
2. [Install the scanner](#)
3. [Get an Azure AD token for the scanner](#)
4. [Configure the scanner to apply classification and protection](#)

Perform the following additional configuration procedures as needed for your system:

| PROCEDURE                                                       | DESCRIPTION                                                                                                                                        |
|-----------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">Change which file types to protect</a>              | You may want to scan, classify, or protect different file types than the default. For more information, see <a href="#">AIP scanning process</a> . |
| <a href="#">Upgrading your scanner</a>                          | Upgrade your scanner to leverage the latest features and improvements.                                                                             |
| <a href="#">Editing data repository settings in bulk</a>        | Use import and export options to make changes in bulk for multiple data repositories.                                                              |
| <a href="#">Use the scanner with alternative configurations</a> | Use the scanner without configuring labels with any conditions                                                                                     |
| <a href="#">Optimize performance</a>                            | Guidance to optimize your scanner performance                                                                                                      |

For more information, see also [List of cmdlets for the scanner](#).

# Configure the scanner in the Azure portal

Before you install the scanner, or upgrade it from an older general availability version of the scanner, create a cluster and content scan job for the scanner in the Azure portal.

Then, configure the cluster and content scan job with scanner settings and the data repositories to scan.

To configure your scanner:

1. [Sign in to the Azure portal](#), and navigate to the **Azure Information Protection** pane.

For example, in the search box for resources, services, and docs: Start typing **Information** and select **Azure Information Protection**.

2. Locate the **Scanner** menu options, and select **Clusters**.
3. On the **Azure Information Protection - Clusters** pane, select **Add**:

The screenshot shows the 'Clusters' pane in the Azure Information Protection portal. At the top, there are several buttons: '+ Add' (highlighted with a red box), 'Refresh', 'Export', 'Delete', 'Scan now', and 'Rescan all files'. Below these are filter and search controls: a 'Search to filter items...' input field and a table header with columns: NAME, SCHED..., ENFORCE, REPOSIT..., NODES, LAST SC..., LAST SC..., and CURREN...'. The main table body displays the message 'No Scanner Profiles'.

4. On the **Add a new cluster** pane:
  - a. Specify a meaningful name for the scanner. This name is used to identify the scanner's configuration settings and the data repositories to scan.  
For example, you might specify **Europe** to identify the geographical location of the data repositories that your scanner will cover. When you later install or upgrade the scanner, you will need to specify the same cluster name.
  - b. Optionally, specify a description for administrative purposes, to help you identify the scanner's cluster name.
  - c. Select **Save**.
5. Locate the **Scanner** menu options, and select **Content scan jobs**.
6. On the **Azure Information Protection - Content scan jobs** pane, select **Add**.
7. For this initial configuration, configure the following settings, and then select **Save** but do not close the pane:

| SECTION                   | SETTINGS                                                                                                                                                                                                                                                                                                  |
|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Content scan job settings | <ul style="list-style-type: none"><li>- <b>Schedule:</b> Keep the default of <b>Manual</b></li><li>- <b>Info types to be discovered:</b> Change to <b>Policy only</b></li><li>- <b>Configure repositories:</b> Do not configure at this time because the content scan job must first be saved.</li></ul>  |
| Policy enforcement        | <ul style="list-style-type: none"><li>- <b>Enforce:</b> Select <b>Off</b></li><li>- <b>Label files based on content:</b> Keep the default of <b>On</b></li><li>- <b>Default label:</b> Keep the default of <b>Policy default</b></li><li>- <b>Relabel files:</b> Keep the default of <b>Off</b></li></ul> |

| SECTION                 | SETTINGS                                                                                                                                                                                                                                                                     |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Configure file settings | <ul style="list-style-type: none"> <li>- Preserve "Date modified", "Last modified" and "Modified by": Keep the default of On</li> <li>- File types to scan: Keep the default file types for Exclude</li> <li>- Default owner: Keep the default of Scanner Account</li> </ul> |
|                         |                                                                                                                                                                                                                                                                              |

8. Now that the content scan job is created and saved, you're ready to return to the **Configure repositories** option to specify the data stores to be scanned.

Specify UNC paths, and SharePoint Server URLs for SharePoint on-premises document libraries and folders.

**NOTE**

SharePoint Server 2019, SharePoint Server 2016, and SharePoint Server 2013 are supported for SharePoint. SharePoint Server 2010 is also supported when you have [extended support for this version of SharePoint](#).

To add your first data store, while on the **Add a new content scan job** pane, select **Configure repositories** to open the **Repositories** pane:

**Profile settings**

Schedule i

Manual     Always

Info types to be discovered i

Policy only     All

Configure repositories

0 repositories configured



9. On the **Repositories** pane, select **Add**:

**Repositories**

| Actions                                        |                               | Columns                       |                               |                        |
|------------------------------------------------|-------------------------------|-------------------------------|-------------------------------|------------------------|
| <input checked="" type="button"/> Add          | <input type="button"/> Export | <input type="button"/> Import | <input type="button"/> Delete | <input type="button"/> |
| <input type="text"/> Search to filter items... |                               |                               |                               |                        |
|                                                |                               | PATH                          | DEFAULT LABEL                 | ENFORCE                |
| No Scanner Repositories                        |                               |                               |                               |                        |

10. On the **Repository** pane, specify the path for the data repository, and then select **Save**.

For example:

- For a network share, use `\Server\Folder`.
- For a SharePoint library, use `http://sharepoint.contoso.com/Shared%20Documents/Folder`.

**NOTE**

Wildcards are not supported and WebDav locations are not supported.

Use the following syntax when adding SharePoint paths:

| PATH                                      | SYNTAX                                                                                                                                                                                                                                                                                                                                                                     |
|-------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Root path                                 | <pre>http://&lt;SharePoint server name&gt;</pre> <p>Scans all sites, including any site collections allowed for the scanner user.<br/>Requires <a href="#">additional permissions</a> to automatically discover root content</p>                                                                                                                                           |
| Specific SharePoint subsite or collection | <p>One of the following:</p> <ul style="list-style-type: none"> <li>- <pre>http://&lt;SharePoint server name&gt;/&lt;subsite name&gt;</pre></li> <li>- <pre>http://&lt;SharePoint server name&gt;/&lt;site collection name&gt;/&lt;site name&gt;</pre></li> </ul> <p>Requires <a href="#">additional permissions</a> to automatically discover site collection content</p> |
| Specific SharePoint library               | <p>One of the following:</p> <ul style="list-style-type: none"> <li>- <pre>http://&lt;SharePoint server name&gt;/&lt;library name&gt;</pre></li> <li>- <pre>http://&lt;SharePoint server name&gt;/.../&lt;library name&gt;</pre></li> </ul>                                                                                                                                |
| Specific SharePoint folder                | <pre>http://&lt;SharePoint server name&gt;/.../&lt;folder name&gt;</pre>                                                                                                                                                                                                                                                                                                   |

For the remaining settings on this pane, do not change them for this initial configuration, but keep them as **Content scan job default**. The default setting means that the data repository inherits the settings from the content scan job.

11. If you want to add another data repository, repeat steps 8 and 9.
12. Close the **Repositories** pane and the **content scan job** pane.

Back on the **Azure Information Protection - Content scan job** pane, your content scan name is displayed, together with the **SCHEDULE** column showing **Manual** and the **ENFORCE** column is blank.

You're now ready to install the scanner with the content scanner job that you've created. Continue with [Install the scanner](#).

## Install the scanner

After you've [configured the Azure Information Protection scanner in the Azure portal](#), perform the steps below to install the scanner:

1. Sign in to the Windows Server computer that will run the scanner. Use an account that has local administrator rights and that has permissions to write to the SQL Server master database.

### IMPORTANT

For more information, see [Prerequisites for installing and deploying the Azure Information Protection scanner](#).

2. Open a Windows PowerShell session with the **Run as an administrator** option.
3. Run the **Install-AIPScanner** cmdlet, specifying your SQL Server instance on which to create a database for the Azure Information Protection scanner, and the scanner cluster name that you specified in the preceding section:

```
Install-AIPScanner -SqlServerInstance <name> -Profile <cluster name>
```

Examples, using the profile name of **Europe**:

- For a default instance: `Install-AIPScanner -SqlServerInstance SQLSERVER1 -Profile Europe`
- For a named instance: `Install-AIPScanner -SqlServerInstance SQLSERVER1\AIPSCANNER -Profile Europe`
- For SQL Server Express:  
`Install-AIPScanner -SqlServerInstance SQLSERVER1\SQLEXPRESS -Profile Europe`

When you are prompted, provide the credentials for the scanner service account (`\<domain\user name>`) and password.

#### 4. Verify that the service is now installed by using **Administrative Tools > Services**.

The installed service is named **Azure Information Protection Scanner** and is configured to run by using the scanner service account that you created.

Now that you have installed the scanner, you need to [get an Azure AD token for the scanner](#) service account to authenticate, so that the scanner can run unattended.

## Get an Azure AD token for the scanner

An Azure AD token allows the scanner to authenticate to the Azure Information Protection service.

To get an Azure AD token:

1. Return to the Azure portal to create two Azure AD applications to specify an access token for authentication. This token lets the scanner run non-interactively.

For more information, see [How to label files non-interactively for Azure Information Protection](#).

2. From the Windows Server computer, if your scanner service account has been granted the **Log on locally** right for the installation, sign in with this account and start a PowerShell session.

Run [Set-AIPAuthentication](#), specifying the values that you copied from the previous step:

```
Set-AIPAuthentication -webAppId <ID of the "Web app / API" application> -webAppKey <key value generated in the "Web app / API" application> -nativeAppId <ID of the "Native" application>
```

When prompted, specify the password for your service account credentials for Azure AD, and then click **Accept**.

For example:

```
Set-AIPAuthentication -WebAppId "57c3c1c3-abf9-404e-8b2b-4652836c8c66" -WebAppKey "+LBkMvddz?Wr1NCK5v0e6_=meM59sSAn" -NativeAppId "8ef1c873-9869-4bb1-9c11-8313f9d7f76f").token | clip
Acquired application access token on behalf of the user
```

### TIP

If your scanner service account cannot be granted the **Log on locally** right, [Specify and use the Token parameter for Set-AIPAuthentication](#).

The scanner now has a token to authenticate to Azure AD, which is valid for one year, two years, or never,

according to your configuration of the **Web app /API** in Azure AD.

When the token expires, you must repeat steps 1 and 2.

You're now ready to run your first scan in discovery mode. For more information, see [Run a discovery cycle and view reports for the scanner](#).

If you've already run a discovery scan, continue with [Configure the scanner to apply classification and protection](#).

## Configure the scanner to apply classification and protection

The default settings configure the scanner to run once, and in reporting-only mode.

To change these settings, edit the content scan job:

1. In the Azure portal, on the **Azure Information Protection - Content scan jobs** pane, select the cluster and content scan job to edit it.
2. On the Content scan job pane, change the following, and then select **Save**:
  - From the **Content scan job** section: Change the **Schedule** to **Always**
  - From the **Policy enforcement** section: Change **Enforce** to **On**

### TIP

You may want to change other settings on this pane, such as whether file attributes are changed and whether the scanner can relabel files. Use the information popup help to learn more information about each configuration setting.

3. Make a note of the current time and start the scanner again from the **Azure Information Protection - Content scan jobs** pane:



Alternatively, run the following command in your PowerShell session:

```
Start-AIPScan
```

4. To view reports of files labeled, what classification was applied, and whether protection was applied, monitor the event log for the informational type **911** and the most recent time stamp.

Check reports for details, or use the Azure portal to find this information.

The scanner is now scheduled to run continuously. When the scanner works its way through all configured files, it automatically starts a new cycle so that any new and changed files are discovered.

## Change which file types to protect

By default, the AIP scanner protects Office file types and PDF files only. To change this behavior, such as to configure the scanner to protect all file types, just as the client does, or to protect specific additional file types, edit the registry as follows:

- Specify the additional file types that you want to be protected
- Specify the type of protection you want to apply (native or generic)

For more information, see [File API configuration](#) from the developer guidance. In this documentation for

developers, generic protection is referred to as "PFile".

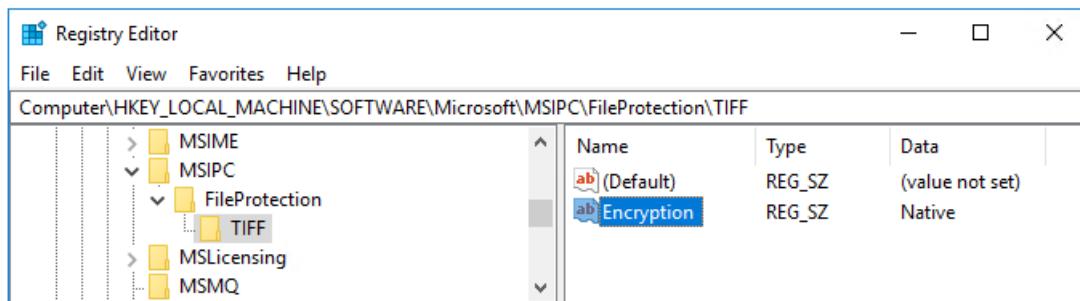
To align the supported file types with the client, where all files are automatically protected with native or generic protection:

1. Specify:

- The `*` wildcard as a registry key
- `Encryption` as the value (REG\_SZ)
- `Default` as the value data

2. Verify whether the **MSIPC** and **FileProtection** keys exist. Create them manually if they don't, and then create a subkey for each file name extension.

For example, for the scanner to protect TIFF images in addition to Office files and PDFs, the registry will look similar to the following after you've edited it:



**NOTE**

As an image file, TIFF files support native protection and the resulting file name extension is `.ptiff`.

For files that don't support native protection, specify the file name extension as a new key, and **PFile** for generic protection. The resulting file name extension for the protected file is `.pfile`.

For a list of text and images file types that similarly support native protection but must be specified in the registry, see [Supported file types for classification and protection](#).

## Upgrading your scanner

If you have previously installed the scanner and want to upgrade, see [Upgrading the Azure Information Protection scanner](#).

Then, [configure](#) and [use your scanner](#) as usual, skipping the steps to install your scanner.

**NOTE**

If you have a version of the scanner that is older than 1.48.204.0 and you're not ready to upgrade it, see [Deploying previous versions of the Azure Information Protection scanner to automatically classify and protect files](#).

## Editing data repository settings in bulk

Use the **Export** and **Import** buttons to make changes for your scanner across several repositories.

This way, you don't need to make the same changes several times, manually, in the Azure portal.

For example, if you have a new file type on several SharePoint data repositories, you may want to update the settings for those repositories in bulk.

To make changes in bulk across repositories:

1. In the Azure portal on the **Repositories** pane, select the **Export** option. For example:

The screenshot shows the 'Repositories' page in the Azure portal. At the top, there are four buttons: '+ Add', 'Export' (which is highlighted with a red box), 'Import', and 'Delete'. Below the buttons is a search bar with the placeholder 'Search to filter items...'. The main area contains a table with three columns: 'PATH', 'DEFAULT LABEL', and 'ENFORCE'. The 'PATH' column has a sorting arrow, and the other two columns have filtering icons.

2. Manually edit the exported file to make your change.
3. Use the **Import** option on the same page to import the updates back across your repositories.

## Using the scanner with alternative configurations

The Azure Information Protection scanner usually looks for conditions specified for your labels in order to classify and protect your content as needed.

In the following scenarios, the Azure Information Protection scanner is also able to scan your content and manage labels, without any conditions configured:

- [Apply a default label to all files in a data repository](#)
- [Identify all custom conditions and known sensitive information types](#)

### Apply a default label to all files in a data repository

In this configuration, all unlabeled files in the repository are labeled with the default label specified for the repository or the content scan job. Files are labeled without inspection.

Configure the following settings:

- **Label files based on content:** Set to Off
- **Default label:** Set to Custom, and then select the label to use

### Identify all custom conditions and known sensitive information types

This configuration enables you to find sensitive information that you might not realize you had, at the expense of scanning rates for the scanner.

Set the **Info types to be discovered** to All.

To identify conditions and information types for labeling, the scanner uses custom conditions specified for labels, and the list of information types available to specify for labels, as listed in the Azure Information Protection policy.

For more information, see [Quickstart: Find what sensitive information you have](#).

## Optimizing scanner performance

### NOTE

If you are looking to improve the responsiveness of the scanner computer rather than the scanner performance, use an advanced client setting to [limit the number of threads used by the scanner](#).

Use the following options and guidance to help you optimize scanner performance:

| OPTION                                                                                                    | DESCRIPTION                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-----------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Have a high speed and reliable network connection between the scanner computer and the scanned data store | <p>For example, place the scanner computer in the same LAN, or preferably, in the same network segment as the scanned data store.</p> <p>The quality of the network connection affects the scanner performance because, to inspect the files, the scanner transfers the contents of the files to the computer running the scanner service.</p> <p>Reducing or eliminating the network hops required for the data to travel also reduces the load on your network.</p> |
| Make sure the scanner computer has available processor resources                                          | <p>Inspecting the file contents and encrypting and decrypting files are processor-intensive actions.</p> <p>Monitor the typical scanning cycles for your specified data stores to identify whether a lack of processor resources is negatively affecting the scanner performance.</p>                                                                                                                                                                                 |
| Install multiple instances of the scanner                                                                 | <p>The Azure Information Protection scanner supports multiple configuration databases on the same SQL server instance when you specify a custom cluster (profile) name for the scanner.</p>                                                                                                                                                                                                                                                                           |
| Grant specific rights and disable low integrity level                                                     | <p>Confirm that the service account that runs the scanner has only the rights documented in <a href="#">Service account requirements</a>. Then, configure the <a href="#">advanced client setting</a> to disable the low integrity level for the scanner.</p>                                                                                                                                                                                                         |
| Check your alternative configuration usage                                                                | <p>The scanner runs more quickly when you use the <a href="#">alternative configuration</a> to apply a default label to all files because the scanner does not inspect the file contents.</p> <p>The scanner runs more slowly when you use the <a href="#">alternative configuration</a> to identify all custom conditions and known sensitive information types.</p>                                                                                                 |
| Decrease scanner timeouts                                                                                 | <p>Decrease the scanner timeouts with <a href="#">advanced client settings</a>. Decreased scanner timeouts provide better scanning rates and lower memory consumption.</p> <p><b>Note:</b> Decreasing scanner timeouts means that some files may be skipped.</p>                                                                                                                                                                                                      |
|                                                                                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

## Additional factors that affect performance

Additional factors that affect the scanner performance include:

| FACTOR                             | DESCRIPTION                                                                                                                                                                              |
|------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Load/response times                | The current load and response times of the data stores that contain the files to scan will also affect scanner performance.                                                              |
| Scanner mode (Discovery / Enforce) | <p>Discovery mode typically has a higher scanning rate than enforce mode.</p> <p>Discovery requires a single file read action, whereas enforce mode requires read and write actions.</p> |

| Factor              | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Policy changes      | <p>Your scanner performance may be affected if you've made changes to the conditions in the Azure Information Protection policy.</p> <p>Your first scan cycle, when the scanner must inspect every file, will take longer than subsequent scan cycles that by default, inspect only new and changed files.</p> <p>If you change the conditions, all files are scanned again. For more information, see <a href="#">Rescanning files</a>.</p>                                                     |
| Regex constructions | <p>Scanner performance is affected by how your regex expressions for custom conditions are constructed.</p> <p>To avoid heavy memory consumption and the risk of timeouts (15 minutes per file), review your regex expressions for efficient pattern matching.</p> <p>For example:</p> <ul style="list-style-type: none"> <li>- Avoid <a href="#">greedy quantifiers</a></li> <li>- Use non-capturing groups such as <code>(?:expression)</code> instead of <code>(expression)</code></li> </ul> |
| Log level           | <p>Log level options include <b>Debug</b>, <b>Info</b>, <b>Error</b> and <b>Off</b> for the scanner reports.</p> <ul style="list-style-type: none"> <li>- <b>Off</b> results in the best performance</li> <li>- <b>Debug</b> considerably slows down the scanner and should be used only for troubleshooting.</li> </ul> <p>For more information, see the <i>ReportLevel</i> parameter for the <a href="#">Set-AIPScannerConfiguration</a> cmdlet.</p>                                           |
| Files being scanned | <ul style="list-style-type: none"> <li>- With the exception of Excel files, Office files are more quickly scanned than PDF files.</li> <li>- Unprotected files are quicker to scan than protected files.</li> <li>- Large files obviously take longer to scan than small files.</li> </ul>                                                                                                                                                                                                       |
|                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

## List of cmdlets for the scanner

This section lists PowerShell cmdlets supported for the Azure Information Protection scanner.

### NOTE

The Azure Information Protection scanner is configured from the Azure portal. Therefore, cmdlets used in previous versions to configure data repositories and the scanned file types list are now deprecated.

Supported cmdlets for the scanner include:

- [Get-AIPScannerConfiguration](#)
- [Get-AIPScannerStatus](#)
- [Import-AIPScannerConfiguration](#)
- [Install-AIPScanner](#)
- [Set-AIPScanner](#)

- [Set-AIPScannerConfiguration](#)
- [Start-AIPScanDiagnostics](#)
- [Start-AIPScan](#)
- [Stop-AIPScan](#)
- [Uninstall-AIPScanner](#)
- [Update-AIPScanner](#)

## Next steps

Once you've installed and configured your scanner, start scanning your files.

See also: [Deploying the Azure Information Protection scanner to automatically classify and protect files](#).

### More information:

Interested in how the Core Services Engineering and Operations team in Microsoft implemented this scanner?

Read the technical case study: [Automating data protection with Azure Information Protection scanner](#).

You might be wondering: [What's the difference between Windows Server FCI and the Azure Information Protection scanner?](#)

You can also use PowerShell to interactively classify and protect files from your desktop computer. For more information about this and other scenarios that use PowerShell, see [Using PowerShell with the Azure Information Protection client](#).

# Running the Azure Information Protection classic scanner

7/20/2020 • 7 minutes to read • [Edit Online](#)

Applies to: [Azure Information Protection](#), Windows Server 2019, Windows Server 2016, Windows Server 2012 R2

## NOTE

To provide a unified and streamlined customer experience, **Azure Information Protection client (classic)** and **Label Management** in the Azure Portal are being **deprecated** as of **March 31, 2021**. This time-frame allows all current Azure Information Protection customers to transition to our unified labeling solution using the Microsoft Information Protection Unified Labeling platform. Learn more in the official [deprecation notice](#).

If you're working with the unified labeling scanner, see [Running the Azure Information Protection scanner](#).

Once you've confirmed your [system requirements](#) and [configured and installed](#) your scanner, [run a discovery scan](#) to get started.

Use other steps detailed below to manage your scans moving forward.

- [Stop a scan](#)
- [Rescanning files](#)
- [Troubleshooting a stopped scan](#)
- [Troubleshooting using the scanner diagnostic tool](#)
- [Scanner event log IDs and descriptions](#)

For more information, see [Deploying the Azure Information Protection scanner to automatically classify and protect files](#).

## Run a discovery cycle and view reports for the scanner

Use the following procedure after you've [configured and installed](#) your scanner to get an initial understanding of your content.

Perform these steps again as needed when your content changes.

1. In the Azure portal, on the **Azure Information Protection - Content scan jobs** pane, select your content scan jobs, and then select the **Scan now** option:



Alternatively, in your PowerShell session, run the following command:

```
Start-AIPScan
```

2. Wait for the scanner to complete its cycle. The scan completes when the scanner has crawled through all the files in the specified data stores.

Do any of the following to monitor scanner progress:

- Refresh the scan jobs. On the Azure Information Protection - Content scan jobs pane, select Refresh.

Wait until you see values for the LAST SCAN RESULTS column and the LAST SCAN (END TIME) column.

- Use a PowerShell command. Run `Get-AIPScannerStatus` to monitor the status change.

- Check Windows event logs. Check the local Windows Applications and Services event log, named **Azure Information Protection**.

This log also reports when the scanner has finished scanning, including a summary of results. Look for the informational event ID 911. For more information, see [Event log IDs and descriptions for the scanner](#).

3. When the scan is complete, review the reports stored in the `%localappdata%\Microsoft\MSIP\Scanner\Reports` directory.

- The .txt summary files include the time taken to scan, the number of scanned files, and how many files had a match for the information types.
- The .csv files have more details for each file. This folder stores up to 60 reports for each scanning cycle and all but the latest report is compressed to help minimize the required disk space.

[Initial configurations](#) instruct you to set the **Info types to be discovered to Policy only**. This configuration means that only files that meet the conditions you've configured for automatic classification are included in the detailed reports.

If you don't see any labels applied, check that your label configuration includes automatic rather than recommended classification, or enable **Treat recommended labeling as automatic** (available in scanner version 2.7.x.x and above).

If the results are still not as you expect, you might need to reconfigure the conditions that you specified for your labels. If that's the case, reconfigure the conditions as needed, and repeat this procedure until you are satisfied with the results. Then, update your configuration automatically, and optionally protection.

### **Viewing updates in the Azure portal**

Scanners send this information to Azure Information Protection every five minutes, so that you can view the results in near real time from the Azure portal. For more information, see [Reporting for Azure Information Protection](#).

The Azure portal displays information about the last scan only. If you need to see the results of previous scans, return to the reports that are stored on the scanner computer, in the `%localappdata%\Microsoft\MSIP\Scanner\Reports` folder.

### **Changing log levels or locations**

Change the level of logging by using the *ReportLevel* parameter with [Set-AIPScannerConfiguration](#).

The report folder location or name cannot be changed. If you want to store reports in a different location, consider using a directory junction for the folder.

For example, use the [Mklink](#) command:

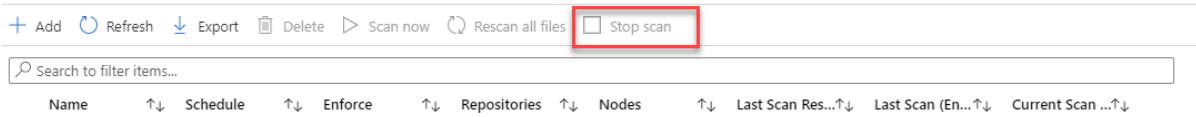
```
mklink /j D:\Scanner_reports C:\Users\aipscannersvc\AppData\Local\Microsoft\MSIP\Scanner\Reports
```

If you've performed these steps after an initial configuration and installation, continue with [Configure the scanner to apply classification and protection](#).

## Stopping a scan

To stop a currently running scan before it's complete, use one of the following methods:

- **Azure portal.** Select **Stop scan**:



- **Run a PowerShell command.** Run the following command:

```
Stop-AIPScan
```

## Rescanning files

For the [first scan cycle](#), the scanner inspects all files in the configured data stores. For subsequent scans, only new or modified files are inspected.

Inspecting all files again is typically useful when you want the reports to include all files, and when the scanner runs in discovery mode.

Run a new scan of all your files using one the following methods:

- [Manually run a full rescan](#)
- [Trigger a full rescan by refreshing the policy](#)

### Manually run a full rescan

Force the scanner to inspect all files again, as needed, from the **Azure Information Protection - Content scan jobs** pane in the Azure portal.

Select your content scan job from the list, and then select the **Rescan all files** option:



When a full scan is complete, the scan type automatically changes to incremental so that for subsequent scans, only new or modified files are scanned again.

### Trigger a full rescan by refreshing the policy

All files are also inspected in the following scenarios whenever the scanner downloads an Azure Information Protection policy that has new or changed conditions.

The scanner automatically refreshes the policy every hour, as well as each time the service starts and the policy is found to be over an hour old.

To refresh the policy sooner, such as while testing, manually delete the **Policy.msip** policy file from the **%LocalAppData%\Microsoft\MSIP** directory and restart the Azure Information Protection service.

#### NOTE

If you've also changed protection settings for your labels, wait an extra 15 minutes from when you saved the updated protection settings before restarting the Azure Information Protection service.

## Troubleshooting a stopped scan

If the scanner stops in the middle unexpectedly, and doesn't complete scanning a large number of files in a repository, you may need to modify one of the following settings:

- **Number of dynamic ports.** You may need to increase the number of dynamic ports for the operating system hosting the files. Server hardening for SharePoint can be one reason why the scanner exceeds the number of allowed network connections, and therefore stops.

To check whether this is the cause of the scanner stopping, look to see if the following error message is logged for the scanner in the `%localappdata%\Microsoft\MSIP\Logs\MSIPScanner.iplog` file.

**Unable to connect to the remote server ---> System.Net.Sockets.SocketException: Only one usage of each socket address (protocol/network address/port) is normally permitted IP:port**

### NOTE

This file will be zipped if there are multiple logs.

For more information about how to view the current port range and increase the range, see [Settings that can be Modified to Improve Network Performance](#).

- **List view threshold.** For large SharePoint farms, you may need to increase the list view threshold. By default, the list view threshold is set to 5,000.

For more information, see [Manage large lists and libraries in SharePoint](#).

## Troubleshooting using the scanner diagnostic tool

If you're having issues with the Azure Information Scanner, verify whether your deployment is healthy using the following PowerShell command:

```
Start-AIPScannerDiagnostics
```

The diagnostics tool checks the following details and then exports a log file with the results:

- Whether the database is up to date
- Whether network URLs are accessible
- Whether there's a valid authentication token and the policy can be acquired
- Whether the profile is defined in the Azure portal
- Whether offline/online configuration exists and can be acquired
- Whether the rules configured are valid

### TIP

If you are running the command under a user that is not the scanner user, be sure to add the `-OnBehalf` parameter.

### NOTE

The `Start-AIPScannerDiagnostics` tool does not run a full prerequisites check. If you're having issues with the scanner, also ensure that your system complies with [scanner requirements](#), and that your [scanner configuration and installation](#) is complete.

## Event log IDs and descriptions for the scanner

The following AIP scanner log events are stored in the Windows Applications and Services event log named **Azure Information Protection**.

| EVENT ID | ACTIVITY               | DESCRIPTION                                                                                                          |
|----------|------------------------|----------------------------------------------------------------------------------------------------------------------|
| 910      | Scanner cycle started  | Logged when the scanner service is started and begins to scan for files in the data repositories that you specified. |
| 911      | Scanner cycle finished | Logged when the scanner has finished a manual scan, or the scanner has finished a cycle for a continuous schedule.   |
|          |                        |                                                                                                                      |

### TIP

If the scanner was configured to run manually rather than continuously, to scan the files again, set the **Schedule to Manual** or **Always** in the content scan job, and then restart the service. For more information, see [Rescanning files](#).

## Next steps

- Interested in how the Core Services Engineering and Operations team in Microsoft implemented this scanner? Read the technical case study: [Automating data protection with Azure Information Protection scanner](#).
- You might be wondering: [What's the difference between Windows Server FCI and the Azure Information Protection scanner?](#)
- You can also use PowerShell to interactively classify and protect files from your desktop computer. For more information about this and other scenarios that use PowerShell, see [Using PowerShell with the Azure Information Protection client](#).

# Central reporting for Azure Information Protection (public preview)

7/20/2020 • 14 minutes to read • [Edit Online](#)

*Applies to:* [Azure Information Protection](#)

Use Azure Information Protection analytics for central reporting to help you track the adoption of your labels that classify and protect your organization's data. In addition:

- Monitor labeled and protected documents and emails across your organization
- Identify documents that contain sensitive information within your organization
- Monitor user access to labeled documents and emails, and track document classification changes.
- Identify documents that contain sensitive information that might be putting your organization at risk if they are not protected, and mitigate your risk by following recommendations.
- Identify when protected documents are accessed by internal or external users from Windows computers, and whether access was granted or denied.

The data that you see is aggregated from your Azure Information Protection clients and scanners, from Microsoft Cloud App Security, from Windows 10 computers using Microsoft Defender Advanced Threat Protection, and from [protection usage logs](#).

For example, you'll be able to see the following:

- From the **Usage report**, where you can select a time period:
  - Which labels are being applied
  - How many documents and emails are being labeled
  - How many documents and emails are being protected
  - How many users and how many devices are labeling documents and emails
  - Which applications are being used for labeling
- From the **Activity logs**, where you can select a time period:
  - Which files previously discovered by scanner were deleted from the scanned repository
  - What labeling actions were performed by a specific user
  - What labeling actions were performed from a specific device
  - Which users have accessed a specific labeled document
  - What labeling actions were performed for a specific file path
  - What labeling actions were performed by a specific application, such File Explorer and right-click, PowerShell, the scanner, or Microsoft Cloud App Security
  - Which protected documents were accessed successfully by users or denied access to users, even if those users don't have the Azure Information Protection client installed or are outside your

- organization
  - Drill down into reported files to view **Activity Details** for additional information
- From the **Data discovery** report:
  - What files are on your scanned data repositories, Windows 10 computers, or computers running the Azure Information Protection clients
  - Which files are labeled and protected, and the location of files by labels
  - Which files contain sensitive information for known categories, such as financial data and personal information, and the location of files by these categories
- From the **Recommendations** report:
  - Identify unprotected files that contain a known sensitive information type. A recommendation lets you immediately configure the corresponding condition for one of your labels to apply automatic or recommended labeling.

If you follow the recommendation: The next time the files are opened by a user or scanned by the Azure Information Protection scanner, the files can be automatically classified and protected.
  - Which data repositories have files with identified sensitive information but are not being scanned by the Azure Information Protection. A recommendation lets you immediately add the identified data store to one of your scanner's profiles.

If you follow the recommendation: On the next scanner cycle, the files can be automatically classified and protected.

The reports use [Azure Monitor](#) to store the data in a Log Analytics workspace that your organization owns. If you're familiar with the query language, you can modify the queries, and create new reports and Power BI dashboards. You might find the following tutorial helpful to understand the query language: [Get started with Azure Monitor log queries](#).

For more information, read the following blog posts:

- [Data discovery, reporting and analytics for all your data with Microsoft Information Protection](#)
- [Discover and protect sensitive data through Azure Information Protection and Microsoft Defender ATP](#)

### **Information collected and sent to Microsoft**

To generate these reports, endpoints send the following types of information to Microsoft:

- The label action. For example, set a label, change a label, add or remove protection, automatic and recommended labels.
- The label name before and after the label action.
- Your organization's tenant ID.
- The user ID (email address or UPN).
- The name of the user's device.
- For documents: The file path and file name of documents that are labeled.
- For emails: The email subject and email sender for emails that are labeled.
- The sensitive information types ([predefined](#) and custom) that were detected in content.
- The Azure Information Protection client version.

- The client operating system version.

This information is stored in an Azure Log Analytics workspace that your organization owns and can be viewed independently from Azure Information Protection by users who have access rights to this workspace.

For more details, see:

- [Permissions required for Azure Information Protection analytics](#)
- [Manage access to Log Analytics Workspace using Azure permissions](#)
- [Azure Information Protection audit log reference](#)

To prevent Azure Information Protection clients (classic) from sending this data, set the [policy setting](#) of **Send audit data to Azure Information Protection analytics** to **Off**:

- For most users to send this data and a subset of users cannot send auditing data:
  - Set **Send audit data to Azure Information Protection analytics** to **Off** in a scoped policy for the subset of users. This configuration is typical for production scenarios.
- For only a subset of users to send auditing data:
  - Set **Send audit data to Azure Information Protection analytics** to **Off** in the global policy, and **On** in a scoped policy for the subset of users. This configuration is typical for testing scenarios.

To prevent Azure Information Protection unified clients from sending this data, configure a label policy [advanced setting](#).

#### **Content matches for deeper analysis**

Azure Information Protection lets you collect and store the actual data that's identified as being a sensitive information type (predefined or custom). For example, this can include credit card numbers that are found, as well as social security numbers, passport numbers, and bank account numbers. The content matches are displayed when you select an entry from **Activity logs**, and view the **Activity Details**.

By default, Azure Information Protection clients don't send content matches. To change this behavior so that content matches are sent:

- For the classic client, select a checkbox as part of the [configuration](#) for Azure Information Protection analytics. The checkbox is named **Enable deeper analytics into your sensitive data**.

If you want most users who are using this client to send content matches but a subset of users cannot send content matches, select the checkbox and then configure an [advanced client setting](#) in a scoped policy for the subset of users.

- For the unified labeling client, configure an [advanced setting](#) in a label policy.

## Prerequisites

To view the Azure Information Protection reports and create your own, make sure that the following requirements are in place.

| REQUIREMENT                                                                                                       | MORE INFORMATION                                                                                                                                                                                             |
|-------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| An Azure subscription that includes Log Analytics and that is for the same tenant as Azure Information Protection | <p>See the <a href="#">Azure Monitor pricing</a> page.</p> <p>If you don't have an Azure subscription or you don't currently use Azure Log Analytics, the pricing page includes a link for a free trial.</p> |

| Requirement                                                                                                                                                 | More Information                                                                                                                                                                                        |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| For reporting information from labeling clients:<br>- Azure Information Protection clients                                                                  | Both the unified labeling client and the classic client are supported.<br><br>If not already installed, you can download and install these clients from the <a href="#">Microsoft Download Center</a> . |
| For reporting information from cloud-based data stores:<br>- Microsoft Cloud App Security                                                                   | To display information from Microsoft Cloud App Security, configure <a href="#">Azure Information Protection integration</a> .                                                                          |
| For reporting information from on-premises data stores:<br>- Azure Information Protection scanner                                                           | For installation instructions for the scanner, see <a href="#">Deploying the Azure Information Protection scanner to automatically classify and protect files</a> .                                     |
| For reporting information from Windows 10 computers:<br>- Minimum build of 1809 with Microsoft Defender Advanced Threat Protection (Microsoft Defender ATP) | You must enable the Azure Information Protection integration feature from Microsoft Defender Security Center. For more information, see <a href="#">Information protection in Windows overview</a> .    |

### Permissions required for Azure Information Protection analytics

Specific to Azure Information Protection analytics, after you have configured your Azure Log Analytics workspace, you can use the Azure AD administrator role of Security Reader as an alternative to the other Azure AD roles that support managing Azure Information Protection in the Azure portal. This additional role is supported only if your tenant isn't on the [unified labeling platform](#).

Because Azure Information Protection analytics uses Azure Monitoring, role-based access control (RBAC) for Azure also controls access to your workspace. You therefore need an Azure role as well as an Azure AD administrator role to manage Azure Information Protection analytics. If you're new to Azure roles, you might find it useful to read [Differences between Azure RBAC roles and Azure AD administrator roles](#).

Details:

- One of the following [Azure AD administrator roles](#) to access the Azure Information Protection analytics pane:
  - To create your Log Analytics workspace or to create custom queries:
    - Azure Information Protection administrator**
    - Security administrator**
    - Compliance administrator**
    - Compliance data administrator**
    - Global administrator**
  - After the workspace has been created, you can then use the following roles with fewer permissions to view the data collected:
    - Security reader**
    - Global reader**
- In addition, you need one of the following [Azure Log Analytics roles](#) or standard [Azure roles](#) to access your Azure Log Analytics workspace:
  - To create the workspace or to create custom queries, one of the following:
    - Log Analytics Contributor**
    - Contributor**

- Owner
- After the workspace has been created, you can then use one of the following roles with fewer permissions to view the data collected:
  - Log Analytics Reader
  - Reader

#### **Minimum roles to view the reports**

After you have configured your workspace for Azure Information Protection analytics, the minimum roles needed to view the Azure Information Protection analytics reports are both of the following:

- Azure AD administrator role: **Security reader**
- Azure role: **Log Analytics Reader**

However, a typical role assignment for many organizations is the Azure AD role of **Security reader** and the Azure role of **Reader**.

#### **Storage requirements and data retention**

The amount of data collected and stored in your Azure Information Protection workspace will vary significantly for each tenant, depending on factors such as how many Azure Information Protection clients and other supported endpoints you have, whether you're collecting endpoint discovery data, you've deployed scanners, the number of protected documents that are accessed, and so on.

However, as a starting point, you might find the following estimates useful:

- For audit data generated by Azure Information Protection clients only: 2 GB per 10,000 active users per month.
- For audit data generated by Azure Information Protection clients, scanners, and Microsoft Defender ATP: 20 GB per 10,000 active users per month.

If you use mandatory labeling or you've configured a default label for most users, your rates are likely to be significantly higher.

Azure Monitor Logs has a **Usage and estimated costs** feature to help you estimate and review the amount of data stored, and you can also control the data retention period for your Log Analytics workspace. For more information, see [Manage usage and costs with Azure Monitor Logs](#).

## **Configure a Log Analytics workspace for the reports**

1. If you haven't already done so, open a new browser window and [sign in to the Azure portal](#) with an account that has the [permissions required for Azure Information Protection analytics](#). Then navigate to the **Azure Information Protection** pane.

For example, in the search box for resources, services, and docs: Start typing **Information** and select **Azure Information Protection**.

2. Locate the **Manage** menu options, and select **Configure analytics (Preview)**.
3. On the **Azure Information Protection log analytics** pane, you see a list of any Log Analytics workspaces that are owned by your tenant. Do one of the following:
  - To create a new Log Analytics workspace: Select **Create new workspace**, and on the **Log analytics workspace** pane, supply the requested information.
  - To use an existing Log Analytics workspace: Select the workspace from the list.

If you need help with creating the Log Analytics workspace, see [Create a Log Analytics workspace in the Azure portal](#).

[Azure portal](#).

4. If you have Azure Information Protection clients (classic), select the checkbox **Enable deeper analytics into your sensitive data** if you want to store the actual data that's identified as being a sensitive information type. For more information about this setting, see the [Content matches for deeper analysis](#) section on this page.
5. Select **OK**.

You're now ready to view the reports.

## How to view the reports

From the Azure Information Protection pane, locate the **Dashboards** menu options, and select one of the following options:

- **Usage report (Preview)**: Use this report to see how your labels are being used.
- **Activity logs (Preview)**: Use this report to see labeling actions from users, and on devices and file paths. In addition, for protected documents, you can see access attempts (successful or denied) for users both inside and outside your organization, even if they don't have the Azure Information Protection client installed  
  
This report has a **Columns** option that lets you display more activity information than the default display. You can also see more details about a file by selecting it to display **Activity Details**.
- **Data discovery (Preview)**: Use this report to see information about labeled files found by scanners and supported endpoints.

Tip: From the information collected, you might find users accessing files that contain sensitive information from location that you didn't know about or aren't currently scanning:

- If the locations are on-premises, consider adding the locations as additional data repositories for the Azure Information Protection scanner.
- If the locations are in the cloud, consider using Microsoft Cloud App Security to manage them.
- **Recommendations (Preview)**: Use this report to identify files that have sensitive information and mitigate your risk by following the recommendations.

When you select an item, the **View data** option displays the audit activities that triggered the recommendation.

## How to modify the reports and create custom queries

Select the query icon in the dashboard to open a **Log Search** pane:



The logged data for Azure Information Protection is stored in the following table:

**InformationProtectionLogs\_CL**

When you create your own queries, use the friendly schema names that have been implemented as **InformationProtectionEvents** functions. These functions are derived from the attributes that are supported for custom queries (some attributes are for internal use only) and their names will not change over time, even if the underlying attributes change for improvements and new functionality.

### Friendly schema reference for event functions

Use the following table to identify the friendly name of event functions that you can use for custom queries

with Azure Information Protection analytics.

| COLUMN NAME        | DESCRIPTION                                                                                                                                                                |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Time               | Event time: UTC in format YYYY-MM-DDTHH:MM:SS                                                                                                                              |
| User               | User: Format UPN or DOMAIN\USER                                                                                                                                            |
| ItemPath           | Full item path or email subject                                                                                                                                            |
| ItemName           | File name or email subject                                                                                                                                                 |
| Method             | Label assigned method: Manual, Automatic, Recommended, Default, or Mandatory                                                                                               |
| Activity           | Audit activity: DowngradeLabel, UpgradeLabel, RemoveLabel, NewLabel, Discover, Access, RemoveCustomProtection, ChangeCustomProtection, NewCustomProtection, or FileRemoved |
| ResultStatus       | Result status of the action:<br><br>Succeeded or Failed (reported by AIP scanner only)                                                                                     |
| ErrorMessage_s     | Includes Error message details if ResultStatus=Failed.<br>Reported by AIP scanner only                                                                                     |
| LabelName          | Label name (not localized)                                                                                                                                                 |
| LabelNameBefore    | Label name before change (not localized)                                                                                                                                   |
| ProtectionType     | Protection type [JSON]<br>{<br>"Type": ["Template", "Custom", "DoNotForward"],<br>"TemplateID": "GUID"<br>}                                                                |
| ProtectionBefore   | Protection type before change [JSON]                                                                                                                                       |
| MachineName        | FQDN when available; otherwise host name                                                                                                                                   |
| DeviceRisk         | Device risk score from WDATP when available                                                                                                                                |
| Platform           | Device platform (Win, OSX, Android, iOS)                                                                                                                                   |
| ApplicationName    | Application friendly name                                                                                                                                                  |
| AIPVersion         | Version of the Azure Information Protection client that performed the audit action                                                                                         |
| TenantId           | Azure AD tenant ID                                                                                                                                                         |
| AzureApplicationId | Azure AD registered application ID (GUID)                                                                                                                                  |
| ProcessName        | Process that hosts MIP SDK                                                                                                                                                 |

| COLUMN NAME                | DESCRIPTION                                                                                                                                                                                            |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| LabelId                    | Label GUID or null                                                                                                                                                                                     |
| IsProtected                | Whether protected: Yes/No                                                                                                                                                                              |
| ProtectionOwner            | Rights Management owner in UPN format                                                                                                                                                                  |
| LabelIdBefore              | Label GUID or null before change                                                                                                                                                                       |
| InformationTypesAbove55    | JSON array of <a href="#">SensitiveInformation</a> found in data with confidence level 55 or above                                                                                                     |
| InformationTypesAbove65    | JSON array of <a href="#">SensitiveInformation</a> found in data with confidence level 65 or above                                                                                                     |
| InformationTypesAbove75    | JSON array of <a href="#">SensitiveInformation</a> found in data with confidence level 75 or above                                                                                                     |
| InformationTypesAbove85    | JSON array of <a href="#">SensitiveInformation</a> found in data with confidence level 85 or above                                                                                                     |
| InformationTypesAbove95    | JSON array of <a href="#">SensitiveInformation</a> found in data with confidence level 95 or above                                                                                                     |
| DiscoveredInformationTypes | JSON array of <a href="#">SensitiveInformation</a> found in data and their matched content (if enabled) where an empty array means no information types found, and null means no information available |
| ProtectedBefore            | Whether the content was protected before change: Yes/No                                                                                                                                                |
| ProtectionOwnerBefore      | Rights Management owner before change                                                                                                                                                                  |
| UserJustification          | Justification when downgrading or removing label                                                                                                                                                       |
| LastModifiedBy             | User in UPN format who last modified the file. Available for Office and SharePoint only                                                                                                                |
| LastModifiedDate           | UTC in format YYYY-MM-DDTHH:MM:SS: Available for Office and SharePoint only                                                                                                                            |

#### Examples using InformationProtectionEvents

Use the following examples to see how you might use the friendly schema to create custom queries.

**Example 1:** Return all users who sent audit data in the last 31 days

```
InformationProtectionEvents
| where Time > ago(31d)
| distinct User
```

**Example 2:** Return the number of labels that were downgraded per day in the last 31 days

```
InformationProtectionEvents
| where Time > ago(31d)
| where Activity == "DowngradeLabel"
| summarize Label_Downgrades_per_Day = count(Activity) by bin(Time, 1d)
```

Example 3: Return the number of labels that were downgraded from Confidential by user, in the last 31 days

```
InformationProtectionEvents
| where Time > ago(31d)
| where Activity == "DowngradeLabel"
| where LabelNameBefore contains "Confidential" and LabelName !contains "Confidential"
| summarize Label_Downgrades_by_User = count(Activity) by User | sort by Label_Downgrades_by_User desc
```

In this example, a downgraded label is counted only if the label name before the action contained the name **Confidential** and the label name after the action didn't contain the name of **Confidential**.

## Next steps

After reviewing the information in the reports, if you are using the Azure Information Protection client, you might decide to make changes to your Azure Information Protection policy. For instructions, see [Configuring the Azure Information Protection policy](#).

If you have a Microsoft 365 subscription, you can also view label usage in the Microsoft 365 compliance center and Microsoft 365 security center. For more information, see [View label usage with label analytics](#).

# Deploying the Azure Rights Management connector

7/20/2020 • 5 minutes to read • [Edit Online](#)

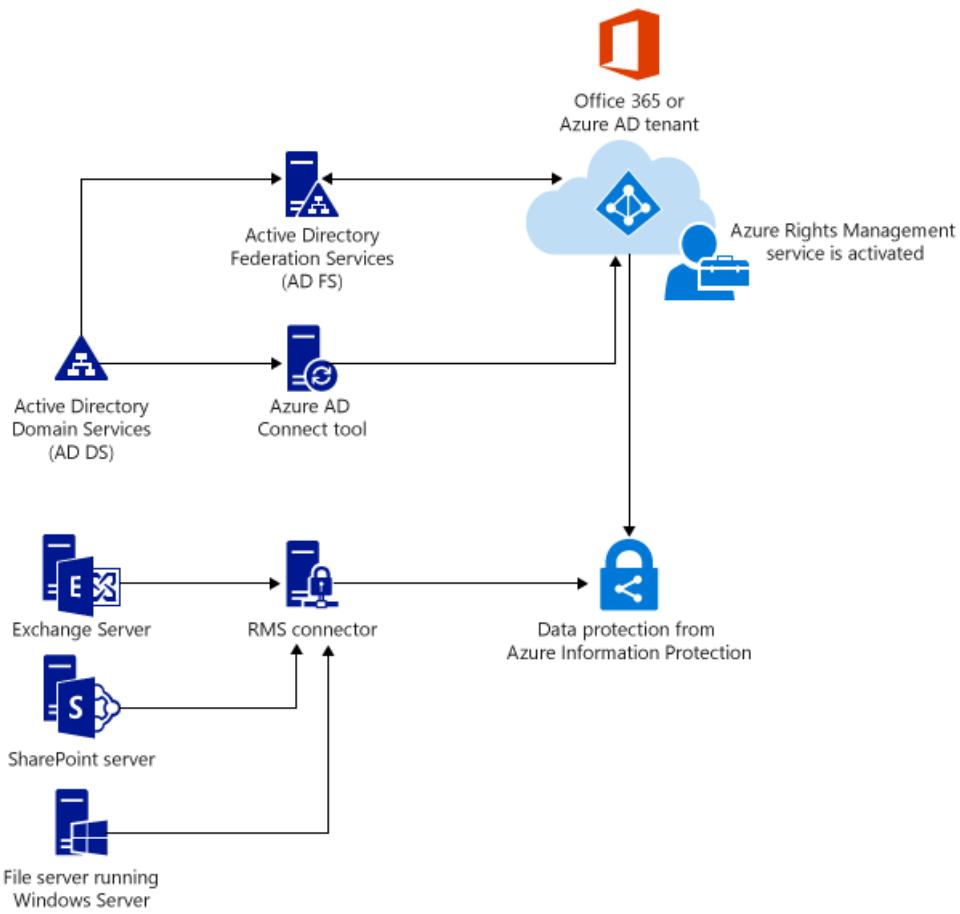
*Applies to: Azure Information Protection, Windows Server 2019, 2016, Windows Server 2012 R2, Windows Server 2012*

Use this information to learn about the Azure Rights Management connector, and then how to successfully deploy it for your organization. This connector provides data protection for existing on-premises deployments that use Microsoft Exchange Server, SharePoint Server, or file servers that run Windows Server and File Classification Infrastructure (FCI).

## Overview of the Microsoft Rights Management connector

The Microsoft Rights Management (RMS) connector lets you quickly enable existing on-premises servers to use their Information Rights Management (IRM) functionality with the cloud-based Microsoft Rights Management service (Azure RMS). With this functionality, IT and users can easily protect documents and pictures both inside your organization and outside, without having to install additional infrastructure or establish trust relationships with other organizations.

The RMS connector is a small-footprint service that you install on-premises, on servers that run Windows Server 2016, Windows Server 2012 R2, Windows Server 2012. In addition to running the connector on physical computers, you can also run it on virtual machines, including Azure IaaS VMs. After you deploy the connector, it acts as a communications interface (a relay) between the on-premises servers and the cloud service, as shown in the following picture. The arrows indicate the direction in which network connections are initiated.



### On-premises servers supported

The RMS connector supports the following on-premises servers: Exchange Server, SharePoint Server, and file servers that run Windows Server and use File Classification Infrastructure to classify and apply policies to Office documents in a folder.

#### NOTE

If you want to protect multiple file types (not just Office documents) by using File Classification Infrastructure, do not use the RMS connector, but instead, use the [AzureInformationProtection cmdlets](#).

For the versions of these on-premises servers that are supported by the RMS connector, see [On-premises servers that support Azure RMS](#).

### Support for hybrid scenarios

You can use the RMS connector even if some of your users are connecting to online services, in a hybrid scenario. For example, some users' mailboxes use Exchange Online and some users' mailboxes use Exchange Server. After you install the RMS connector, all users can protect and consume emails and attachments by using Azure RMS, and information protection works seamlessly between the two deployment configurations.

### Support for customer-managed keys (BYOK)

If you manage your own tenant key for Azure RMS (the bring your own key, or BYOK scenario), the RMS connector and the on-premises servers that use it do not access the hardware security module (HSM) that contains your tenant key. This is because all cryptographic operations that use the tenant key are performed in Azure RMS, and not on-premises.

If you want to learn more about this scenario where you manage your tenant key, see [Planning and implementing your Azure Information Protection tenant key](#).

## Prerequisites for the RMS connector

Before you install the RMS connector, make sure that the following requirements are in place.

| Requirement                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | More Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| The protection service is activated                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | <p><a href="#">Activating the protection service from Azure Information Protection</a></p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Directory synchronization between your on-premises Active Directory forests and Azure Active Directory                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | <p>After RMS is activated, Azure Active Directory must be configured to work with the users and groups in your Active Directory database.</p> <p><b>Important:</b> You must do this directory synchronization step for the RMS connector to work, even for a test network. Although you can use Office 365 and Azure Active Directory by using accounts that you manually create in Azure Active Directory, this connector requires that the accounts in Azure Active Directory are synchronized with Active Directory Domain Services; manual password synchronization is not sufficient.</p> <p>For more information, see the following resources:</p> <ul style="list-style-type: none"><li>- <a href="#">Integrate on-premises Active Directory domains with Azure Active Directory</a></li><li>- <a href="#">Hybrid Identity directory integration tools comparison</a></li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| A minimum of two member computers on which to install the RMS connector: <ul style="list-style-type: none"><li>- A 64-bit physical or virtual computer running one of the following operating systems: Windows Server 2016, Windows Server 2012 R2, Windows Server 2012.</li><li>- At least 1 GB of RAM.</li><li>- A minimum of 64 GB of disk space.</li><li>- At least one network interface.</li><li>- Access to the internet via a firewall (or web proxy) that does not require authentication.</li><li>- Must be in a forest or domain that trusts other forests in the organization that contain installations of Exchange or SharePoint servers that you want to use with the RMS connector.</li></ul> | <p>For fault tolerance and high availability, you must install the RMS connector on a minimum of two computers.</p> <p><b>Tip:</b> If you are using Outlook Web Access or mobile devices that use Exchange ActiveSync IRM and it is critical that you maintain access to emails and attachments that are protected by Azure RMS, we recommend that you deploy a load-balanced group of connector servers to ensure high availability.</p> <p>You do not need dedicated servers to run the connector but you must install it on a separate computer from the servers that will use the connector.</p> <p><b>Important:</b> Do not install the connector on a computer that runs Exchange Server, SharePoint Server, or a file server that is configured for file classification infrastructure if you want to use the functionality from these services with Azure RMS. Also, do not install this connector on a domain controller.</p> <p>If you have server workloads that you want to use with the RMS connector but their servers are in domains that are not trusted by the domain from which you want to run the connector, you can install additional RMS connector servers in these untrusted domains or other domains in their forest.</p> <p>There is no limit to the number of connector servers that you can run for your organization and all connector servers installed in an organization share the same configuration. However, to configure the connector to authorize servers, you must be able to browse for the server or service accounts you want to authorize, which means that you must run the RMS administration tool in a forest from which you can browse those accounts.</p> |

# Steps to deploy the RMS connector

The connector does not automatically check all the [prerequisites](#) that it needs for a successful deployment, so make sure that these are in place before you start. The deployment requires you to install the connector, configure the connector, and then configure the servers that you want to use the connector.

- [Step 1: Installing the RMS connector](#)
- [Step 2: Entering credentials](#)
- [Step 3: Authorizing servers to use the RMS connector](#)
- [Step 4: Configuring load balancing and high availability](#)
- Optional: [Configuring the RMS connector to use HTTPS](#)
- Optional: [Configuring the RMS connector for a web proxy server](#)
- Optional: [Installing the RMS connector administration tool on administrative computers](#)
- [Step 5: Configuring servers to use the RMS connector](#)
  - [Configuring an Exchange server to use the connector](#)
  - [Configuring a SharePoint server to use the connector](#)
  - [Configuring a file server for File Classification Infrastructure to use the connector](#)

## Next steps

Go to Step 1: [Installing and configuring the Azure Rights Management connector](#).

# Installing and configuring the Azure Rights Management connector

7/20/2020 • 13 minutes to read • [Edit Online](#)

Applies to: [Azure Information Protection](#), Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Use the following information to help you install and configure the Azure Rights Management (RMS) connector. These procedures cover steps 1 through 4 from [Deploying the Azure Rights Management connector](#).

Before you begin, make sure that you have reviewed and checked the [prerequisites](#) for this deployment.

## Installing the RMS connector

1. Identify the computers (minimum of two) to run the RMS connector. These computers must meet the minimum specification listed in the [prerequisites](#).

### NOTE

You install a single RMS connector (consisting of multiple servers for high availability) per tenant (Office 365 tenant or Azure AD tenant). Unlike Active Directory RMS, you do not have to install an RMS connector in each forest.

2. Download the source files for the RMS connector from the [Microsoft Download Center](#).

To install the RMS connector, download RMSConnectorSetup.exe.

In addition:

- If you later want to configure the connector from a 32-bit computer, also download RMSConnectorAdminToolSetup\_x86.exe.
  - If you want to use the server configuration tool for the RMS connector, to automate the configuration of registry settings on your on-premises servers, also download GenConnectorConfig.ps1.
3. On the computer on which you want to install the RMS connector, run **RMSConnectorSetup.exe** with administrator privileges.
  4. On the Welcome page of Microsoft Rights Management Connector Setup, select **Install Microsoft Rights Management connector on the computer**, and then click **Next**.
  5. Read and agree to the RMS connector license terms, and then click **Next**.

To continue, enter an account and password to configure the RMS connector.

## Entering credentials

Before you can configure the RMS connector, you must enter credentials for an account that has sufficient privileges to configure the RMS connector. For example, you might type **admin@contoso.com** and then specify the password for this account.

This account must not require multi-factor authentication (MFA) because Microsoft Rights Management Connector Setup does not support MFA. In addition, if you use Azure AD Conditional Access, do not [block legacy](#)

[authentication](#) for this account.

The connector setup also has some character restrictions for this password. You cannot use a password that has any of the following characters: Ampersand ( & ); left angle bracket ( [ ); right angle bracket ( ] ); straight quotation ( " ); and apostrophe ( ' ). If your password has any of these characters, authentication fails for the RMS connector setup and you see the error message **That user name and password combination is not correct**, even though you can successfully sign in using this account and password for other scenarios. If this scenario applies to your password, either use a different account with a password that does not have any of these special characters, or reset your password so it doesn't have any of these special characters.

In addition, if you have implemented [onboarding controls](#), make sure that the account you specify is able to protect content. For example, if you restricted the ability to protect content to the "IT department" group, the account that you specify here must be a member of that group. If not, you see the error message: **The attempt to discover the location of the administration service and organization failed. Make sure Microsoft Rights Management service is enabled for your organization.**

You can use an account that has one of the following privileges:

- **Global administrator for your tenant:** An account that is a global administrator for your Office 365 tenant or Azure AD tenant.
- **Azure Rights Management global administrator:** An account in Azure Active Directory that has been assigned the Azure RMS global administrator role.
- **Azure Rights Management connector administrator:** An account in Azure Active Directory that has been granted rights to install and administer the RMS connector for your organization.

## NOTE

The Azure Rights Management global administrator role and Azure Rights Management connector administrator role are assigned to accounts by using the [Add-AipServiceRoleBasedAdministrator](#) cmdlet.

To run the RMS connector with least privileges, create a dedicated account for this purpose that you then assign the Azure RMS connector administrator role by doing the following:

1. If you haven't already done so, download and install the AIPService PowerShell module. For more information, see [Installing the AIPService PowerShell module](#).

Start Windows PowerShell with the **Run as administrator** command, and connect to the protection service by using the [Connect-AipService](#) command:

```
Connect-AipService //provide Office 365 tenant administrator or Azure RMS
global administrator credentials
```

2. Then run the [Add-AipServiceRoleBasedAdministrator](#) command, using just one of the following parameters:

```
Add-AipServiceRoleBasedAdministrator -EmailAddress <email address> -Role
"ConnectorAdministrator"
```

```
Add-AipServiceRoleBasedAdministrator -ObjectId <object id> -Role "ConnectorAdministrator"
```

```
Add-AipServiceRoleBasedAdministrator -SecurityGroupDisplayName <group Name> -Role
"ConnectorAdministrator"
```

For example, type: **Add-AipServiceRoleBasedAdministrator -EmailAddress melisa@contoso.com -Role "ConnectorAdministrator"**

Although these commands assign the connector administrator role, you could also use the GlobalAdministrator role here, as well.

During the RMS connector installation process, all prerequisite software is validated and installed, Internet Information Services (IIS) is installed if not already present, and the connector software is installed and configured. In addition, Azure RMS is prepared for configuration by creating the following:

- An empty table of servers that are authorized to use the connector to communicate with Azure RMS. You add servers to this table later.
- A set of security tokens for the connector, which authorize operations with Azure RMS. These tokens are downloaded from Azure RMS and installed on the local computer in the registry. They are protected by using the data protection application programming interface (DPAPI) and the Local System account credentials.

On the final page of the wizard, do the following, and then click **Finish**:

- If this is the first connector that you have installed, do not select **Launch connector administrator console to authorize servers** at this time. You will select this option after you have installed your second (or final) RMS connector. Instead, run the wizard again on at least one other computer. You must install a minimum of two connectors.
- If you have installed your second (or final) connector, select **Launch connector administrator console to authorize servers**.

#### TIP

At this point, there is a verification test that you can perform to test whether the web services for the RMS connector are operational:

- From a web browser, connect to [http://<connectoraddress>/\\_wmcs/certification/servercertification.asmx](http://<connectoraddress>/_wmcs/certification/servercertification.asmx), replacing <connectoraddress> with the server address or name that has the RMS connector installed. A successful connection displays a **ServerCertificationWebService** page.

If you need to uninstall the RMS connector, run the wizard again and select the uninstall option.

If you experience any problems during the installation, check the installation log:

`%LocalAppData%\Temp\Microsoft Rights Management connector_<date and time>.log`

As an example, your install log might look similar to C:\Users\Administrator\AppData\Local\Temp\Microsoft Rights Management connector\_20170803110352.log

## Authorizing servers to use the RMS connector

When you have installed the RMS connector on at least two computers, you are ready to authorize the servers and services that you want to use the RMS connector. For example, servers running Exchange Server 2013 or SharePoint Server 2013.

To define these servers, run the RMS connector administration tool and add entries to the list of allowed servers. You can run this tool when you select **Launch connector administration console to authorize servers** at the end of the Microsoft Rights Management connector Setup wizard, or you can run it separately from the wizard.

When you authorize these servers, be aware of the following considerations:

- Servers that you add are granted special privileges. All accounts that you specify for the Exchange Server role in the connector configuration are granted the **super user role** in Azure RMS, which gives them access to all content for this RMS tenant. The super user feature is automatically enabled at this point, if necessary. To avoid the security risk of elevation of privileges, be careful to specify only the accounts that are used by your organization's Exchange servers. All servers configured as SharePoint servers or file servers that use FCI are granted regular user privileges.
- You can add multiple servers as a single entry by specifying an Active Directory security or distribution group, or a service account that is used by more than one server. When you use this configuration, the group of servers shares the same RMS certificates and are all be considered owners for content that any of them have protected. To minimize administrative overheads, we recommend that you use this configuration of a single group rather than individual servers to authorize your organization's Exchange servers or a SharePoint server farm.

On the **Servers allowed to utilize the connector** page, click **Add**.

#### NOTE

Authorizing servers is the equivalent configuration in Azure RMS to the AD RMS configuration of manually applying NTFS rights to ServerCertification.asmx for the service or server computer accounts, and manually granting user super rights to the Exchange accounts. Applying NTFS rights to ServerCertification.asmx is not required on the connector.

### Add a server to the list of allowed servers

On the **Allow a server to utilize the connector** page, enter the name of the object, or browse to identify the object to authorize.

It is important that you authorize the correct object. For a server to use the connector, the account that runs the on-

premises service (for example, Exchange or SharePoint) must be selected for authorization. For example, if the service is running as a configured service account, add the name of that service account to the list. If the service is running as Local System, add the name of the computer object (for example, SERVERNAME\$). As a best practice, create a group that contains these accounts and specify the group instead of individual server names.

More information about the different server roles:

- For servers that run Exchange: You must specify a security group and you can use the default group (**Exchange Servers**) that Exchange automatically creates and maintains of all Exchange servers in the forest.
- For servers that run SharePoint:
  - If a SharePoint 2010 server is configured to run as Local System (it's not using a service account), manually create a security group in Active Directory Domain Services, and add the computer name object for the server in this configuration to this group.
  - If a SharePoint server is configured to use a service account (the recommended practice for SharePoint 2010 and the only option for SharePoint 2016 and SharePoint 2013), do the following:
    1. Add the service account that runs the SharePoint Central Administration service to enable SharePoint to be configured from its administrator console.
    2. Add the account that is configured for the SharePoint App Pool.

**TIP**

If these two accounts are different, consider creating a single group that contains both accounts to minimize the administrative overheads.

- For file servers that use File Classification Infrastructure, the associated services run as the Local System account, so you must authorize the computer account for the file servers (for example, SERVERNAME\$) or a group that contains those computer accounts.

When you have finished adding servers to the list, click **Close**.

If you haven't already done so, you must now configure load balancing for the servers that have the RMS connector installed, and consider whether to use HTTPS for the connections between these servers and the servers that you have just authorized.

## Configuring load balancing and high availability

After you have installed the second or final instance of the RMS connector, define a connector URL server name and configure a load-balancing system.

The connector URL server name can be any name under a namespace that you control. For example, you could create an entry in your DNS system for **rmsconnector.contoso.com** and configure this entry to use an IP address in your load-balancing system. There are no special requirements for this name and it doesn't need to be configured on the connector servers themselves. Unless your Exchange and SharePoint servers are going to be communicating with the connector over the internet, this name doesn't have to resolve on the internet.

**IMPORTANT**

We recommend that you don't change this name after you have configured Exchange or SharePoint servers to use the connector, because you have to then clear these servers of all IRM configurations and then reconfigure them.

After the name is created in DNS and is configured for an IP address, configure load balancing for that address, which directs traffic to the connector servers. You can use any IP-based load balancer for this purpose, which includes the Network Load Balancing (NLB) feature in Windows Server. For more information, see [Load Balancing Deployment Guide](#).

Use the following settings to configure the NLB cluster:

- Ports: 80 (for HTTP) or 443 (for HTTPS)

For more information about whether to use HTTP or HTTPS, see the next section.

- Affinity: None

- Distribution method: Equal

This name that you define for the load-balanced system (for the servers running the RMS connector service) is your organization's RMS connector name that you use later, when you configure the on-premises servers to use Azure RMS.

## Configuring the RMS connector to use HTTPS

### NOTE

This configuration step is optional, but recommended for additional security.

Although the use of TLS or SSL is optional for the RMS connector, we recommend it for any HTTP-based security-sensitive service. This configuration authenticates the servers running the connector to your Exchange and SharePoint servers that use the connector. In addition, all data that is sent from these servers to the connector is encrypted.

To enable the RMS connector to use TLS, on each server that runs the RMS connector, install a server authentication certificate that contains the name that you use for the connector. For example, if your RMS connector name that you defined in DNS is **rmsconnector.contoso.com**, deploy a server authentication certificate that contains **rmsconnector.contoso.com** in the certificate subject as the common name. Or, specify **rmsconnector.contoso.com** in the certificate alternative name as the DNS value. The certificate does not have to include the name of the server. Then in IIS, bind this certificate to the Default Web Site.

If you use the HTTPS option, ensure that all servers that run the connector have a valid server authentication certificate that chains to a root CA that your Exchange and SharePoint servers trust. In addition, if the certification authority (CA) that issued the certificates for the connector servers publishes a certificate revocation list (CRL), the Exchange and SharePoint servers must be able to download this CRL.

### TIP

You can use the following information and resources to help you request and install a server authentication certificate, and to bind this certificate to the Default Web Site in IIS:

- If you use Active Directory Certificate Services (AD CS) and an enterprise certification authority (CA) to deploy these server authentication certificates, you can duplicate and then use the Web Server certificate template. This certificate template uses **Supplied in the request** for the certificate subject name, which means that you can provide the FQDN of the RMS connector name for the certificate subject name or subject alternative name when you request the certificate.
- If you use a stand-alone CA or purchase this certificate from another company, see [Configuring Internet Server Certificates \(IIS 7\)](#) in the [Web Server \(IIS\)](#) documentation library on TechNet.
- To configure IIS to use the certificate, see [Add a Binding to a Site \(IIS 7\)](#) in the [Web Server \(IIS\)](#) documentation library on TechNet.

## Configuring the RMS connector for a web proxy server

If your connector servers are installed in a network that does not have direct internet connectivity and requires manual configuration of a web proxy server for outbound internet access, you must configure the registry on these servers for the RMS connector.

### To configure the RMS connector to use a web proxy server

1. On each server running the RMS connector, open a registry editor, such as Regedit.
2. Navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\AADRM\Connector`
3. Add the string value of `ProxyAddress` and then set the Data for this value to be  
`http://<MyProxyDomainOrIPAddress>:<MyProxyPort>`  
For example: `http://proxyserver.contoso.com:8080`

4. Close the registry editor, and then restart the server or perform an `IISReset` command to restart IIS.

## Installing the RMS connector administration tool on administrative computers

You can run the RMS connector administration tool from a computer that does not have the RMS connector installed, if that computer meets the following requirements:

- A physical or virtual computer running Windows Server 2012 or Windows Server 2012 R2 (all editions), Windows 8.1, Windows 8.
- 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).

To install the RMS connector administration tool, run the following files:

- For a 32-bit computer: `RMSConnectorAdminToolSetup_x86.exe`
- For a 64-bit computer: `RMSConnectorSetup.exe`

If you haven't already downloaded these files, you can do so from the [Microsoft Download Center](#).

## Next steps

Now that the RMS connector is installed and configured, you are ready to configure your on-premises servers to use it. Go to [Configuring servers for the Azure Rights Management connector](#).

# Configuring servers for the Azure Rights Management connector

3/9/2020 • 10 minutes to read • [Edit Online](#)

Applies to: [Azure Information Protection](#), Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Use the following information to help you configure your on-premises servers that will use the Azure Rights Management (RMS) connector. These procedures cover step 5 from [Deploying the Azure Rights Management connector](#).

Before you begin, make sure that you have installed and configured the RMS connector and you have checked any [prerequisites](#) that are applicable for the servers that will use the connector.

## Configuring servers to use the RMS connector

After you have installed and configured the RMS connector, you are ready to configure your on-premises servers that will connect to the Azure Rights Management service and use this protection technology by using the connector. This means configuring the following servers:

- **For Exchange 2016 and Exchange 2013:** Client access servers and mailbox servers
- **For Exchange 2010:** Client access servers and hub transport servers
- **For SharePoint:** Front-end SharePoint web servers, including those hosting the Central Administration server
- **For File Classification Infrastructure:** Windows Server computers that have installed File Resource Manager

This configuration requires registry settings. To do this, you have two options: Automatically by using the server configuration tool for Microsoft RMS connector, or manually by editing the registry.

### Automatically by using the server configuration tool for Microsoft RMS connector:

- Advantages:
  - No direct editing of the registry. This is automated for you by using a script.
  - No need to run a Windows PowerShell cmdlet to obtain your Microsoft RMS URL.
  - The prerequisites are automatically checked for you (but not automatically remediated) if you run it locally.

Disadvantages:

- When you run the tool, you must make a connection to a server that is already running the RMS connector.

### Manually by editing the registry:

- Advantages:
  - No connectivity to a server running the RMS connector is required.

- Disadvantages:
  - More administrative overheads that are error-prone.
  - You must obtain your Microsoft RMS URL, which requires you to run a Windows PowerShell command.
  - You must always make all the prerequisites checks yourself.

#### **IMPORTANT**

In both cases, you must manually install any prerequisites and configure Exchange, SharePoint, and File Classification Infrastructure to use Rights Management.

For most organizations, automatic configuration by using the server configuration tool for Microsoft RMS connector will be the better option, because it provides greater efficiency and reliability than manual configuration.

After making the configuration changes on these servers, you must restart them if they are running Exchange or SharePoint and previously configured to use AD RMS. There is no need to restart these servers if you are configuring them for Rights Management for the first time. You must always restart the file server that is configured to use File Classification Infrastructure after you make these configuration changes.

#### **How to use the server configuration tool for Microsoft RMS connector**

1. If you haven't already downloaded the script for the server configuration tool for Microsoft RMS connector (GenConnectorConfig.ps1), download it from the [Microsoft Download Center](#).
2. Save the GenConnectorConfig.ps1 file on the computer where you will run the tool. If you will run the tool locally, this must be the server that you want to configure to communicate with the RMS connector. Otherwise, you can save it on any computer.
3. Decide how to run the tool:
  - **Locally:** You can run the tool interactively, from the server to be configured to communicate with the RMS connector. This is useful for a one-off configuration, such as a testing environment.
  - **Software deployment:** You can run the tool to produce registry files that you then deploy to one or more relevant servers by using a systems management application that supports software deployment, such as System Center Configuration Manager.
  - **Group Policy:** You can run the tool to produce a script that you give to an administrator who can create Group Policy objects for the servers to be configured. This script creates one Group Policy object for each server type to be configured, which the administrator can then assign to the relevant servers.

#### **NOTE**

This tool configures the servers that will communicate with the RMS connector and that are listed at the beginning of this section. Do not run this tool on the servers that run the RMS connector.

4. Start Windows PowerShell with the **Run as an administrator** option, and use the Get-help command to read instructions how to the use the tool for your chosen configuration method:

```
Get-help .\GenConnectorConfig.ps1 -detailed
```

To run the script, you must enter the URL of the RMS connector for your organization. Enter the protocol prefix

(HTTP:// or HTTPS://) and the name of the connector that you defined in DNS for the load balanced address of your connector. For example, https://connector.contoso.com. The tool then uses that URL to contact the servers running the RMS connector and obtain other parameters that are used to create the required configurations.

#### **IMPORTANT**

When you run this tool, make sure that you specify the name of the load-balanced RMS connector for your organization and not the name of a single server that runs the RMS connector service.

Use the following sections for specific information for each service type:

- [Configuring an Exchange server to use the connector](#)
- [Configuring a SharePoint server to use the connector](#)
- [Configuring a file server for File Classification Infrastructure to use the connector](#)

#### **NOTE**

After these servers are configured to use the connector, client applications that are installed locally on these servers might not work with RMS. When this happens, it is because the applications try to use the connector rather than use RMS directly, which is not supported.

In addition, if Office 2010 is installed locally on an Exchange server, the client app's IRM features might work from that computer after the server is configured to use the connector, but this is not supported.

In both scenarios, you must install the client applications on separate computers that are not configured to use the connector. They will then correctly use RMS directly.

## Configuring an Exchange server to use the connector

The following Exchange roles communicate with the RMS connector:

- For Exchange 2016 and Exchange 2013: Client access server and mailbox server
- For Exchange 2010: Client access server and hub transport server

To use the RMS connector, these servers running Exchange must be running one of the following software versions:

- Exchange Server 2016
- Exchange Server 2013 with Exchange 2013 Cumulative Update 3
- Exchange Server 2010 with Exchange 2010 Service Pack 3 Rollup Update 6

You will also need on these servers, a version 1 of the RMS client (also known as MSDRM) that includes support for RMS Cryptographic Mode 2. All Windows operating systems include the MSDRM client but early versions of the client did not support Cryptographic Mode 2. If your Exchange servers are running at least Windows Server 2012, no further action is required because the RMS client installed with these operating systems natively supports Cryptographic Mode 2.

#### **IMPORTANT**

If these versions or later versions of Exchange and the MSDRM client are not installed, you will not be able to configure Exchange to use the connector. Check that these versions are installed before you continue.

## To configure Exchange servers to use the connector

1. Make sure that the Exchange servers are authorized to use the RMS connector, by using the RMS connector administration tool and the information from the [Authorizing servers to use the RMS connector](#) section. This configuration is required so that Exchange can use the RMS connector.
2. On the Exchange server roles that communicate with the RMS connector, do one of the following:
  - Run the server configuration tool for Microsoft RMS connector. For more information, see [How to use the server configuration tool for Microsoft RMS connector](#) in this article.For example, to run the tool locally to configure a server running Exchange 2016 or Exchange 2013:

```
.\GenConnectorConfig.ps1 -ConnectorUri https://rmsconnector.contoso.com -SetExchange2013
```
3. Enable IRM functionality for Exchange by using the Exchange PowerShell cmdlet [Set-IRMConfiguration](#) and set `InternalLicensingEnabled $true` and `ClientAccessServerEnabled $true`.

## Configuring a SharePoint server to use the connector

The following SharePoint roles communicate with the RMS connector:

- Front-end SharePoint web servers, including those hosting the Central Administration server

To use the RMS connector, these servers running SharePoint must be running one of the following software versions:

- SharePoint Server 2019
- SharePoint Server 2016
- SharePoint Server 2013
- SharePoint Server 2010

A server running SharePoint 2019, 2016 or SharePoint 2013 must also be running a version of the MSIPC client 2.1 that is supported with the RMS connector. To make sure that you have a supported version, download the latest client from the [Microsoft Download Center](#).

### WARNING

There are multiple versions of the MSIPC 2.1 client, so make sure that you have version 1.0.2004.0 or later.

You can verify the client version by checking the version number of MSIPC.dll, which is located in \Program Files\Active Directory Rights Management Services Client 2.1. The properties dialog box shows the version number of the MSIPC 2.1 client.

Servers running SharePoint 2010 must have installed a version of the MSDRM client that includes support for RMS Cryptographic Mode 2. Windows Server 2012 and Windows Server 2012 R2 natively support Cryptographic Mode 2.

## To configure SharePoint servers to use the connector

1. Make sure that the SharePoint servers are authorized to use the RMS connector, by using the RMS connector administration tool and the information from the [Authorizing servers to use the RMS connector](#) section. This configuration is required so that your SharePoint servers can use the RMS connector.

2. On the SharePoint servers that communicate with the RMS connector, do one of the following:

- Run the server configuration tool for Microsoft RMS connector. For more information, see [How to use the server configuration tool for Microsoft RMS connector](#) in this article.

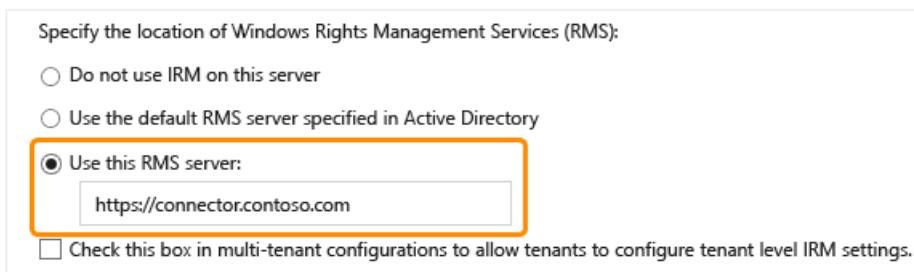
For example, to run the tool locally to configure a server running SharePoint 2019, 2016 or SharePoint 2013:

```
. \GenConnectorConfig.ps1 -ConnectorUri https://rmsconnector.contoso.com -SetSharePoint2013
```

- If you are using SharePoint 2019, 2016 or SharePoint 2013, make manual registry edits by using the information in [Registry settings for the RMS connector](#) to manually add registry settings on the servers.

3. Enable IRM in SharePoint. For more information, see [Configure Information Rights Management \(SharePoint Server 2010\)](#) in the SharePoint library.

When you follow these instructions, you must configure SharePoint to use the connector by specifying **Use this RMS server**, and then enter the load-balancing connector URL that you configured. Enter the protocol prefix (HTTP:// or HTTPS://) and the name of the connector that you defined in DNS for the load balanced address of your connector. For example, if your connector name is https://connector.contoso.com, your configuration will look like the following picture:



After IRM is enabled on a SharePoint farm, you can enable IRM on individual libraries by using the **Information Rights Management** option on the **Library Settings** page for each of the libraries.

## Configuring a file server for File Classification Infrastructure to use the connector

To use the RMS connector and File Classification Infrastructure to protect Office documents, the file server must be running one of the following operating systems:

- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012

### To configure file servers to use the connector

- Make sure that the file servers are authorized to use the RMS connector, by using the RMS connector administration tool and the information from the [Authorizing servers to use the RMS connector](#) section. This configuration is required so that your file servers can use the RMS connector.
- On the file servers configured for File Classification Infrastructure and that will communicate with the RMS connector, do one of the following:
  - Run the server configuration tool for Microsoft RMS connector. For more information, see [How to use the server configuration tool for Microsoft RMS connector](#) in this article.

For example, to run the tool locally to configure a file server running FCI:

```
.\GenConnectorConfig.ps1 -ConnectorUri https://rmsconnector.contoso.com -SetFCI2012
```

- Make manual registry edits by using the information in [Registry settings for the RMS connector](#) to manually add registry settings on the servers.
3. Create classification rules and file management tasks to protect documents with RMS Encryption, and then specify an RMS template to automatically apply RMS policies. For more information, see [File Server Resource Manager Overview](#) in the Windows Server documentation library.

## Next steps

Now that the RMS connector is installed and configured, and your servers are configured to use it, IT administrators and users can protect and consume email messages and documents by using the Azure Rights Management service. To make this easy for users, deploy the Azure Information Protection client, which installs an add-on for Office and adds new right-click options to File Explorer. For more information, see the [Azure Information Protection client administrator guide](#).

Note that if you configure departmental templates that you want to use with Exchange transport rules or Windows Server FCI, the scope configuration must include the application compatibility option such that the **Show this template to all users when the applications do not support user identity** check box is selected.

You can use the [Azure Information Protection deployment roadmap](#) to check whether there are other configuration steps that you might want to do before you roll out Azure Rights Management to users and administrators.

To monitor the RMS connector, see [Monitor the Azure Rights Management connector](#).

# Registry setting for the Rights Management connector

7/20/2020 • 2 minutes to read • [Edit Online](#)

Applies to: [Azure Information Protection](#), Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Use the tables in the following sections only if you want to manually add or check registry settings on the servers that run Exchange, SharePoint, or Windows Server. These registry settings configure the servers to use the [RMS connector](#). The recommended method to configure these servers is to use the server configuration tool for Microsoft RMS connector.

Instructions for when you use these settings:

- <YourTenantURL> is the Azure Rights Management service URL for your Azure Information Protection tenant. To find this value:
  1. Run the [Get-AipServiceConfiguration](#) cmdlet for the Azure Rights Management service. If you haven't already installed the AIPService module, see [Installing the AIPService PowerShell module](#).
  2. From the output, identify the **LicensingIntranetDistributionPointUrl** value.

For example: **LicensingIntranetDistributionPointUrl** : [https://5c6bb73b-1038-4eec-863d-49bded473437.rms.na.aadrm.com/\\_wmcs/licensing](https://5c6bb73b-1038-4eec-863d-49bded473437.rms.na.aadrm.com/_wmcs/licensing)

3. From the value, remove `/_wmcs/licensing` from this string. The remaining string is your Azure Rights Management service URL. In our example, the Azure Rights Management service URL would be the following value:

<https://5c6bb73b-1038-4eec-863d-49bded473437.rms.na.aadrm.com>

You can verify that you have correct value by running the following PowerShell command:

```
(Get-AipServiceConfiguration).LicensingIntranetDistributionPointUrl -match "https:\/\/[0-9A-Za-z\.-]*" | Out-Null; $matches[0]
```

- <ConnectorFQDN> is the load-balancing name that you defined in DNS for the connector. For example, `rmsconnector.contoso.com`.
- Use the HTTPS prefix for the connector URL if you have configured the connector to use HTTPS to communicate with your on-premises servers. For more information, see the [Configuring the RMS connector to use HTTPS](#) section from the main instructions. The Azure Rights Management service URL always uses HTTPS.

## Exchange 2016 or Exchange 2013 registry settings

Registry path: HKEY\_LOCAL\_MACHINE\Software\Microsoft\MSDRM\ServiceLocation\Activation

Type: Reg\_SZ

Value: Default

Data: `https://<YourTenantURL>/_wmcs/certification`

---

**Registry path:** HKEY\_LOCAL\_MACHINE\Software\Microsoft\MSDRM\ServiceLocation\EnterprisePublishing

**Type:** Reg\_SZ

**Value:** Default

**Data:** https://<YourTenantURL>/\_wmcs/Licensing

---

**Registry path:**

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\ExchangeServer\v15\IRM\CertificationServerRedirection

**Type:** Reg\_SZ

**Value:** https://<YourTenantURL>

**Data:** One of the following, depending on whether you are using HTTP or HTTPS from your Exchange server to the RMS connector:

- http://<|ConnectorFQDN>
  - https://<|ConnectorFQDN>
- 

**Registry path:**

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\ExchangeServer\v15\IRM\LicenseServerRedirection

**Type:** Reg\_SZ

**Value:** https://<|YourTenantURL>

**Data:** One of the following, depending on whether you are using HTTP or HTTPS from your Exchange server to the RMS connector:

- http://<|ConnectorFQDN>
- https://<|ConnectorFQDN>

## Exchange 2010 registry settings

**Registry path:** HKEY\_LOCAL\_MACHINE\Software\Microsoft\MSDRM\ServiceLocation\Activation

**Type:** Reg\_SZ

**Value:** Default

**Data:** https://<|YourTenantURL>/\_wmcs/certification

---

**Registry path:** HKEY\_LOCAL\_MACHINE\Software\Microsoft\MSDRM\ServiceLocation\EnterprisePublishing

**Type:** Reg\_SZ

**Value:** Default

**Data:** https://<|YourTenantURL>/\_wmcs/Licensing

---

**Registry path:**

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\ExchangeServer\v14\IRM\CertificationServerRedirection

**Type:** Reg\_SZ

**Value:** https://<|YourTenantURL>

**Data:** One of the following, depending on whether you are using HTTP or HTTPS from your Exchange server to the

RMS connector:

- http://<|ConnectorFQDN>
  - https://<|ConnectorFQDN>
- 

**Registry path:**

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\ExchangeServer\v14\IRM\LicenseServerRedirection

**Type:** Reg\_SZ

**Value:** https://<|YourTenantURL>

**Data:** One of the following, depending on whether you are using HTTP or HTTPS from your Exchange server to the RMS connector:

- http://<|ConnectorFQDN>
- https://<|ConnectorFQDN>

## SharePoint 2016 or SharePoint 2013 registry settings

**Registry path:** HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\MSIPC\ServiceLocation\LicensingRedirection

**Type:** Reg\_SZ

**Value:** https://<|YourTenantURL>/\_wmcs/licensing

**Data:** One of the following, depending on whether you are using HTTP or HTTPS from your SharePoint server to the RMS connector:

- http://<|ConnectorFQDN>/\_wmcs/licensing
  - https://<|ConnectorFQDN>/\_wmcs/licensing
- 

**Registry path:** HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\MSIPC\ServiceLocation\EnterpriseCertification

**Type:** Reg\_SZ

**Value:** Default

**Data:** One of the following, depending on whether you are using HTTP or HTTPS from your SharePoint server to the RMS connector:

- http://<|ConnectorFQDN>/\_wmcs/certification
  - https://<|ConnectorFQDN>/\_wmcs/certification
- 

**Registry path:** HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\MSIPC\ServiceLocation\EnterprisePublishing

**Type:** Reg\_SZ

**Value:** Default

**Data:** One of the following, depending on whether you are using HTTP or HTTPS from your SharePoint server to the RMS connector:

- http://<|ConnectorFQDN>/\_wmcs/licensing
- https://<|ConnectorFQDN>/\_wmcs/licensing

## File server and File Classification Infrastructure registry settings

**Registry path:** HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\MSDRM\ServiceLocation\EnterprisePublishing

**Type:** Reg\_SZ

**Value:** Default

**Data:** http://<|ConnectorFQDN>/\_wmcs/licensing

---

**Registry path:** HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\MSDRM\ServiceLocation\Activation

**Type:** Reg\_SZ

**Value:** Default

**Data:** http://<|ConnectorFQDN>/\_wmcs/certification

[Back to Deploying the Azure Rights Management connector](#)

# Monitor the Azure Rights Management connector

7/20/2020 • 7 minutes to read • [Edit Online](#)

Applies to: [Azure Information Protection](#), Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

After you install and configure the RMS connector, you can use the following methods and information to help you monitor the connector and your organization's use of the Azure Rights Management service from Azure Information Protection.

## Application event log entries

The RMS connector uses the Application event log to record entries for the **Microsoft RMS connector**.

For example, Information events such as:

- ID 1000 confirm that the connector service has started
- ID 1002 when a server successfully connects to the RMS connector
- ID 1004 each time the list of authorized accounts (each account is listed) is downloaded to the connector

If you have not configured the connector to use HTTPS, expect to see a Warning ID 2002 that a client is using a non-secure (HTTP) connection.

If the connector fails to connect to the Azure Rights Management service, you will most likely see Error 3001. For example, this connection failure might be as a result of a DNS problem or lack of internet access for one or more servers running the RMS connector.

### TIP

When RMS connector servers can't connect to Azure Rights Management service, web proxy configurations are often the reason.

As with all event log entries, drill in to the message for more details.

In addition to checking the event log when you first deploy the connector, check for warnings and errors on an ongoing basis. The connector might be working as expected initially, but other administrators might change dependent configurations. For example, another administrator changes the web proxy server configuration so that RMS connector servers can no longer access the internet (Error 3001) or removes a computer account from a group that you specified as authorized to use the connector (Warning 2001).

### Event log IDs and descriptions

Use the following sections to identify the possible event IDs, descriptions, and any additional information.

#### Information 1000

**The Microsoft RMS connector web service has started.**

This event is logged when the RMS connector first attempts to start.

#### Information 1001

## **The Microsoft RMS connector web service has stopped.**

This event is logged when the RMS connector stops as a result of normal operation. For example, IIS is restarted or the computer is shut down.

---

### **Information 1002**

#### **Access to the Microsoft RMS connector has been allowed for an authorized server.**

This event is logged when an account from an on-premises server first connects to the RMS connector, after the account has been authorized by the Azure RMS administrator in the RMS connector administrator tool. The SID, account name, and the name of the computer making the connection is contained in the event message.

---

### **Information 1003**

#### **The connection from the client listed below has switched from a non-secure (HTTP) connection to a secure (HTTPS) connection.**

This event is logged when an on-premises server changes its connection to the RMS connector from HTTP (less secure) to HTTPS (more secure). The SID, account name, and the name of the computer making the connection is contained in the event message.

---

### **Information 1004**

#### **The list of authorized accounts has been updated.**

This event is logged when the RMS connector has downloaded the latest list of accounts (existing accounts and any changes) that are authorized to use the RMS connector. This list is downloaded every 15 minutes, providing the RMS connector can communicate with the Azure Rights Management service.

---

### **Warning 2000**

#### **The user principal in the HTTP context is missing or invalid, please verify that the Microsoft RMS connector web site has Anonymous Authentication disabled in IIS and only Windows Authentication is enabled.**

This event is logged when the RMS connector can't uniquely identify the account trying to connect to the RMS connector. This might be a result of anonymous authentication incorrectly configured for IIS or the account is from an untrusted forest.

---

### **Warning 2001**

#### **Unauthorized access attempt to Microsoft RMS connector.**

This event is logged when an account tries to connect to the RMS connector but fails. The most typical reason for this warning is because the account that makes the connection is not in the downloaded list of authorized accounts that the RMS connector downloads from the Azure Rights Management service. For example, the latest list is not yet downloaded (this event happens every 15 minutes) or the account is missing from the list.

Another reason can be if you installed the RMS connector on the same server that is configured to use the connector. For example, you install the RMS connector on a server that runs Exchange Server and you authorize an Exchange account to use the connector. This configuration is not supported because the RMS connector cannot correctly identify the account when it attempts to connect.

The event message contains information about the account and computer trying to connect to the RMS connector:

- If the account trying to connect to the RMS connector is a valid account, use the RMS connector administrator tool to add the account to the list of authorized accounts. For more information about which

accounts must be authorized, see [Add a server to the list of allowed servers](#).

- If the account trying to connect to the RMS connector is from the same computer as the RMS connector server, install the connector on a separate server. For more information about the prerequisites for the connector, see [Prerequisites for the RMS connector](#).
- 

## Warning 2002

**The connection from the client listed below is using a non-secure (HTTP) connection.**

This event is logged when an on-premises server makes a successful connection to the RMS connector, but the connection uses HTTP (less secure) instead of HTTPS (more secure). One event is logged per account rather than per connection. This event is triggered again if the account successfully switched to using HTTPS but reverts to HTTP.

The event message contains the account SID, account name, and the name of the computer that makes the connection to the RMS connector.

For information about how to configure the RMS connector for HTTPS connections, see [Configuring the RMS connector to use HTTPS](#).

---

## Warning 2003

**The list of authorizations is empty. The service will not be usable until the list of authorized users and groups for the connector is populated.**

This event is logged when the RMS connector does not have a list of authorized accounts, so no on-premises servers can connect to it. The RMS connector downloads the list every 15 minutes from Azure RMS.

To specify the accounts, use the RMS connector administrator tool. For more information, see [Authorizing servers to use the RMS connector](#).

---

## Error 3000

**An unhandled exception occurred in the Microsoft RMS connector.**

This event is logged each time the RMS connector encounters an unexpected error, with the details of the error in the event message.

One possible cause can be identified by the text **The request failed with an empty response** in the event message. If you see this text, it might be because you have a network device that is doing SSL inspection on the packets between the on-premises servers and the RMS connector server. The Azure Rights Management service does not support this configuration and it results in a failed communication and this event log message.

---

## Error 3001

**An exception occurred while downloading authorization information.**

This event is logged if the RMS connector cannot download the latest list of accounts that are authorized to use the RMS connector. Details of the error are in the event message.

---

## Performance counters

When you install the RMS connector, it automatically creates **Microsoft Rights Management connector** performance counters that you might find useful to help you monitor and improve the performance of using the Azure Rights Management service.

For example, you regularly experience delays when documents or emails are protected. Or, you experience delays

when protected documents or emails are opened. For these cases, the performance counters can help you determine whether the delays are due to processing time on the connector, processing time from the Azure Rights Management service, or network delays.

To help you identify where the delay is occurring, look for counters that include average counts for **Connector Processing Time**, **Service Response Time**, and **Connector Response Time**. For example: **Licensing Successful Batched Request Average Connector Response Time**.

If you have recently added new server accounts to use the connector, a good counter to check is **Time since last authorization policy update** to confirm that the connector has downloaded the list since you updated it, or whether you need to wait a little longer (up to 15 minutes).

## Logging

Usage logging helps you identify when emails and documents are protected and consumed. When the RMS connector is used to protect and consume content, the user ID field in the logs contains the service principal name of **Aadrm\_S-1-7-0**. This name is automatically created for the RMS connector.

For more information about usage logging, see [Logging and analyzing the protection usage from Azure Information Protection](#).

If you need more detailed logging for diagnosis purposes, you can use [Debugview](#) from Windows Sysinternals. Enable tracing for the RMS connector by modifying the web.config file for the Default site in IIS:

1. Locate the web.config file from %programfiles%\Microsoft Rights Management connector\Web Service.
2. Locate the following line:

```
<trace enabled="false" requestLimit="10" pageOutput="false" traceMode="SortByTime" localOnly="true"/>
```

3. Replace that line with the following text:

```
<trace enabled="true" requestLimit="10" pageOutput="false" traceMode="SortByTime" localOnly="true"/>
```

4. Stop and start IIS to activate tracing.
5. When you have captured the traces that you need, revert the line in step 3, and stop and start IIS again.

# Verifying the Azure Rights Management service

5/3/2020 • 2 minutes to read • [Edit Online](#)

*Applies to:* [Azure Information Protection](#), [Office 365](#)

When the protection service (Azure Rights Management) from Azure Information Protection is activated and you have performed any additional configuration steps that are required for your organization, you are ready to verify that this protection service is working as expected.

A simple verification test is to protect a document or email message by using one user account, and then attempt to open and use that protected content from another user account on a different computer.

For instructions to complete this testing, see the information in [Helping users to protect files by using the Azure Rights Management service](#).

If your testing is unsuccessful, review the configuration steps in [Azure Information Protection deployment roadmap](#).

## TIP

If you need additional help, see the [Support options and community resources](#) section in the [Information and support for Azure Information Protection](#) article.

## Next steps

You can monitor how your organization is using this protection service by using usage logging. For more information, see [Logging and analyzing the protection usage from Azure Information Protection](#).

# Helping users to protect files by using the Azure Rights Management service

7/20/2020 • 6 minutes to read • [Edit Online](#)

Applies to: [Azure Information Protection](#), [Office 365](#)

After you have deployed and configured Azure Information Protection for your organization, provide help and guidance for users, administrators, and your help desk:

- **End-user information**

Let users know how and when to protect documents and emails that contain sensitive information.

Whenever possible, provide this information for their existing work flows so that they can incorporate the additional steps to an already-familiar process rather than introducing new processes. Be sure to let them know the benefits (and the risks) that are specific to your business, as well as providing guidance for when they should protect files and emails. If you have configured [templates](#), provide instructions about which one to select if the template name and description is not sufficient for them to choose the correct one.

**TIP**

Example videos for end users:

- [Microsoft Azure Information Protection](#)
- [Azure RMS Document Tracking and Revocation](#)

- **Administrator information**

Some applications automatically apply information protection, by using policies and settings that administrators configure. For these applications, you might need to provide instructions for other administrators who manage these applications and services.

For more information, see [How applications support the Azure Rights Management service](#) and [Configuring applications for the Azure Rights Management service](#).

- **Help desk information**

If users have the Azure Information Protection client, help desk operators can ask them to use the **Help and Feedback** option for information such as whether the edition of Office is unable to support protection, and the currently signed in user account. You can also use this option to collect log files and reset the client. For more information, see the admin guide: [Install checks and troubleshooting](#).

If there are legitimate requests to have full rights access to protected documents, make sure the help desk has processes to request this access by using the Azure Information Protection [super user feature](#). For example, these requests might be from the legal department or a manager after an employee has left the organization.

In addition, some of the typical problems that users might report include the following categories:

- **Sign in help**

Users might be prompted for credentials when the Azure Rights Management service needs to authenticate a user and cannot use cached credentials. The required credentials are usually for the

user's work or school account and password that is associated with your Office 365 tenant or Azure Active Directory tenant. Although the Azure Rights Management service can authenticate Azure AD accounts, some applications can also open protected content when a Microsoft account is used for authentication. [More information](#)

Provide users and your help desk with instructions about which account to use when users are prompted for credentials when they have applications that use the Azure Rights Management service.

- **Problems protecting or consuming content**

Make sure that users have the appropriate instructions for the applications that they use, and that they use applications and devices that are supported by the Azure Rights Management service. For more information about supported applications and devices, see [Requirements for Azure Information Protection](#).

To confirm that a specific user or group can be authorized by Azure Active Directory to protect or consume protected content, use the verification checks in [Preparing users and groups for Azure Information Protection](#).

If users report that they can open protected content but they don't have the rights that they need, the problem might be that the user is not in the correct group that's configured for a Rights Management template. Or, the problem might be that the [template needs reconfiguring](#) for the user or group.

If the rights that users have are not as expected, check the description of the rights and any application-specific implementation from the [usage rights table](#).

Use the following sections for application-specific information to help users protect documents and emails.

## Using information protection with the Azure Information Protection client

If users have Office 2010, the Azure Information Protection client is required to protect and consume protected documents and emails. However, the Azure Information Protection client is also recommended for all computers and mobile devices that support this service.

In addition to making it easier for users to protect documents and emails, the Azure Information Protection client lets users track the documents that they have protected. Tracked documents can also be revoked if the previously authorized users should no longer have access to them.

For instructions to use this client for Windows computers, see the [Azure Information Protection client user guide](#).

## Using information protection with Office 365, Office 2019, Office 2016, or Office 2013

If you are using the Azure Rights Management service and have not installed the Azure Information Protection client, users do not see the Azure Information Protection bar in their Office desktop apps. They also don't see the **Protect** button on the ribbon, or **Classify and protect** from File Explorer. These additions make it easier for users to protect documents and emails. For these users, they must follow instructions similar to the steps that follow.

**TIP**

To find application-specific help and instructions for using information protection with these applications, search for **IRM** and the application name and version.

**To protect a document in Word from Office 365 ProPlus**

1. Within Microsoft Word, create a document.
2. From the **File** menu: **Info > Protect Document > Restrict Access**.
3. Choose a template to quickly apply the appropriate usage rights, or select **Restrict Access** and select the usage rights yourself.

**NOTE**

If you have not previously used Rights Management on your computer, the **Restrict Access** option connects to the Azure Rights Management service and you are prompted for credentials to configure the Office IRM client. You can then choose a template or usage rights.

4. Save the document.

When others open the document, they are first authenticated. If they are not authorized to open the document, the document does not open. If they are authorized to open the document, it opens with the restricted **usage rights** that were specified for that user.

For example, a usage right of View-only does not allow the user to edit or save the document, even if it is first copied to another location.

The usage rights are displayed at the top of the document by using a restriction banner. The banner might display the permissions that are applied to the document, or it might provide a link to display them.

**To protect an email message using Outlook from Office 365 ProPlus, connecting to Exchange Online**

1. Within Outlook, create a mail message that is addressed to a recipient within your organization.
2. From the **OPTIONS** tab: **Permission > Select an option**. For example: **Do Not Forward**, or **<Company Name>- Confidential**, or **<Company Name> - Confidential View Only**.
3. Send the message.

Similarly to viewing a protected document, when the recipients open the protected email message, they are first authenticated. If they are authorized to see the email message, it opens with the restricted **usage rights** that were specified for that user.

For example, if the email message is protected by using the **Do Not Forward** option, the **Forward** button on the ribbon is not available.

**To protect an email message using Outlook on the web**

1. Using Outlook on the web, create a mail message addressed to a recipient within your organization.
2. Select **Protect**. Unless the default has been changed by an administrator, the **Do Not Forward** option is automatically selected. If you want to change the default, select **Change Permissions** and then select an option from the drop-down. For example: **Encrypt** or **<Company Name>- Confidential**.
3. Send the message.

Similarly to viewing a protected document, when the recipients open the email message, they are first authenticated. If they are authorized to see the email message, it opens with the restricted **usage rights** that were specified for that user.

For example, with the default **Do Not Forward** option, the **Forward** option in the message window is not available.

# Logging and analyzing the protection usage from Azure Information Protection

7/20/2020 • 13 minutes to read • [Edit Online](#)

*Applies to:* [Azure Information Protection](#), [Office 365](#)

Use this information to help you understand how you can use usage logging for the protection service (Azure Rights Management) from Azure Information Protection. This protection service provides the data protection for your organization's documents and emails and it can log every request to it. These requests include when users protect documents and email and also consume this content, actions performed by your administrators for this service, and actions performed by Microsoft operators to support your Azure Information Protection deployment.

You can then use these protection usage logs to support the following business scenarios:

- **Analyze for business insights**

The logs generated by the protection service can be imported into a repository of your choice (such as a database, an online analytical processing (OLAP) system, or a map-reduce system) to analyze the information and produce reports. As an example, you could identify who is accessing your protected data. You can determine what protected data people are accessing, and from what devices and from where. You can find out whether people can successfully read protected content. You can also identify which people have read an important document that was protected.

- **Monitor for abuse**

Logging information about the protection use is available to you in near-real time, so that you can continuously monitor your company's use of the protection service. 99.9% of logs are available within 15 minutes of an initiated action to the service.

For example, you might want to be alerted if there is a sudden increase of people reading protected data outside standard working hours, which could indicate that a malicious user is collecting information to sell to competitors. Or, if the same user apparently accesses data from two different IP addresses within a short time frame, which could indicate that a user account has been compromised.

- **Perform forensic analysis**

If you have an information leak, you are likely to be asked who recently accessed specific documents and what information did a suspected person access recently. You can answer these types of questions when you use this logging because people who use protected content must always get a Rights Management license to open documents and pictures that are protected by Azure Information Protection, even if these files are moved by email or copied to USB drives or other storage devices. This means that you can use these logs as a definitive source of information for forensic analysis when you protect your data by using Azure Information Protection.

In addition to this usage logging, you also have the following logging options:

LOGGING OPTION	DESCRIPTION
----------------	-------------

Logging option	Description
Admin log	<p>Logs administrative tasks for the protection service. For example, if the service is deactivated, when the super user feature is enabled, and when users are delegated admin permissions to the service.</p> <p>For more information, see the PowerShell cmdlet, <a href="#">Get-AipServiceAdminLog</a>.</p>
Document tracking	<p>Lets users track and revoke their documents that they have tracked with the Azure Information Protection client. Global administrators can also track these documents on behalf of users.</p> <p>For more information, see <a href="#">Configuring and using document tracking for Azure Information Protection</a>.</p>
Client event logs	<p>Usage activity for the Azure Information Protection client, logged in the local Windows <b>Applications and Services</b> event log, <b>Azure Information Protection</b>.</p> <p>For more information, see <a href="#">Usage logging for the Azure Information Protection client</a>.</p>
Client log files	<p>Troubleshooting logs for the Azure Information Protection client, located in <b>%localappdata%\Microsoft\MSIP</b>. These files are designed for Microsoft Support.</p>

In addition, information from the Azure Information Protection client usage logs and the Azure Information Protection scanner is collected and aggregated to create reports in the Azure portal. For more information, see [Reporting for Azure Information Protection](#).

Use the following sections for more information about the usage logging for the protection service.

## How to enable logging for protection usage

Protection usage logging is enabled by default for all customers.

There is no extra cost for the log storage or for the logging feature functionality.

## How to access and use your protection usage logs

Azure Information Protection writes logs as a series of blobs to an Azure storage account that it automatically creates for your tenant. Each blob contains one or more log records, in W3C extended log format. The blob names are numbers, in the order in which they were created. The [How to interpret your Azure Rights Management usage logs](#) section later in this document contains more information about the log contents and their creation.

It can take a while for logs to appear in your storage account after a protection action. Most logs appear within 15 minutes. We recommend that you download the logs to local storage, such as a local folder, a database, or a map-reduce repository.

To download your usage logs, you will use the AIPService PowerShell module for Azure Information Protection. For installation instructions, see [Installing the AIPService PowerShell module](#).

### To download your usage logs by using PowerShell

1. Start Windows PowerShell with the **Run as administrator** option and use the [Connect-AipService](#) cmdlet to connect to Azure Information Protection:

```
Connect-AipService
```

2. Run the following command to download the logs for a specific date:

```
Get-AipServiceUserLog -Path <location> -fordate <date>
```

For example, after creating a folder called Logs on your E: drive:

- To download logs for a specific date (such as 2/1/2016), run the following command:

```
Get-AipServiceUserLog -Path E:\Logs -fordate 2/1/2016
```

- To download logs for a date range (such as from 2/1/2016 through 2/14/2016), run the following command:

```
Get-AipServiceUserLog -Path E:\Logs -fromdate 2/1/2016 -todate 2/14/2016
```

When you specify the day only, as in our examples, the time is assumed to be 00:00:00 in your local time, and then converted to UTC. When you specify a time with your -fromdate or -todate parameters (for example, -fordate "2/1/2016 15:00:00"), that date and time is converted to UTC. The Get-AipServiceUserLog command then gets the logs for that UTC time period.

You cannot specify less than a whole day to download.

By default, this cmdlet uses three threads to download the logs. If you have sufficient network bandwidth and want to decrease the time required to download the logs, use the -NumberOfThreads parameter, which supports a value from 1 through 32. For example, if you run the following command, the cmdlet spawns 10 threads to download the logs:

```
Get-AipServiceUserLog -Path E:\Logs -fromdate 2/1/2016 -todate 2/14/2016 -numberofthreads 10
```

#### TIP

You can aggregate all your downloaded log files into a CSV format by using [Microsoft's Log Parser](#), which is a tool to convert between various well-known log formats. You can also use this tool to convert data to SYSLOG format, or import it into a database. After you have installed the tool, run `LogParser.exe /?` for help and information to use this tool.

For example, you might run the following command to import all information into a .log file format:

```
logparser -i:w3c -o:csv "SELECT * INTO AllLogs.csv FROM *.log"
```

## How to interpret your usage logs

Use the following information to help you interpret the protection usage logs.

### The log sequence

Azure Information Protection writes the logs as a series of blobs.

Each entry in the log has a UTC timestamp. Because the protection service runs on multiple servers across multiple data centers, sometimes the logs might seem to be out of sequence, even when they are sorted by their timestamp. However, the difference is small and usually within a minute. In most cases, this is not an issue that would be a problem for log analysis.

### The blob format

Each blob is in W3C extended log format. It starts with the following two lines:

#Software: RMS

#Version: 1.1

The first line identifies that these are protection logs from Azure Information Protection. The second line identifies that the rest of the blob follows the version 1.1 specification. We recommend that any applications that parse these logs verify these two lines before continuing to parse the rest of the blob.

The third line enumerates a list of field names that are separated by tabs:

**#Fields:** date time row-id request-type user-id result correlation-id content-id owner-email issuer template-id file-name date-published c-info c-ip admin-action acting-as-user

Each of the subsequent lines is a log record. The values of the fields are in the same order as the preceding line, and are separated by tabs. Use the following table to interpret the fields.

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.	2013-06-25
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. If a value is not present, use the correlation-id value to identify the entry.  This value is useful when you aggregate logs or copy logs into another format.	1c3fe7a9-d9e0-4654-97b7-14fafaf72ea63
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. Calls from a tenant key that is managed by you (BYOK) have a value of "", which also applies when the request types are anonymous.	'joe@contoso.com'

FIELD NAME	W3C DATA TYPE	DESCRIPTION	EXAMPLE VALUE
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}
owner-email	String	Email address of the owner of the document.  This field is blank if the request type is RevokeAccess.	alice@contoso.com
issuer	String	Email address of the document issuer.  This field is blank if the request type is RevokeAccess.	alice@contoso.com (or) FederatedEmail.4c1f4d-93bf-00a95fa1e042@contoso.onmicrosoft.com'
template-id	String	ID of the template used to protect the document.  This field is blank if the request type is RevokeAccess.	{6d9371a6-4e2d-4e97-9a38-202233fed26e}

FIELD NAME	W3C DATA TYPE	DESCRIPTION	EXAMPLE VALUE
file-name	String	<p>File name of a protected document that is tracked by using the Azure Information Protection client for Windows.</p> <p>Currently, some files (such as Office documents) display as GUIDs rather than the actual file name.</p> <p>This field is blank if the request type is RevokeAccess.</p>	TopSecretDocument.docx
date-published	Date	<p>Date when the document was protected.</p> <p>This field is blank if the request type is RevokeAccess.</p>	2015-10-15T21:37:00
c-info	String	<p>Information about the client platform that is making the request.</p> <p>The specific string varies, depending on the application (for example, the operating system or the browser).</p>	'MSIPC;version=1.0.623.47;AppName=WINWORD.EXE;AppVersion=15.0.4753.1000;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
admin-action	Bool	Whether an administrator has accessed the document tracking site in Administrator mode.	True
acting-as-user	String	The email address of the user for whom an administrator is accessing the document tracking site.	'joe@contoso.com'

#### Exceptions for the user-id field

Although the user-id field usually indicates the user who made the request, there are two exceptions where the value does not map to a real user:

- The value 'microsoftrmsonline@<YourTenantID>.rms.<region>.aadrm.com'.

This indicates an Office 365 service, such as Exchange Online or Microsoft SharePoint, is making the request. In the string, <YourTenantID> is the GUID for your tenant and <region> is the region where your tenant is registered. For example, **na** represents North America, **eu** represents Europe, and **ap** represents Asia.

- If you are using the RMS connector.

Requests from this connector are logged with the service principal name of **Aadrm\_S-1-7-0**, which is automatically generated when you install the RMS connector.

#### Typical request types

There are many request types for the protection service but the following table identifies some of the most typically used request types.

REQUEST TYPE	DESCRIPTION
AcquireLicense	A client from a Windows-based computer is requesting a license for protected content.
AcquirePreLicense	A client, on behalf of the user, is requesting for a license for protected content.
AcquireTemplates	A call was made to acquires templates based on template IDs
AcquireTemplateInformation	A call was made to get the IDs of the template from the service.
AddTemplate	A call is made from the Azure portal to add a template.
AllDocsCsv	A call is made from the document tracking site to download the CSV file from the <b>All Documents</b> page.
BECREATEEndUserLicenseV1	A call is made from a mobile device to create an end-user license.
BEGetAllTemplatesV1	A call is made from a mobile device (back-end) to get all the templates.
Certify	The client is certifying the user for the consumption and creation of protected content.
DeleteTemplateById	A call is made from the Azure portal, to delete a template by template ID.
DocumentEventsCsv	A call is made from the document tracking site to download the .CSV file for a single document.
ExportTemplateById	A call is made from the Azure portal to export a template based on a template ID.
FECREATEEndUserLicenseV1	Similar to the AcquireLicense request but from mobile devices.
FECREATEPublishingLicenseV1	The same as Certify and GetClientLicensorCert combined, from mobile clients.
FEGetAllTemplates	A call is made, from a mobile device (front-end) to get the templates.
FindServiceLocationsForUser	A call is made to query for URLs, which is used to call Certify or AcquireLicense.

REQUEST TYPE	DESCRIPTION
GetAllDocs	<p>A call is made from the document tracking site to load the <b>all documents</b> page for a user, or search all documents for the tenant. Use this value with the admin-action and acting-as-admin fields:</p> <ul style="list-style-type: none"> <li>- admin-action is empty: A user views the <b>all documents</b> page for their own documents.</li> <li>- admin-action is true and acting-as-user is empty: An administrator views all documents for their tenant.</li> <li>- admin-action is true and acting-as-user is not empty: An administrator views the <b>all documents</b> page for a user.</li> </ul>
GetAllTemplates	A call is made from the Azure portal, to get all the templates.
GetClientLicensorCert	The client is requesting a publishing certificate (that is later used to protect content) from a Windows-based computer.
GetConfiguration	An Azure PowerShell cmdlet is called to get the configuration of the Azure RMS tenant.
GetConnectorAuthorizations	A call is made from the RMS connectors to get their configuration from the cloud.
GetRecipients	A call is made from the document tracking site to navigate to the list view for a single document.
GetSingle	A call is made from the document tracking site to navigate to a <b>single document</b> page.
GetTenantFunctionalState	The Azure portal is checking whether the protection service (Azure Rights Management) is activated.
GetTemplateById	A call is made from the Azure portal to get a template by specifying a template ID.
KeyVaultDecryptRequest	The client is attempting to decrypt the RMS-protected content. Applicable only for a customer-managed tenant key (BYOK) in Azure Key Vault.
KeyVaultGetKeyInfoRequest	A call is made to verify that the key specified to be used in Azure Key Vault for the Azure Information Protection tenant key is accessible and not already used.
KeyVaultSignDigest	A call is made when a customer-managed key (BYOK) in Azure Key Vault is used for signing purposes. This is called typically once per AcquireLicence (or FECREATEENDUSERLICENSEV1), Certify, and GetClientLicensorCert (or FECREATEPUBLISHINGLICENSEV1).
KMSPDecrypt	The client is attempting to decrypt the RMS-protected content. Applicable only for a legacy customer-managed tenant key (BYOK).

REQUEST TYPE	DESCRIPTION
KMSPSignDigest	A call is made when a legacy customer-managed key (BYOK) is used for signing purposes. This is called typically once per AcquireLicence (or FECREATEENDUSERLICENSEV1), Certify, and GetClientLicenserCert (or FECREATEPUBLISHINGLICENSEV1).
LoadEventsForMap	A call is made from the document tracking site to navigate to the map view for a single document.
LoadEventsForSummary	A call is made from the document tracking site to navigate to the timeline view for a single document.
LoadEventsForTimeline	A call is made from the document tracking site to navigate to the map view for a single document.
ImportTemplate	A call is made from the Azure portal to import a template.
RevokeAccess	A call is made from the document tracking site to revoke a document.
SearchUsers	A call is made from the document tracking site to search all users in a tenant.
ServerCertify	A call is made from an RMS-enabled client (such as SharePoint) to certify the server.
SetUsageLogFeatureState	A call is made to enable usage logging.
SetUsageLogStorageAccount	A call is made to specify the location of the Azure Rights Management service logs.
UpdateNotificationSettings	A call is made from the document tracking site to change the notification settings for a single document.
UpdateTemplate	A call is made from the Azure portal to update an existing template.

## PowerShell reference

The only PowerShell cmdlet that you need to access your protection usage logging is [Get-AipServiceUserLog](#).

For more information about using PowerShell for Azure Information Protection, see [Administering protection from Azure Information Protection by using PowerShell](#).

# Operations for your Azure Information Protection tenant key

7/20/2020 • 2 minutes to read • [Edit Online](#)

Applies to: [Azure Information Protection](#), [Office 365](#)

Depending on your tenant key topology for Azure Information Protection, you have different levels of control and responsibility for your Azure Information Protection tenant key. The two key topologies are **Microsoft-managed** and **customer-managed**.

When you manage your own tenant key in Azure Key Vault, this is often referred to as bring your own key (BYOK). For more information about this scenario and how to choose between the two tenant key topologies, see [Planning and implementing your Azure Information Protection tenant key](#).

The following table identifies the operations that you can do, depending on the topology that you've chosen for your Azure Information Protection tenant key.

LIFE CYCLE OPERATION	MICROSOFT-MANAGED (DEFAULT)	CUSTOMER-MANAGED (BYOK)
Revoke your tenant key	No (automatic)	Yes
Rekey 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

After you have identified which topology you have implemented, select one of the following links for more information about these operations for your Azure Information Protection tenant key:

- [Microsoft-managed tenant key](#)
- [Customer-managed tenant key](#)

However, if you want to create an Azure Information Protection tenant key by importing a trusted publishing domain (TPD) from Active Directory Rights Management Services, this import operation is part of the [migration from AD RMS to Azure Information Protection](#).

# Microsoft-managed: Tenant key life cycle operations

7/20/2020 • 6 minutes to read • [Edit Online](#)

Applies to: [Azure Information Protection](#), [Office 365](#)

If Microsoft manages your tenant key for Azure Information Protection (the default), use the following sections for more information about the life cycle operations that are relevant to this topology.

## Revoke your tenant key

When you cancel your subscription for Azure Information Protection, Azure Information Protection stops using your tenant key and no action is needed from you.

## Rekey your tenant key

Rekeying is also known as rolling your key. When you do this operation, Azure Information Protection stops using the existing tenant key to protect documents and emails, and starts to use a different key. Policies and templates are immediately resigned but this changeover is gradual for existing clients and services using Azure Information Protection. So for some time, some new content continues to be protected with the old tenant key.

To rekey, you must configure the tenant key object and specify the alternative key to use. Then, the previously used key is automatically marked as archived for Azure Information Protection. This configuration ensures that content that was protected by using this key remains accessible.

Examples of when you might need to rekey for Azure Information Protection:

- You have migrated from Active Directory Rights Management Services (AD RMS) with a cryptographic mode 1 key. When the migration is complete, you want to change to using a key that uses cryptographic mode 2.
- Your company has split into two or more companies. When you rekey 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 want to move from one key management topology to another.
- You believe the master copy of your tenant key is compromised.

To rekey, you can select a different Microsoft-managed key to become your tenant key, but you cannot create a new Microsoft-managed key. To create a new key, you must change your key topology to be customer-managed (BYOK).

You have more than one Microsoft-managed key if you migrated from Active Directory Rights Management Services (AD RMS) and chose the Microsoft-managed key topology for Azure Information Protection. In this scenario, you have at least two Microsoft-managed keys for your tenant. One key, or more, is the key or keys that you imported from AD RMS. You will also have the default key that was automatically created for your Azure Information Protection tenant.

To select a different key to be your active tenant key for Azure Information Protection, use the [Set-AipServiceKeyProperties](#) cmdlet from the AIPService module. To help you identify which key to use, use the [Get-AipServiceKeys](#) cmdlet. You can identify the default key that was automatically created for your Azure Information Protection tenant by running the following command:

```
(Get-AipServiceKeys) | Sort-Object CreationTime | Select-Object -First 1
```

To change your key topology to be customer-managed (BYOK), see [Implementing BYOK for your Azure Information Protection tenant key](#).

## Backup and recover your tenant key

Microsoft is responsible for backing up your tenant key and no action is required from you.

## Export your tenant key

You can export your Azure Information Protection configuration and tenant key by following the instructions in the following three steps:

### Step 1: Initiate export

- [Contact Microsoft Support](#) to open an **Azure Information Protection support case with a request for an Azure Information Protection key export**. You must prove you are a Global administrator for your tenant, and understand that this process takes several days to confirm. Standard support charges apply; exporting your tenant key is not a free-of-charge support service.

### Step 2: Wait for verification

- Microsoft verifies that your request to release your Azure Information Protection tenant key is legitimate. This process can take up to three weeks.

### Step 3: Receive key instructions from CSS

- Microsoft Customer Support Services (CSS) sends you your Azure Information Protection configuration and tenant key encrypted in a password-protected file. This file has a .tpd file name extension. To do this, CSS first sends you (as the person who initiated the export) a tool by email. You must run the tool from a command prompt as follows:

```
AadrmTpD.exe -createkey
```

This generates an RSA key pair and saves the public and private halves as files in the current folder. For example: **PublicKey-FA29D0FE-5049-4C8E-931B-96C6152B0441.txt** and **PrivateKey-FA29D0FE-5049-4C8E-931B-96C6152B0441.txt**.

Respond to the email from CSS, attaching the file that has a name that starts with **PublicKey**. CSS next sends you a TPD file as an .xml file that is encrypted with your RSA key. Copy this file to the same folder as you ran the AadrmTpD tool originally, and run the tool again, using your file that starts with **PrivateKey** and the file from CSS. For example:

```
AadrmTpD.exe -key PrivateKey-FA29D0FE-5049-4C8E-931B-96C6152B0441.txt -target TPD-77172C7B-8E21-48B7-9854-7A4CEAC474D0.xml
```

The output of this command should be two files: One contains the plain text password for the password-protected TPD, and the other is the password-protected TPD itself. The files have a new GUID, for example:

- Password-5E4C2018-8C8C-4548-8705-E3218AA1544E.txt
- ExportedTPD-5E4C2018-8C8C-4548-8705-E3218AA1544E.xml

Back up these files and store them safely to ensure that you can continue to decrypt content that is protected with this tenant key. In addition, if you are migrating to AD RMS, you can import this TPD

file (the file that starts with ExportedTDP) to your AD RMS server.

#### Step 4: Ongoing: Protect your tenant key

After you receive your tenant key, keep it well-guarded, because if somebody gets access to it, they can decrypt all documents that are protected by using that key.

If the reason for exporting your tenant key is because you no longer want to use Azure Information Protection, as a best practice, now deactivate the Azure Rights Management service from your Azure Information Protection tenant. Do not delay doing this after you receive your tenant key because this precaution helps to minimize the consequences if your tenant key is accessed by somebody who should not have it. For instructions, see [Decommissioning and deactivating Azure Rights Management](#).

## Respond to a breach

No security system, no matter how strong, is complete without a breach response process. Your tenant key might be compromised or stolen. Even when it's protected well, vulnerabilities might be found in current generation key technology or in current key lengths and algorithms.

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, Microsoft will notify the Global administrators for your tenant by email.

If you have a breach, the best action that you or Microsoft can take depends on the scope of the breach; Microsoft will work with you through this process. The following table shows some typical situations and the likely response, although the exact response depends on all the information that is revealed during the investigation.

INCIDENT DESCRIPTION	LIKELY RESPONSE
Your tenant key is leaked.	Rekey your tenant key. See the <a href="#">Rekey your tenant key</a> section in this article.
An unauthorized individual or malware got rights to use your tenant key but the key itself did not leak.	Rekeying your tenant key does not help here and requires root-cause analysis. If a process or software bug was responsible for the unauthorized individual to get access, that situation must be resolved.
Vulnerability discovered in the RSA algorithm, or key length, or brute-force attacks become computationally feasible.	Microsoft must update Azure Information Protection to support new algorithms and longer key lengths that are resilient, and instruct all customers to rekey their tenant key.

# Customer-managed: Tenant key life cycle operations

7/20/2020 • 5 minutes to read • [Edit Online](#)

Applies to: [Azure Information Protection](#), [Office 365](#)

If you manage your tenant key for Azure Information Protection (the bring your own key, or BYOK, scenario), use the following sections for more information about the life cycle operations that are relevant to this topology.

## Revoke your tenant key

There are very few scenarios when you might need to revoke your key instead of rekeying. When you revoke your key, all content that has been protected by your tenant using that key will become inaccessible to everybody (including Microsoft, your global admins, and super users) unless you have a backup of the key that you can restore. After revoking your key, you won't be able to protect new content until you create and configure a new tenant key for Azure Information Protection.

To revoke your customer-managed tenant key, in Azure Key Vault, change the permissions on the key vault that contains your Azure Information Protection tenant key so that the Azure Rights Management service can no longer access the key. This action effectively revokes the tenant key for Azure Information Protection.

When you cancel your subscription for Azure Information Protection, Azure Information Protection stops using your tenant key and no action is needed from you.

## Rekey your tenant key

Rekeying is also known as rolling your key. When you do this operation, Azure Information Protection stops using the existing tenant key to protect documents and emails, and starts to use a different key. Policies and templates are immediately resigned but this changeover is gradual for existing clients and services using Azure Information Protection. So for some time, some new content continues to be protected with the old tenant key.

To rekey, you must configure the tenant key object and specify the alternative key to use. Then, the previously used key is automatically marked as archived for Azure Information Protection. This configuration ensures that content that was protected by using this key remains accessible.

Examples of when you might need to rekey for Azure Information Protection:

- Your company has split into two or more companies. When you rekey 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 want to move from one key management topology to another.
- You believe the master copy of your tenant key (the copy in your possession) is compromised.

To rekey to another key that you manage, you can either create a new key in Azure Key Vault or use a different key that is already in Azure Key Vault. Then follow the same procedures that you did to implement BYOK for Azure Information Protection.

1. Only if the new key is in a different key vault to the one you are already using for Azure Information Protection: Authorize Azure Information Protection to use the key vault, by using the [Set-AzKeyVaultAccessPolicy](#) cmdlet.
2. If Azure Information Protection doesn't already know about the key you want to use, run [Use-](#)

[AipServiceKeyVaultKey](#) cmdlet.

3. Configure the tenant key object, by using the run [Set-AipServiceKeyProperties](#) cmdlet.

For more information about each of these steps:

- To rekey to another key that you manage, see [Implementing BYOK for your Azure Information Protection tenant key](#).

If you are rekeying an HSM-protected key that you create on-premises and transfer to Key Vault, you can use the same security world and access cards as you used for your current key.

- To rekey, changing to a key that Microsoft manages for you, see the [Rekey your tenant key](#) section for Microsoft-managed operations.

## Backup and recover your tenant key

Because you are managing your tenant key, you are responsible for backing up the key that Azure Information Protection uses.

If you generated your tenant key on premises, in a nCipher HSM: To back up the key, back up the tokenized key file, the world file, and the administrator cards. When you transfer your key to Azure Key Vault, the service saves the tokenized key file, to protect against failure of any service nodes. This file is bound to the security world for the specific Azure region or instance. However, do not consider this tokenized key file to be a full backup. For example, if you ever need a plain text copy of your key to use outside a nCipher HSM, Azure Key Vault cannot retrieve it for you, because it has only a non-recoverable copy.

Azure Key Vault has a [backup cmdlet](#) that you can use to back up a key by downloading it and storing it in a file. Because the downloaded content is encrypted, it cannot be used outside Azure Key Vault.

## Export your tenant key

If you use BYOK, you cannot export your tenant key from Azure Key Vault or Azure Information Protection. The copy in Azure Key Vault is non-recoverable.

## Respond to a breach

No security system, no matter how strong, is complete without a breach response process. Your tenant key might be compromised or stolen. Even when it's protected well, vulnerabilities might be found in current generation key technology or in current key lengths and algorithms.

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, Microsoft notifies your tenant Global administrators by email.

If you have a breach, the best action that you or Microsoft can take depends on the scope of the breach; Microsoft will work with you through this process. The following table shows some typical situations and the likely response, although the exact response depends on all the information that is revealed during the investigation.

INCIDENT DESCRIPTION	LIKELY RESPONSE
Your tenant key is leaked.	Rekey your tenant key. See <a href="#">Rekey your tenant key</a> .
An unauthorized individual or malware got rights to use your tenant key but the key itself did not leak.	Rekeying your tenant key does not help here and requires root-cause analysis. If a process or software bug was responsible for the unauthorized individual to get access, that situation must be resolved.

INCIDENT DESCRIPTION	LIKELY RESPONSE
Vulnerability discovered in the current-generation HSM technology.	Microsoft must update the HSMs. If there is reason to believe that the vulnerability exposed keys, Microsoft will instruct all customers to rekey their tenant keys.
Vulnerability discovered in the RSA algorithm, or key length, or brute-force attacks become computationally feasible.	Microsoft must update Azure Key Vault or Azure Information Protection to support new algorithms and longer key lengths that are resilient, and instruct all customers to rekey their tenant key.

# Manage personal data for Azure Information Protection

7/20/2020 • 10 minutes to read • [Edit Online](#)

When you configure and use Azure Information Protection, email addresses and IP addresses are stored and used by the Azure Information Protection service. This personal data can be found in the following items:

- The Azure Information Protection policy
- Templates for the protection service
- Super users and delegated administrators for the protection service
- Administration logs for the protection service
- Usage logs for the protection service
- Document tracking logs
- Usage logs for the Azure Information Protection clients and RMS client

## NOTE

This article provides steps for how to delete personal data from the device or service and can be used to support your obligations under the GDPR. If you're looking for general info about GDPR, see the [GDPR section of the Service Trust portal](#).

## Viewing personal data that Azure Information Protection uses

Using the Azure portal, an administrator can specify email addresses for scoped policies and for protection settings within a label configuration. For more information, see [How to configure the Azure Information Protection policy for specific users by using scoped policies](#) and [How to configure a label for Rights Management protection](#).

For labels that are configured to apply protection from the Azure Rights Management service, email address can also be found in protection templates, by using PowerShell cmdlets from the [AIPService module](#). This PowerShell module also lets an administrator specify users by email address to be a [super user](#), or an administrator for the Azure Rights Management service.

When Azure Information Protection is used to classify and protect documents and emails, email addresses and the users' IP addresses might be saved in log files.

### Protection templates

Run the [Get-AipServiceTemplate](#) cmdlet to get a list of protection templates. You can use the template ID to get details of a specific template. The `RightsDefinitions` object displays the personal data, if any.

Example:

```

PS C:\Users> Get-AipServiceTemplate -TemplateId fcdbbc36-1f48-48ca-887f-265ee1268f51 | select *

TemplateId : fcdbbc36-1f48-48ca-887f-265ee1268f51
Names : {1033 -> Confidential}
Descriptions : {1033 -> This data includes sensitive business information. Exposing this data to unauthorized users may cause damage to the business. Examples for Confidential information
 are employee information, individual customer projects or contracts and sales account data.}
Status : Archived
RightsDefinitions : {admin@aip500.onmicrosoft.com -> VIEW, VIEWRIGHTSDATA, EDIT, DOCEDIT, PRINT, EXTRACT, REPLY, REPLYALL, FORWARD, EXPORT, EDITRIGHTSDATA, OBJMODEL, OWNER, AllStaff-7184AB3F-CCD1-46F3-8233-3E09E9CF0E66@aip500.onmicrosoft.com -> VIEW, VIEWRIGHTSDATA, EDIT, DOCEDIT, PRINT, EXTRACT, REPLY, REPLYALL, FORWARD, EXPORT, EDITRIGHTSDATA, OBJMODEL, OWNER, admin2@aip500.onmicrosoft.com -> VIEW, VIEWRIGHTSDATA, EDIT, DOCEDIT, PRINT, EXTRACT, REPLY, REPLYALL, FORWARD, EXPORT, EDITRIGHTSDATA, OBJMODEL, OWNER}
ContentExpirationDate : 1/1/0001 12:00:00 AM
ContentValidityDuration : 0
ContentExpirationOption : Never
LicenseValidityDuration : 7
ReadOnly : False
LastModifiedTimeStamp : 1/26/2018 6:17:00 PM
ScopedIdentities : {}
EnableInLegacyApps : False
LabelId :

```

## Super users and delegated administrators for the protection service

Run the [Get-AipServiceSuperUser](#) cmdlet and [get-aipservicerolebasedadministrator](#) cmdlet to see which users have been assigned the super user role or global administrator role for the protection service (Azure Rights Management) from Azure Information Protection. For users who have been assigned either of these roles, their email addresses are displayed.

## Administration logs for the protection service

Run the [Get-AipServiceAdminLog](#) cmdlet to get a log of admin actions for the protection service (Azure Rights Management) from Azure Information Protection. This log includes personal data in the form of email addresses and IP addresses. The log is in plaintext and after it is downloaded, the details of a specific administrator can be searched offline.

For example:

```

PS C:\Users> Get-AipServiceAdminLog -Path '.\Desktop\admin.log' -FromTime 4/1/2018 -ToTime 4/30/2018 -Verbose
The Rights Management administration log was successfully generated and can be found at .\Desktop\admin.log.

```

## Usage logs for the protection service

Run the [Get-AipServiceUserLog](#) cmdlet to retrieve a log of end-user actions that use the protection service from Azure Information Protection. The log could include personal data in the form of email addresses and IP addresses. The log is in plaintext and after it is downloaded, the details of a specific administrator can be searched offline.

For example:

```
PS C:\Users> Get-AipServiceUserLog -Path '.\Desktop\' -FromDate 4/1/2018 -ToDate 4/30/2018 -NumberOfThreads 10
Acquiring access to your user log..
Downloading the log for 2018-04-01.
Downloading the log for 2018-04-03.
Downloading the log for 2018-04-06.
Downloading the log for 2018-04-09.
Downloading the log for 2018-04-10.
Downloaded the log for 2018-04-01. The log is available at .\Desktop\rmslog-2018-04-01.log.
Downloaded the log for 2018-04-03. The log is available at .\Desktop\rmslog-2018-04-03.log.
Downloaded the log for 2018-04-06. The log is available at .\Desktop\rmslog-2018-04-06.log.
Downloaded the log for 2018-04-09. The log is available at .\Desktop\rmslog-2018-04-09.log.
Downloaded the log for 2018-04-10. The log is available at .\Desktop\rmslog-2018-04-10.log.
Downloading the log for 2018-04-12.
Downloading the log for 2018-04-13.
Downloading the log for 2018-04-14.
Downloading the log for 2018-04-16.
Downloading the log for 2018-04-18.
Downloaded the log for 2018-04-12. The log is available at .\Desktop\rmslog-2018-04-12.log.
Downloaded the log for 2018-04-13. The log is available at .\Desktop\rmslog-2018-04-13.log.
Downloaded the log for 2018-04-14. The log is available at .\Desktop\rmslog-2018-04-14.log.
Downloaded the log for 2018-04-16. The log is available at .\Desktop\rmslog-2018-04-16.log.
Downloaded the log for 2018-04-18. The log is available at .\Desktop\rmslog-2018-04-18.log.
Downloading the log for 2018-04-24.
Downloaded the log for 2018-04-24. The log is available at .\Desktop\rmslog-2018-04-24.log.
```

## Document tracking logs

Run the [Get-AipServiceDocumentLog](#) cmdlet to retrieve information from the document tracking site about a specific user. To get tracking information associated with the document logs, use the [Get-AipServiceTrackingLog](#) cmdlet.

For example:

```
PS C:\Users> Get-AipServiceDocumentLog -UserEmail "admin@aip500.onmicrosoft.com"
```

```
ContentId : 6326fcb2-c465-4c24-a7f6-1cace7a9cb6f
Issuer : admin@aip500.onmicrosoft.com
Owner : admin@aip500.onmicrosoft.com
ContentName :
CreatedTime : 3/6/2018 10:24:00 PM
Recipients :
 PrimaryEmail: johndoe@contoso.com
 DisplayName: JOHNDOE@CONTOSO.COM
 UserType: External,
 PrimaryEmail: alice@contoso0110.onmicrosoft.com
 DisplayName: ALICE@CONTOSO0110.ONMICROSOFT.COM
 UserType: External
TemplateId :
PolicyExpires :
EULDuration :
SendRegistrationEmail : True
NotificationInfo : Enabled: False
 DeniedOnly: False
 Culture:
 TimeZoneId:
 TimeZoneOffset: 0
 TimeZoneDaylightName:
 TimeZoneStandardName:

RevocationInfo : Revoked: False
 RevokedTime:
 RevokedBy:
```

```
PS C:\Users> Get-AipServiceTrackingLog -UserEmail "admin@aip500.onmicrosoft.com"
```

```
ContentId : 6326fcb2-c465-4c24-a7f6-1cace7a9cb6f
Issuer : admin@aip500.onmicrosoft.com
RequestTime : 3/6/2018 10:45:57 PM
RequesterType : External
RequesterEmail : johndoe@contoso.com
RequesterDisplayName : johndoe@contoso.com
RequesterLocation : IP: 167.220.1.54
 Country: US
 City: redmond
 Position: 47.6812453974602, -122.120736471666

Rights : {VIEW,OBJMODEL}
Successful : False
IsHiddenInfo : False
```

There is no search by ObjectId. However, you are not restricted by the `-UserEmail` parameter and the email address you provide doesn't need to be part of your tenant. If the email address provided is stored anywhere in the document tracking logs, the document tracking entry is returned in the cmdlet output.

### Usage logs for the Azure Information Protection clients and RMS client

When labels and protection are applied to documents and emails, email addresses and IP addresses can be stored in log files on a user's computer in the following locations:

- For the Azure Information Protection unified labeling client and the Azure Information Protection client:  
%localappdata%\Microsoft\MSIP\Logs
- For the RMS client: %localappdata%\Microsoft\MSIPC\msip\Logs

In addition, the Azure Information Protection client logs this personal data to the local Windows event log

## Applications and Services Logs > Azure Information Protection.

When the Azure Information Protection client runs the scanner, personal data is saved to %localappdata%\Microsoft\MSIP\Scanner\Reports on the Windows Server computer that runs the scanner.

You can turn off logging information for the Azure Information Protection client and the scanner by using the following configurations:

- For the Azure Information Protection client: Create an [advanced client setting](#) that configures the **LogLevel** to Off.
- For the Azure Information Protection scanner: Use the [Set-AIPScannerConfiguration](#) cmdlet to set the *ReportLevel* parameter to Off.

### NOTE

If you're interested in viewing or deleting personal data, please review Microsoft's guidance in the [Microsoft Compliance Manager](#) and in the [GDPR section of the Microsoft 365 Enterprise Compliance](#) site. If you're looking for general information about GDPR, see the [GDPR section of the Service Trust portal](#).

## Securing and controlling access to personal information

Personal data that you view and specify in the Azure portal is accessible only to users who have been assigned one of the following [administrator roles from Azure Active Directory](#):

- **Azure Information Protection administrator**
- **Compliance administrator**
- **Compliance data administrator**
- **Security administrator**
- **Security reader**
- **Global administrator**
- **Global reader**

Personal data that you view and specify by using the AIPService module (or the older module, AADRM) is accessible only to users who have been assigned the **Azure Information Protection administrator**, **Compliance administrator**, **Compliance data administrator**, or **Global Administrator** roles from Azure Active Directory, or the global administrator role for the protection service.

## Updating personal data

You can update email addresses for scoped policies and protection settings in the Azure Information Protection policy. For more information, see [How to configure the Azure Information Protection policy for specific users by using scoped policies](#) and [How to configure a label for Rights Management protection](#).

For the protection settings, you can update the same information by using PowerShell cmdlets from the [AIPService module](#).

You cannot update email addresses for the super users and delegated administrators. Instead, remove the specified user account, and add the user account with the updated email address.

### Protection templates

Run the [Set-AipServiceTemplateProperty](#) cmdlet to update the protection template. Because the personal data is

within the `RightsDefinitions` property, you will also need to use the `New-AipServiceRightsDefinition` cmdlet to create a rights definitions object with the updated information, and use the rights definitions object with the `Set-AipServiceTemplateProperty` cmdlet.

## Super users and delegated administrators for the protection service

When you need update an email address for a super user:

1. Use `Remove-AipServiceSuperUser` to remove the user and old email address.
2. Use `Add-AipServiceSuperUser` to add the user and new email address.

When you need update an email address for a delegated administrator:

1. Use `Remove-AipServiceRoleBasedAdministrator` to remove the user and old email address.
2. Use `Add-AipServiceRoleBasedAdministrator` to add the user and new email address.

## Deleting personal data

You can delete email addresses for scoped policies and protection settings in the Azure Information Protection policy. For more information, see [How to configure the Azure Information Protection policy for specific users by using scoped policies](#) and [How to configure a label for Rights Management protection](#).

For the protection settings, you can delete the same information by using PowerShell cmdlets from the [AIPService module](#).

To delete email addresses for super users and delegated administrators, remove these users by using the `Remove-AipServiceSuperUser` cmdlet and `Remove-AipServiceRoleBasedAdministrator`.

To delete personal data in document tracking logs, administration logs, or usage logs for the protection service, use the following section to raise a request with Microsoft Support.

To delete personal data in the client log files and scanner logs that are stored on computers, use any standard Windows tools to delete the files or personal data within the files.

### To delete personal data with Microsoft Support

Use the following three steps to request that Microsoft deletes personal data in document tracking logs, administration logs, or usage logs for the protection service.

**Step 1: Initiate delete request** [Contact Microsoft Support](#) to open an Azure Information Protection support case with a request for deleting data from your tenant. You must prove that you are an administrator for your Azure Information Protection tenant and understand that this process takes several days to confirm. While submitting your request, you will need to provide additional information, depending on the data that needs to be deleted.

- To delete the administration log, provide the **end date**. All admin logs until that end date will be deleted.
- To delete the usage logs, provide the **end date**. All usage logs until that end date will be deleted.
- To delete the document tracking logs, provide the **UserEmail**. All document tracking information relating to the **UserEmail** will be deleted.

Deleting this data is a permanent action. There is no means to recover the data after a delete request has been processed. It is recommended that administrators export the required data before submitting a delete request.

**Step 2: Wait for verification** Microsoft will verify that your request to delete one or more logs is legitimate. This process can take up to five working days.

**Step 3: Get confirmation of the deletion** Microsoft Customer Support Services (CSS) will send you a confirmation email that the data has been deleted.

## Exporting personal data

When you use the AIPService or AADRM PowerShell cmdlets, the personal data is made available for search and export as a PowerShell object. The PowerShell object can be converted into JSON and saved by using the `ConvertTo-Json` cmdlet.

## Restricting the use of personal data for profiling or marketing without consent

Azure Information Protection follows Microsoft's [privacy terms](#) for profiling or marketing based on personal data.

## Auditing and reporting

Only users who have been assigned [administrator permissions](#) can use the AIPService or ADDRM module for search and export of personal data. These operations are recorded in the administration log that can be downloaded.

For delete actions, the support request acts as the auditing and reporting trail for the actions performed by Microsoft. After deletion, the deleted data will not be available for search and export, and the administrator can verify this using the Get cmdlets from the AIPService module.

# Decommissioning and deactivating protection for Azure Information Protection

7/20/2020 • 4 minutes to read • [Edit Online](#)

Applies to: [Azure Information Protection](#), [Office 365](#)

You are always in control of whether your organization protects content by using the Azure Rights Management service from Azure Information Protection. If you decide you no longer want to use this information protection service, you have the assurance that you won't be locked out of content that was previously protected.

If you don't need continued access to previously protected content, deactivate the service and let your subscription for Azure Information Protection expire. For example, this would be appropriate for when you have completed testing Azure Information Protection before you deploy it in a production environment.

However, if you have deployed Azure Information Protection in production and protected documents and emails, make sure that you have a copy of your Azure Information Protection tenant key and suitable trusted publishing domain (TPD) before you deactivate the Azure Rights Management service. Make sure that you have a copy of your key and the TPD before your subscription expires to ensure that you can retain access to content that was protected by Azure Rights Management after the service is deactivated.

If you used the bring your own key solution (BYOK) where you generate and manage your own key in an HSM, you already have your Azure Information Protection tenant key. You will also have a suitable TPD if you followed the instructions that [prepare for a future cloud exit](#). However, if your tenant key was managed by Microsoft (the default), see the instructions for exporting your tenant key in [Operations for your Azure Information Protection tenant key](#) article.

## TIP

Even after your subscription expires, your Azure Information Protection tenant remains available for consuming content for an extended period. However, you will no longer be able to export your tenant key.

When you have your Azure Information Protection tenant key and the TPD, you can deploy Rights Management on premises (AD RMS) and import your tenant key as a trusted publishing domain (TPD). You then have the following options for decommissioning your Azure Information Protection deployment:

IF THIS APPLIES TO YOU ...	... DO THIS:
You want all users to continue using Rights Management, but use an on-premises solution rather than using Azure Information Protection →	Redirect your clients to the on-premises deployment by using the <b>LicensingRedirection</b> registry key for Office 2016 or Office 2013. For instructions, see the <a href="#">service discovery section</a> in the RMS client deployment notes. For Office 2010, use the <b>LicenseServerRedirection</b> registry key for Office 2010, as described in <a href="#">Office Registry Settings</a> .

IF THIS APPLIES TO YOU ...	... DO THIS:
You want to stop using Rights Management technologies completely →	<p>Grant a designated administrator <a href="#">super user rights</a> and install the <a href="#">Azure Information Protection client</a> for this user.</p> <p>This administrator can then use the PowerShell module from this client to bulk-decrypt files in folders that were protected by Azure Information Protection. Files revert to being unprotected and can therefore be read without a Rights Management technology such as Azure Information Protection or AD RMS. Because this PowerShell module can be used with both Azure Information Protection and AD RMS, you have the choice of decrypting files before or after you deactivate the protection service from Azure Information Protection, or a combination.</p>
You are not able to identify all the files that were protected by Azure Information Protection. Or, you want all users to be able to automatically read any protected files that were missed →	<p>Deploy a registry setting on all client computers by using the <a href="#">LicensingRedirection</a> registry key for Office 2016 and Office 2013, as described in the <a href="#">service discovery section</a> in the RMS client deployment notes. For Office 2010, use the <a href="#">LicenseServerRedirection</a> registry key, as described in <a href="#">Office Registry Settings</a>.</p> <p>Also deploy another registry setting to prevent users from protecting new files by setting <a href="#">DisableCreation</a> to 1, as described in <a href="#">Office Registry Settings</a>.</p>
You want a controlled, manual recovery service for any files that were missed →	<p>Grant designated users in a data recovery group <a href="#">super user rights</a> and install the <a href="#">Azure Information Protection client</a> for these users so that they can unprotect files when this action is requested by standard users.</p> <p>On all computers, deploy the registry setting to prevent users from protecting new files by setting <a href="#">DisableCreation</a> to 1, as described in <a href="#">Office Registry Settings</a>.</p>

For more information about the procedures in this table, see the following resources:

- For information about AD RMS and deployment references, see [Active Directory Rights Management Services Overview](#).
- For instructions to import your Azure Information Protection tenant key as a TPD file, see [Add a Trusted Publishing Domain](#).
- To use PowerShell with the Azure Information Protection client, see [Using PowerShell with the Azure Information Protection client](#).

When you are ready to deactivate the protection service from Azure Information Protection, use the following instructions.

## Deactivating Rights Management

Use one of the following procedures to deactivate the protection service, Azure Rights Management.

### TIP

You can also use the PowerShell cmdlet, [Disable-AipService](#), to deactivate Rights Management.

**To deactivate Rights Management from the Microsoft 365 admin center**

1. Go to the [Rights Management page](#) for Office 365 administrators.

If you are prompted to sign in, use an account that is a global administrator for Office 365.

2. On the **rights management** page, click **deactivate**.
3. When prompted **Do you want to deactivate Rights Management?** click **deactivate**.

You should now see **Rights Management is not activated** and the option to activate.

**To deactivate Rights Management from the Azure portal**

1. If you haven't already done so, open a new browser window and [sign in to the Azure portal](#). Then navigate to the **Azure Information Protection** pane.

For example, in the search box for resources, services, and docs: Start typing **Information** and select **Azure Information Protection**.

2. On the initial **Azure Information Protection** pane, select **Protection activation**.
3. On the **Azure Information Protection - Protection activation** pane, select **Deactivate**. Select **Yes** to confirm your choice.

The information bar displays **Deactivation finished successfully** and **Deactivate** is now replaced with **Activate**.

# Administering protection from Azure Information Protection by using PowerShell

4/28/2020 • 2 minutes to read • [Edit Online](#)

Applies to: [Azure Information Protection](#), [Office 365](#)

Do you need to use PowerShell to administer the protection service from Azure Information Protection? You might not need to if all your configuration can be done in the Azure portal or the Microsoft 365 admin center. However, you need to use PowerShell for some advanced configurations and you might also prefer to use PowerShell for more efficient command-line control and scripting.

The table in the next section includes some of the advanced configuration scenarios that use PowerShell. When the configuration can also be completed without using PowerShell, this information is also included in the table.

For a complete list of the available cmdlets for this module, with more information about each one, see [AIPService](#).

## NOTE

To install this PowerShell module, see [Installing the AIPService PowerShell module](#).

In addition to this service-side PowerShell module, the Azure Information Protection client installs a supplemental PowerShell module, **AzureInformationProtection**. This client module supports classifying and protecting multiple files so that, for example, you can bulk-protect all files in a folder. For more information, see [Using PowerShell with the Azure Information Protection client](#) from the admin guide.

## Cmdlets grouped by administration task

IF YOU NEED TO...	...USE THE FOLLOWING CMDLETS
Migrate from on-premises Rights Management (AD RMS or Windows RMS) to Azure Information Protection.	<a href="#">Import-AipServiceTpD</a> <a href="#">Set-AipServiceKeyProperties</a>
Connect to or disconnect from the Rights Management service for your organization.	<a href="#">Connect-AipService</a> <a href="#">Disconnect-AipServiceService</a>
Generate and manage your own tenant key – the bring your own key (BYOK) scenario.	<a href="#">Set-AipServiceKeyProperties</a> <a href="#">Use-AipServiceKeyVaultKey</a> <a href="#">Get-AipServiceKeys</a>
Activate or deactivate the Rights Management service for your organization.  You can also do these actions from the management portals. For more information, see <a href="#">Activating the protection service from Azure Information Protection</a> .	<a href="#">Enable-AipService</a> <a href="#">Disable-AipService</a>

IF YOU NEED TO...	...USE THE FOLLOWING CMDETS
Manage the document tracking site for Azure Information Protection.	<a href="#">Disable-AipServiceDocumentTrackingFeature</a> <a href="#">Enable-AipServiceDocumentTrackingFeature</a> <a href="#">Get-AipServiceDocumentTrackingFeature</a> <a href="#">Set-AipServiceDoNotTrackUserGroup</a> <a href="#">Clear-AipServiceDoNotTrackUserGroup</a> <a href="#">Get-AipServiceDoNotTrackUserGroup</a> <a href="#">Get-AipServiceTrackingLog</a> <a href="#">Get-AipServiceDocumentLog</a>
Configure onboarding controls for a phased deployment of the Azure Rights Management service.	<a href="#">Get-AipServiceOnboardingControlPolicy</a> <a href="#">Set-AipServiceOnboardingControlPolicy</a>
<p>Create and manage Rights Management templates for your organization.</p> <p>You can also do most of these actions from the Azure portal, although PowerShell offers more fine-grain control. For more information, see <a href="#">Configuring and managing templates for Azure Information Protection</a>.</p>	<a href="#">Add-AipServiceTemplate</a> <a href="#">Export-AipServiceTemplate</a> <a href="#">Get-AipServiceTemplate</a> <a href="#">Get-AipServiceTemplateProperty</a> <a href="#">Import-AipServiceTemplate</a> <a href="#">New-AipServiceRightsDefinition</a> <a href="#">Remove-AipServiceTemplate</a> <a href="#">Set-AipServiceTemplateProperty</a>
Configure the maximum number of days that content that your organization protects can be accessed without an internet connection (the use license validity period).	<a href="#">Get-AipServiceMaxUseLicenseValidityTime</a> <a href="#">Set-AipServiceMaxUseLicenseValidityTime</a>
Manage the super user feature of Rights Management for your organization.	<a href="#">Enable-AipServiceSuperUserFeature</a> <a href="#">Disable-AipServiceSuperUserFeature</a> <a href="#">Add-AipServiceSuperUser</a> <a href="#">Get-AipServiceSuperUser</a> <a href="#">Remove-AipServiceSuperUser</a> <a href="#">Set-AAipServiceSuperUserGroup</a> <a href="#">Get-AipServiceSuperUserGroup</a> <a href="#">Clear-AipServiceSuperUserGroup</a>

IF YOU NEED TO...	...USE THE FOLLOWING CMDETS
Manage users and groups who are authorized to administer the Rights Management service for your organization.	<a href="#">Add-Aip-ServiceRoleBasedAdministrator</a> <a href="#">Get-Aip-ServiceRoleBasedAdministrator</a> <a href="#">Remove-Aip-ServiceRoleBasedAdministrator</a>
Get a log of Rights Management administrative tasks for your organization.	<a href="#">Get-AipServiceAdminLog</a>
Log and analyze usage logging for Rights Management.	<a href="#">Get-AipServiceUserLog</a>
Display the current Rights Management service configuration for your organization.	<a href="#">Get-AipServiceConfiguration</a>
Migrate your organization from Azure Information Protection to an on-premises AD RMS deployment.	<a href="#">Set-AipServiceMigrationUrl</a> <a href="#">Get-AipServiceMigrationUrl</a>

# Installing the AIPService PowerShell module

7/20/2020 • 3 minutes to read • [Edit Online](#)

Applies to: [Azure Information Protection](#), [Office 365](#)

Use the following information to help you install the Windows PowerShell module for the protection service from Azure Information Protection. The name of this module is AIPService, and it replaces the previous version that was named AADRM.

You can use this PowerShell module to administer the protection service (Azure Rights Management) from the command line by using any Windows computer that has an internet connection and that meets the prerequisites listed in the next section. Windows PowerShell for Azure Information Protection supports scripting for automation or might be necessary for advanced configuration scenarios. For more information about the administration tasks and configurations that the module supports, see [Administering protection from Azure Information Protection by using PowerShell](#).

## Prerequisites

This table lists the prerequisites to install and use the AIPService PowerShell module for the protection service from Azure Information Protection.

Requirement	More Information
Minimum version of Windows PowerShell: 3.0	You can confirm the version of Windows PowerShell that you are running by typing <code>\$PSVersionTable</code> in a PowerShell session.  If you need to install a later version of Windows PowerShell, see <a href="#">Upgrading existing Windows PowerShell</a> .
Minimum version of the Microsoft .NET Framework: 4.5  Note: This version of the Microsoft .NET Framework is included with the later operating systems, so you should need to manually install it only if your client operating system is less than Windows 8.0 or your server operating system is less than Windows Server 2012.	If the minimum version of the Microsoft .NET Framework is not already installed, you can download <a href="#">Microsoft .NET Framework 4.5</a> .  This minimum version of the Microsoft .NET Framework is required for some of the classes that the AIPService module uses.

## If you have the AADRM module installed

The AIPService module replaces the older module, AADRM. If you have the older module installed, uninstall it and then install the AIPService module.

The newer module has aliases to the cmdlet names in the older module so that any existing scripts will continue to work. However, plan to update these references before the old module falls out of support. Support for the AADRM module will end July 15, 2020.

If you installed the AADRM module from the PowerShell Gallery, to uninstall it, start a PowerShell session with the **Run as Administrator** option, and type:

```
Uninstall-Module -Name AADRM
```

If you installed the AADRM module with the Azure Rights Management Administration Tool, use **Programs and Features** to uninstall Windows Azure AD Rights Management Administration.

## How to install the AIPService module

The AIPService module is on the [PowerShell Gallery](#) and is not available from the Microsoft Download Center.

### To install the AIPService module from the PowerShell Gallery

If you're new to the PowerShell Gallery, see [Get Started with the PowerShell Gallery](#). Follow the instructions for the gallery requirements, which include installing the PowerShellGet module and the NuGet provider.

To see details about the AIPService module on the PowerShell Gallery, visit the [AIPService page](#).

To install the AIPService module, start a PowerShell session with the **Run as Administrator** option, and type:

```
Install-Module -Name AIPService
```

If you are warned about installing from an untrusted repository, you can press Y to confirm. Or, press N and configure the PowerShell Gallery as a trusted repository by using the command

`Set-PSRepository -Name PSGallery -InstallationPolicy Trusted` and then rerun the command to install the AIPService module.

If you have a previous version of the AIPService module installed from the Gallery, update it to the latest by typing:

```
Update-Module -Name AIPService
```

## Next steps

In a Windows PowerShell session, confirm the version of the installed module. This check is particularly important if you upgraded from an older version:

```
(Get-Module AIPService -ListAvailable).Version
```

### NOTE

If this command fails, first run **Import-Module AIPService**.

To see which cmdlets are available, type the following:

```
Get-Command -Module AIPService
```

Use the `Get-Help <cmdlet_name>` command to see the Help for a specific cmdlet, and use the **-online** parameter to see the latest help on the Microsoft documentation site. For example:

```
Get-Help Connect-AipService -online
```

For more information:

- Full list of cmdlets available: [AIPService Module](#)
- List of main configuration scenarios that support PowerShell: [Administering protection from Azure](#)

## Information Protection by using PowerShell

Before you can run any commands that configure the protection service, you must connect to the service by using the [Connect-AipService](#) cmdlet.

When you have finished running your configuration commands, as a best practice, disconnect from the service by using the [Disconnect-AipService](#) cmdlet. If you do not disconnect, the connection is automatically disconnected after a period of inactivity. Because of the automatic disconnection behavior, you might find that you need to occasionally reconnect in a PowerShell session.

### NOTE

If the protection service is not yet activated, you can do this after you have connected to the service, by using the [Enable-AipService](#) cmdlet.

# The client side of Azure Information Protection

7/20/2020 • 14 minutes to read • [Edit Online](#)

*Applies to: Active Directory Rights Management Services, Azure Information Protection, Windows 10, Windows 8.1, Windows 8, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012*

## NOTE

To provide a unified and streamlined customer experience, **Azure Information Protection client (classic)** and **Label Management** in the Azure Portal are being **deprecated** as of March 31, 2021. This time-frame allows all current Azure Information Protection customers to transition to our unified labeling solution using the Microsoft Information Protection Unified Labeling platform. Learn more in the official [deprecation notice](#).

Azure Information Protection provides a client-server solution that helps to protect an organization's documents and emails:

- The client can be the built-in labeling client for Office, the Azure Information Protection unified labeling client for Windows, the Azure Information Protection client (classic) for Windows, or the Rights Management client.

These clients are often referred to as the **Office built-in labeling client**, the **unified labeling client**, the **classic client**, and the **RMS client**, respectively. Whichever client you use, it integrates with applications that you run on computers and mobile devices.

- The service resides in the cloud or on-premises. The cloud service is Azure Information Protection, which uses the Azure Rights Management service for the data protection. The on-premises service is Active Directory Rights Management Services, more commonly known as AD RMS.

All these clients integrate with Office applications but the unified labeling client and the classic client must be installed separately and support additional features and components. For example, these clients include support for File Explorer, so you can classify and protect files outside Office. Additional components include a viewer for protected PDF documents and protected images, and a scanner for on-premises data stores.

The RMS client provides protection only. This client is automatically installed with some applications, such as Office applications, the Azure Information Protection clients, and RMS-enlightened applications from software vendors. However, it can also be [installed by itself](#), to support [synchronizing files from IRM-protected libraries and OneDrive](#), and for developers who want to integrate rights management protection into line-of-business applications.

## Choose which labeling client to use for Windows computers

Where possible, use one of the labeling clients because labels abstract the complexity of applying protection for users, and labels also provide classification so you can track and manage your data.

Your choice of labeling client for your Windows computers might be influenced by which management portal you use:

- The Office built-in labeling client and the Azure Information Protection unified labeling client download labels and policy settings from the following admin centers:
  - Office 365 Security & Compliance Center

- Microsoft 365 security center
- Microsoft 365 compliance center
- The Azure Information Protection client (classic) downloads label and policy settings from the Azure portal.

Because the unified labeling client and the classic client require a separate installation to Office, you must download and install these clients from the [Microsoft Download Center](#).

Use the following sections to help you determine which client is best for your organization:

- [Built-in Office labeling client](#)
- [Azure Information Protection unified labeling client](#)
- [Azure Information Protection classic client](#)
- [Using multiple clients in the same environment](#)

For more information, see: [Detailed comparisons for the AIP clients](#) and [Features not planned for the unified labeling client](#).

#### **NOTE**

The latest version of the unified labeling client brings it to close parity in features with the classic client. As this gap closes, you can expect new features to be added only to the unified labeling client.

We recommend that you deploy the unified labeling client if its current feature set and functionality meet your business requirements.

### **Built-in Office labeling client**

The labeling client that's built in to Microsoft Office:

- Requires a Windows computer with Office 365 applications, minimum version 1910
- Enables you to share labels and policy settings that can also be used by macOS, iOS, and Android
- Supports switching accounts
- Provides better performance in Office applications
- Does not require a separate installation and maintenance
- Cannot be disabled.

**Don't use** the built-in Office labeling client if you need features provided only by the classic or unified labeling clients, such as the Information Protection bar under the ribbon. This bar provides easier label selection and visibility.

### **Azure Information Protection unified labeling client**

The unified labeling client requires a Windows computer, and enables you to share labels and policy settings that can also be used by macOS, iOS, and Android.

**Don't use** the unified labeling client if the current unified labeling features not meet your business requirements, or if you have configured labels in the Azure portal that you haven't yet [migrated to the unified labeling store](#).

### **Azure Information Protection classic client**

The classic client:

- Requires a Windows computer
- Provides access to features not yet available on the unified labeling client, such as holding your own on-premises key (HYOK), and a general availability version of the scanner for on-premises data stores.
- Enables you to share labels with macOS, iOS, and Android

However, the classic client has different policy settings for macOS, iOS, and Android. So, while you may want to use

the additional features, you'll have to work with a separate management portal and user experience to protect content across operating systems.

**Don't use** the classic client if you want newer features available only in the unified labeling client, or to provide a centralized, unified user experience.

### Using multiple clients in the same environment

You can use different clients in the same environment to support different business requirements, as demonstrated in the following deployment example. In a mixed client environment, we recommend you use unified labels so that clients share the same set of labels for ease of administration. New customers have unified labels by default because their tenants are on the unified labeling platform. For more information, see [How can I determine if my tenant is on the unified labeling platform?](#)

When you have a Windows computer that runs Office 365 apps that are a minimum version 1910 and one of the Azure Information Protection clients is installed, by default the built-in labeling client is disabled in Office apps. However, you can change this behavior to use the built-in labeling client for just your Office apps. With this configuration, the Azure Information Protection client (classic or unified labeling) remains available for labeling in File Explorer, PowerShell, and the scanner. For instructions to disable the Azure Information Protection client in Office 365 apps, see the section [Office built-in labeling client and the Azure Information Protection client](#) from the Microsoft 365 Compliance documentation.

#### Example deployment strategy:

- For the majority of users, you deploy the Azure Information Protection unified labeling client because this client meets the business needs for these users.

For these users, their labeling experience is similar across Windows, Mac, iOS, and Android because they have the same labels published to them and the same policy settings. As an admin, you manage these labels and policy settings in the same management center.

- You also install the unified labeling client for yourself, to test the Azure Information Protection scanner.
- For a subset of users, you deploy the classic client because these users require labels that apply hold your own key (HYOK) protection.

For these users, they have a slightly different labeling experience when they use this client. For example, they see a **Protect** button rather than a **Sensitivity** button in Office apps. As an admin, you need to manage their labels for HYOK settings and policy settings in a different management center to the labels and settings for the other client platforms.

- You have on-premises data stores with documents that need to be scanned for sensitive information, or classified and protected. For production use, you deploy the classic client on servers to run the Azure Information Protection scanner.

## Compare the labeling clients for Windows computers

Use the following table to help compare which features are supported by the three labeling clients for Windows computers.

To compare the Office built-in sensitivity labeling features across different operating system platforms (Windows, macOS, iOS, and Android) and for the web, see the Microsoft 365 Compliance documentation, [Support for sensitivity label capabilities in apps](#). This documentation also includes the Office build numbers or Office update channel information for the supported features.

FEATURE	CLASSIC CLIENT	UNIFIED LABELING CLIENT	OFFICE BUILT-IN LABELING CLIENT
Manual labeling:	Yes	Yes	Yes

FEATURE	CLASSIC CLIENT	UNIFIED LABELING CLIENT	OFFICE BUILT-IN LABELING CLIENT
Default label:	Yes	Yes	Yes
Recommended or automatic labeling: - For Word, Excel, PowerPoint	Yes	Yes	Yes
Recommended or automatic labeling: - For Outlook	Yes	Yes	No
Mandatory labeling:	Yes	Yes	No
User-defined permissions for a label: - Do Not Forward for emails	Yes	Yes	Yes
User-defined permissions for a label: - Custom permissions for Word, Excel, PowerPoint	Yes	Yes	Yes
Multilanguage support for labels:	Yes	Yes	Yes
Label inheritance from email attachments:	Yes	Yes	No
Customizations that include: - Default label for email - Pop up messages in Outlook - S/MIME support - Report an Issue option	Yes <sup>1</sup>	Yes <sup>2</sup>	No
Scanner for on-premises data stores:	Yes	Yes	No
Central reporting (analytics):	Yes	Yes	No
Custom permissions set independently from a label:	Yes	Yes <sup>3</sup>	No
Information Protection bar in Office apps:	Yes	Yes	No
Visual markings as a label action (header, footer, watermark):	Yes	Yes	Yes
Per app visual markings:	Yes	Yes	No
Dynamic visual markings with variables:	Yes	Yes	No

FEATURE	CLASSIC CLIENT	UNIFIED LABELING CLIENT	OFFICE BUILT-IN LABELING CLIENT
Label with File Explorer:	Yes	Yes	No
A viewer for protected files (text, images, PDF, .pfile):	Yes	Yes	No
PPDF support for applying labels:	Yes	No	No
PowerShell labeling cmdlets:	Yes	Yes <sup>4</sup>	No
Offline support for protection actions:	Yes	Yes <sup>5</sup>	Yes
Manual policy file management for disconnected computers:	Yes	Yes	No
HYOK support:	Yes	No	No
Usage logging in Event Viewer:	Yes	No	No
Display the Do Not Forward button in Outlook:	Yes	No	No
Track protected documented:	Yes	Yes <sup>6</sup>	No
Revoke protected documents:	Yes	No	No
Protection-only mode (no labels):	Yes	No	No
Support for account switching:	No	No	Yes
Support for Remote Desktop Services:	Yes	Yes	Yes
Support for AD RMS:	Yes	No <sup>7</sup>	No
Remove external content marking in app:	Yes	Yes	No

Footnotes:

<sup>1</sup> These settings, and many more are supported as [advanced client settings that you configure in the Azure portal](#).

<sup>2</sup> These settings, and many more are supported as [advanced settings that you configure with PowerShell](#).

<sup>3</sup> Supported by File Explorer and PowerShell. In Office apps, users can select **File Info > Protect Document > Restrict Access**.

<sup>4</sup> No support to remove protection from container files (zip).

<sup>5</sup> For File Explorer and PowerShell commands, the user must be connected to the internet to protect files.

<sup>6</sup> The document tracking site that's supported by the classic client isn't supported by the unified labeling client. However, without the need to first register the document for tracking, administrators can use [central reporting](#) to identify whether protected documents are accessed from Windows computers, and whether access was granted or denied.

<sup>7</sup> Labeling and protection actions aren't supported. However, for an AD RMS deployment, the viewer can open protected documents when you use the [Active Directory Rights Management Services Mobile Device Extension](#).

### Detailed comparisons for the Azure Information Protection clients

When the Azure Information Protection client (classic) and the Azure Information Protection unified labeling client both support the same feature, use the following table to help identify some functional differences between the two clients.

FUNCTIONALITY	CLASSIC CLIENT	UNIFIED LABELING CLIENT
Setup:	Option to install local demo policy	No local demo policy
Label selection and display when applied in Office apps:	From the <b>Protect</b> button on the ribbon  From the Information Protection bar (horizontal bar under the ribbon)	From the <b>Sensitivity</b> button on the ribbon  From the Information Protection bar (horizontal bar under the ribbon)
Manage the Information Protection bar in Office apps:	For users:  - Option to show or hide the bar from the <b>Protect</b> button on the ribbon  - When a user selects to hide the bar, by default, the bar is hidden in that app, but continues to automatically display in newly opened apps  For admins:  - Policy settings to automatically show or hide the bar when an app first opens, and control whether the bar automatically remains hidden for newly opened apps after a user selects to hide the bar	For users:  - Option to show or hide the bar from the <b>Sensitivity</b> button on the ribbon  - When a user selects to hide the bar, the bar is hidden in that app and also in newly opened apps  For admins:  - PowerShell setting to manage the bar
Label color:	Configure in the Azure portal	Retained after label migration and configurable with <a href="#">PowerShell</a>
Labels support different languages:	Configure in the Azure portal	Configure by using <a href="#">Office 365 Security &amp; Compliance PowerShell</a>

FUNCTIONALITY	CLASSIC CLIENT	UNIFIED LABELING CLIENT
Policy update:	<p>When an Office app opens</p> <p>When you right-click to classify and protect a file or folder</p> <p>When you run the PowerShell cmdlets for labeling and protection</p> <p>Every 24 hours</p> <p>For the scanner: Every hour and when the service starts and the policy is older than one hour</p>	<p>When an Office app opens</p> <p>When you right-click to classify and protect a file or folder</p> <p>When you run the PowerShell cmdlets for labeling and protection</p> <p>Every 4 hours</p> <p>For the scanner: Every 4 hours</p>
Supported formats for PDF:	<p>Protection:</p> <ul style="list-style-type: none"> <li>- ISO standard for PDF encryption (default)</li> <li>- .ppdf</li> </ul> <p>Consumption:</p> <ul style="list-style-type: none"> <li>- ISO standard for PDF encryption</li> <li>- .ppdf</li> <li>- SharePoint IRM protection</li> </ul>	<p>Protection:</p> <ul style="list-style-type: none"> <li>- ISO standard for PDF encryption</li> </ul> <p>Consumption:</p> <ul style="list-style-type: none"> <li>- ISO standard for PDF encryption</li> <li>- .ppdf</li> <li>- SharePoint IRM protection</li> </ul>
Generically protected files (.pfile) opened with the viewer:	File opens in the original app where it can then be viewed, modified, and saved without protection	File opens in the original app where it can then be viewed and modified, but not saved

FUNCTIONALITY	CLASSIC CLIENT	UNIFIED LABELING CLIENT
Supported cmdlets:	<p>Cmdlets for labeling and cmdlets for protection-only</p>	<p>Cmdlets for labeling: Set-AIPFileClassification and Set-AIPFileLabel don't support the <i>Owner</i> parameter</p> <p>In addition, there is a single comment of "No label to apply" for all scenarios where a label isn't applied</p> <p>Set-AIPFileClassification supports the <i>WhatIf</i> parameter, so it can be run in discovery mode</p> <p>Set-AIPFileLabel doesn't support the <i>EnableTracking</i> parameter</p> <p>Get-AIPFileStatus doesn't return label information from other tenants and doesn't display the <i>RMSIssuedTime</i> parameter</p> <p>In addition, the <i>LabelingMethod</i> parameter for Get-AIPFileStatus displays <b>Privileged</b> or <b>Standard</b> instead of <b>Manual</b> or <b>Automatic</b>. For more information, see the <a href="#">online documentation</a>.</p>
Justification prompts (if configured) per action in Office:	<p>Frequency: Per file Lowering the sensitivity level Removing a label Removing protection</p>	<p>Frequency: Per session Lowering the sensitivity level Removing a label</p>
Remove applied label actions:	<p>User is prompted to confirm Default label or automatic label (if configured) isn't automatically applied next time the Office app opens the file</p>	<p>User isn't prompted to confirm Default label or automatic label (if configured) is automatically applied next time the Office app opens the file</p>

FUNCTIONALITY	CLASSIC CLIENT	UNIFIED LABELING CLIENT
Automatic and recommended labels:	<p>Configured as <a href="#">label conditions</a> in the Azure portal with built-in information types and custom conditions that use phrases or regular expressions</p> <p>Configuration options include:</p> <ul style="list-style-type: none"> <li>- Unique / Not unique count</li> <li>- Minimum count</li> </ul>	<p>Configured in the admin centers with built-in sensitive information types and <a href="#">custom information types</a></p> <p>Configuration options include:</p> <ul style="list-style-type: none"> <li>- Unique count only</li> <li>- Minimum and maximum count</li> <li>- AND and OR support with information types</li> <li>- Keyword dictionary</li> <li>- Customizable confidence level and character proximity</li> </ul>
Order support for sublabels on attachments:	Enabled with an <a href="#">advanced client setting</a>	Enabled by default, no configuration required
Change the default protection behavior for file types:	You can use <a href="#">registry edits</a> to override the defaults of native and generic protection	You can use <a href="#">PowerShell</a> to change which file types get protected

For a detailed comparison of behavior differences for specific protection settings, see [Comparing the behavior of protection settings for a label](#).

### Features not planned to be in the Azure Information Protection unified labeling client

Although the Azure Information Protection unified labeling client is still under development, the following features and behavior differences from the classic client are not currently planned to be available in future releases for the unified labeling client:

- Custom permissions as a [separate option that users can select in Office apps: Word, Excel, and PowerPoint](#)
- [Track and revoke](#) options from Office apps and File Explorer
- Information Protection bar title and tooltip
- [Protection-only mode](#) (no labels) using templates
- Protect PDF document as [.ppdf \(older format\)](#)
- Display the Do Not Forward button in Outlook
- Demo policy
- Confirmation prompt **Do you want to delete this label?** for users when you don't use the policy setting for justification
- Separate PowerShell cmdlets to connect to a Rights Management service
- Display of the user identity that applied a label

### Parent labels and their sublabels

The Azure Information Protection client (classic) doesn't support configurations that specify a parent label that has sublabels. These configurations include specifying a default label, and a label for recommended or automatic classification. When a label has sublabels, you can specify one of the sublabels but not the parent label.

For parity, the Azure Information Protection unified labeling client also doesn't support applying parent labels that have sublabels, even though you can select these labels in the admin centers. In this scenario, the Azure Information Protection unified labeling client will not apply the parent label.

## Next steps

To install and configure the Azure Information Protection clients, use the following documentation:

- [Azure Information Protection client](#)
- [Azure Information Protection unified labeling client](#)

For more information about using the built-in labeling client for Office 365 apps, see [Sensitivity labels in Office apps](#).

# Azure Information Protection unified labeling client for Windows

7/20/2020 • 2 minutes to read • [Edit Online](#)

*Applies to:* [Azure Information Protection](#), Windows 10, Windows 8.1, Windows 8, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

*\*Customers with extended Microsoft support for Windows 7 and Office 2010 can also get Azure Information Protection support for these versions. Check with your support contact for full details.*

*Instructions for:* [Azure Information Protection unified labeling client for Windows](#)

The Azure Information Protection unified labeling client for Windows is a downloadable client for organizations that use [sensitivity labels](#) to classify and protect documents and emails. This client also has a viewer for organizations that don't have their own information protection infrastructure but want to consume content that has been protected by other organizations that use a Rights Management service from Microsoft.

## NOTE

This client, also known as just the unified labeling client, is replacing the Azure Information Protection client (classic). If you're not sure which client to use, see [Choose which labeling client to use for Windows computers](#).

Use the following resources for the unified labeling client:

- [Azure Information Protection unified labeling client: Version release history](#)
- [Administrator guide for the Azure Information Protection unified labeling client](#)
- [User guide for the Azure Information Protection unified labeling client](#)

## TIP

There's also an Azure Information Protection app for iOS and Android. For more information, see [FAQs for Azure Information Protection app for iOS and Android](#).

## Install instructions

- [Administrators](#)
- [End users](#)

# Azure Information Protection unified labeling client - Version release history and support policy

7/20/2020 • 12 minutes to read • [Edit Online](#)

*Applies to:* [Azure Information Protection](#), Windows 10, Windows 8.1, Windows 8, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

\*Customers with extended Microsoft support for Windows 7 and Office 2010 can also get Azure Information Protection support for these versions. Check with your support contact for full details.

*Instructions for:* [Azure Information Protection unified labeling client for Windows](#)

You can download the Azure Information Protection unified labeling client from the [Microsoft Download Center](#).

After a short delay of typically a couple of weeks, the latest general availability version is also included in the Microsoft Update Catalog with a product name of **Microsoft Azure Information Protection > Microsoft Azure Information Protection Unified Labeling Client**, and the classification of **Updates**. This inclusion in the catalog means that you can upgrade the client by using WSUS or Configuration Manager, or other software deployment mechanisms that use Microsoft Update.

For more information, see [Upgrading and maintaining the Azure Information Protection unified labeling client](#).

## Servicing information and timelines

Each general availability (GA) version of the Azure Information Protection unified labeling client is supported for up to six months after the release of the subsequent GA version. The documentation does not include information about unsupported versions of the client. Fixes and new functionality are always applied to the latest GA version and will not be applied to older GA versions.

Preview versions should not be deployed for end users on production networks. Instead, use the latest preview version to see and try new functionality or fixes that are coming in the next GA version. Preview versions that are not current are not supported.

**General availability versions that are no longer supported:**

CLIENT VERSION	DATE RELEASED
2.2.21.0	09/03/2019
2.2.19.0	08/06/2019
2.2.14.0	07/15/2019
2.0.779.0	05/01/2019
2.0.778.0	04/16/2019

The date format used on this page is *month/day/year*.

## Release information

Use the following information to see what's new or changed for a supported release of the Azure Information Protection unified labeling client for Windows. The most current release is listed first. The date format used on this

page is *month/day/year*.

#### NOTE

Minor fixes are not listed so if you experience a problem with the unified labeling client, we recommend that you check whether it is fixed with the latest GA release. If the problem remains, check the current preview version (if available).

For technical support, see the [Support options and community resources](#) information. We also invite you to engage with the Azure Information Protection team, on their [Yammer site](#).

This client is replacing the Azure Information Protection client (classic). To compare features and functionality with the classic client, see [Compare the labeling clients for Windows computers](#).

## Version 2.7.99.0

Unified labeling scanner and client version 2.7.99.0

#### Fixes and improvements:

Fixed issues in file labeling actions for **New Label** audit logs.

For more information, see [Version 2.7.96.0](#) and [Azure Information Protection audit log reference \(public preview\)](#).

## Version 2.7.96.0

Unified labeling scanner and client version 2.7.96.0

**Released** 06/29/2020

#### New features for the unified labeling scanner:

- [Use scanner to apply labels based on recommended conditions](#). AIP customers can now choose to implement service side only auto-labeling. This feature allows AIP end users to always follow recommendations instead of the previous scenario, which only enabled automatic labeling on the user side.
- [Learn which files previously discovered by scanner were deleted from the scanned repository](#) These deleted files were not previously reported in AIP analytics and are now available in the scanner discovery report.
- [Get reports from scanner on failures to apply action events](#). Use reports to learn about failed action events and discover ways to prevent future occurrences.
- Introduction of AIP scanner diagnostic analyzer tool for detection and analysis of common scanner errors. To begin using AIP scanner diagnostics, [run the new Start-AIPScannerDiagnostics cmdlet](#).
- You can now manage and limit max CPU consumption on the scanner machine. Learn how to prevent 100% CPU usage and manage your CPU usage using [two new advanced settings ScannerMaxCPU](#), and [ScannerMinCPU](#).
- Now you can configure the unified labeling scanner to skip specific files depending on their file attributes. Define the list of file attributes that triggers a file to be skipped using the new [ScannerFSAttributesToSkip](#) advanced setting.

#### New features for the unified labeling client:

- [Justification popups](#) now appear for changes made to default labels in the unified labeling client.
- Smoother integration with visual content markings applied by Office. For more information about configuring content markings in Office document, see [How to configure a label for visual markings for](#)

## Azure Information Protections.

- New **WordShapeNameToRemove** advanced property enables removal of content marking in Word documents made by third-party applications. Learn more about how to [identify existing shape names and define them for removal using WordShapeNameToRemove](#).

## New audit logs generated for removed files

Audit logs are now generated each time the scanner detects that a file that had previously been scanned is now removed.

For more information, see:

- [File removed audit logs](#)
- [Central reporting for Azure Information Protection](#)

### IMPORTANT

In this version, file labeling actions do not generate **New Label** audit logs. If you run the scanner in **Enforce=On** mode, we recommend that upgrade to [Version 2.7.99.0](#).

## TLS 1.2 enforcement

Starting with this version of the Azure Information Protection client, only TLS versions 1.2 or higher are supported.

Customers that have a TLS setup that does not support TLS 1.2 must move to setup that supports TLS 1.2 to use Azure Information Protection policies, tokens, audit, and protection, and to receive Azure Information Protection-based communication.

For more requirement details, see [Firewalls and network infrastructure requirements](#).

## Fixes and improvements

- Scanner SQL improvements for:
  - Performance
  - Files with large numbers of information types
- SharePoint scanning improvements for:
  - Scanning performance
  - Files with special characters in the path
  - Libraries with large file count
- Improved user notifications for missing policies. For more information about label policies for the unified labeling client, see [What label policies can do](#) in the Microsoft 365 documentation.
- **Automatic labels** are now applied in Excel for scenarios where a user starts to close a file without saving, just as they are when a user actively saves a file.
- Headers and footers are removed as expected, and not on each document save, when the [ExternalContentMarkingToRemove](#) setting is configured.
- **Dynamic user variables** are now displayed in a document's visual markings as expected.
- Issue where only the first page of content of a PDF was being used for applying auto-classification rules is

now resolved, and auto-classification based on all content in the PDF now proceeds as expected. For more information about classification and labeling, see the [classification and labeling FAQ](#).

- When multiple Exchange accounts are configured and the Azure Information Protection Outlook client is enabled, mails are sent from the secondary account as expected. For more information about configuring the unified labeling client with Outlook, see [Additional prerequisites for the Azure Information Protection unified labeling client](#).
- When a document with a higher confidentiality label is dragged and dropped into an email, the email now automatically receives the higher confidentiality label as expected. For more information about labeling client features, see the [labeling client comparison table](#).
- Custom permissions are now applied to emails as expected, when email addresses include both an apostrophe ('') and period (.) For more information about configuring the unified labeling client with Outlook, see [Additional prerequisites for the Azure Information Protection unified labeling client](#).
- By default, a file's NTFS owner is lost when the file is labeled by the unified labeling scanner, PowerShell, or the File Explorer extension. Now you can configure the system to keep the file's NTFS owner by setting the new [UseCopyAndPreserveNTFSOwner](#) advanced setting to true.

The [UseCopyAndPreserveNTFSOwner](#) advanced setting requires a low latency, reliable network connection between the scanner and the scanned repository.

## Version 2.6.111.0

Released 03/09/2020

Supported through 12/29/2020

### New features:

- General availability version of the [scanner](#), to inspect and label documents in on-premises data stores.
- [Scanner](#) related:
  - [Easier SharePoint on-premises and subsite discovery](#). Setting each specific site is no longer required.
  - Advanced property for [SQL chunk sizing](#) added.
  - Administrators now have the ability to [stop existing scans and perform a re-scan](#) if a change was made to the default label.
  - By default, scanner now sets minimal telemetry for faster scans and reduced log size and information types are now cached in the database. Learn more about [scanner optimization](#).
  - Scanner now supports separate deployments for database and the service, while **Sysadmin** rights are needed only for database deployment.
  - Improvements made to scanner performance.
- Modification of [PowerShell](#) cmdlet **Set-AIPFileLabel** to enable removal of protection from PST, rar, 7zip and MSG files. This feature is disabled by default and must be turned on using the [Set-LabelPolicy](#) cmdlet, as described [here](#).
- Added ability for Azure Information Protection administrators to control when .pfile extensions are used for files. Learn more about [changing protected file types](#).
- Dynamic visual marking support added for applications and variables. Learn more about how to [configure labels for visual markings](#).
- Improvements made to [customizable policy tips for automatic and recommended labels](#).
- Support added for [offline labeling capability](#) with Office apps in the unified labeling client.

## Fixes:

- In instances where users attempted unsuccessfully to open protected TIFF files, and TIFF files created by RightFax, the TIFF files now open and remain stable as expected.
- Previous corruptions of protected txt and PDF files are resolved.
- Inconsistent labeling between **Automatic** and **Manual** in Log Analytics was corrected.
- Unexpected inheritance issues identified between new emails and a user's last opened email is now resolved.
- Protection of .msg files as .msg.pfiles now works as expected.
- Co-owner permissions added from Office user defined settings is now applied as expected.
- When entering permissions downgrade justification, text can no longer be entered when other options are already selected.

## Version 2.5.33.0

Released: 10/23/2019

Supported through 09/09/2020

### New features:

- Preview version of the [scanner](#), to inspect and label documents on-premises data stores. With this version of the scanner:
  - Multiple scanners can share the same SQL Server database when you configure the scanners to use the same scanner profile. This configuration makes it easier to manage multiple scanners, and results in faster scanning times. When you use this configuration, always wait for a scanner to finish installing before installing another scanner with the same profile.
  - You must specify a profile when you install the scanner and the scanner database is named **AIPScannerUL\_<profile\_name>**. The *Profile* parameter is also mandatory for Set-AIPScanner.
  - You can set a default label on all documents, even if documents are already labeled. In the scanner profile or repository settings, set the **Relabel files** option to **On** with the new **Enforce default label** checkbox selected.
  - You can remove existing labels from all documents and this act includes removing protection if it was previously applied by a label. Protection applied independently from a label is preserved. This scanner configuration is achieved in the scanner profile or repository settings with the following settings:
    - **Label files based on content:** Off
    - **Default label:** None
    - **Relabel files:** On with the **Enforce default label** checkbox selected
  - As with the scanner from the classic client, by default, the scanner protects Office files and PDF files. You can protect other file types when you use a [PowerShell advanced setting](#).
  - Event IDs for the scanner cycles starting and finishing are not written to the Windows event log. Instead, use the Azure portal for this information.
  - Known issue: New and renamed labels aren't available to select as a default label for the scanner profile or repository settings. Workarounds:
    - For new labels: In the Azure portal, [add the label](#) you want to use to the global policy or a scoped policy.
    - For renamed labels: Close and reopen the Azure portal.

You can upgrade scanners from the Azure Information Protection client (classic). After the upgrade, which

creates a new database, the scanner rescans all files the first time it runs. For instructions, see [Upgrading the Azure Information Protection scanner](#) from the admin guide.

For additional information, see the blog post announcement: [Unified labeling AIP scanner preview brings scaling out and more!](#)

- The PowerShell cmdlet [Set-AIPAuthentication](#) has new parameters (*AppId*, *AppSecret*, *TenantId*, *DelegatedUser*, and *OnBehalfOf*) for when you want to label files non-interactively, and also a new procedure to register an app in Azure AD. Example scenarios include the scanner and automated PowerShell scripts to label documents. For instructions, see [How to label files non-interactively](#) from the admin guide.

Note that *DelegatedUser* is a new parameter since the last preview version of the unified labeling client, and that the API permissions for the registered app have consequently changed.

- New PowerShell label policy advanced setting to [change which file types to protect](#).
- New PowerShell label policy advanced setting to [extend your label migration rules to SharePoint properties](#).
- Matched custom sensitive information types are sent to [Azure Information Protection analytics](#).
- The applied label displays the configured color for the label, if a [color has been configured](#).
- When you add or change protection settings to a label, the client reapplies the label with these latest protection settings when the document is next saved. Similarly, the scanner reapplies the label with these latest protection settings when the document is next scanned in enforce mode.
- [Support for disconnected computers](#) by exporting files from one client and manually copying them to the disconnected computer. Note that this configuration is supported for labeling with File Explorer, PowerShell, and the scanner. This configuration is not supported for labeling with Office apps.
- New cmdlet, [Export-AIPLogs](#), to gather all log files from %localappdata%\Microsoft\MSIP\Logs and saves them to a single, compressed file that has a .zip format. This file can then be sent to Microsoft Support if you are requested to send log files to help investigate a reported issue.

#### Fixes:

- You can successfully make changes to a protected file using File Explorer and right-click after a password for the file has been removed.
- You can successfully open natively protected files in the viewer without requiring the Save As, Export (EXPORT) [usage right](#).
- Labels and policy settings refresh as expected without having to run [Clear-AIPAuthentication](#), or manually delete the %LocalAppData%\Microsoft\MSIP\mip folder.

#### Additional changes

- [Reset Settings](#) now deletes the %LocalAppData%\Microsoft\MSIP\mip\<ProcessName.exe> folders instead of the %LocalAppData%\Microsoft\MSIP\mip\<ProcessName>\mip folder.
- [Get-AIPFileStatus](#) now includes the content ID for a protected document.

## Next steps

Not sure if unified labeling is the right client to install? See [Choose which labeling client to use for Windows computers](#).

For more information about installing and using the unified labeling client:

- For users: [Download and install the client](#)
- For admins: [Azure Information Protection unified labeling client administrator guide](#)

# Azure Information Protection unified labeling client administrator guide

7/20/2020 • 14 minutes to read • [Edit Online](#)

*Applies to: Azure Information Protection, Windows 10, Windows 8.1, Windows 8, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012*

*\*Customers with extended Microsoft support for Windows 7 and Office 2010 can also get Azure Information Protection support for these versions. Check with your support contact for full details.*

*Instructions for: Azure Information Protection unified labeling client for Windows*

Use the information in this guide if you are responsible for the Azure Information Protection unified labeling client on an enterprise network, or if you want more technical information than is in the [Azure Information Protection unified labeling client user guide](#).

For example:

- Understand the different components of this client and whether you should install it
- How to install the client for users, with information about prerequisites, installation options and parameters, and verification checks
- Locate the client files and usage logs
- Identify the file types supported by the client
- Use the client with PowerShell for command-line control

Have a question that's not addressed by this documentation? Visit our [Azure Information Protection Yammer site](#).

## Technical overview of the Azure Information Protection unified labeling client

The Azure Information Protection unified labeling client includes the following:

- An Office add-in, that installs a **Sensitivity** button on the ribbon for users to select sensitivity labels, and an option to display the Azure Information Protection bar for better label visibility.
- Windows File Explorer, right-click options for users to apply classification labels and protection to files.
- A viewer to display protected files when a native application cannot open it.
- A PowerShell module to discover sensitive information in files, and apply or remove classification labels and protection from files.

The client includes cmdlets to install and configure the [Azure Information Protection scanner](#) that runs as a service on Windows Server. This service lets you discover, classify, and protect files on data stores such as network shares and SharePoint Server libraries

- The Rights Management client that communicates with the protection service (Azure Rights Management) to encrypt and protect files.

With the exception of the viewer, the Azure Information Protection unified labeling client cannot be used with applications and services that communicate directly with the protection service or Active Directory Rights Management Services.

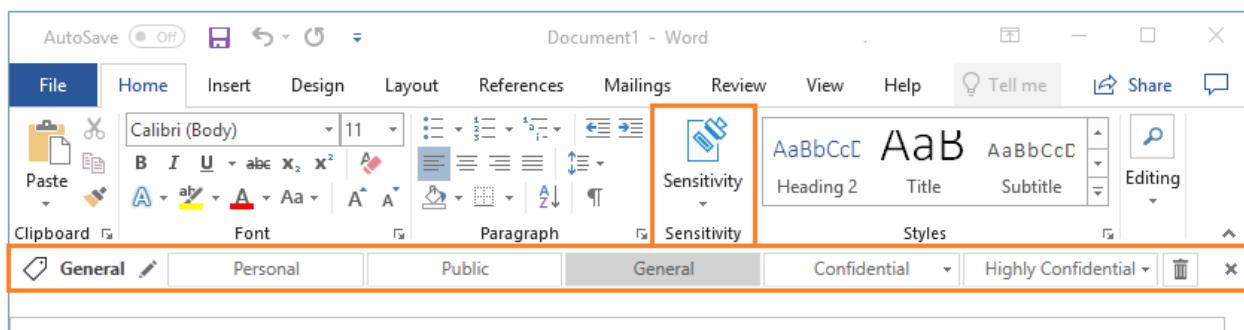
If you have AD RMS and want to migrate to Azure Information Protection, see [Migrating from AD RMS to Azure Information Protection](#).

## Should you deploy the Azure Information Protection unified labeling client?

Deploy the Azure Information Protection unified labeling client if you are using [sensitivity labels in the Office 365 Security & Compliance Center](#), and any of the following applies:

- You want to classify (and optionally, protect) documents and email messages by selecting labels from within your Office apps (Word, Excel, PowerPoint, Outlook) on Windows computers.
- You want to classify (and optionally, protect) files by using File Explorer, supporting additional file types than those supported by Office, multi-select, and folders.
- You want to run scripts that classify (and optionally, protect) documents by using PowerShell commands.
- You want to test a service that discovers, classifies (and optionally, protects) files that are stored on-premises.
- You want to view protected documents when a native application to display the file is not installed or cannot open these documents.

Example showing the Office add-in for the Azure Information Protection unified labeling client, displaying the new **Sensitivity** button on the ribbon and the optional Azure Information Protection bar:



## Installing and supporting the Azure Information Protection unified labeling client

You can install the Azure Information Protection unified labeling client by using an executable or a Windows installer file. For more information about each choice, and instructions, see [Install the Azure Information Protection unified labeling client for users](#).

Use the following sections for supporting information about installing the client.

### Installation checks and troubleshooting

When the client is installed, use the **Help and Feedback** option to open the **Microsoft Azure Information Protection** dialog box:

- From an Office application: On the **Home** tab, in the **Sensitivity** group, select **Sensitivity**, and then select **Help and Feedback**.
- From File Explorer: Right-select a file, files, or folder, select **Classify and protect**, and then select **Help**

and Feedback.

#### Help and Feedback section

The **Tell me more link** by default, goes to the [Azure Information Protection website](#). You can configure your own URL link that goes to a custom help page as one of the policy settings in your labeling management center: Office 365 Security & Compliance Center, Microsoft 365 security center, or Microsoft 365 compliance center.

The **Report an Issue** link displays only if you specify an [advanced setting](#). When you configure this setting, you specify an HTTP link such as the email address of your help desk.

The **Export Logs** automatically collects and attaches log files for the Azure Information Protection unified labeling client if you have been asked to send these to Microsoft Support. This option can also be used by end users to send these log files to your help desk. Alternatively, you could use the [Export-AIPLogs](#) PowerShell cmdlet.

The **Reset Settings** signs out the user, deletes the currently downloaded sensitivity labels and label policies, and resets the user settings for the Azure Rights Management service.

#### NOTE

If you have technical problems with the client, see [Support options and community resources](#).

#### More information about the Reset Settings option

- You do not have to be a local administrator to use this option and this action is not logged in the Event Viewer.
- Unless files are locked, this action deletes all the files in the following locations. These files include client certificates, protection templates, sensitivity labels and policies from your labeling management center, and the cached user credentials. The client log files are not deleted.
  - %LocalAppData%\Microsoft\DRM
  - %LocalAppData%\Microsoft\MSIPC
  - %LocalAppData%\Microsoft\MSIP\mip\<ProcessName.exe>
  - %LocalAppData%\Microsoft\MSIP\AppDetails
  - %LocalAppData%\Microsoft\MSIP\TokenCache
- The following registry keys and settings are deleted. If the settings for any of these registry keys have custom values, these must be reconfigured after you reset the client.

Typically for enterprise networks, these settings are configured by using group policy, in which case they are automatically reapplied when group policy is refreshed on the computer. However, there might be some settings that are configured one time with a script, or manually configured. In these cases, you must take additional steps to reconfigure these settings. As an example, computers might run a script one time to configure settings for redirection to Azure Information Protection because you are migrating from AD RMS and still have a Service Connection Point on your network. After resetting the client, the computer must run this script again.

- HKEY\_CURRENT\_USER\SOFTWARE\Microsoft\Office\15.0\Common\Identity
- HKEY\_CURRENT\_USER\SOFTWARE\Microsoft\Office\14.0\Common\DRM
- HKEY\_CURRENT\_USER\SOFTWARE\Microsoft\Office\15.0\Common\DRM
- HKEY\_CURRENT\_USER\SOFTWARE\Microsoft\Office\16.0\Common\DRM
- HKEY\_CURRENT\_USER\SOFTWARE\Classes\Local Settings\Software\Microsoft\MSIPC

- The currently signed in user is signed out.

#### Client status section

Use the **Connected as** value to confirm that the displayed user name identifies the account to be used for Azure Information Protection authentication. This user name must match an account used for Office 365 or Azure Active Directory. The account must also belong to an Office 365 tenant that is configured for sensitivity labels in your labeling management portal.

If you need to sign in as a different user to the one displayed, see the [Sign in as a different user](#) instructions.

Use the **Version** information to confirm which version of the client is installed. You can check whether this is the latest release version and the corresponding fixes and new features by reading the [Version release information](#) for the client.

## Support for multiple languages

The Azure Information Protection unified labeling client supports the same languages that Office 365 supports. For a list of these languages, see the **Office 365, Exchange Online Protection, and Power BI** section from the [International availability](#) page from Office.

For these languages, menu options, dialog boxes, and messages from the Azure Information Protection unified labeling client display in the user's language. There is a single installer that detects the language, so no additional configuration is required to install the Azure Information Protection unified labeling client for different languages.

However, label names and descriptions that you specify are not automatically translated when you configure labels in your labeling center. For users to see labels in their preferred language, provide your own translations and configure them for the labels by using by using Office 365 Security & Compliance PowerShell and the *LocaleSettings* parameter for [Set-Label](#). Visual markings are not translated and do not support more than one language.

## Post installation tasks

After you have installed the Azure Information Protection unified labeling client, make sure that you give users instructions for how to label their documents and emails, and guidance for which labels to choose for specific scenarios. For example:

- Online user instructions: [Azure Information Protection unified labeling user guide](#)
- Download a customizable user guide: [Azure Information Protection End User Adoption Guide](#)

## Installing the Azure Information Protection scanner

The scanner for the unified labeling client is generally available. Install the current version of the unified labeling client, from the [Microsoft Download Center](#).

If you are installing the scanner for the first time on a computer, download and install this client and then follow the instructions in [Deploying the Azure Information Protection scanner to automatically classify and protect files](#).

If you are upgrading the scanner from the Azure Information Protection client (classic), or a previous version of the unified labeling client, see the [Upgrading the Azure Information Protection scanner](#) section for instructions.

## Upgrading and maintaining the Azure Information Protection unified labeling client

#### **NOTE**

The Azure Information Protection unified labeling client supports upgrading the Azure Information Protection client (classic), as well as upgrading from previous versions of the Azure Information Protection unified labeling client.

The Azure Information Protection team regularly updates the Azure Information Protection unified labeling client for new functionality and fixes. Announcements are posted to the team's [Yammer site](#).

If you are using Windows Update, the Azure Information Protection unified labeling client automatically upgrades the general availability version of this client, irrespective of how the client was installed. New client releases are published to the catalog a few weeks after the release.

Alternatively, you can manually upgrade the client by downloading the new release from the [Microsoft Download Center](#). Then install the new version to upgrade the client. You must use this method to upgrade preview versions and if you are upgrading from the Azure Information Protection client (classic).

If you are upgrading from the Azure Information Protection client (classic) on Windows 7, any Office applications will automatically restart during the client upgrade. This automatic restart does not apply to later operating systems, or if you are upgrading from an older version of the unified labeling client.

When you manually upgrade, uninstall the previous version first only if you're changing the installation method. For example, you change from the executable (.exe) version of the client to the Windows installer (.msi) version of the client. Or, if you need to install a previous version of the client. For example, you had a preview version installed for testing and now need to revert to the current general availability version.

Use the [Version release history and support policy](#) to understand the support policy for the Azure Information Protection unified labeling client, which versions are currently supported, and what's new and changed for the supported releases.

### **Upgrading the Azure Information Protection scanner**

Instructions for upgrading the scanner depend on whether you are upgrading from an earlier version of the scanner from the Azure Information Protection unified labeling client, or from the Azure Information Protection client (classic).

#### **To upgrade the scanner from an earlier version of the unified labeling client**

1. On the scanner computer, stop the scanner service, **Azure Information Protection Scanner**.
2. Upgrade the Azure Information Protection unified labeling client by downloading and installing the latest version of the unified labeling client from the [Microsoft Download Center](#).
3. In a PowerShell session, run the `Update-AIPScanner` command with your scanner's profile. For example:  
`Update-AIPScanner -Profile Europe`
4. Restart the Azure Information Protection Scanner service, **Azure Information Protection Scanner**.

You can now use the rest of the instructions in [Deploying the Azure Information Protection scanner to automatically classify and protect files](#), omitting the step to install the scanner. Because the scanner is already installed, there's no reason to install it again.

#### **To upgrade the scanner from the classic client**

If you are currently using the Azure Information Protection scanner from the Azure Information Protection client (classic), you can upgrade it to use sensitive information types and sensitivity labels that are published from the Office 365 Security & Compliance Center (or the Microsoft 365 security center or the Microsoft 365 compliance center).

How to upgrade the scanner depends on the version of the classic client that you are currently running:

- [Upgrade from version 1.48.204.0 and later versions](#)
- [Upgrade from versions earlier than 1.48.204.0](#)

The upgrade creates a new database named **AIPScannerUL\_<profile\_name>**, and the previous scanner database is retained in case you need it for the previous version. When you are confident you don't need the previous scanner database, you can delete it. Because the upgrade creates a new database, the scanner rescans all files the first time it runs.

Upgrade from the Azure Information Protection client (classic) version 1.48.204.0 and later versions of this client

If you upgraded the scanner by using the preview version of the unified labeling client, you don't need to run these instructions again.

1. On the scanner computer, stop the scanner service, **Azure Information Protection Scanner**.
2. Upgrade to the Azure Information Protection unified labeling client by downloading and installing the unified labeling client from the [Microsoft Download Center](#).
3. In a PowerShell session, run the `Update-AIPScanner` command with your scanner's profile. For example:

```
Update-AIPScanner -Profile Europe .
```

This step creates a new database with the name **AIPScannerUL\_<profile\_name>**

4. Restart the Azure Information Protection Scanner service, **Azure Information Protection Scanner**.

You can now use the rest of the instructions in [Deploying the Azure Information Protection scanner to automatically classify and protect files](#), omitting the step to install the scanner. Because the scanner is already installed, there's no reason to install it again.

Upgrade from the Azure Information Protection client (classic) versions earlier than 1.48.204.0

#### **IMPORTANT**

For a smooth upgrade path, do not install the the Azure Information Protection unified labeling client on the computer running the scanner as your first step to upgrade the scanner. Instead, use the following upgrade instructions.

Beginning with version 1.48.204.0, the scanner gets its configuration settings from the Azure portal, by using a configuration profile. Upgrading the scanner includes instructing the scanner to use this online configuration and for the unified labeling client, offline configuration for the scanner is not supported.

1. Use the Azure portal to create a new scanner profile that includes settings for the scanner and your data repositories with any settings that they need. For help with this step, see [Configure the scanner in the Azure portal](#) from the scanner deployment instructions.
2. On the scanner computer, stop the scanner service, **Azure Information Protection Scanner**.
3. Upgrade to the Azure Information Protection unified labeling client by downloading and installing the unified labeling client from the [Microsoft Download Center](#).
4. In a PowerShell session, run the `Update-AIPScanner` command with the same profile name that you specified in step 1. For example: `Update-AIPScanner -Profile Europe`
5. Restart the Azure Information Protection Scanner service, **Azure Information Protection Scanner**.

You can now use the rest of the instructions in [Deploying the Azure Information Protection scanner to automatically classify and protect files](#), omitting the step to install the scanner. Because the scanner is already installed, there's no reason to install it again.

Upgrading in a different order to the recommended steps

when you upgrade from a version earlier than 1.48.204.0 and you don't configure the scanner in the Azure portal before you run the `Update-AIPScanner` command, you won't have a profile name to specify that identifies your

scanner configuration settings for the upgrade process.

In this scenario, when you configure the scanner in the Azure portal, you must specify exactly the same profile name that was used when you ran the Update-AIPScanner command. If the name doesn't match, the scanner will not be configured for your settings.

**TIP**

To identify scanners that have this misconfiguration, use the **Azure Information Protection - Nodes** pane in the Azure portal.

For scanners that have internet connectivity, they display their computer name with the GA version number of the Azure Information Protection client, but no profile name. Only scanners that have a version number 1.41.51.0 should display no profile name on this pane.

## Uninstalling the Azure Information Protection unified labeling client

You can use any of the following options to uninstall the client:

- Use Control Panel to uninstall a program: Click **Microsoft Azure Information Protection** > **Uninstall**
- Rerun the executable (for example, **AzInfoProtection\_UL.exe**), and from the **Modify Setup** page, click **Uninstall**.
- Run the executable with **/uninstall**. For example: `AzInfoProtection.exe /uninstall`

## Next steps

To install the client, see [Install the Azure Information Protection unified labeling client for users](#).

If you've already installed the client, see the following for additional information that you might need to support this client:

- [Customizations](#)
- [Client files and usage logging](#)
- [File types supported](#)
- [PowerShell commands](#)

# Admin Guide: Install the Azure Information Protection unified labeling client for users

7/20/2020 • 10 minutes to read • [Edit Online](#)

*Applies to:* [Azure Information Protection](#), Windows 10, Windows 8.1, Windows 8, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

*\*Customers with extended Microsoft support for Windows 7 and Office 2010 can also get Azure Information Protection support for these versions. Check with your support contact for full details.*

*Instructions for:* [Azure Information Protection unified labeling client for Windows](#)

Before you install the Azure Information Protection unified labeling client on your enterprise network, check that computers have the required operating system versions and applications for Azure Information Protection: [Requirements for Azure Information Protection](#).

Then check the additional prerequisites that might be needed for the Azure Information Protection unified labeling client, as documented in the next section. Not all the prerequisites are checked by the installation program.

## Additional prerequisites for the Azure Information Protection unified labeling client

- Microsoft .NET Framework 4.6.2

The full installation of the Azure Information Protection unified labeling client by default, requires a minimum version of Microsoft .NET Framework 4.6.2 and if this is missing, the setup wizard from the executable installer tries to download and install this prerequisite. When this prerequisite is installed as part of the client installation, the computer must be restarted. Although not recommended, you can bypass this prerequisite when you use the setup wizard by using a [custom installation parameter](#).

- Microsoft .NET Framework 4.5.2

If the Azure Information Protection Viewer is installed separately, this requires a minimum version of Microsoft .NET Framework 4.5.2 and if this is missing, the executable installer does not download or install it.

- Windows PowerShell minimum version 4.0

The PowerShell module for the client requires a minimum version of 4.0 for Windows PowerShell, which might need to be installed on older operating systems. For more information, see [How to Install Windows PowerShell 4.0](#). The installer does not check or install this prerequisite for you. To confirm the version of Windows PowerShell that you are running, type `$PSVersionTable` in a PowerShell session.

- Screen resolution greater than 800x600

Resolutions 800x600 and lower can't fully display the **Classify and protect - Azure Information Protection** dialog box when you right-click a file or folder in File Explorer.

- Microsoft Online Services Sign-in Assistant 7.250.4303.0

Computers running Office 2010 require Microsoft Online Services Sign-in Assistant version 7.250.4303.0. This version is included with the client installation. If you have a later version of the Sign-in Assistant, uninstall it before you install the Azure Information Protection unified labeling client. For example, check the

version and uninstall the Sign-in Assistant by using **Control Panel > Program and Features > Uninstall or change a program**.

- KB 4482887

For Windows 10 version 1809 only, operation system builds older than 17763.348, install [March 1, 2019—KB4482887 \(OS Build 17763.348\)](#) to ensure the Information Protection bar displays correctly in Office applications. This update is not needed if you have Office 365 1902 or later.

- Configure group policy to prevent the Azure Information Protection add-in from being disabled

For Office 2013 and later versions, configure group policy to ensure that the **Microsoft Azure Information Protection** add-in for Office applications is always enabled. Without this configuration, the Microsoft Azure Information Protection add-in can get disabled and users will not be able to label their documents and emails in their Office application.

- For Outlook: Use the group policy setting documented in [System Administrator control over add-ins](#) from the Office documentation.
- For Word, Excel, and PowerPoint: Use the group policy setting [list of managed add-ins](#) documented in the Support article [No Add-ins loaded due to group policy settings for Office 2013 and Office 2016 programs](#).

Specify the following programmatic identifiers (ProgID) for Azure Information Protection, and set the option to **1: The add-in is always enabled**.

For Word: `MSIP.WordAddin`

For Excel: `MSIP.ExcelAddin`

For PowerPoint: `MSIP.PowerPointAddin`

#### **IMPORTANT**

Installation of the Azure Information Protection unified labeling client requires local administrative permissions.

## Applications

The Azure Information Protection unified labeling client can label and protect documents and emails by using the Office applications Word, Excel, PowerPoint, and Outlook from any of the following Office editions:

Office apps minimum version 1805, build 9330.2078 from Office 365 Business or Microsoft 365 Business when the user is assigned a license for Azure Rights Management (also known as Azure Information Protection for Office 365) Office 365 ProPlus Office Professional Plus 2019 Office Professional Plus 2016 Office Professional Plus 2013 with Service Pack 1 Office Professional Plus 2010 with Service Pack 2

Other editions (such as **standard**) of Office cannot protect documents and emails by using a Rights Management service. For these editions, Azure Information Protection is supported for **labeling** only. Consequently, labels that apply protection do not display to users on the Azure Information Protection Sensitivity button or bar.

For information about which Office editions support the protection service, see [Applications that support Azure Rights Management data protection](#).

#### **Office features and capabilities not supported**

The Azure Information Protection unified labeling client does not support multiple versions of Office on the same computer, or switching user accounts in Office.

The Office mail merge feature is not supported with any Azure Information Protection feature.

# Options to install the Azure Information Protection unified labeling client for users

There are two options for installing the client for users:

**Run the executable (.exe) version of the client:** The recommended installation method that you can run interactively, or silently. This method has the most flexibility and it is recommended because the installer checks for many of the prerequisites, and can automatically install missing prerequisites. [Instructions](#)

**Deploy the Windows installer (.msi) version of the client:** Supported for silent installs only that use a central deployment mechanism, such as group policy, Configuration Manager, and Microsoft Intune. This method is necessary for Windows 10 PCs that are managed by Intune and mobile device management (MDM) because for these computers, executable files are not supported for installation. However, when you use this installation method, you must manually check and install or uninstall the dependent software that the installer for the executable would perform for each computer. [Instructions](#)

After the Azure Information Protection unified labeling client is installed, you can update this client by repeating your chosen installation method, or use Windows Update to keep the client automatically upgraded. For more information about upgrading, see the [Upgrading and maintaining the Azure Information Protection client](#) section.

## To install the Azure Information Protection unified labeling client by using the executable installer

Use the following instructions to install the client when you're not using the Microsoft Update catalog, or deploying the .msi by using a central deployment method such as Intune.

1. Download the executable version of the Azure Information Protection unified labeling client (file name of AzInfoProtection\_UL) from the [Microsoft Download Center](#).

If there is a preview version available, keep this version for testing only. It is not intended for end users in a production environment.

2. For a default installation, simply run the executable, for example, AzInfoProtection\_UL.exe. However, to see the installation options, first run the executable with /help: `AzInfoProtection_UL.exe /help`

Example to silently install the client: `AzInfoProtection_UL.exe /quiet`

Example to silently install only the PowerShell cmdlets: `AzInfoProtection_UL.exe PowerShellOnly=true /quiet`

Additional parameters that are not listed on the help screen:

- **ServiceLocation:** Use this parameter if you are installing the client on computers that run Office 2010 and your users are not local administrators on their computers or you do not want them to be prompted. [More information](#)
- **DowngradeDotNetRequirement:** Use this parameter to bypass the requirement for Microsoft Framework .NET version 4.6.2. [More information](#)
- **AllowTelemetry=0:** Use this parameter to disable the install option **Help improve Azure Information Protection by sending usage statistics to Microsoft.**

3. To complete the installation:

- If your computer runs Office 2010, restart your computer.

If the client was not installed with the ServiceLocation parameter, when you first open one of the Office applications that use the Azure Information Protection unified client (for example, Word), you must confirm any prompts to update the registry for this first-time use. [Service discovery](#) is used to populate the registry keys.

- For other versions of Office, restart any Office applications and all instances of File Explorer.

4. You can confirm that the installation was successful by checking the install log file, which by default is created in the %temp% folder. You can change this location with the /log installation parameter.

This file has the following naming format:

```
Microsoft_Azure_Information_Protection_<number>_<number>_MSIP.Setup.Main.msi.log
```

For example:

```
Microsoft_Azure_Information_Protection_20161201093652_000_MSIP.Setup.Main.msi.log
```

In this log file, search for the following string: **Product: Microsoft Azure Information Protection -- Installation completed successfully.** If the installation failed, this log file contains details to help you identify and resolve any problems.

#### More information about the ServiceLocation installation parameter

When you install the client for users who have Office 2010 and they do not have local administrative permissions, specify the ServiceLocation parameter and the URL for your Azure Rights Management service. This parameter and value creates and sets the following registry keys:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\MSDRM\ServiceLocation\Activation
```

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\MSDRM\ServiceLocation\EnterprisePublishing
```

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSDRM\ServiceLocation\EnterprisePublishing
```

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSDRM\ServiceLocation\Activation
```

Use the following procedure to identify the value to specify for the ServiceLocation parameter.

##### To identify the value to specify for the ServiceLocation parameter

1. From a PowerShell session, first run [Connect-AipService](#) and specify your administrator credentials to connect to the Azure Rights Management service. Then run [Get-AipServiceConfiguration](#).

If you haven't already installed the PowerShell module for the Azure Rights Management service, see [Installing the AIPService PowerShell module](#).

2. From the output, identify the **LicensingIntranetDistributionPointUrl** value.

For example: **LicensingIntranetDistributionPointUrl** : [https://5c6bb73b-1038-4eec-863d-49bded473437.rms.na.aadrm.com/\\_wmcs/licensing](https://5c6bb73b-1038-4eec-863d-49bded473437.rms.na.aadrm.com/_wmcs/licensing)

3. From the value, remove **\_wmcs/licensing** from this string. For example: <https://5c6bb73b-1038-4eec-863d-49bded473437.rms.na.aadrm.com>

The remaining string is the value to specify for your ServiceLocation parameter.

Example to install the client silently for Office 2010 and Azure RMS:

```
AzInfoProtection_UL.exe /quiet ServiceLocation=https://5c6bb73b-1038-4eec-863d-49bded473437.rms.na.aadrm.com
```

#### More information about the DowngradeDotNetRequirement installation parameter

To support automatic upgrades by using Windows Update, and for reliable integration with Office applications, the Azure Information Protection unified labeling client uses Microsoft .NET Framework version 4.6.2. By default, an interactive installation by using the executable checks for this version and tries to install it if it is missing. The installation then requires the computer to restart.

If installing this later version of the Microsoft .NET Framework is not practical, you can install the client with the **DowngradeDotNetRequirement=True** parameter and value, which bypasses this requirement if Microsoft .NET Framework version 4.5.1 is installed.

For example: 

```
AzInfoProtection_UL.exe DowngradeDotNetRequirement=True
```

We recommend that you use this parameter with caution, and with the knowledge that there are reported issues

with Office applications hanging when the Azure Information Protection unified labeling client is used with this older version of the Microsoft .NET Framework. If you do experience hanging problems, upgrade to the recommended version before you try other troubleshooting solutions.

Also remember that if you use Windows Update to keep the Azure Information Protection unified labeling client updated, you must have another software deployment mechanism to upgrade the client to later versions.

### To install the Azure Information Protection unified labeling client by using the .msi installer

For central deployment, use the following information that is specific to the .msi installation version of the Azure Information Protection unified labeling client.

If you use Intune for your software deployment method, use these instructions together with [Add apps with Microsoft Intune](#).

1. Download the .msi version of the Azure Information Protection unified labeling client (AzInfoProtection\_UL) from the [Microsoft Download Center](#).

If there is a preview version available, keep this version for testing only. It is not intended for end users in a production environment.

2. For each computer that runs the .msi file, you must make sure that the following software dependencies are in place. For example, package these with the .msi version of the client or only deploy to computers that meet these dependencies:

OFFICE VERSION	OPERATING SYSTEM	SOFTWARE	ACTION
All versions except Office 365 1902 or later	Windows 10 version 1809 only, operation system builds older than 17763.348	<a href="#">KB 4482887</a>	Install
Office 2016	All supported versions	64-bit: <a href="#">KB3178666</a> 32-bit: <a href="#">KB3178666</a> Version: 1.0	Install
Office 2013	All supported versions	64-bit: <a href="#">KB3172523</a> 32-bit: <a href="#">KB3172523</a> Version: 1.0	Install
Office 2010	All supported versions	<a href="#">Microsoft Online Services Sign-in Assistant</a> Version: 2.1	Install
Office 2010	Windows 8.1 and Windows Server 2012 R2	<a href="#">KB2843630</a> Version number included in file name: v3	Install if KB2843630 or KB2919355 is not installed
Office 2010	Windows 8 and Windows Server 2012	<a href="#">KB2843630</a> Version number included in file name: v3	Install

3. For a default installation, run the .msi with /quiet, for example, `AzInfoProtection_UL.msi /quiet`. However,

you might need to specify additional installation parameters that are documented in the [executable installer instructions](#) with one exception:

- Instead of `AllowTelemetry=0` to disable the install option **Help improve Azure Information Protection by sending usage statistics to Microsoft**, specify `ENABLETELEMETRY=0`.

## Next steps

Now that you've installed the Azure Information Protection unified labeling client, see the following for additional information that you might need to support this client:

- [Client files and usage logging](#)
- [File types supported](#)
- [PowerShell commands](#)

# Admin Guide: Custom configurations for the Azure Information Protection unified labeling client

7/20/2020 • 48 minutes to read • [Edit Online](#)

Applies to: [Azure Information Protection](#), Windows 10, Windows 8.1, Windows 8, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

\*Customers with extended Microsoft support for Windows 7 and Office 2010 can also get Azure Information Protection support for these versions. Check with your support contact for full details.

Instructions for: [Azure Information Protection unified labeling client for Windows](#)

Use the following information for advanced configurations that you might need for specific scenarios or a subset of users when you manage the Azure Information Protection unified labeling client.

These settings require editing the registry or specifying advanced settings. The advanced settings use [Office 365 Security & Compliance Center PowerShell](#).

## How to configure advanced settings for the client by using Office 365 Security & Compliance Center PowerShell

When you use Office 365 Security & Compliance Center PowerShell, you can configure advanced settings that support customizations for label policies and labels. For example:

- The setting to display the Information Protection bar in Office apps is a *label policy advanced setting*.
- The setting to specify a label color is a *label advanced setting*.

In both cases, after you [connect to Office 365 Security & Compliance Center PowerShell](#), specify the *AdvancedSettings* parameter with the identity (name or GUID) of the policy or label, and specify key/value pairs in a [hash table](#). Use the following syntax:

For a label policy setting, single string value:

```
Set-LabelPolicy -Identity <PolicyName> -AdvancedSettings @{Key="value1,value2"}
```

For label policy settings, multiple string values for the same key:

```
Set-LabelPolicy -Identity <PolicyName> -AdvancedSettings @{Key=ConvertTo-Json("value1", "value2")}
```

For a label setting, single string value:

```
Set-Label -Identity <LabelGUIDorName> -AdvancedSettings @{Key="value1,value2"}
```

For label settings, multiple string values for the same key:

```
Set-Label -Identity <LabelGUIDorName> -AdvancedSettings @{Key=ConvertTo-Json("value1", "value2")}
```

To remove an advanced setting, use the same syntax but specify a null string value.

## IMPORTANT

Use of white spaces in the string will prevent application of the labels.

### Examples for setting advanced settings

Example 1: Set a label policy advanced setting for a single string value:

```
Set-LabelPolicy -Identity Global -AdvancedSettings @{EnableCustomPermissions="False"}
```

Example 2: Set a label advanced setting for a single string value:

```
Set-Label -Identity Internal -AdvancedSettings @{smimesign="true"}
```

Example 3: Set a label advanced setting for multiple string values:

```
Set-Label -Identity Confidential -AdvancedSettings @{labelByCustomProperties=ConvertTo-Json("Migrate Confidential label,Classification,Confidential", "Migrate Secret label,Classification,Secret")})
```

Example 4: Remove a label policy advanced setting by specifying a null string value:

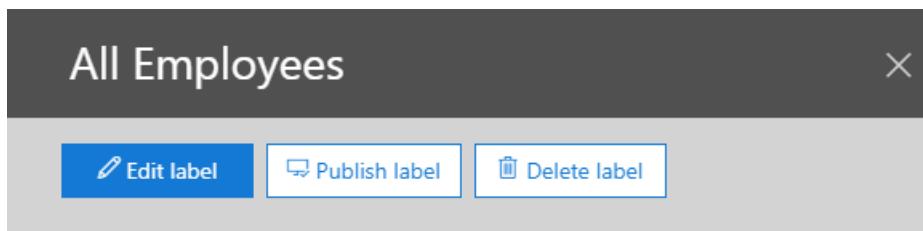
```
Set-LabelPolicy -Identity Global -AdvancedSettings @{EnableCustomPermissions=""}
```

### Specifying the identity for the label policy or label

Specifying the label policy name for the PowerShell *Identity* parameter is straightforward because you see only one policy name in the admin center where you manage your label policies. However, for labels, you see both a **Name** and **Display name** in the admin centers. In some cases, the value for both will be the same but they can be different:

- **Name** is the original name of the label and it is unique across all your labels. If you change the name of your label after it is created, this value remains the same. For labels that have been migrated from Azure Information Protection, you might see the label ID of the label from the Azure portal.
- **Display name** is the name of the label that users see and it doesn't have to be unique across all your labels. For example, users see one **All Employees** sublabel for the **Confidential** label, and another **All Employees** sublabel for the **Highly Confidential** label. These sublabels both display the same name, but are not the same label and have different settings.

For configuring your label advanced settings, use the **Name** value. For example, to identify the label in the following picture, you would specify `-Identity "All Company"`:



#### Name

All Company

#### Display name

Edit

All Employees

If you prefer to specify the label GUID, this value is not displayed in the admin center where you manage your labels. However, you can use the following Office 365 Security & Compliance Center PowerShell command to find this value:

```
Get-Label | Format-Table -Property DisplayName, Name, Guid
```

#### Order of precedence - how conflicting settings are resolved

Using one of the admin centers where you manage your sensitivity labels, you can configure the following label policy settings:

- **Apply this label by default to documents and emails**
- **Users must provide justification to remove a label or lower classification label**
- **Require users to apply a label to their email or document**
- **Provide users with a link to a custom help page**

When more than one label policy is configured for a user, each with potentially different policy settings, the last policy setting is applied according to the order of the policies in the admin center. For more information, see [Label policy priority \(order matters\)](#)

Label advanced settings follow the same logic for precedence: When a label is in multiple label policies and that label has advanced settings, the last advanced setting is applied according to the order of the policies in the admin center.

Label policy advanced settings are applied in the reverse order: With one exception, the advanced settings from the first policy are applied, according to the order of the policies in the admin center. The exception is the advanced setting *OutlookDefaultLabel*, which sets a different default label for Outlook. For this label policy advanced setting only, the last setting is applied according to the order of the policies in the admin center.

#### Available advanced settings for label policies

Use the *AdvancedSettings* parameter with [New-LabelPolicy](#) and [Set-LabelPolicy](#).

SETTING	SCENARIO AND INSTRUCTIONS
AdditionalPPrefixExtensions	Support for changing <EXT>.PFILE to P<EXT> by using this advanced property
AttachmentAction	For email messages with attachments, apply a label that matches the highest classification of those attachments

SETTING	SCENARIO AND INSTRUCTIONS
AttachmentActionTip	For email messages with attachments, apply a label that matches the highest classification of those attachments
DisableMandatoryInOutlook	Exempt Outlook messages from mandatory labeling
EnableAudit	Disable sending audit data to Azure Information Protection analytics
EnableContainerSupport	Enable removal of protection from PST, rar, 7zip and MSG files
EnableCustomPermissions	Disable custom permissions in File Explorer
EnableCustomPermissionsForCustomProtectedFiles	For files protected with custom permissions, always display custom permissions to users in File Explorer
EnableLabelByMailHeader	Migrate labels from Secure Islands and other labeling solutions
EnableLabelBySharePointProperties	Migrate labels from Secure Islands and other labeling solutions
HideBarByDefault	Display the Information Protection bar in Office apps
LogMatchedContent	Send information type matches to Azure Information Protection analytics
OutlookBlockTrustedDomains	Implement pop-up messages in Outlook that warn, justify, or block emails being sent
OutlookBlockUntrustedCollaborationLabel	Implement pop-up messages in Outlook that warn, justify, or block emails being sent
OutlookDefaultLabel	Set a different default label for Outlook
OutlookJustifyTrustedDomains	Implement pop-up messages in Outlook that warn, justify, or block emails being sent
OutlookJustifyUntrustedCollaborationLabel	Implement pop-up messages in Outlook that warn, justify, or block emails being sent
OutlookRecommendationEnabled	Enable recommended classification in Outlook
OutlookOverrideUnlabeledCollaborationExtensions	Implement pop-up messages in Outlook that warn, justify, or block emails being sent
OutlookUnlabeledCollaborationActionOverrideMailBodyBehavior	Implement pop-up messages in Outlook that warn, justify, or block emails being sent
OutlookWarnTrustedDomains	Implement pop-up messages in Outlook that warn, justify, or block emails being sent
OutlookWarnUntrustedCollaborationLabel	Implement pop-up messages in Outlook that warn, justify, or block emails being sent

SETTING	SCENARIO AND INSTRUCTIONS
PFileSupportedExtensions	Change which file types to protect
PostponeMandatoryBeforeSave	Remove "Not now" for documents when you use mandatory labeling
RemoveExternalContentMarkingInApp	Remove headers and footers from other labeling solutions
ReportAnIssueLink	Add "Report an Issue" for users
RunAuditInformationTypesDiscovery	Disable sending discovered sensitive information in documents to Azure Information Protection analytics
RunPolicyInBackground	Turn on classification to run continuously in the background
ScannerConcurrencyLevel	Limit the number of threads used by the scanner
ScannerFSAttributesToSkip	Skip or ignore files during scans depending on file attributes
UseCopyAndPreserveNTFSOwner	Preserve NTFS owners during labeling

Example PowerShell command to check your label policy settings in effect for a label policy named "Global":

```
(Get-LabelPolicy -Identity Global).settings
```

#### Available advanced settings for labels

Use the *AdvancedSettings* parameter with [New-Label](#) and [Set-Label](#).

SETTING	SCENARIO AND INSTRUCTIONS
color	Specify a color for the label
customPropertiesByLabel	Apply a custom property when a label is applied
DefaultSubLabelId	Specify a default sublabel for a parent label
labelByCustomProperties	Migrate labels from Secure Islands and other labeling solutions
SMimeEncrypt	Configure a label to apply S/MIME protection in Outlook
SMimeSign	Configure a label to apply S/MIME protection in Outlook

Example PowerShell command to check your label settings in effect for a label named "Public":

```
(Get-Label -Identity Public).settings
```

## Display the Information Protection bar in Office apps

This configuration uses a policy [advanced setting](#) that you must configure by using Office 365 Security & Compliance Center PowerShell.

By default, users must select the **Show Bar** option from the **Sensitivity** button to display the Information Protection bar in Office apps. Use the **HideBarByDefault** key and set the value to **False** to automatically display this bar for users so that they can select labels from either the bar or the button.

For the selected label policy, specify the following strings:

- Key: **HideBarByDefault**
- Value: **False**

Example PowerShell command, where your label policy is named "Global":

```
Set-LabelPolicy -Identity Global -AdvancedSettings @{HideBarByDefault="False"}
```

## Exempt Outlook messages from mandatory labeling

This configuration uses a policy [advanced setting](#) that you must configure by using Office 365 Security & Compliance Center PowerShell.

By default, when you enable the label policy setting of **All documents and emails must have a label**, all saved documents and sent emails must have a label applied. When you configure the following advanced setting, the policy setting applies only to Office documents and not to Outlook messages.

For the selected label policy, specify the following strings:

- Key: **DisableMandatoryInOutlook**
- Value: **True**

Example PowerShell command, where your label policy is named "Global":

```
Set-LabelPolicy -Identity Global -AdvancedSettings @{DisableMandatoryInOutlook="True"}
```

## Enable recommended classification in Outlook

This configuration uses a policy [advanced setting](#) that you must configure by using Office 365 Security & Compliance Center PowerShell.

When you configure a label for recommended classification, users are prompted to accept or dismiss the recommended label in Word, Excel, and PowerPoint. This setting extends this label recommendation to also display in Outlook.

For the selected label policy, specify the following strings:

- Key: **OutlookRecommendationEnabled**
- Value: **True**

Example PowerShell command, where your label policy is named "Global":

```
Set-LabelPolicy -Identity Global -AdvancedSettings @{OutlookRecommendationEnabled="True"}
```

## Enable removal of protection from compressed files

This configuration uses a policy [advanced setting](#) that you must configure by using Office 365 Security & Compliance Center PowerShell.

When you configure this setting, the [PowerShell](#) cmdlet `Set-AIPFileLabel` is enabled to allow removal of protection from PST, rar, 7zip and MSG files.

- Key: `EnableContainerSupport`
- Value: `True`

Example PowerShell command where your policy is enabled:

```
Set-LabelPolicy -Identity Global -AdvancedSettings @{EnableContainerSupport="True"}
```

## Set a different default label for Outlook

This configuration uses a policy [advanced setting](#) that you must configure by using Office 365 Security & Compliance Center PowerShell.

When you configure this setting, Outlook doesn't apply the default label that is configured as a policy setting for the option **Apply this label by default to documents and emails**. Instead, Outlook can apply a different default label, or no label.

For the selected label policy, specify the following strings:

- Key: `OutlookDefaultLabel`
- Value: `<label GUID>` or `None`

Example PowerShell command, where your label policy is named "Global":

```
Set-LabelPolicy -Identity Global -AdvancedSettings @{OutlookDefaultLabel="None"}
```

## Change which file types to protect

These configurations use a policy [advanced setting](#) that you must configure by using Office 365 Security & Compliance Center PowerShell.

By default, the Azure Information Protection unified labeling client protects all file types, and the scanner from the client protects only Office file types and PDF files.

You can change this default behavior for a selected label policy, by specifying one of the following:

### PFileSupportedExtension

- Key: `PFileSupportedExtensions`
- Value: `<string value>`

Use the following table to identify the string value to specify:

STRING VALUE	CLIENT	SCANNER
*	Default value: Apply protection to all file types	Apply protection to all file types
<code>&lt;null value&gt;</code>	Apply protection to Office file types and PDF files	Default value: Apply protection to Office file types and PDF files

STRING VALUE	CLIENT	SCANNER
ConvertTo-Json(".jpg", ".png")	In addition to Office file types and PDF files, apply protection to the specified file name extensions	In addition to Office file types and PDF files, apply protection to the specified file name extensions

Example 1: PowerShell command for the unified client to protect only Office file types and PDF files, where your label policy is named "Client":

```
Set-LabelPolicy -Identity Client -AdvancedSettings @{PFileSupportedExtensions=""}
```

Example 2: PowerShell command for the scanner to protect all file types, where your label policy is named "Scanner":

```
Set-LabelPolicy -Identity Scanner -AdvancedSettings @{PFileSupportedExtensions="*"}
```

Example 3: PowerShell command for the scanner to protect .txt files and .csv files in addition to Office files and PDF files, where your label policy is named "Scanner":

```
Set-LabelPolicy -Identity Scanner -AdvancedSettings @{PFileSupportedExtensions=ConvertTo-Json(".txt", ".csv")}
```

With this setting, you can change which file types are protected but you cannot change the default protection level from native to generic. For example, for users running the unified labeling client, you can change the default setting so that only Office files and PDF files are protected instead of all file types. But you cannot change these file types to be generically protected with a .pfile file name extension.

### AdditionalPPrefixExtensions

The unified labeling client supports changing <EXT>.PFILE to P<EXT> by using the advanced property, **AdditionalPPrefixExtensions**. This advanced property is supported in right-click, PowerShell, and scanner. All apps have similar behavior.

- Key: **AdditionalPPrefixExtensions**
- Value: <string value>

Use the following table to identify the string value to specify:

STRING VALUE	CLIENT AND SCANNER
*	All PFile extensions become P<EXT>
<null value>	Default value behaves like the default protection value.
ConvertTo-Json(".dwg", ".zip")	In addition to the previous list, ".dwg" and ".zip" become P<EXT>

Example 1: PowerShell command to behave like the default behavior where Protect ".dwg" becomes ".dwg.pfile":

```
Set-LabelPolicy -AdvancedSettings @{ AdditionalPPrefixExtensions =""}
```

Example 2: PowerShell command to change all PFile extensions from generic protection (dwg.pfile) to native protection (.pdwg) when the files is protected:

```
Set-LabelPolicy -AdvancedSettings @{ AdditionalPPrefixExtensions =""}
```

Example 3: PowerShell command to change ".dwg" to ".pdwg" when using this service protect this file:

```
Set-LabelPolicy -AdvancedSettings @{ AdditionalPPrefixExtensions =ConvertTo-Json(".dwg")}
```

With this setting, the following extensions ( ".txt", ".xml", ".bmp", "jt", ".jpg", ".jpeg", ".jpe", ".jif", ".jfif", ".jfi", ".png", ".tif", ".tiff", ".gif") always become P<EXT>. Notable exclusion is that "ptxt" does not become "txt.pfile".

**AdditionalPPrefixExtensions** only works if protection of PFiles with the advanced property - **PFileSupportedExtension** is enabled.

For example, in a case where the following command is used:

```
Set-LabelPolicy -AdvancedSettings @{PFileSupportedExtensions=""}
```

PFile protection is not possible, and the value in **AdditionalPPrefixExtensions** is ignored.

## Remove "Not now" for documents when you use mandatory labeling

This configuration uses a policy [advanced setting](#) that you must configure by using Office 365 Security & Compliance Center PowerShell.

When you use the label policy setting of **All documents and emails must have a label**, users are prompted to select a label when they first save an Office document and when they send an email. For documents, users can select **Not now** to temporarily dismiss the prompt to select a label and return to the document. However, they cannot close the saved document without labeling it.

When you configure this setting, it removes the **Not now** option so that users must select a label when the document is first saved.

For the selected label policy, specify the following strings:

- Key: **PostponeMandatoryBeforeSave**
- Value: **False**

Example PowerShell command, where your label policy is named "Global":

```
Set-LabelPolicy -Identity Global -AdvancedSettings @{PostponeMandatoryBeforeSave="False"}
```

## Remove headers and footers from other labeling solutions

This configuration uses policy [advanced settings](#) that you must configure by using Office 365 Security & Compliance Center PowerShell.

There are two methods to remove classifications from other labeling solutions. The first method removes any shape from Word documents where the shape name matches the name as defined in the advanced property **WordShapeNameToRemove**, the second method lets you remove or replace text-based headers or footers from Word, Excel and PowerPoint documents as defined in the **RemoveExternalContentMarkingInApp** advanced property.

### Use the **WordShapeNameToRemove** advanced property

*The **WordShapeNameToRemove** advanced property is supported from version 2.6.101.0 and above*

This setting lets you remove or replace shape based labels from Word documents when those visual markings have been applied by another labeling solution. For example, the shape contains the name of an old label that you have now migrated to sensitivity labels to use a new label name and its own shape.

To use this advanced property, you'll need to find the shape name in the Word document and then define them in the **WordShapeNameToRemove** advanced property list of shapes. The service will remove any shape in Word that starts with a name defined in list of shapes in this advanced property.

Avoid removing shapes that contain the text that you wish to ignore, by defining the name of all shapes to remove and avoid checking the text in all shapes, which is a resource-intensive process.

If you do not specify Word shapes in this additional advanced property setting, and Word is included in the **RemoveExternalContentMarkingInApp** key value, all shapes will be checked for the text that you specify in the **ExternalContentMarkingToRemove** value.

To find the name of the shape that you're using and wish to exclude:

1. In Word, display the **Selection** pane: **Home** tab > **Editing** group > **Select** option > **Selection Pane**.
2. Select the shape on the page that you wish to mark for removal. The name of the shape you mark is now highlighted in the **Selection** pane.

Use the name of the shape to specify a string value for the **WordShapeNameToRemove** key.

Example: The shape name is **dc**. To remove the shape with this name, you specify the value: `dc`.

- Key: **WordShapeNameToRemove**
- Value: `<Word shape name>`

Example PowerShell command, where your label policy is named "Global":

```
Set-LabelPolicy -Identity Global -AdvancedSettings @{WordShapeNameToRemove="dc"}
```

When you have more than one Word shape to remove, specify as many values as you have shapes to remove.

### Use the **RemoveExternalContentMarkingInApp** advanced property

This setting lets you remove or replace text-based headers or footers from documents when those visual markings have been applied by another labeling solution. For example, the old footer contains the name of an old label that you have now migrated to sensitivity labels to use a new label name and its own footer.

When the unified labeling client gets this configuration in its policy, the old headers and footers are removed or replaced when the document is opened in the Office app and any sensitivity label is applied to the document.

This configuration is not supported for Outlook, and be aware that when you use it with Word, Excel, and PowerPoint, it can negatively affect the performance of these apps for users. The configuration lets you define settings per application, for example, search for text in the headers and footers of Word documents but not Excel spreadsheets or PowerPoint presentations.

Because the pattern matching affects the performance for users, we recommend that you limit the Office application types (**Word**, **EXcel**, **PowerPoint**) to just those that need to be searched. For the selected label policy, specify the following strings:

- Key: **RemoveExternalContentMarkingInApp**
- Value: `<Office application types WXP>`

Examples:

- To search Word documents only, specify **W**.
- To search Word documents and PowerPoint presentations, specify **WP**.

Example PowerShell command, where your label policy is named "Global":

```
Set-LabelPolicy -Identity Global -AdvancedSettings @{RemoveExternalContentMarkingInApp="WX"}
```

You then need at least one more advanced client setting, **ExternalContentMarkingToRemove**, to specify the contents of the header or footer, and how to remove or replace them.

### How to configure ExternalContentMarkingToRemove

When you specify the string value for the **ExternalContentMarkingToRemove** key, you have three options that use regular expressions:

- Partial match to remove everything in the header or footer.

Example: Headers or footers contain the string **TEXT TO REMOVE**. You want to completely remove these headers or footers. You specify the value: `*TEXT*`.

- Complete match to remove just specific words in the header or footer.

Example: Headers or footers contain the string **TEXT TO REMOVE**. You want to remove the word **TEXT** only, which leaves the header or footer string as **TO REMOVE**. You specify the value: `TEXT`.

- Complete match to remove everything in the header or footer.

Example: Headers or footers have the string **TEXT TO REMOVE**. You want to remove headers or footers that have exactly this string. You specify the value: `^TEXT TO REMOVE$`.

The pattern matching for the string that you specify is case-insensitive. The maximum string length is 255 characters, and cannot include white spaces.

Because some documents might include invisible characters or different kinds of spaces or tabs, the string that you specify for a phrase or sentence might not be detected. Whenever possible, specify a single distinguishing word for the value and be sure to test the results before you deploy in production.

For the same label policy, specify the following strings:

- Key: **ExternalContentMarkingToRemove**
- Value: **<string to match, defined as regular expression>**

Example PowerShell command, where your label policy is named "Global":

```
Set-LabelPolicy -Identity Global -AdvancedSettings @{ExternalContentMarkingToRemove="*TEXT*"}
```

### Multiline headers or footers

If a header or footer text is more than a single line, create a key and value for each line. For example, you have the following footer with two lines:

#### The file is classified as Confidential

#### Label applied manually

To remove this multiline footer, you create the following two entries for the same label policy:

- Key: **ExternalContentMarkingToRemove**

- Key Value 1: \*Confidential\*
- Key Value 2: \*Label applied\*

Example PowerShell command, where your label policy is named "Global":

```
Set-LabelPolicy -Identity Global -AdvancedSettings @{ExternalContentMarkingToRemove="*Confidential*,*Label applied"}
```

#### **Optimization for PowerPoint**

Footers in PowerPoint are implemented as shapes. To avoid removing shapes that contain the text that you have specified but are not headers or footers, use an additional advanced client setting named

**PowerPointShapeNameToRemove**. We also recommend using this setting to avoid checking the text in all shapes, which is a resource-intensive process.

If you do not specify this additional advanced client setting, and PowerPoint is included in the **RemoveExternalContentMarkingInApp** key value, all shapes will be checked for the text that you specify in the **ExternalContentMarkingToRemove** value.

To find the name of the shape that you're using as a header or footer:

1. In PowerPoint, display the **Selection** pane: **Format** tab > **Arrange** group > **Selection Pane**.
2. Select the shape on the slide that contains your header or footer. The name of the selected shape is now highlighted in the **Selection** pane.

Use the name of the shape to specify a string value for the **PowerPointShapeNameToRemove** key.

Example: The shape name is **fc**. To remove the shape with this name, you specify the value: **fc**.

- Key: **PowerPointShapeNameToRemove**
- Value: <PowerPoint shape name>

Example PowerShell command, where your label policy is named "Global":

```
Set-LabelPolicy -Identity Global -AdvancedSettings @{PowerPointShapeNameToRemove="fc"}
```

When you have more than one PowerPoint shape to remove, specify as many values as you have shapes to remove.

By default, only the Master slides are checked for headers and footers. To extend this search to all slides, which is a much more resource-intensive process, use an additional advanced client setting named **RemoveExternalContentMarkingInAllSlides**:

- Key: **RemoveExternalContentMarkingInAllSlides**
- Value: **True**

Example PowerShell command, where your label policy is named "Global":

```
Set-LabelPolicy -Identity Global -AdvancedSettings @{RemoveExternalContentMarkingInAllSlides="True"}
```

## Disable custom permissions in File Explorer

This configuration uses a policy [advanced setting](#) that you must configure by using Office 365 Security & Compliance Center PowerShell.

By default, users see an option named **Protect with custom permissions** when they right-click in File Explorer and choose **Classify and protect**. This option lets them set their own protection settings that can override any protection settings that you might have included with a label configuration. Users can also see an option to remove protection. When you configure this setting, users do not see these options.

To configure this advanced setting, enter the following strings for the selected label policy:

- Key: **EnableCustomPermissions**
- Value: **False**

Example PowerShell command, where your label policy is named "Global":

```
Set-LabelPolicy -Identity Global -AdvancedSettings @{EnableCustomPermissions="False"}
```

## For files protected with custom permissions, always display custom permissions to users in File Explorer

This configuration uses a policy [advanced setting](#) that you must configure by using Office 365 Security & Compliance Center PowerShell.

When you configure the advanced client setting to [disable custom permissions in File Explorer](#), by default, users are not able to see or change custom permissions that are already set in a protected document.

However, there's another advanced client setting that you can specify so that in this scenario, users can see and change custom permissions for a protected document when they use File Explorer and right-click the file.

To configure this advanced setting, enter the following strings for the selected label policy:

- Key: **EnableCustomPermissionsForCustomProtectedFiles**
- Value: **True**

Example PowerShell command:

```
Set-LabelPolicy -Identity Global -AdvancedSettings @{EnableCustomPermissionsForCustomProtectedFiles="True"}
```

## For email messages with attachments, apply a label that matches the highest classification of those attachments

This configuration uses policy [advanced settings](#) that you must configure by using Office 365 Security & Compliance Center PowerShell.

This setting is for when users attach labeled documents to an email, and do not label the email message itself. In this scenario, a label is automatically selected for them, based on the classification labels that are applied to the attachments. The highest classification label is selected.

The attachment must be a physical file, and cannot be a link to a file (for example, a link to a file on Microsoft SharePoint or OneDrive).

You can configure this setting to **Recommended**, so that users are prompted to apply the selected label to their email message, with a customizable tooltip. Users can accept the recommendation or dismiss it. Or, you can configure this setting to **Automatic**, where the selected label is automatically applied but users can remove the label or select a different label before sending the email.

#### **NOTE**

When the attachment with the highest classification label is configured for protection with the setting of user-defined permissions:

- When the label's user-defined permissions include Outlook (Do Not Forward), that label is selected and Do Not Forward protection is applied to the email.
- When the label's user-defined permissions are just for Word, Excel, PowerPoint, and File Explorer, that label is not applied to the email message, and neither is protection.

To configure this advanced setting, enter the following strings for the selected label policy:

- Key 1: **AttachmentAction**
- Key Value 1: **Recommended** or **Automatic**
- Key 2: **AttachmentActionTip**
- Key Value 2: "<customized tooltip>"

The customized tooltip supports a single language only.

Example PowerShell command, where your label policy is named "Global":

```
Set-LabelPolicy -Identity Global -AdvancedSettings @{AttachmentAction="Automatic"}
```

## Add "Report an Issue" for users

This configuration uses a policy [advanced setting](#) that you must configure by using Office 365 Security & Compliance Center PowerShell.

When you specify the following advanced client setting, users see a **Report an Issue** option that they can select from the **Help and Feedback** client dialog box. Specify an HTTP string for the link. For example, a customized web page that you have for users to report issues, or an email address that goes to your help desk.

To configure this advanced setting, enter the following strings for the selected label policy:

- Key: **ReportAnIssueLink**
- Value: <HTTP string>

Example value for a website: `https://support.contoso.com`

Example value for an email address: `mailto:helpdesk@contoso.com`

Example PowerShell command, where your label policy is named "Global":

```
Set-LabelPolicy -Identity Global -AdvancedSettings @{ReportAnIssueLink="mailto:helpdesk@contoso.com"}
```

## Implement pop-up messages in Outlook that warn, justify, or block emails being sent

This configuration uses policy [advanced settings](#) that you must configure by using Office 365 Security & Compliance Center PowerShell.

When you create and configure the following advanced client settings, users see pop-up messages in Outlook that

can warn them before sending an email, or ask them to provide justification why they are sending an email, or prevent them from sending an email for either of the following scenarios:

- **Their email or attachment for the email has a specific label:**
  - The attachment can be any file type
- **Their email or attachment for the email doesn't have a label:**
  - The attachment can be an Office document or PDF document

When these conditions are met, the user sees a pop-up message with one of the following actions:

- **Warn:** The user can confirm and send, or cancel.
- **Justify:** The user is prompted for justification (predefined options or free-form). The user can then send or cancel the email. The justification text is written to the email x-header, so that it can be read by other systems. For example, data loss prevention (DLP) services.
- **Block:** The user is prevented from sending the email while the condition remains. The message includes the reason for blocking the email, so the user can address the problem. For example, remove specific recipients, or label the email.

When the popup-messages are for a specific label, you can configure exceptions for recipients by domain name.

**TIP**

See the video [Azure Information Protection Outlook Popup Configuration](#) for a walkthrough example of how to configure these settings.

**To implement the warn, justify, or block pop-up messages for specific labels:**

For the selected policy, create one or more of the following advanced settings with the following keys. For the values, specify one or more labels by their GUIDs, each one separated by a comma.

Example value for multiple label GUIDs as a comma-separated string:

```
dcf781ba-727f-4860-b3c1-73479e31912b,1ace2cc3-14bc-4142-9125-bf946a70542c,3e9df74d-3168-48af-8b11-037e3021813f
```

- Warn messages:
  - Key: **OutlookWarnUntrustedCollaborationLabel**
  - Value: <label GUIDs, comma-separated>
- Justification messages:
  - Key: **OutlookJustifyUntrustedCollaborationLabel**
  - Value: <label GUIDs, comma-separated>
- Block messages:
  - Key: **OutlookBlockUntrustedCollaborationLabel**
  - Value: <label GUIDs, comma-separated>

Example PowerShell command, where your label policy is named "Global":

```

Set-LabelPolicy -Identity Global -AdvancedSettings @{OutlookWarnUntrustedCollaborationLabel="8faca7b8-8d20-48a3-8ea2-0f96310a848e,b6d21387-5d34-4dc8-90ae-049453cec5cf,bb48a6cb-44a8-49c3-9102-2d2b017dcead,74591a94-1e0e-4b5d-b947-62b70fc0f53a,6c375a97-2b9b-4cccd-9c5b-e24e4fd67f73"}

Set-LabelPolicy -Identity Global -AdvancedSettings @{OutlookJustifyUntrustedCollaborationLabel="dc284177-b2ac-4c96-8d78-e3e1e960318f,d8bb73c3-399d-41c2-a08a-6f0642766e31,750e87d4-0e91-4367-be44-c9c24c9103b4,32133e19-ccb9-4ff1-9254-3a6464bf89fd,74348570-5f32-4df9-8a6b-e6259b74085b,3e8d34df-e004-45b5-ae3d-efdc4731df24"}

Set-LabelPolicy -Identity Global -AdvancedSettings @{OutlookBlockUntrustedCollaborationLabel="0eb351a6-0c2d-4c1d-a5f6-caa80c9bdeec,40e82af6-5dad-45ea-9c6a-6fe6d4f1626b"}

```

#### To exempt domain names for pop-up messages configured for specific labels

For the labels that you've specified with these pop-up messages, you can exempt specific domain names so that users do not see the messages for recipients who have that domain name included in their email address. In this case, the emails are sent without interruption. To specify multiple domains, add them as a single string, separated by commas.

A typical configuration is to display the pop-up messages only for recipients who are external to your organization or who aren't authorized partners for your organization. In this case, you specify all the email domains that are used by your organization and by your partners.

For the same label policy, create the following advanced client settings and for the value, specify one or more domains, each one separated by a comma.

Example value for multiple domains as a comma-separated string: `contoso.com,fabrikam.com,litware.com`

- Warn messages:
  - Key: **OutlookWarnTrustedDomains**
  - Value: <domain names, comma separated>
- Justification messages:
  - Key: **OutlookJustifyTrustedDomains**
  - Value: <domain names, comma separated>
- Block messages:
  - Key: **OutlookBlockTrustedDomains**
  - Value: <domain names, comma separated>

For example, you have specified the **OutlookBlockUntrustedCollaborationLabel** advanced client setting for the **Confidential \ All Employees** label. You now specify the additional advanced client setting of **OutlookJustifyTrustedDomains** and **contoso.com**. As a result, a user can send an email to **john@sales.contoso.com** when it is labeled **Confidential \ All Employees** but will be blocked from sending an email with the same label to a Gmail account.

Example PowerShell commands, where your label policy is named "Global":

```

Set-LabelPolicy -Identity Global -AdvancedSettings @{OutlookBlockTrustedDomains="gmail.com"}

Set-LabelPolicy -Identity Global -AdvancedSettings
@{OutlookJustifyTrustedDomains="contoso.com,fabrikam.com,litware.com"}

```

#### To implement the warn, justify, or block pop-up messages for emails or attachments that don't have a label:

For the same label policy, create the following advanced client setting with one of the following values:

- Warn messages:
  - Key: **OutlookUnlabeledCollaborationAction**
  - Value: **Warn**
- Justification messages:
  - Key: **OutlookUnlabeledCollaborationAction**
  - Value: **Justify**
- Block messages:
  - Key: **OutlookUnlabeledCollaborationAction**
  - Value: **Block**
- Turn off these messages:
  - Key: **OutlookUnlabeledCollaborationAction**
  - Value: **Off**

Example PowerShell command, where your label policy is named "Global":

```
Set-LabelPolicy -Identity Global -AdvancedSettings @{OutlookUnlabeledCollaborationAction="Warn"}
```

**To define specific file name extensions for the warn, justify, or block pop-up messages for email attachments that don't have a label**  
 By default, the warn, justify, or block pop-up messages apply to all Office documents and PDF documents. You can refine this list by specifying which file name extensions should display the warn, justify, or block messages with an additional advanced setting and a comma-separated list of file name extensions.

Example value for multiple file name extensions to define as a comma-separated string:

```
.XLSX, .XLSM, .XLS, .XLTX, .XLTM, .DOCX, .DOCM, .DOC, .DOCX, .DOCM, .PPTX, .PPTM, .PPT, .PPTX, .PPTM
```

In this example, an unlabeled PDF document will not result in warn, justify, or block pop-up messages.

For the same label policy, enter the following strings:

- Key: **OutlookOverrideUnlabeledCollaborationExtensions**
- Value: <file name extensions to display messages, comma separated>

Example PowerShell command, where your label policy is named "Global":

```
Set-LabelPolicy -Identity Global -AdvancedSettings @{OutlookOverrideUnlabeledCollaborationExtensions=".PPTX, .PPTM, .PPT, .PPTX, .PPTM"}
```

**To specify a different action for email messages without attachments**

By default, the value that you specify for OutlookUnlabeledCollaborationAction to warn, justify, or block pop-up messages applies to emails or attachments that don't have a label. You can refine this configuration by specifying another advanced setting for email messages that don't have attachments.

Create the following advanced client setting with one of the following values:

- Warn messages:
  - Key: **OutlookUnlabeledCollaborationActionOverrideMailBodyBehavior**
  - Value: **Warn**

- Justification messages:
  - Key: **OutlookUnlabeledCollaborationActionOverrideMailBodyBehavior**
  - Value: **Justify**
- Block messages:
  - Key: **OutlookUnlabeledCollaborationActionOverrideMailBodyBehavior**
  - Value: **Block**
- Turn off these messages:
  - Key: **OutlookUnlabeledCollaborationActionOverrideMailBodyBehavior**
  - Value: **Off**

If you don't specify this client setting, the value that you specify for **OutlookUnlabeledCollaborationAction** is used for unlabeled email messages without attachments as well as unlabeled email messages with attachments.

Example PowerShell command, where your label policy is named "Global":

```
Set-LabelPolicy -Identity Global -AdvancedSettings
@{OutlookUnlabeledCollaborationActionOverrideMailBodyBehavior="Warn"}
```

## Disable sending audit data to Azure Information Protection analytics

This configuration uses a policy [advanced setting](#) that you must configure by using Office 365 Security & Compliance Center PowerShell.

The Azure Information Protection unified labeling client supports central reporting and by default, sends its audit data to [Azure Information Protection analytics](#). For more information about what information is sent and stored, see the [Information collected and sent to Microsoft](#) section from the central reporting documentation.

To change this behavior so that this information is not sent by the unified labeling client, enter the following strings for the selected label policy:

- Key: **EnableAudit**
- Value: **False**

Example PowerShell command, where your label policy is named "Global":

```
Set-LabelPolicy -Identity Global -AdvancedSettings @{EnableAudit="False"}
```

## Disable sending discovered sensitive information in documents to Azure Information Protection analytics

This configuration uses a policy [advanced setting](#) that you must configure by using Office 365 Security & Compliance Center PowerShell.

When the Azure Information Protection unified labeling client is used in Office apps, it looks for sensitive information in documents when they are first saved. Providing the [EnableAudit](#) advanced setting is not set to **False**, any predefined and custom sensitive information types found are then sent to [Azure Information Protection analytics](#).

To change this behavior so that sensitive information types found by the unified labeling client are not sent, enter

the following strings for the selected label policy:

- Key: **RunAuditInformationTypesDiscovery**
- Value: **False**

If you set this advanced client setting, auditing information can still be sent from the client, but the information is limited to reporting when a user has accessed labeled content.

For example:

- With this setting, you can see that a user accessed Financial.docx that is labeled **Confidential \ Sales**.
- Without this setting, you can see that Financial.docx contains 6 credit card numbers.
  - If you also enable [content matches for deeper analysis](#), you will additionally be able to see what those credit card numbers are.

Example PowerShell command, where your label policy is named "Global":

```
Set-LabelPolicy -Identity Global -AdvancedSettings @{RunAuditInformationTypesDiscovery="False"}
```

## Send information type matches to Azure Information Protection analytics

This configuration uses a policy [advanced setting](#) that you must configure by using Office 365 Security & Compliance Center PowerShell.

By default, the unified labeling client does not send content matches for sensitive info types to [Azure Information Protection analytics](#). For more information about this additional information that can be sent, see the [Content matches for deeper analysis](#) section from the central reporting documentation.

To send content matches when sensitive information types are sent, create the following advanced client setting in a label policy:

- Key: **LogMatchedContent**
- Value: **True**

Example PowerShell command, where your label policy is named "Global":

```
Set-LabelPolicy -Identity Global -AdvancedSettings @{LogMatchedContent="True"}
```

## Limit CPU consumption

Starting from scanner version 2.7.x.x, we recommend limiting CPU consumption using the following **ScannerMaxCPU** and **ScannerMinCPU** advanced settings method.

### IMPORTANT

When the following thread limiting policy is in use, **ScannerMaxCPU** and **ScannerMinCPU** advanced settings are ignored. To limit CPU consumption using **ScannerMaxCPU** and **ScannerMinCPU** advanced settings, cancel use of policies that limit the number of threads.

This configuration uses a policy [advanced setting](#) that you must configure by using Office 365 Security & Compliance Center PowerShell.

To limit CPU consumption on the scanner machine, it is manageable by creating two advanced settings: **ScannerMaxCPU** and **ScannerMinCPU**.

By default, **ScannerMaxCPU** is set to 100, which means there is no limit of maximum CPU consumption. In this case, the scanner process will try to use all available CPU time to maximize your scan rates.

If you set **ScannerMaxCPU** to less than 100, scanner will monitor the CPU consumption over the past 30 minutes, and if the max CPU crossed the limit you set, it will start to reduce number of threads allocated for new files. The limit on the number of threads will continue as long as CPU consumption is higher than the limit set for **ScannerMaxCPU**.

**ScannerMinCPU**, is only checked if **ScannerMaxCPU** is not equal to 100. **ScannerMinCPU** cannot be set to a number higher than the **ScannerMaxCPU** number. We recommend keeping **ScannerMinCPU** set at least 15 points lower than the value of **ScannerMaxCPU**.

The default value of this setting is 50, which means that if CPU consumption in last 30 minutes went lower than this value, scanner will start adding new threads to scan more files in parallel, until the CPU consumption reaches the level you have set for **ScannerMaxCPU**-15.

## Limit the number of threads used by the scanner

### IMPORTANT

When the following thread limiting policy is in use, **ScannerMaxCPU** and **ScannerMinCPU** advanced settings are ignored. To limit CPU consumption using **ScannerMaxCPU** and **ScannerMinCPU** advanced settings, cancel use of policies that limit the number of threads.

This configuration uses a policy [advanced setting](#) that you must configure by using Office 365 Security & Compliance Center PowerShell.

By default, the scanner uses all available processor resources on the computer running the scanner service. If you need to limit the CPU consumption while this service is scanning, create the following advanced setting in a label policy.

For the value, specify the number of concurrent threads that the scanner can run in parallel. The scanner uses a separate thread for each file that it scans, so this throttling configuration also defines the number of files that can be scanned in parallel.

When you first configure the value for testing, we recommend you specify 2 per core, and then monitor the results. For example, if you run the scanner on a computer that has 4 cores, first set the value to 8. If necessary, increase or decrease that number, according to the resulting performance you require for the scanner computer and your scanning rates.

- Key: **ScannerConcurrencyLevel**
- Value: <number of concurrent threads>

Example PowerShell command, where your label policy is named "Scanner":

```
Set-LabelPolicy -Identity Scanner -AdvancedSettings @{ScannerConcurrencyLevel="8"}
```

## Migrate labels from Secure Islands and other labeling solutions

This configuration uses a label [advanced setting](#) that you must configure by using Office 365 Security & Compliance Center PowerShell.

This configuration is not compatible with protected PDF files that have a .ppdf file name extension. These files cannot be opened by the client using File Explorer or PowerShell.

For Office documents that are labeled by Secure Islands, you can relabel these documents with a sensitivity label by using a mapping that you define. You also use this method to reuse labels from other solutions when their labels are on Office documents.

As a result of this configuration option, the new sensitivity label is applied by the Azure Information Protection unified labeling client as follows:

- For Office documents: When the document is opened in the desktop app, the new sensitivity label is shown as set and is applied when the document is saved.
- For PowerShell: [Set-AIPFileLabel](#) and [Set-AIPFileClassification](#) can apply the new sensitivity label.
- For File Explorer: In the Azure Information Protection dialog box, the new sensitivity label is shown but isn't set.

This configuration requires you to specify an advanced setting named **labelByCustomProperties** for each sensitivity label that you want to map to the old label. Then for each entry, set the value by using the following syntax:

```
[migration rule name],[Secure Islands custom property name],[Secure Islands metadata Regex value]
```

Specify your choice of a migration rule name. Use a descriptive name that helps you to identify how one or more labels from your previous labeling solution should be mapped to sensitivity label.

Note that this setting does not remove the original label from the document or any visual markings in the document that the original label might have applied. To remove headers and footers, see the earlier section, [Remove headers and footers from other labeling solutions](#).

#### **Example 1: One-to-one mapping of the same label name**

Requirement: Documents that have a Secure Islands label of "Confidential" should be relabeled as "Confidential" by Azure Information Protection.

In this example:

- The Secure Islands label is named **Confidential** and stored in the custom property named **Classification**.

The advanced setting:

- Key: **labelByCustomProperties**
- Value: **Secure Islands label is Confidential,Classification,Confidential**

Example PowerShell command, where your label is named "Confidential":

```
Set-Label -Identity Confidential -AdvancedSettings @{labelByCustomProperties="Secure Islands label is Confidential,Classification,Confidential"}
```

#### **Example 2: One-to-one mapping for a different label name**

Requirement: Documents labeled as "Sensitive" by Secure Islands should be relabeled as "Highly Confidential" by Azure Information Protection.

In this example:

- The Secure Islands label is named **Sensitive** and stored in the custom property named **Classification**.

The advanced setting:

- Key: **labelByCustomProperties**
- Value: **Secure Islands label is Sensitive,Classification,Sensitive**

Example PowerShell command, where your label is named "Highly Confidential":

```
Set-Label -Identity "Highly Confidential" -AdvancedSettings @{labelByCustomProperties="Secure Islands label is Sensitive,Classification,Sensitive"}
```

#### **Example 3: Many-to-one mapping of label names**

Requirement: You have two Secure Islands labels that include the word "Internal" and you want documents that have either of these Secure Islands labels to be relabeled as "General" by the Azure Information Protection unified labeling client.

In this example:

- The Secure Islands labels include the word **Internal** and are stored in the custom property named **Classification**.

The advanced client setting:

- Key: **labelByCustomProperties**
- Value: **Secure Islands label contains Internal,Classification,.Internal.\***

Example PowerShell command, where your label is named "General":

```
Set-Label -Identity General -AdvancedSettings @{labelByCustomProperties="Secure Islands label contains Internal,Classification,.Internal.*"}
```

#### **Example 4: Multiple rules for the same label**

When you need multiple rules for the same label, define multiple string values for the same key.

In this example, the Secure Islands labels named "Confidential" and "Secret" are stored in the custom property named **Classification**, and you want the Azure Information Protection unified labeling client to apply the sensitivity label named "Confidential":

```
Set-Label -Identity Confidential -AdvancedSettings @{labelByCustomProperties=ConvertTo-Json("Migrate Confidential label,Classification,Confidential", "Migrate Secret label,Classification,Secret")}
```

#### **Extend your label migration rules to emails**

You can use your labelByCustomProperties advanced settings with Outlook emails in addition to Office documents by specifying an additional label policy advanced setting. However, this setting has a known negative impact on the performance of Outlook, so configure this additional setting only when you have a strong business requirement for it and remember to set it to a null string value when you have completed the migration from the other labeling solution.

To configure this advanced setting, enter the following strings for the selected label policy:

- Key: **EnableLabelByMailHeader**
- Value: **True**

Example PowerShell command, where your label policy is named "Global":

```
Set-LabelPolicy -Identity Global -AdvancedSettings @{EnableLabelByMailHeader="True"}
```

## Extend your label migration rules to SharePoint properties

You can use your labelByCustomProperties advanced settings with SharePoint properties that you might expose as columns to users.

This setting is supported when you use Word, Excel, and PowerPoint.

To configure this advanced setting, enter the following strings for the selected label policy:

- Key: **EnableLabelBySharePointProperties**
- Value: **True**

Example PowerShell command, where your label policy is named "Global":

```
Set-LabelPolicy -Identity Global -AdvancedSettings @{EnableLabelBySharePointProperties="True"}
```

## Apply a custom property when a label is applied

This configuration uses a label [advanced setting](#) that you must configure by using Office 365 Security & Compliance Center PowerShell.

There might be some scenarios when you want to apply one or more custom properties to a document or email message in addition to the metadata that's applied by a sensitivity label.

For example:

- You are in the process of [migrating from another labeling solution](#), such as Secure Islands. For interoperability during the migration, you want sensitivity labels to also apply a custom property that is used by the other labeling solution.
- For your content management system (such as SharePoint or a document management solution from another vendor) you want to use a consistent custom property name with different values for the labels, and with user-friendly names instead of the label GUID.

For Office documents and Outlook emails that users label by using the Azure Information Protection unified labeling client, you can add one or more custom properties that you define. You can also use this method for the unified labeling client to display a custom property as a label from other solutions for content that isn't yet labeled by the unified labeling client.

As a result of this configuration option, any additional custom properties are applied by the Azure Information Protection unified labeling client as follows:

- For Office documents: When the document is labeled in the desktop app, the additional custom properties are applied when the document is saved.
- For Outlook emails: When the email message is labeled in Outlook, the additional properties are applied to the x-header when the email is sent.
- For PowerShell: [Set-AIPFileLabel](#) and [Set-AIPFileClassification](#) applies the additional custom properties when the document is labeled and saved. [Get-AIPFileStatus](#) displays custom properties as the mapped label if a sensitivity label isn't applied.
- For File Explorer: When the user right-clicks the file and applies the label, the custom properties are applied.

This configuration requires you to specify an advanced setting named **customPropertiesByLabel** for each sensitivity label that you want to apply the additional custom properties. Then for each entry, set the value by using the following syntax:

```
[custom property name],[custom property value]
```

## IMPORTANT

Use of white spaces in the string will prevent application of the labels.

### Example 1: Add a single custom property for a label

Requirement: Documents that are labeled as "Confidential" by the Azure Information Protection unified labeling client should have the additional custom property named "Classification" with the value of "Secret".

In this example:

- The sensitivity label is named **Confidential** and creates a custom property named **Classification** with the value of **Secret**.

The advanced setting:

- Key: **customPropertiesByLabel**
- Value: **Classification,Secret**

Example PowerShell command, where your label is named "Confidential":

```
Set-Label -Identity Confidential -AdvancedSettings @{customPropertiesByLabel="Classification,Secret"}
```

### Example 2: Add multiple custom properties for a label

To add more than one custom property for the same label, you need to define multiple string values for the same key.

Example PowerShell command, where your label is named "General" and you want to add one custom property named **Classification** with the value of **General** and a second custom property named **Sensitivity** with the value of **Internal**:

```
Set-Label -Identity General -AdvancedSettings @{customPropertiesByLabel=ConvertToJson("Classification,General", "Sensitivity,Internal")}
```

## Configure a label to apply S/MIME protection in Outlook

This configuration uses label [advanced settings](#) that you must configure by using Office 365 Security & Compliance Center PowerShell.

Use these settings only when you have a working [S/MIME deployment](#) and want a label to automatically apply this protection method for emails rather than Rights Management protection from Azure Information Protection. The resulting protection is the same as when a user manually selects S/MIME options from Outlook.

To configure an advanced setting for an S/MIME digital signature, enter the following strings for the selected label:

- Key: **SMimeSign**
- Value: **True**

To configure an advanced setting for S/MIME encryption, enter the following strings for the selected label:

- Key: **SMimeEncrypt**
- Value: **True**

If the label you specify is configured for encryption, for the Azure Information Protection unified labeling client, S/MIME protection replaces the Rights Management protection only in Outlook. The general availability version of the unified labeling client continues to use the encryption settings specified for the label in the admin center. For Office apps with built-in labeling, these do not apply the S/MIME protection but instead, apply Do Not Forward protection.

If you want the label to be visible in Outlook only, configure the label to apply encryption to **Only email messages in Outlook**.

Example PowerShell commands, where your label is named "Recipients Only":

```
Set-Label -Identity "Recipients Only" -AdvancedSettings @{SMimeSign="True"}
Set-Label -Identity "Recipients Only" -AdvancedSettings @{SMimeEncrypt="True"}
```

## Specify a default sublabel for a parent label

This configuration uses a label [advanced setting](#) that you must configure by using Office 365 Security & Compliance Center PowerShell.

When you add a sublabel to a label, users can no longer apply the parent label to a document or email. By default, users select the parent label to see the sublabels that they can apply, and then select one of those sublabels. If you configure this advanced setting, when users select the parent label, a sublabel is automatically selected and applied for them:

- Key: **DefaultSubLabelId**
- Value: <sublabel GUID>

Example PowerShell command, where your parent label is named "Confidential" and the "All Employees" sublabel has a GUID of 8faca7b8-8d20-48a3-8ea2-0f96310a848e:

```
Set-Label -Identity "Confidential" -AdvancedSettings @{DefaultSubLabelId="8faca7b8-8d20-48a3-8ea2-0f96310a848e"}
```

## Turn on classification to run continuously in the background

This configuration uses a label [advanced setting](#) that you must configure by using Office 365 Security & Compliance Center PowerShell. This setting is in preview and might change.

When you configure this setting, it changes the default behavior of how the Azure Information Protection unified labeling client applies automatic and recommended labels to documents:

For Word, Excel, and PowerPoint, automatic classification runs continuously in the background.

The behavior does not change for Outlook. When the Azure Information Protection unified labeling client periodically checks documents for the condition rules that you specify, this behavior enables automatic and recommended classification and protection for documents that are stored in SharePoint. Large files also save more quickly because the condition rules have already run.

The condition rules do not run in real time as a user types. Instead, they run periodically as a background task if the document is modified.

To configure this advanced setting, enter the following strings:

- Key: **RunPolicyInBackground**

- Value: **True**

Example PowerShell command:

```
Set-LabelPolicy -Identity PolicyName -AdvancedSettings @{RunPolicyInBackground = "true"}
```

## Specify a color for the label

This configuration uses label [advanced settings](#) that you must configure by using Office 365 Security & Compliance Center PowerShell.

Use this advanced setting to set a color for a label. To specify the color, enter a hex triplet code for the red, green, and blue (RGB) components of the color. For example, #40e0d0 is the RGB hex value for turquoise.

If you need a reference for these codes, you'll find a helpful table from the [<color>](#) page from the MSDN web docs. You also find these codes in many applications that let you edit pictures. For example, Microsoft Paint lets you choose a custom color from a palette and the RGB values are automatically displayed, which you can then copy.

To configure the advanced setting for a label's color, enter the following strings for the selected label:

- Key: **color**
- Value: <RGB hex value>

Example PowerShell command, where your label is named "Public":

```
Set-Label -Identity Public -AdvancedSettings @{color="#40e0d0"}
```

## Sign in as a different user

In a production environment, users wouldn't usually need to sign in as a different user when they are using the Azure Information Protection unified labeling client. However, as an administrator, you might need to sign in as a different user during a testing phase.

You can verify which account you're currently signed in as by using the **Microsoft Azure Information Protection** dialog box: Open an Office application and on the **Home** tab, select the **Sensitivity** button, and then select **Help and feedback**. Your account name is displayed in the **Client status** section.

Be sure to also check the domain name of the signed in account that's displayed. It can be easy to miss that you're signed in with the right account name but wrong domain. A symptom of using the wrong account includes failing to download the labels, or not seeing the labels or behavior that you expect.

To sign in as a different user:

1. Navigate to %localappdata%\Microsoft\MSIP and delete the **TokenCache** file.
2. Restart any open Office applications and sign in with your different user account. If you do not see a prompt in your Office application to sign in to the Azure Information Protection service, return to the **Microsoft Azure Information Protection** dialog box and select **Sign in** from the updated **Client status** section.

Additionally:

- If the Azure Information Protection unified labeling client is still signed in with the old account after completing these steps, delete all cookies from Internet Explorer, and then repeat steps 1 and 2.

- If you are using single sign-on, you must sign out from Windows and sign in with your different user account after deleting the token file. The Azure Information Protection unified labeling client then automatically authenticates by using your currently signed in user account.
- This solution is supported for signing in as another user from the same tenant. It is not supported for signing in as another user from a different tenant. To test Azure Information Protection with multiple tenants, use different computers.
- You can use the **Reset settings** option from **Help and Feedback** to sign out and delete the currently downloaded labels and policy settings from the Office 365 Security & Compliance Center, the Microsoft 365 Security center, or the Microsoft 365 Compliance center.

## Support for disconnected computers

### **IMPORTANT**

Disconnected computers are supported for the following labeling scenarios: File Explorer, PowerShell, your Office apps and the scanner.

By default, the Azure Information Protection unified labeling client automatically tries to connect to the internet to download the labels and label policy settings from your labeling management center: The Office 365 Security & Compliance Center, the Microsoft 365 security center, or the Microsoft 365 compliance center. If you have computers that cannot connect to the internet for a period of time, you can export and copy files that manually manages the policy for the unified labeling client.

Instructions:

1. Choose or create a user account in Azure AD that you will use to download labels and policy settings that you want to use on your disconnected computer.
2. As an additional label policy setting for this account, [disable sending audit data to Azure Information Protection analytics](#) by using the **EnableAudit** advanced setting.

We recommend this step because if the disconnected computer does have periodic internet connectivity, it will send logging information to Azure Information Protection analytics that includes the user name from step 1. That user account might be different from the local account you're using on the disconnected computer.

3. From a computer with internet connectivity that has the unified labeling client installed and signed in with the user account from step 1, download the labels and policy settings.
4. From this computer, export the log files.

For example, run the [Export-AIPLogs](#) cmdlet, or use the **Export Logs** option from the client's **Help and Feedback** dialog box.

The log files are exported as a single compressed file.

5. Open the compressed file, and from the MSIP folder, copy any files that have a .xml file name extension.
6. Paste these files into the %localappdata%\Microsoft\MSIP folder on the disconnected computer.
7. If your chosen user account is one that usually connects to the internet, enable sending audit data again, by setting the **EnableAudit** value to True.

Be aware that if a user on this computer selects the **Reset Settings** option from **Help and feedback**, this action deletes the policy files and renders the client inoperable until you manually replace the files or the client connects to the internet and downloads the files.

If your disconnected computer is running the Azure Information Protection scanner, there are additional configuration steps you must take. For more information, see [Restriction: The scanner server cannot have internet connectivity](#) from the scanner deployment instructions.

## Change the local logging level

By default, the Azure Information Protection unified labeling client writes client log files to the `%localappdata%\Microsoft\MSIP` folder. These files are intended for troubleshooting by Microsoft Support.

To change the logging level for these files, locate the following value name in the registry and set the value data to the required logging level:

`HKEY_CURRENT_USER\SOFTWARE\Microsoft\MSIP\LogLevel`

Set the logging level to one of the following values:

- **Off:** No local logging.
- **Error:** Errors only.
- **Warn:** Errors and warnings.
- **Info:** Minimum logging, which includes no event IDs (the default setting for the scanner).
- **Debug:** Full information.
- **Trace:** Detailed logging (the default setting for clients).

This registry setting does not change the information that's sent to Azure Information Protection for [central reporting](#).

## Skip or ignore files during scans depending on file attributes

This configuration uses a policy [advanced setting](#) that you must configure by using Office 365 Security & Compliance Center PowerShell.

By default, the Azure Information Protection unified labeling scanner scans all relevant files. However, you may want to define specific files to be skipped, such as for archived files or files that have been moved.

Enable the scanner to skip specific files based on their file attributes by using the `ScannerFSAttributesToSkip` advanced setting. In the setting value, list the file attributes that will enable the file to be skipped when they are all set to `true`. This list of file attributes uses the AND logic.

The following sample PowerShell commands illustrate how to use this advanced setting with a label named "Global".

### Skip files that are both read-only and archived

```
Set-LabelPolicy -Identity Global -AdvancedSettings @{ ScannerFSAttributesToSkip ="FILE_ATTRIBUTE_READONLY, FILE_ATTRIBUTE_ARCHIVE"}
```

### Skip files that are either read-only or archived

To use an OR logic, run the same property multiple times. For example:

```
Set-LabelPolicy -Identity Global -AdvancedSettings @{ ScannerFSAttributesToSkip ="FILE_ATTRIBUTE_READONLY"}
Set-LabelPolicy -Identity Global -AdvancedSettings @{ ScannerFSAttributesToSkip ="FILE_ATTRIBUTE_ARCHIVE"}
```

#### TIP

We recommend that you consider enabling the scanner to skip files with the following attributes:

- FILE\_ATTRIBUTE\_SYSTEM
- FILE\_ATTRIBUTE\_HIDDEN
- FILE\_ATTRIBUTE\_DEVICE
- FILE\_ATTRIBUTE\_OFFLINE
- FILE\_ATTRIBUTE\_RECALL\_ON\_DATA\_ACCESS
- FILE\_ATTRIBUTE\_RECALL\_ON\_OPEN
- FILE\_ATTRIBUTE\_TEMPORARY

For a list of all file attributes that can be defined in the **ScannerFSAttributesToSkip** advanced setting, see the [Win32 File Attribute Constants](#)

## Preserve NTFS owners during labeling (public preview)

This configuration uses a policy [advanced setting](#) that you must configure by using Office 365 Security & Compliance Center PowerShell.

By default, scanner, PowerShell, and File Explorer extension labeling do not preserve the NTFS owner that was defined before the labeling.

To ensure that the NTFS owner value is preserved, set the **UseCopyAndPreserveNTFSOwner** advanced setting to **true** for the selected label policy.

#### Caution

Define this advanced setting only when you can ensure a low-latency, reliable network connection between the scanner and the scanned repository. A network failure during the automatic labeling process can cause the file to be lost.

Sample PowerShell command, when your label policy is named "Global":

```
Set-LabelPolicy -Identity Global -AdvancedSettings @{ UseCopyAndPreserveNTFSOwner ="true"}
```

## Next steps

Now that you've customized the Azure Information Protection unified labeling client, see the following resources for additional information that you might need to support this client:

- [Client files and usage logging](#)
- [File types supported](#)
- [PowerShell commands](#)

# Admin Guide: Azure Information Protection unified labeling client files and client usage logging

7/20/2020 • 2 minutes to read • [Edit Online](#)

*Applies to:* [Azure Information Protection](#), Windows 10, Windows 8.1, Windows 8, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

*\*Customers with extended Microsoft support for Windows 7 and Office 2010 can also get Azure Information Protection support for these versions. Check with your support contact for full details.*

*Instructions for:* [Azure Information Protection unified labeling client for Windows](#)

After you have installed the Azure Information Protection unified labeling client, you might need to know where files are located and monitor how the client is being used.

## File locations for the Azure Information Protection unified labeling client

Client files:

- For 64-bit operating systems: \ProgramFiles (x86)\Microsoft Azure Information Protection
- For 32-bit operating systems: \Program Files\Microsoft Azure Information Protection

Client logs files and currently installed policy files:

- For 64-bit and 32-bit operating systems: %localappdata%\Microsoft\MSIP

## Usage logging for the Azure Information Protection unified labeling client

The unified labeling client doesn't log user activity to the local Windows event log. Instead, use the [central reporting](#) feature of Azure Information Protection.

## Next steps

Now that you've identified all the log files associated with the Azure Information Protection unified labeling client, see the following for additional information that you might need to support this client:

- [Customizations](#)
- [File types supported](#)
- [PowerShell commands](#)

# Admin Guide: File types supported by the Azure Information Protection unified labeling client

7/20/2020 • 10 minutes to read • [Edit Online](#)

*Applies to: Azure Information Protection, Windows 10, Windows 8.1, Windows 8, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012>*

*\*Customers with extended Microsoft support for Windows 7 and Office 2010 can also get Azure Information Protection support for these versions. Check with your support contact for full details.*

*Instructions for: Azure Information Protection unified labeling client for Windows*

The Azure Information Protection unified labeling client can apply the following to documents and emails:

- Classification only
- Classification and protection
- Protection only

The Azure Information Protection unified labeling client can also inspect the content of some file types using well-known sensitive information types or regular expressions that you define.

Use the following information to check which file types the Azure Information Protection unified labeling client supports, understand the different levels of protection and how to change the default protection level, and to identify which files are automatically excluded (skipped) from classification and protection.

For the listed file types, WebDav locations are not supported.

## File types supported for classification only

The following file types can be classified even when they are not protected.

- **Adobe Portable Document Format:** .pdf
- **Microsoft Project:** .mpp, .mpt
- **Microsoft Publisher:** .pub
- **Microsoft XPS:** .xps .oxps
- **Images:** jpg, jpe, jpeg, jif, jifif, jfi, png, .tif, .tiff
- **Autodesk Design Review 2013:** .dwfx
- **Adobe Photoshop:** .psd
- **Digital Negative:** .dng
- **Microsoft Office:** File types in the following table.

The supported file formats for these file types are the 97-2003 file formats and Office Open XML formats for the following Office programs: Word, Excel, and PowerPoint.

OFFICE FILE TYPE	OFFICE FILE TYPE
.doc	.vsdm
.docm	.vsdx
.docx	.vss
.dot	.vssm
.dotm	.vst
.dotx	.vstm
.potm	.vssx
.potx	.vstx
.pps	.xls
.ppsm	.xlsb
.ppsx	.xlt
.ppt	.xlsm
.pptm	.xlsx
.pptx	.xltm
.vdw	.xltx
.vsd	

Additional file types support classification when they are also protected. For these file types, see the [Supported file types for classification and protection](#) section.

Examples:

- If the **General** sensitivity label applies classification and does not apply protection: You could apply the **General** label to a file named sales.pdf but you could not apply this label to a file named sales.txt.
- If the **Confidential \ All Employees** sensitivity label applies classification and protection: You could apply this label to a file named sales.pdf and a file named sales.txt. You could also apply just protection to these files, without classification.

## File types supported for protection

The Azure Information Protection unified labeling client supports protection at two different levels, as described in the following table.

TYPE OF PROTECTION	NATIVE	GENERIC

Type of protection	Native	Generic
Description	For text, image, Microsoft Office (Word, Excel, PowerPoint) files, .pdf files, and other application file types that support a Rights Management service, native protection provides a strong level of protection that includes both encryption and enforcement of rights (permissions).	For all other applications and file types, generic protection provides a level of protection that includes both file encapsulation using the .pfile file type and authentication to verify if a user is authorized to open the file.
Protection	<p>File protection is enforced in the following ways:</p> <ul style="list-style-type: none"> <li>- Before protected content is rendered, successful authentication must occur for those who receive the file through email or are given access to it through file or share permissions.</li> <li>- Additionally, usage rights and policy that were set by the content owner when the files were protected are enforced when the content is rendered in either the Azure Information Protection viewer (for protected text and image files) or the associated application (for all other supported file types).</li> </ul>	<p>File protection is enforced in the following ways:</p> <ul style="list-style-type: none"> <li>- Before protected content is rendered, successful authentication must occur for people who are authorized to open the file and given access to it. If authorization fails, the file does not open.</li> <li>- Usage rights and policy set by the content owner are displayed to inform authorized users of the intended usage policy.</li> <li>- Audit logging of authorized users opening and accessing files occurs. However, usage rights are not enforced.</li> </ul>
Default for file types	<p>This is the default level of protection for the following file types:</p> <ul style="list-style-type: none"> <li>- Text and image files</li> <li>- Microsoft Office (Word, Excel, PowerPoint) files</li> <li>- Portable document format (.pdf)</li> </ul> <p>For more information, see the following section, <a href="#">Supported file types for classification and protection</a>.</p>	This is the default protection for all other file types (such as .vsdx, .rtf, and so on) that are not supported by native protection.

You cannot change the default protection level that the Azure Information Protection unified labeling client or the scanner applies. However, you can change which file types are protected. For more information, see [Change which file types to protect](#).

The protection can be applied automatically when a user selects a sensitivity label that an administrator has configured, or users can specify their own custom protection settings by using [permission levels](#).

### File sizes supported for protection

There are maximum file sizes that the Azure Information Protection unified labeling client supports for protection.

- For Office files:

OFFICE APPLICATION	MAXIMUM FILE SIZE SUPPORTED
Word 2010	32-bit: 512 MB
Word 2013	64-bit: 512 MB
Word 2016	
Excel 2010	32-bit: 2 GB
Excel 2013	64-bit: Limited only by available disk space and memory
Excel 2016	
PowerPoint 2010	32-bit: Limited only by available disk space and memory
PowerPoint 2013	64-bit: Limited only by available disk space and memory
PowerPoint 2016	

- **For all other files:**

- To protect other file types, and to open these file types in the Azure Information Protection viewer: The maximum file size is limited only by available disk space and memory.
- To unprotect files by using the [Unprotect-RMSFile](#) cmdlet: The maximum file size supported for .pst files is 5 GB. Other file types are limited only by available disk space and memory

Tip: If you need to search or recover protected items in large .pst files, see [Guidance for using Unprotect-RMSFile for eDiscovery](#).

### Supported file types for classification and protection

The following table lists a subset of file types that support native protection by the Azure Information Protection unified labeling client, and that can also be classified.

These file types are identified separately because when they are natively protected, the original file name extension is changed, and these files become read-only. Note that when files are generically protected, the original file name extension is always changed to .pfile.

#### WARNING

If you have firewalls, web proxies, or security software that inspect and take action according to file name extensions, you might need to reconfigure these network devices and software to support these new file name extensions.

ORIGINAL FILE NAME EXTENSION	PROTECTED FILE NAME EXTENSION
.txt	.ptxt
.xml	.pxml
.jpg	.pjjpg
.jpeg	.pjjpeg
.png	.ppng

ORIGINAL FILE NAME EXTENSION	PROTECTED FILE NAME EXTENSION
.tif	.ptif
.tiff	.ptiff
.bmp	.pbmp
.gif	.pgif
.jpe	.pjpe
.jfif	.pjfif
.jt	.pjt

The next table lists the remaining file types that support native protection by the Azure Information Protection unified labeling client, and that can also be classified. You will recognize these as file types for Microsoft Office apps. The supported file formats for these file types are the 97-2003 file formats and Office Open XML formats for the following Office programs: Word, Excel, and PowerPoint.

For these files, the file name extension remains the same after the file is protected by a Rights Management service.

FILE TYPES SUPPORTED BY OFFICE	FILE TYPES SUPPORTED BY OFFICE
.doc	.vsdx
.docm	.vssm
.docx	.vssx
.dot	.vstm
.dotm	.vstx
.dotx	.xla
.potm	.xlam
.potx	.xls
.pps	.xlbs
.ppsm	.xlt
.ppsx	.xlsm
.ppt	.xlsx
.pptm	.xltm
.pptx	.xltx
.vsdm	.xps

## File types that are excluded from classification and protection

To help prevent users from changing files that are critical for computer operations, some file types and folders are automatically excluded from classification and protection. If users try to classify or protect these files by using the Azure Information Protection unified labeling client, they see a message that they are excluded.

- **Excluded file types:** .lnk, .exe, .com, .cmd, .bat, .dll, .ini, .pst, .sca, .drm, .sys, .cpl, .inf, .drv, .dat, .tmp, .msp, .msi, .pdb, .jar

- **Excluded folders:**

- Windows
- Program Files (\Program Files and \Program Files (x86))
- \ProgramData
- \AppData (for all users)

### **File types that are excluded from classification and protection by the Azure Information Protection scanner**

By default, the scanner also excludes the same file types as the Azure Information Protection unified labeling client with the following exceptions:

- .msg, .rtf, and .rar, are also excluded

You can change the file types included or excluded for file inspection by the scanner:

- Configure **File types to scan** in the scanner profile, by [using the Azure portal](#).

**NOTE**

If you include .rtf files for scanning, carefully monitor the scanner. Some .rtf files cannot be successfully inspected by the scanner and for these files, the inspection doesn't complete and the service must be restarted.

By default, the scanner protects only Office file types, and PDF files when they are protected by using the ISO standard for PDF encryption. To change this behavior for the scanner, use the PowerShell advanced setting, **PFileSupportedExtensions**. For more information, see [Use PowerShell to change which file types are protected](#) from the scanner deployment instructions.

### **Files that cannot be protected by default**

Any file that is password-protected cannot be natively protected by the Azure Information Protection unified labeling client unless the file is currently open in the application that applies the protection. You most often see PDF files that are password-protected but other applications, such as Office apps, also offer this functionality.

### **Limitations for container files, such as .zip files**

Container files are files that include other files, with a typical example being .zip files that contain compressed files. Other examples include .rar, .7z, .msg files, and PDF documents that include attachments.

You can classify and protect these container files, but the classification and protection is not applied to each file inside the container.

If you have a container file that includes classified and protected files, you must first extract the files to change their classification or protection settings.

The Azure Information Protection viewer cannot open attachments in a protected PDF document. In this scenario, when the document is opened in the viewer, the attachments are not visible.

## **File types supported for inspection**

Without any additional configuration, the Azure Information Protection unified labeling client uses Windows IFilter to inspect the contents of documents. Windows IFilter is used by Windows Search for indexing. As a result,

the following file types can be inspected when you use the [Set-AIPFileClassification](#) PowerShell command.

APPLICATION TYPE	FILE TYPE
Word	.doc; .docx; .docm; .dot; .dotm; .dotx
Excel	.xls; .xlt; .xlsx; .xltx; .xltm; .xslm; .xlsb
PowerPoint	.ppt; .pps; .pot; .pptx; .ppsx; .pptm; .ppsm; .potx; .potm
PDF	.pdf
Text	.txt; .xml; .csv

With additional configuration, other file types can also be inspected. For example, you can [register a custom file name extension to use the existing Windows filter handler for text files](#), and you can install additional filters from software vendors.

To check what filters are installed, see the [Finding a Filter Handler for a Given File Extension](#) section from the Windows Search Developer's Guide.

The following sections have configuration instructions to inspect .zip files, and .tiff files.

### To inspect .zip files

The Azure Information Protection scanner and the [Set-AIPFileClassification](#) PowerShell command can inspect .zip files when you follow these instructions:

1. For the computer running the scanner or the PowerShell session, install the [Office 2010 Filter Pack SP2](#).
2. For the scanner: After finding sensitive information, if the .zip file should be classified and protected with a label, specify the .zip file name extension with the PowerShell advanced setting, **PFileSupportedExtensions**, as described in [Use PowerShell to change which file types are protected](#) from the scanner deployment instructions.

Example scenario after doing these steps:

A file named **accounts.zip** contains Excel spreadsheets with credit card numbers. You have a sensitivity label named **Confidential \ Finance**, which is configured to discover credit card numbers and automatically apply the label with protection that restricts access to the Finance group.

After inspecting the file, the unified labeling client from your PowerShell session classifies this file as **Confidential \ Finance**, applies generic protection to the file so that only members of the Finance groups can unzip it, and renames the file **accounts.zip.pfile**.

### To inspect .tiff files by using OCR

The [Set-AIPFileClassification](#) PowerShell command can use optical character recognition (OCR) to inspect TIFF images with a .tiff file name extension when you install the Windows TIFF IFilter feature, and then configure [Windows TIFF IFilter Settings](#) on the computer running the PowerShell session.

For the scanner: After finding sensitive information, if the .tiff file should be classified and protected with a label, specify this file name extension with the PowerShell advanced setting, **PFileSupportedExtensions**, as described in [Use PowerShell to change which file types are protected](#) from the scanner deployment instructions.

## Next steps

Now that you've identified the file types supported by the Azure Information Protection unified labeling client, see

the following resources for additional information that you might need to support this client:

- [Customizations](#)
- [Client files and usage logging](#)
- [PowerShell commands](#)

# Admin Guide: Using PowerShell with the Azure Information Protection unified client

7/20/2020 • 8 minutes to read • [Edit Online](#)

*Applies to: Azure Information Protection, Windows 10, Windows 8.1, Windows 8, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012*

*\*Customers with extended Microsoft support for Windows 7 and Office 2010 can also get Azure Information Protection support for these versions. Check with your support contact for full details.*

*Instructions for: Azure Information Protection unified labeling client for Windows*

When you install the Azure Information Protection unified labeling client, PowerShell commands are automatically installed. This lets you manage the client by running commands that you can put into scripts for automation.

The cmdlets are installed with the PowerShell module `AzureInformationProtection`, which has cmdlets for labeling. For example:

LABELING CMDLET	EXAMPLE USAGE
<code>Get-AIPFileStatus</code>	For a shared folder, identify all files with a specific label.
<code>Set-AIPFileClassification</code>	For a shared folder, inspect the file contents and then automatically label unlabeled files, according to the conditions that you have specified.
<code>Set-AIPFileLabel</code>	For a shared folder, apply a specified label to all files that do not have a label.
<code>Set-AIPAuthentication</code>	Label files non-interactively, for example by using a script that runs on a schedule.

## TIP

To use cmdlets with path lengths greater than 260 characters, use the following [group policy setting](#) that is available starting Windows 10, version 1607:

**Local Computer Policy > Computer Configuration > Administrative Templates > All Settings > Enable Win32 long paths**

For Windows Server 2016, you can use the same group policy setting when you install the latest Administrative Templates (.admx) for Windows 10.

For more information, see the [Maximum Path Length Limitation](#) section from the Windows 10 developer documentation.

This module installs in `\ProgramFiles (x86)\Microsoft Azure Information Protection` and adds this folder to the `PSModulePath` system variable. The .dll for this module is named `AIP.dll`.

## **IMPORTANT**

The AzureInformationProtection module doesn't support configuring advanced settings for labels or label policies. For these settings, you need the Office 365 Security & Compliance Center PowerShell. For more information, see [Custom configurations for the Azure Information Protection unified labeling client](#).

## **Prerequisites for using the AzureInformationProtection module**

In addition to the prerequisites for installing the AzureInformationProtection module, there are additional prerequisites for when you use the labeling cmdlets for Azure Information Protection:

1. The Azure Rights Management service must be activated.
2. To remove protection from files for others using your own account:
  - The super user feature must be enabled for your organization and your account must be configured to be a super user for Azure Rights Management.

### **Prerequisite 1: The Azure Rights Management service must be activated**

If your Azure Information Protection tenant is not activated, see the instructions for [Activating the protection service from Azure Information Protection](#).

### **Prerequisite 2: To remove protection from files for others using your own account**

Typical scenarios for removing protection from files for others include data discovery or data recovery. If you are using labels to apply the protection, you could remove the protection by setting a new label that doesn't apply protection or by removing the label.

You must have a Rights Management usage right to remove protection from files, or be a super user. For data discovery or data recovery, the super user feature is typically used. To enable this feature and configure your account to be a super user, see [Configuring super users for Azure Information Protection and discovery services or data recovery](#).

## **How to label files non-interactively for Azure Information Protection**

You can run the labeling cmdlets non-interactively by using the [Set-AIPAuthentication](#) cmdlet.

By default, when you run the cmdlets for labeling, the commands run in your own user context in an interactive PowerShell session. To run them unattended, use a Windows account that can sign in interactively, and use an account in Azure AD that will be used for delegated access. For ease of administration, use a single account that's synchronized from Active Directory to Azure AD.

You also need to request an access token from Azure AD, which sets and stores credentials for the delegated user to authenticate to Azure Information Protection.

The computer running the AIPAuthentication cmdlet downloads the label policies with labels that are assigned to the delegated user account by using your labeling management center, such as the Office 365 Security & Compliance Center.

## **NOTE**

If you use label policies for different users, you might need to create a new label policy that publishes all your labels, and publish the policy to just this delegated user account.

When the token in Azure AD expires, you must run the cmdlet again to acquire a new token. You can configure the access token in Azure AD for one year, two years, or to never expire. The parameters for Set-AIPAuthentication use values from an app registration process in Azure AD, as described in the next section.

For the delegated user account:

- Make sure that you have a label policy assigned to this account and that the policy contains the published labels you want to use.
- If this account needs to decrypt content, for example, to reprotect files and inspect files that others have protected, make it a [super user](#) for Azure Information Protection and make sure the super user feature is enabled.
- If you have implemented [onboarding controls](#) for a phased deployment, make sure that this account is included in your onboarding controls you've configured.

## To create and configure the Azure AD applications for Set-AIPAuthentication

### IMPORTANT

These instructions are for the current general availability version of the unified labeling client and also apply to the general availability version of the scanner for this client.

Set-AIPAuthentication requires an app registration for the *AppId* and *AppSecret* parameters. If you upgraded from a previous version of the client and created an app registration for the previous *WebAppId* and *NativeAppId* parameters, they won't work with the unified labeling client. You must create a new app registration as follows:

1. In a new browser window, sign in to the [Azure portal](#).
  2. For the Azure AD tenant that you use with Azure Information Protection, navigate to **Azure Active Directory > Manage > App registrations**.
  3. Select **+ New registration**. On the **Register an application** pane, specify the following values, and then click **Register**:
    - **Name:** `AIP-DelegatedUser`  
If you prefer, specify a different name. It must be unique per tenant.
    - **Supported account types:** Accounts in this organizational directory only
    - **Redirect URI (optional):** Web and `https://localhost`
  4. On the **AIP-DelegatedUser** pane, copy the value for the **Application (client) ID**. The value looks similar to the following example: `77c3c1c3-abf9-404e-8b2b-4652836c8c66`. This value is used for the *AppId* parameter when you run the Set-AIPAuthentication cmdlet. Paste and save the value for later reference.
  5. From the sidebar, select **Manage > Certificates & secrets**.
  6. On the **AIP-DelegatedUser - Certificates & secrets** pane, in the **Client secrets** section, select **+ New client secret**.
  7. For **Add a client secret**, specify the following, and then select **Add**:
    - **Description:** `Azure Information Protection unified labeling client`
    - **Expires:** Specify your choice of duration (1 year, 2 years, or never expires)
  8. Back on the **AIP-DelegatedUser - Certificates & secrets** pane, in the **Client secrets** section, copy the string for the **VALUE**. This string looks similar to the following example: `0Ak+rnYc/u+]ah2kNxVbtrDGbS47L4`. To make sure you copy all the characters, select the icon to **Copy to clipboard**.
- It's important that you save this string because it is not displayed again and it cannot be retrieved. As with any sensitive information that you use, store the saved value securely and restrict access to it.
9. From the sidebar, select **Manage > API permissions**.

10. On the **AIP-DelegatedUser - API permissions** pane, select **+ Add a permission**.
11. On the **Request API permissions** pane, make sure that you're on the **Microsoft APIs** tab, and select **Azure Rights Management Services**. When you're prompted for the type of permissions that your application requires, select **Application permissions**.
12. For **Select permissions**, expand **Content** and select the following:
  - **Content.DelegatedReader**
  - **Content.DelegatedWriter**
13. Select **Add permissions**.
14. Back on the **AIP-DelegatedUser - API permissions** pane, select **+ Add a permission** again.
15. On the **Request AIP permissions** pane, select **APIs my organization uses**, and search for **Microsoft Information Protection Sync Service**.
16. On the **Request API permissions** pane, select **Application permissions**.
17. For **Select permissions**, expand **UnifiedPolicy** and select the following:
  - **UnifiedPolicy.Tenant.Read**
18. Select **Add permissions**.
19. Back on the **AIP-DelegatedUser - API permissions** pane, select **Grant admin consent for <your tenant name>** and select **Yes** for the confirmation prompt.

Your API permissions should look like the following:

API permissions				
API / Permissions name	Type	Description	Admin Consent Required	Status
<b>✓ Azure Rights Management Services (2)</b>				
<b>Content.DelegatedReader</b>	Application	Read protected content on behalf of a user	Yes	Granted ...
<b>Content.DelegatedWriter</b>	Application	Create protected content on behalf of a user	Yes	Granted ...
<b>✓ Microsoft Graph (1)</b>				
<b>User.Read</b>	Delegated	Sign in and read user profile	-	Granted ...
<b>✓ Microsoft Information Protection Sync Service (1)</b>				
<b>UnifiedPolicy.Tenant.Read</b>	Application	Read all unified policies of the tenant.	Yes	Granted ...

These are the permissions that this application requests statically. You may also request user consentable permissions dynamically through code. [See best practices for requesting permissions](#)

Now you've completed the registration of this app with a secret, you're ready to run [Set-AIPAuthentication](#) with the parameters *AppId*, and *AppSecret*. Additionally, you'll need your tenant ID.

#### TIP

You can quickly copy your tenant ID by using Azure portal: **Azure Active Directory > Manage > Properties > Directory ID**.

1. Open Windows PowerShell with the **Run as administrator** option.
2. In your PowerShell session, create a variable to store the credentials of the Windows user account that will run non-interactively. For example, if you created a service account for the scanner:

```
$pscreds = Get-Credential "CONTOSO\srvc-scanner"
```

You're prompted for this account's password.

- Run the Set-AIPAuthentication cmdlet, with the *OnBehalfOf* parameter, specifying as its value the variable that you just created. Also specify your app registration values, your tenant ID, and the name of the delegated user account in Azure AD. For example:

```
Set-AIPAuthentication -AppId "77c3c1c3-abf9-404e-8b2b-4652836c8c66" -AppSecret
"0Akk+rnuYc/u+]ah2kNxVbtrDGbS47L4" -TenantId "9c11c87a-ac8b-46a3-8d5c-f4d0b72ee29a" -DelegatedUser
scanner@contoso.com -OnBehalfOf $pscreds
```

#### NOTE

If the computer cannot have internet access, there's no need to create the app in Azure AD and run Set-AIPAuthentication. Instead, follow the instructions for [disconnected computers](#).

## Next steps

For cmdlet help when you are in a PowerShell session, type `Get-Help <cmdlet name> -online`. For example:

```
Get-Help Set-AIPFileLabel -online
```

See the following for additional information that you might need to support the Azure Information Protection client:

- [Customizations](#)
- [Client files and usage logging](#)
- [File types supported](#)

# Azure Information Protection unified labeling user guide

7/20/2020 • 2 minutes to read • [Edit Online](#)

*Applies to:* [Azure Information Protection](#), Windows 10, Windows 8.1, Windows 8

*\*Customers with extended Microsoft support for Windows 7 and Office 2010 can also get Azure Information Protection support for these versions. Check with your support contact for full details.*

*Instructions for:* [Azure Information Protection unified labeling client for Windows](#)

The Azure Information Protection unified labeling client for Windows helps you keep important documents and emails safe from people who shouldn't see them, even if your email is forwarded or your document is saved to another location. You can also use this client to open documents that other people have protected by using the Rights Management protection technology from Azure Information Protection.

All you need is a computer that runs at least Windows 8. Then download and install this free client from Microsoft.

## What do you want to do?

- [Download and install the Azure Information Protection unified labeling client](#)
- [Classify a file or email](#)
- [Classify and protect a file or email](#)
- [Open files that have been protected](#)
- [Remove labels and protection from files and emails](#)

### NOTE

If you are an administrator who is responsible for the Azure Information Protection unified labeling client on an enterprise network, see the [Azure Information Protection unified labeling client administrator guide](#) for additional technical information.

# User Guide: Download and install the Azure Information Protection unified labeling client

7/20/2020 • 2 minutes to read • [Edit Online](#)

*Applies to:* [Azure Information Protection](#), Windows 10, Windows 8.1, Windows 8

*Instructions for:* [Azure Information Protection unified labeling client for Windows](#)

If your administrator does not install the Azure Information Protection unified labeling client for you, you can do this yourself. You must be a local administrator for your PC to install this client so that it can label and protect your documents and emails.

In addition:

- The Azure Information Protection unified labeling client requires a minimum version of Microsoft .NET Framework 4.6.2 and if this is missing, the installer tries to download and install this prerequisite. When this prerequisite is installed as part of the client installation, your computer must be restarted.

## To download and install the Azure Information Protection unified labeling client

Before you install the Azure Information Protection unified labeling client, confirm with your administrator or help desk that you are using [sensitivity labels](#) to classify and protect documents and emails.

1. Download **AzInfoProtection\_UL.exe** from the [Microsoft Download Center](#).
2. Run the executable file that was downloaded, and if you are prompted to continue, click **Yes**.
3. On the **Install the Azure Information Protection client** page, click **I agree** when you have read the license terms and conditions.
4. If you are prompted to continue, click **Yes**, and wait for the installation to finish.
5. Click **Close**. Before you start to use the Azure Information Protection unified labeling client:
  - If your computer runs Office 2010, restart your computer and then go to the next section for your final step.
  - For other versions of Office, restart all Office applications and all instances of File Explorer. Your installation is now complete and you can use the client to label and protect your documents and emails.

### **Installing the Azure Information Protection unified labeling client with Office 2010**

After you have installed the Azure Information Protection unified labeling client by using the previous instructions:

1. Open Microsoft Word. When this is the first time that you have run an Office 2010 application after you have installed the Azure Information Protection client, you see a **Microsoft Azure Information Protection** dialog box. This dialog box tells you that administrator credentials are required to complete the sign in process.
2. In the **Microsoft Azure Information Protection** dialog box, click **OK**.
3. If you see a **User Access Control** dialog box, click **Yes** so that the Azure Information Protection client can

update the registry.

Your installation is now complete and you can use the Azure Information Protection unified labeling client to label and protect your documents and emails.

## Other instructions

More how-to instructions from the Azure Information Protection unified labeling client user guide:

- [What do you want to do?](#)

## Additional information for administrators

See [Install the Azure Information Protection unified labeling client for users](#) from the [admin guide](#).

# User Guide: Classify a file or email by using the Azure Information Protection unified labeling client for Windows

7/20/2020 • 4 minutes to read • [Edit Online](#)

Applies to: [Azure Information Protection](#), Windows 10, Windows 8.1, Windows 8

\*Customers with extended Microsoft support for Windows 7 and Office 2010 can also get Azure Information Protection support for these versions. Check with your support contact for full details.

Instructions for: [Azure Information Protection unified labeling client for Windows](#)

## NOTE

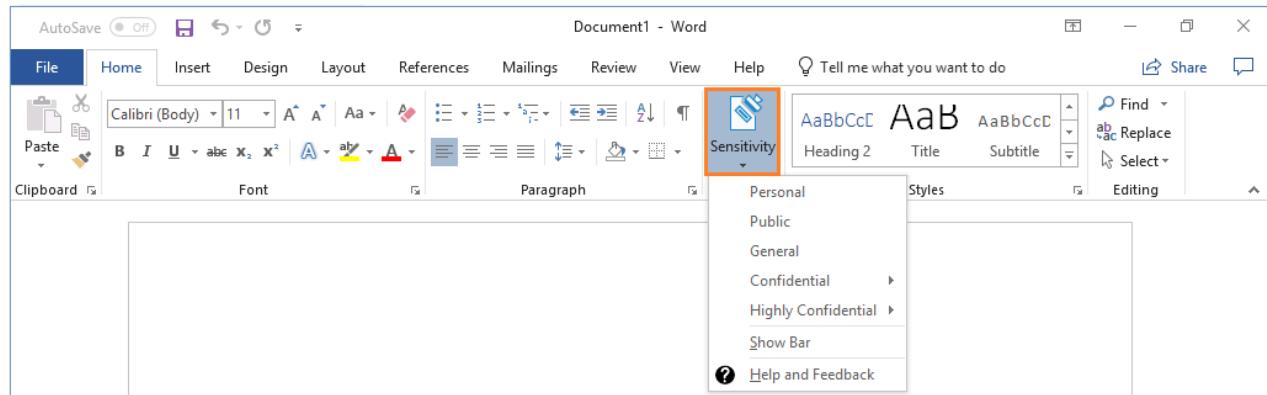
Use these instructions to help you classify (but not protect) your documents and emails. If you need to also protect your documents and emails, see the [classify and protect instructions](#). If you are not sure which set of instructions to use, check with your administrator or help desk.

The easiest way to classify your documents and emails is when you are creating or editing them from within your Office desktop apps: [Word](#), [Excel](#), [PowerPoint](#), [Outlook](#).

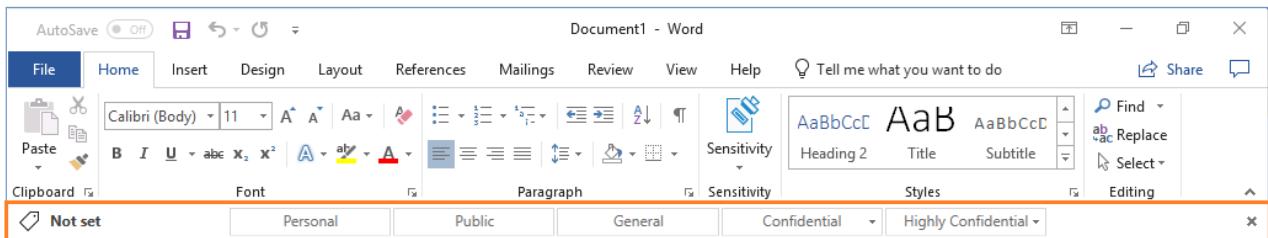
However, you can also classify files by using [File Explorer](#). This method supports additional file types and is a convenient way to classify multiple files at once.

## Using Office apps to classify your documents and emails

From the Home tab, select the **Sensitivity** button on the ribbon, and then select one of the labels that has been configured for you. For example:



Or, if you have selected **Show Bar** from the **Sensitivity** button, you can select a label from the Azure Information Protection bar. For example:



To set a label, such as "General", select **General**. If you're not sure which label to apply to the current document or email, use the label tooltips to learn more about each label and when to apply it.

If a label is already applied to the document and you want to change it, you can select a different label. If you have displayed the Azure Information Protection bar, and the labels are not displayed on the bar for you to select, first click the **Edit Label** icon, next to the current label value.

In addition to manually selecting labels, labels can also be applied in the following ways:

- Your administrator configured a default label, which you can keep or change.
- Your administrator configured labels to be set automatically when sensitive information is detected.
- Your administrator configured recommended labels when sensitive information is detected, and you are prompted to accept the recommendation (and the label is applied), or reject it (the recommended label is not applied).

### Exceptions for the Sensitivity button

Don't see the Sensitivity button in your Office apps?

- You might not have the Azure Information Protection unified labeling client [installed](#).
- If you don't see a **Sensitivity** button on the ribbon, but do see a **Protect** button with labels instead, you have the Azure Information Protection client (classic) installed and not the Azure Information Protection unified labeling client. [More information](#)

Is the label that you expect to see not displayed?

- If your administrator has recently configured a new label for you, try closing all instances of your Office app and reopening it. This action checks for changes to your labels.
- The label might be in a scoped policy that doesn't include your account. Check with your help desk or administrator.

## Using File Explorer to classify files

When you use File Explorer, you can quickly classify a single file, multiple files, or a folder.

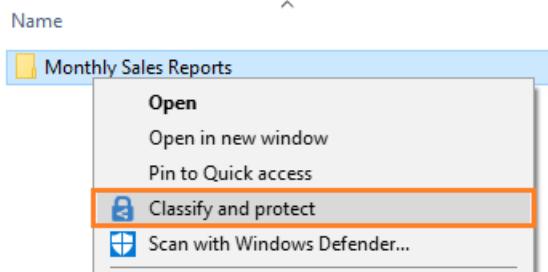
When you select a folder, all the files in that folder and any subfolders it has are automatically selected for the classification that you set. However, new files that you create in that folder or subfolders are not automatically classified.

When you use File Explorer to classify your files, if one or more of the labels appear dimmed, the files that you selected do not support classification without also protecting them.

The admin guide contains a full list of the file types that support classification without protection: [File types supported for classification only](#).

### To classify a file by using File Explorer

1. In File Explorer, select your file, multiple files, or a folder. Right-click, and select **Classify and protect**. For example:



2. In the **Classify and protect - Azure Information Protection** dialog box, use the labels as you would do in an Office application, which sets the classification as defined by your administrator.

If none of the labels can be selected (they appear dimmed): The selected file does not support classification. For example:



3. If you selected a file that does not support classification, click **Close**. You cannot classify this file without also protecting it.

If you selected a label, click **Apply** and wait for the **Work finished** message to see the results. Then click **Close**.

If you change your mind about the label you chose, simply repeat this process and choose a different label.

The classification that you specified stays with the file, even if you email the file or save it to another location.

## Other instructions

More how-to instructions from the user guide for the Azure Information Protection unified labeling client for Windows:

- [What do you want to do?](#)

## Additional information for administrators

See [Learn about sensitivity labels](#).

# User Guide: Classify and protect with the Azure Information Protection unified labeling client

7/20/2020 • 8 minutes to read • [Edit Online](#)

Applies to: [Azure Information Protection](#), Windows 10, Windows 8.1, Windows 8

\*Customers with extended Microsoft support for Windows 7 and Office 2010 can also get Azure Information Protection support for these versions. Check with your support contact for full details.

Instructions for: [Azure Information Protection unified labeling client for Windows](#)

## NOTE

Use these instructions to help you classify and protect your documents and emails. If you need to only classify and not protect your documents and emails, see the [classify-only instructions](#). If you are not sure which set of instructions to use, check with your administrator or help desk.

The easiest way to classify and protect your documents and emails is when you are creating or editing them from within your Office desktop apps: [Word](#), [Excel](#), [PowerPoint](#), [Outlook](#).

However, you can also classify and protect files by using [File Explorer](#). This method supports additional file types and is a convenient way to classify and protect multiple files at once. This method supports protecting Office documents, PDF files, text and image files, and a wide range of other files.

If your label applies protection to a document, the protected document might not be suitable to be saved on SharePoint or OneDrive. Check whether your administrator has [enabled sensitivity labels for Office files in SharePoint and OneDrive](#).

## Safely share a file with people outside your organization

Files that are protected are safe to share with others. For example, you attach a protected document to an email.

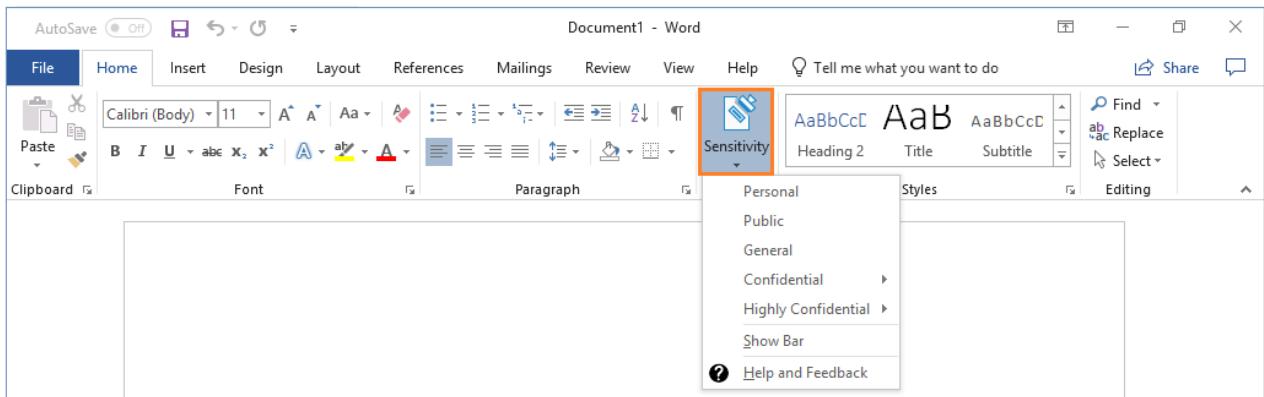
Before you share files with people outside your organization, check with your help desk or administrator how to protect files for external users.

For example, if your organization regularly communicates with people in another organization, your administrator might have configured labels that sets protection such that these people can read and use protected documents. Then, select these labels to classify and protect the documents to share.

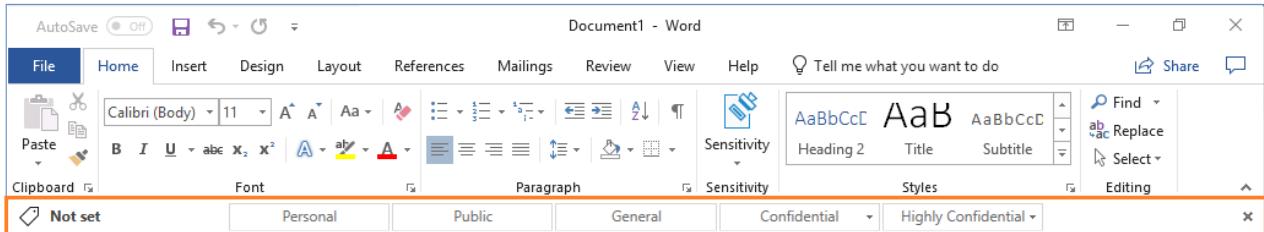
Alternatively, if the external users have [business-to-business \(B2B\) accounts](#) created for them, you can use [File Explorer to set custom permissions](#) for a document before you share it. If you set your own custom permissions and the document is already protected for internal use, first make a copy of it to retain the original permissions. Then use the copy to set the custom permissions.

## Using Office apps to classify and protect your documents and emails

From the **Home** tab, select the **Sensitivity** button on the ribbon, and then select one of the labels that has been configured for you. For example:



Or, if you have selected **Show Bar** from the **Sensitivity** button, you can select a label from the Azure Information Protection bar. For example:



To set a label, such as "**Confidential \ All Employees**", select **Confidential** and then **All Employees**. If you're not sure which label to apply to the current document or email, use the label tooltips to learn more about each label and when to apply it.

If a label is already applied to the document and you want to change it, you can select a different label. If you have displayed the Azure Information Protection bar, and the labels are not displayed on the bar for you to select, first click the **Edit Label** icon, next to the current label value.

In addition to manually selecting labels, labels can also be applied in the following ways:

- Your administrator configured a default label, which you can keep or change.
- Your administrator configured labels to be set automatically when sensitive information is detected.
- Your administrator configured recommended labels when sensitive information is detected, and you are prompted to accept the recommendation (and the label is applied), or reject it (the recommended label is not applied).

### Exceptions for the Sensitivity button

Don't see the **Sensitivity** button in your Office apps?

- You might not have the Azure Information Protection unified labeling client [installed](#).
- If you don't see a **Sensitivity** button on the ribbon, but do see a **Protect** button with labels instead, you have the Azure Information Protection client (classic) installed and not the Azure Information Protection unified labeling client. [More information](#)

Is the label that you expect to see not displayed?

Possible reasons:

- If your administrator has recently configured a new label for you, try closing all instances of your Office app and reopening it. This action checks for changes to your labels.
- If the missing label applies protection, you might have an edition of Office that does not support applying Rights Management protection. To verify, click **Sensitivity** > **Help and Feedback**. In the dialog box, check if you have a message in the **Client status** section that says **This client is not licensed for Office Professional Plus**.

You do not need Office Professional Plus if you have Office apps from Office 365 Business or Microsoft 365 Business when the user is assigned a license for Azure Rights Management (also known as Azure Information Protection for Office 365).

- The label might be in a scoped policy that doesn't include your account. Check with your help desk or administrator.

### Safely sharing by email

When you share Office documents by email, you can attach the document to an email that you protect, and the document is automatically protected with the same restrictions that apply to the email.

However, you might want to protect the document first, and then attach it to the email. Protect the email as well if the email message contains sensitive information. A benefit of protecting the document before you attach it to an email is that you can apply different permissions to the document than to the email message.

## Using File Explorer to classify and protect files

When you use File Explorer, you can quickly classify and protect a single file, multiple files, or a folder.

When you select a folder, all the files in that folder and any subfolders it has are automatically selected for the classification and protection options that you set. However, new files that you create in that folder or subfolders are not automatically configured with those options.

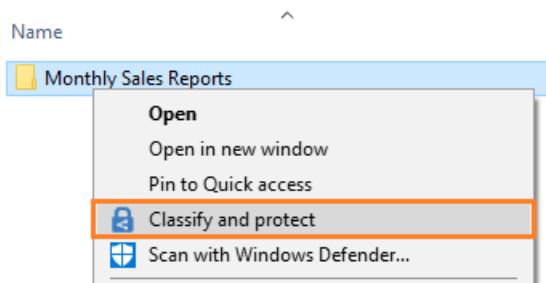
When you use File Explorer to classify and protect your files, if one or more of the labels appear dimmed, the files that you selected do not support classification. For these files, you can select a label only if your administrator has configured the label to apply protection. Or, you can specify your own protection settings.

Some files are automatically excluded from classification and protection, because changing them might stop your PC from running. Although you can select these files, they are skipped as an excluded folder or file. Examples include executable files and your Windows folder.

The admin guide contains a full list of the file types supported and the files and folders that are automatically excluded: [File types supported by the Azure Information Protection unified labeling client](#).

### To classify and protect a file by using File Explorer

1. In File Explorer, select your file, multiple files, or a folder. Right-click, and select **Classify and protect**. For example:



2. In the **Classify and protect - Azure Information Protection** dialog box, use the labels as you would do in an Office application, which sets the classification and protection as defined by your administrator.

- If none of the labels can be selected (they appear dimmed): The selected file does not support classification but you can protect it with custom permissions (step 3). For example:



3. You can specify your own protection settings rather than use the protection settings that your administrator might have included with your selected label. To do this, select **Protect with custom permissions**.

Any custom permissions that you specify replace rather than supplement protection settings that your administrator might have defined for your chosen label.

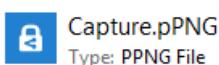
4. If you selected the custom permissions option, now specify the following:

- **Select permissions:** Select the level of access that you want people to have when you protect the selected file or files.
- **Select users, groups, or organizations:** Specify the people who should have the permissions you selected for your file or files. Type their full email address, a group email address, or a domain name from the organization for all users in that organization.  
Alternatively, you can use the address book icon to select users or groups from the Outlook address book.
- **Expire access:** Select this option only for time-sensitive files so that the people you specified can't open your selected file or files after a date that you set. You will still be able to open the original file but after midnight (your current time zone), on the day that you set, the people that you specified will not be able to open the file.

Note that if this setting was previously configured by using custom permissions from an Office 2010 app, the specified expiry date does not display in this dialog box but the expiry date is still set. This is a display issue only for when the expiry date was configured in Office 2010.

5. Click **Apply** and wait for the **Work finished** message to see the results. Then click **Close**.

The selected file or files are now classified and protected, according to your selections. In some cases (when adding protection changes the file name extension), the original file in File Explorer is replaced with a new file that has the Azure Information Protection lock icon. For example:



If you change your mind about the classification and protection, or later need to modify your settings, simply repeat this process with your new settings.

The classification and protection that you specified stays with the file, even if you email the file or save it to another location.

## Other instructions

More how-to instructions from the user guide for Azure Information Protection unified labeling client:

- [What do you want to do?](#)

## Additional information for administrators

See [Learn about sensitivity labels](#).

# User Guide: View protected files with the Azure Information Protection unified labeling client

7/20/2020 • 4 minutes to read • [Edit Online](#)

Applies to: [Azure Information Protection](#), Windows 10, Windows 8.1, Windows 8

\*Customers with extended Microsoft support for Windows 7 and Office 2010 can also get Azure Information Protection support for these versions. Check with your support contact for full details.

Instructions for: [Azure Information Protection unified labeling client for Windows](#)

You can often view a protected file by simply opening it. For example, you might double-click an attachment in an email message or double-click a file from File Explorer, or you might click a link to a file.

If the files don't immediately open, the **Azure Information Protection viewer** might be able to open it. This viewer can open protected text files, protected image files, protected PDF files, and all files that have a .pfile file name extension.

The viewer automatically installs as part of the Azure Information Protection unified labeling client, or you can install it separately. You can install both this client and the viewer from the [Microsoft Azure Information Protection](#) page on the Microsoft website. For more information about installing this client, see [Download and install the Azure Information Protection unified labeling client](#).

## NOTE

Although installing the client provides more functionality, it requires local administrator permissions and the full functionality requires a corresponding service for your organization. For example, Azure Information Protection.

Install the viewer if you have been sent a protected document by somebody from another organization or if you do not have local administrator permissions to your PC.

To be able to open a protected document, the application must be "RMS-enlightened". Office apps and the Azure Information Protection viewer are examples of RMS-enlightened applications. To see a list of applications by type and supported devices, see the [RMS-enlightened applications](#) table.

## Message.rpmmsg as an email attachment

If you see **message.rpmmsg** as a file attachment in an email, this file is not a protected document but a protected email message that displays as an attachment. You can't use the Azure Information Protection viewer for Windows to view this protected email message on your Windows PC. Instead, you need an email application for Windows that supports Rights Management protection, such as Office Outlook. Or you can use Outlook on the web.

However, if you have an iOS or Android device, you can use the Azure Information Protection app to open these protected email messages. You can download this app for these mobile devices from the [Microsoft Azure Information Protection](#) page on the Microsoft website.

## Prompts for authentication

Before you can view the protected file, the Rights Management service that was used to protect the file must first confirm that you are authorized to view the file. The service does this confirmation by checking your user name and password. In some cases, these credentials might be cached and you do not see a prompt that asks you to sign

in. In other cases, you are prompted to supply your credentials.

If your organization does not have a cloud-based account for you to use (for Office 365 or Azure) and does not use an equivalent on-premises version (AD RMS), you have two options:

- If you were sent a protected email, follow the instructions to sign in with your social identity provider (such as Google for a Gmail account) or apply for a one-time passcode.
- You can apply for a free account that will accept your credentials so that you can open documents that are protected by Rights Management. To apply for this account, click the link to apply for [RMS for individuals](#) and use your company email address rather than a personal email address.

## To view a protected file

1. Open the protected file (for example, by double-clicking the file or attachment, or by clicking the link to the file). If you are prompted to select an app, select **Azure Information Protection Viewer**.
2. If you see a page to **Sign in** or **Sign up**: Click **Sign in** and enter your credentials. If the protected file was sent to you as an attachment, be sure to specify the same email address that was used to send you the file.  
If you do not have an account that is accepted, see the [Prompts for authentication](#) section on this page.
3. A read-only version of the file opens in the **Azure Information Protection Viewer** or in the application associated with the file name extension.
4. If you have additional protected files to open, you can browse directly to them from the viewer, by using the **Open** option. Your selected file replaces the original file in the viewer.

### TIP

If the protected file does not open and you have the full Azure Information Protection client installed, try the **Reset Settings** option. To access this option, from an Office app, select the **Sensitivity** button > **Help and Feedback** > **Reset Settings**.

[More information about the Reset Settings option](#)

## Other instructions

More how-to instructions from the Azure Information Protection user guide:

- [What do you want to do?](#)

# User Guide: Remove labels and protection from files and emails that have been labeled by Azure Information Protection

7/20/2020 • 2 minutes to read • [Edit Online](#)

Applies to: [Azure Information Protection](#), Windows 10, Windows 8.1, Windows 8

\*Customers with extended Microsoft support for Windows 7 and Office 2010 can also get Azure Information Protection support for these versions. Check with your support contact for full details.

Instructions for: [Azure Information Protection unified labeling client for Windows](#)

When the Azure Information Protection unified client is [installed on your computer](#), you can remove sensitivity labels and protection from files and emails.

When the sensitivity label that you remove is configured to apply protection, this action also removes protection from the file. You might be prompted to record why you are removing the label.

## IMPORTANT

You must be the owner of the file to remove protection, or been granted permissions to remove protection (the Rights Management permission of Export or Full Control).

If you want to choose a different label or a different set of protection settings, you do not need to remove the label or protection. Instead, choose a new label and if necessary, you can define custom permissions by using File Explorer.

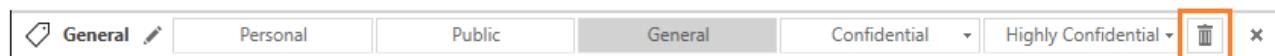
You can remove labels and protection from Office documents and emails when you are creating or editing them from within your Office desktop apps: **Word**, **Excel**, **PowerPoint**, **Outlook**.

You can also remove labels and protection by using **File Explorer**, which supports additional file types and is a convenient way to remove labels and protection from multiple files at once.

## Using Office apps to remove labels and protection from documents and emails

From the **Home** tab, select the **Sensitivity** button on the ribbon, and clear the currently selected label.

Or, if you have selected **Show Bar** from the **Sensitivity** button, you can select the **Delete Label** icon from the Azure Information Protection bar:



If the **Delete Label** icon is not immediately available, first select the **Edit Label** icon:



If you still do not see the **Delete Label** icon, your administrator does not allow you to use this option because all documents and email must have a label.

## Using File Explorer to remove labels and protection from files

When you use File Explorer, you can quickly remove labels and protection from a single file, multiple files, or a folder. When you select a folder, all the files in that folder and any subfolders it has are automatically selected.

1. In File Explorer, select your file, multiple files, or a folder. Right-click, and select **Classify and protect**.
2. To remove a label: In the **Classify and protect - Azure Information Protection** dialog box, click **Delete Label**. If the label was configured to apply protection, that protection is automatically removed.
3. To remove custom protection from a single file: In the **Classify and protect - Azure Information Protection** dialog box, clear the **Protect with custom permissions** option.
4. To remove custom protection from multiple files: In the **Classify and protect - Azure Information Protection** dialog box, click **Remove custom permissions**.
5. Click **Apply** and wait for the **Work finished** message to see the results. Then click **Close**.

## Other instructions

More how-to instructions from the Azure Information Protection user guide:

- [What do you want to do?](#)

## Additional information for administrators

See [Learn about sensitivity labels](#).

# Azure Information Protection client for Windows

7/20/2020 • 2 minutes to read • [Edit Online](#)

*Applies to:* Active Directory Rights Management Services, [Azure Information Protection](#), Windows 10, Windows 8.1, Windows 8, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012\*

*Instructions for:* [Azure Information Protection client for Windows](#)

## NOTE

To provide a unified and streamlined customer experience, **Azure Information Protection client (classic)** and **Label Management** in the Azure Portal are being **deprecated** as of **March 31, 2021**. This time-frame allows all current Azure Information Protection customers to transition to our unified labeling solution using the Microsoft Information Protection Unified Labeling platform. Learn more in the official [deprecation notice](#).

The Azure Information Protection client (classic) is the original downloadable client for organizations that use [Azure Information Protection](#) to classify and protect documents and emails, or use a Rights Management service to protect their data. This client also has a viewer for organizations that don't have their own information protection infrastructure but want to consume content that has been protected by other organizations that use a Rights Management service from Microsoft.

## NOTE

This client, also known as the classic client, is being replaced by the Azure Information Protection unified labeling client. If you're not sure which client to use, see [Choose which labeling client to use for Windows computers](#).

Use the following resources for the classic client:

- [Azure Information Protection client: Version release history](#)
- [Azure Information Protection client administrator guide](#)
- [Azure Information Protection user guide](#)

## TIP

There's also an Azure Information Protection app for iOS and Android. For more information, see [FAQs for Azure Information Protection app for iOS and Android](#)

For Mac computers: Use the RMS sharing app and read the [FAQ for Rights Management Sharing Application for Mobile and Mac Platforms](#).

## Install instructions

- [Administrators](#)
- [End users](#)

# Azure Information Protection client: Version release history and support policy

7/20/2020 • 3 minutes to read • [Edit Online](#)

*Applies to: Active Directory Rights Management Services, Azure Information Protection, Windows 10, Windows 8.1, Windows 8, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012*

*Instructions for: Azure Information Protection client for Windows*

## NOTE

To provide a unified and streamlined customer experience, **Azure Information Protection client (classic)** and **Label Management** in the Azure Portal are being **deprecated** as of March 31, 2021. This time-frame allows all current Azure Information Protection customers to transition to our unified labeling solution using the Microsoft Information Protection Unified Labeling platform. Learn more in the official [deprecation notice](#).

You can download the latest general availability release version and the current preview version (if available) from the [Microsoft Download Center](#).

After a short delay of typically a couple of weeks, the latest general availability version is also included in the Microsoft Update Catalog with a product name of **Microsoft Azure Information Protection > Microsoft Azure Information Protection Client**, and the classification of **Updates**. This inclusion in the catalog means that you can upgrade the client by using WSUS or Configuration Manager, or other software deployment mechanisms that use Microsoft Update.

For more information, see [Upgrading and maintaining the Azure Information Protection client](#).

## TIP

Interested in using the Azure Information Protection unified labeling client because your labels are published from the Office 365 Security & Compliance Center, Microsoft 365 security center, or Microsoft 365 compliance center? When you download and then install the unified labeling client from the Microsoft Download Center, you can upgrade your Azure Information Protection client to the [unified labeling client](#).

## Servicing information and timelines

Each general availability (GA) version of the Azure Information Protection client is supported for up to six months after the release of the subsequent GA version. With the exception of this section, the documentation does not include information about unsupported versions of the client. Fixes and new functionality are always applied to the latest GA version and will not be applied to older GA versions.

Preview versions should not be deployed for end users on production networks. Instead, use the latest preview version to see and try new functionality or fixes that are coming in the next GA version. Preview versions that are not current are not supported.

General availability versions that are no longer supported:

CLIENT VERSION	DATE RELEASED
1.53.10	07/15/2019
1.48.204.0	04/16/2019
1.41.51.0	11/27/2018
1.37.19.0	09/17/2018
1.29.5.0	06/26/2018
1.27.48.0	05/30/2018
1.26.6.0	04/17/2018
1.10.56.0	09/18/2017
1.7.210.0	06/06/2017
1.4.21.0	03/15/2017
1.3.155.2	02/08/2017
1.2.4.0.0	10/27/2016
1.1.23.0	10/01/2016

The date format used on this page is *month/day/year*.

Starting 6/2/2019, the labeling service for Azure Information Protection requires connections that use TLS 1.2.

All client versions from 1.4.21.0 released 03/15/2017 support TLS 1.2. Client versions 1.3.155.2, 1.2.4.0, and 1.1.23.0 do not use TLS 1.2 and therefore can no longer download the Azure Information Protection policy.

## Release history

Use the following information to see what's new or changed for a supported release of the Azure Information Protection client for Windows. The most current release is listed first.

### NOTE

Minor fixes are not listed so if you experience a problem with the Azure Information Protection client, we recommend that you check whether it is fixed with the latest GA release. If the problem remains, check the current preview version (if available).

For technical support, see the [Support options and community resources](#) information. We also invite you to engage with the Azure Information Protection team, on their [Yammer site](#).

## Version 1.54.59.0

**Released:** 12/02/2020

This version includes fixes only.

**Fixes:**

- Issue where files protected by IQP displayed **recover** and/or **save as** options after protection was removed, are resolved.
- Numerous product feature tooltip texts were improved for clarity and ease of understanding.
- Issues surrounding client stability when working with protected PDF files is resolved.
- Protection labels are now removed as expected if the label is deleted on the email during the email creation process.

## Version 1.54.33.0

**Released:** 10/23/2019

Supported through 08/12/2020

This version includes the MSIPC version 1.0.4008.0813 of the RMS client.

This release has general fixes for stability and performance.

## Next steps

Not sure if this is the right client to install? See [Choose which labeling client to use for Windows computers](#).

For more information about installing and using the client:

- For users: [Download and install the client](#)
- For admins: [Azure Information Protection client administrator guide](#)

# Azure Information Protection client administrator guide

7/20/2020 • 13 minutes to read • [Edit Online](#)

*Applies to: Active Directory Rights Management Services, Azure Information Protection, Windows 10, Windows 8.1, Windows 8, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012*

*Instructions for: Azure Information Protection client for Windows*

## NOTE

To provide a unified and streamlined customer experience, **Azure Information Protection client (classic)** and **Label Management** in the Azure Portal are being **deprecated** as of **March 31, 2021**. This time-frame allows all current Azure Information Protection customers to transition to our unified labeling solution using the Microsoft Information Protection Unified Labeling platform. Learn more in the official [deprecation notice](#).

Use the information in this guide if you are responsible for the Azure Information Protection client on an enterprise network, or if you want more technical information than is in the [Azure Information Protection client user guide](#).

For example:

- Understand the different components of this client and whether you should install it
- How to install the client for users, with information about prerequisites, installation options and parameters, and verification checks
- How to accommodate custom configurations that often require editing the registry
- Locate the client files and usage logs
- Identify the file types supported by the client
- Configure and use the document tracking site for users
- Use the client with PowerShell for command-line control

Have a question that's not addressed by this documentation? Visit our [Azure Information Protection Yammer site](#).

## Technical overview of the Azure Information Protection client

The Azure Information Protection client includes the following:

- An Office add-in, that installs the Azure Information Protection bar for users to select classification labels, and a **Protect** button on the ribbon for additional options. For Outlook, a **Do Not Forward** button is also available for the ribbon.
- Windows File Explorer, right-click options for users to apply classification labels and protection to files.
- A viewer to display protected files when a native application cannot open it.

- A PowerShell module to apply and remove classification labels and protection from files.

This module includes [cmdlets to install and configure the Azure Information Protection scanner](#), which runs as a service on Windows Server. This service lets you discover, classify, and protect files on data stores such as network shares and SharePoint Server libraries.

- The Rights Management client that communicates with Azure Rights Management (Azure RMS) or Active Directory Rights Management Services (AD RMS).

The Azure Information Protection client is best suited to work with its Azure services; Azure Information Protection and its data protection service, Azure Rights Management. However, with some limitations, the Azure Information Protection client also works with the on-premises version of Rights Management, AD RMS. For a comprehensive comparison of features that are supported by Azure Information Protection and AD RMS, see [Comparing Azure Information Protection and AD RMS](#).

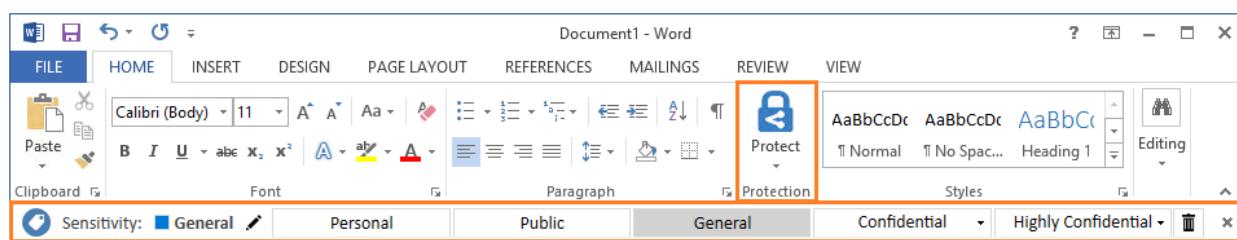
If you have AD RMS and want to migrate to Azure Information Protection, see [Migrating from AD RMS to Azure Information Protection](#).

## Should you deploy the Azure Information Protection client?

Deploy the Azure Information Protection client if you are not using [sensitivity labels in the Office 365 Security & Compliance Center](#) but instead, using Azure Information Protection labels that you download from Azure, and any of the following applies:

- You want to classify (and optionally, protect) documents and email messages by selecting labels from within your Office applications (Word, Excel, PowerPoint, Outlook).
- You want to classify (and optionally, protect) files by using File Explorer, supporting additional file types than those supported by Office, multi-select, and folders.
- You want to run scripts that classify (and optionally, protect) documents by using PowerShell commands.
- You want to run a service that discovers, classifies (and optionally, protects) files that are stored on-premises.
- You want to view protected documents when a native application to display the file is not installed or cannot open these documents.
- You want to just protect files by using File Explorer or by using PowerShell commands.
- You want users and administrators to be able to track and revoke protected documents.
- You want to remove encryption from files and containers (unprotect) in bulk for data recovery purposes.
- You run Office 2010 and want to protect documents and email messages by using the Azure Rights Management service.

Example showing the Azure Information Protection client add-in for an Office application, displaying the classification labels for your organization, and the new **Protect** button on the ribbon:



# Installing and supporting the Azure Information Protection client

You can install the Azure Information Protection client by using an executable or a Windows installer file. For more information about each choice, and instructions, see [Install the Azure Information Protection client for users](#).

Use the following sections for supporting information about installing the client.

## Installation checks and troubleshooting

When the client is installed, use the **Help and Feedback** option to open the **Microsoft Azure Information Protection** dialog box:

- From an Office application: On the **Home** tab, in the **Protection** group, select **Protect**, and then select **Help and Feedback**.
- From File Explorer: Right-select a file, files, or folder, select **Classify and protect**, and then select **Help and Feedback**.

### Help and Feedback section

The **Tell me more** link by default, goes to the [Azure Information Protection](#) website but you can configure it for a custom URL as one of the [policy settings](#) in the Azure Information Protection policy.

The **Report an Issue** link displays only if you specify an [advanced client setting](#). When you configure this setting, you specify an HTTP link such as the email address of your help desk.

The **Export Logs** automatically collects and attaches log files for the Azure Information Protection client if you have been asked to send these to Microsoft Support. This option can also be used by end users to send these log files to your help desk.

The **Reset Settings** signs out the user, deletes the currently downloaded Azure Information Protection policy, and resets the user settings for the Azure Rights Management service.

#### NOTE

If you have technical problems with the client, see [Support options and community resources](#).

#### More information about the Reset Settings option

- You do not have to be a local administrator to use this option and this action is not logged in the Event Viewer.
- Unless files are locked, this action deletes all the files in the following locations. These files include client certificates, Rights Management templates, the Azure Information Protection policy, and the cached user credentials. The client log files are not deleted.
  - %LocalAppData%\Microsoft\DRM
  - %LocalAppData%\Microsoft\MSIPC
  - %LocalAppData%\Microsoft\MSIP\Policy.msip
  - %LocalAppData%\Microsoft\MSIP\TokenCache
- The following registry keys and settings are deleted. If the settings for any of these registry keys have custom values, these must be reconfigured after you reset the client.

Typically for enterprise networks, these settings are configured by using group policy, in which case they are automatically reapplied when group policy is refreshed on the computer. However, there might be some settings that are configured one time with a script, or manually configured. In these cases, you must take additional steps to reconfigure these settings. As an example, computers might run a script one time

to configure settings for redirection to Azure Information Protection because you are migrating from AD RMS and still have a Service Connection Point on your network. After resetting the client, the computer must run this script again.

- HKEY\_CURRENT\_USER\SOFTWARE\Microsoft\Office\15.0\Common\Identity
  - HKEY\_CURRENT\_USER\SOFTWARE\Microsoft\Office\14.0\Common\DRM
  - HKEY\_CURRENT\_USER\SOFTWARE\Microsoft\Office\15.0\Common\DRM
  - HKEY\_CURRENT\_USER\SOFTWARE\Microsoft\Office\16.0\Common\DRM
  - HKEY\_CURRENT\_USER\SOFTWARE\Classes\Local Settings\Software\Microsoft\MSIPC
- The currently signed in user is signed out.

#### **Client status section**

Use the **Connected as** value to confirm that the displayed user name identifies the account to be used for Azure Information Protection authentication. This user name must match an account used for Office 365 or Azure Active Directory. The account must also belong to a tenant that is configured for Azure Information Protection.

If you need to sign in as a different user to the one displayed, see the [Sign in as a different user](#) customization.

The **Last connection** displays when the client last connected to your organization's Azure Information Protection service. You can use this information with the **Information Protection policy was installed on** date and time to confirm when the Azure Information Protection policy was last installed or updated. When the client connects to the service, it automatically downloads the latest policy if it finds changes from its current policy, and also every 24 hours. If you have made policy changes after the displayed time, close and reopen the Office application.

If you see **This client is not licensed for Office Professional Plus**: The Azure Information Protection client has detected that the installed edition of Office does not support applying Rights Management protection. When this detection is made, labels that apply protection do not display on the Azure Information Protection bar.

Use the **Version** information to confirm which version of the client is installed. You can check whether this is the latest release version and the corresponding fixes and new features by clicking the **What's New** link, to read the [Version release history](#) for the client.

## Support for multiple languages

The Azure Information Protection client supports the same languages that Office 365 supports. For a list of these languages, see the **Office 365, Exchange Online Protection, and Power BI** section from the [International availability](#) page from Office.

For these languages, menu options, dialog boxes, and messages from the Azure Information Protection client display in the user's language. There is a single installer that detects the language, so no additional configuration is required to install the Azure Information Protection client for different languages.

However, label names and descriptions that you specify are not automatically translated when you configure labels in the Azure Information Protection policy. Beginning with August 30, 2017, the current [default policy](#) includes support for some languages. For users to see labels in their preferred language, provide your own translations and configure the Azure Information Protection policy to use these translations. For more information, see [How to configure labels for different languages in Azure Information Protection](#). Visual markings are not translated and do not support more than one language.

## Post installation tasks

After you have installed the Azure Information Protection client, make sure that you give users instructions for

how to label their documents and emails, and guidance for which labels to choose for specific scenarios. For example:

- Online user instructions: [Azure Information Protection user guide](#)
- Download a customizable user guide: [Azure Information Protection End User Adoption Guide](#)

## Upgrading and maintaining the Azure Information Protection client

The Azure Information Protection team regularly updates the Azure Information Protection client for new functionality and fixes. Announcements are posted to the team's [Yammer site](#).

If you are using Windows Update, the Azure Information Protection client automatically upgrades the general availability version of the client, irrespective of how the client was installed. New client releases are published to the catalog a few weeks after the release.

Alternatively, you can manually upgrade the client by downloading the new release from the [Microsoft Download Center](#). Then install the new version to upgrade the client. You must use this method to upgrade preview versions.

When you manually upgrade, uninstall the previous version first only if you're changing the installation method. For example, you change from the executable (.exe) version of the client to the Windows installer (.msi) version of the client. Or, if you need to install a previous version of the client. For example, you have the current preview version installed for testing and now need to revert to the current general availability version.

Use the [Version release history and support policy](#) to understand the support policy for the Azure Information Protection client, which versions are currently supported, and what's new and changed for the supported releases.

### Upgrading the Azure Information Protection scanner

Use the following instructions to upgrade the scanner from a general availability version older than 1.48.204.0 to the current version of the scanner.

#### To upgrade the scanner to the current version

##### IMPORTANT

For a smooth upgrade path, do not install the the Azure Information Protection client on the computer running the scanner as your first step to upgrade the scanner. Instead, use the following upgrade instructions.

Beginning with version 1.48.204.0, the upgrade process from previous versions automatically changes the scanner to gets its configuration settings from the Azure portal. In addition, the schema is updated for the scanner's configuration database, and this database is also renamed from AzInfoProtection:

- If you do not specify your own profile name, the configuration database is renamed `AIPScanner_<computer_name>`.
- If you specify your own profile name, the configuration database is renamed `AIPScanner_<profile_name>`.

Although it's possible to upgrade the scanner in a different order, we recommend the following steps:

1. Use the Azure portal to create a new scanner profile that includes settings for the scanner and your data repositories with any settings that they need. For help with this step, see [Configure the scanner in the Azure portal](#) from the scanner deployment instructions.

If the computer running the scanner is disconnected from the internet, you still need to do this step. Then, from the Azure portal, use the **Export** option to export your scanner profile to a file.

2. On the scanner computer, stop the scanner service, **Azure Information Protection Scanner**.
3. Upgrade the Azure Information Protection client by installing the current general availability (GA) version from the [Microsoft Download Center](#).
4. In a PowerShell session, run the `Update-AIPScanner` command with the same profile name that you specified in step 1. For example: `Update-AIPScanner -Profile Europe`
5. Only if the scanner is running on a disconnected computer: Now run [Import-AIPScannerConfiguration](#) and specify the file that contains the exported settings.
6. Restart the Azure Information Protection Scanner service, **Azure Information Protection Scanner**.

You can now use the rest of the instructions in [Deploying the Azure Information Protection scanner to automatically classify and protect files](#), omitting the step to install the scanner. Because the scanner is already installed, there's no reason to install it again.

Upgrading in a different order to the recommended steps

If you don't configure the scanner in the Azure portal before you run the `Update-AIPScanner` command, you won't have a profile name to specify that identifies your scanner configuration settings for the upgrade process.

In this scenario, when you configure the scanner in the Azure portal, you must specify exactly the same profile name that was used when you ran the `Update-AIPScanner` command. If the name doesn't match, the scanner will not be configured for your settings.

**TIP**

To identify scanners that have this misconfiguration, use the **Azure Information Protection - Nodes** pane in the Azure portal.

For scanners that have internet connectivity, they display their computer name with the GA version number of the Azure Information Protection client, but no profile name. Only scanners that have a version number 1.41.51.0 should display no profile name on this pane.

If you didn't specify a profile name when you ran the `Update-AIPScanner` command, the computer name is used to automatically create the profile name for the scanner.

**Moving the scanner configuration database to a different SQL Server instance**

In the current GA version, there is a known issue if you try to move the scanner configuration database to a new SQL Server instance after you run the upgrade command.

If you know that you want move the scanner configuration database for the GA version, do the following:

1. Uninstall the scanner by using [Uninstall-AIPScanner](#).
2. If you haven't yet upgraded to the current GA version of the Azure Information Protection client, upgrade the client now.
3. Install the scanner by using [Install-AIPScanner](#), specifying the new SQL Server instance and profile name.
4. Optional: If you do not want the scanner to rescan all files, export the `ScannerFiles` table and import it to the new database.

## Uninstalling the Azure Information Protection client

You can use any of the following options to uninstall the client:

- Use Control Panel to uninstall a program: Click **Microsoft Azure Information Protection > Uninstall**
- Rerun the executable (for example, `AzInfoProtection.exe`), and from the **Modify Setup** page, click

## Uninstall.

- Run the executable with `/uninstall`. For example: `AzInfoProtection.exe /uninstall`

## Next steps

To install the client, see [Install the Azure Information Protection client for users](#).

If you've already installed the client, see the following for additional information that you might need to support this client:

- [Customizations](#)
- [Client files and usage logging](#)
- [Document tracking](#)
- [File types supported](#)
- [PowerShell commands](#)

# Admin Guide: Install the Azure Information Protection client for users

7/20/2020 • 10 minutes to read • [Edit Online](#)

*Applies to: Active Directory Rights Management Services, Azure Information Protection, Windows 10, Windows 8.1, Windows 8, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012*

*Instructions for: Azure Information Protection client for Windows*

## NOTE

To provide a unified and streamlined customer experience, **Azure Information Protection client (classic)** and **Label Management** in the Azure Portal are being **deprecated** as of **March 31, 2021**. This time-frame allows all current Azure Information Protection customers to transition to our unified labeling solution using the Microsoft Information Protection Unified Labeling platform. Learn more in the official [deprecation notice](#).

Before you install the Azure Information Protection client on your enterprise network, check that computers have the required operating system versions and applications for Azure Information Protection: [Requirements for Azure Information Protection](#).

Then check the additional prerequisites that might be needed for the Azure Information Protection client, as documented in the next section. Not all the prerequisites are checked by the installation program.

## Additional prerequisites for the Azure Information Protection client

- Microsoft .NET Framework 4.6.2

The full installation of the Azure Information Protection client by default, requires a minimum version of Microsoft .NET Framework 4.6.2 and if this is missing, the setup wizard from the executable installer tries to download and install this prerequisite. When this prerequisite is installed as part of the client installation, the computer must be restarted. Although not recommended, you can bypass this prerequisite when you use the setup wizard by using a [custom installation parameter](#).

This prerequisite is not automatically installed when you install the client silently by using the executable installer, Windows Update, or Windows installer. For these scenarios, you must install this prerequisite separately if it is needed, or the install fails. You can download the Microsoft .NET Framework 4.6.2 (Offline Installer) from the [Microsoft Download Center](#).

- Microsoft .NET Framework 4.5.2

If the Azure Information Protection Viewer is installed separately, this requires a minimum version of Microsoft .NET Framework 4.5.2 and if this is missing, the executable installer does not download or install it.

- Windows PowerShell minimum version 4.0

The PowerShell module for the client requires a minimum version of 4.0 for Windows PowerShell, which might need to be installed on older operating systems. For more information, see [How to Install Windows PowerShell 4.0](#). The installer does not check or install this prerequisite for you. To confirm the version of Windows PowerShell that you are running, type `$PSVersionTable` in a PowerShell session.

- Screen resolution greater than 800x600

Resolutions 800x600 and lower can't fully display the **Classify and protect - Azure Information Protection** dialog box when you right-click a file or folder in File Explorer.

- Microsoft Online Services Sign-in Assistant 7.250.4303.0

Computers running Office 2010 require Microsoft Online Services Sign-in Assistant version 7.250.4303.0. This version is included with the client installation. If you have a later version of the Sign-in Assistant, uninstall it before you install the Azure Information Protection client. For example, check the version and uninstall the Sign-in Assistant by using **Control Panel > Program and Features > Uninstall or change a program**.

- KB 4482887

For Windows 10 version 1809 only, operation system builds older than 17763.348, install [March 1, 2019—KB4482887 \(OS Build 17763.348\)](#) to ensure the Information Protection bar displays correctly in Office applications. This update is not needed if you have Office 365 1902 or later.

- Configure group policy to prevent the Azure Information Protection add-in from being disabled

For Office 2013 and later versions, configure group policy to ensure that the **Microsoft Azure Information Protection** add-in for Office applications is always enabled. Without this configuration, the Microsoft Azure Information Protection add-in can get disabled and users will not be able to label their documents and emails in their Office application.

- For Outlook: Use the group policy setting documented in [System Administrator control over add-ins](#) from the Office documentation.
- For Word, Excel, and PowerPoint: Use the group policy setting [list of managed add-ins](#) documented in the Support article [No Add-ins loaded due to group policy settings for Office 2013 and Office 2016 programs](#).

Specify the following programmatic identifiers (ProgID) for Azure Information Protection, and set the option to **1: The add-in is always enabled**.

For Word: `MSIP.WordAddin`

For Excel: `MSIP.ExcelAddin`

For PowerPoint: `MSIP.PowerPointAddin`

#### **IMPORTANT**

Installation of the Azure Information Protection client requires local administrative permissions.

## Options to install the Azure Information Protection client for users

Use one of the following options to install the client for users:

INSTALL OPTION	DESCRIPTION
<b>Run the client executable (.exe)</b> <a href="#">Instructions</a>	We recommend running the .exe version of the client to run the installation interactively or silently. Running the .exe file has the most flexibility, and is recommended because it also checks for many of the prerequisites and can also install any prerequisites that are missing.

Install option	Description
<p><b>Deploy the client's Windows installer (.msi)</b>  <a href="#">Instructions</a></p>	<p>The Azure Information Protection client Windows installer is supported for silent installations only that use a central deployment mechanism. For example, use the .msi file when deploying with a group policy, Configuration Manager, and Microsoft Intune.</p> <p>You must use this method for Windows 10 PCs that are managed by Intune and mobile device management (MDM) as .exe files are not supported for these computers.</p> <p><b>Note:</b> When using the .msi installation, you must manually check for prerequisites and install or uninstall any dependent software required.</p>

After installing the client, perform updates by repeating the same installation method, or use Windows Update to keep the client updated automatically. You are not required to uninstall legacy versions of the client before installing a new version.

For more information, see [Upgrading and maintaining the Azure Information Protection client](#).

#### NOTE

To uninstall the client, use the Windows **Add or remove programs** option, such as from the [Windows Control Panel](#).

### To install the Azure Information Protection client by using the executable installer

Use the following instructions to install the client when you're not using the Microsoft Update catalog, or deploying the .msi by using a central deployment method such as Intune.

1. Download the executable version Azure Information Protection client from the [Microsoft Download Center](#).

If there is a preview version available, keep this version for testing only. It is not intended for end users in a production environment.

2. For a default installation, simply run the executable, for example, **AzInfoProtection.exe**. However, to see the installation options, first run the executable with **/help**: `AzInfoProtection.exe /help`

Example to silently install the client: `AzInfoProtection.exe /quiet`

Example to silently install only the PowerShell cmdlets: `AzInfoProtection.exe PowerShellOnly=true /quiet`

Additional parameters that are not listed on the help screen:

- **ServiceLocation**: Use this parameter if you are installing the client on computers that run Office 2010 and your users are not local administrators on their computers or you do not want them to be prompted. [More information](#)
- **DowngradeDotNetRequirement**: Use this parameter to bypass the requirement for Microsoft Framework .NET version 4.6.2. [More information](#)
- **AllowTelemetry=0**: Use this parameter to disable the install option **Help improve Azure Information Protection by sending usage statistics to Microsoft**.

3. If you are installing interactively, select the option to install a **demo policy** if you cannot connect to Office 365 or Azure Active Directory, but want to see and experience the client side of Azure Information Protection by using a local policy for demonstration purposes. When your client connects to an Azure Information Protection service, this demo policy is replaced with your organization's Azure Information Protection policy.

4. To complete the installation:

- If your computer runs Office 2010, restart your computer.
- If the client was not installed with the ServiceLocation parameter, when you first open one of the Office applications that use the Azure Information Protection bar (for example, Word), you must confirm any prompts to update the registry for this first-time use. [Service discovery](#) is used to populate the registry keys.

- For other versions of Office, restart any Office applications and all instances of File Explorer.

5. You can confirm that the installation was successful by checking the install log file, which by default is created in the %temp% folder. You can change this location with the /log installation parameter.

This file has the following naming format:

```
Microsoft_Azure_Information_Protection_<number>_<number>_MSIP.Setup.Main.msi.log
```

For example:

```
Microsoft_Azure_Information_Protection_20161201093652_000_MSIP.Setup.Main.msi.log
```

In this log file, search for the following string: **Product: Microsoft Azure Information Protection -- Installation completed successfully.** If the installation failed, this log file contains details to help you identify and resolve any problems.

**More information about the ServiceLocation installation parameter**

When you install the client for users who have Office 2010 and they do not have local administrative permissions, specify the ServiceLocation parameter and the URL for your Azure Rights Management service. This parameter and value creates and sets the following registry keys:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\MSDRM\ServiceLocation\Activation
```

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\MSDRM\ServiceLocation\EnterprisePublishing
```

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSDRM\ServiceLocation\EnterprisePublishing
```

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSDRM\ServiceLocation\Activation
```

Use the following procedure to identify the value to specify for the ServiceLocation parameter.

**To identify the value to specify for the ServiceLocation parameter**

1. From a PowerShell session, first run [Connect-AipService](#) and specify your administrator credentials to connect to the Azure Rights Management service. Then run [Get-AipServiceConfiguration](#).

If you haven't already installed the PowerShell module for the Azure Rights Management service, see [Installing the AIPService PowerShell module](#).

2. From the output, identify the **LicensingIntranetDistributionPointUrl** value.

For example: **LicensingIntranetDistributionPointUrl** : [https://5c6bb73b-1038-4eec-863d-49bded473437.rms.na.aadrm.com/\\_wmcs/licensing](https://5c6bb73b-1038-4eec-863d-49bded473437.rms.na.aadrm.com/_wmcs/licensing)

3. From the value, remove **\_wmcs/licensing** from this string. For example: <https://5c6bb73b-1038-4eec-863d-49bded473437.rms.na.aadrm.com>

The remainin' string is the value to specify for your ServiceLocation parameter.

Example to install the client silently for Office 2010 and Azure RMS:

```
AzInfoProtection.exe /quiet ServiceLocation=https://5c6bb73b-1038-4eec-863d-49bded473437.rms.na.aadrm.com
```

**More information about the DowngradeDotNetRequirement installation parameter**

To support automatic upgrades by using Windows Update, and for reliable integration with Office applications,

the Azure Information Protection client uses Microsoft .NET Framework version 4.6.2. By default, an interactive installation by using the executable checks for this version and tries to install it if it is missing. The installation then requires the computer to restart.

If installing this later version of the Microsoft .NET Framework is not practical, you can install the client with the **DowngradeDotNetRequirement=True** parameter and value, which bypasses this requirement if Microsoft .NET Framework version 4.5.1 is installed.

For example: `AzInfoProtection.exe DowngradeDotNetRequirement=True`

We recommend that you use this parameter with caution, and with the knowledge that there are reported issues with Office applications hanging when the Azure Information Protection client is used with this older version of the Microsoft .NET Framework. If you do experience hanging problems, upgrade to the recommended version before you try other troubleshooting solutions.

Also remember that if you use Windows Update to keep the Azure Information Protection client updated, you must have another software deployment mechanism to upgrade the client to later versions.

### To install the Azure Information Protection client by using the .msi installer

For central deployment, use the following information that is specific to the .msi installation version of the Azure Information Protection client.

If you use Intune for your software deployment method, use these instructions together with [Add apps with Microsoft Intune](#).

1. Download the .msi version of the Azure Information Protection client from the [Microsoft Download Center](#).

If there is a preview version available, keep this version for testing only. It is not intended for end users in a production environment.

2. For each computer that runs the .msi file, you must make sure that the following software dependencies are in place. For example, package these with the .msi version of the client or only deploy to computers that meet these dependencies:

OFFICE VERSION	OPERATING SYSTEM	SOFTWARE	ACTION
All versions except Office 365 1902 or later	Windows 10 version 1809 only, operation system builds older than 17763.348	<a href="#">KB 4482887</a>	Install
Office 2013	All supported versions	64-bit: <a href="#">KB3172523</a> 32-bit: <a href="#">KB3172523</a> Version: 1.0	Install
Office 2010	All supported versions	<a href="#">Microsoft Online Services Sign-in Assistant</a> Version: 2.1	Install
Office 2016	All supported versions	64-bit: <a href="#">KB3178666</a> 32-bit: <a href="#">KB3178666</a> Version: 1.0	Install

OFFICE VERSION	OPERATING SYSTEM	SOFTWARE	ACTION
Office 2010	All supported versions	<a href="#">Microsoft Online Services Sign-in Assistant</a>  Version: 2.1	Install
Office 2010	Windows 8.1 and Windows Server 2012 R2	<a href="#">KB2843630</a>  Version number included in file name: v3	Install if KB2843630 or KB2919355 is not installed
Office 2010	Windows 8 and Windows Server 2012	<a href="#">KB2843630</a>  Version number included in file name: v3	Install

3. For a default installation, run the .msi with `/quiet`, for example, `AzInfoProtection.msi /quiet`. However, you might need to specify additional installation parameters that are documented in the [executable installer instructions](#) with one exception:

- Instead of `AllowTelemetry=0` to disable the install option **Help improve Azure Information Protection by sending usage statistics to Microsoft**, specify `ENABLETELEMETRY=0`.

## How to install the Azure Information Protection scanner

The PowerShell module that is included with the Azure Information Protection client has cmdlets to install and configure the scanner. However, to use the scanner, you must install the full version of the client and cannot install just the PowerShell module.

To install the client for the scanner, follow the same instructions in the preceding sections. You're then ready to configure and then install the scanner. For instructions, see [Deploying the Azure Information Protection scanner to automatically classify and protect files](#).

## Next steps

Now that you've installed the Azure Information Protection client, see the following for additional information that you might need to support this client:

- [Customizations](#)
- [Client files and usage logging](#)
- [Document tracking](#)
- [File types supported](#)
- [PowerShell commands](#)

# Admin Guide: Custom configurations for the Azure Information Protection client

7/20/2020 • 46 minutes to read • [Edit Online](#)

*Applies to:* Active Directory Rights Management Services, [Azure Information Protection](#), Windows 10, Windows 8.1, Windows 8, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

*Instructions for:* [Azure Information Protection client for Windows](#)

## NOTE

To provide a unified and streamlined customer experience, **Azure Information Protection client (classic)** and **Label Management** in the Azure Portal are being **deprecated** as of **March 31, 2021**. This time-frame allows all current Azure Information Protection customers to transition to our unified labeling solution using the Microsoft Information Protection Unified Labeling platform. Learn more in the official [deprecation notice](#).

Use the following information for advanced configurations that you might need for specific scenarios or a subset of users when you manage the Azure Information Protection client.

Some of these settings require editing the registry and some use advanced settings that you must configure in the Azure portal, and then publish for clients to download.

## How to configure advanced client configuration settings in the portal

1. If you haven't already done so, in a new browser window, [sign in to the Azure portal](#), and then navigate to the **Azure Information Protection** pane.
2. From the **Classifications > Labels** menu option: Select **Policies**.
3. On the **Azure Information Protection - Policies** pane, select the context menu (...) next to the policy to contain the advanced settings. Then select **Advanced settings**.

You can configure advanced settings for the Global policy, as well as for scoped policies.

4. On the **Advanced settings** pane, type the advanced setting name and value, and then select **Save and close**.
5. Make sure that users for this policy restart any Office applications that they had open.
6. If you no longer need the setting and want to revert to the default behavior: On the **Advanced settings** pane, select the context menu (...) next to the setting you no longer need, and then select **Delete**. Then click **Save and close**.

## Available advanced client settings

SETTING	SCENARIO AND INSTRUCTIONS
DisableDNF	<a href="#">Hide or show the Do Not Forward button in Outlook</a>
DisableMandatoryInOutlook	<a href="#">Exempt Outlook messages from mandatory labeling</a>

SETTING	SCENARIO AND INSTRUCTIONS
CompareSubLabelsInAttachmentAction	Enable order support for sublabels
ContentExtractionTimeout	Change the timeout settings for the scanner
EnableBarHiding	Permanently hide the Azure Information Protection bar
EnableCustomPermissions	Make the custom permissions options available or unavailable to users
EnableCustomPermissionsForCustomProtectedFiles	For files protected with custom permissions, always display custom permissions to users in File Explorer
EnablePDFv2Protection	Don't protect PDF files by using the ISO standard for PDF encryption
FileProcessingTimeout	Change the timeout settings for the scanner
LabelbyCustomProperty	Migrate labels from Secure Islands and other labeling solutions
LabelToSMIME	Configure a label to apply S/MIME protection in Outlook
LogLevel	Change the local logging level
LogMatchedContent	Disable sending information type matches for a subset of users
OutlookBlockTrustedDomains	Implement pop-up messages in Outlook that warn, justify, or block emails being sent
OutlookBlockUntrustedCollaborationLabel	Implement pop-up messages in Outlook that warn, justify, or block emails being sent
OutlookDefaultLabel	Set a different default label for Outlook
OutlookJustifyTrustedDomains	Implement pop-up messages in Outlook that warn, justify, or block emails being sent
OutlookJustifyUntrustedCollaborationLabel	Implement pop-up messages in Outlook that warn, justify, or block emails being sent
OutlookRecommendationEnabled	Enable recommended classification in Outlook
OutlookOverrideUnlabeledCollaborationExtensions	Implement pop-up messages in Outlook that warn, justify, or block emails being sent
OutlookUnlabeledCollaborationActionOverrideMailBodyBehavior	Implement pop-up messages in Outlook that warn, justify, or block emails being sent
OutlookWarnTrustedDomains	Implement pop-up messages in Outlook that warn, justify, or block emails being sent

SETTING	SCENARIO AND INSTRUCTIONS
OutlookWarnUntrustedCollaborationLabel	Implement pop-up messages in Outlook that warn, justify, or block emails being sent
PostponeMandatoryBeforeSave	Remove "Not now" for documents when you use mandatory labeling
ProcessUsingLowIntegrity	Disable the low integrity level for the scanner
PullPolicy	Support for disconnected computers
RemoveExternalContentMarkingInApp	Remove headers and footers from other labeling solutions
ReportAnIssueLink	Add "Report an Issue" for users
RunAuditInformationTypesDiscovery	Disable sending discovered sensitive information in documents to Azure Information Protection analytics
RunPolicyInBackground	Turn on classification to run continuously in the background
ScannerConcurrencyLevel	Limit the number of threads used by the scanner
SyncPropertyName	Label an Office document by using an existing custom property
SyncPropertyState	Label an Office document by using an existing custom property

## Prevent sign-in prompts for AD RMS only computers

By default, the Azure Information Protection client automatically tries to connect to the Azure Information Protection service. For computers that only communicate with AD RMS, this configuration can result in a sign-in prompt for users that is not necessary. You can prevent this sign-in prompt by editing the registry.

- Locate the following value name, and then set the value data to 0:

`HKEY_CURRENT_USER\SOFTWARE\Microsoft\MSIP\EnablePolicyDownload`

Regardless of this setting, the Azure Information Protection client still follows the standard [RMS service discovery process](#) to find its AD RMS cluster.

## Sign in as a different user

In a production environment, users wouldn't usually need to sign in as a different user when they are using the Azure Information Protection client. However, as an administrator, you might need to sign in as a different user during a testing phase.

You can verify which account you're currently signed in as by using the **Microsoft Azure Information Protection** dialog box: Open an Office application and on the **Home** tab, in the **Protection** group, click **Protect**, and then click **Help and feedback**. Your account name is displayed in the **Client status** section.

Be sure to also check the domain name of the signed in account that's displayed. It can be easy to miss that you're signed in with the right account name but wrong domain. A symptom of using the wrong account includes failing to download the Azure Information Protection policy, or not seeing the labels or behavior that you expect.

To sign in as a different user:

1. Navigate to %localappdata%\Microsoft\MSIP and delete the **TokenCache** file.
2. Restart any open Office applications and sign in with your different user account. If you do not see a prompt in your Office application to sign in to the Azure Information Protection service, return to the **Microsoft Azure Information Protection** dialog box and click **Sign in** from the updated **Client status** section.

Additionally:

- If the Azure Information Protection client is still signed in with the old account after completing these steps, delete all cookies from Internet Explorer, and then repeat steps 1 and 2.
- If you are using single sign-on, you must sign out from Windows and sign in with your different user account after deleting the token file. The Azure Information Protection client then automatically authenticates by using your currently signed in user account.
- This solution is supported for signing in as another user from the same tenant. It is not supported for signing in as another user from a different tenant. To test Azure Information Protection with multiple tenants, use different computers.
- You can use the **Reset settings** option from **Help and Feedback** to sign out and delete the currently downloaded Azure Information Protection policy.

## Enforce protection-only mode when your organization has a mix of licenses

If your organization does not have any licenses for Azure Information Protection, but does have licenses for Office 365 that include the Azure Rights Management service for protecting data, the Azure Information Protection client for Windows automatically runs in [protection-only mode](#).

However, if your organization has a subscription for Azure Information Protection, by default all Windows computers can download the Azure Information Protection policy. The Azure Information Protection client does not do license checking and enforcement.

If you have some users who do not have a license for Azure Information Protection but do have a license for Office 365 that includes the Azure Rights Management service, edit the registry on these users' computers to prevent users from running the unlicensed classification and labeling features from Azure Information Protection.

Locate the following value name and set the value data to 0:

**HKEY\_CURRENT\_USER\SOFTWARE\Microsoft\MSIP\EnablePolicyDownload**

In addition, check that these computers do not have a file named **Policy.msip** in the **%LocalAppData%\Microsoft\MSIP** folder. If this file exists, delete it. This file contains the Azure Information Protection policy and might have downloaded before you edited the registry, or if the Azure Information Protection client was installed with the demo option.

## Add "Report an Issue" for users

This configuration uses an [advanced client setting](#) that you must configure in the Azure portal.

When you specify the following advanced client setting, users see a **Report an Issue** option that they can select from the **Help and Feedback** client dialog box. Specify an HTTP string for the link. For example, a customized web page that you have for users to report issues, or an email address that goes to your help desk.

To configure this advanced setting, enter the following strings:

- Key: **ReportAnIssueLink**
- Value: <HTTP string>

Example value for a website: `https://support.contoso.com`

Example value for an email address: `mailto:helpdesk@contoso.com`

## Hide the Classify and Protect menu option in Windows File Explorer

Create the following DWORD value name (with any value data):

`HKEY_CLASSES_ROOT\AllFilesystemObjects\shell\Microsoft.Azip.RightClick\LegacyDisable`

## Support for disconnected computers

By default, the Azure Information Protection client automatically tries to connect to the Azure Information Protection service to download the latest Azure Information Protection policy. If you have computers that you know will not be able to connect to the internet for a period of time, you can prevent the client from attempting to connect to the service by editing the registry.

Note that without an internet connection, the client cannot apply protection (or remove protection) by using your organization's cloud-based key. Instead, the client is limited to using labels that apply classification only, or protection that uses [HYOK](#).

You can prevent a sign-in prompt to the Azure Information Protection service by using an [advanced client setting](#) that you must configure in the Azure portal and then download the policy for computers. Or, you can prevent this sign-in prompt by editing the registry.

- To configure the advanced client setting:

1. Enter the following strings:

- Key: **PullPolicy**
- Value: **False**

2. Download the policy with this setting and install it on computers by using the instructions that follow.

- Alternatively, to edit the registry:

- Locate the following value name, and then set the value data to **0**:

`HKEY_CURRENT_USER\SOFTWARE\Microsoft\MSIP\EnablePolicyDownload`

The client must have a valid policy file named **Policy.msip**, in the `%LocalAppData%\Microsoft\MSIP` folder.

You can export the global policy or a scoped policy from the Azure portal, and copy the exported file to the client computer. You can also use this method to replace an-out-of-date policy file with the latest policy. However, exporting the policy does not support the scenario where a user belongs to more than one scoped policy. Also be aware that if users select the **Reset Settings** option from [Help and feedback](#), this action deletes the policy file and renders the client inoperable until you manually replace the policy file or the client connects to the service to download the policy.

When you export the policy from the Azure portal, a zipped file is downloaded that contains multiple versions of the policy. These policy versions correspond to different versions of the Azure Information Protection client:

1. Unzip the file and use the following table to identify which policy file you need.

FILE NAME	CORRESPONDING CLIENT VERSION
Policy1.1.msip	version 1.2
Policy1.2.msip	version 1.3 - 1.7
Policy1.3.msip	version 1.8 - 1.29
Policy1.4.msip	version 1.32 and later

2. Rename the identified file to **Policy.msip**, and then copy it to the **%LocalAppData%\Microsoft\MSIP** folder on computers that have the Azure Information Protection client installed.

If your disconnected computer is running the current GA version of the Azure Information Protection scanner, there are additional configuration steps you must take. For more information, see [Restriction: The scanner server cannot have internet connectivity](#) in the scanner deployment prerequisites.

## Hide or show the Do Not Forward button in Outlook

The recommended method to configure this option is by using the [policy setting Add the Do Not Forward button to the Outlook ribbon](#). However, you can also configure this option by using an [advanced client setting](#) that you configure in the Azure portal.

When you configure this setting, it hides or shows the **Do Not Forward** button on the ribbon in Outlook. This setting has no effect on the Do Not Forward option from Office menus.

To configure this advanced setting, enter the following strings:

- Key: **DisableDNF**
- Value: **True** to hide the button, or **False** to show the button

## Make the custom permissions options available or unavailable to users

The recommended method to configure this option is by using the [policy setting Make the custom permissions option available for users](#). However, you can also configure this option by using an [advanced client setting](#) that you configure in the Azure portal.

When you configure this setting and publish the policy for users, the custom permissions options become visible for users to select their own protection settings, or they are hidden so that users can't select their own protection settings unless prompted.

To configure this advanced setting, enter the following strings:

- Key: **EnableCustomPermissions**
- Value: **True** to make the custom permissions option visible, or **False** to hide this option

## For files protected with custom permissions, always display custom permissions to users in File Explorer

This configuration uses an [advanced client setting](#) that you must configure in the Azure portal. This setting is in preview and might change.

When you configure the [policy setting Make the custom permissions option available for users](#) or the equivalent advanced client setting in the previous section, users are not able to see or change custom permissions

that are already set in a protected document.

When you create and configure this advanced client setting, users can see and change custom permissions for a protected document when they use File Explorer, and right-click the file. The **Custom Permissions** option from the **Protect** button on the Office ribbon remains hidden.

To configure this advanced setting, enter the following strings:

- Key: **EnableCustomPermissionsForCustomProtectedFiles**
- Value: **True**

## Permanently hide the Azure Information Protection bar

This configuration uses an [advanced client setting](#) that you must configure in the Azure portal. Use it only when the [policy setting](#) **Display the Information Protection bar in Office apps** is set to **On**.

By default, if a user clears the **Show Bar** option from the **Home** tab, **Protection** group, **Protect** button, the Information Protection bar no longer displays in that Office app. However, the bar automatically displays again the next time an Office app is opened.

To prevent the bar from displaying again automatically after a user has chosen to hide it, use this client setting. This setting has no effect if the user closes the bar by using the **Close this bar** icon.

Even though the Azure Information Protection bar remains hidden, users can still select a label from a temporarily displayed bar if you have configured recommended classification, or when a document or email must have a label.

To configure this advanced setting, enter the following strings:

- Key: **EnableBarHiding**
- Value: **True**

## Enable order support for sublabels on attachments

This configuration uses an [advanced client setting](#) that you must configure in the Azure portal.

Use this setting when you have sublabels and you have configured the following [policy setting](#):

- **For email messages with attachments, apply a label that matches the highest classification of those attachments**

Configure the following strings:

- Key: **CompareSubLabelsInAttachmentAction**
- Value: **True**

Without this setting, the first label that's found from the parent label with the highest classification is applied to the email.

With this setting, the sublabel that's ordered last from the parent label with the highest classification is applied to the email. If you need to reorder your labels to apply the label that you want for this scenario, see [How to delete or reorder a label for Azure Information Protection](#).

## Exempt Outlook messages from mandatory labeling

This configuration uses an [advanced client setting](#) that you must configure in the Azure portal.

By default, when you enable the [policy setting](#) **All documents and emails must have a label**, all saved

documents and sent emails must have a label applied. When you configure the following advanced setting, the policy setting applies only to Office documents and not to Outlook messages.

To configure this advanced setting, enter the following strings:

- Key: **DisableMandatoryInOutlook**
- Value: **True**

## Enable recommended classification in Outlook

This configuration uses an [advanced client setting](#) that you must configure in the Azure portal. This setting is in preview and might change.

When you configure a label for recommended classification, users are prompted to accept or dismiss the recommended label in Word, Excel, and PowerPoint. This setting extends this label recommendation to also display in Outlook.

To configure this advanced setting, enter the following strings:

- Key: **OutlookRecommendationEnabled**
- Value: **True**

## Implement pop-up messages in Outlook that warn, justify, or block emails being sent

This configuration uses multiple [advanced client settings](#) that you must configure in the Azure portal.

When you create and configure the following advanced client settings, users see pop-up messages in Outlook that can warn them before sending an email, or ask them to provide justification why they are sending an email, or prevent them from sending an email for either of the following scenarios:

- **Their email or attachment for the email has a specific label:**
  - The attachment can be any file type
- **Their email or attachment for the email doesn't have a label:**
  - The attachment can be an Office document or PDF document

When these conditions are met, the user sees a pop-up message with one of the following actions:

- **Warn:** The user can confirm and send, or cancel.
- **Justify:** The user is prompted for justification (predefined options or free-form). The user can then send or cancel the email. The justification text is written to the email x-header, so that it can be read by other systems. For example, data loss prevention (DLP) services.
- **Block:** The user is prevented from sending the email while the condition remains. The message includes the reason for blocking the email, so the user can address the problem. For example, remove specific recipients, or label the email.

When the popup-messages are for a specific label, you can configure exceptions for recipients by domain name.

The resulting actions from the pop-up messages are logged to the local Windows event log **Applications and Services Logs > Azure Information Protection**:

- Warn messages: Information ID 301
- Justify messages: Information ID 302

- Block messages: Information ID 303

Example event entry from a justify message:

```
Client Version: 1.53.10.0
Client Policy ID: e5287fe6-f82c-447e-bf44-6fa8ff146ef4
Item Full Path: Price list.msg
Item Name: Price list
Process Name: OUTLOOK
Action: Justify
User Justification: My manager approved sharing of this content
Action Source:
User Response: Confirmed
```

The following sections contain configuration instructions for each advanced client setting, and you can see them in action for yourself with [Tutorial: Configure Azure Information Protection to control oversharing of information using Outlook](#).

#### To implement the warn, justify, or block pop-up messages for specific labels:

To implement the pop-up messages for specific labels, you must know the label ID for those labels. The label ID value is displayed on the **Label** pane, when you view or configure the Azure Information Protection policy in the Azure portal. For files that have labels applied, you can also run the `Get-AIPFileStatus` PowerShell cmdlet to identify the label ID (MainLabelId or SubLabelId). When a label has sublabels, always specify the ID of just a sublabel and not the parent label.

Create one or more of the following advanced client settings with the following keys. For the values, specify one or more labels by their IDs, each one separated by a comma.

Example value for multiple label IDs as a comma-separated string:

```
dcf781ba-727f-4860-b3c1-73479e31912b,1ace2cc3-14bc-4142-9125-bf946a70542c,3e9df74d-3168-48af-8b11-037e3021813f
```

- Warn messages:
  - Key: **OutlookWarnUntrustedCollaborationLabel**
  - Value: <label IDs, comma-separated>
- Justification messages:
  - Key: **OutlookJustifyUntrustedCollaborationLabel**
  - Value: <label IDs, comma-separated>
- Block messages:
  - Key: **OutlookBlockUntrustedCollaborationLabel**
  - Value: <label IDs, comma-separated>

#### To exempt domain names for pop-up messages configured for specific labels

For the labels that you've specified with these pop-up messages, you can exempt specific domain names so that users do not see the messages for recipients who have that domain name included in their email address. In this case, the emails are sent without interruption. To specify multiple domains, add them as a single string, separated by commas.

A typical configuration is to display the pop-up messages only for recipients who are external to your organization or who aren't authorized partners for your organization. In this case, you specify all the email domains that are used by your organization and by your partners.

Create the following advanced client settings and for the value, specify one or more domains, each one separated

by a comma.

Example value for multiple domains as a comma-separated string: `contoso.com,fabrikam.com,litware.com`

- Warn messages:
  - Key: **OutlookWarnTrustedDomains**
  - Value: <**domain names, comma separated**>
- Justification messages:
  - Key: **OutlookJustifyTrustedDomains**
  - Value: <**domain names, comma separated**>
- Block messages:
  - Key: **OutlookBlockTrustedDomains**
  - Value: <**domain names, comma separated**>

For example, you have specified the **OutlookBlockUntrustedCollaborationLabel** advanced client setting for the **Confidential \ All Employees** label. You now specify the additional advanced client setting of **OutlookBlockTrustedDomains** and **contoso.com**. As a result, a user can send an email to **john@sales.contoso.com** when it is labeled **Confidential \ All Employees** but will be blocked from sending an email with the same label to a Gmail account.

#### To implement the warn, justify, or block pop-up messages for emails or attachments that don't have a label:

Create the following advanced client setting with one of the following values:

- Warn messages:
  - Key: **OutlookUnlabeledCollaborationAction**
  - Value: **Warn**
- Justification messages:
  - Key: **OutlookUnlabeledCollaborationAction**
  - Value: **Justify**
- Block messages:
  - Key: **OutlookUnlabeledCollaborationAction**
  - Value: **Block**
- Turn off these messages:
  - Key: **OutlookUnlabeledCollaborationAction**
  - Value: **Off**

#### To define specific file name extensions for the warn, justify, or block pop-up messages for email attachments that don't have a label

By default, the warn, justify, or block pop-up messages apply to all Office documents and PDF documents. You can refine this list by specifying which file name extensions should display the warn, justify, or block messages with an additional advanced client property and a comma-separated list of file name extensions.

Example value for multiple file name extensions to define as a comma-separated string:

`.XLSX,.XLSM,.XLS,.XLTX,.XLTM,.DOCX,.DOCM,.DOC,.DOCX,.DOCM,.PPTX,.PPTM,.PPT,.PPTX,.PPTM`

In this example, an unlabeled PDF document will not result in warn, justify, or block pop-up messages.

- Key: **OutlookOverrideUnlabeledCollaborationExtensions**
- Value: <file name extensions to display messages, comma separated>

**To specify a different action for email messages without attachments**

By default, the value that you specify for OutlookUnlabeledCollaborationAction to warn, justify, or block pop-up messages applies to emails or attachments that don't have a label. You can refine this configuration by specifying another advanced client setting for email messages that don't have attachments.

Create the following advanced client setting with one of the following values:

- Warn messages:
  - Key: **OutlookUnlabeledCollaborationActionOverrideMailBodyBehavior**
  - Value: **Warn**
- Justification messages:
  - Key: **OutlookUnlabeledCollaborationActionOverrideMailBodyBehavior**
  - Value: **Justify**
- Block messages:
  - Key: **OutlookUnlabeledCollaborationActionOverrideMailBodyBehavior**
  - Value: **Block**
- Turn off these messages:
  - Key: **OutlookUnlabeledCollaborationActionOverrideMailBodyBehavior**
  - Value: **Off**

If you don't specify this client setting, the value that you specify for OutlookUnlabeledCollaborationAction is used for unlabeled email messages without attachments as well as unlabeled email messages with attachments.

## Set a different default label for Outlook

This configuration uses an [advanced client setting](#) that you must configure in the Azure portal.

When you configure this setting, Outlook doesn't apply the default label that is configured in the Azure Information Protection policy for the setting **Select the default label**. Instead, Outlook can apply a different default label, or no label.

To apply a different label, you must specify the label ID. The label ID value is displayed on the **Label** pane, when you view or configure the Azure Information Protection policy in the Azure portal. For files that have labels applied, you can also run the [Get-AIPFileStatus](#) PowerShell cmdlet to identify the label ID (MainLabelId or SubLabelId). When a label has sublabels, always specify the ID of just a sublabel and not the parent label.

So that Outlook doesn't apply the default label, specify **None**.

To configure this advanced setting, enter the following strings:

- Key: **OutlookDefaultLabel**
- Value: <label ID> or **None**

## Configure a label to apply S/MIME protection in Outlook

This configuration uses an [advanced client setting](#) that you must configure in the Azure portal.

Use this setting only when you have a working [S/MIME deployment](#) and want a label to automatically apply this protection method for emails rather than Rights Management protection from Azure Information Protection. The resulting protection is the same as when a user manually selects S/MIME options from Outlook.

This configuration requires you to specify an advanced client setting named **LabelToSMIME** for each Azure Information Protection label that you want to apply S/MIME protection. Then for each entry, set the value by using the following syntax:

```
[Azure Information Protection label ID];[S/MIME action]
```

The label ID value is displayed on the **Label** pane, when you view or configure the Azure Information Protection policy in the Azure portal. To use S/MIME with a sublabel, always specify the ID of just the sublabel and not the parent label. When you specify a sublabel, the parent label must be in the same scope, or in the global policy.

The S/MIME action can be:

- `Sign;Encrypt` : To apply a digital signature and S/MIME encryption
- `Encrypt` : To apply S/MIME encryption only
- `Sign` : To apply a digital signature only

Example values for a label ID of **dcf781ba-727f-4860-b3c1-73479e31912b**:

- To apply a digital signature and S/MIME encryption:

**dcf781ba-727f-4860-b3c1-73479e31912b;Sign;Encrypt**

- To apply S/MIME encryption only:

**dcf781ba-727f-4860-b3c1-73479e31912b;Encrypt**

- To apply a digital signature only:

**dcf781ba-727f-4860-b3c1-73479e31912b;Sign**

As a result of this configuration, when the label is applied for an email message, S/MIME protection is applied to the email in addition to the label's classification.

If the label you specify is configured for Rights Management protection in the Azure portal, S/MIME protection replaces the Rights Management protection only in Outlook. For all other scenarios that support labeling, Rights Management protection will be applied.

If you want the label to be visible in Outlook only, configure the label to apply the single user-defined action of **Do Not Forward**, as described in the [Quickstart: Configure a label for users to easily protect emails that contain sensitive information](#).

## Remove "Not now" for documents when you use mandatory labeling

This configuration uses an [advanced client setting](#) that you must configure in the Azure portal.

When you use the [policy setting](#) of **All documents and emails must have a label**, users are prompted to select a label when they first save an Office document and when they send an email. For documents, users can select **Not now** to temporarily dismiss the prompt to select a label and return to the document. However, they cannot close the saved document without labeling it.

When you configure this setting, it removes the **Not now** option so that users must select a label when the document is first saved.

To configure this advanced setting, enter the following strings:

- Key: **PostponeMandatoryBeforeSave**
- Value: **False**

## Turn on classification to run continuously in the background

This configuration uses an [advanced client setting](#) that you must configure in the Azure portal. This setting is in preview and might change.

When you configure this setting, it changes the [default behavior](#) of how the Azure Information Protection client applies automatic and recommended labels to documents:

- For Word, Excel, and PowerPoint, automatic classification runs continuously in the background.

The behavior does not change for Outlook.

When the Azure Information Protection client periodically checks documents for the condition rules that you specify, this behavior enables automatic and recommended classification and protection for documents that are stored in Microsoft SharePoint. Large files also save more quickly because the condition rules have already run.

The condition rules do not run in real time as a user types. Instead, they run periodically as a background task if the document is modified.

To configure this advanced setting, enter the following strings:

- Key: **RunPolicyInBackground**
- Value: **True**

## Don't protect PDF files by using the ISO standard for PDF encryption

This configuration uses an [advanced client setting](#) that you must configure in the Azure portal.

When the latest version of the Azure Information Protection client protects a PDF file, the resulting file name extension remains as .pdf and adheres to the ISO standard for PDF encryption. For more information about this standard, see section [7.6 Encryption](#) from the [document that is derived from ISO 32000-1](#) and published by Adobe Systems Incorporated.

If you need the client to revert to the behavior in older versions of the client that protected PDF files by using a .ppdf file name extension, use the following advanced setting by entering the following string:

- Key: **EnablePDFv2Protection**
- Value: **False**

For example, you might need this setting for all users if you use a PDF reader that doesn't support the ISO standard for PDF encryption. Or, you might need to configure it for some users as you gradually phase in a change of PDF reader that supports the new format. Another potential reason to use this setting is if you need to add protection to signed PDF documents. Signed PDF documents can be additionally protected with the .ppdf format because this protection is implemented as a wrapper for the file.

For the Azure Information Protection scanner to use the new setting, the scanner service must be restarted. In addition, the scanner will no longer protect PDF documents by default. If you want PDF documents to be protected by the scanner when **EnablePDFv2Protection** is set to **False**, you must [edit the registry](#).

For more information about the new PDF encryption, see the blog post [New support for PDF encryption with Microsoft Information Protection](#).

For a list of PDF readers that support the ISO standard for PDF encryption, and readers that support older formats, see [Supported PDF readers for Microsoft Information Protection](#).

## To convert existing .ppdf files to protected .pdf files

When the Azure Information Protection client has downloaded the client policy with the new setting, you can use PowerShell commands to convert existing .ppdf files to protected .pdf files that use the ISO standard for PDF encryption.

To use the following instructions for files that you didn't protect yourself, you must have a [Rights Management usage right](#) to remove protection from files, or be a super user. To enable the super user feature and configure your account to be a super user, see [Configuring super users for Azure Rights Management and Discovery Services or Data Recovery](#).

In addition, when you use these instructions for files that you didn't protect yourself, you become the [RMS Issuer](#). In this scenario, the user who originally protected the document can no longer track and revoke it. If users need to track and revoke their protected PDF documents, ask them to manually remove and then reapply the label by using File Explorer, right-click.

To use PowerShell commands to convert existing .ppdf files to protected .pdf files that use the ISO standard for PDF encryption:

1. Use [Get-AIPFileStatus](#) with the .ppdf file. For example:

```
Get-AIPFileStatus -Path \\Finance\Projectx\sales.ppdf
```

2. From the output, take a note of the following parameter values:

- The value (GUID) for **SubLabelId**, if there is one. If this value is blank, a sublabel wasn't used, so note the value for **MainLabelId** instead.

Note: If there is no value for **MainLabelId** either, the file isn't labeled. In this case, you can use the [Unprotect-RMSFile](#) command and [Protect-RMSFile](#) command instead of the commands in step 3 and 4.

- The value for **RMSTemplateId**. If this value is **Restricted Access**, a user has protected the file using custom permissions rather than the protection settings that are configured for the label. If you continue, those custom permissions will be overwritten by the label's protection settings. Decide whether to continue or ask the user (value displayed for the **RMSIssuer**) to remove the label and reapply it, together with their original custom permissions.

3. Remove the label by using [Set-AIPFileLabel](#) with the *RemoveLabel* parameter. If you are using the [policy setting of Users must provide justification to set a lower classification label, remove a label, or remove protection](#), you must also specify the *Justification* parameter with the reason. For example:

```
Set-AIPFileLabel \\Finance\Projectx\sales.ppdf -RemoveLabel -JustificationMessage 'Removing .ppdf protection to replace with .pdf ISO standard'
```

4. Reapply the original label, by specifying the value for the label that you identified in step 1. For example:

```
Set-AIPFileLabel \\Finance\Projectx\sales.pdf -LabelId d9f23ae3-1234-1234-f515f824c57b
```

The file retains the .pdf file name extension but is classified as before, and it is protected by using the ISO standard for PDF encryption.

## Support for files protected by Secure Islands

This configuration option is in preview and might change.

If you used Secure Islands to protect documents, you might have protected text and picture files, and generically protected files as a result of this protection. For example, files that have a file name extension of .ptxt, .jpeg, or .file. When you edit the registry as follows, Azure Information Protection can decrypt these files:

Add the following DWORD value of **EnableIQPFormats** to the following registry path, and set the value data to 1:

- For a 64-bit version of Windows: HKEY\_LOCAL\_MACHINE\SOFTWARE\WOW6432Node\Microsoft\MSIP
- For a 32-bit version of Windows: HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\MSIP

As a result of this registry edit, the following scenarios are supported:

- The Azure Information Protection viewer can open these protected files.
- The Azure Information Protection scanner can inspect these files for sensitive information.
- File Explorer, PowerShell, and the Azure Information Protection scanner can label these files. As a result, you can apply an Azure Information Protection label that applies new protection from Azure Information Protection, or that removes the existing protection from Secure Islands.
- You can use the [labeling migration client customization](#) to automatically convert the Secure Islands label on these protected files to an Azure Information Protection label.

## Migrate labels from Secure Islands and other labeling solutions

This configuration uses an [advanced client setting](#) that you must configure in the Azure portal.

This configuration is currently not compatible with the new default behavior that protects PDF files by using the ISO standard for PDF encryption. In this scenario, .ppdf files cannot be opened by File Explorer, PowerShell, or the scanner. To resolve this, use the advanced client setting to [don't use the ISO standard for PDF encryption](#).

For Office documents and PDF documents that are labeled by Secure Islands, you can relabel these documents with an Azure Information Protection label by using a mapping that you define. You also use this method to reuse labels from other solutions when their labels are on Office documents.

### NOTE

If you have files other than PDF and Office documents that are protected by Secure Islands, these can be relabeled after you edit the registry as described in the [preceding section](#).

As a result of this configuration option, the new Azure Information Protection label is applied by the Azure Information Protection client as follows:

- For Office documents: When the document is opened in the desktop app, the new Azure Information Protection label is shown as set and is applied when the document is saved.
- For File Explorer: In the Azure Information Protection dialog box, the new Azure Information Protection label is shown as set and is applied when the user selects **Apply**. If the user selects **Cancel**, the new label is not applied.
- For PowerShell: [\*\*Set-AIPFileLabel\*\*](#) applies the new Azure Information Protection label. [\*\*Get-AIPFileStatus\*\*](#) doesn't display the new Azure Information Protection label until it is set by another method.
- For the Azure Information Protection scanner: Discovery reports when the new Azure Information

Protection label would be set and this label can be applied with the enforce mode.

This configuration requires you to specify an advanced client setting named **LabelbyCustomProperty** for each Azure Information Protection label that you want to map to the old label. Then for each entry, set the value by using the following syntax:

```
[Azure Information Protection label ID],[migration rule name],[Secure Islands custom property name],[Secure Islands metadata Regex value]
```

The label ID value is displayed on the **Label** pane, when you view or configure the Azure Information Protection policy in the Azure portal. To specify a sublabel, the parent label must be in the same scope, or in the global policy.

Specify your choice of a migration rule name. Use a descriptive name that helps you to identify how one or more labels from your previous labeling solution should be mapped to an Azure Information Protection label. The name displays in the scanner reports and in Event Viewer. Note that this setting does not remove the original label from the document or any visual markings in the document that the original label might have applied. To remove headers and footers, see the next section, [Remove headers and footers from other labeling solutions](#).

#### **Example 1: One-to-one mapping of the same label name**

Requirement: Documents that have a Secure Islands label of "Confidential" should be relabeled as "Confidential" by Azure Information Protection.

In this example:

- The Azure Information Protection label that you want to use is named **Confidential** and has a label ID of **1ace2cc3-14bc-4142-9125-bf946a70542c**.
- The Secure Islands label is named **Confidential** and stored in the custom property named **Classification**.

The advanced client setting:

NAME	VALUE
LabelbyCustomProperty	1ace2cc3-14bc-4142-9125-bf946a70542c,"Secure Islands label is Confidential",Classification,Confidential

#### **Example 2: One-to-one mapping for a different label name**

Requirement: Documents labeled as "Sensitive" by Secure Islands should be relabeled as "Highly Confidential" by Azure Information Protection.

In this example:

- The Azure Information Protection label that you want to use is named **Highly Confidential** and has a label ID of **3e9df74d-3168-48af-8b11-037e3021813f**.
- The Secure Islands label is named **Sensitive** and stored in the custom property named **Classification**.

The advanced client setting:

NAME	VALUE
LabelbyCustomProperty	3e9df74d-3168-48af-8b11-037e3021813f,"Secure Islands label is Sensitive",Classification,Sensitive

#### **Example 3: Many-to-one mapping of label names**

Requirement: You have two Secure Islands labels that include the word "Internal" and you want documents that have either of these Secure Islands labels to be relabeled as "General" by Azure Information Protection.

In this example:

- The Azure Information Protection label that you want to use is named **General** and has a label ID of **2beb8fe7-8293-444c-9768-7fdc6f75014d**.
- The Secure Islands labels include the word **Internal** and are stored in the custom property named **Classification**.

The advanced client setting:

NAME	VALUE
LabelbyCustomProperty	2beb8fe7-8293-444c-9768-7fdc6f75014d,"Secure Islands label contains Internal",Classification,*Internal.*

## Remove headers and footers from other labeling solutions

This configuration uses multiple [advanced client settings](#) that you must configure in the Azure portal. These settings are in preview and might change.

The settings let you remove or replace text-based headers or footers from documents when those visual markings have been applied by another labeling solution. For example, the old footer contains the name of an old label that you have now migrated to Azure Information Protection with a new label name and its own footer.

When the client gets this configuration in its policy, the old headers and footers are removed or replaced when the document is opened in the Office app and any Azure Information Protection label is applied to the document.

This configuration is not supported for Outlook, and be aware that when you use it with Word, Excel, and PowerPoint, it can negatively affect the performance of these apps for users. The configuration lets you define settings per application, for example, search for text in the headers and footers of Word documents but not Excel spreadsheets or PowerPoint presentations.

Because the pattern matching affects the performance for users, we recommend that you limit the Office application types (Word, EXcel, PowerPoint) to just those that need to be searched:

- Key: **RemoveExternalContentMarkingInApp**
- Value: <Office application types WXP>

Examples:

- To search Word documents only, specify **W**.
- To search Word documents and PowerPoint presentations, specify **WP**.

You then need at least one more advanced client setting, **ExternalContentMarkingToRemove**, to specify the contents of the header or footer, and how to remove or replace them.

### How to configure ExternalContentMarkingToRemove

When you specify the string value for the **ExternalContentMarkingToRemove** key, you have three options that use regular expressions:

- Partial match to remove everything in the header or footer.

Example: Headers or footers contain the string **TEXT TO REMOVE**. You want to completely remove these headers or footers. You specify the value: **\*TEXT\***.

- Complete match to remove just specific words in the header or footer.

Example: Headers or footers contain the string **TEXT TO REMOVE**. You want to remove the word **TEXT** only, which leaves the header or footer string as **TO REMOVE**. You specify the value: `TEXT`.

- Complete match to remove everything in the header or footer.

Example: Headers or footers have the string **TEXT TO REMOVE**. You want to remove headers or footers that have exactly this string. You specify the value: `^TEXT TO REMOVE$`.

The pattern matching for the string that you specify is case-insensitive. The maximum string length is 255 characters.

Because some documents might include invisible characters or different kinds of spaces or tabs, the string that you specify for a phrase or sentence might not be detected. Whenever possible, specify a single distinguishing word for the value and be sure to test the results before you deploy in production.

- Key: **ExternalContentMarkingToRemove**
- Value: `<string to match, defined as regular expression>`

#### **Multiline headers or footers**

If a header or footer text is more than a single line, create a key and value for each line. For example, you have the following footer with two lines:

**The file is classified as Confidential**

**Label applied manually**

To remove this multiline footer, you create the following two entries:

- Key 1: **ExternalContentMarkingToRemove**
- Key Value 1: `*Confidential*`
- Key 2: **ExternalContentMarkingToRemove**
- Key Value 2: `*Label applied*`

#### **Optimization for PowerPoint**

Footers in PowerPoint are implemented as shapes. To avoid removing shapes that contain the text that you have specified but are not headers or footers, use an additional advanced client setting named **PowerPointShapeNameToRemove**. We also recommend using this setting to avoid checking the text in all shapes, which is a resource-intensive process.

If you do not specify this additional advanced client setting, and PowerPoint is included in the **RemoveExternalContentMarkingInApp** key value, all shapes will be checked for the text that you specify in the **ExternalContentMarkingToRemove** value.

To find the name of the shape that you're using as a header or footer:

1. In PowerPoint, display the **Selection** pane: **Format** tab > **Arrange** group > **Selection Pane**.
2. Select the shape on the slide that contains your header or footer. The name of the selected shape is now highlighted in the **Selection** pane.

Use the name of the shape to specify a string value for the **PowerPointShapeNameToRemove** key.

Example: The shape name is `fc`. To remove the shape with this name, you specify the value: `fc`.

- Key: **PowerPointShapeNameToRemove**
- Value: `<PowerPoint shape name>`

When you have more than one PowerPoint shape to remove, create as many **PowerPointShapeNameToRemove** keys as you have shapes to remove. For each entry, specify the name of the shape to remove.

By default, only the Master slides are checked for headers and footers. To extend this search to all slides, which is a much more resource-intensive process, use an additional advanced client setting named **RemoveExternalContentMarkingInAllSlides**:

- Key: **RemoveExternalContentMarkingInAllSlides**
- Value: **True**

## Label an Office document by using an existing custom property

### NOTE

If you use this configuration and the configuration to [migrate labels from Secure Islands and other labeling solutions](#), the labeling migration setting takes precedence.

This configuration uses an [advanced client setting](#) that you must configure in the Azure portal.

When you configure this setting, you can classify (and optionally, protect) an Office document when it has an existing custom property with a value that matches one of your label names. This custom property can be set from another classification solution, or can be set as a property by SharePoint.

As a result of this configuration, when a document without an Azure Information Protection label is opened and saved by a user in an Office app, the document is then labeled to match the corresponding property value.

This configuration requires you to specify two advanced settings that work together. The first is named **SyncPropertyName**, which is the custom property name that has been set from the other classification solution, or a property that is set by SharePoint. The second is named **SyncPropertyState** and must be set to **OneWay**.

To configure this advanced setting, enter the following strings:

- Key 1: **SyncPropertyName**
- Key 1 Value: <property name>
- Key 2: **SyncPropertyState**
- Key 2 Value: **OneWay**

Use these keys and corresponding values for only one custom property.

As an example, you have a SharePoint column named **Classification** that has possible values of **Public**, **General**, and **Highly Confidential All Employees**. Documents are stored in SharePoint and have **Public**, **General**, or **Highly Confidential All Employees** as values set for the Classification property.

To label an Office document with one of these classification values, set **SyncPropertyName** to **Classification**, and **SyncPropertyState** to **OneWay**.

Now, when a user opens and saves one of these Office documents, it is labeled **Public**, **General**, or **Highly Confidential \ All Employees** if you have labels with these names in your Azure Information Protection policy. If you do not have labels with these names, the document remains unlabeled.

## Disable sending discovered sensitive information in documents to Azure Information Protection analytics

This configuration uses an [advanced client setting](#) that you must configure in the Azure portal.

When the Azure Information Protection client is used in Office apps, it looks for sensitive information in documents when they are first saved. Providing the client isn't configured to not sent audit information, any sensitive information types found (predefined or custom) are then sent to [Azure Information Protection analytics](#).

The configuration that controls whether the client sends audit information is the [policy setting](#) of **Send audit data to Azure Information Protection log analytics**. When this policy setting is **On** because you want to send audit information that includes labeling actions but you don't want to send sensitive information types found by the client, enter the following strings:

- Key: **RunAuditInformationTypesDiscovery**
- Value: **False**

If you set this advanced client setting, auditing information can still be sent from the client but the information is limited to labeling activity.

For example:

- With this setting, you can see that a user accessed Financial.docx that is labeled **Confidential \ Sales**.
- Without this setting, you can see that Financial.docx contains 6 credit card numbers.
  - If you also enable [deeper analytics into your sensitive data](#), you will additionally be able to see what those credit card numbers are.

## Disable sending information type matches for a subset of users

This configuration uses an [advanced client setting](#) that you must configure in the Azure portal.

When you select the checkbox for [Azure Information Protection analytics](#) that enables deeper analytics into your sensitive data collects the content matches for your sensitive information types or your custom conditions, by default, this information is sent by all users, which includes service accounts that run the Azure Information Protection scanner. If you have some users who should not send this data, create the following advanced client setting in a [scoped policy](#) for these users:

- Key: **LogMatchedContent**
- Value: **Disable**

## Limit the number of threads used by the scanner

This configuration uses an [advanced client setting](#) that you must configure in the Azure portal.

By default, the scanner uses all available processor resources on the computer running the scanner service. If you need to limit the CPU consumption while this service is scanning, create the following advanced setting.

For the value, specify the number of concurrent threads that the scanner can run in parallel. The scanner uses a separate thread for each file that it scans, so this throttling configuration also defines the number of files that can be scanned in parallel.

When you first configure the value for testing, we recommend you specify 2 per core, and then monitor the results. For example, if you run the scanner on a computer that has 4 cores, first set the value to 8. If necessary, increase or decrease that number, according to the resulting performance you require for the scanner computer and your scanning rates.

- Key: **ScannerConcurrencyLevel**
- Value: <number of concurrent threads>

## Disable the low integrity level for the scanner

This configuration uses an [advanced client setting](#) that you must configure in the Azure portal.

By default, the Azure Information Protection scanner runs with a low integrity level. This setting provides higher security isolation but at the cost of performance. A low integrity level is suitable if you run the scanner with an account that has privileged rights (such as a local administrator account) because this setting helps to protect the computer running the scanner.

However, when the service account that runs the scanner has only the rights documented in the [scanner deployment prerequisites](#), the low integrity level is not necessary and is not recommended because it negatively affects performance.

For more information about the Windows integrity levels, see [What is the Windows Integrity Mechanism?](#)

To configure this advanced setting so that the scanner runs with an integrity level that's automatically assigned by Windows (a standard user account runs with a medium integrity level), enter the following strings:

- Key: **ProcessUsingLowIntegrity**
- Value: **False**

## Change the timeout settings for the scanner

This configuration uses [advanced client settings](#) that you must configure in the Azure portal.

By default, the Azure Information Protection scanner has a timeout period of 00:15:00 (15 minutes) to inspect each file for sensitive information types or the regex expressions that you've configured for custom conditions. When the timeout period is reached for this content extraction process, any results before the timeout are returned and further inspection for the file stops. In this scenario, the following error message is logged in `%localappdata%\Microsoft\MSIP\Logs\MSIPScanner.iplog` (zipped if there are multiple logs): **GetContentParts failed with The operation was canceled** in the details.

If you experience this timeout problem because of large files, you can increase this timeout period for full content extraction:

- Key: **ContentExtractionTimeout**
- Value: **<hh:min:sec>**

The file type can influence how long it takes to scan a file. Example scanning times:

- A typical 100 MB Word file: 0.5-5 minutes
- A typical 100 MB PDF file: 5-20 minutes
- A typical 100 MB Excel file: 12-30 minutes

For some file types that are very large, such as video files, consider excluding them from the scan by adding the file name extension to the **File types to scan** option in the scanner profile.

In addition, the Azure Information Protection scanner has a timeout period of 00:30:00 (30 minutes) for each file that it processes. This value takes into account the time it can take to retrieve a file from a repository and temporarily save it locally for actions that can include decryption, content extraction for inspection, labeling, and encryption.

Although the Azure Information Protection scanner can scan dozens to hundreds of files per minute, if you have a data repository that has a high number of very large files, the scanner can exceed this default timeout period and in the Azure portal, seem to stop after 30 minutes. In this scenario, the following error message is logged in `%localappdata%\Microsoft\MSIP\Logs\MSIPScanner.iplog` (zipped if there are multiple logs) and the scanner .csv

log file: The operation was canceled.

A scanner with 4 core processors by default has 16 threads for scanning and the probability of encountering 16 large files in a 30 minute time period depends on the ratio of the large files. For example, if the scanning rate is 200 files per minute, and 1% of files exceed the 30 minute timeout, there is a probability of more than 85% that the scanner will encounter the 30 minute timeout situation. These timeouts can result in longer scanning times and higher memory consumption.

In this situation, if you cannot add more core processors to the scanner computer, consider decreasing the timeout period for better scanning rates and lower memory consumption, but with the acknowledgment that some files will be excluded. Alternatively, consider increasing the timeout period for more accurate scanning results but with the acknowledgment that this configuration will likely result in lower scanning rates and higher memory consumption.

To change the timeout period for file processing, configure the following advanced client setting:

- Key: **FileProcessingTimeout**
- Value: <hh:min:sec>

## Change the local logging level

This configuration uses an [advanced client setting](#) that you must configure in the Azure portal.

By default, the Azure Information Protection client writes client log files to the %localappdata%\Microsoft\MSIP folder. These files are intended for troubleshooting by Microsoft Support.

To change the logging level for these files, configure the following advanced client setting:

- Key: **LogLevel**
- Value: <logging level>

Set the logging level to one of the following values:

- **Off:** No local logging.
- **Error:** Errors only.
- **Info:** Minimum logging, which includes no event IDs (the default setting for the scanner).
- **Debug:** Full information.
- **Trace:** Detailed logging (the default setting for clients). For the scanner, this setting has a significant performance impact and should be enabled for the scanner only if requested by Microsoft Support. If you are instructed to set this level of logging for the scanner, remember to set a different value when the relevant logs have been collected.

This advanced client setting does not change the information that's sent to Azure Information Protection for [central reporting](#), or change the information that's written to the local [event log](#).

## Integration with Exchange message classification for a mobile device labeling solution

Outlook on the web now supports built-in labeling for Exchange Online, which is the recommended method to label emails in Outlook on the web. However, if you're not yet using sensitivity labels that are published from the Office 365 Security & Compliance Center, Microsoft 365 security center, or Microsoft compliance center, you can use Exchange message classification to extend Azure Information Protection labels to your mobile users when they use Outlook on the web. You can also use this method for Exchange Server.

Outlook Mobile does not support Exchange message classification.

To achieve this solution:

1. Use the [New-MessageClassification](#) Exchange PowerShell cmdlet to create message classifications with the Name property that maps to your label names in your Azure Information Protection policy.
2. Create an Exchange mail flow rule for each label: Apply the rule when the message properties include the classification that you configured, and modify the message properties to set a message header.

For the message header, you find the information to specify by inspecting the internet headers of an email that you sent and classified by using your Azure Information Protection label. Look for the header **msip\_labels** and the string that immediately follows, up to and excluding the semicolon. For example:

**msip\_labels: MSIP\_Label\_0e421e6d-ea17-4fdb-8f01-93a3e71333b8\_Enabled=True**

Then, for the message header in the rule, specify **msip\_labels** for the header, and the remainder of this string for the header value. For example:

\*Do the following...  
Set the message header to this value... ▾ Set the message header '**msip\_labels**' to the value  
[\*\*'MSIP\\_Label\\_0e421e6d-ea17-4fdb-8f01-93a3e71333b8\\_Enabled=True'\*\*](#)

Note: When the label is a sublabel, you must also specify the parent label before the sublabel in the header value, using the same format. For example, if your sublabel has a GUID of 27efdf94-80a0-4d02-b88c-b615c12d69a9, your value might look like the following:

**MSIP\_Label\_ab70158b-bdcc-42a3-8493-2a80736e9cbd\_Enabled=True;MSIP\_Label\_27efdf94-80a0-4d02-b88c-b615c12d69a9\_Enabled=True**

Before you test this configuration, remember that there is often a delay when you create or edit mail flow rules (for example, wait an hour). When the rule is in effect, the following events now happen when users use Outlook on the web:

- Users select the Exchange message classification and send the email.
- The Exchange rule detects the Exchange classification and accordingly modifies the message header to add the Azure Information Protection classification.
- When internal recipients view the email in Outlook and they have the Azure Information Protection client installed, they see the Azure Information Protection label assigned.

If your Azure Information Protection labels apply protection, add this protection to the rule configuration: Selecting the option to modify the message security, apply rights protection, and then select the protection template or Do Not Forward option.

You can also configure mail flow rules to do the reverse mapping. When an Azure Information Protection label is detected, set a corresponding Exchange message classification:

- For each Azure Information Protection label: Create a mail flow rule that is applied when the **msip\_labels** header includes the name of your label (for example, **General**), and apply a message classification that maps to this label.

## Next steps

Now that you've customized the Azure Information Protection client, see the following resources for additional information that you might need to support this client:

- [Client files and usage logging](#)
- [Document tracking](#)

- File types supported
- PowerShell commands

# Admin Guide: Azure Information Protection client files and client usage logging

7/20/2020 • 2 minutes to read • [Edit Online](#)

*Applies to:* Active Directory Rights Management Services, [Azure Information Protection](#), Windows 10, Windows 8.1, Windows 8, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

*Instructions for:* [Azure Information Protection client for Windows](#)

## NOTE

To provide a unified and streamlined customer experience, **Azure Information Protection client (classic)** and **Label Management** in the Azure Portal are being **deprecated** as of **March 31, 2021**. This time-frame allows all current Azure Information Protection customers to transition to our unified labeling solution using the Microsoft Information Protection Unified Labeling platform. Learn more in the official [deprecation notice](#).

After you have installed the Azure Information Protection client, you might need to know where files are located and monitor how the client is being used.

## File locations for the Azure Information Protection client

Client files:

- For 64-bit operating systems: \ProgramFiles (x86)\Microsoft Azure Information Protection
- For 32-bit operating systems: \Program Files\Microsoft Azure Information Protection

Client logs files and currently installed policy file:

- For 64-bit and 32-bit operating systems: %localappdata%\Microsoft\MSIP

## Usage logging for the Azure Information Protection client

The client logs user activity to the local Windows event log **Applications and Services Logs > Azure Information Protection**. The events include the following information:

- Client version, policy ID
- IP addresses of the signed in user
- File name and location
- Action:
  - Set label: Information ID 101
  - Set label (lower): Information ID 101
  - Set label (higher): Information ID 101
  - Remove label: Information ID 104

- Recommended label tooltip: Information 105
  - Apply custom protection: Information ID 201
  - Remove custom protection: Information ID 202
  - Outlook warn message: Information ID 301
  - Outlook justify message: Information ID 302
  - Outlook block message: Information ID 303
  - Sign in (operational): Information ID 902
  - Download policy (operational): Information ID 901
- Action source:
    - Manual
    - Recommended
    - Automatic
    - System (for sign in and download policy)
    - Default
  - Label before and after action
  - Protection before and after action
  - User justification (when applicable)
  - Custom permissions (when applicable) that includes the [usage rights by their encoding name](#) for the specified users, groups, or organizations

The events for Outlook warn, justify, and block messages require advanced client settings. For more information, see [Implement pop-up messages in Outlook that warn, justify, or block emails being sent](#).

## Next steps

Now that you've identified all the log files associated with the Azure Information Protection client, see the following for additional information that you might need to support this client:

- [Customizations](#)
- [Document tracking](#)
- [File types supported](#)
- [PowerShell commands](#)

# Admin Guide: Configuring and using document tracking for Azure Information Protection

7/20/2020 • 6 minutes to read • [Edit Online](#)

*Applies to:* [Azure Information Protection](#), Windows 10, Windows 8.1, Windows 8, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

*Instructions for:* [Azure Information Protection client for Windows](#)

## NOTE

To provide a unified and streamlined customer experience, Azure Information Protection client (classic) and Label Management in the Azure Portal are being **deprecated** as of **March 31, 2021**. This time-frame allows all current Azure Information Protection customers to transition to our unified labeling solution using the Microsoft Information Protection Unified Labeling platform. Learn more in the official [deprecation notice](#).

If you have a [subscription that supports document tracking](#), the document tracking site is enabled by default for all users in your organization. Document tracking provides information for users and administrators about when a protected document was accessed and if necessary, a tracked document can be revoked.

## Using PowerShell to manage the document tracking site

The following sections contain information about how you can manage the document tracking site by using PowerShell. For installation instructions for the PowerShell module, see [Installing the AIPService PowerShell module](#).

For more information about each of the cmdlets, use the links provided.

### Privacy controls for your document tracking site

If displaying all document tracking information is prohibited in your organization because of privacy requirements, you can disable document tracking by using the [Disable-AipServiceDocumentTrackingFeature](#) cmdlet.

This cmdlet disables access to the document tracking site so that all users in your organization cannot track or revoke access to documents that they have protected. You can re-enable document tracking any time, by using the [Enable-AipServiceDocumentTrackingFeature](#), and you can check whether document tracking is currently enabled or disabled by using [Get-AipServiceDocumentTrackingFeature](#).

When the document tracking site is enabled, by default, it shows information such as the email addresses of the people who attempted to access the protected documents, when these people tried to access them, and their location. This level of information can be helpful to determine how the shared documents are used and whether they should be revoked if suspicious activity is seen. However, for privacy reasons, you might need to disable this user information for some or all users.

If you have users who should not have this activity tracked by other users, add them to a group that is stored in Azure AD, and specify this group with the [Set-AipServiceDoNotTrackUserGroup](#) cmdlet. When you run this cmdlet, you must specify a single group. However, the group can contain nested groups.

For these group members, users cannot see any activity on the document tracking site when that activity is related to documents that they shared with them. In addition, no email notifications are sent to the user who

shared the document.

When you use this configuration, all users can still use the document tracking site and revoke access to documents that they have protected. However, they do not see activity for the users who you have specified by using the Set-AipServiceDoNotTrackUserGroup cmdlet.

This setting affects end users only. Administrators for Azure Information Protection can always track activities of all users, even when those users are specified by using Set-AipServiceDoNotTrackUserGroup. For more information about how administrators can track documents for users, see the [Tracking and revoking documents for users](#) section.

### Logging information from the document tracking site

You can use the following cmdlets to download logging information from the document tracking site:

- [Get-AipServiceTrackingLog](#)

This cmdlet returns tracking information about protected documents for a specified user who protected documents (the Rights Management issuer) or who accessed protected documents. Use this cmdlet to help answer the question "Which protected documents did a specified user track or access?"

- [Get-AipServiceDocumentLog](#)

This cmdlet returns protection information about the tracked documents for a specified user if that user protected documents (the Rights Management issuer) or was the Rights Management owner for documents, or protected documents were configured to grant access directly to the user. Use this cmdlet to help answer the question "How are documents protected for a specified user?"

## Destination URLs used by the document tracking site

The following URLs are used for document tracking and must be allowed on all devices and services between the clients that run the Azure Information Protection client and the internet. For example, add these URLs to firewalls, or to your Trusted Sites if you're using Internet Explorer with Enhanced Security.

- `https://*.azurerms.com`
- `https://*.microsoftonline.com`
- `https://*.microsoftonline-p.com`
- `https://ecn.dev.virtualearth.net`

These URLs are standard for the Azure Rights Management service, with the exception of the virtualearth.net URL that is used for Bing maps to display the user location.

## Tracking and revoking documents for users

When users sign in to the document tracking site, they can track and revoke documents that they have protected by using the Azure Information Protection client. When you sign in as an Azure AD global administrator for your tenant, you can click the Admin icon, which switches to Administrator mode. Other administrator roles do not support this mode for the document tracking site.



The Administrator mode lets you see the documents that users in your organization have selected to track by using the Azure Information Protection client.

#### NOTE

If you do not see this icon, despite being a global administrator, it's because you haven't yet shared any documents yourself. In this case, use the following URL to access the document tracking site: <https://portal.azure.com/#/admin>

Actions that you take in Administrator mode are audited and logged in the usage log files, and you must confirm to continue. For more information about this logging, see the next section.

When you are in Administrator mode, you can then search by user or document. If you search by user, you see all the documents that the specified user has selected to track by using the Azure Information Protection client.

If you search by document, you see all the users in your organization who tracked that document by using the Azure Information Protection client. You can then drill into the search results to track the documents that users have protected and revoke these documents, if necessary.

To leave the Administrator mode, click X next to **Exit administrator mode**:



For instructions how to use the document tracking site, see [Track and revoke your documents](#) from the user guide.

#### Using PowerShell to register labeled documents with the document tracking site

To be able to track and revoke a document, it must first be registered with the document tracking site. This action occurs when users select the **Track and revoke** option from File Explorer or their Office apps when they use the Azure Information Protection client.

If you label and protect files for users by using the `Set-AIPFileLabel` cmdlet, you can use the `EnableTracking` parameter to register the file with the document tracking site. For example:

```
Set-AIPFileLabel -Path C:\Projects\ -LabelId ade72bf1-4714-4714-4714-a325f824c55a -EnableTracking
```

## Usage logging for the document tracking site

Two fields in the usage log files are applicable to document tracking: **AdminAction** and **ActingAsUser**.

**AdminAction** - This field has a value of true when an administrator uses the document tracking site in Administrator mode, for example, to revoke a document on a user's behalf or to see when it was shared. This field is empty when a user signs in to the document tracking site.

**ActingAsUser** - When the AdminAction field is true, this field contains the user name that the administrator is acting on behalf of as the searched for user or document owner. This field is empty when a user signs in to the document tracking site.

There are also request types that log how users and administrators are using the document tracking site. For example, **RevokeAccess** is the request type when a user or an administrator on behalf of a user has revoked a document in the document tracking site. Use this request type in combination with the AdminAction field to determine whether the user revoked their own document (the AdminAction field is empty) or an administrator revoked a document on behalf of a user (the AdminAction is true).

For more information about usage logging, see [Logging and analyzing the protection usage from Azure Information Protection](#)

## Next steps

Now that you've configured the document tracking site for the Azure Information Protection client, see the following for additional information that you might need to support this client:

- [Customizations](#)
- [Client files and usage logging](#)
- [File types supported](#)
- [PowerShell commands](#)

# Admin Guide: File types supported by the Azure Information Protection client

7/20/2020 • 15 minutes to read • [Edit Online](#)

*Applies to:* Active Directory Rights Management Services, [Azure Information Protection](#), Windows 10, Windows 8.1, Windows 8, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

*Instructions for:* [Azure Information Protection client for Windows](#)

## NOTE

To provide a unified and streamlined customer experience, **Azure Information Protection client (classic)** and **Label Management** in the Azure Portal are being **deprecated** as of **March 31, 2021**. This time-frame allows all current Azure Information Protection customers to transition to our unified labeling solution using the Microsoft Information Protection Unified Labeling platform. Learn more in the official [deprecation notice](#).

The Azure Information Protection client can apply the following to documents and emails:

- Classification only
- Classification and protection
- Protection only

The Azure Information Protection client can also inspect the content of some file types using well-known sensitive information types or regular expressions that you define.

Use the following information to check which file types the Azure Information Protection client supports, understand the different levels of protection and how to change the default protection level, and to identify which files are automatically excluded (skipped) from classification and protection.

For the listed file types, WebDav locations are not supported.

## File types supported for classification only

The following file types can be classified even when they are not protected.

- **Adobe Portable Document Format:** .pdf
- **Microsoft Project:** .mpp, .mpt
- **Microsoft Publisher:** .pub
- **Microsoft XPS:** .xps .oxps
- **Images:** jpg, jpe, jpeg, jif, jfif, jfi, png, .tif, .tiff
- **Autodesk Design Review 2013:** .dwfx
- **Adobe Photoshop:** .psd
- **Digital Negative:** .dng

- **Microsoft Office:** File types in the following table.

The supported file formats for these file types are the 97-2003 file formats and Office Open XML formats for the following Office programs: Word, Excel, and PowerPoint.

OFFICE FILE TYPE	OFFICE FILE TYPE
.doc	.vsdm
.docm	.vsdx
.docx	.vss
.dot	.vssm
.dotm	.vst
.dotx	.vstm
.potm	.vssx
.potx	.vstx
.pps	.xls
.ppsm	.xlsb
.ppsx	.xlt
.ppt	.xlsm
.pptm	.xlsx
.pptx	.xltm
.vdw	.xltx
.vsd	

Additional file types support classification when they are also protected. For these file types, see the [Supported file types for classification and protection](#) section.

For example, in the current [default policy](#), the **General** label applies classification and does not apply protection. You could apply the **General** label to a file named sales.pdf but you could not apply this label to a file named sales.txt.

Also in the current default policy, the **Confidential \ All Employees** applies classification and protection. You could apply this label to a file named sales.pdf and a file named sales.txt. You could also apply just protection to these files, without classification.

## File types supported for protection

The Azure Information Protection client supports protection at two different levels, as described in the following table.

TYPE OF PROTECTION	NATIVE	GENERIC
--------------------	--------	---------

Type of protection	Native	Generic
Description	For text, image, Microsoft Office (Word, Excel, PowerPoint) files, .pdf files, and other application file types that support a Rights Management service, native protection provides a strong level of protection that includes both encryption and enforcement of rights (permissions).	For all other applications and file types, generic protection provides a level of protection that includes both file encapsulation using the .pfile file type and authentication to verify if a user is authorized to open the file.
Protection	<p>Files protection is enforced in the following ways:</p> <ul style="list-style-type: none"> <li>- Before protected content is rendered, successful authentication must occur for those who receive the file through email or are given access to it through file or share permissions.</li> <li>- Additionally, usage rights and policy that were set by the content owner when the files were protected are enforced when the content is rendered in either the Azure Information Protection viewer (for protected text and image files) or the associated application (for all other supported file types).</li> </ul>	<p>File protection is enforced in the following ways:</p> <ul style="list-style-type: none"> <li>- Before protected content is rendered, successful authentication must occur for people who are authorized to open the file and given access to it. If authorization fails, the file does not open.</li> <li>- Usage rights and policy set by the content owner are displayed to inform authorized users of the intended usage policy.</li> <li>- Audit logging of authorized users opening and accessing files occurs. However, usage rights are not enforced.</li> </ul>
Default for file types	<p>This is the default level of protection for the following file types:</p> <ul style="list-style-type: none"> <li>- Text and image files</li> <li>- Microsoft Office (Word, Excel, PowerPoint) files</li> <li>- Portable document format (.pdf)</li> </ul> <p>For more information, see the following section, <a href="#">Supported file types for classification and protection</a>.</p>	This is the default protection for all other file types (such as .vsdx, .rtf, and so on) that are not supported by native protection.

You can change the default protection level that the Azure Information Protection client applies. You can change the default level of native to generic, from generic to native, and even prevent the Azure Information Protection client from applying protection. For more information, see the [Changing the default protection level of files](#) section in this article.

The data protection can be applied automatically when a user selects a label that an administrator has configured, or users can specify their own custom protection settings by using [permission levels](#).

### File sizes supported for protection

There are maximum file sizes that the Azure Information Protection client supports for protection.

- For Office files:

OFFICE APPLICATION	MAXIMUM FILE SIZE SUPPORTED
Word 2007 (supported by AD RMS only)	32-bit: 512 MB
Word 2010	64-bit: 512 MB
Word 2013	
Word 2016	
Excel 2007 (supported by AD RMS only)	32-bit: 2 GB
Excel 2010	64-bit: Limited only by available disk space and memory
Excel 2013	
Excel 2016	
PowerPoint 2007 (supported by AD RMS only)	32-bit: Limited only by available disk space and memory
PowerPoint 2010	64-bit: Limited only by available disk space and memory
PowerPoint 2013	
PowerPoint 2016	

- **For all other files:**

- To protect other file types, and to open these file types in the Azure Information Protection viewer: The maximum file size is limited only by available disk space and memory.
- To unprotect files by using the [Unprotect-RMSFile](#) cmdlet: The maximum file size supported for .pst files is 5 GB. Other file types are limited only by available disk space and memory

Tip: If you need to search or recover protected items in large .pst files, see [Guidance for using Unprotect-RMSFile for eDiscovery](#).

### Supported file types for classification and protection

The following table lists a subset of file types that support native protection by the Azure Information Protection client, and that can also be classified.

These file types are identified separately because when they are natively protected, the original file name extension is changed, and these files become read-only. Note that when files are generically protected, the original file name extension is always changed to .pfile.

#### WARNING

If you have firewalls, web proxies, or security software that inspect and take action according to file name extensions, you might need to reconfigure these network devices and software to support these new file name extensions.

ORIGINAL FILE NAME EXTENSION	PROTECTED FILE NAME EXTENSION
.txt	.ptxt
.xml	.pxml
.jpg	.pjpg

ORIGINAL FILE NAME EXTENSION	PROTECTED FILE NAME EXTENSION
.jpeg	.pjpeg
.pdf	.ppdf [1]
.png	.ppng
.tif	.ptif
.tiff	.ptiff
.bmp	.pbmp
.gif	.pgif
.jpe	.pjpe
.jfif	.pjfif
.jt	.pjt

Footnote 1

With the latest version of the Azure Information Protection client, [by default](#), the file name extension of the protected PDF document remains as .pdf.

The next table lists the remaining file types that support native protection by the Azure Information Protection client, and that can also be classified. You will recognize these as file types for Microsoft Office apps. The supported file formats for these file types are the 97-2003 file formats and Office Open XML formats for the following Office programs: Word, Excel, and PowerPoint.

For these files, the file name extension remains the same after the file is protected by a Rights Management service.

FILE TYPES SUPPORTED BY OFFICE	FILE TYPES SUPPORTED BY OFFICE
.doc	.vsdx
.docm	.vssm
.docx	.vssx
.dot	.vstm
.dotm	.vstx
.dotx	.xla
.potm	.xlam
.potx	.xls
.pps	.xlsb
.ppsm	.xlt
.ppsx	.xlsm
.ppt	.xlsx
.pptm	.xltm
.pptx	.xltx
.vsdm	.xps

### Changing the default protection level of files

You can change how the Azure Information Protection client protects files by editing the registry. For example, you can force files that support native protection to be generically protected by the Azure Information Protection client.

Reasons for why you might want to do this:

- To ensure that all users can open the file if they don't have an application that supports native protection.
- To accommodate security systems that take action on files by their file name extension and can be reconfigured to accommodate the .pfile file name extension but cannot be reconfigured to accommodate multiple file name extensions for native protection.

Similarly, you can force the Azure Information Protection client to apply native protection to files that by default, would have generic protection applied. This action might be appropriate if you have an application that supports the RMS APIs. For example, a line-of-business application written by your internal developers or an application purchased from an independent software vendor (ISV).

You can also force the Azure Information Protection client to block the protection of files (not apply native protection or generic protection). For example, this action might be required if you have an automated application or service that must be able to open a specific file to process its contents. When you block protection for a file type, users cannot use the Azure Information Protection client to protect a file that has that file type. When they try, they see a message that the administrator has prevented protection and they must cancel their action to protect the file.

To configure the Azure Information Protection client to apply generic protection to all files that by default, would have native protection applied, make the following registry edits. Note if the FileProtection key does not exist, you must manually create it.

1. Create a new key named \* for the following registry path, which denotes files with any file name extension:
  - For 32-bit version of Windows:  
`HKEY_LOCAL_MACHINE\Software\Microsoft\MSIPC\FileProtection`
  - For 64-bit version of Windows:  
`HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\MSIPC\FileProtection`  
and `HKEY_LOCAL_MACHINE\Software\Microsoft\MSIPC\FileProtection`
2. In the newly added key (for example, `HKEY_LOCAL_MACHINE\Software\Microsoft\MSIPC\FileProtection\*`), create a new string value (REG\_SZ) named **Encryption** that has the data value of **Pfile**.

This setting results in the Azure Information Protection client applying generic protection.

These two settings result in the Azure Information Protection client applying generic protection to all files that have a file name extension. If this is your goal, no further configuration is required. However, you can define exceptions for specific file types, so that they are still natively protected. To do this, you must make three (for 32-bit Windows) or 6 (for 64-bit Windows) additional registry edits for each file type:

1. For `HKEY_LOCAL_MACHINE\Software\Microsoft\MSIPC\FileProtection` and `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\MSIPC\FileProtection` (if applicable): Add a new key that has the name of the file name extension (without the preceding period).

For example, for files that have a .docx file name extension, create a key named **DOCX**.

2. In the newly added file type key (for example, `HKEY_LOCAL_MACHINE\Software\Microsoft\MSIPC\FileProtection\DOCX`), create a new DWORD Value named **AllowPFILEEncryption** that has a value of 0.
3. In the newly added file type key (for example, `HKEY_LOCAL_MACHINE\Software\Microsoft\MSIPC\FileProtection\DOCX`), create a new String Value named **Encryption** that has a value of **Native**.

As a result of these settings, all files are generically protected except files that have a .docx file name extension. These files are natively protected by the Azure Information Protection client.

Repeat these three steps for other file types that you want to define as exceptions because they support native protection and you do not want them to be generically protected by the Azure Information Protection client.

You can make similar registry edits for other scenarios by changing the value of the **Encryption** string that supports the following values:

- **Pfile**: Generic protection
- **Native**: Native protection
- **Off**: Block protection

After making these registry changes, there's no need to restart the computer. However, if you're using PowerShell commands to protect files, you must start a new PowerShell session for the changes to take effect.

For more information about editing the registry to change the default protection level of files, see [File API configuration](#) from the developer guidance. In this documentation for developers, generic protection is referred to as "PFile".

## File types that are excluded from classification and protection

To help prevent users from changing files that are critical for computer operations, some file types and folders are automatically excluded from classification and protection. If users try to classify or protect these files by using the Azure Information Protection client, they see a message that they are excluded.

- **Excluded file types:** .lnk, .exe, .com, .cmd, .bat, .dll, .ini, .pst, .sca, .drm, .sys, .cpl, .inf, .drv, .dat, .tmp, .msg, .msp, .msi, .pdb, .jar
- **Excluded folders:**
  - Windows
  - Program Files (\Program Files and \Program Files (x86))
  - \ProgramData
  - \AppData (for all users)

### **File types that are excluded from classification and protection by the Azure Information Protection scanner**

By default, the scanner also excludes the same file types as the Azure Information Protection client with the following exceptions:

- .rtf, and .rar, are also excluded

You can change the file types included or excluded for file inspection by the scanner:

- Configure **File types to scan** in the scanner profile, [using the Azure portal](#).

#### **NOTE**

If you include .rtf files for scanning, carefully monitor the scanner. Some .rtf files cannot be successfully inspected by the scanner and for these files, the inspection doesn't complete and the service must be restarted.

By default, the scanner protects only Office file types, and PDF files when they are protected by using the ISO standard for PDF encryption. To change this behavior for the scanner, edit the registry and specify the additional file types that you want to be protected. For instructions, see [Use the registry to change which file types are protected](#) from the scanner deployment instructions.

### **Files that cannot be protected by default**

Any file that is password-protected cannot be natively protected by the Azure Information Protection client unless the file is currently open in the application that applies the protection. You most often see PDF files that are password-protected but other applications, such as Office apps, also offer this functionality.

If you change the [default behavior](#) of the Azure Information Protection client so that it protects PDF files with a .ppdf file name extension, the client cannot natively protect or unprotect PDF files in either of the following circumstances:

- A PDF file that is form-based.
- A protected PDF file that has a .pdf file name extension.

The Azure Information Protection client can protect an unprotected PDF file, and it can unprotect and reprotect a protected PDF file when it has a .ppdf file name extension.

### **Limitations for container files, such as .zip files**

Container files are files that include other files, with a typical example being .zip files that contain compressed files. Other examples include .rar, .7z, .msg files, and PDF documents that include attachments.

You can classify and protect these container files, but the classification and protection is not applied to each file inside the container.

If you have a container file that includes classified and protected files, you must first extract the files to change their classification or protection settings. However, you can remove the protection for all files in supported container files by using the [Unprotect-RMSFile](#) cmdlet.

The Azure Information Protection viewer cannot open attachments in a protected PDF document. In this scenario, when the document is opened in the viewer, the attachments are not visible.

## File types supported for inspection

Without any additional configuration, the Azure Information Protection client uses Windows IFilter to inspect the contents of documents. Windows IFilter is used by Windows Search for indexing. As a result, the following file types can be inspected when you use the [Azure Information Protection scanner](#), or the [Set-AIPFileClassification](#) PowerShell command.

APPLICATION TYPE	FILE TYPE
Word	.doc; .docx; .docm; .dot; .dotm; .dotx
Excel	.xls; .xlt; .xlsx; .xltx; .xltm; .xlsm; .xlsb
PowerPoint	.ppt; .pps; .pot; .pptx; .ppsx; .pptm; .ppsm; .potx; .potm
PDF	.pdf
Text	.txt; .xml; .csv

With additional configuration, other file types can also be inspected. For example, you can [register a custom file name extension to use the existing Windows filter handler for text files](#), and you can install additional filters from software vendors.

To check what filters are installed, see the [Finding a Filter Handler for a Given File Extension](#) section from the Windows Search Developer's Guide.

The following sections have configuration instructions to inspect .zip files, and .tiff files.

### To inspect .zip files

The Azure Information Protection scanner and the [Set-AIPFileClassification](#) PowerShell command can inspect .zip files when you follow these instructions:

1. For the computer running the scanner or the PowerShell session, install the [Office 2010 Filter Pack SP2](#).
2. For the scanner: After finding sensitive information, if the .zip file should be classified and protected with a label, add a registry entry for this file name extension to have generic protection (pfile), as described in [Use the registry to change which file types are protected](#) from the scanner deployment instructions.

Example scenario after doing these steps:

A file named **accounts.zip** contains Excel spreadsheets with credit card numbers. Your Azure Information Protection policy has a label named **Confidential \ Finance**, which is configured to discover credit card numbers, and automatically apply the label with protection that restricts access to the Finance group.

After inspecting the file, the scanner classifies this file as **Confidential \ Finance**, applies generic protection to the file so that only members of the Finance groups can unzip it, and renames the file **accounts.zip.pfile**.

### To inspect .tiff files by using OCR

The Azure Information Protection scanner and the [Set-AIPFileClassification](#) PowerShell command can use optical

character recognition (OCR) to inspect TIFF images with a .tiff file name extension when you install the Windows TIFF IFilter feature, and then configure [Windows TIFF IFilter Settings](#) on the computer running the scanner or the PowerShell session.

For the scanner: After finding sensitive information, if the .tiff file should be classified and protected with a label, add a registry entry for this file name extension to have native protection, as described in [Use the registry to change which file types are protected](#) from the scanner deployment instructions.

## Next steps

Now that you've identified the file types supported by the Azure Information Protection client, see the following resources for additional information that you might need to support this client:

- [Customizations](#)
- [Client files and usage logging](#)
- [Document tracking](#)
- [PowerShell commands](#)

# Admin Guide: Using PowerShell with the Azure Information Protection client

7/20/2020 • 25 minutes to read • [Edit Online](#)

*Applies to: Active Directory Rights Management Services, Azure Information Protection, Windows 10, Windows 8.1, Windows 8, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012*

*Instructions for: Azure Information Protection client for Windows*

## NOTE

To provide a unified and streamlined customer experience, **Azure Information Protection client (classic)** and **Label Management** in the Azure Portal are being **deprecated** as of **March 31, 2021**. This time-frame allows all current Azure Information Protection customers to transition to our unified labeling solution using the Microsoft Information Protection Unified Labeling platform. Learn more in the official [deprecation notice](#).

When you install the Azure Information Protection client, PowerShell commands are automatically installed. This lets you manage the client by running commands that you can put into scripts for automation.

The cmdlets are installed with the PowerShell module **AzureInformationProtection**. This module includes all the Rights Management cmdlets from the RMS Protection Tool (no longer supported). There are also cmdlets that use Azure Information Protection for labeling. For example:

LABELING CMDLET	EXAMPLE USAGE
<a href="#">Get-AIPFileStatus</a>	For a shared folder, identify all files with a specific label.
<a href="#">Set-AIPFileClassification</a>	For a shared folder, inspect the file contents and then automatically label unlabeled files, according to the conditions that you have specified.
<a href="#">Set-AIPFileLabel</a>	For a shared folder, apply a specified label to all files that do not have a label.
<a href="#">Set-AIPAuthentication</a>	Label files non-interactively, for example by using a script that runs on a schedule.

## TIP

To use cmdlets with path lengths greater than 260 characters, use the following [group policy setting](#) that is available starting Windows 10, version 1607:

**Local Computer Policy > Computer Configuration > Administrative Templates > All Settings > Enable Win32 long paths**

For Windows Server 2016, you can use the same group policy setting when you install the latest Administrative Templates (.admx) for Windows 10.

For more information, see the [Maximum Path Length Limitation](#) section from the Windows 10 developer documentation.

The [Azure Information Protection scanner](#) uses cmdlets from the AzureInformationProtection module to install and configure a service on Windows Server. This scanner then lets you discover, classify, and protect files on data stores.

For a list of all the cmdlets and their corresponding help, see [AzureInformationProtection Module](#). Within a PowerShell session, type `Get-Help <cmdlet name> -online` to see the latest help.

This module installs in `\ProgramFiles (x86)\Microsoft Azure Information Protection` and adds this folder to the **PSModulePath** system variable. The .dll for this module is named **AIP.dll**.

Currently, if you install the module as one user and run the cmdlets on the same computer as another user, you must first run the `Import-Module AzureInformationProtection` command. In this scenario, the module doesn't autoload when you first run a cmdlet.

The current release of the AzureInformationProtection module has the following limitations:

- You can unprotect Outlook personal folders (.pst files), but you cannot currently natively protect these files or other container files by using this PowerShell module.
- You can unprotect Outlook protected email messages (.rpmsg files) when they are in an Outlook personal folder (.pst), but you cannot unprotect .rpmsg files outside a personal folder.

Before you start to use these cmdlets, see the additional prerequisites and instructions that corresponds to your deployment:

- [Azure Information Protection and Azure Rights Management service](#)
  - Applicable if you use classification-only or classification with Rights Management protection: You have a subscription that includes Azure Information Protection (for example, Enterprise Mobility + Security).
  - Applicable if you use protection-only with the Azure Rights Management service: You have a subscription that includes the Azure Rights Management service (for example, Office 365 E3 and Office 365 E5).
- [Active Directory Rights Management Services](#)
  - Applicable if you use protection-only with the on-premises version of Azure Rights Management; Active Directory Rights Management Services (AD RMS).

## Azure Information Protection and Azure Rights Management service

Read this section before you start using the PowerShell commands when your organization uses Azure Information Protection for classification and protection, or just the Azure Rights Management service for data protection.

### Prerequisites

In addition to the prerequisites for installing the AzureInformationProtection module, there are additional prerequisites for Azure Information Protection labeling and the Azure Rights Management data protection service:

1. The Azure Rights Management service must be activated.
2. To remove protection from files for others using your own account:
  - The super user feature must be enabled for your organization and your account must be configured to be a super user for Azure Rights Management.
3. To directly protect or unprotect files without user interaction:
  - Create a service principal account, run `Set-RMSServerAuthentication`, and consider making this

service principal a super user for Azure Rights Management.

4. For regions outside North America:

- Edit the registry for service discovery.

**Prerequisite 1: The Azure Rights Management service must be activated**

This prerequisite applies whether you apply the data protection by using labels or by directly connecting to the Azure Rights Management service to apply the data protection.

If your Azure Information Protection tenant is not activated, see the instructions for [Activating the protection service from Azure Information Protection](#).

**Prerequisite 2: To remove protection from files for others using your own account**

Typical scenarios for removing protection from files for others include data discovery or data recovery. If you are using labels to apply the protection, you could remove the protection by setting a new label that doesn't apply protection or by removing the label. But you will more likely connect directly to the Azure Rights Management service to remove the protection.

You must have a Rights Management usage right to remove protection from files, or be a super user. For data discovery or data recovery, the super user feature is typically used. To enable this feature and configure your account to be a super user, see [Configuring super users for Azure Rights Management and Discovery Services or Data Recovery](#).

**Prerequisite 3: To protect or unprotect files without user interaction**

You can connect directly to the Azure Rights Management service non-interactively to protect or unprotect files.

You must use a service principal account to connect to the Azure Rights Management service non-interactively, which you do by using the `Set-RMServerAuthentication` cmdlet. You must do this for each Windows PowerShell session that runs cmdlets that directly connect to the Azure Rights Management service. Before you run this cmdlet, you must have these three identifiers:

- `BposTenantId`
- `AppPrincipalId`
- Symmetric Key

You can use the following PowerShell commands and commented instructions to automatically get the values for the identifiers and run the `Set-RMServerAuthentication` cmdlet. Or, you can manually get and specify the values.

To automatically get the values and run `Set-RMServerAuthentication`:

```
Make sure that you have the AIPService and MSOnline modules installed

$ServicePrincipalName=<new service principal name>
Connect-AipService
$bposTenantID=(Get-AipServiceConfiguration).BPOSID
Disconnect-AipService
Connect-MsolService
New-MsolServicePrincipal -DisplayName $ServicePrincipalName

Copy the value of the generated symmetric key

$symmetricKey=<value from the display of the New-MsolServicePrincipal command>
$appPrincipalID=(Get-MsolServicePrincipal | Where { $_.DisplayName -eq $ServicePrincipalName }).AppPrincipalID
Set-RMServerAuthentication -Key $symmetricKey -AppPrincipalID $appPrincipalID -BposTenantID
$bposTenantID
```

The next sections explain how to manually get and specify these values, with more information about each one.

To get the `BposTenantId`

Run the `Get-AipServiceConfiguration` cmdlet from the Azure RMS Windows PowerShell module:

1. If this module is not already installed on your computer, see [Installing the AIPService PowerShell module](#).
2. Start Windows PowerShell with the **Run as Administrator** option.
3. Use the `Connect-AipService` cmdlet to connect to the Azure Rights Management service:

```
Connect-AipService
```

When prompted, enter your Azure Information Protection tenant administrator credentials. Typically, you use an account that is a global administrator for Azure Active Directory or Office 365.

4. Run `Get-AipServiceConfiguration` and make a copy of the `BPOSId` value.

An example of output from `Get-AipServiceConfiguration`:

```
BPOSId : 23976bc6-dcd4-4173-9d96-dad1f48efd42
RightsManagement ServiceId : 1a302373-f233-440600909-4cdf305e2e76
LicensingIntranetDistributionPointUrl : https://1s302373-f233-4406-9090-4cdf305e2e76.rms.na.aadrm.com/_wmcs/licensing
LicensingExtranetDistributionPointUrl : https://1s302373-f233-4406-9090-4cdf305e2e76.rms.na.aadrm.com/_wmcs/licensing
CertificationIntranetDistributionPointUrl: https://1s302373-f233-4406-9090-4cdf305e2e76.rms.na.aadrm.com/_wmcs/certification
CertificationExtranetDistributionPointUrl: https://1s302373-f233-4406-9090-4cdf305e2e76.rms.na.aadrm.com/_wmcs/certification
```

5. Disconnect from the service:

```
Disconnect-AipService
```

To get the `AppPrincipalId` and `Symmetric Key`

Create a new service principal by running the `New-MsolServicePrincipal` cmdlet from the MSOnline PowerShell module for Azure Active Directory and use the following instructions.

**IMPORTANT**

Do not use the newer Azure AD PowerShell cmdlet, `New-AzureADServicePrincipal`, to create this service principal. The Azure Rights Management service does not support `New-AzureADServicePrincipal`.

1. If the MSOnline module is not already installed on your computer, run `Install-Module MSOnline`.
2. Start Windows PowerShell with the **Run as Administrator** option.
3. Use the `Connect-MsolService` cmdlet to connect to Azure AD:

```
Connect-MsolService
```

When prompted, enter your Azure AD tenant administrator credentials (typically, you use an account that is a global administrator for Azure Active Directory or Office 365).

- Run the New-MsolServicePrincipal cmdlet to create a new service principal:

```
New-MsolServicePrincipal
```

When prompted, enter your choice of a display name for this service principal that helps you to identify its purpose later as an account for you to connect to the Azure Rights Management service so that you can protect and unprotect files.

An example of the output of New-MsolServicePrincipal:

```
Supply values for the following parameters:
```

```
DisplayName: AzureRMSProtectionServicePrincipal
The following symmetric key was created as one was not supplied
zIeMu8zNJ6U377CLtppkhkb14gjodmYSXUVwAO5ycgA=
```

```
Display Name: AzureRMSProtectionServicePrincipal
ServicePrincipalNames: (b5e3f7g1-b5c2-4c96-a594-a0807f65bba4)
ObjectId: 23720996-593c-4122-bfc7-1abb5a0b5109
AppPrincialId: b5e3f76a-b5c2-4c96-a594-a0807f65bba4
TrustedForDelegation: False
AccountEnabled: True
Addresses: ()
KeyType: Symmetric
KeyId: 8ef61651-ca11-48ea-a350-25834a1ba17c
StartDate: 3/7/2014 4:43:59 AM
EndDate: 3/7/2014 4:43:59 AM
Usage: Verify
```

- From this output, make a note of the symmetric key and the AppPrincialId.

It is important that you make a copy of this symmetric key, now. You cannot retrieve this key later, so if you do not know it when you next need to authenticate to the Azure Rights Management service, you will have to create a new service principal.

From these instructions and our examples, we have the three identifiers required to run Set-RMSServerAuthentication:

- Tenant Id: **23976bc6-dcd4-4173-9d96-dad1f48efd42**
- Symmetric key: **zIeMu8zNJ6U377CLtppkhkb14gjodmYSXUVwAO5ycgA=**
- AppPrincialId: **b5e3f76a-b5c2-4c96-a594-a0807f65bba4**

Our example command would then look like the following:

```
Set-RMSServerAuthentication -Key zIeMu8zNJ6U377CLtppkhkb14gjodmYSXUVwAO5ycgA=-AppPrincipialId b5e3f76a-b5c2-4c96-a594-a0807f65bba4-BposTenantId 23976bc6-dcd4-4173-9d96-dad1f48efd42
```

As shown in the previous command, you can supply the values with a single command, which you would do in a script to run non-interactively. But for testing purposes, you can just type Set-RMSServerAuthentication, and supply the values one-by-one when prompted. When the command completes, the client is now operating in "server mode", which is suitable for non-interactive use such as scripts and Windows Server File

## Classification Infrastructure.

Consider making this service principal account a super user: To ensure that this service principal account can always unprotect files for others, it can be configured to be a super user. In the same way as you configure a standard user account to be a super user, you use the same Azure RMS cmdlet, [Add-AipServiceSuperUser](#), but specify the **ServicePrincipalId** parameter with your AppPrincipalId value.

For more information about super users, see [Configuring super users for Azure Information Protection and discovery services or data recovery](#).

### NOTE

To use your own account to authenticate to the Azure Rights Management service, there's no need to run Set-RMSServerAuthentication before you protect or unprotect files, or get templates.

### Prerequisite 4: For regions outside North America

When you use a service principal account to protect files and download templates outside the Azure North America region, you must edit the registry:

1. Run the Get-AipServiceConfiguration cmdlet again, and make a note of the values for **CertificationExtranetDistributionPointUrl** and **LicensingExtranetDistributionPointUrl**.
2. On each computer where you will run the AzureInformationProtection cmdlets, open the registry editor.
3. Navigate to the following path: `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSIPC\ServiceLocation`.

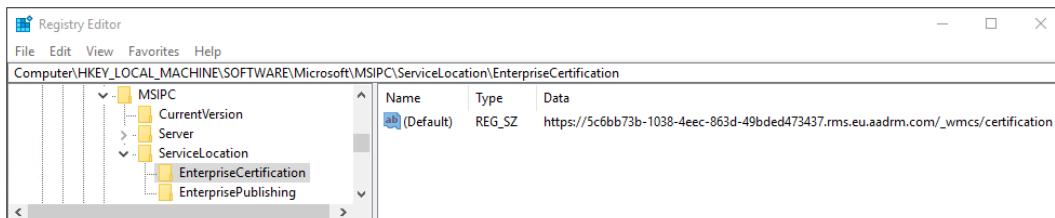
If you do not see the **MSIPC** key or **ServiceLocation** key, create them.

4. For the **ServiceLocation** key, create two keys if they do not exist, named **EnterpriseCertification** and **EnterprisePublishing**.

For the string value that's automatically created for these keys, do not change the Name of "(Default)", but edit the string to set the Value data:

- For **EnterpriseCertification**, paste your **CertificationExtranetDistributionPointUrl** value.
- For **EnterprisePublishing**, paste your **LicensingExtranetDistributionPointUrl** value.

For example, your registry entry for **EnterpriseCertification** should look similar to the following:



5. Close the registry editor. There is no need to restart your computer. However, if you are using a service principal account rather than your own user account, you must run the **Set-RMSServerAuthentication** command after making this registry edit.

### Example scenarios for using the cmdlets for Azure Information protection and the Azure Rights Management service

It's more efficient to use labels to classify and protect files, because there are just two cmdlets that you need, which can be run by themselves or together: [Get-AIPFileStatus](#) and [Set-AIPFileLabel](#). Use the help for both these cmdlets for more information and examples.

However, to protect or unprotect files by directly connecting to the Azure Rights Management service, you

must typically run a series of cmdlets as described next.

First, if you need to authenticate to the Azure Rights Management service with a service principal account rather than use your own account, in a PowerShell session, type:

```
Set-RMSServerAuthentication
```

When prompted, enter the three identifiers as described in [Prerequisite 3: To protect or unprotect files without user interaction](#).

Before you can protect files, you must download the Rights Management templates to your computer and identify which one to use and its corresponding ID number. From the output, you can then copy the template ID:

```
Get-RMSTemplate
```

Your output might look similar to the following:

```
TemplateId : {82bf3474-6efe-4fa1-8827-d1bd93339119}
CultureInfo : en-US
Description : This content is proprietary information intended for internal users only. This
content cannot be modified.
Name : Contoso, Ltd - Confidential View Only
IssuerDisplayName : Contoso, Ltd
FromTemplate : True

TemplateId : {e6ee2481-26b9-45e5-b34a-f744eacd53b0}
CultureInfo : en-US
Description : This content is proprietary information intended for internal users only. This
content can be modified but cannot be copied and printed.
Name : Contoso, Ltd - Confidential
IssuerDisplayName : Contoso, Ltd
FromTemplate : True
FromTemplate : True
```

Note that if you didn't run the Set-RMSServerAuthentication command, you are authenticated to the Azure Rights Management service by using your own user account. If you are on a domain-joined computer, your current credentials are always used automatically. If you are on a workgroup computer, you are prompted to sign in to Azure, and these credentials are then cached for subsequent commands. In this scenario, if you later need to sign in as a different user, use the `Clear-RMSAuthentication` cmdlet.

Now you know the template ID, you can use it with the `Protect-RMSFile` cmdlet to protect a single file or all files in a folder. For example, if you want to protect a single file only and overwrite the original, by using the "Contoso, Ltd - Confidential" template:

```
Protect-RMSFile -File C:\Test.docx -InPlace -TemplateId e6ee2481-26b9-45e5-b34a-f744eacd53b0
```

Your output might look similar to the following:

InputFile	EncryptedFile
-----	-----
C:\Test.docx	C:\Test.docx

To protect all files in a folder, use the `-Folder` parameter with a drive letter and path, or UNC path. For example:

```
Protect-RMSFile -Folder \\Server1\Documents -InPlace -TemplateId e6ee2481-26b9-45e5-b34a-f744eacd53b0
```

Your output might look similar to the following:

InputFile	EncryptedFile
-----	-----
\\Server1\Documents\Test1.docx	\\Server1\Documents\Test1.docx
\\Server1\Documents\Test2.docx	\\Server1\Documents\Test2.docx
\\Server1\Documents\Test3.docx	\\Server1\Documents\Test3.docx
\\Server1\Documents\Test4.docx	\\Server1\Documents\Test4.docx

When the file name extension does not change after the protection is applied, you can always use the `Get-RMSFileStatus` cmdlet later to check whether the file is protected. For example:

```
Get-RMSFileStatus -File \\Server1\Documents\Test1.docx
```

Your output might look similar to the following:

FileName	Status
-----	-----
\\Server1\Documents\Test1.docx	Protected

To unprotect a file, you must have Owner or Extract rights from when the file was protected. Or, you must run the cmdlets as a super user. Then, use the Unprotect cmdlet. For example:

```
Unprotect-RMSFile C:\\test.docx -InPlace
```

Your output might look similar to the following:

InputFile	DecryptedFile
-----	-----
C:\\Test.docx	C:\\Test.docx

Note that if the Rights Management templates are changed, you must download them again with

```
Get-RMSTemplate -force .
```

## Active Directory Rights Management Services

Read this section before you start using the PowerShell commands to protect or unprotect files when your organization uses just Active Directory Rights Management Services.

### Prerequisites

In addition to the prerequisites for installing the AzureInformationProtection module, the account used to protect or unprotect files must have Read and Execute permissions to access ServerCertification.asmx:

1. Log on to an AD RMS server.
2. Click **Start**, and then click **Computer**.
3. In File Explorer, navigate to %systemdrive%\Initpub\wwwroot\_wmsc\Certification.
4. Right-click **ServerCertification.asmx**, then click **Properties**.
5. In the **ServerCertification.asmx Properties** dialog box, click the **Security** tab.

6. Click the **Continue** button or the **Edit** button.
7. In the **Permissions for ServerCertification.asmx** dialog box, click **Add**.
8. Add your account name. If other AD RMS administrators or service accounts will also use these cmdlets to protect and unprotect files, add those accounts as well.

To protect or unprotect files non-interactively, add the relevant computer account or accounts. For example, add the computer account of the Windows Server computer that is configured for File Classification Infrastructure and will use a PowerShell script to protect files.

9. In the **Allow** column, make sure that the **Read and Execute**, and the **Read** checkboxes are selected.
10. Click **OK** twice.

### **Example scenarios for using the cmdlets for Active Directory Rights Management Services**

A typical scenario for these cmdlets is to protect all files in a folder by using a rights policy template, or to unprotect a file.

First, if you have more than one deployment of AD RMS, you need the names of your AD RMS servers, which you do by using the **Get-RMSServer** cmdlet to display a list of available servers:

```
Get-RMSServer
```

Your output might look similar to the following:

ConnectionInfo	DisplayName	AllowFromScratch
Microsoft.InformationAnd... RmsContoso		True
Microsoft.InformationAnd... RmsFabrikam		True

Before you can protect files, you need to get a list of RMS templates to identify which one to use and its corresponding ID number. Only when you have more than one AD RMS deployment do you need to specify the RMS server as well.

From the output, you can then copy the template ID:

```
Get-RMSTemplate -RMSServer RmsContoso
```

Your output might look similar to the following:

TemplateId	: {82bf3474-6efe-4fa1-8827-d1bd93339119}
CultureInfo	: en-US
Description	: This content is proprietary information intended for internal users only. This content cannot be modified.
Name	: Contoso, Ltd - Confidential View Only
IssuerDisplayName	: Contoso, Ltd
FromTemplate	: True
TemplateId	: {e6ee2481-26b9-45e5-b34a-f744eacd53b0}
CultureInfo	: en-US
Description	: This content is proprietary information intended for internal users only. This content can be modified but cannot be copied and printed.
Name	: Contoso, Ltd - Confidential
IssuerDisplayName	: Contoso, Ltd
FromTemplate	: True
FromTemplate	: True

Now you know the template ID, you can use it with the Protect-RMSFile cmdlet to protect a single file or all files in a folder. For example, if you want to protect a single file only and replace the original, by using the "Contoso, Ltd - Confidential" template:

```
Protect-RMSFile -File C:\Test.docx -InPlace -TemplateId e6ee2481-26b9-45e5-b34a-f744eacd53b0
```

Your output might look similar to the following:

InputFile	EncryptedFile
-----	-----
C:\Test.docx	C:\Test.docx

To protect all files in a folder, use the -Folder parameter with a drive letter and path, or UNC path. For example:

```
Protect-RMSFile -Folder \\Server1\Documents -InPlace -TemplateId e6ee2481-26b9-45e5-b34a-f744eacd53b0
```

Your output might look similar to the following:

InputFile	EncryptedFile
-----	-----
\\\Server1\Documents\Test1.docx	\\\Server1\Documents\Test1.docx
\\\Server1\Documents\Test2.docx	\\\Server1\Documents\Test2.docx
\\\Server1\Documents\Test3.docx	\\\Server1\Documents\Test3.docx
\\\Server1\Documents\Test4.docx	\\\Server1\Documents\Test4.docx

When the file name extension does not change after protection is applied, you can always use the Get-RMSFileStatus cmdlet later to check whether the file is protected. For example:

```
Get-RMSFileStatus -File \\Server1\Documents\Test1.docx
```

Your output might look similar to the following:

FileName	Status
-----	-----
\\Server1\Documents\Test1.docx	Protected

To unprotect a file, you must have Owner or Extract usage rights from when the file was protected, or be super user for AD RMS. Then, use the Unprotect cmdlet. For example:

```
Unprotect-RMSFile C:\test.docx -InPlace
```

Your output might look similar to the following:

InputFile	DecryptedFile
-----	-----
C:\Test.docx	C:\Test.docx

## How to label files non-interactively for Azure Information Protection

You can run the labeling cmdlets non-interactively by using the Set-AIPAuthentication cmdlet. Non-interactive operation is also required for the Azure Information Protection scanner.

By default, when you run the cmdlets for labeling, the commands run in your own user context in an interactive PowerShell session. To run them unattended, create a new Azure AD user account for this purpose. Then, in the context of that user, run the Set-AIPAuthentication cmdlet to set and store credentials by using an access token from Azure AD. This user account is then authenticated and bootstrapped for the Azure Rights Management service. The account downloads the Azure Information Protection policy and any Rights Management templates that the labels use.

**NOTE**

If you use [scoped policies](#), remember that you might need to add this account to your scoped policies.

The first time you run this cmdlet, you are prompted to sign in for Azure Information Protection. Specify the user account name and password that you created for the unattended user. After that, this account can then run the labeling cmdlets non-interactively until the authentication token expires.

For the user account to be able to sign in interactively this first time, the account must have the **Log on locally** right. This right is standard for user accounts but your company policies might prohibit this configuration for service accounts. If that's the case, you can run Set-AIPAuthentication with the *Token* parameter so that authentication completes without the sign-in prompt. You can run this command as a scheduled task and grant the account the lower right of **Log on as batch job**. For more information, see the following sections.

When the token expires, run the cmdlet again to acquire a new token.

If you run this cmdlet without parameters, the account acquires an access token that is valid for 90 days or until your password expires.

To control when the access token expires, run this cmdlet with parameters. This lets you configure the access token for one year, two years, or to never expire. This configuration requires you to have two applications registered in Azure Active Directory: A **Web app / API** application and a **native application**. The parameters for this cmdlet use values from these applications.

After you have run this cmdlet, you can run the labeling cmdlets in the context of the user account that you created.

### To create and configure the Azure AD applications for Set-AIPAuthentication

1. In a new browser window, sign in to the [Azure portal](#).
2. For the Azure AD tenant that you use with Azure Information Protection, navigate to **Azure Active Directory > Manage > App registrations**.
3. Select **+ New registration**, to create your Web app /API application. On the **Register an application** pane, specify the following values, and then click **Register**:
  - **Name:** `AIPOnBehalfOf`  
If you prefer, specify a different name. It must be unique per tenant.
  - **Supported account types:** **Accounts in this organizational directory only**
  - **Redirect URI (optional):** **Web** and `http://localhost`
4. On the **AIPOnBehalfOf** pane, copy the value for the **Application (client) ID**. The value looks similar to the following example: `57c3c1c3-abf9-404e-8b2b-4652836c8c66`. This value is used for the *WebAppId* parameter when you run the Set-AIPAuthentication cmdlet. Paste and save the value for later reference.
5. Still on the **AIPOnBehalfOf** pane, from the **Manage** menu, select **Authentication**.

6. On the **AIPOnBehalfOf - Authentication** pane, in the **Advanced settings** section, select the **ID tokens** checkbox, and then select **Save**.
7. Still on the **AIPOnBehalfOf - Authentication** pane, from the **Manage** menu, select **Certificates & secrets**.
8. On the **AIPOnBehalfOf - Certificates & secrets** pane, in the **Client secrets** section, select **+ New client secret**.
9. For **Add a client secret**, specify the following, and then select **Add**:
  - **Description:** `Azure Information Protection client`
  - **Expires:** Specify your choice of duration (1 year, 2 years, or never expires)
10. Back on the **AIPOnBehalfOf - Certificates & secrets** pane, in the **Client secrets** section, copy the string for the **VALUE**. This string looks similar to the following example:  
`+LBkMvddz?Wr1NCK5v0e6_=meM59sSAn`. To make sure you copy all the characters, select the icon to **Copy to clipboard**.

It's important that you save this string because it is not displayed again and it cannot be retrieved. As with any sensitive information that you use, store the saved value securely and restrict access to it.
11. Still on the **AIPOnBehalfOf - Certificates & secrets** pane, from the **Manage** menu, select **Expose an API**.
12. On the **AIPOnBehalfOf - Expose an API** pane, select **Set** for the **Application ID URI** option, and in the **Application ID URI** value, change **api** to **http**. This string looks similar to the following example:  
`http://d244e75e-870b-4491-b70d-65534953099e`.

Select **Save**.
13. Back on the **AIPOnBehalfOf - Expose an API** pane, select **+ Add a scope**.
14. On the **Add a scope** pane, specify the following, using the suggested strings as examples, and then select **Add scope**:
  - **Scope name:** `user-impersonation`
  - **Who can consent?:** `Admins and users`
  - **Admin consent display name:** `Access Azure Information Protection scanner`
  - **Admin consent description:** `Allow the application to access the scanner for the signed-in user`
  - **User consent display name:** `Access Azure Information Protection scanner`
  - **User consent description:** `Allow the application to access the scanner for the signed-in user`
  - **State:** `Enabled` (the default)
15. Back on the **AIPOnBehalfOf - Expose an API** pane, close this pane.
16. Select **API permissions**.
17. On the **AIPOnBehalfOf | API permissions** pane, select **+ Add a permission**.
18. Choose **Azure Right Management**, select **Delegated Permissions** and then select **Create and access protected content for users**.
19. Click on **Add a permission**.
20. Back on the **API permissions** pane, in the **Grant consent** section, select **Grant admin consent for** and select **Yes** for the confirmation prompt.
21. On the **App registrations** pane, select **+ New application registration** to create your native application now.

22. On the **Register an application** pane, specify the following settings, and then select **Register**:

- **Name:** AIPClient
- **Supported account types:** Accounts in this organizational directory only
- **Redirect URI (optional):** Public client (mobile & desktop) and `http://localhost`

23. On the **AIPClient** pane, copy the value of the **Application (client) ID**. The value looks similar to the following example: `8ef1c873-9869-4bb1-9c11-8313f9d7f76f`.

This value is used for the `NativeAppId` parameter when you run the `Set-AIPAuthentication` cmdlet. Paste and save the value for later reference.

24. Still on the **AIPClient** pane, from the **Manage** menu, select **Authentication**.

25. On the **AIPClient - Authentication** pane, from the **Manage** menu, select **API permissions**.

26. On the **AIPClient - permissions** pane, select **+ Add a permission**.

27. On the **Request API permissions** pane, select **My APIs**.

28. In the **Select an API** section, select **APIOnBehalfOf**, then select the checkbox for **user-impersonation**, as the permission. Select **Add permissions**.

29. Back on the **API permissions** pane, in the **Grant consent** section, select **Grant admin consent for <your tenant name>** and select **Yes** for the confirmation prompt.

You've now completed configuration of the two apps and you have the values that you need to run [Set-AIPAuthentication](#) with the parameters `WebAppId`, `WebAppKey` and `NativeAppId`. From our examples:

```
Set-AIPAuthentication -WebAppId "57c3c1c3-abf9-404e-8b2b-4652836c8c66" -WebAppKey "+LBkMvddz?Wn1NCK5v0e6_=meM59sSAN" -NativeAppId "8ef1c873-9869-4bb1-9c11-8313f9d7f76f"
```

Run this command in the context of the account that will label and protect the documents non-interactively. For example, a user account for your PowerShell scripts or the service account to run the Azure Information Protection scanner.

When you run this command for the first time, you are prompted to sign in, which creates and securely stores the access token for your account in `%localappdata%\Microsoft\MSIP`. After this initial sign-in, you can label and protect files non-interactively on the computer. However, if you use a service account to label and protect files, and this service account cannot sign in interactively, use the instructions in the following section so that the service account can authenticate by using a token.

### Specify and use the Token parameter for Set-AIPAuthentication

Use the following additional steps and instructions to avoid the initial interactive sign-in for an account that labels and protects files. Typically, these additional steps are required only if this account cannot be granted the **Log on locally** right but is granted the **Log on as a batch job** right. For example, this might be the case for your service account that runs the Azure Information Protection scanner.

High-level steps:

1. Create a PowerShell script on your local computer.
2. Run `Set-AIPAuthentication` to get an access token and copy it to the clipboard.
3. Modify the PowerShell script to include the token.
4. Create a task that runs the PowerShell script in the context of the service account that will label and protect files.

5. Confirm that the token is saved for the service account, and delete the PowerShell script.

#### Step 1: Create a PowerShell script on your local computer

1. On your computer, create a new PowerShell script named Aipauthentication.ps1.
2. Copy and paste the following command into this script:

```
Set-AIPAuthentication -WebAppId <ID of the "Web app / API" application> -WebAppKey <key value generated in the "Web app / API" application> -NativeAppId <ID of the "Native" application > -Token <token value>
```

3. Using the instructions in the preceding section, modify this command by specifying your own values for the **WebAppId**, **WebAppkey**, and **NativeAppId** parameters. At this time, you do not have the value for the **Token** parameter, which you specify later.

For example:

```
Set-AIPAuthentication -WebAppId "57c3c1c3-abf9-404e-8b2b-4652836c8c66" -WebAppKey "sc9qxh4lmv31GbIBCy36TxEEuM1VmKex5sAdBzABH+M=" -NativeAppId "8ef1c873-9869-4bb1-9c11-8313f9d7f76f" -Token <token value>
```

#### Step 2: Run Set-AIPAuthentication to get an access token and copy it to the clipboard

1. Open a Windows PowerShell session.
2. Using the same values as you specified in the script, run the following command:

```
(Set-AIPAuthentication -WebAppId <ID of the "Web app / API" application> -WebAppKey <key value generated in the "Web app / API" application> -NativeAppId <ID of the "Native" application >).token | clip
```

For example:

```
(Set-AIPAuthentication -WebAppId "57c3c1c3-abf9-404e-8b2b-4652836c8c66" -WebAppKey "sc9qxh4lmv31GbIBCy36TxEEuM1VmKex5sAdBzABH+M=" -NativeAppId "8ef1c873-9869-4bb1-9c11-8313f9d7f76f").token | clip`
```

#### Step 3: Modify the PowerShell script to supply the token

1. In your PowerShell script, specify the token value by pasting the string from the clipboard, and save the file.
2. Sign the script. If you do not sign the script (more secure), you must configure Windows PowerShell on the computer that will run the labeling commands. For example, run a Windows PowerShell session with the **Run as Administrator** option, and type: `Set-ExecutionPolicy RemoteSigned`. However, this configuration lets all unsigned scripts run when they are stored on this computer (less secure).

For more information about signing Windows PowerShell scripts, see [about\\_Signing](#) in the PowerShell documentation library.

3. Copy this PowerShell script to the computer that will label and protect files, and delete the original on your computer. For example, you copy the PowerShell script to C:\Scripts\Aipauthentication.ps1 on a Windows Server computer.

#### Step 4: Create a task that runs the PowerShell script

1. Make sure that the service account that will label and protect files has the **Log on as a batch job** right.

2. On the computer that will label and protect files, open Task Scheduler and create a new task. Configure this task to run as the service account that will label and protect files, and then configure the following values for the **Actions**:

- **Action:** `Start a program`
- **Program/script:** `Powershell.exe`
- **Add arguments (optional):**  
`-NoProfile -WindowStyle Hidden -command "&{C:\Scripts\Aipauthentication.ps1}"`

For the argument line, specify your own path and file name, if these are different from the example.

3. Manually run this task.

**Step 5: Confirm that the token is saved and delete the PowerShell script**

1. Confirm that the token is now stored in the `%localappdata%\Microsoft\MSIP` folder for the service account profile. This value is protected by the service account.
2. Delete the PowerShell script that contains the token value (for example, `Aipauthentication.ps1`).

Optionally, delete the task. If your token expires, you must repeat this process, in which case it might be more convenient to leave the configured task so that it's ready to rerun when you copy over the new PowerShell script with the new token value.

## Next steps

For cmdlet help when you are in a PowerShell session, type `Get-Help <cmdlet name> cmdlet`, and use the `-online` parameter to read the most up-to-date information. For example:

```
Get-Help Get-RMSTemplate -online
```

See the following for additional information that you might need to support the Azure Information Protection client:

- [Customizations](#)
- [Client files and usage logging](#)
- [Document tracking](#)
- [File types supported](#)

# Azure Information Protection user guide

7/20/2020 • 2 minutes to read • [Edit Online](#)

*Applies to:* Active Directory Rights Management Services, [Azure Information Protection](#), Windows 10, Windows 8.1, Windows 8

*Instructions for:* [Azure Information Protection client for Windows](#)

The Azure Information Protection client for Windows helps you keep important documents and emails safe from people who shouldn't see them, even if your email is forwarded or your document is saved to another location. You can also use this client to open documents that other people have protected by using the Rights Management protection technology from Azure Information Protection.

All you need is a computer that runs at least Windows 8. Then download and install this free client from Microsoft.

## What do you want to do?

- [Download and install the Azure Information Protection client](#)
- [Classify a file or email](#)
- [Classify and protect a file or email](#)
- [Track and revoke your documents](#)
- [Open files that have been protected](#)
- [Remove labels and protection from files and emails](#)
- [Tasks that you used to do with the RMS sharing application](#)

### NOTE

If you are an administrator who is responsible for the Azure Information Protection client on an enterprise network, see the [Azure Information Protection client administrator guide](#) for additional technical information.

# User Guide: Download and install the Azure Information Protection client

7/20/2020 • 2 minutes to read • [Edit Online](#)

*Applies to: Active Directory Rights Management Services, Azure Information Protection, Windows 10, Windows 8.1, Windows 8*

*Instructions for: Azure Information Protection client for Windows*

If your administrator does not install the Azure Information Protection client for you, you can do this yourself. You must be a local administrator for your PC to install this client so that it can label and protect your documents and emails.

In addition:

- The Azure Information Protection client requires a minimum version of Microsoft .NET Framework 4.6.2 and if this is missing, the installer tries to download and install this prerequisite. When this prerequisite is installed as part of the client installation, your computer must be restarted.

## To download and install the Azure Information Protection client

1. Go to the [Microsoft Azure Information Protection](#) page on the Microsoft website.

This page has links for all the popular devices you might use, so that you can easily download a viewer app if it's needed to open protected files. If you're not a local administrator for your PC, you can still install the viewer app for Windows. But these instructions are to install the full client, which lets you label and protect files.

2. Locate the **Azure Information Protection client** section and click the Windows icon. Click **Download** and save the **AzInfoProtection.exe** file.

3. Run the executable file that was downloaded. If you are prompted to continue, click **Yes**.

4. On the **Install the Azure Information Protection client** page:

- Select the option to install a demo policy if you cannot connect to the cloud but want to see and experience the client side of Azure Information Protection by using a local policy for demonstration purposes. When your client connects to an Azure Information Protection service, this demo policy is replaced with your organization's Azure Information Protection policy.
- Click **I agree** when you have read the license terms and conditions.

5. If you are prompted to continue, click **Yes**, and wait for the installation to finish.

6. Click **Close**. Before you start to use the Azure Information Protection client:

- If your computer runs Office 2010, restart your computer and then go to the next section for your final step.
- For other versions of Office, restart all Office applications and all instances of File Explorer. Your installation is now complete and you can use the client to label and protect your documents and emails.

### **Installing the Azure Information Protection client with Office 2010**

After you have installed the Azure Information Protection client by using the previous instructions:

1. Open Microsoft Word. When this is the first time that you have run an Office 2010 application after you have installed the Azure Information Protection client, you see a **Microsoft Azure Information Protection** dialog box. This dialog box tells you that administrator credentials are required to complete the sign in process.
2. In the **Microsoft Azure Information Protection** dialog box, click **OK**.
3. If you see a **User Access Control** dialog box, click **Yes** so that the Azure Information Protection client can update the registry.

Your installation is now complete and you can use Azure Information Protection to label and protect your documents and emails.

## Other instructions

More how-to instructions from the Azure Information Protection user guide:

- [What do you want to do?](#)

## Additional information for administrators

See [Install the Azure Information Protection client for users](#) from the [admin guide](#).

# User Guide: Classify a file or email with the Azure Information Protection client

7/20/2020 • 4 minutes to read • [Edit Online](#)

Applies to: Active Directory Rights Management Services, [Azure Information Protection](#), Windows 10, Windows 8.1, Windows 8

Instructions for: [Azure Information Protection client for Windows](#)

## NOTE

To provide a unified and streamlined customer experience, **Azure Information Protection client (classic)** and **Label Management** in the Azure Portal are being **deprecated** as of **March 31, 2021**. This time-frame allows all current Azure Information Protection customers to transition to our unified labeling solution using the Microsoft Information Protection Unified Labeling platform. Learn more in the official [deprecation notice](#).

## NOTE

Use these instructions to help you classify (but not protect) your documents and emails. If you need to also protect your documents and emails, see the [classify and protect instructions](#). If you are not sure which set of instructions to use, check with your administrator or help desk.

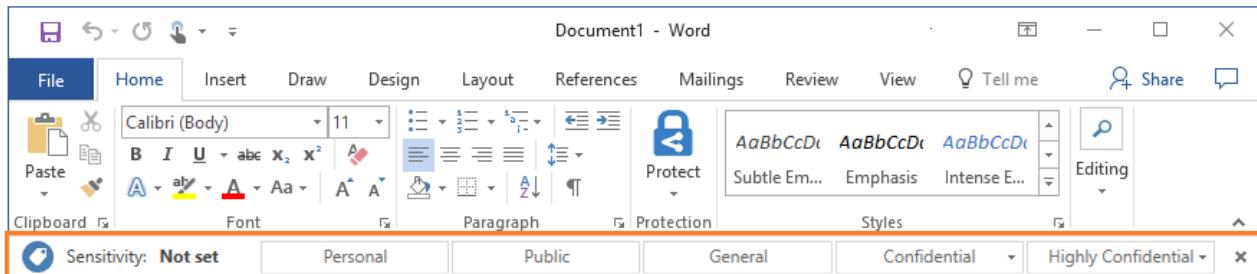
The easiest way to classify your documents and emails is when you are creating or editing them from within your Office desktop apps: **Word**, **Excel**, **PowerPoint**, **Outlook**.

However, you can also classify files by using **File Explorer**. This method supports additional file types and is a convenient way to classify multiple files at once.

## Using Office apps to classify your documents and emails

Use the Azure Information Protection bar and select one of the labels that has been configured for you.

For example, the following picture shows that the document hasn't yet been labeled because the **Sensitivity** shows **Not set**. To set a label, such as "General", click **General**. If you're not sure which label to apply to the current document or email, use the label tooltips to learn more about each label and when to apply it.



If a label is already applied to the document and you want to change it, you can select a different label. If the labels are not displayed on the bar, first click the **Edit Label** icon, next to the current label value.

## TIP

You can also select labels from the **Protect** button, on the **File** tab.

In addition to manually selecting labels, labels can also be applied in the following ways:

- Your administrator configured a default label, which you can keep or change.
- Your administrator configured recommended prompts to select a specific label when sensitive data is detected. You can accept the recommendation (and the label is applied), or reject it (the recommended label is not applied).

### Exceptions for the Azure Information Protection bar

Don't see this Information Protection bar in your Office apps?

- You might not have the Azure Information Protection client [installed](#).
- You have the client installed, but your administrator has configured a setting that doesn't display the bar. Instead, select labels from the **Protect** button, on the **File** tab from the Office ribbon.

Is the label that you expect to see not displayed on the bar?

- If your administrator has recently configured a new label for you, try closing all instances of your Office app and reopening it. This action checks for changes to your labels.
- The label might be in a scoped policy that doesn't include your account. Check with your help desk or administrator.

## Using File Explorer to classify files

When you use File Explorer, you can quickly classify a single file, multiple files, or a folder.

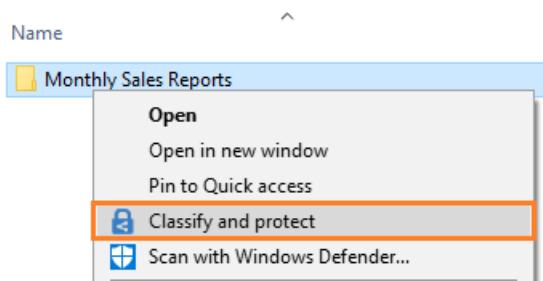
When you select a folder, all the files in that folder and any subfolders it has are automatically selected for the classification that you set. However, new files that you create in that folder or subfolders are not automatically classified.

When you use File Explorer to classify your files, if one or more of the labels appear dimmed, the files that you selected do not support classification without also protecting them.

The admin guide contains a full list of the file types that support classification without protection: [File types supported for classification only](#).

### To classify a file by using File Explorer

1. In File Explorer, select your file, multiple files, or a folder. Right-click, and select **Classify and protect**. For example:



2. In the **Classify and protect - Azure Information Protection** dialog box, use the labels as you would do in an Office application, which sets the classification as defined by your administrator.

If none of the labels can be selected (they appear dimmed): The selected file does not support classification. For example:

Sensitivity: Not set

Personal    Public    Internal    Confidential    Secret

Delete Label

This file type supports only labels that apply protection

3. If you selected a file that does not support classification, click **Close**. You cannot classify this file without also protecting it.

If you selected a label, click **Apply** and wait for the **Work finished** message to see the results. Then click **Close**.

If you change your mind about the label you chose, simply repeat this process and choose a different label.

The classification that you specified stays with the file, even if you email the file or save it to another location.

## Other instructions

More how-to instructions from the Azure Information Protection user guide:

- [What do you want to do?](#)

## Additional information for administrators

See [Configuring the Azure Information Protection policy](#).

# User Guide: Classify and protect with the Azure Information Protection client

7/20/2020 • 10 minutes to read • [Edit Online](#)

*Applies to:* Active Directory Rights Management Services, [Azure Information Protection](#), Windows 10, Windows 8.1, Windows 8

*Instructions for:* [Azure Information Protection client for Windows](#)

## NOTE

To provide a unified and streamlined customer experience, **Azure Information Protection client (classic)** and **Label Management** in the Azure Portal are being **deprecated** as of **March 31, 2021**. This time-frame allows all current Azure Information Protection customers to transition to our unified labeling solution using the Microsoft Information Protection Unified Labeling platform. Learn more in the official [deprecation notice](#).

## NOTE

Use these instructions to help you classify and protect your documents and emails. If you need to only classify and not protect your documents and emails, see the [classify-only instructions](#). If you are not sure which set of instructions to use, check with your administrator or help desk.

The easiest way to classify and protect your documents and emails is when you are creating or editing them from within your Office desktop apps: **Word**, **Excel**, **PowerPoint**, **Outlook**.

However, you can also classify and protect files by using **File Explorer**. This method supports additional file types and is a convenient way to classify and protect multiple files at once. This method supports protecting Office documents, PDF files, text and image files, and a wide range of other files.

If your label applies protection to a document, the protected document is not suitable to be saved on SharePoint or OneDrive. These locations do not support the following for protected files: Co-authoring, Office for the web, search, document preview, thumbnail, and eDiscovery.

## TIP

Ask your administrator about migrating your labels to unified sensitivity labels that are supported for these locations when [SharePoint is enabled for sensitivity labels](#).

## Safely share a file with people outside your organization

Files that are protected are safe to share with others. For example, you attach a protected document to an email.

Before you share files with people outside your organization, check with your help desk or administrator how to protect files for external users.

For example, if your organization regularly communicates with people in another organization, your administrator might have configured labels such that these people can read and use protected documents. If that's the case, select these labels to classify and protect the documents to share.

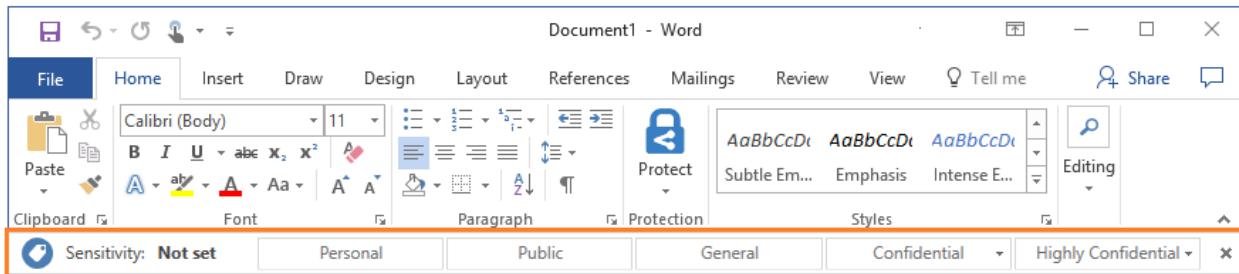
Alternatively, if the external users have [business-to-business \(B2B\) accounts](#) created for them, you can use your

Office app to set custom permissions or use [File Explorer to set custom permissions](#) for a document before you share it. If you set your own custom permissions and the document is already protected for internal use, first make a copy of it to retain the original permissions. Then use the copy to set the custom permissions.

## Using Office apps to classify and protect your documents and emails

Use the Azure Information Protection bar or the **Protect** button on the ribbon to select one of the labels that has been configured for you.

For example, the following picture shows that the document hasn't yet been labeled because the **Sensitivity** shows **Not set** on the Azure Information Protection bar. To set a label, such as "General", click **General**. If you're not sure which label to apply to the current document or email, use the label tooltips to learn more about each label and when to apply it.



If a label is already applied to the document and you want to change it, you can select a different label. If the labels are not displayed on the bar, first click the **Edit Label** icon, next to the current label value.

In addition to manually selecting labels, labels can also be applied in the following ways:

- Your administrator configured a default label, which you can keep or change.
- Your administrator configured recommended prompts to select a specific label when sensitive data is detected. You can accept the recommendation (and the label is applied), or reject it (the recommended label is not applied).

### Exceptions for the Azure Information Protection bar

Don't see this Information Protection bar in your Office apps?

Possible reasons:

- You don't have the Azure Information Protection client [installed](#).
- You have the client installed, but your administrator has configured a setting that doesn't display the bar. Instead, select labels from the **Protect** button, on the **File** tab from the Office ribbon.
- Your client is running in [protection-only mode](#).

Is the label that you expect to see not displayed?

Possible reasons:

- If your administrator has recently configured a new label for you, try closing all instances of your Office app and reopening it. This action checks for changes to your labels.
- If the missing label applies protection, you might have an edition of Office that does not support applying Rights Management protection. To verify, click **Protect > Help and Feedback**. In the dialog box, check if you have a message in the **Client status** section that says **This client is not licensed for Office Professional Plus**.

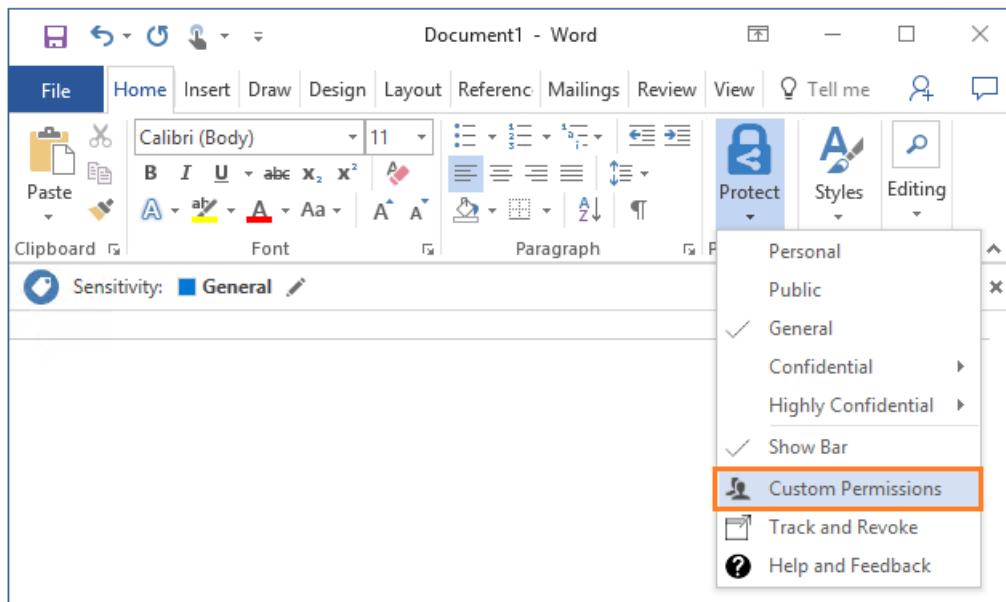
You do not need Office Professional Plus if you have Office apps from Office 365 Business or Microsoft 365 Business when the user is assigned a license for Azure Rights Management (also known as Azure Information Protection for Office 365).

- The label might be in a scoped policy that doesn't include your account. Check with your help desk or administrator.

## Set custom permissions for a document

If allowed by your administrator, you can specify your own protection settings for documents rather than use the protection settings that your administrator might have included with your selected label. This option is specific to documents and is not available with Outlook.

- On the Home tab, in the Protection group, click Protect > Custom Permissions:



If you do not see **Custom Permissions**, your administrator does not allow you to use this option.

Note that any custom permissions that you specify replace rather than supplement protection settings that your administrator might have defined for your chosen label.

- In the Microsoft Azure Information Protection dialog box, specify the following:

- Protect with custom permissions:** Make sure that this is selected so that you can specify and apply your custom permissions. Clear this option to remove any custom permissions.
- Select permissions:** If you want to protect the file so that only you can access it, select **Only for me**. Otherwise, select the level of access that you want people to have.
- Select users, groups, or organizations:** Specify the people who should have the permissions you selected for your file or files. Type their full email address, a group email address, or a domain name from the organization for all users in that organization.

You can also use the address book icon to select users or groups from the Outlook address book.

- Expire access:** Select this option only for time-sensitive files so that the people you specified can't open your selected file or files after a date that you set. You will still be able to open the original file but after midnight (your current time zone), on the day that you set, the people that you specified will not be able to open the file.

- Click **Apply** and wait for the **Custom permissions applied** message. Then click **Close**.

## Safely sharing by email

When you share Office documents by email, you can attach the document to an email that you protect, and the document is automatically protected with the same restrictions that apply to the email.

However, we recommend that you protect the document first, and then attach it to the email. Protect the email as

well if the email message contains sensitive information. Two benefits of protecting the document before you attach it to an email:

- You can track and if necessary, revoke the document after you have emailed it.
- You can apply different permissions to the document than to the email message.

## Using File Explorer to classify and protect files

When you use File Explorer, you can quickly classify and protect a single file, multiple files, or a folder.

When you select a folder, all the files in that folder and any subfolders it has are automatically selected for the classification and protection options that you set. However, new files that you create in that folder or subfolders are not automatically configured with those options.

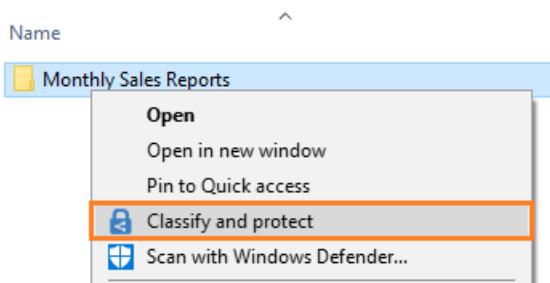
When you use File Explorer to classify and protect your files, if one or more of the labels appear dimmed, the files that you selected do not support classification. For these files, you can select a label only if your administrator has configured the label to apply protection. Or, you can specify your own protection settings.

Some files are automatically excluded from classification and protection, because changing them might stop your PC from running. Although you can select these files, they are skipped as an excluded folder or file. Examples include executable files and your Windows folder.

The admin guide contains a full list of the file types supported and the files and folders that are automatically excluded: [File types supported by the Azure Information Protection client](#).

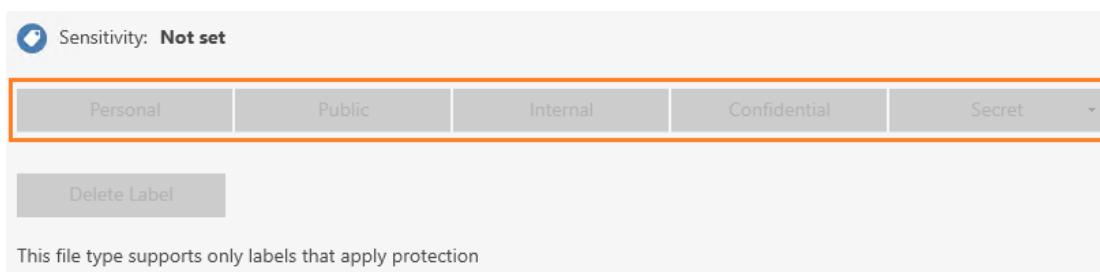
### To classify and protect a file by using File Explorer

1. In File Explorer, select your file, multiple files, or a folder. Right-click, and select **Classify and protect**. For example:



2. In the **Classify and protect - Azure Information Protection** dialog box, use the labels as you would do in an Office application, which sets the classification and protection as defined by your administrator.

- If none of the labels can be selected (they appear dimmed): The selected file does not support classification but you can protect it with custom permissions (step 3). For example:



- If you do not see labels but an option for **Company pre-defined protection** in this dialog box: The client is running in [protection-only mode](#). Either select a template to apply protection that your administrator has configured for you, or, select **Custom permissions** to specify your own protection settings and go to step 4.



3. If allowed by your administrator, you can specify your own protection settings rather than use the protection settings that your administrator might have included with your selected label. To do this, select **Protect with custom permissions**.

If you do not see **Protect with custom permissions**, your administrator does not allow you to use this option.

Any custom permissions that you specify replace rather than supplement protection settings that your administrator might have defined for your chosen label.

4. If you selected the custom permissions option, now specify the following:

- **Select permissions:** Select the level of access that you want people to have when you protect the selected file or files.
- **Select users, groups, or organizations:** Specify the people who should have the permissions you selected for your file or files. Type their full email address, a group email address, or a domain name from the organization for all users in that organization.

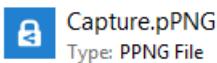
Alternatively, you can use the address book icon to select users or groups from the Outlook address book.

- **Expire access:** Select this option only for time-sensitive files so that the people you specified will not be able to open your selected file or files after a date that you set. You will still be able to open the original file but after midnight (your current time zone), on the day that you set, the people that you specified will not be able to open the file.

Note that if this setting was previously configured by using custom permissions from an Office 2010 app, the specified expiry date does not display in this dialog box but the expiry date is still set. This is a display issue only for when the expiry date was configured in Office 2010.

5. Click **Apply** and wait for the **Work finished** message to see the results. Then click **Close**.

The selected file or files are now classified and protected, according to your selections. In some cases (when adding protection changes the file name extension), the original file in File Explorer is replaced with a new file that has the Azure Information Protection lock icon. For example:



If you change your mind about the classification and protection, or later need to modify your settings, simply repeat this process with your new settings.

The classification and protection that you specified stays with the file, even if you email the file or save it to another location. If you protected the file, you can track how people are using it and if necessary, revoke access to it. For more information, see [Track and revoke your protected documents when you use Azure Information Protection](#).

## Other instructions

More how-to instructions from the Azure Information Protection user guide:

- [What do you want to do?](#)

## Additional information for administrators

For configuration instructions to enable the policy setting **Make the custom permissions option available to users**, see [Configuring the Azure Information Protection policy settings](#).

Other configuration instructions: [Configuring the Azure Information Protection policy](#).

# User Guide: Track and revoke your documents when you use Azure Information Protection

7/20/2020 • 4 minutes to read • [Edit Online](#)

Applies to: [Azure Information Protection](#), Windows 10, Windows 8.1, Windows 8

Instructions for: [Azure Information Protection client for Windows](#)

After you have protected your documents by using Azure Information Protection, you can track how people are using these documents. If necessary, you can also revoke access to them if people should no longer be able to read them. To do this, you use the **document tracking site**. You can access this site from Windows computers, Mac computers, and even from tablets and phones.

When you access this site, sign in to track your documents. When your organization has a [subscription that supports document tracking and revocation](#) and you are assigned a license for this subscription, you can see who tried to open the files that you protected and whether they were successful (they were successfully authenticated) or not. You also see each time they tried to access the document, and their location at the time. However, in rare cases, the location reported might not be accurate. For example, when a user opening a protected document is using a VPN connection, or their computer has an IPv6 address.

Actions you can take in the document tracking site:

- If you need to stop sharing a document:
  - Click **Revoke access**. Note the period of time that the document continues to be available. Decide whether to let people know that you're revoking access to the document you previously shared by providing a customized message. When you revoke a document, it doesn't delete the document that you shared, but authorized users can no longer open it:



- If you want to export to Excel:
  - Click **Export to CSV**, so that you can then modify the data, and create your own views and graphs:



- If you want to configure email notifications:
  - Click **Settings** and select how and whether to be emailed when the document is accessed:

## Email notifications

- Notify me by email when someone tries to open this document
- Notify me only when access to the document is denied
- Don't notify me

- If you want to track and revoke shared documents for others:
  - Administrators for Azure Information Protection can click the Admin icon to track and revoke protected documents for users when those users have registered their documents with the document tracking site. Only administrators see this icon:



If you do not see this icon, despite being a global admin, it's because you haven't yet shared any documents. In this case, use the following URL to access the document tracking site:

<https://portal.azure.com/#/admin>

Unless you are an administrator, you can track and revoke only the documents that you have protected. You cannot track your protected emails by using the document tracking site.

### NOTE

If your administrator has configured privacy controls for the document tracking site, you might not see when users from your organization have accessed a document that you track. An administrator can exempt all users or just some users. However, you can always revoke access to the documents that you track.

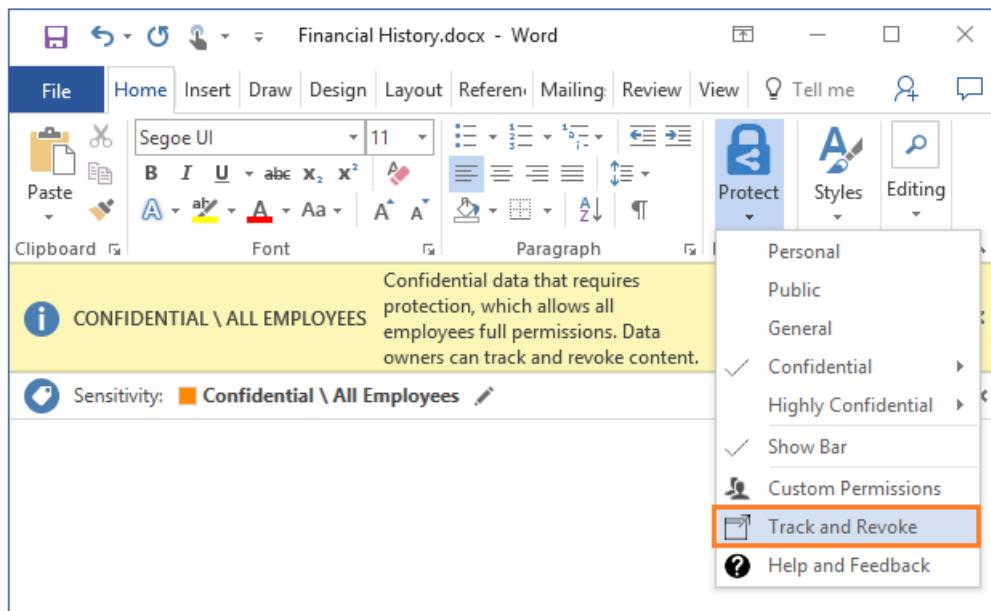
To track a document that you have protected, you must use your Windows computer to register it with the document tracking site. To do this, use either File Explorer, or your Office apps.

If you have the current general availability version of the Azure Information Protection client, you can also register the protected document with PowerShell when you use the *EnableTracking* parameter with the [Set-AIPFileLabel](#) cmdlet.

## Using Office to track or revoke the document

For the Office applications, Word, Excel, and PowerPoint:

1. Open the protected document that you want to track or revoke.
2. On the **Home** tab, in the **Protection** group, click **Protect > Track and Revoke**:



If you do not see these options in your Office applications, it's likely to be because of one of these reasons:

- The Azure Information Protection client is not installed on your computer.
- Your Office applications must be restarted.
- Your computer must be restarted to complete the installation.

For more information about how to install the Azure Information Protection client, see [Download and install the Azure Information Protection client](#).

## Using File Explorer to track or revoke the document

1. Right-click the protected file, and select **Classify and protect**.
2. From the **Classify and protect - Azure Information Protection** dialog box, select **Track and revoke**.



## Using a web browser to track and revoke documents that you have registered

After you have registered the protected document by using your Office apps or File Explorer, you can track and revoke these documents by using a supported web browser:

- Using your Windows PC, Mac computer, or mobile device, visit the [document tracking site](#).

**Supported browsers:** We recommend using Internet Explorer that is at least version 10, but you can use any of following browsers to use the document tracking site:

- Internet Explorer: At least version 10
- Internet Explorer 9 with at least MS12-037: Cumulative Security Update for Internet Explorer: June 12, 2012
- Mozilla Firefox: At least version 12
- Apple Safari 5: At least version 5
- Google Chrome: At least version 18

## Other instructions

More how-to instructions from the Azure Information Protection user guide:

- [What do you want to do?](#)

## Additional information for administrators

See [Configuring and using document tracking for Azure Information Protection](#) from the [admin guide](#).

# User Guide: View protected files with the Azure Information Protection viewer

7/20/2020 • 4 minutes to read • [Edit Online](#)

*Applies to:* Active Directory Rights Management Services, [Azure Information Protection](#), Windows 10, Windows 8.1, Windows 8

*Instructions for:* [Azure Information Protection client for Windows](#)

You can often view a protected file by simply opening it. For example, you might double-click an attachment in an email message or double-click a file from File Explorer, or you might click a link to a file.

If the files don't immediately open, the **Azure Information Protection viewer** might be able to open it. This viewer can open protected text files, protected image files, protected PDF files, and all files that have a .pfile file name extension.

The viewer automatically installs as part of the Azure Information Protection client, or you can install it separately. You can install both the client and the viewer from the [Microsoft Azure Information Protection](#) page on the Microsoft website. For more information about installing the client, see [Download and install the Azure Information Protection client](#).

## NOTE

Although installing the client provides more functionality, it requires local administrator permissions and the full functionality requires a corresponding service for your organization. For example, Azure Information Protection or Active Directory Rights Management Services.

Install the viewer if you have been sent a protected document by somebody from another organization or if you do not have local administrator permissions to your PC.

To be able to open a protected document, the application must be "RMS-enlightened". Office apps and the Azure Information Protection viewer are examples of RMS-enlightened applications. To see a list of applications by type and supported devices, see the [RMS-enlightened applications](#) table.

## Message.rpmmsg as an email attachment

If you see **message.rpmmsg** as a file attachment in an email, this file is not a protected document but a protected email message that displays as an attachment. You can't use the Azure Information Protection viewer for Windows to view this protected email message on your Windows PC. Instead, you need an email application for Windows that supports Rights Management protection, such as Office Outlook. Or you can use Outlook on the web.

However, if you have an iOS or Android device, you can use the Azure Information Protection app to open these protected email messages. You can download this app for these mobile devices from the [Microsoft Azure Information Protection](#) page on the Microsoft website.

## Prompts for authentication

Before you can view the protected file, the Rights Management service that was used to protect the file must first confirm that you are authorized to view the file. The service does this confirmation by checking your user name and password. In some cases, these credentials might be cached and you do not see a prompt that asks you to sign

in. In other cases, you are prompted to supply your credentials.

If your organization does not have a cloud-based account for you to use (for Office 365 or Azure) and does not use an equivalent on-premises version (AD RMS), you have two options:

- If you were sent a protected email, follow the instructions to sign in with your social identity provider (such as Google for a Gmail account) or apply for a one-time passcode.
- You can apply for a free account that will accept your credentials so that you can open documents that are protected by Rights Management. To apply for this account, click the link to apply for [RMS for individuals](#) and use your company email address rather than a personal email address.

## To view and use a protected document

1. Open the protected file (for example, by double-clicking the file or attachment, or by clicking the link to the file). If you are prompted to select an app, select **Azure Information Protection Viewer**.
2. If you see a page to **Sign in** or **Sign up**: Click **Sign in** and enter your credentials. If the protected file was sent to you as an attachment, be sure to specify the same email address that was used to send you the file.  
If you do not have an account that is accepted, see the [Prompts for authentication](#) section on this page.
3. A read-only version of the file opens in the **Azure Information Protection Viewer**. If you have sufficient permissions, you can print the file, and edit it.

You can check your permissions for the file by clicking **Permissions**. From the **Permissions** dialog box, you can also identify the file owner to contact if you want to request a new version of the file with additional permissions.

For more detailed information about the permissions and the usage rights that each contains, see [Rights included in permissions levels](#).

4. To edit the file, click **Save As**, which lets you save the protected file to its original file name extension. You can then edit the file by using the application that's associated with that file type. At this point, the file's label and protection is removed.

Note that because the viewer is for protected files, the **Save As** button is enabled only for protected files.

5. When you have finished editing the file, in File Explorer, right-click the file to reapply the label. This action reapplies the protection.
6. If you have additional protected files to open, you can browse directly to them from the viewer, by using the **Open** option. Your selected file replaces the original file in the viewer.

### TIP

If the protected file does not open and you have the full Azure Information Protection client installed, try the **Reset Settings** option. To access this option, from an Office app, select the **Protect** button > **Help and Feedback** > **Reset Settings**.

[More information about the Reset Settings option](#)

## Other instructions

More how-to instructions from the Azure Information Protection user guide:

- [What do you want to do?](#)

# User Guide: Remove labels and protection from files and emails that have been labeled by Azure Information Protection or protected by Rights Management

7/20/2020 • 2 minutes to read • [Edit Online](#)

*Applies to:* Active Directory Rights Management Services, [Azure Information Protection](#), Windows 10, Windows 8.1, Windows 8

*Instructions for:* [Azure Information Protection client for Windows](#)

When the [Azure Information Protection client is installed on your computer](#), you can remove classification labels and protection from files and emails.

When the label that you remove is configured to apply protection, this action also removes protection from the file. You might be prompted to record why you are removing the label.

## IMPORTANT

You must be the owner of the file to remove protection, or been granted permissions to remove protection (the Rights Management permission of **Export** or **Full Control**).

If you want to choose a different label or a different set of protection settings, you do not need to remove the label or protection. Instead, choose a new label and if necessary, you can define custom permissions if your administrator allows this configuration.

You can remove labels and protection from Office documents and emails when you are creating or editing them from within your Office desktop apps: **Word**, **Excel**, **PowerPoint**, **Outlook**.

You can also remove labels and protection by using **File Explorer**, which supports additional file types and is a convenient way to remove labels and protection from multiple files at once.

## Using Office apps to remove labels and protection from documents and emails

On the Information Protection bar, click the **Delete Label** icon:



If the **Delete Label** icon is not immediately available, first click the **Edit Label** icon:



If you still do not see the **Delete Label** icon, your administrator does not allow you to use this option because all documents and email must have a label.

#### **NOTE**

If you don't see this Information Protection bar in your Office apps:

- If you see a **Protect** button on the ribbon: Select **Protect**, and then select **Show Bar**.
- You might not have the Azure Information Protection client [installed](#), or the client is running in [protection-only mode](#).

## Using File Explorer to remove labels and protection from files

When you use File Explorer, you can quickly remove labels and protection from a single file, multiple files, or a folder. When you select a folder, all the files in that folder and any subfolders it has are automatically selected.

1. In File Explorer, select your file, multiple files, or a folder. Right-click, and select **Classify and protect**.
2. To remove a label: In the **Classify and protect - Azure Information Protection** dialog box, click **Delete Label**. If the label was configured to apply protection, that protection is automatically removed.
3. To remove custom protection from a single file: In the **Classify and protect - Azure Information Protection** dialog box, clear the **Protect with custom permissions** option.  
If you do not see the **Protect with custom permissions** option, your administrator does not allow you to use this option.
4. To remove custom protection from multiple files: In the **Classify and protect - Azure Information Protection** dialog box, click **Remove custom permissions**.  
If you do not see the **Remove custom permissions** option, your administrator does not allow you to use this option.
5. Click **Apply** and wait for the **Work finished** message to see the results. Then click **Close**.

## Other instructions

More how-to instructions from the Azure Information Protection user guide:

- [What do you want to do?](#)

## Additional information for administrators

For configuration instructions to enable the policy setting **Make the custom permissions option available to users**, see [Configuring the Azure Information Protection policy settings](#).

Other configuration instructions: [Configuring the Azure Information Protection policy](#).

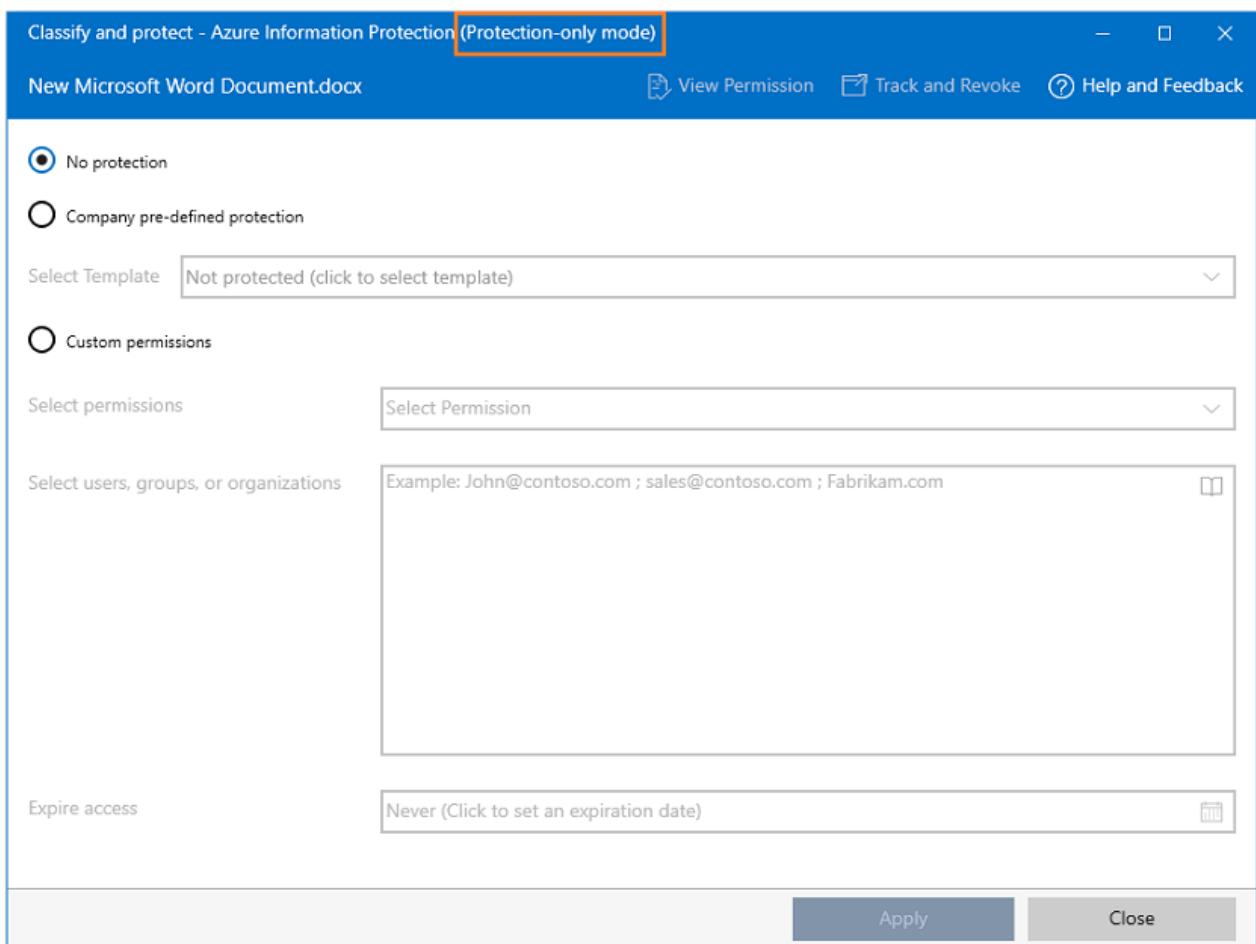
# User Guide: Protection-only mode for the Azure Information Protection client

7/20/2020 • 2 minutes to read • [Edit Online](#)

*Applies to:* Active Directory Rights Management Services, [Azure Information Protection](#), Windows 10, Windows 8.1, Windows 8

*Instructions for:* [Azure Information Protection client for Windows](#)

When the Azure Information Protection client doesn't have labels to classify your documents and emails, it runs in **protection-only mode**. For example, in this mode, you might see the following when you use Windows File Explorer, right-click, **Classify and protect**:



Protection-only mode runs in the following scenarios:

- Your organization does not have a subscription for Azure Information Protection that includes classification and labeling features, but has a subscription for Office 365 that includes data protection by using the Azure Rights Management service.
  - You can use the Azure Information Protection client to protect files and view protected files. You can't classify or label documents and emails.
- Your organization has a subscription for Azure Information Protection for only a subset of users:
  - For this mix of subscriptions, it's the administrator's responsibility to ensure that only the subset of users can use the classification and labeling features. The remainder of users should be running the

Azure Information Protection client in protection-only mode.

- Your organization has a subscription for Azure Information Protection but you don't have any labels configured for you.
  - This can happen when all the labels in the global policy are disabled and your account is not added to a scoped policy. This might be because your IT department has just started to roll out Azure Information Protection but not yet provided you with labels to classify your documents and emails. In the meantime, you can use the Azure Information Protection client to protect files and view protected files.
- Your organization has a subscription for Azure Information Protection but you cannot download the Azure Information Protection policy.
  - This can happen because of a misconfiguration or because your sign-in is not successful. Contact your help desk or administrator but in the meantime, you might be able to use the Azure Information Protection client to protect files and view protected files.
- Your organization uses Active Directory Rights Management Services (AD RMS) only.

## Limitations for protection-only mode

- In Office apps, the Azure Information Protection bar does not display. When you click **Protect > Show Bar**, this menu option is unavailable.
- When you use the **Classify and protect - Azure Information Protection** dialog box with File Explorer, you do not see labels for classification. Instead, as in the previous picture, you see an option to select Rights Management (RMS) templates.

## Supported tasks for protection-only mode

- Protect (and unprotect) documents and emails from within your Office apps, by using the Office Information Rights Management (IRM) feature: For example: Click **File > Info > Protect Document > Restrict Access**. For more information, see [Using information protection with Office 365, Office 2019, Office 2016, or Office 2013]([./help-users.md#using-information-protection-with-Office-365-Office-2019-Office-2016-or-Office-2013](#)).
- Protect (and unprotect) files by using Windows File Explorer: Right-click the file, files, or folder > **Classify and protect**. To apply protection that has been configured by your administrator, in the **Classify and protect - Azure Information Protection** dialog box, click **Select template** and choose one of the available templates.
- View protected files by using the Azure Information Protection Viewer.
- Access the document tracking site from your Office apps. However, you must have a valid subscription to track and revoke documents from this site.

# User Guide: Tasks that you used to do with the RMS sharing application

7/20/2020 • 4 minutes to read • [Edit Online](#)

*Applies to: Active Directory Rights Management Services, Azure Information Protection, Windows 10, Windows 8.1, Windows 8, Windows 7 with SP1, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012*

*Instructions for: Azure Information Protection client for Windows*

Recently upgraded from the Rights Management sharing application (also known as just the "RMS sharing app") to the Azure Information Protection client?

Use the following information to help you get up and running quickly.

THE RMS SHARING APP	HOW TO DO THIS WITH THE AZURE INFORMATION PROTECTION CLIENT
Protect a file on a device  Also known as "protect in place"	For Office apps: Select a label that applies the required protection, or set custom permissions.  For other files: Use the File Explorer menu option, <b>Classify and protect</b> to open the <b>Classify and protect - Azure Information Protection</b> dialog box. Then select a label that applies the required protection, or specify your own custom permissions.  For more information, see <a href="#">Classify and protect a file or email</a> .
Protect a file that you share by email  Also known as "share protected"	Using Outlook, apply a label with the required protection to your email message, or select the Outlook <b>Do Not Forward</b> option. Unprotected attachments that have a <a href="#">supported file type</a> are automatically protected.  Note: To track a protected document that you email, protect it first and then attach it to the email message.  For more information, see <a href="#">Classify and protect a file or email</a> .
Change permissions on protected files  Also known as "re-protect"	For Office apps that display the Azure Information Protection bar: Select a label that applies the required protection.  For other files, and if the Azure Information Protection client is in <a href="#">protection-only mode</a> : Use the File Explorer menu option, <b>Classify and protect</b> to open the <b>Classify and protect - Azure Information Protection</b> dialog box. Then select a label that applies the required protection, or specify your own custom permissions.  For more information, see <a href="#">Classify and protect a file or email</a> .

THE RMS SHARING APP	HOW TO DO THIS WITH THE AZURE INFORMATION PROTECTION CLIENT
Track and revoke documents	<p>From Word, Excel, and PowerPoint: Open the document and then, on the <b>Home</b> tab &gt; <b>Protection</b> group &gt; <b>Protect</b> &gt; <b>Track and revoke</b></p> <p>From File Explorer: Right click a file or folder &gt; <b>Classify and protect</b>. Then in the <b>Classify and protect - Azure Information Protection</b> dialog box, click <b>Track and revoke</b>.</p> <p>When you use PowerShell for the Azure Information Protection client: Use the <i>EnableTracking</i> parameter with the <a href="#">Set-AIPFileLabel</a> cmdlet to register the labeled document for tracking.</p> <p>For more information, see <a href="#">Track and revoke your documents</a>.</p>
View and use files that have been protected	<p>You must have Office installed for protected Office documents. The Azure Information Protection Viewer can open many other protected files so that you can read them, and also print and save these files if you have permissions to do these actions. This viewer is automatically installed with the client, or you can install it separately.</p> <p>For more information, see <a href="#">Open files that have been protected</a>.</p>
Remove protection from files	<p>Use the File Explorer menu option, <b>Classify and protect</b> to open the <b>Classify and protect - Azure Information Protection</b> dialog box.</p> <p>Then, for a single file, clear the <b>Protect with custom permissions</b> option. For multiple files or a folder, click <b>Remove custom permissions</b>.</p> <p>For more information, see <a href="#">Remove labels and protection from files and emails</a>.</p>

## Can't find the option you're looking for?

If you're looking for a specific option that you're used to selecting with the RMS sharing application, check the following table.

OPTION IN THE RMS SHARING APP	INFORMATION
<b>Share Protected</b>	<p>This option is no longer available from the Office ribbon. Instead of sharing directly from within your Office application, use File Explorer's right-click option, <b>Classify and protect</b> to protect a copy of the document with custom permissions, and then share the file using your choice of email client, or sharing location.</p> <p>You can also attach an unprotected Office document to an email that you protect, and the document is automatically protected with the same restrictions. However, you cannot track and revoke this document.</p>

OPTION IN THE RMS SHARING APP	INFORMATION
Email me when somebody tries to open these documents	Use the document tracking site to configure your preferred email notification setting: Locate the protected document that you shared > <b>Settings</b> > <b>Email notifications</b>
Allow me to instantly revoke access to these documents	This option is no longer available. Use administrator-defined protection settings that do not allow offline access. Additionally, an administrator can reduce the use license validity period for your tenant, by running <a href="#">Set-AipServiceMaxUseLicenseValidityTime</a> .
Track Usage in Outlook	The ability to access the document tracking site from Outlook is no longer available. Instead, use the <b>Track and revoke</b> option from Word, PowerPoint, Excel, or File Explorer. Or, using a browser, you can go directly to the <a href="#">document tracking site</a> .

## Next steps

More how-to instructions from the Azure Information Protection user guide:

- [What do you want to do?](#)

## Additional information for administrators

See the [Azure Information Protection client administrator guide](#).

# What is the Azure Information Protection app for iOS or Android?

7/20/2020 • 2 minutes to read • [Edit Online](#)

*Applies to: Active Directory Rights Management Services, Azure Information Protection*

The Azure Information Protection (AIP) apps for iOS and Android enable you to view rights-protected email messages (.rpmsg files) when your email app doesn't natively support rights management data protection.

The AIP apps also enable you to view rights-protected PDF documents (protected PDF and\*\*.ppdf\*\* files), images, and text files.

## NOTE

The AIP apps are viewers only, and do not enable you to create new or reply to protected email messages, or create or edit protected files. The apps also cannot open attachments for files that you view, such as attachments to protected PDF documents or email messages.

## AIP mobile app requirements

The AIP mobile apps for iOS and Android can be used with the following systems:

- [Supported mobile OS versions](#)
- [Supported sign in credentials](#)
- [Supported file extensions](#)

### Supported mobile OS versions

The AIP mobile apps require one of the following minimum mobile operating systems:

- iOS 11
- Android 6.0

## NOTE

The AIP mobile apps are not supported on Intel CPUs.

### Supported sign in credentials

Use one of the following to sign in to AIP:

- **Work or school credentials.** Use if your organization already has AD RMS on-premises with the mobile device extension, or uses Azure Information Protection.
- **A Microsoft account.** If your personal email address was used to protect the file, sign in with a [Microsoft account](#).
  - You can use your own Hotmail, Gmail, or any other email address you own when you apply for a Microsoft account.

**NOTE**

Not all applications can open protected content when a Microsoft account is used. For more information, see [Supported scenarios for opening protected documents](#).

## Supported file extensions

You can open .rpmsg, .pdf, .ppdf, .pjpg, .pjpeg, .ptiff, .ppng, .ptxt, .pxml, and several other text and image file formats.

For the full list of text and image file name extensions, see the first table in the [Supported file types for classification and protection](#) section from the admin guide.

## Installing your AIP mobile apps and viewing files

If your mobile device is managed by Microsoft Intune, you may be able to download the apps from your company portal.

Otherwise, access the apps from:

- The [iTunes or Google Play store](#)
- The [Azure Information Protection download page](#). Select the [iOS](#) or [Android](#) icons in the **Mobile Devices** section.

Once installed, wait until you've received a protected email or file, and select the **AIP Viewer** when opening it.

You'll be prompted to sign in with your work or school account, or prompted to select a certificate. Once you've been authenticated, your email or file will open and you'll be able to read its contents.

**TIP**

To try this out right away, send yourself a protected email or file to view.

For more information, see [Get started with the Microsoft Azure Information Protection app for iOS and Android](#).

## Next steps

Use one of the following methods to provide feedback about the AIP mobile apps:

- Go to **Settings > Send feedback**
- Post your question on our [Yammer site](#)

# Get started with the Microsoft Azure Information Protection app for iOS and Android

7/20/2020 • 2 minutes to read • [Edit Online](#)

*Applies to: Active Directory Rights Management Services, Azure Information Protection*

This page describes how to test run the Azure Information Protection apps for iOS or Android.

Most users will typically use the Azure Information Protection app when they need to open a protected email or file. However, if you're an admin testing the app for your users, or if you simply want to try it out before you need it, use the instructions below to view protected files on your device.

## IMPORTANT

Before you start, read through the requirements and instructions on [What is the Azure Information Protection app for iOS or Android?](#)

## Access a protected file from your device

To test out the AIP mobile app, make sure that you can access one of the following types of protected files from your device:

FILE TYPE	INSTRUCTIONS
A .rpmsg file	<p>A rights-protected email message. If your mobile email app doesn't natively support rights management data protection, protected email messages are displayed as email attachments. Use another device, such as Outlook from a Windows computer, to send yourself a rights-protected email message that you can access from your mobile device.</p> <p>**Note:**For a list of email clients that natively support rights management, see the <a href="#">Email</a> column in <a href="#">RMS-enlightened applications</a>.</p>
A rights-protected PDF file	<ol style="list-style-type: none"><li>From a Windows computer, protect a PDF file using the AIP <a href="#">classic</a> or <a href="#">unified labeling client</a> client.</li><li>Send yourself the protected PDF, or upload it to a SharePoint protected library and share it to your own email address.</li></ol>
A .ptxt or .pjjpg or .ppng	<ol style="list-style-type: none"><li>From a Windows computer, protect a text or image file using the AIP <a href="#">classic</a> or <a href="#">unified labeling client</a> client.</li><li>Send yourself the protected file, or upload it to a SharePoint protected library and share it to your own email address.</li></ol> <p><b>Note:</b> For more information, see <a href="#">Supported file types for classification and protection</a></p>

## Open the protected file on your mobile

- Tap the email attachment or link to open your protected content.

2. When prompted, select the **AIP Viewer** app to view the protected content.
3. When prompted, sign in with your work or school account or select a certificate.

Once authenticated, the AIP Viewer app displays the email or file for you.

**NOTE**

Always open the AIP app by opening protected content. Do not try to sign in to the app until you're prompted, or open a protected file from inside the AIP Viewer app.

## Next steps

Use one of the following methods to provide feedback about the AIP mobile apps:

- Go to **Settings > Send feedback**
- Post your question on our [Yammer site](#)

# PDF readers that support Microsoft Information Protection

7/20/2020 • 2 minutes to read • [Edit Online](#)

If you need to open a PDF document that's been protected by Microsoft Information Protection, use the following links and information.

A PDF document that has been protected is likely to contain sensitive information. For added security, the document is encrypted so that unauthorized people can't read it, and that authorized people cannot share screens or screenshots displaying the document.

To open this document, you need a reader (sometimes called a viewer) that verifies you have been granted permissions to open the document, and then decrypt it for you.

## Install PDF readers for your device

Select the device you're using to install a PDF reader that can open protected PDF documents. All these readers can open protected documents that adhere to the ISO standard for PDF encryption:

- **Computers:** [Windows](#) | [MacOS](#)
- **Mobile devices:** [Android](#) | [iOS](#)

### Support for previous formats

The PDF readers in the following table support protected PDF documents that have a .ppdf file name extension, and older formats that have a .pdf file name extension.

Currently, Microsoft SharePoint uses an older format for PDF documents in IRM-protected libraries.

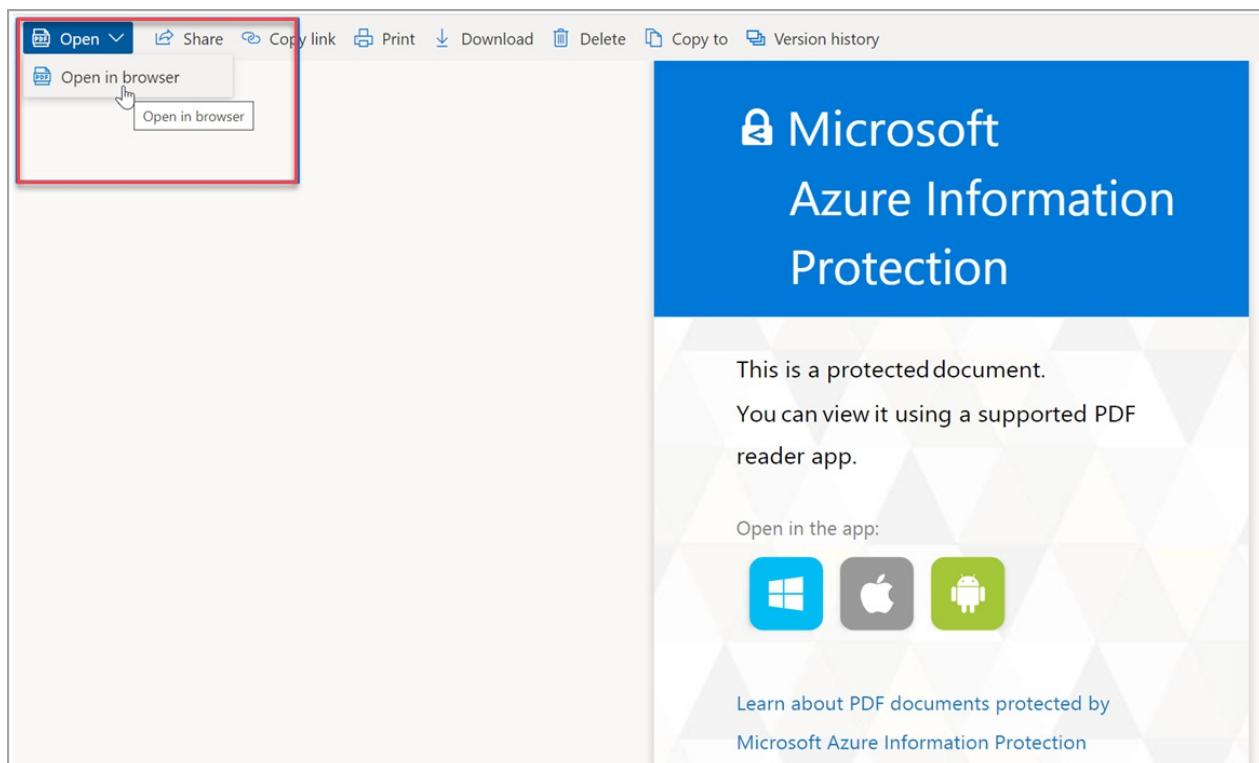
OPERATING SYSTEM	SUPPORTED READERS
Windows 10 and previous versions through Windows 7 Service Pack 1	Microsoft Edge Azure Information Protection viewer Gaaiho Doc GigaTrust Desktop PDF Client for Adobe Foxit Reader Nitro PDF Reader Nuance Power PDF
Android	Azure Information Protection app Foxit MobilePDF with RMS GigaTrust App for Android

OPERATING SYSTEM	SUPPORTED READERS
iOS	Azure Information Protection app
	Foxit MobilePDF with RMS
	TITUS Docs

## Using Microsoft Edge to view protected PDF files

Microsoft Edge offers native support for viewing PDF files that are classified and protected. Use of Microsoft Edge ensures that users can open protected PDF files seamlessly without the need to install or configure any additional settings or software. settings.

With Microsoft Edge, when a user encounters a locally saved protected PDF file, they can view the file directly in the browser. If the file is available on SharePoint, the user only needs to click **Open > Open in browser** from Microsoft Edge, to view the file.



Protected files can be opened on both [Windows](#) and [MacOS](#).

## Using Adobe Acrobat Reader with Adobe plug-in

A collaboration between Microsoft and Adobe gives you a more simplified and consistent experience for PDF documents that have been classified and optionally, protected. This collaboration provides support for Adobe Acrobat native integration with Microsoft Information Protection solutions, such as [Azure Information Protection](#).

This native integration has the following benefits:

- You can view PDF documents that have been protected because they contain sensitive information.
- You can see the classification value for your organization's label that has been applied to the document.
- Support for the ISO standard for PDF encryption.

Unless this capability has been [disabled by an administrator](#), this protected PDF file format is enabled by default for the Azure Information Protection client (classic) and is always used by the Azure Information

Protection unified labeling client.

You can use the Adobe plug with [Windows](#) and [MacOS](#).

For more information, see the following blog posts:

- [General Availability of Adobe Acrobat Reader Integration with Microsoft Information Protection](#)
- [Adobe reader and Microsoft Information Protection integration FAQs](#)

## Next steps

Use the links from this page to install a PDF reader so that you can open protected PDF documents.

If you need help using the reader after it's installed, use the instructions and documentation that accompanies that reader. For example, for the Azure Information Protection viewer for Windows, see [User Guide: View protected files with the Azure Information Protection unified labeling client](#).

# Install a PDF reader for Windows

7/20/2020 • 2 minutes to read • [Edit Online](#)



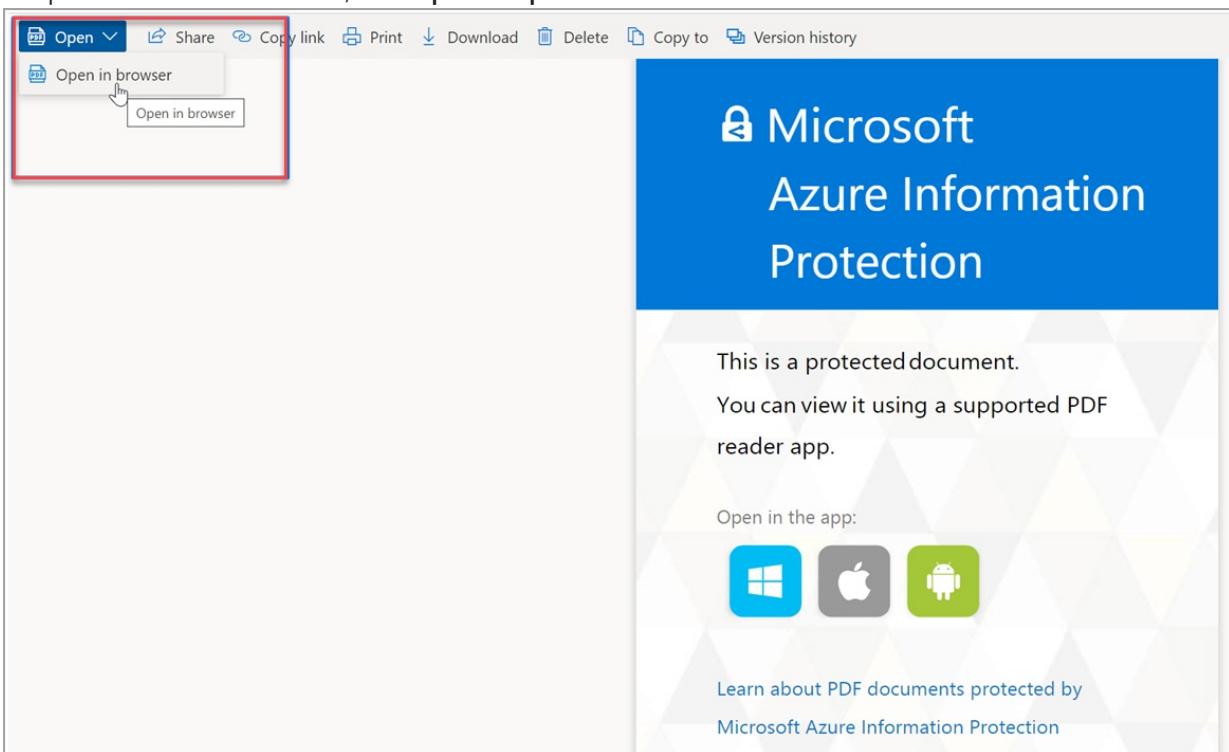
If you need to open a protected PDF document on your Windows computer, use the new [Microsoft Edge](#) browser, or install the Adobe plug-in for the Adobe Acrobat Reader.

## Use Microsoft Edge to view protected files

**Supported versions:** Windows 10 and previous versions through Windows 7

Instructions:

1. Check which [Microsoft Edge version](#) is installed on your system.
2. If the Microsoft Edge version is 83.0.478.37 or above, you can open protected files directly in the Edge browser.
3. To open PDF files in SharePoint, click **Open > Open in browser**.



## Use Adobe Acrobat Reader to view protected files

**Supported versions:** Windows 10 and previous versions through Windows 8

Instructions:

1. Read the [Adobe General Terms of Use](#).
2. If you haven't already, install the Adobe Reader for Windows from the [Adobe site](#).
3. Install the [Adobe plug-in](#) for Windows.

4. If prompted for admin approval, ask your admin to authorize the plug-in.

The admin instructions for this step are included in the release announcement: [General Availability of Adobe Acrobat Reader Integration with Microsoft Information Protection](#).

Alternative readers that open protected PDF documents that adhere to the ISO standard for PDF encryption:

- Azure Information Protection viewer: [Download](#)
- Foxit Reader: [Download](#)

If the document doesn't open, it might be because it has been protected with an older format. In this case, try one of the readers listed as [supported for previous formats](#).

## Next steps

For more information about readers for protected documents, and links to download readers for other platforms, see [PDF readers that supports Microsoft Information Protection](#).

# Install a PDF reader for MacOS

7/20/2020 • 2 minutes to read • [Edit Online](#)



If you need to open a protected PDF document on your Mac computer, use the new [Microsoft Edge](#), or install the Adobe plug-in for the Adobe Acrobat Reader.

## Use Microsoft Edge to view protected files

**Supported versions:** 10.12 and above

Instructions:

1. Check which [Microsoft Edge version](#) is installed on your system.
2. If the Microsoft Edge version is 83.0.478.37 or above, you can open protected files directly in the Edge browser.
3. To open PDF files in SharePoint, click **Open** > **Open in browser**.

## Use Adobe Acrobat Reader to view protected files

**Supported versions:** 10.12 - 10.14

Instructions:

1. Read the [Adobe General Terms of Use](#).
2. If you haven't already, install the Adobe Reader for Mac from the [Adobe site](#).
3. Install the [Adobe plug-in](#) for Mac.
4. If prompted for admin approval, ask your admin to authorize the plug-in.

The admin instructions for this step are included in the release announcement: [General Availability of Adobe Acrobat Reader Integration with Microsoft Information Protection](#).

## Next steps

For more information about readers for protected documents, and links to download readers for other platforms, see [PDF readers that supports Microsoft Information Protection](#).

# Install a PDF reader for iOS

12/22/2019 • 2 minutes to read • [Edit Online](#)



If you need to open a protected PDF document on your iOS device, download the [Azure Information Protection app](#) from the Apple App store.

## Next steps

For more information about readers for protected documents, and links to download readers for other platforms, see [PDF readers that supports Microsoft Information Protection](#).

# Install a PDF reader for Android

12/22/2019 • 2 minutes to read • [Edit Online](#)



If you need to open a protected PDF document on your Android device, download the [Azure Information Protection app](#) from the Google Play store.

## Next steps

For more information about readers for protected documents, and links to download readers for other platforms, see [PDF readers that supports Microsoft Information Protection](#).

# Rights Management Service client deployment notes

3/29/2020 • 16 minutes to read • [Edit Online](#)

*Applies to: Active Directory Rights Management Services, Azure Information Protection, Windows 8, Windows 8.1, Windows 10, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016*

The Rights Management Service client (RMS client) version 2 is also known as the MSIPC client. It is software for Windows computers that communicates with Microsoft Rights Management services on-premises or in the cloud to help protect access to and usage of information as it flows through applications and devices, within the boundaries of your organization, or outside those managed boundaries.

In addition to shipping with the [Azure Information Protection unified labeling client](#), the RMS client is available [as an optional download](#) that can, with acknowledgment and acceptance of its license agreement, be freely distributed with third-party software so that clients can protect and consume content that has been protected by Rights Management services.

## Redistributing the RMS client

The RMS client can be freely redistributed and bundled with other applications and IT solutions. If you are an application developer or solution provider and want to redistribute the RMS client, you have two options:

- Recommended: Embed the RMS client installer in your application installation and run it in silent mode (the `/quiet` switch, detailed in the next section).
- Make the RMS client a prerequisite for your application. With this option, you might need to provide users with additional instructions for them to obtain, install, and update their computers with the client before they can use your application.

## Installing the RMS client

The RMS client is contained in an installer executable file named `setup_msipc_<arch>.exe`, where `<arch>` is either **x86** (for 32-bit client computers) or **x64** (for 64-bit client computers). The 64-bit (x64) installer package installs both a 32-bit runtime executable for compatibility with 32-bit applications that run on a 64-bit operating system installation, as well as a 64-bit runtime executable for supporting native 64-bit applications. The 32-bit (x86) installer does not run on a 64-bit Windows installation.

### NOTE

You must have elevated privileges to install the RMS client, such as a member of the Administrators group on the local computer.

You can install the RMS client by using either of the following installation methods:

- **Silent mode.** By using the `/quiet` switch as part of the command-line options, you can silently install the RMS client on computers. The following example shows a silent mode installation for the RMS client on a 64-bit client computer:

```
setup_msipc_x64.exe /quiet
```

- **Interactive mode.** Alternately, you can install the RMS client by using the GUI-based setup program that's

provided by the RMS Client Installation wizard. To install interactively, double-click the RMS client installer package (`setup_msipc_<arch>.exe`) in the folder to which it was copied or downloaded on your local computer.

## Questions and answers about the RMS client

The following section contains frequently asked questions about the RMS client and the answers to them.

### Which operating systems support the RMS client?

The RMS client is supported with the following operating systems:

WINDOWS SERVER OPERATING SYSTEM	WINDOWS CLIENT OPERATING SYSTEM
Windows Server 2016	Windows 10
Windows Server 2012 R2	Windows 8.1
Windows Server 2012	Windows 8
Windows Server 2008 R2	Windows 7 with minimum of SP1

### Which processors or platforms support the RMS client?

The RMS client is supported on x86 and x64 computing platforms.

### Where is the RMS client installed?

By default, the RMS client is installed in %ProgramFiles%\Active Directory Rights Management Services Client 2. <minor version number>.

### What files are associated with the RMS client software?

The following files are installed as part of the RMS client software:

- Msipc.dll
- Ipcsecproc.dll
- Ipcsecproc\_ssp.dll
- MSIPCEvents.man

In addition to these files, the RMS client also installs multilingual user interface (MUI) support files in 44 languages. To verify the languages supported, run the RMS client installation and when the installation is complete, review the contents of the multilingual support folders under the default path.

### Is the RMS client included by default when I install a supported operating system?

No. This version of the RMS client ships as an optional download that can be installed separately on computers running supported versions of the Microsoft Windows operating system.

### Is the RMS client automatically updated by Microsoft Update?

If you installed this RMS client by using the silent installation option, the RMS client inherits your current Microsoft Update settings. If you installed the RMS client by using the GUI-based setup program, the RMS client installation wizard prompts you to enable Microsoft Update.

## RMS client settings

The following section contains settings information about the RMS client. This information might be helpful if you have problems with applications or services that use the RMS client.

**NOTE**

Some settings depend on whether the RMS-enlightened application runs as a client mode application (such as Microsoft Word and Outlook, or the Azure Information Protection client with Windows File Explorer), or server mode application (such as SharePoint and Exchange). In the following tables, these settings are identified as **Client Mode** and **Server Mode**, respectively.

**Where the RMS client stores licenses on client computers**

The RMS client stores licenses on the local disk and also caches some information in the Windows registry.

DESCRIPTION	CLIENT MODE PATHS	SERVER MODE PATHS
License store location	%localappdata%\Microsoft\MSIPC	%allusersprofile%\Microsoft\MSIPC\Server\<SID>
Template store location	%localappdata%\Microsoft\MSIPC\Templates	%allusersprofile%\Microsoft\MSIPC\Server\<SID>
Registry location	HKEY_CURRENT_USER \Software \Classes \Local Settings \Software \Microsoft \MSIPC	HKEY_CURRENT_USER \Software \Microsoft \MSIPC \Server \<SID>

**NOTE**

<SID> is the secure identifier (SID) for the account under which the server application is running. For example, if the application is running under the built-in Network Service account, replace <SID> with the value of the well-known SID for that account (S-1-5-20).

**Windows registry settings for the RMS client**

You can use Windows registry keys to set or modify some RMS client configurations. For example, as an administrator for RMS-enlightened applications that communicate with AD RMS servers, you might want to update the enterprise service location (override the AD RMS server that is currently selected for publishing) depending on the client computer's current location within your Active Directory topology. Or, you might want to enable RMS tracing at the client computer, to help troubleshoot a problem with an RMS-enlightened application. Use the following table to identify the registry settings that you can change for the RMS client.

TASK	SETTINGS

TASK	SETTINGS
<p>If the client is version 1.03102.0221 or later:</p> <p><b>To control application data collection</b></p>	<p><b>Important:</b> In order to honor user privacy, you as the administrator, must ask the user for consent before enabling data collection.</p> <p>If you enable data collection, you are agreeing to send data to Microsoft over the internet. Microsoft uses this data to provide and improve the quality, security, and integrity of Microsoft products and services. For example, Microsoft analyzes performance and reliability, such as what features you use, how quickly the features respond, device performance, user interface interactions, and any problems you experience with the product. Data also includes information about the configuration of your software, such as the software that you are currently running, and the IP address.</p> <p>For version 1.0.3356 or later:</p> <p>HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft\MSI PC REG_DWORD: DiagnosticAvailability</p> <p>For versions before 1.0.3356:</p> <p>HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft\MSI PC REG_DWORD: DiagnosticState</p> <p><b>Value:</b> 0 for Application defined (default) by using the environment property <a href="#">IPC_EI_DATA_COLLECTION_ENABLED</a>, 1 for Disabled, 2 for Enabled</p> <p><b>Note:</b> If your 32-bit MSIPC-based application is running on a 64-bit version of Windows, the location is HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\MSIPC.</p>
<p>AD RMS only:</p> <p><b>To update the enterprise service location for a client computer</b></p>	<p>Update the following registry keys:</p> <p>HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSIPC\Service Location\EnterpriseCertification REG_SZ: default</p> <p><b>Value:</b> &lt;http or https&gt;://RMS_Cluster_Name/_wmcs/Certification</p> <p>HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSIPC\Service Location\EnterprisePublishing REG_SZ: default</p> <p><b>Value:</b> &lt;http or https&gt;://RMS_Cluster_Name/_wmcs/Licensing</p>
<p><b>To enable and disable tracing</b></p>	<p>Update the following registry key:</p> <p>HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSIPC REG_DWORD: Trace</p> <p><b>Value:</b> 1 to enable tracing, 0 to disable tracing (default)</p>

Task	Settings
<p><b>To change the frequency in days to refresh templates</b></p> <p><b>Important:</b> If this setting is specified, the value to refresh templates in days is ignored. Specify one or the other, not both.</p>	<p>The following registry values specify how often templates refresh on the user's computer if the TemplateUpdateFrequencyInSeconds value is not set. If neither of these values are set, the default refresh interval for applications using the RMS client (version 1.0.1784.0) to download templates is 1 day. Prior versions have a default value of every 7 days.</p> <p><b>Client Mode:</b></p> <p>HKEY_CURRENT_USER\Software\Classes\Local Settings\Software\Microsoft\MSIPC REG_DWORD: TemplateUpdateFrequency</p> <p><b>Value:</b> An integer value that specifies the number of days (minimum of 1) between downloads.</p> <p><b>Server Mode:</b></p> <p>HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSIPC\Server\<i>&lt;SID&gt;</i> REG_DWORD: TemplateUpdateFrequency</p> <p><b>Value:</b> An integer value that specifies the number of days (minimum of 1) between downloads.</p>
<p><b>To change the frequency in seconds to refresh templates</b></p> <p><b>Important:</b> If this setting is specified, the value to refresh templates in days is ignored. Specify one or the other, not both.</p>	<p>The following registry values specify how often templates refresh on the user's computer. If this value or the value to change the frequency in days (TemplateUpdateFrequency) is not set, the default refresh interval for applications using the RMS client (version 1.0.1784.0) to download templates is 1 day. Prior versions have a default value of every 7 days.</p> <p><b>Client Mode:</b></p> <p>HKEY_CURRENT_USER\Software\Classes\Local Settings\Software\Microsoft\MSIPC REG_DWORD: TemplateUpdateFrequencyInSeconds</p> <p><b>Value:</b> An integer value that specifies the number of seconds (minimum of 1) between downloads.</p> <p><b>Server Mode:</b></p> <p>HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSIPC\Server\<i>&lt;SID&gt;</i> REG_DWORD: TemplateUpdateFrequencyInSeconds</p> <p><b>Value:</b> An integer value that specifies the number of seconds (minimum of 1) between downloads.</p>

TASK	SETTINGS
AD RMS only: <b>To download templates immediately at the next publishing request</b>	<p>During testing and evaluations, you might want the RMS client to download templates as soon as possible. For this configuration, remove the following registry key and the RMS client then downloads templates immediately at the next publishing request rather than wait for the time specified by the TemplateUpdateFrequency registry setting:</p> <p>HKEY_CURRENT_USER\Software\Classes\Local Settings\Software\Microsoft\MSIPC\&lt;Server Name&gt;\Template</p> <p><b>Note:</b> &lt;Server Name&gt; could have both external (corprights.contoso.com) and internal (corprights) URLs and therefore two different entries.</p>
AD RMS only: <b>To enable support for federated authentication</b>	<p>If the RMS client computer connects to an AD RMS cluster by using a federated trust, you must configure the federation home realm.</p> <p>HKEY_LOCAL_MACHINE\Software\Microsoft\MSIPC\Federation REG_SZ: FederationHomeRealm</p> <p><b>Value:</b> The value of this registry entry is the uniform resource identifier (URI) for the federation service (for example, "<a href="http://TreyADFS.trey.net/adfs/services/trust">http://TreyADFS.trey.net/adfs/services/trust</a>").</p> <p><b>Note:</b> It is important that you specify http and not https for this value. In addition, if your 32-bit MSIPC-based application is running on a 64-bit version of Windows, the location is HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\MSIPC\Federation. For an example configuration, see <a href="#">Deploying Active Directory Rights Management Services with Active Directory Federation Services</a>.</p>
AD RMS only: <b>To support partner federation servers that require forms-based authentication for user input</b>	<p>By default, the RMS client operates in silent mode and user input is not required. Partner federation servers, however, might be configured to require user input such as by way of forms-based authentication. In this case, you must configure the RMS client to ignore silent mode so that the federated authentication form appears in a browser window and the user is promoted for authentication.</p> <p>HKEY_LOCAL_MACHINE\Software\Microsoft\MSIPC\Federation REG_DWORD: EnableBrowser</p> <p><b>Note:</b> If the federation server is configured to use forms-based authentication, this key is required. If the federation server is configured to use integrated Windows authentication, this key is not required.</p>

TASK	SETTINGS
<p>AD RMS only:</p> <p><b>To block ILS service consumption</b></p>	<p>By default, the RMS client enables consuming content protected by the ILS service but you can configure the client to block this service by setting the following registry key. If this registry key is set to block the ILS service, any attempts to open and consume content protected by the ILS service returns the following error: HRESULT_FROM_WIN32(ERROR_ACCESS_DISABLED_BY_POLICY)</p> <p>HKEY_CURRENT_USER\Software\Classes\Local Settings\Software\Microsoft\MSIPC REG_DWORD: <b>DisablePassportCertification</b></p> <p><b>Value:</b> 1 to block ILS consumption, 0 to allow ILS consumption (default)</p>

### Managing template distribution for the RMS client

Templates make it easy for users and administrators to quickly apply Rights Management protection and the RMS client automatically downloads templates from its RMS servers or service. If you put the templates in the following folder location, the RMS client does not download any templates from its default location and instead, download the templates that you have put in this folder. The RMS client might continue to download templates from other available RMS servers.

**Client Mode:** %localappdata%\Microsoft\MSIPC\UnmanagedTemplates

**Server Mode:** %allusersprofile%\Microsoft\MSIPC\Server\UnmanagedTemplates\<SID>

When you use this folder, there is no special naming convention required except that the templates should be issued by the RMS server or service and they must have the .xml file name extension. For example, Contoso-Confidential.xml or Contoso-ReadOnly.xml are valid names.

## AD RMS only: Limiting the RMS client to use trusted AD RMS servers

The RMS client can be limited to using only specific trusted AD RMS servers by making the following changes to the Windows registry on local computers.

### To enable limiting RMS client to use only trusted AD RMS servers

- HKEY\_LOCAL\_MACHINE\Software\Microsoft\MSIPC\TrustedServers\

REG\_DWORD:AllowTrustedServersOnly

**Value:** If a non-zero value is specified, the RMS client trusts only the specified servers that are configured in the TrustedServers list and the Azure Rights Management service.

### To add members to the list of trusted AD RMS servers

- HKEY\_LOCAL\_MACHINE\Software\Microsoft\MSIPC\TrustedServers\

REG\_SZ:<URL\_or\_HostName>

**Value:** The string values in this registry key location can be either DNS domain name format (for example, adrms.contoso.com) or full URLs to trusted AD RMS servers (for example, <https://adrms.contoso.com>). If a specified URL starts with https://, the RMS client uses SSL or TLS to contact the specified AD RMS server.

## RMS service discovery

RMS service discovery lets the RMS client check which RMS server or service to communicate with before protecting content. Service discovery might also happen when the RMS client consumes protected content, but this type of discovery is less likely to happen because the policy attached to the content contains the preferred RMS server or service. Only if those sources are unsuccessful does the client then run service discovery.

To perform service discovery, the RMS client checks the following:

1. **The Windows registry on the local computer:** If service discovery settings are configured in the registry, these settings are tried first.

By default, these settings are not configured in the registry but an administrator can configure them for AD RMS as documented in a [following section](#). An administrator typically configures these settings for the Azure Rights Management service during the [migration process](#) from AD RMS to Azure Information Protection.

2. **Active Directory Domain Services:** A domain-joined computer queries Active Directory for a service connection point (SCP).

If an SCP is registered as documented in the [following section](#), the URL of the AD RMS server is returned to the RMS client to use.

3. **The Azure Rights Management discovery service:** The RMS client connects to

`https://discover.aadrm.com`, which prompts the user to authenticate.

When authentication is successful, the user name (and domain) from the authentication is used to identify the Azure Information Protection tenant to use. The Azure Information Protection URL to use for that user account is returned to the RMS client. The URL is in the following format:

`https://<YourTenantURL>/_wmcs/licensing`

For example: `5c6bb73b-1038-4eec-863d-49bded473437.rms.na.aadrm.com/_wmcs/licensing`

`<YourTenantURL>` has the following format: `{GUID}.rms.[Region].aadrm.com`. You can find this value by identifying the **RightsManagementServiceId** value when you run the [Get-AipServiceConfiguration](#) cmdlet.

#### NOTE

There are four important exceptions for this service discovery flow:

- Mobile devices are best suited to use a cloud service, so by default they use service discovery for the Azure Rights Management service (<https://discover.aadrm.com>). To override this default so that mobile devices use AD RMS rather than the Azure Rights Management service, specify SRV records in DNS and install the mobile device extension as documented in [Active Directory Rights Management Services Mobile Device Extension](#).
- When the Rights Management service is invoked by an Azure Information Protection label, service discovery is not performed. Instead, the URL is specified directly in the label setting that is configured in the Azure Information Protection policy.
- When a user initiates sign in from an Office application, the user name (and domain) from the authentication is used to identify the Azure Information Protection tenant to use. In this case, registry settings are not needed and the SCP is not checked.
- When you have configured [DNS redirection](#) for Office click-to-run desktop apps, the RMS client finds the Azure Rights Management service by being denied access to the AD RMS cluster that it previously found. This deny action triggers the client to look for the SRV record, which redirects the client to the Azure Rights Management service for your tenant. This SRV record also lets Exchange Online decrypt emails that have been protected by your AD RMS cluster.

#### AD RMS only: Enabling server-side service discovery by using Active Directory

If your account has sufficient privileges (Enterprise Admins and local administrator for the AD RMS server), you can automatically register a service connection point (SCP) when you install the AD RMS root cluster server. If an SCP already exists in the forest, you must first delete the existing SCP before you can register a new one.

You can register and delete an SCP after AD RMS is installed by using the following procedure. Before you start, make sure that your account has the required privileges (Enterprise Admins and local administrator for the AD RMS server).

#### To enable AD RMS service discovery by registering an SCP in Active Directory

1. Open the Active Directory Management Services console at the AD RMS server:

- For Windows Server 2012 R2 or Windows Server 2012, in Server Manager, select Tools > Active Directory Rights Management Services.
- For Windows Server 2008 R2, select Start > Administrative Tools > Active Directory Rights Management Services.

2. In the AD RMS console, right-click the AD RMS cluster, and then click **Properties**.

3. Click the **SCP** tab.

4. Select the **Change SCP** check box.

5. Select the **Set SCP to current certification cluster** option, and then click **OK**.

#### Enabling client-side service discovery by using the Windows registry

As an alternative to using an SCP or where an SCP does not exist, you can configure the registry on the client computer so that the RMS client can locate its AD RMS server.

#### To enable client-side AD RMS service discovery by using the Windows registry

1. Open the Windows registry editor, Regedit.exe:

- On the client computer, in the Run window, type **regedit**, and then press Enter to open the Registry Editor.

2. In Registry Editor, navigate to **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\MSIPC**.

##### NOTE

If you are running a 32-bit application on a 64-bit computer, navigate to  
**HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\MSIPC**

3. To create the **ServiceLocation** subkey, right-click **MSIPC**, point to **New**, click **Key**, and then type **ServiceLocation**.
4. To create the **EnterpriseCertification** subkey, right-click **ServiceLocation**, point to **New**, click **Key**, and then type **EnterpriseCertification**.
5. To set the enterprise certification URL, double-click the **(Default)** value, under the **EnterpriseCertification** subkey. When the **Edit String** dialog box appears, for **Value data**, type  
`<http or https>://<AD RMS_cluster_name>/_wmcs/Certification`, and then click **OK**.
6. To create the **EnterprisePublishing** subkey, right-click **ServiceLocation**, point to **New**, click **Key**, and then type **EnterprisePublishing**.
7. To set the enterprise publishing URL, double-click **(Default)** under the **EnterprisePublishing** subkey. When the **Edit String** dialog box appears, for **Value data**, type  
`<http or https>://<AD RMS_cluster_name>/_wmcs/Licensing`, and then click **OK**.
8. Close Registry Editor.

If the RMS client can't find an SCP by querying Active Directory and it's not specified in the registry, service discovery calls for AD RMS fails.

## Redirecting licensing server traffic

In some cases, you might need to redirect traffic during service discovery, for example, when two organizations are merged and the old licensing server in one organization is retired and clients need to be redirected to a new licensing server. Or, you migrate from AD RMS to Azure RMS. To enable licensing redirection, use the following procedure.

### To enable RMS licensing redirection by using the Windows registry

1. Open the Windows registry editor, Regedit.exe.
2. In Registry Editor, navigate to one of the following:
  - For 64-bit version of Office on x64 platform: HKLM\SOFTWARE\Microsoft\MSIPC\ServiceLocation
  - For 32-bit version of Office on x64 platform:  
HKLM\SOFTWARE\Wow6432Node\Microsoft\MSIPC\ServiceLocation
3. Create a **LicensingRedirection** subkey, by right-clicking **ServiceLocation**, point to **New**, click **Key**, and then type **LicensingRedirection**.
4. To set the licensing redirection, right-click the **LicensingRedirection** subkey, select **New**, and then select **String value**. For **Name**, specify the previous server licensing URL and for **Value** specify the new server licensing URL.

For example, to redirect licensing from a server at Contoso.com to one at Fabrikam.com, you might enter the following values:

**Name:** `https://contoso.com/_wmcs/licensing`

**Value:** `https://fabrikam.com/_wmcs/licensing`

#### NOTE

If the old licensing server has both intranet and extranet URLs specified, a new name and value mapping must be set for both these URLs under the **LicensingRedirection** key.

5. Repeat the previous step for all servers that need to be redirected.
6. Close Registry Editor.

# RMS protection with Windows Server File Classification Infrastructure (FCI)

7/20/2020 • 16 minutes to read • [Edit Online](#)

*Applies to:* [Azure Information Protection](#), Windows Server 2016, Windows Server 2012, Windows Server 2012 R2

*Instructions for:* [Azure Information Protection client for Windows](#)

Use this article for instructions and a script to use the Azure Information Protection client and PowerShell to configure File Server Resource Manager and File Classification Infrastructure (FCI).

This solution lets you automatically protect all files in a folder on a file server running Windows Server, or automatically protect files that meet a specific criteria. For example, files that have been classified as containing confidential or sensitive information. This solution connects directly to the Azure Rights Management service from Azure Information Protection to protect the files, so you must have this service deployed for your organization.

## NOTE

Although Azure Information Protection includes a [connector](#) that supports File Classification Infrastructure, that solution supports native protection only—for example, Office files.

To support multiple file types with Windows Server file classification infrastructure, you must use the PowerShell **AzureInformationProtection** module, as documented in this article. The Azure Information Protection cmdlets, like the Azure Information Protection client, support generic protection as well as native protection, which means that file types other than Office documents can be protected. For more information, see [File types supported by the Azure Information Protection client](#) from the Azure Information Protection client admin guide.

The instructions that follow are for Windows Server 2012 R2 or Windows Server 2012. If you run other supported versions of Windows, you might need to adapt some of the steps for differences between your operating system version and the one documented in this article.

## Prerequisites for Azure Rights Management protection with Windows Server FCI

Prerequisites for these instructions:

- On each file server where you will run File Resource Manager with file classification infrastructure:
  - You have installed File Server Resource Manager as one of the role services for the File Services role.
  - You have identified a local folder that contains files to protect with Rights Management. For example, C:\FileShare.
  - You have installed the **AzureInformationProtection** PowerShell module and configured the prerequisites for this module to connect to the Azure Rights Management service.

The **AzureInformationProtection** PowerShell module is included with the Azure Information Protection client. For installation instructions, see [Install the Azure Information Protection client for users](#) from the Azure Information Protection admin guide. If required, you can install just the PowerShell module by using the `PowerShellOnly=true` parameter.

The [prerequisites for using this PowerShell module](#) include activating the Azure Rights Management service, creating a service principal, and editing the registry if your tenant is outside North America.

Before you start the instructions in this article, make sure that you have values for your

**BposTenantId**, **AppPrincipalId**, and **Symmetric key**, as documented in these prerequisites.

- If you want to change the default level of protection (native or generic) for specific file name extensions, you have edited the registry as described in the [Changing the default protection level of files](#) section from the admin guide.
- You have an internet connection, and you have configured your computer settings if these are required for a proxy server. For example: `netsh winhttp import proxy source=ie`
- You have synchronized your on-premises Active Directory user accounts with Azure Active Directory or Office 365, including their email addresses. This is required for all users that might need to access files after they are protected by FCI and the Azure Rights Management service. If you do not do this step (for example, in a test environment), users might be blocked from accessing these files. If you need more information about this requirement, see [Preparing users and groups for Azure Information Protection](#).
- This scenario does not support departmental templates so you must either use a template that is not configured for a scope, or use the [Set-AipServiceTemplateProperty](#) cmdlet and the *EnableInLegacyApps* parameter.

## Instructions to configure File Server Resource Manager FCI for Azure Rights Management protection

Follow these instructions to automatically protect all files in a folder, by using a PowerShell script as a custom task. Do these procedures in this order:

1. Save the PowerShell script
2. Create a classification property for Rights Management (RMS)
3. Create a classification rule (Classify for RMS)
4. Configure the classification schedule
5. Create a custom file management task (Protect files with RMS)
6. Test the configuration by manually running the rule and task

At the end of these instructions, all files in your selected folder will be classified with the custom property of RMS, and these files will then be protected by Rights Management. For a more complex configuration that selectively protects some files and not others, you can then create or use a different classification property and rule, with a file management task that protects just those files.

Note that if you make changes to the Rights Management template that you use for FCI, the computer account that runs the script to protect the files does not automatically get the updated template. To do so, in the script, locate the commented out `Get-RMSTemplate -Force` command, and remove the `#` comment character. When the updated template is downloaded (the script has run at least one time), you can comment out this additional command so that the templates are not unnecessarily downloaded each time. If the changes to the template are important enough to reprotect the files on the file server, you can do this interactively by running the `Protect-RMSFile` cmdlet with an account that has the Export or Full Control usage rights for the files. You must also run `Get-RMSTemplate -Force` if you publish a new template that you want to use for FCI.

### Save the Windows PowerShell script

1. Copy the contents of the [Windows PowerShell script](#) for Azure RMS protection by using File Server Resource Manager. Paste the contents of the script and name the file **RMS-Protect-FCI.ps1** on your own

computer.

2. Review the script and make the following changes:

- Search for the following string and replace it with your own AppPrincipalId that you use with the [Set-RMSServerAuthentication](#) cmdlet to connect to the Azure Rights Management service:

```
<enter your AppPrincipalId here>
```

For example, the script might look like this:

```
[Parameter(Mandatory = $false)]
```

```
[Parameter(Mandatory = $false)] [string]$AppPrincipalId = "b5e3f76a-b5c2-4c96-a594-a0807f65bba4",
```

- Search for the following string and replace it with your own symmetric key that you use with the [Set-RMSServerAuthentication](#) cmdlet to connect to the Azure Rights Management service:

```
<enter your key here>
```

For example, the script might look like this:

```
[Parameter(Mandatory = $false)]
```

```
[string]$SymmetricKey = "zIeMu8zNJ6U377CLtppkhkb14gjodmYSXUVwAO5ycgA="
```

- Search for the following string and replace it with your own BposTenantId (tenant ID) that you use with the [Set-RMSServerAuthentication](#) cmdlet to connect to the Azure Rights Management service:

```
<enter your BposTenantId here>
```

For example, the script might look like this:

```
[Parameter(Mandatory = $false)]
```

```
[string]$BposTenantId = "23976bc6-dcd4-4173-9d96-dad1f48efd42",
```

3. Sign the script. If you do not sign the script (more secure), you must configure Windows PowerShell on the servers that run it. For example, run a Windows PowerShell session with the **Run as Administrator** option, and type: **Set-ExecutionPolicy RemoteSigned**. However, this configuration lets all unsigned scripts run when they are stored on this server (less secure).

For more information about signing Windows PowerShell scripts, see [about\\_Signing](#) in the PowerShell documentation library.

4. Save the file locally on each file server that runs File Resource Manager with file classification infrastructure. For example, save the file in **C:\RMS-Protection**. If you use a different path or folder name, choose a path and folder that does not include spaces. Secure this file by using NTFS permissions so that unauthorized users cannot modify it.

You're now ready to start configuring File Server Resource Manager.

### Create a classification property for Rights Management (RMS)

- In File Server Resource Manager, Classification Management, create a new local property:
  - **Name:** Type RMS
  - **Description:** Type Rights Management protection

- **Property Type:** Select Yes/No
- **Value:** Select Yes

We can now create a classification rule that uses this property.

### Create a classification rule (Classify for RMS)

- Create a new classification rule:

- On the **General** tab:
  - **Name:** Type **Classify for RMS**
  - **Enabled:** Keep the default, which is that this checkbox is selected.
  - **Description:** Type **Classify all files in the <folder name> folder for Rights Management.**

Replace *<folder name>* with your chosen folder name. For example, **Classify all files in the C:\FileShare folder for Rights Management**

- **Scope:** Add your chosen folder. For example, **C:\FileShare**.

Do not select the checkboxes.

- On the **Classification** tab:
  - **Classification method:** Select **Folder Classifier**
  - **Property name:** Select **RMS**
  - **Property value:** Select **Yes**

Although you can run the classification rules manually, for ongoing operations, you want this rule to run on a schedule so that new files are classified with the RMS property.

### Configure the classification schedule

- On the **Automatic Classification** tab:

- **Enable fixed schedule:** Select this checkbox.
- Configure the schedule for all classification rules to run, which includes our new rule to classify files with the RMS property.
- **Allow continuous classification for new files:** Select this check box so that new files are classified.
- Optional: Make any other changes that you want, such as configuring options for reports and notifications.

Now you've completed the classification configuration, you're ready to configure a management task to apply the RMS protection to the files.

### Create a custom file management task (Protect files with RMS)

- In **File Management Tasks**, create a new file management task:

- On the **General** tab:
  - **Task name:** Type **Protect files with RMS**
  - Keep the **Enable** checkbox selected.
  - **Description:** Type **Protect files in <folder name> with Rights Management and a**

template by using a Windows PowerShell script.

Replace *<folder name>* with your chosen folder name. For example, **Protect files in C:\FileShare with Rights Management and a template by using a Windows PowerShell script**

- **Scope:** Select your chosen folder. For example, **C:\FileShare**.

Do not select the checkboxes.

- On the **Action** tab:

- **Type:** Select **Custom**

- **Executable:** Specify the following:

```
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
```

If Windows is not on your C: drive, modify this path or browse to this file.

- **Argument:** Specify the following, supplying your own values for *<path>* and *<template ID>*:

```
-Noprofile -Command "<path>\RMS-Protect-FCI.ps1 -File '[Source File Path]' -TemplateID
<template GUID> -OwnerMail '[Source File Owner Email]'"
```

For example, if you copied the script to C:\RMS-Protection and the template ID you identified from the prerequisites is e6ee2481-26b9-45e5-b34a-f744eacd53b0, specify the following:

```
-Noprofile -Command "C:\RMS-Protection\RMS-Protect-FCI.ps1 -File '[Source File Path]' -
TemplateID e6ee2481-26b9-45e5-b34a-f744eacd53b0 -OwnerMail '[Source File Owner Email]'"
```

In this command, **[Source File Path]** and **[Source File Owner Email]** are both FCI-specific variables, so type these exactly as they appear in the preceding command. The first variable is used by FCI to automatically specify the identified file in the folder, and the second variable is for FCI to automatically retrieve the email address of the named Owner of the identified file. This command is repeated for each file in the folder, which in our example, is each file in the C:\FileShare folder that additionally, has RMS as a file classification property.

#### **NOTE**

The **-OwnerMail [Source File Owner Email]** parameter and value ensures that the original owner of the file is granted the Rights Management owner of the file after it is protected. This configuration ensures that the original file owner has all Rights Management rights to their own files. When files are created by a domain user, the email address is automatically retrieved from Active Directory by using the user account name in the file's Owner property. To do this, the file server must be in the same domain or trusted domain as the user.

Whenever possible, assign the original owners to protected documents, to ensure that these users continue to have full control over the files that they created. However, if you use the **[Source File Owner Email]** variable as in the preceding command, and a file does not have a domain user defined as the owner (for example, a local account was used to create the file, so the owner displays SYSTEM), the script fails.

For files that do not have a domain user as owner, you can either copy and save these files yourself as a domain user, so that you become the owner for just these files. Or, if you have permissions, you can manually change the owner. Or alternatively, you can supply a specific email address (such as your own or a group address for the IT department) instead of the **[Source File Owner Email]** variable, which means that all files you protect by using this script uses this email address to define the new owner.

- Run the command as: Select Local System

- On the Condition tab:

- **Property:** Select RMS
- **Operator:** Select Equal
- **Value:** Select Yes

- On the Schedule tab:

- **Run at:** Configure your preferred schedule.

Allow plenty of time for the script to complete. Although this solution protects all files in the folder, the script runs once for each file, each time. Although this takes longer than protecting all the files at the same time, which the Azure Information Protection client supports, this file-by-file configuration for FCI is more powerful. For example, the protected files can have different owners (retain the original owner) when you use the **[Source File Owner Email]** variable, and this file-by-file action is required if you later change the configuration to selectively protect files rather than all files in a folder.

- **Run continuously on new files:** Select this checkbox.

#### **Test the configuration by manually running the rule and task**

1. Run the classification rule:
  - a. Click **Classification Rules > Run Classification With All Rules Now**
  - b. Click **Wait for classification to complete**, and then click **OK**.
2. Wait for the **Running Classification** dialog box to close and then view the results in the automatically displayed report. You should see 1 for the **Properties** field and the number of files in your folder. Confirm by using File Explorer and checking the properties of files in your chosen folder. On the **Classification** tab, you should see **RMS** as a property name and **Yes** for its **Value**.
3. Run the file management task:

- a. Click **File Management Tasks > Protect files with RMS > Run File Management Task Now**
  - b. Click **Wait for the task to complete**, and then click **OK**.
4. Wait for the **Running File Management Task** dialog box to close and then view the results in the automatically displayed report. You should see the number of files that are in your chosen folder in the **Files** field. Confirm that the files in your chosen folder are now protected by Rights Management. For example, if your chosen folder is C:\FileShare, type the following command in a Windows PowerShell session and confirm that no files have a status of **Unprotected**:

```
foreach ($file in (Get-ChildItem -Path C:\FileShare -Force | where {!$_.PSIsContainer})) {Get-RMSFileStatus -f $file.PSPPath}
```

#### TIP

Some troubleshooting tips:

- If you see **0** in the report, instead of the number of files in your folder, this output indicates that the script did not run. First, check the script itself by loading it in Windows PowerShell ISE to validate the script contents and try running it one time in the same PowerShell session, to see if any errors are displayed. With no arguments specified, the script tries to connect and authenticate to the Azure Rights Management service.
  - If the script reports that it couldn't connect to the Azure Rights Management service (Azure RMS), check the values it displays for the service principal account, which you specified in the script. For more information about how to create this service principal account, see [Prerequisite 3: To protect or unprotect files without interaction](#) from the Azure Information Protection client admin guide.
  - If the script reports that it could connect to Azure RMS, next check that it can find the specified template by running **Get-RMSTemplate** directly from Windows PowerShell on the server. You should see the template you specified returned in the results.
- If the script by itself runs in Windows PowerShell ISE without errors, try running it as follows from a PowerShell session, specifying a file name to protect and without the **-OwnerEmail** parameter:

```
powershell.exe -Noprofile -Command "<path>\RMS-Protect-FCI.ps1 -File '<full path and name of a file>' -TemplateID <template GUID>"
```

- If the script runs successfully in this Windows PowerShell session, check your entries for **Executive** and **Argument** in the file management task action. If you have specified **-OwnerEmail [Source File Owner Email]**, try removing this parameter.

If the file management task works successfully without **-OwnerEmail [Source File Owner Email]**, check that the unprotected files have a domain user listed as the file owner, rather than **SYSTEM**. To make this check, use the **Security** tab for the file's properties, and then click **Advanced**. The **Owner** value is displayed immediately after the file **Name**. Also, verify that the file server is in the same domain or a trusted domain to look up the user's email address from Active Directory Domain Services.

- If you see the correct number of files in the report but the files are not protected, try protecting the files manually by using the **Protect-RMSFile** cmdlet, to see if any errors are displayed.

When you have confirmed that these tasks run successfully, you can close File Resource Manager. New files are automatically classified and protected when the scheduled tasks run.

## Action required if you make changes to the Rights Management template

If you make changes to the Rights Management template that the script references, the computer account that runs the script to protect the files does not automatically get the updated template. In the script, locate the commented out `Get-RMSTemplate -Force` command in the Set-RMSConnection function, and remove the comment character at the beginning of the line. The next time the script runs, the updated template is downloaded. To optimize performance so that templates don't download unnecessarily, you can then comment out this line again.

If the changes to the template are important enough to reprotect the files on the file server, you can do this interactively by running the Protect-RMSFile cmdlet with an account that has the Export or Full Control usage rights for the files.

Also run this line in the script if you publish a new template that you want to use for FCI, and change the template ID in the argument line for the custom file management task.

## Modifying the instructions to selectively protect files

When you have the preceding instructions working, it's then easy to modify them for a more sophisticated configuration. For example, protect files by using the same script but only for files that contain personal identifiable information, and perhaps select a template that has more restrictive rights.

To make this modification, use one of the built-in classification properties (for example, **Personally Identifiable Information**) or create your own new property. Then create a new rule that uses this property. For example, you might select the **Content Classifier**, choose the **Personally Identifiable Information** property with a value of **High**, and configure the string or expression pattern that identifies the file to be configured for this property (such as the string "**Date of Birth**").

Now all you need to do is create a new file management task that uses the same script but perhaps with a different template, and configure the condition for the classification property that you have just configured. For example, instead of the condition that we configured previously (**RMS property, Equal, Yes**), select the **Personally Identifiable Information** property with the **Operator** value set to **Equal** and the **Value of High**.

## Next steps

You might be wondering: [What's the difference between Windows Server FCI and the Azure Information Protection scanner?](#)

# Windows PowerShell script for Azure RMS protection by using File Server Resource Manager FCI

7/20/2020 • 3 minutes to read • [Edit Online](#)

Applies to: [Azure Information Protection](#), Windows Server 2016, Windows Server 2012, Windows Server 2012 R2

Instructions for: [Azure Information Protection client for Windows](#)

This page contains the sample script to copy and edit, as described in [RMS protection with Windows Server File Classification Infrastructure](#).

This script uses a minimum version of 1.3.155.2 for the AzureInformationProtection module. Run the following command to check the version: `(Get-Module AzureInformationProtection -ListAvailable).Version`

**\*\*Disclaimer\*\*: This sample script is not supported under any Microsoft standard support program or service. This sample script is provided AS IS without warranty of any kind.**

```
<#
.SYNOPSIS
 Helper script to protect all file types using the Azure Rights Management service and FCI.
.DESCRIPTION
 Protect files with the Azure Rights Management service and Windows Server FCI, using an RMS template ID
 and AzureInformationProtection module minimum version 1.3.155.2.
#>
param(
 [Parameter(Mandatory = $false)]
 [ValidateScript({ If($_ -eq "") {$true} else { if (Test-Path -Path $_ -PathType Leaf) {$true} else
{throw "Can't find file specified"} } })]
 [string]$File,

 [Parameter(Mandatory = $false)]
 [string]$TemplateID,

 [Parameter(Mandatory = $false)]
 [string]$OwnerMail,

 [Parameter(Mandatory = $false)]
 [string]$AppPrincipalId = "<enter your AppPrincipalId here>",

 [Parameter(Mandatory = $false)]
 [string]$SymmetricKey = "<enter your key here>",

 [Parameter(Mandatory = $false)]
 [string]$BposTenantId = "<enter your BposTenantId here>"
)

script information
[String] $Script:Version = 'version 3.4'
[String] $Script:Name = "RMS-Protect-FCI.ps1"

#global working variables
[switch] $Script:isScriptProcess = $False # Controls the script process. If false, the script gracefully stops
running.

Functions (general helper)**
function Get-ScriptName(){
```

```

 return $MyInvocation.ScriptName.Substring($MyInvocation.ScriptName.LastIndexOf('\') + 1,
$MyInvocation.ScriptName.LastIndexOf('.') - $MyInvocation.ScriptName.LastIndexOf('\') - 1)
}

Functions (script specific)**
function Check-Module{

 param ([String]$Module = $(Throw "Module name not specified"))

 [bool]$isResult = $False

 #try to load the module
 if ((get-module -list -name $Module) -ne $nil)
 {

 $isResult = $True
 } else

 {

 $isResult = $False
 }

 return $isResult
}

function Protect-File ($ffile, $ftemplateId, $fownermail) {

 [bool] $returnValue = $false
 try {
 If ($OwnerMail -eq $null -or $OwnerMail -eq "") {
 $protectReturn = Protect-RMSFile -File $ffile -InPlace -DoNotPersistEncryptionKey All -TemplateID
$ftemplateId
 $returnValue = $true
 Write-Host ("Information: " + "Protected File: $ffile with Template: $ftemplateId")
 } else {
 $protectReturn = Protect-RMSFile -File $ffile -InPlace -DoNotPersistEncryptionKey All -TemplateID
$ftemplateId -OwnerEmail $fownermail
 $returnValue = $true
 Write-Host ("Information: " + "Protected File: $ffile with Template: $ftemplateId, set Owner:
$fownermail")
 }
 } catch {
 Write-Host ("ERROR" + "During protection of file: $ffile with Template: $ftemplateId")
 }
 return $returnValue
}

function Set-RMSConnection ($fappId, $fkey, $fbposId) {

 [bool] $returnValue = $false
 try {
 Set-RMSServerAuthentication -AppPrincipalId $fappId -Key $fkey -BposTenantId $fbposId
 Write-Host ("Information: " + "Connected to Azure RMS Service with BposTenantId: $fbposId using
AppPrincipalId: $fappId")
Get-RMSTemplate -Force
 $returnValue = $true
 } catch {
 Write-Host ("ERROR" + "During connection to Azure RMS Service with BposTenantId: $fbposId using
AppPrincipalId: $fappId")

 }
 return $returnValue
}

Main Script (Script)**
Write-Host ("== " + $Script:Name + " " + $Version + " ==")

$Script:isScriptProcess = $True

```

```

Validate Azure RMS connection by checking the module and then connection
if ($Script:isScriptProcess) {
 if (Check-Module -Module AzureInformationProtection){
 $Script:isScriptProcess = $True
 } else {

 Write-Host ("The AzureInformationProtection module is not loaded") -foregroundcolor "yellow" -
backgroundcolor "black"
 $Script:isScriptProcess = $False
 }
}

if ($Script:isScriptProcess) {
#Write-Host ("Try to connect to Azure RMS with AppId: $AppPrincipalId and BPOSID: $BposTenantId")
 if (Set-RMSConnection $AppPrincipalId $SymmetricKey $BposTenantId) {
 Write-Host ("Connected to Azure RMS")

 } else {
 Write-Host ("Couldn't connect to Azure RMS") -foregroundcolor "yellow" -backgroundcolor "black"
 $Script:isScriptProcess = $False
 }
}

Start working loop
if ($Script:isScriptProcess) {
 if (!($File -eq $null) -or ($File -eq ""))) {
 if (!(Protect-File -ffile $File -ftemplateID $TemplateID -fownermail $OwnerMail)) {
 $Script:isScriptProcess = $False
 }
 }
}

Closing
if (!$Script:isScriptProcess) { Write-Host "ERROR occurred during script process" -foregroundcolor "red" -
backgroundcolor "black"}
write-host ("== " + $Script:Name + " " + $Version + " ==")
if (!$Script:isScriptProcess) { exit(-1) } else {exit(0)}

```

[Back to RMS protection with Windows Server File Classification Infrastructure.](#)

# Azure Information Protection Developer's Guide

5/8/2020 • 3 minutes to read • [Edit Online](#)

This guide will orient you to tools for extending and integrating with Azure Information Protection's rights management service.

The current Azure Information Protection SDK has the rights management component. A classification and labeling component are under development.

## Service Applications

Service applications provide capabilities to protect information when exporting from an enterprise content management system, a business application, or a cloud-based business solution. Data Loss Prevention (DLP) and Cloud Application Security (CAS) applications are examples of service applications. Our SDK for developing service applications is available through two programming models.

- [C++](#)
- [C# Managed API](#)

### Examples of service applications

- [IpcDlp](#) is a sample RMS-enabled DLP application that takes you through the basic steps that a DLP RMS-enabled application should perform by using the RMS File API for protecting and consuming restricted content.
- [IpcAzureApp](#) is a sample that demonstrates how to use RMS SDK in Azure applications to protect data in an Azure Blob Storage.
- [RmsFileWatcher](#) is a sample that demonstrates how to build a Windows application that watches directories in the file system and applies RMS protection policies on every change, for example file added or file modified.
- [ProtectFilesInDir](#) is a simple console application sample that takes a directory as input and protects all the files in that directory only, no recursion.

## PowerShell guides

Used by Azure Rights management administrators, PowerShell cmdlets are also useful for developing and testing your service applications. For more information, see [Using PowerShell with the Azure Information Protection client](#).

## User applications

User applications can be built with either the RMS SDK 2.1 or the RMS SDK 4.2. The 4.2 version is REST client based with operating system specific APIs for several popular OSs; iOS/OSX, Android, Linux, Windows. The 2.1 version is used for building native Windows-based applications.

### User application development guides

- [Developing your application](#)
- [Testing your application](#)
- [Deploying your application](#)

### User application samples

- [AzureIP Test](#) is a sample console application that allows you to encrypt documents with an Azure template or an ad-hoc policy.
- [IPCNotepad](#) is a sample RMS-enabled application that takes you through the basic steps each RMS-enabled

application should perform when protecting and consuming restricted content.

- [RmsDocumentInspector](#) is a tool can give information about any RMS protected file such as content-id or user rights.

## Development environment setup

The following guides lead you through OS specific setup steps for an application development environment using common tools.



## How-tos

Each of the following topics presents specific guidance for an aspect of implementing your application. Service applications are built using the RMS SDK 2.x. User applications are built using RMS SDK 4.x. The article link is attributed with the application type; service, user.

### General

- [How to enable document tracking and revocation \(service\)](#)
- [How to deploy your client](#)
- [How to deploy your service app into a different tenant](#)
- [How to install and configure an RMS Server \(service\)](#)
- [How to use document tracking \(user\)](#)
- [How to renew a symmetric key in Azure Information Protection](#)

### Security and authentication

- [How to configure your app service application to use Azure Active Directory login](#)
- [How to use Azure Active Directory Authentication \(ADAL\) authentication](#)
- [Configuring Azure RMS for authentication \(service\)](#)
- [How to set the API security mode \(service\)](#)
- [Enable your applications to use Azure RMS \(service\)](#)
- [How to register and RMS enable your app with Azure AD \(user\)](#)

### Configuration and performance management

- [How to add explicit owner rights \(service\)](#)
- [File API configuration \(service\)](#)
- [How to use built in rights \(user\)](#)
- [How to enable error and performance logging \(user\)](#)

## Introduction and datasheets

[Introduction to Azure Information Protection](#)

## Other resources

- [Security best practice guide](#)
- [Frequently Asked Questions for Azure Information Protection](#)

## Support articles

- [Supported file formats](#)
- [Supported platforms](#)
- [Understanding usage restrictions](#)

## **Message protocol and file formats**

- [Client-to-Server Protocol](#)
- [Rights-Managed Email Object Protocol](#)
- [Compound File Binary File Format](#)

## **Rights Managed email message**

- [.MSG File Format \(Part 1\)](#)
- [.MSG File Format \(Part 2\)](#)

## **API reference**

- [Windows API Reference](#)
  - [Windows SDK Error Codes](#)
- [Windows Phone and Windows Store API reference](#)
- [iOS/OSX API reference](#)
- [Android API reference](#)
- [Linux API reference](#)

## **Previous versions**

- [AD RMS SDK](#) is the first version of the RMS SDK.
- [AD RMS Scripting Tool](#) is an administrative tool for an AD RMS installation.

## **See also**

- [Developer terminology](#)
- [Terminology for Azure Information Protection - ITPro](#)

# Azure Information Protection Developer's Guide

5/8/2020 • 3 minutes to read • [Edit Online](#)

This guide will orient you to tools for extending and integrating with Azure Information Protection's rights management service.

The current Azure Information Protection SDK has the rights management component. A classification and labeling component are under development.

## Service Applications

Service applications provide capabilities to protect information when exporting from an enterprise content management system, a business application, or a cloud-based business solution. Data Loss Prevention (DLP) and Cloud Application Security (CAS) applications are examples of service applications. Our SDK for developing service applications is available through two programming models.

- [C++](#)
- [C# Managed API](#)

### Examples of service applications

- [IpcDlp](#) is a sample RMS-enabled DLP application that takes you through the basic steps that a DLP RMS-enabled application should perform by using the RMS File API for protecting and consuming restricted content.
- [IpcAzureApp](#) is a sample that demonstrates how to use RMS SDK in Azure applications to protect data in an Azure Blob Storage.
- [RmsFileWatcher](#) is a sample that demonstrates how to build a Windows application that watches directories in the file system and applies RMS protection policies on every change, for example file added or file modified.
- [ProtectFilesInDir](#) is a simple console application sample that takes a directory as input and protects all the files in that directory only, no recursion.

## PowerShell guides

Used by Azure Rights management administrators, PowerShell cmdlets are also useful for developing and testing your service applications. For more information, see [Using PowerShell with the Azure Information Protection client](#).

## User applications

User applications can be built with either the RMS SDK 2.1 or the RMS SDK 4.2. The 4.2 version is REST client based with operating system specific APIs for several popular OSs; iOS/OSX, Android, Linux, Windows. The 2.1 version is used for building native Windows-based applications.

### User application development guides

- [Developing your application](#)
- [Testing your application](#)
- [Deploying your application](#)

### User application samples

- [AzureIP Test](#) is a sample console application that allows you to encrypt documents with an Azure template or an ad-hoc policy.

- [IPCNotepad](#) is a sample RMS-enabled application that takes you through the basic steps each RMS-enabled application should perform when protecting and consuming restricted content.
- [RmsDocumentInspector](#) is a tool can give information about any RMS protected file such as content-id or user rights.

## Development environment setup

The following guides lead you through OS specific setup steps for an application development environment using common tools.



## How-tos

Each of the following topics presents specific guidance for an aspect of implementing your application. Service applications are built using the RMS SDK 2.x. User applications are built using RMS SDK 4.x. The article link is attributed with the application type; service, user.

### General

- [How to enable document tracking and revocation \(service\)](#)
- [How to deploy your client](#)
- [How to deploy your service app into a different tenant](#)
- [How to install and configure an RMS Server \(service\)](#)
- [How to use document tracking \(user\)](#)
- [How to renew a symmetric key in Azure Information Protection](#)

### Security and authentication

- [How to configure your app service application to use Azure Active Directory login](#)
- [How to use Azure Active Directory Authentication \(ADAL\) authentication](#)
- [Configuring Azure RMS for authentication \(service\)](#)
- [How to set the API security mode \(service\)](#)
- [Enable your applications to use Azure RMS \(service\)](#)
- [How to register and RMS enable your app with Azure AD \(user\)](#)

### Configuration and performance management

- [How to add explicit owner rights \(service\)](#)
- [File API configuration \(service\)](#)
- [How to use built in rights \(user\)](#)
- [How to enable error and performance logging \(user\)](#)

## Introduction and datasheets

[Introduction to Azure Information Protection](#)

## Other resources

- [Security best practice guide](#)
- [Frequently Asked Questions for Azure Information Protection](#)

## **Support articles**

- [Supported file formats](#)
- [Supported platforms](#)
- [Understanding usage restrictions](#)

## **Message protocol and file formats**

- [Client-to-Server Protocol](#)
- [Rights-Managed Email Object Protocol](#)
- [Compound File Binary File Format](#)

## **Rights Managed email message**

- [.MSG File Format \(Part 1\)](#)
- [.MSG File Format \(Part 2\)](#)

## **API reference**

- [Windows API Reference](#)
  - [Windows SDK Error Codes](#)
- [Windows Phone and Windows Store API reference](#)
- [iOS/OSX API reference](#)
- [Android API reference](#)
- [Linux API reference](#)

## **Previous versions**

- [AD RMS SDK](#) is the first version of the RMS SDK.
- [AD RMS Scripting Tool](#) is an administrative tool for an AD RMS installation.

## **See also**

- [Developer terminology](#)
- [Terminology for Azure Information Protection - ITPro](#)

# Rights Management SDK 4.2

3/11/2020 • 2 minutes to read • [Edit Online](#)

## IMPORTANT

Versions of the Microsoft Rights Management Service SDK released prior to March 2020 are deprecated; applications using earlier versions must be updated to use the March 2020 release. For full details, see the [deprecation notice](#).

No further enhancements are planned for the Microsoft Rights Management Service SDK. We strongly recommend adoption of the [Microsoft Information Protection SDK](#) for classification, labeling, and protection services.

## Purpose

The Rights Management SDK 4.2 is a simplified, next-generation API that enables a lightweight development experience in upgrading your device apps with information protection via Rights Management Services.

Developers can build apps that leverage Active Directory Rights Management Services (AD RMS) or Azure Rights Management to provide information protection and can easily protect or consume information, while transparently handling complex security practices such as key management, encryption and decryption, policy and permissions creation, secure caching, and communication with AD RMS and Azure RMS services.

## Developer audience

The RMS SDK 4.2 APIs use standard programming languages and models for each operating system so, they are easy and familiar to work with.

## Supported Operating Systems

This release, RMS SDK 4.2, is available for the following operating systems:

- Google Android
- Apple iOS and Mac OS X
- Windows Phone
- Windows Store
- Portable C++ for Linux flavored operating systems

## Sections

[Overview](#) - Rights Management Services is an information protection technology that helps safeguard digital information from unauthorized use. Through your rights-enabled applications, content owners will be able to define who can open, modify, print, forward, or take other actions with their content.

[Get started](#)- For this release of the RMS SDK 4.2, your quick start approach to a first application is through the development environment setup guides for each of the operating systems / platforms.

[Developer guidance and terms](#) - The focus of RMS SDK 4.2 is to help you build AD RMS-enabled applications that leverage Right Management Services, as simply as possible.

[API reference](#) - The RMS SDK 4.2 supports several operating systems noted in the table of contents following.

# RMS SDK 4.2 Deprecation Notice

7/20/2020 • 2 minutes to read • [Edit Online](#)

*Applicable to all RMS SDK 4.2 versions release before March 2020*

On March 3, 2020, an update to the RMS SDK 4.2 for Android, iOS, and OSX was released via Microsoft Download Center. This update is mandatory for all applications that use these RMS SDK platforms today.

On Tuesday, September 15, 2020 versions of the RMS SDK released prior to March of 2020 will fail to connect to the Azure Rights Management Service endpoint. Applications consuming RMS SDK 4.2 must update prior to this date.

## Reason for Change

Previous versions of the RMS SDK use certificate pinning to ensure that the RMS-enabled client is communicating with the RMS service, receiving a certificate chained to a specific, expected root CA.

Modern browsers use certificate transparency logs to verify that certificates have been issued to legitimate domain owners and that those certificates are issued by trusted root certification authorities.

To better support modern browsers, on September 15, 2020, the Microsoft will update the certificate for <https://api.aadrm.com> to a new certificate issued by a globally trusted root CA that reports issued certificates to certificate transparency logs trusted by modern browsers. Once this change is complete, legacy versions of RMS SDK attempting to perform certificate pinning to the expected root certificate will fail to find that certificate and will fail to connect.

## Client Impact

The following Microsoft applications use the RMS SDKs today. Updates will be made available for these platforms and devices should be updated prior to the September deadline.

- Office 2019 for Mac
- Office 2016 for Mac
- Word, Excel, and PowerPoint for iOS
- Word, Excel, and PowerPoint for Android

## Resources

- Android: <https://www.microsoft.com/download/details.aspx?id=43673>
- iOS: <https://www.microsoft.com/download/details.aspx?id=43674>
- macOS: <https://www.microsoft.com/download/details.aspx?id=43675>
- Linux: <https://azuread.github.io/rms-sdk-for-cpp/annotated.html>

# Overview

3/17/2020 • 3 minutes to read • [Edit Online](#)

## IMPORTANT

Versions of the Microsoft Rights Management Service SDK released prior to March 2020 are deprecated; applications using earlier versions must be updated to use the March 2020 release. For full details, see the [deprecation notice](#).

No further enhancements are planned for the Microsoft Rights Management Service SDK. We strongly recommend adoption of the [Microsoft Information Protection SDK](#) for classification, labeling, and protection services.

Microsoft Rights Management SDK 4.2 is an information protection technology and is available for several platforms. It provides a software developer kit (SDK) or framework, which is designed for client computers and devices to help protect access to and usage of information flowing through applications that are "rights-enabled". The SDKs for these platforms provide a simple API for an application developer to protect or consume digital content, retrieve templates and acquire policies from a server, and other related rights management tasks.

For more information on the currently supported platforms, see our developer documentation portal for [Microsoft Rights Management SDK](#).

The following are just a few of the scenarios possible:

- A law firm wants to prevent sensitive email messages from being printed or forwarded on a mobile device.
- The developers of computer-aided design and manufacturing software want to limit drawing access to a small group of users within the research division without requiring the use of passwords.
- The owners of a graphic design mobile app want to use a single license that allows free viewing of low-resolution copies of their images but requires payment for access to the high-resolution versions.
- The owners of an online document library want to enable rights to view, print, or edit documents based on the identity of the user, when documents are downloaded to a mobile device.
- A corporation wants to publish sensitive employee information to an internal website that restricts viewing and editing privileges to certain users.

MS RMS SDK 4.2 can be downloaded, with acknowledgment and acceptance of its license agreement, freely distributed with your third-party software to enable client access to content that has been rights-protected by use and deployment of AD RMS servers in your environment or Azure RMS services. For more information, see [Get started](#).

## SDK Highlights

MS RMS SDK 4.2 offers some new cool features that include the following:

- **Re-designed API** – MS RMS SDK 4.2 API was re-designed for maximum simplicity, so developers can enjoy a simple and transparent encryption and decryption API, which provides consistent RMS behaviors with minimum efforts.
- **Hybrid support for AD RMS and Azure RMS** – a single RMS enabled app can consume and protect content from both AD RMS server (using AD RMS's mobile device extension) and Azure RMS service. MS RMS SDK 4.2 transparently discovers the relevant end-point that IT administrators can configure.
- **Bring your own authentication library** – as an app developer you can choose which authentication library is used with MS RMS SDK 4.2. Whether it is [Azure AD Authentication Library](#) or your organization's custom library, MS RMS SDK 4.2 segregates the auth stack so you can choose the library that most fits your needs.

- **Bring your own user interface** - MS RMS SDK 4.2 now allows you to implement your customize user interface. From protecting content and choosing templates to showing and changing permissions while consuming protected content, MS RMS SDK 4.2 does not enforce any built-in UI on your apps. If you would like, however, you can use Microsoft RMS UI libraries for all platforms via our [GitHub account](#).
- **Access protected content offline** – MS RMS SDK 4.2 allows your app users to access protected content even when there is no internet connectivity. MS RMS SDK 4.2 securely caches the consumption policies of the protected content so your users can access RMS protected data offline.

Use the [Get started](#) guide to begin your protected information device app project.

## Related topics

- [Microsoft Rights Management SDK](#)
- [Get started](#)
- [Azure AD Authentication Library](#)
- [GitHub account](#)

# Get started

3/17/2020 • 2 minutes to read • [Edit Online](#)

## IMPORTANT

Versions of the Microsoft Rights Management Service SDK released prior to March 2020 are deprecated; applications using earlier versions must be updated to use the March 2020 release. For full details, see the [deprecation notice](#).

No further enhancements are planned for the Microsoft Rights Management Service SDK. We strongly recommend adoption of the [Microsoft Information Protection SDK](#) for classification, labeling, and protection services.

For this release of the Microsoft Rights Management SDK 4.2, your quick start approach to a first application is through the development environment setup guides for each of the operating systems / platforms. Begin creating your rights enabled application by:

1. Download the SDK package for your target operating system using the following table of links.

<a href="#">RMS SDK 4.2</a>
<a href="#">Android SDK</a>
<a href="#">iOS SDK</a>
<a href="#">Linux / C++ SDK</a> available on Github as an open source project
<a href="#">OS X SDK</a>
<a href="#">Windows Phone</a>
<a href="#">Windows Store Applications</a>

2. Proceed to the setup guide for your operating system.

The setup guides walk you through configuring up your development environment for creating your own based apps.

- [Android setup](#)
- [iOS and OS X setup](#)
- [Linux setup](#)
- [Windows Phone](#)
- [Windows Store Applications](#)

3. Check out the [SDK overview map](#).

4. For important **release notes** and **developer guidance**, see the [What's new](#) topic.

TOPIC	DESCRIPTION
<a href="#">What's new</a>	MS RMS SDK 4.2 takes RMS application enablement to a new level of ease and flexibility.

TOPIC	DESCRIPTION
<a href="#">Setup developer environment</a>	The following topics show you have to setup your development environment to work with the AD RMS SDK APIs for your particular operating system.
<a href="#">Code examples</a>	MS RMS SDK 4.2 includes example code and working projects for some supported operating systems.
<a href="#">Community resources</a>	Active Directory Rights Management Services is well supported by a growing community of developers on multiple platforms.

# What's new and Release notes

5/8/2020 • 7 minutes to read • [Edit Online](#)

## IMPORTANT

Versions of the Microsoft Rights Management Service SDK released prior to March 2020 are deprecated; applications using earlier versions must be updated to use the March 2020 release. For full details, see the [deprecation notice](#).

No further enhancements are planned for the Microsoft Rights Management Service SDK. We strongly recommend adoption of the [Microsoft Information Protection SDK](#) for classification, labeling, and protection services.

## What's new

This topic outlines important changes and features in this new version of the RMS SDK v4.x.

- [New for July 2017](#)
- [October 2016 update](#)
- [June 2016 update](#)
- [December 2015 update](#)
- [July 2015 update - Adds support for Linux / C++ development](#)
- [May 2015 update - Adds logging control](#)
- [February 2015 update - Adds Windows Store application support](#)
- [January 2015 Update - Adds WinPhone platform support](#)
- [October 2014 update - Upgrade to Microsoft RMS SDK 4.1](#)
- [Release notes](#)
- [Frequently asked questions](#)

### New for July 2017

The update for our July release included incrementing the revision of the SDK, now 4.2.5.

- Android SDK: Your app can now **set the logging level on-the-fly** with the Android SDK. For more information, see [How to: Enable error and performance logging](#)
- The iOS SDK does not support logging level.
- The SDK now returns an error for a NULL access token.

### October 2016 update

- Implement a few back-end bug fixes.
- Enable bitcode for the Apple iOS/OSX SDK.

### June 2016 update

- **Support for Modern Authentication** - brings Active Directory Authentication Library (ADAL)-based sign-in to RMS enlightened apps. It enables sign-in features like Multi-Factor Authentication (MFA), SAML-based third-party Identity Providers with RMS client applications, smart card, and certificate-based authentication and it removes the need for RMS enlightened apps to use the basic authentication protocol.
- **Document Tracking support** - developers can now enable document tracking when protecting document in their apps
- Performance improvements
- Bug fixes

## **December 2015 update**

With this release, the RMS SDK for devices is now at version 4.2 and adds:

- Document tracking, RMS On-line only, for iOS/OS X and Android operating systems.

For details and usage guidance on iOS/OS X, see the [MSLicenseMetadata](#) class, which provides tracking information and the additional document tracking registration method on [MSUserPolicy](#). There are similar additions for Android to [LicenseMetadata](#) and [UserPolicy](#).

For a detailed description of the document tracking feature, see [How to: Use document tracking](#).

- A set of synchronous methods that parallel the asynchronous versions for the Android API:

[CustomProtectedInputStream.create synchronous method](#)

[CustomProtectedOutputStream.create synchronous method](#)

[ProtectedFileInputStream.create synchronous method](#)

[ProtectedFileOutputStream.create synchronous method](#)

[TemplateDescriptor.getTemplates synchronous method](#)

[UserPolicy.acquire synchronous method](#)

[UserPolicy.create \(PolicyDescriptor...\) synchronous method\\*\\*](#)

[UserPolicy.create \(TempalteDescriptor...\) synchronous method](#)

- A new [ProtectedBuffer](#) class has been added to the Android API.
- Updates to improve error messaging and troubleshooting experience.
- Significant performance improvements for cryptographic operations.

## **July 2015 Update - Adds support for Linux / C++ development**

This release adds the following updates:

- RMS SDK 4.1 for Linux platforms

For more information, see [Get started](#).

## **May 2015 Update - Adds logging control**

This release adds support for the following updates:

- iOS

App encrypt and decrypt can operate independently and in parallel.

For more information, see [MSProtector](#).

Log level control settings enabled.

For more information, see [How to: Enable error and performance logging](#)

Cache clearing support added.

For more information, see [MSProtection:resetStateWithCompletionBlock](#).

## **February 2015 Update - Adds Windows Store application support**

This release adds support for Windows Store applications and provides functional parity with the Windows Phone, Android, and iOS/OS X release of the RMS SDK 4.1.

## **January 2015 Update - Adds WinPhone platform support**

This release adds support for the Windows Phone operating system and provides functional parity with the Android and iOS/OS X release of the RMS SDK 4.1.

## October 2014 Update - Upgrade to Microsoft RMS SDK 4.1

The version 4.1 release of the RMS SDK adds the following new features to the Google Android and Apple iOS / OS X.

- Android and iOS/OS X SDK API extensions for *user consent* processing, allowing user confirmation of SDK behaviors. Currently, document tracking and accessing unknown AD RMS service URLs are the supported consent types.

For more information, see as example, the Android API version of [ConsentCallback interface](#).

- iOS 8 and OS X 10.10 (Yosemite) are now supported. There have also been a few property name changes required by Xcode 6.

Example; MSUserPolicy.name changed to [MSUserPolicy.policyName](#).

## Release notes

This section outlines information about the current and previous releases of the Microsoft Rights Management SDK 4.x APIs that you, as a developer, want to be aware of.

### AD RMS SDK 4.1 - iOS / OS X and Android platforms Global Availability Release

- **AD RMS support** - IT administrators can use RMS enabled apps on mobile devices with the new AD RMS server's mobile device extensions.
- **Offline Consumption** - end users can access RMS protected data offline.
- **Segregated Auth** - developers can use their own authentication library for Azure RMS and AD RMS (or use the recommended [Azure AD Authentication Library \(ADAL\)](#)).
- **Segregated UI** - developers can build their user interface to protect and consume RMS protected documents.
- **Redesigned API** - developers can now enjoy a straightforward and transparent encryption and decryption API, which provides consistent RMS behaviors and user experience, with minimum effort.

### Common to all platforms

- The RMS SDK 4.x APIs are not *thread-safe*.

### Android

- When you use a sample app on an Amazon® Kindle device to view .ptxt attachments, you must first download the file before you view it.

**Solution** - a known issue that will be addressed later.

- An application that uses the SDK may crash if multi-instance is allowed.

**Solution** - Make sure the application does not allow multi-instance calls to the Android API.

- When I use the `ProtectedFileOutputStream.write( byte[] array, int offset, int length )` method with a length different from the `array.length` value, I am not able to consume the content later using the SDK.

**Solution** - This is a known issue. To mitigate it, either always pass a `byte[]` array with the same length value as the length parameter, or use the `ProtectedFileOutputStream.write(byte[] array)` method.

### iOS and OS X

- There are two dialects of Portuguese that our iOS and OS X SDKs support. Unfortunately, due to a bug, we do not currently support the first localization completely. Because of this bug, Portuguese is not fully

supported. Most of the text is translated, but not the UI.

1. Portuguese
2. Portuguese (Portugal)

#### iOS only

- The RMS SDK 4.x does not show the network activity indicator.

This is a known optional behavior for iOS according to the Apple Human Interface Guidelines.

#### OS X only

- The RMS SDK 4.x does not show the network activity indicator.

This is a known optional behavior for OS X according to the Apple Human Interface Guidelines.

- **Solution** - To create a multiple document interface (MDI) application using our OS X SDK, use the following guidance.

The following methods must not be run concurrently. In order to monitor for execution completion, use the completion block approach as noted.

- [MSProtectedData.protectedDataWithProtectedFile](#)
- [MSCustomProtectedData.customProtectedDataWithPolicy](#)

**Note** MDI applications are not supported by our iOS API.

## Frequently asked questions

### All platforms

**Q:** I don't see a **Custom Permissions** selection UI in the protection workflow. Why?

**A:** This is a known issue and will be addressed later.

**Q:** How do I get new organizational tenants to try out the SDK and sample applications?

**A:** To request credentials for Azure AD RMS test organizations, send email to [rmcstbeta@microsoft.com](mailto:rmcstbeta@microsoft.com).

**Q:** I don't see any test hierarchy discussion here in the documentation. Why?

**A:** There is no test hierarchy concept with the new AD RMS SDKs. You will always work with the production hierarchy.

**Q:** In the 2.1 version of the RMS SDK, a generated manifest was needed for each application implementing information protection. Is this still true for the 4.0 and later versions of the SDK?

**A:** No, manifests are no longer needed for the 3.0 and later versions of the Rights Management SDK.

### Android

**Q:** Which development environments has the SDK been tested with?

**A:** Eclipse Juno using Google API 15 and above.

**Q:** Can I call cancel() a cancel method from the UI thread? **A:** You should call cancel() from a non-UI thread, as it may abort network a connection.

### iOS

**Q:** Which platforms were verified for SDK development?

A: Xcode 5.0 with iOS 7 and later.

Q: I called a cancel() method on an operation, however I still got notification that the operation completed. Why?

A: Not all operations can be canceled, so a cancellation operation is executed as best as is possible.

OS x

Q: Sample app framework is adapted to Xcode 5, can I work with Xcode 4.6?

A: The OS X SDK works with Xcode 4.6 and later only, as well as OS X 10.8 and later.

# Setup developer environment

3/17/2020 • 2 minutes to read • [Edit Online](#)

## IMPORTANT

Versions of the Microsoft Rights Management Service SDK released prior to March 2020 are deprecated; applications using earlier versions must be updated to use the March 2020 release. For full details, see the [deprecation notice](#).

No further enhancements are planned for the Microsoft Rights Management Service SDK. We strongly recommend adoption of the [Microsoft Information Protection SDK](#) for classification, labeling, and protection services.

The following topics show you how to setup your development environment to work with the AD RMS SDK APIs for your particular operating system.

PLATFORM	DESCRIPTION
Android	Android applications can use the Microsoft Rights Management SDK 4.2 to enable integrated information protection in their applications by using Azure Active Directory Rights Management (AAD RM ).
Linux	Several flavors of Linux operating systems can now make use of the MS RMS SDK 4.2 to enable integrated information protection in their application by using the Azure Active Directory Rights Management (AAD RM).
iOS and OSX	iOS and OS X applications can use the MS RMS SDK 4.2 to enable integrated information protection in their application by using the Azure Active Directory Rights Management (AAD RM).
Windows Phone	Windows Phone applications can use the MS RMS SDK 4.2 to enable integrated information protection in their application by using the Azure Active Directory Rights Management (AAD RM).
Windows Store	Windows Store applications can use the MS RMS SDK 4.2 to enable integrated information protection in their application by using the Azure Active Directory Rights Management (AAD RM).

# Android setup

5/8/2020 • 3 minutes to read • [Edit Online](#)

## IMPORTANT

Versions of the Microsoft Rights Management Service SDK released prior to March 2020 are deprecated; applications using earlier versions must be updated to use the March 2020 release. For full details, see the [deprecation notice](#).

No further enhancements are planned for the Microsoft Rights Management Service SDK. We strongly recommend adoption of the [Microsoft Information Protection SDK](#) for classification, labeling, and protection services.

Android applications can use the Microsoft Rights Management SDK 4.2 to enable integrated information protection in their applications by using Azure Active Directory Rights Management (AAD RM).

This topic will guide you through setting up your environment for creating your own new apps .

- [Prerequisites](#)
- [Optional](#)
- [Configuring your development environment](#)
- [See Also](#)

## Prerequisites

We recommend the following software on your development system:

- Windows or OS X operating system to run the [Eclipse](#) development environment.
- This guide assumes that you are using the Eclipse SDK beginning with Eclipse Juno 4.2 and using a default installation.
- Java starting with Java 1.6.
- [Android Developer Tools \(ADT\) Plugin](#). NOTE - You might be asked to restart Eclipse to complete the installation.
- The MS RMS SDK 4.2 package for Android. For more information see, [Get started](#).

This SDK can be used to develop for Android 4.0.3 (API level 15) and later.

- Authentication library: We recommend that you use the [Azure AD Authentication Library \(ADAL\)](#). However, other authentication libraries that support OAuth 2.0 can be used as well.

For more information see, [ADAL for Android](#)

**Note** If your application will not be using the ADAL Library as the OAuth 2.0 authentication library, you should review this Android guidance, [Some SecureRandom Thoughts](#).

Read the [What's new](#) topic for information about API updates, release notes, and frequently asked questions (FAQ).

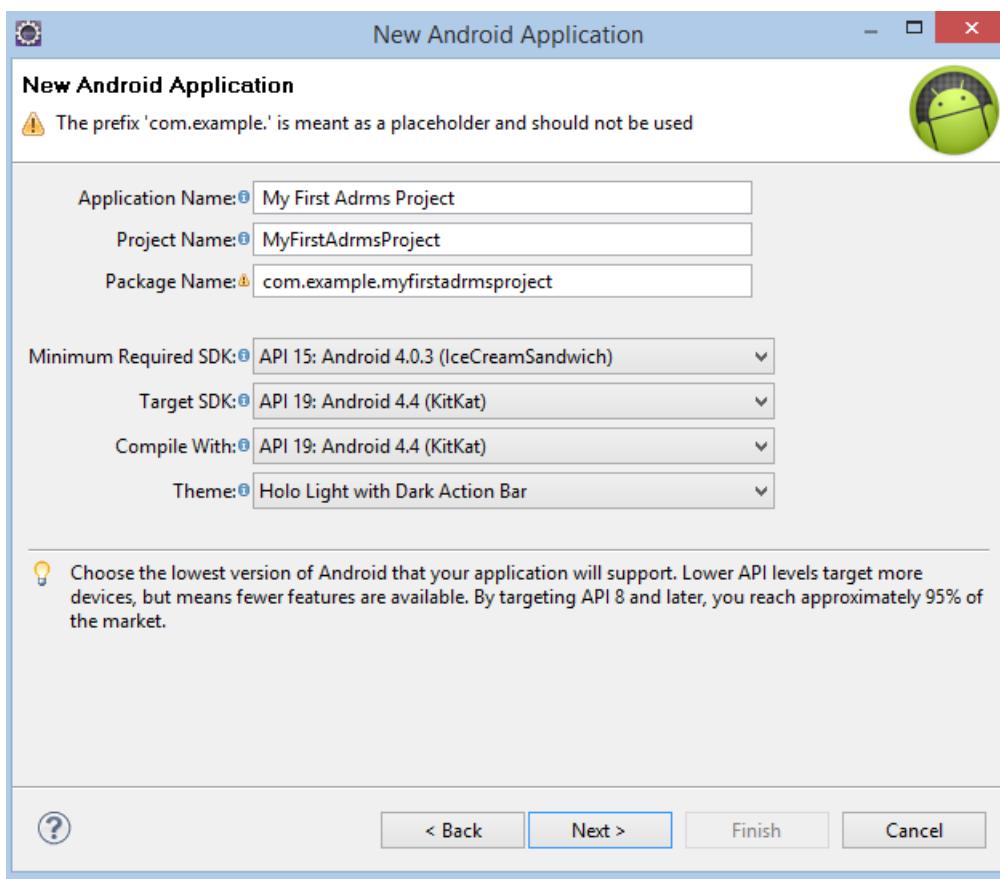
## Optional

Our UI library provides re-usable UI for consumption and protection operations for developers who don't want to create their own custom UI - [UI Library and Sample app for Android](#).

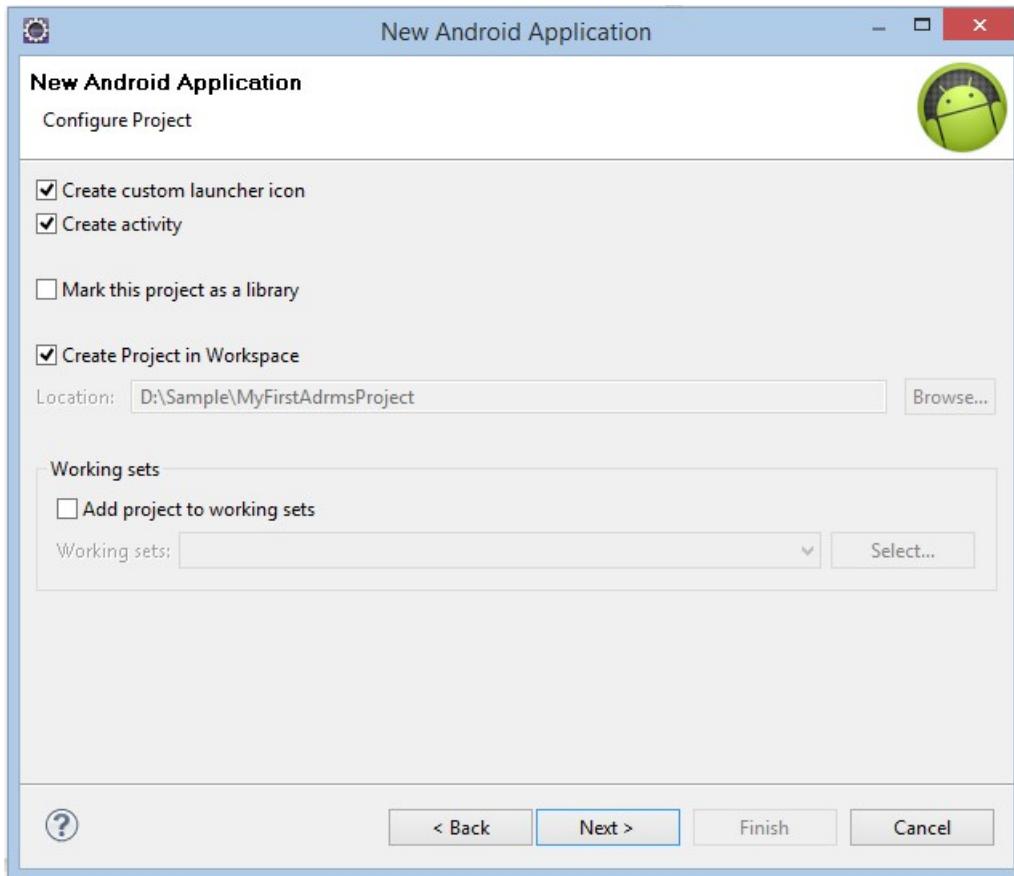
# Configuring your development environment

**Note** MS RMS SDK 4.2 Preview Release: In this preview release, the screen shots have not been updated to show the change in name of the pathes from com/microsoft/protection to com/microsoft/rightsmanagement. The text though, has been updated.

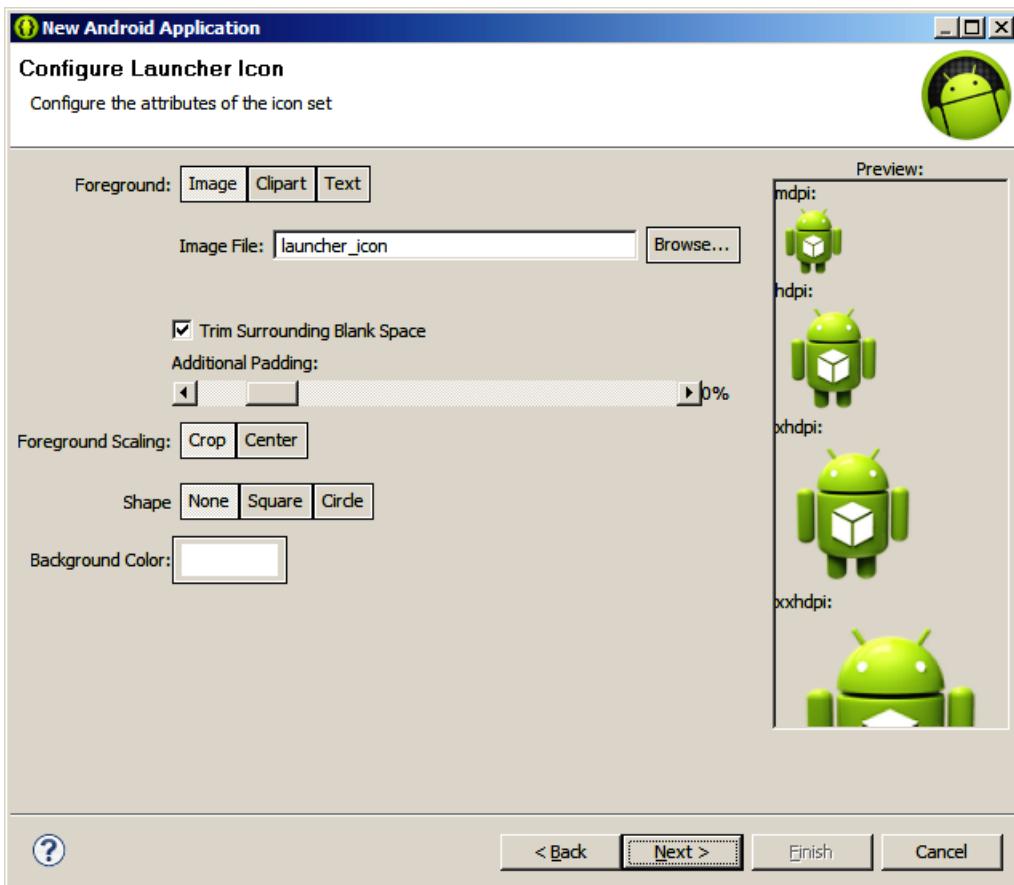
- Open the Eclipse development environment.
- To create a new Android Application project, on the **File** menu, click **New**, click **Project**, and then select **Android Application Project**.



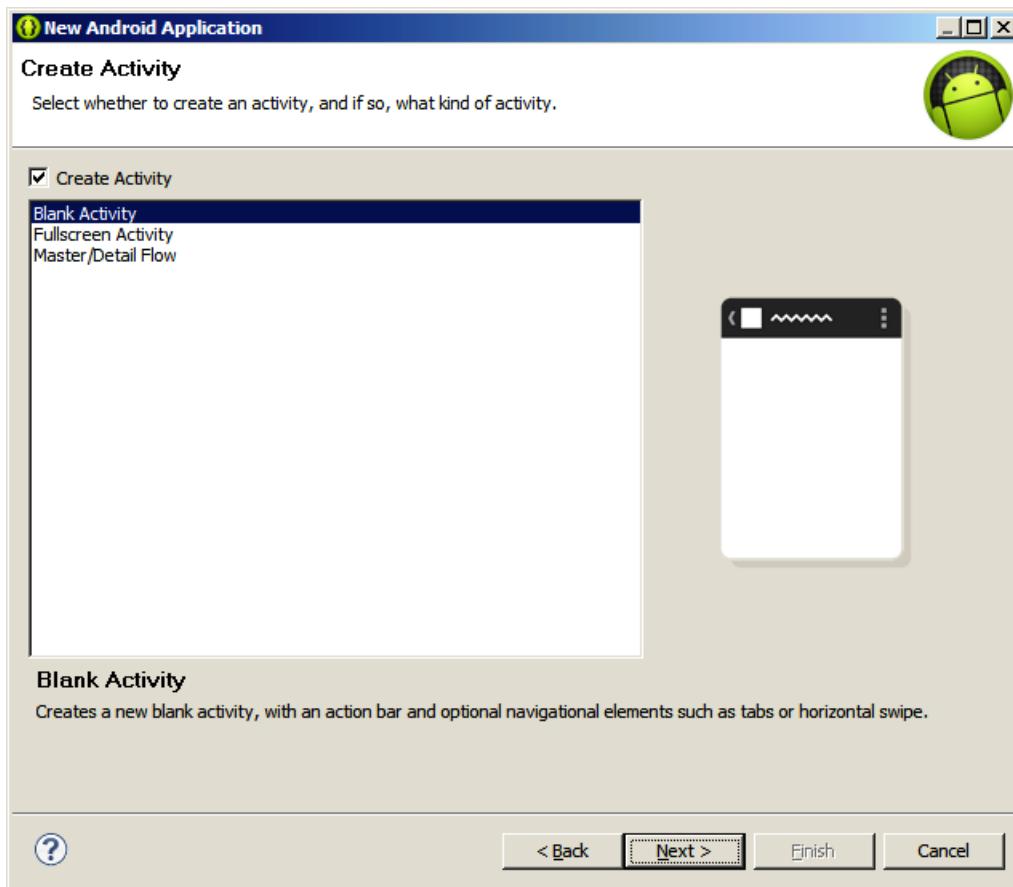
- Enter the application name. The project name and package name is filled based on the application name.
- Click **Next** and select where you want to create the workspace.



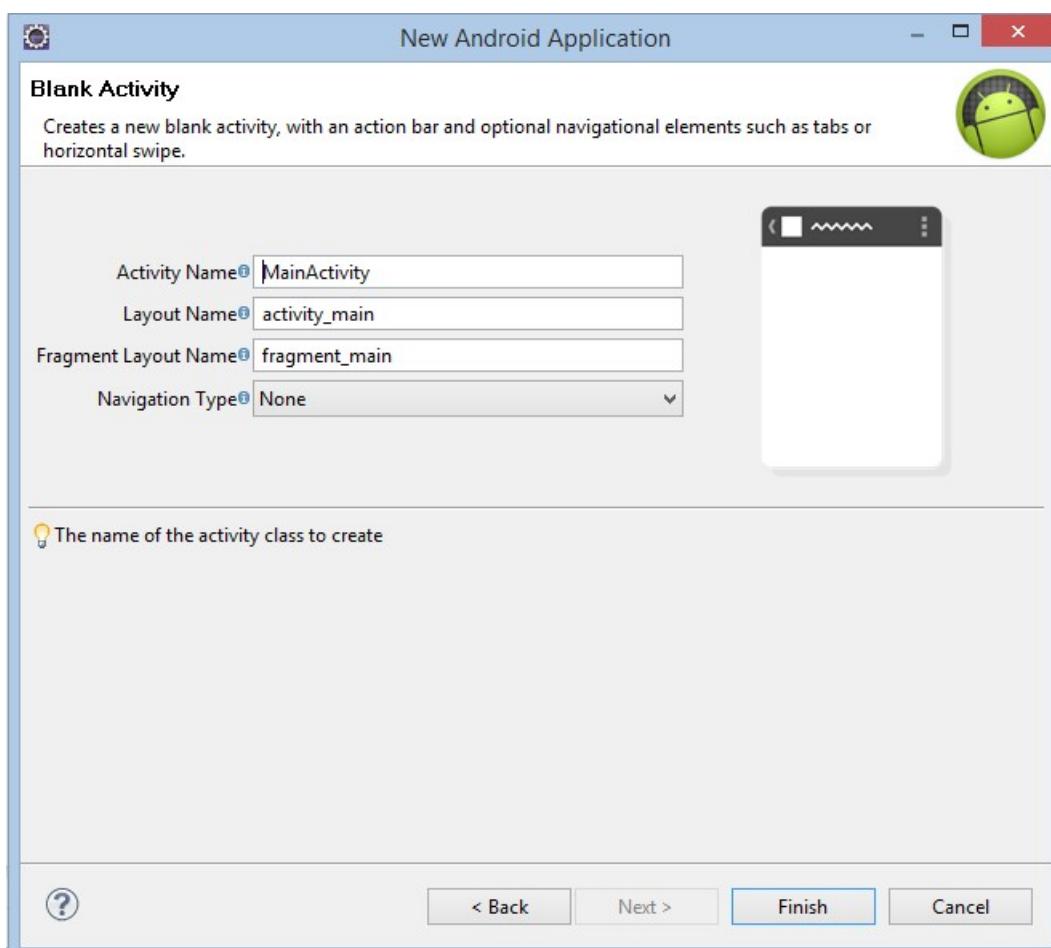
- Click **Next** and select an icon for your app.



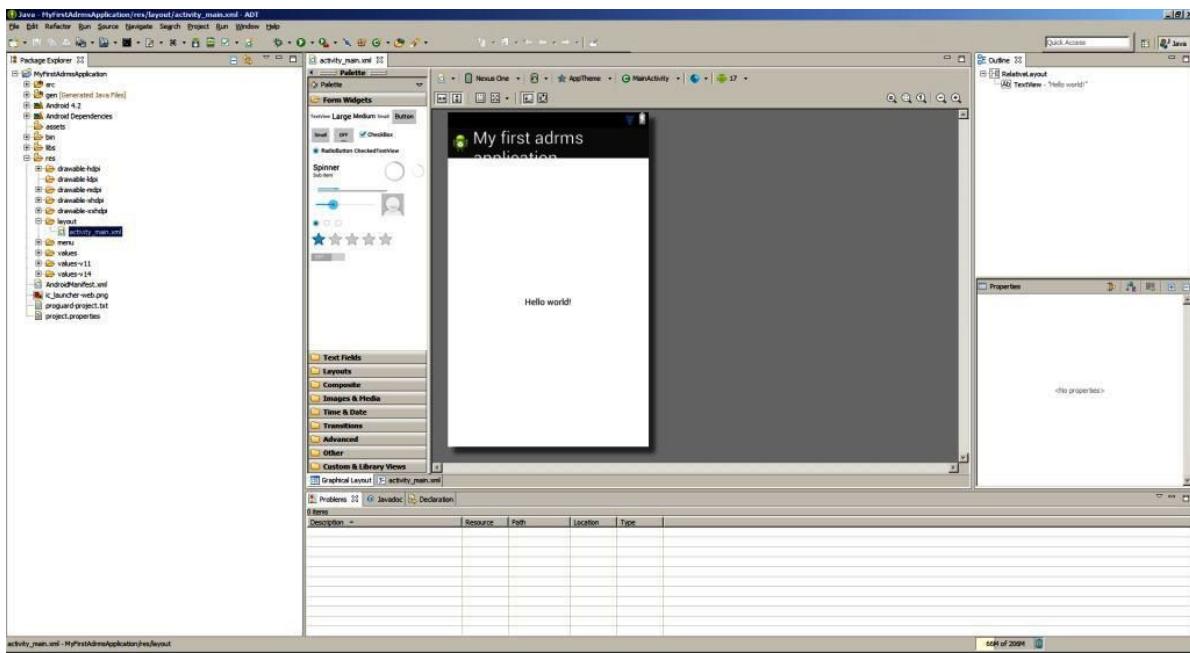
- Click **Next** and select **Blank Activity** to create the activity.



- Click **Next** and provide a name for the activity. You can leave *MainActivity* as the default name with a layout name of *activity\_main*.



- Click **Finish**.

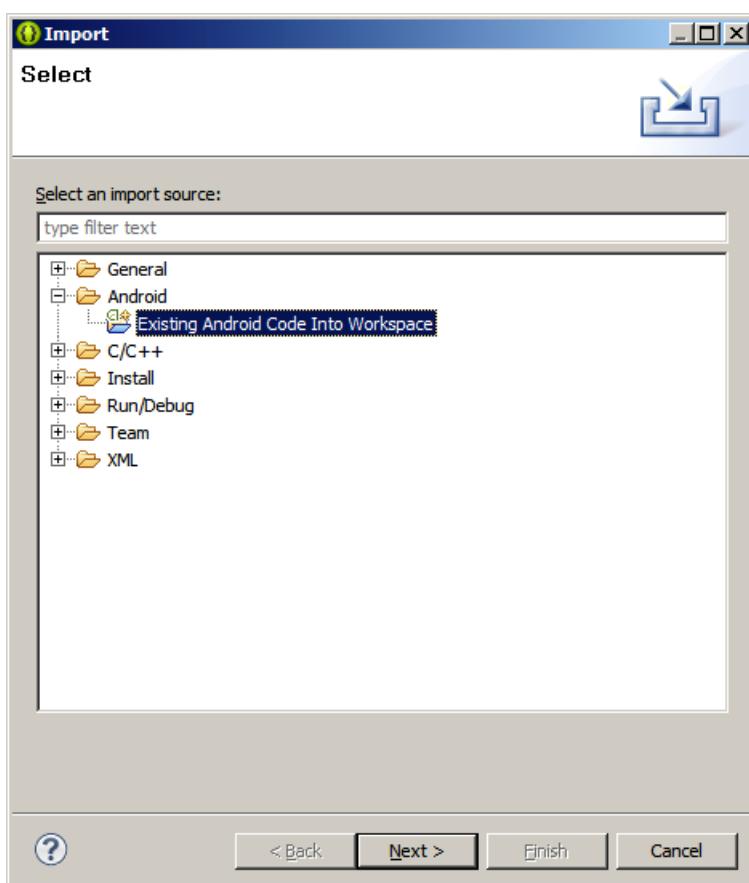


- Your project has been created, along with the main activity class *MainActivity.java*.

## Referencing the SDK

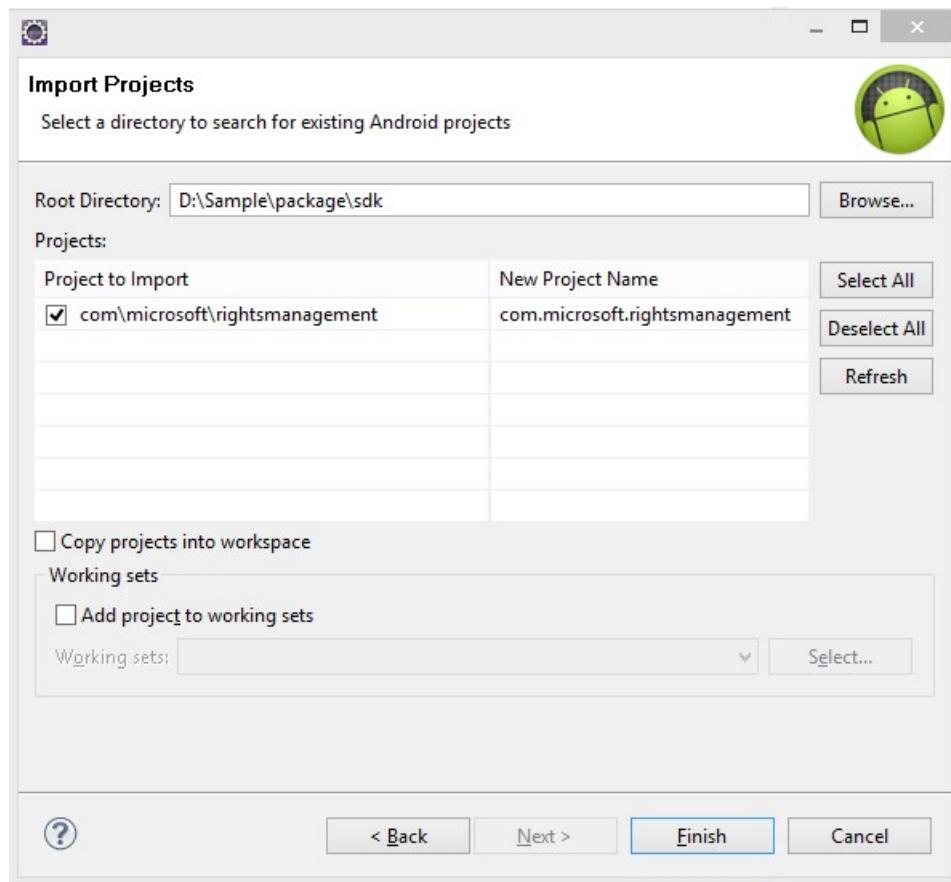
- Navigate to the folder in which you extracted the *adrms\_android\_sdk.zip*. In the "SDK > com > microsoft > rightsmanagement" folder, make sure the files *.classpath*, *.project*, and *project.properties* are not marked as read-only.
- To reference the SDK, you must import it to the workspace.

In Eclipse, click **File**. On the **File** menu, click **Import**. In the **Import** dialog box, select **Android / Existing Android Code into Workspace**.

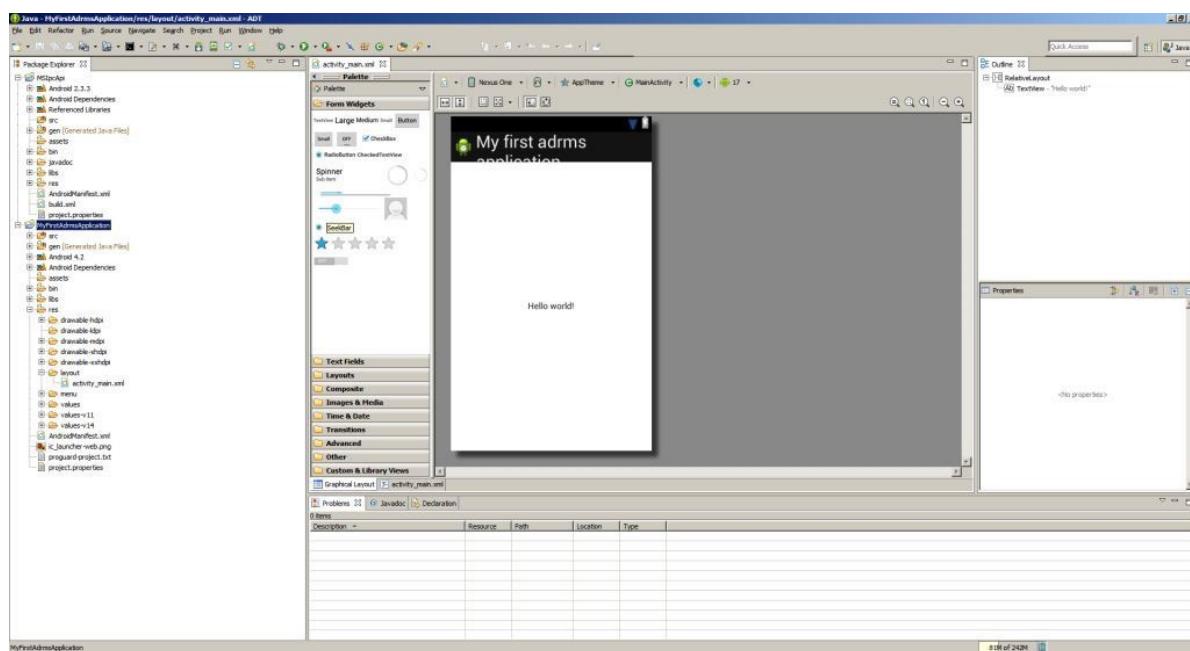


- Click **Next**. Navigate to select the folder in which you extracted the *adrms\_android\_sdk.zip*. The SDK should

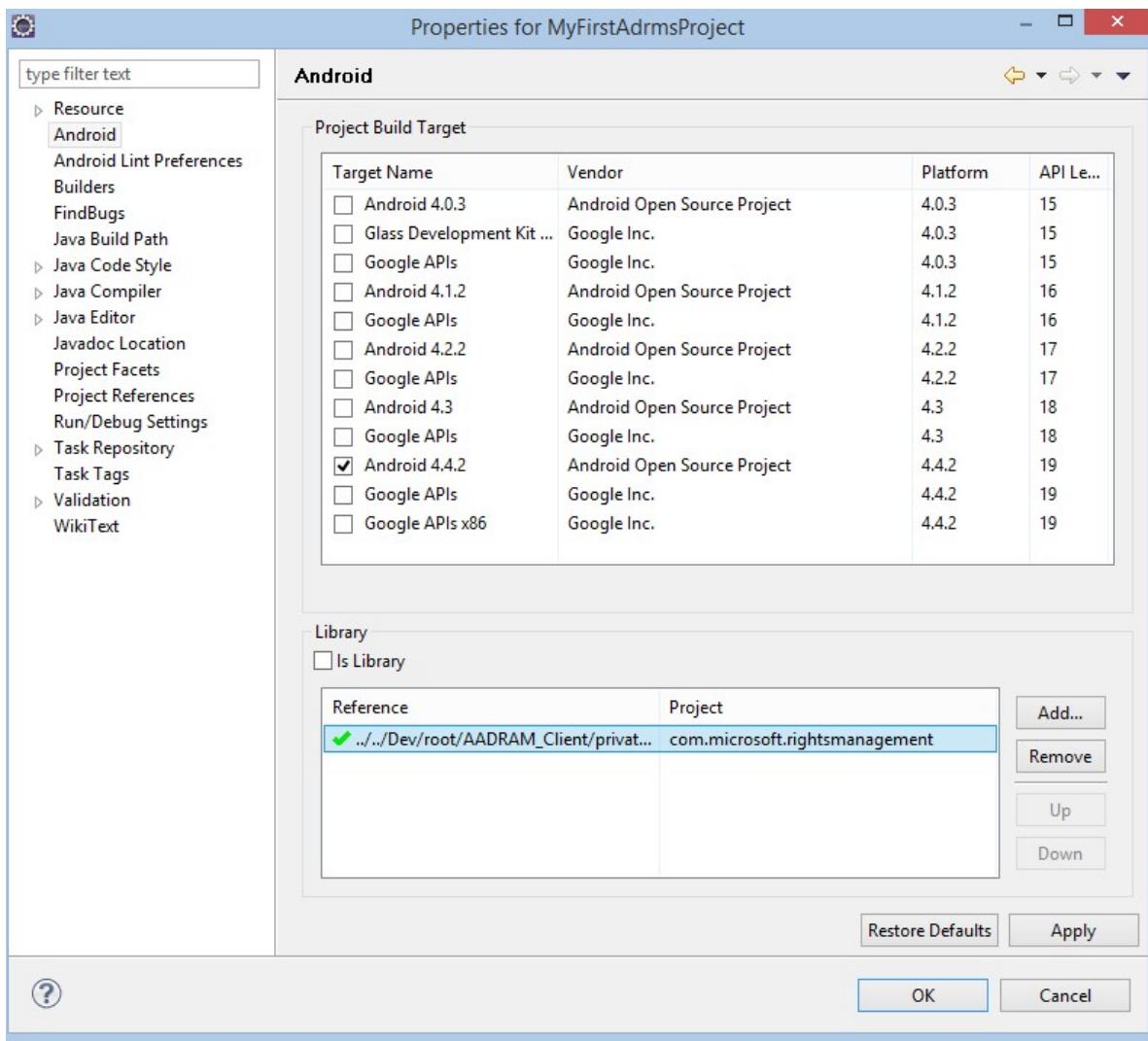
appear in the list as `com.microsoft.rightsmanagement`.



- When you click **Finish**, the SDK project appears as a sibling of your previously created application.



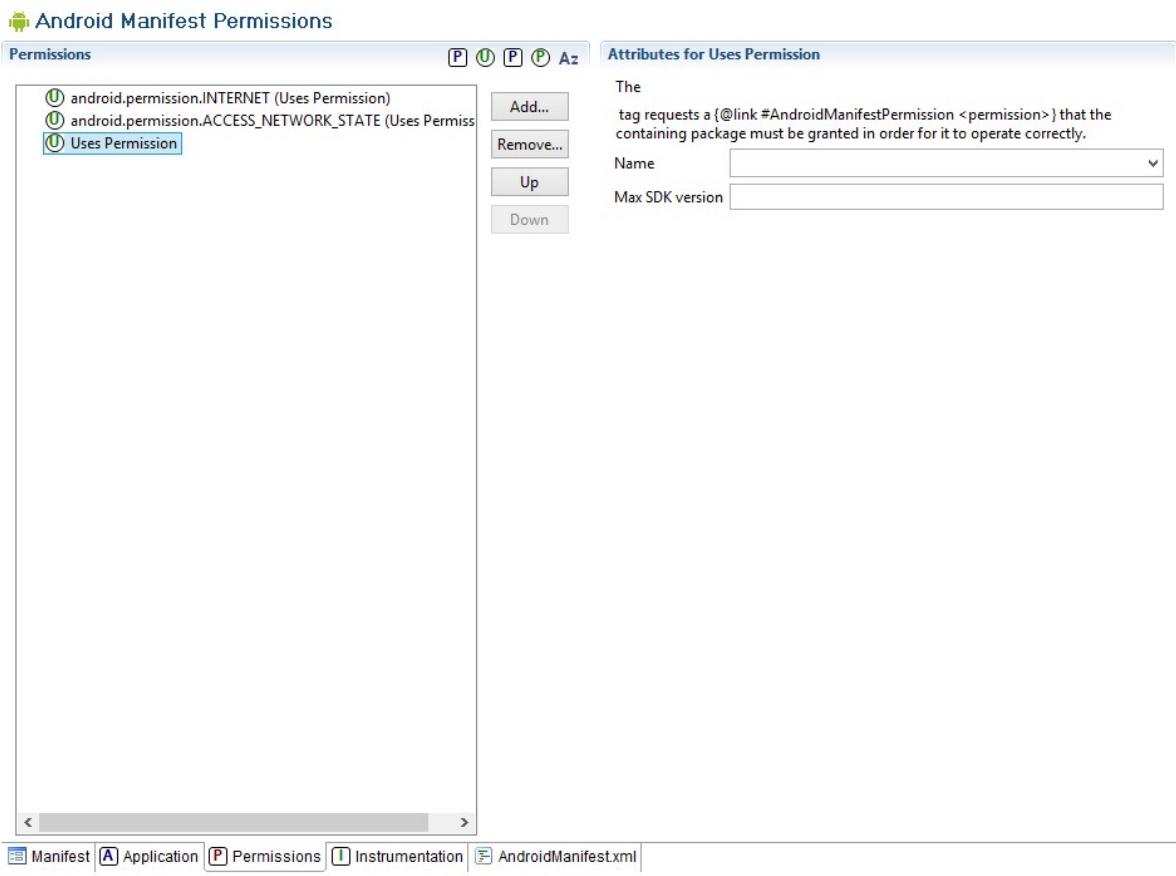
- Right-click the **Project** icon and view the properties for the project.
- Navigate to the **Android** tab.
- Click **Add**, and then select the `com.microsoft.rightsmanagement` library from the workspace.



- Click OK.

Because the MS RMS SDK 4.2 connects with AAD RM, the application has to be granted the **INTERNET** and **ACCESS\_NETWORK\_STATE**. To do so, open the *AndroidManifest.xml* file in the root of the project.

To add the permissions, click **Add**, and then select **Uses Permissions**.



- You can verify the manifest step by viewing the manifest in the text editor view. Make sure the following lines appear:

```
<uses-sdk
 android:minSdkVersion="15"
 android:targetSdkVersion="19"/>
<uses-permission android:name="android.permission.INTERNET"/>
<uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>
<uses-permission/>
```

**Note** The SDK uses the *android.support.v4*

- You are now ready to create your own new Android apps.

## See Also

[Get started](#)

[What's new](#)

[Developer terms and concepts](#)

[Android API Reference](#)

# Linux setup

3/17/2020 • 2 minutes to read • [Edit Online](#)

## IMPORTANT

Versions of the Microsoft Rights Management Service SDK released prior to March 2020 are deprecated; applications using earlier versions must be updated to use the March 2020 release. For full details, see the [deprecation notice](#).

No further enhancements are planned for the Microsoft Rights Management Service SDK. We strongly recommend adoption of the [Microsoft Information Protection SDK](#) for classification, labeling, and protection services.

Several flavors of Linux operating systems can now make use of the Microsoft Rights Management SDK 4.x to enable integrated information protection in their application by using the Azure Active Directory Rights Management (AAD RM).

- [Supported operating systems](#)
- [How to build and use](#)
- [See Also](#)

## Supported operating systems

- Ubuntu 14.04
- OpenSUSE 13.2
- CentOS 7

Libraries and samples have been successfully compiled on Windows and OSX as well, but these are not fully supported at this time.

## How to build and use

- [How to build libs and sample apps](#)
- [How to install and use app on user systems](#)

## See Also

- [Get started](#)
- [What's new](#)
- [Developer terms and concepts](#)

# iOS and OS X setup

5/8/2020 • 2 minutes to read • [Edit Online](#)

## IMPORTANT

Versions of the Microsoft Rights Management Service SDK released prior to March 2020 are deprecated; applications using earlier versions must be updated to use the March 2020 release. For full details, see the [deprecation notice](#).

No further enhancements are planned for the Microsoft Rights Management Service SDK. We strongly recommend adoption of the [Microsoft Information Protection SDK](#) for classification, labeling, and protection services.

iOS and OS X applications can use the Microsoft Rights Management SDK 4.2 to enable integrated information protection in their application by using the Azure Rights Management (Azure RMS).

This topic will guide you through setting up your environment for creating your own new apps.

**Note** This SDK does not support iPod Touch.

- [Prerequisites](#)
- [Optional](#)
- [Configuring your development environment](#)
- [See Also](#)

## Prerequisites

We recommend the following software on your development system:

- OS X is required for all iOS development.
- Xcode version 6.0 and later

Xcode is available through the [Mac App Store](#).

- The MS RMS SDK 4.2 package for iOS and OS X. For more information see, [Get started](#).

This SDK can be used to develop for iOS 7.0 and OS X 10.8 and later.

- Authentication library: We recommend that you use the [Azure AD Authentication Library \(ADAL\)](#). However, other authentication libraries that support OAuth 2.0 can be used as well.

For more information see, [ADAL for iOS](#) or [ADAL for OS X](#)

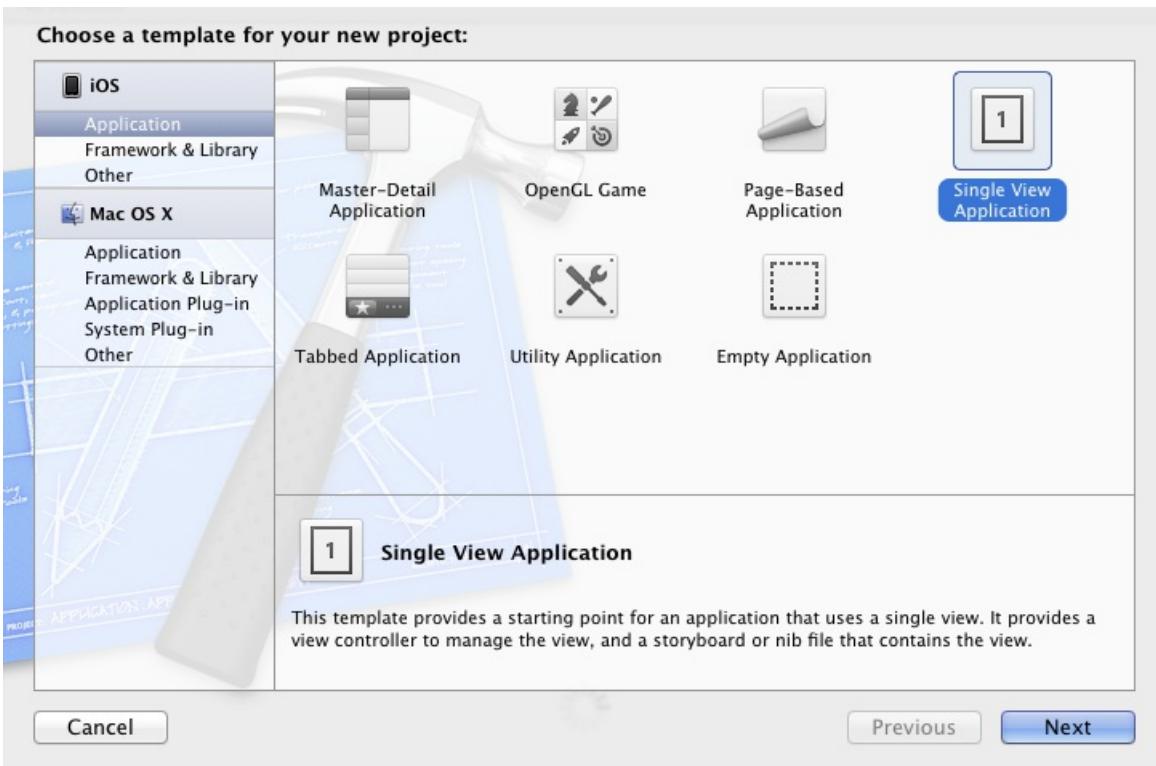
Read the [What's new](#) topic for information about API updates, release notes, and frequently asked questions (FAQ).

## Optional

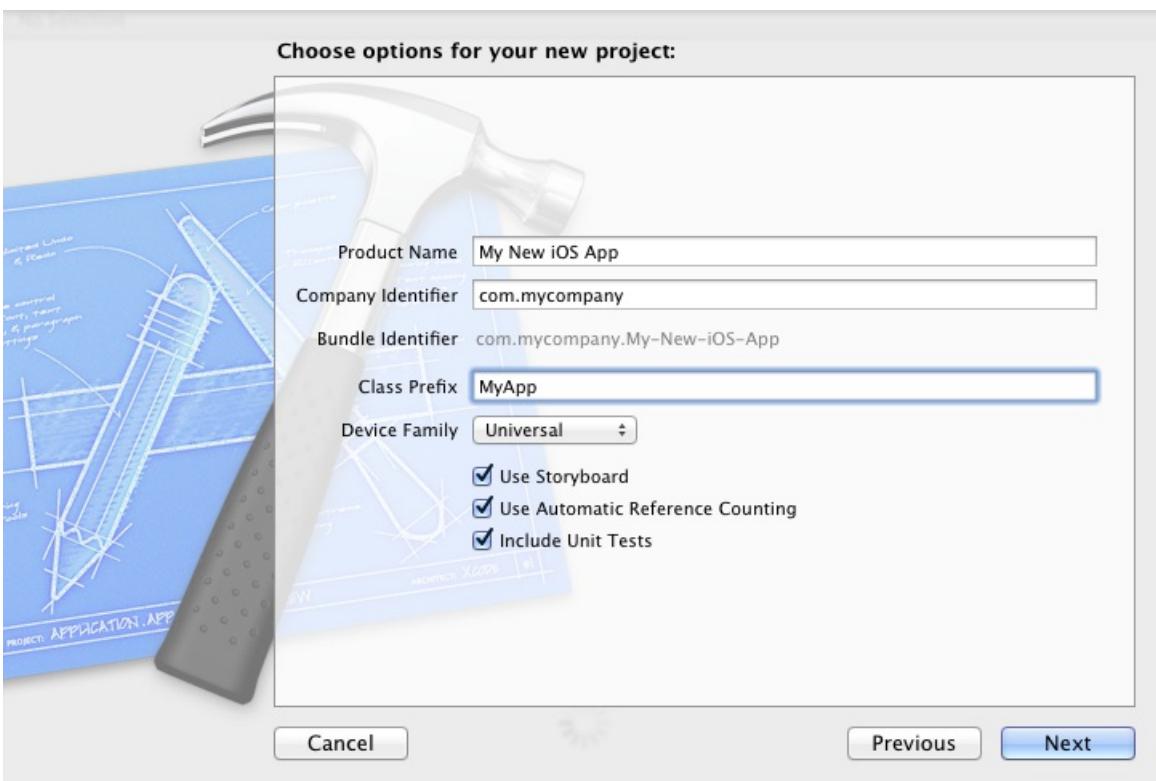
Our UI library provides re-usable UI for consumption and protection operations for developers who don't want to create their own custom UI - [UI Library and Sample app for iOS](#).

## Configuring your development environment

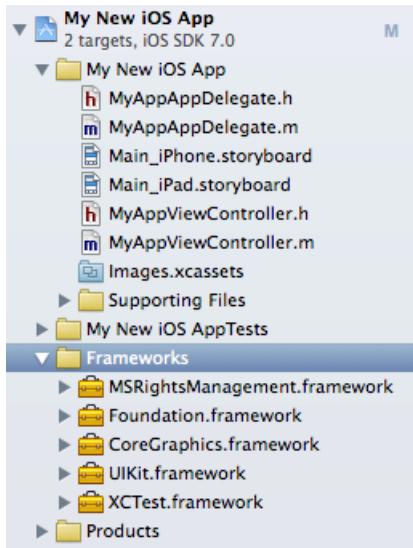
- To create a new project, on the File menu, click **New**, and then click **Project**.
- Select **Single View Application**.



- Enter a name and identifier for your new project.

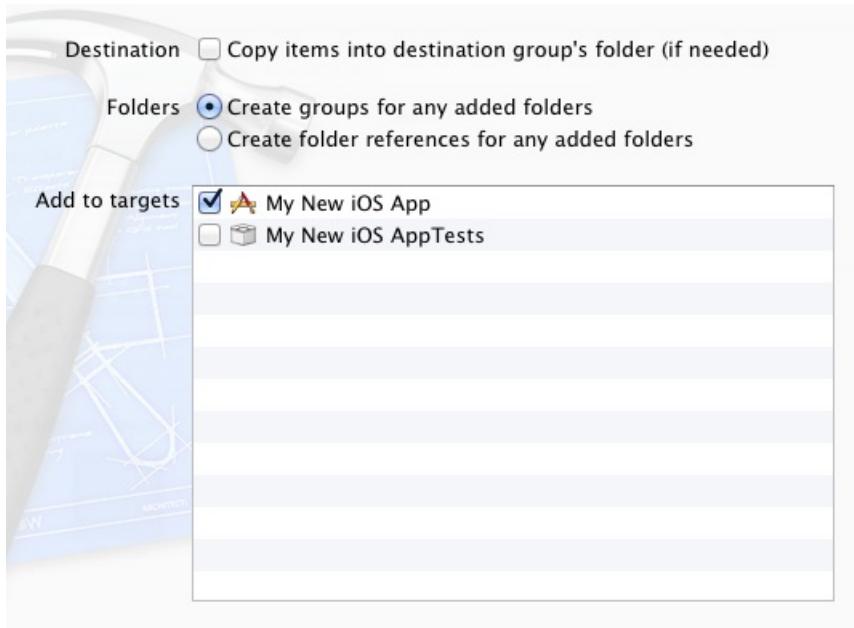


- Click Next and select the location for your project.
- To add the **MSRightsManagement** framework for iOS Frameworks, drag the .framework folder from the SDK installation folder into the **Frameworks** section of your **Project Navigator**.

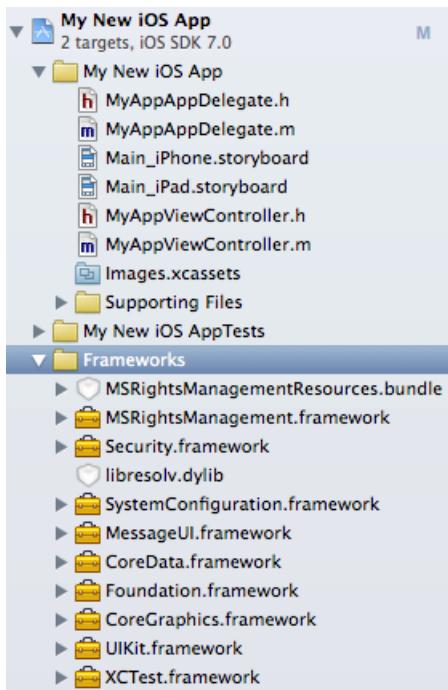


- Select **Create groups for any added folders** option button and clear the **Copy items into destination group's folder (if needed)** check box.

This action maintains the reference to the SDK installation folder instead of creating a copy.

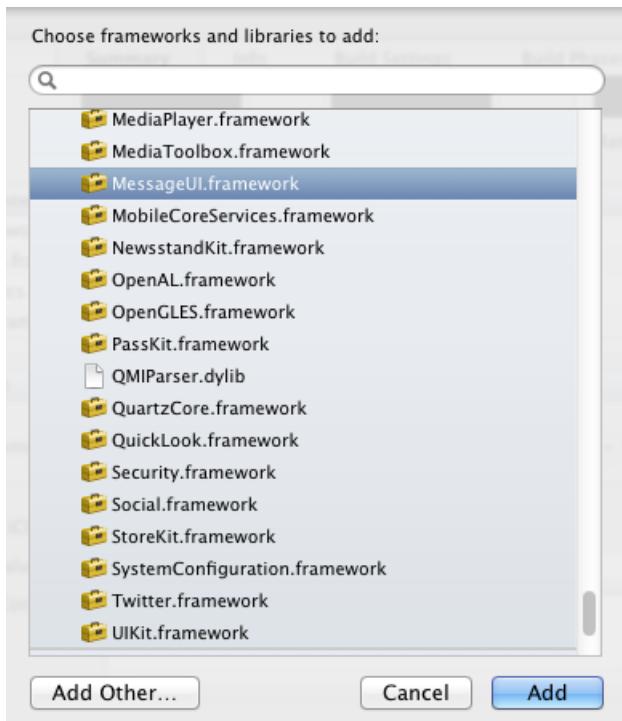


- To add the MS RMS SDK 4.2 for the resource bundle, drag the MSRightsManagementResources.bundle file from the MSRightsManagement.framework/Resources folder into the **Frameworks** section of your Project Navigator.



- As you did when you copied the Framework, select **Create groups for any added folders** option button and clear the **Copy items into destination group's folder** (if needed) check box.
- The SDK relies on other frameworks including: **CoreData**, **MessageUI**, **SystemConfiguration**, **Libresolv** and **Security**. To add these frameworks, navigate to the **Linked Frameworks and Libraries** section of the target's **Summary** pane, and expand that section to add them.

The **UIKit** and **Foundation** frameworks are required and generally present by default.

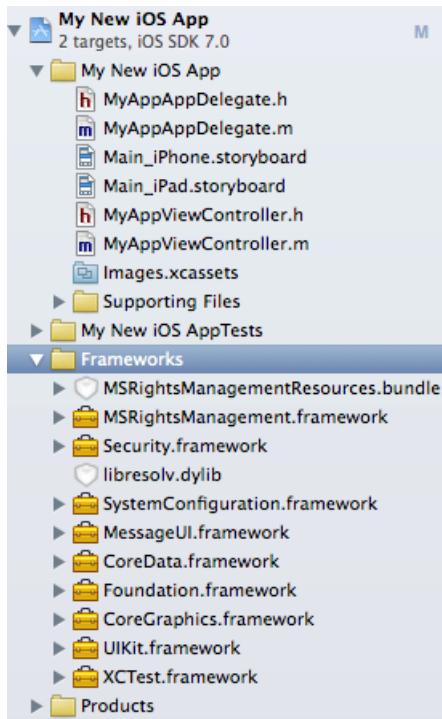


- Add the **-ObjC** flag to **Other Linker Flags** in your target **Build Settings**.

Linking

- Bundle Loader
- Compatibility Version
- Current Library Version
- Dead Code Stripping Yes ▾
- Display Mangled Names No ▾
- Don't Create Position Independent Executables No ▾
- Don't Dead-Strip Inits and Terms No ▾
- Dynamic Library Install Name
- Exported Symbols File
- Initialization Routine
- Link With Standard Libraries Yes ▾
- Mach-O Type Executable ▾
- Order File
- ▶ Other Linker Flags -ObjC
- ▼ Path to Link Map File <Multiple values>

- Now your **Project Navigator** should look something like this tree.



- You are now ready to create your own new iOS/OS X apps.

## See Also

- [Get started](#)
- [What's new](#)
- [Developer terms and concepts](#)
- [iOS / OS X API Reference](#)

# Windows Phone setup

3/17/2020 • 2 minutes to read • [Edit Online](#)

## IMPORTANT

Versions of the Microsoft Rights Management Service SDK released prior to March 2020 are deprecated; applications using earlier versions must be updated to use the March 2020 release. For full details, see the [deprecation notice](#).

No further enhancements are planned for the Microsoft Rights Management Service SDK. We strongly recommend adoption of the [Microsoft Information Protection SDK](#) for classification, labeling, and protection services.

Windows Phone applications can use the Microsoft Rights Management SDK 4.2 to enable integrated information protection in their application by using the Azure Active Directory Rights Management (AAD RM).

This topic will guide you through setting up your environment for creating your own new apps .

- [Prerequisites](#)
- [Configuring your development environment](#)
- [See Also](#)

## Prerequisites

You must have the following software on your development system:

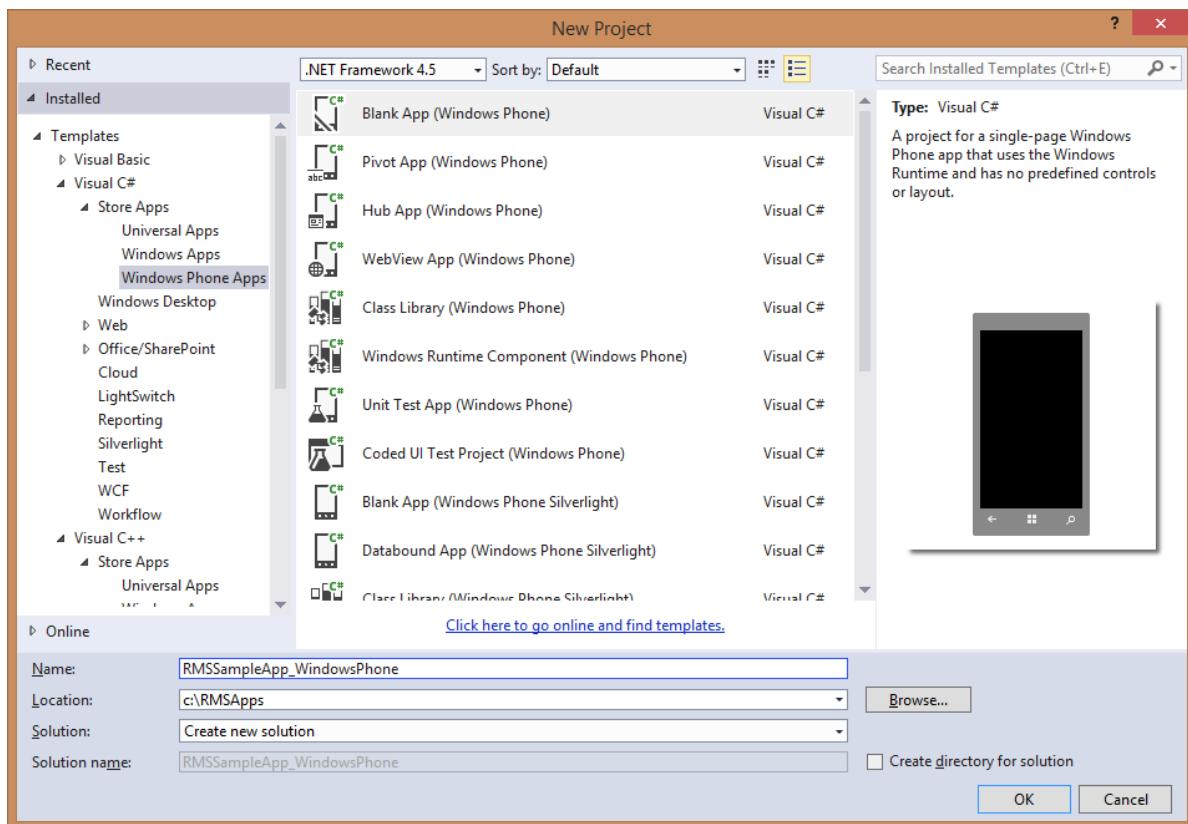
- The [Windows 8.1](#) operating system.
- [Windows Phone 8.1 Development Tools \(SDK\)](#)
- Microsoft [Visual Studio 2012](#) or above, or Visual Studio Express 2012, which is included in the Windows Phone SDK 8.0/8.1
- The MS RMS SDK 4.2 package for Windows Phone. For more information see, [Get started](#).
- Authentication library: We recommend that you use the [Azure AD Authentication Library](#) and other authentication libraries can be used.

Read the [What's new](#) topic for information on API updates, device and environment information, release notes and frequently asked questions (FAQ).

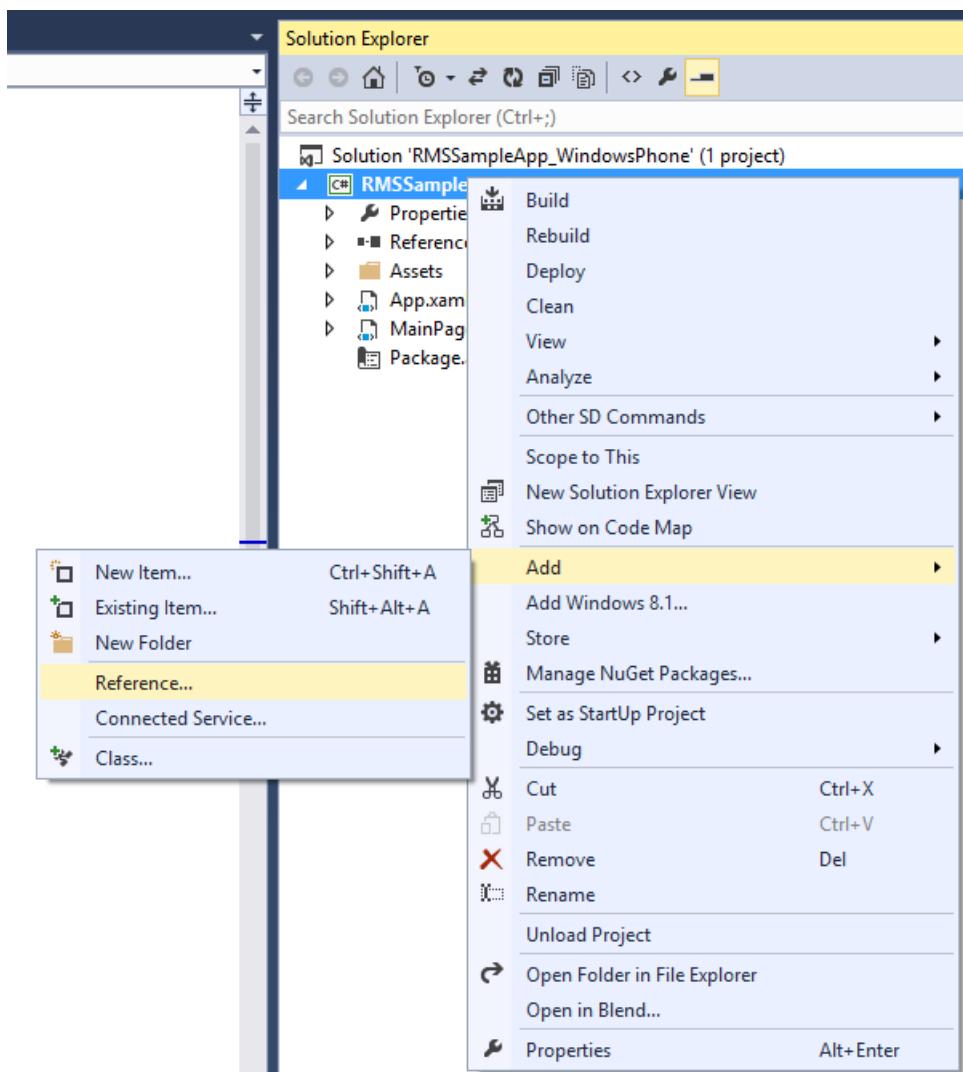
Review the information in the [Windows Phone development](#) guide at the Windows Phone Dev Center.

## Configuring your development environment

- Open *Visual Studio*.
- Click **File**. On the **File** menu, click **New**, and then click **Project**.
- In the **New Project** dialog box, select **Visual C#**, select **Blank App (Windows Phone)**, and then click **OK**.



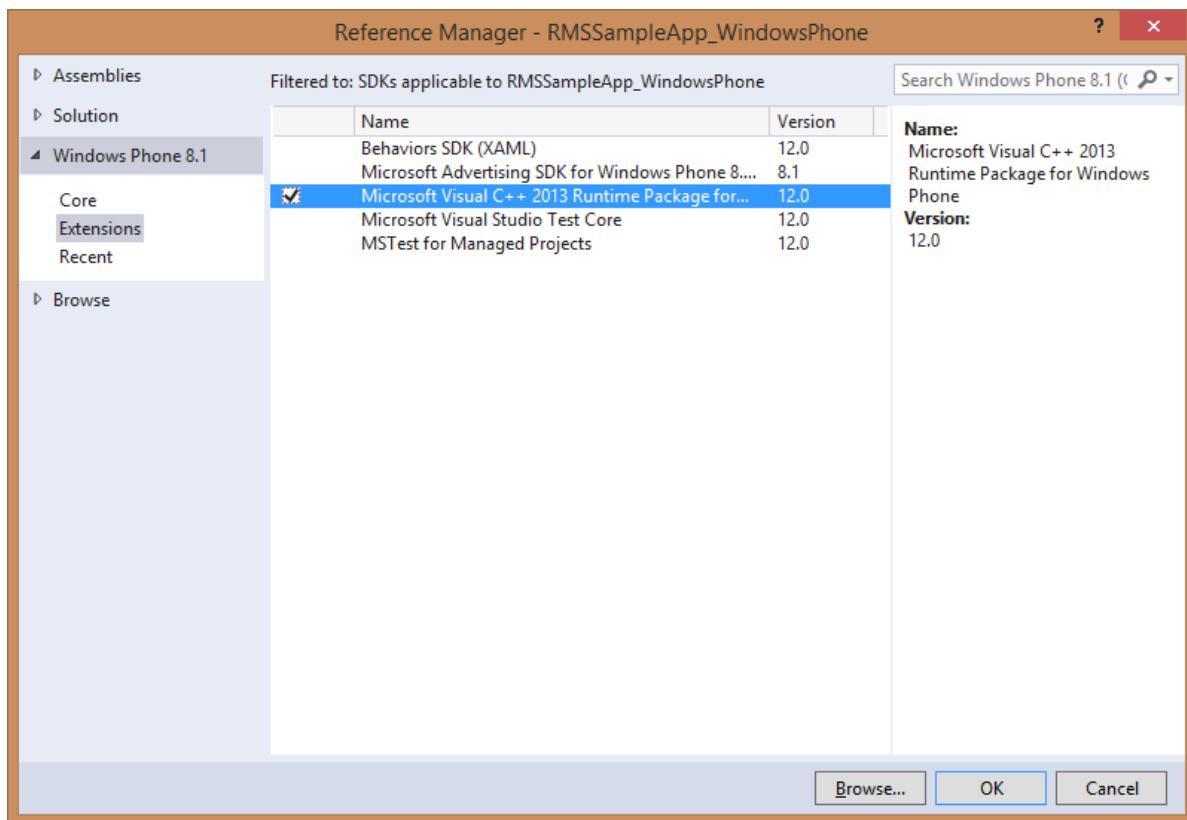
- In Solution Explorer, right-click your project, and then select **Add Reference** to open the Add Reference dialog box.



- Click **Browse** on the lower left of the Add Reference dialog box and select the

*Microsoft.RightsManagement.dll* file that is located in the folder you extracted the package in.

- **Managed Apps** - For building a managed app, you will have to add this reference; select **Windows 8.1** ->**Extensions** and check the box for **Windows Visual C++ Runtime Package for Windows**



- **Adding Capabilities** - Your application will need the "Internet (Client & Server)" capability to use the SDK. To add this capability to your app, open the *Package.appxmanifest* file in the project and navigate to the **Capabilities** tab to add.

You are now ready to create your own new Windows Phone apps.

## See Also

[Get started](#)

[What's new](#)

[Core concepts](#)

[Windows Phone development](#)

[Windows API Reference](#)

[Visual Studio 2012](#)

[Windows Phone SDK](#)

# Windows Store setup

3/17/2020 • 2 minutes to read • [Edit Online](#)

## IMPORTANT

Versions of the Microsoft Rights Management Service SDK released prior to March 2020 are deprecated; applications using earlier versions must be updated to use the March 2020 release. For full details, see the [deprecation notice](#).

No further enhancements are planned for the Microsoft Rights Management Service SDK. We strongly recommend adoption of the [Microsoft Information Protection SDK](#) for classification, labeling, and protection services.

Windows Store applications can use the Microsoft Rights Management SDK 4.2 to enable integrated information protection in their application by using the Azure Active Directory Rights Management (AAD RM).

This topic will guide you through setting up your environment for creating your own new apps.

- [Prerequisites](#)
- [Optional](#)
- [Configuring your development environment](#)
- [See Also](#)

## Prerequisites

You must have the following software on your development system:

- The [Windows 8.1](#) operating system
- The [Windows SDK for Windows 8.1](#)
- Microsoft [Visual Studio 2012](#) or above, or Visual Studio Express 2012, which is included in the Windows SDK for Windows 8.0/8.1.
- The MS RMS SDK 4.2 package for Windows Store Applications. For more information see, [Get started](#).
- Authentication library: We recommend that you use the [Azure AD Authentication Library](#) and other authentication libraries can be used.

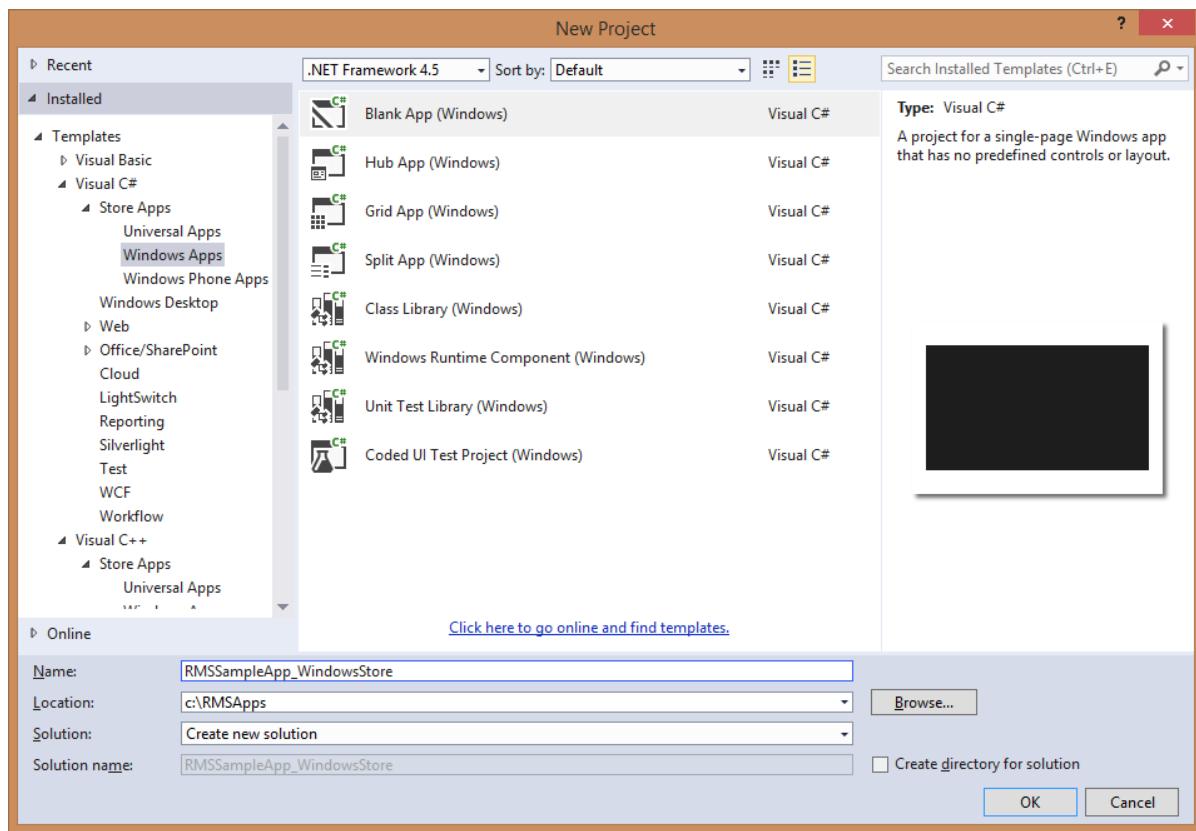
Read the [What's new](#) topic for information on API updates, device and environment information, release notes and frequently asked questions (FAQ).

## Optional

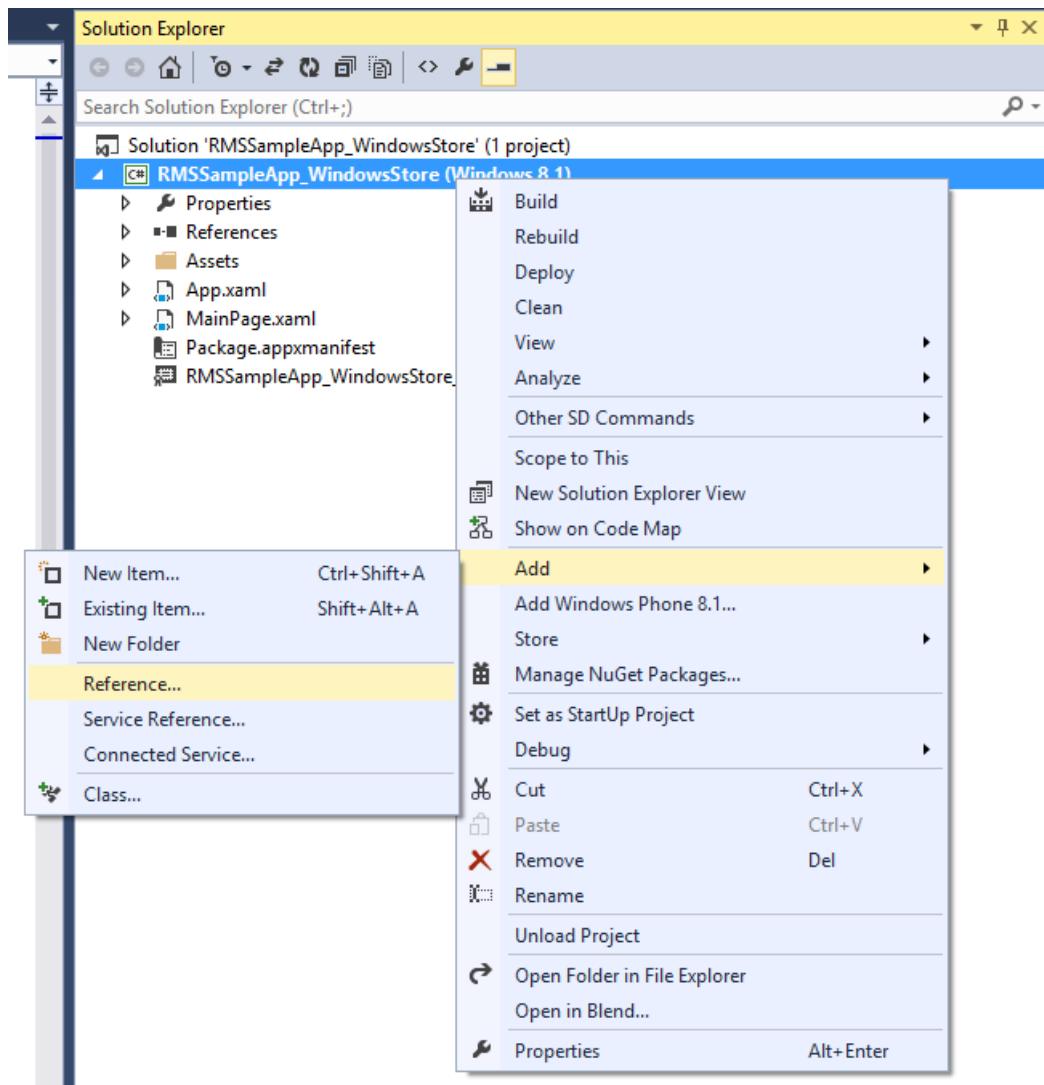
Our UI library provides re-usable UI for consumption and protection operations for developers who don't want to create their own custom UI - [UI Library for Windows Store apps](#). We also provide a Windows Store app sample application - [RMS Sample application for Windows Store](#).

## Configuring your development environment

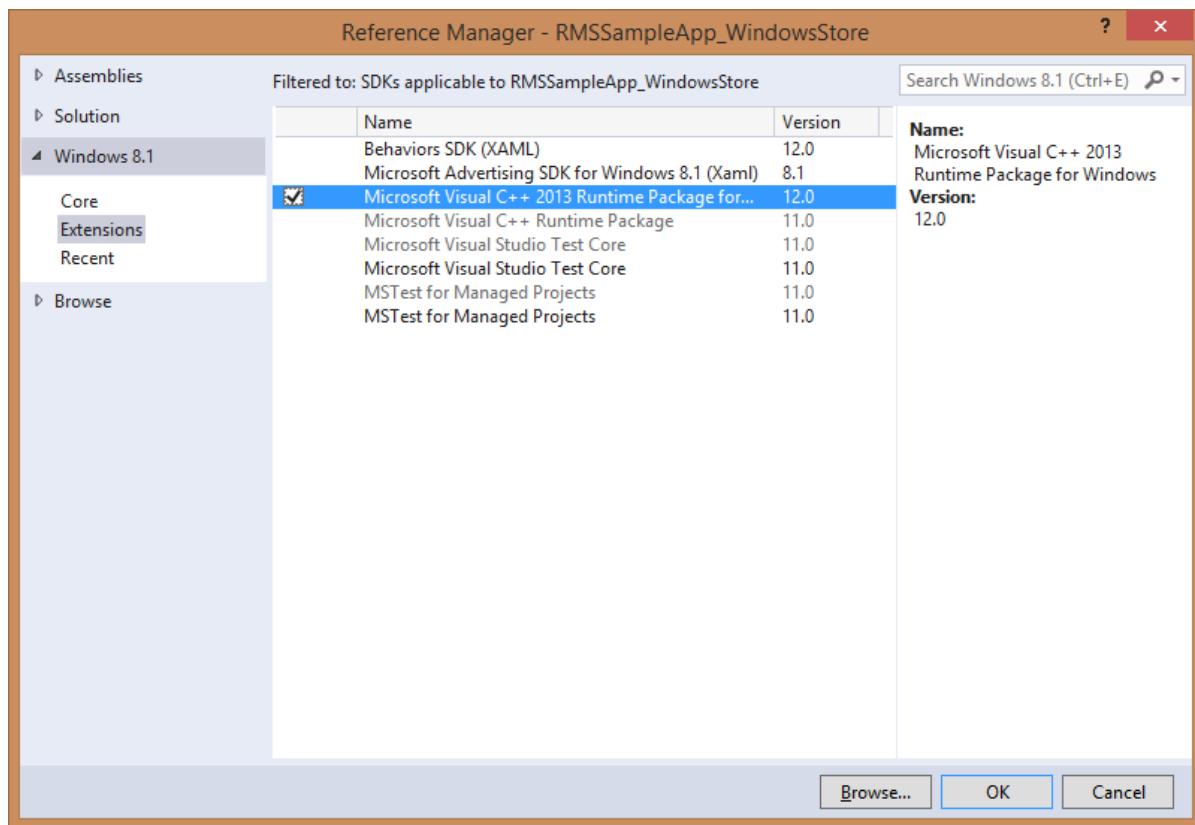
- Open Visual Studio.
- Click **File**, click **New**, and then click **Project**.
- In the **New Project** dialog box, click **Visual C#** and select **Blank App (Windows)** then click **OK**.



- In **Solution Explorer**, right-click your project, and select **Add Reference** to open the Add Reference dialog box.



- In the Add Reference dialog box, click **Browse** and select the *Microsoft.RightsManagement.dll* file that is located in the folder you extracted the SDK package in.
- **Managed Apps** - For building a managed app, you will have to add this reference; select **Windows 8.1 - Extensions** and check the box for **Windows Visual C++ Runtime Package for Windows**



- **Adding Capabilities** - Your application will need "Internet (Client & Server)" capability to use the SDK. To add this capability to your app, open the *Package.appxmanifest* file in the project and navigate to the **Capabilities** tab to add.

You are now ready to create your own new Windows Store apps.

## See Also

[Get started](#)

[What's new](#)

[Developer terms and concepts](#)

[Windows 8](#)

[Visual Studio 2012](#)

[Windows API Reference](#)

# Code examples

3/17/2020 • 2 minutes to read • [Edit Online](#)

## IMPORTANT

Versions of the Microsoft Rights Management Service SDK released prior to March 2020 are deprecated; applications using earlier versions must be updated to use the March 2020 release. For full details, see the [deprecation notice](#).

No further enhancements are planned for the Microsoft Rights Management Service SDK. We strongly recommend adoption of the [Microsoft Information Protection SDK](#) for classification, labeling, and protection services.

Microsoft Rights Management SDK 4.2 includes example code and working projects for some supported operating systems.

## Available via GitHub

Our UI library provides re-usable UI for consumption and protection operations for developers who don't want to create their own custom UI:

- Android - [UI Library and Sample app for Android](#)
- iOS - [UI Library and Sample app for iOS](#)
- Windows Store apps - [UI Library for Windows Store apps](#) and [Sample app for Windows Store](#).

## Examples

These topics will introduce you to important code elements for the associated version of the RMS SDK.

- [Android code examples](#)
- [Linux code examples](#)
- [iOS/OS X code examples](#)

# Android code examples

5/8/2020 • 6 minutes to read • [Edit Online](#)

## IMPORTANT

Versions of the Microsoft Rights Management Service SDK released prior to March 2020 are deprecated; applications using earlier versions must be updated to use the March 2020 release. For full details, see the [deprecation notice](#).

No further enhancements are planned for the Microsoft Rights Management Service SDK. We strongly recommend adoption of the [Microsoft Information Protection SDK](#) for classification, labeling, and protection services.

This article shows how to code elements for the Android version of the RMS SDK.

**Note** In this article, The term *MSIPC*(Microsoft Information Protection and Control) refers to the client process.

## Using the Microsoft Rights Management SDK 4.2 - key scenarios

These code samples are taken from a larger sample application representing development scenarios important to your orientation to this SDK. They show how to use:

- The Microsoft Protected File format, also called a *protected file*.
- Custom protected file formats
- Custom user interface (UI) controls

The *MSIPCSampleApp* sample application is available for use with this SDK for the Android operating system. To learn more, see [rms-sdk-ui-for-android](#).

### Scenario: Consume an RMS protected file

- Step 1: Create a [ProtectedFileInputStream](#).

Source: *MsipcAuthenticationCallback.java*

Description: Instantiate a [ProtectedFileInputStream](#) object and implement service authentication. Use the [AuthenticationRequestCallback](#) to get a token by passing an instance of [AuthenticationRequestCallback](#), as the parameter *mRmsAuthCallback*, to the MSIPC API. See the call to [ProtectedFileInputStream.create](#) near the end of the following example code section.

```

public void startContentConsumptionFromPtxtFileFormat(InputStream inputStream)
{
 CreationCallback<ProtectedFileInputStream> protectedFileInputStreamCreationCallback =
 new CreationCallback<ProtectedFileInputStream>()
 {
 @Override
 public Context getContext()
 {
 ...
 }

 @Override
 public void onCancel()
 {
 ...
 }

 @Override
 public void onFailure(ProtectionException e)
 {
 ...
 }

 @Override
 public void onSuccess(ProtectedFileInputStream protectedFileInputStream)
 {
 ...
 ...

 byte[] dataChunk = new byte[16384];
 try
 {
 while ((nRead = protectedFileInputStream.read(dataChunk, 0,
 dataChunk.length)) != -1)
 {
 ...
 ...
 ...
 protectedFileInputStream.close();
 }
 catch (IOException e)
 {
 ...
 }
 }
 };
 try
 {
 ...
 ProtectedFileInputStream.create(inputStream, null, mRmsAuthCallback,
 PolicyAcquisitionFlags.NONE,
 protectedFileInputStreamCreationCallback);
 }
 catch (com.microsoft.rightsmanagement.exceptions.InvalidParameterException e)
 {
 ...
 }
}

```

- **Step 2:** Set up authentication using the Active Directory Authentication Library (ADAL).

**Source:** *MsipcAuthenticationCallback.java*.

**Description:** This step uses ADAL to implement an [AuthenticationRequestCallback](#) with example authentication parameters. To learn more, see the [Azure AD Authentication Library \(ADAL\)](#).

```
class MsipcAuthenticationCallback implements AuthenticationRequestCallback
```

```

class MsipcAuthenticationCallback implements AuthenticationRequestCallback
{
 ...

 @Override
 public void getToken(Map<String, String> authenticationParametersMap,
 final AuthenticationCompletionCallback
 authenticationCompletionCallbackToMsipc)
 {
 String authority = authenticationParametersMap.get("oauth2.authority");
 String resource = authenticationParametersMap.get("oauth2.resource");
 String userId = authenticationParametersMap.get("userId");
 final String userHint = (userId == null)? "" : userId;
 AuthenticationContext authenticationContext = App.getInstance().getAuthenticationContext();
 if (authenticationContext == null ||
 !authenticationContext.getAuthority().equalsIgnoreCase(authority))
 {
 try
 {
 authenticationContext = new
 AuthenticationContext(App.getInstance().getApplicationContext(), authority, ...);
 App.getInstance().setAuthenticationContext(authenticationContext);
 }
 catch (NoSuchAlgorithmException e)
 {
 ...
 authenticationCompletionCallbackToMsipc.onFailure();
 }
 catch (NoSuchPaddingException e)
 {
 ...
 authenticationCompletionCallbackToMsipc.onFailure();
 }
 }
 App.getInstance().getAuthenticationContext().acquireToken(mParentActivity, resource, mClientId,
 mRedirectURI, userId, mPromptBehavior,
 "&USERNAME=" + userHint, new AuthenticationCallback<AuthenticationResult>()
 {
 @Override
 public void onError(Exception exc)
 {
 ...
 if (exc instanceof AuthenticationCancelError)
 {
 ...
 authenticationCompletionCallbackToMsipc.onCancel();
 }
 else
 {
 ...
 authenticationCompletionCallbackToMsipc.onFailure();
 }
 }

 @Override
 public void onSuccess(AuthenticationResult result)
 {
 ...
 if (result == null || result.getAccessToken() == null
 || result.getAccessToken().isEmpty())
 {
 ...
 }
 else
 {
 // request is successful
 ...
 }
 }
 });
 }
}

```

```
authenticationCompletionCallback.onSuccess(result.getAccessToken());
 }
}
);
}
```

- **Step 3:** Check if the **Edit** right exists for this user with this content via the [UserPolicy.accessCheck](#) method.

Source: *TextEditorFragment.java*

```
//check if user has edit rights and apply enforcements
if (!mUserPolicy.accessCheck(EditableDocumentRights.Edit))
{
 mTextEditor.setFocusableInTouchMode(false);
 mTextEditor.setFocusable(false);
 mTextEditor.setEnabled(false);
 ...
}
```

### Scenario: Create a new protected file using a template

This scenario begins with getting a list of templates, selecting the first one to create a policy, then creates and writes to the new protected file.

- **Step 1:** Get list of templates via a [TemplateDescriptor](#) object.

Source: *MsipcTaskFragment.java*

```

CreationCallback<List<TemplateDescriptor>> getTemplatesCreationCallback = new
CreationCallback<List<TemplateDescriptor>>()
{
 @Override
 public Context getContext()
 {
 ...
 }

 @Override
 public void onCancel()
 {
 ...
 }

 @Override
 public void onFailure(ProtectionException e)
 {
 ...
 }

 @Override
 public void onSuccess(List<TemplateDescriptor> templateDescriptors)
 {
 ...
 }
};

try
{
 ...
 mIAyncControl = TemplateDescriptor.getTemplates(emailId, mRmsAuthCallback,
getTemplatesCreationCallback);
}
catch (com.microsoft.rightsmanagement.exceptions.InvalidParameterException e)
{
 ...
}

```

- **Step 2:** Create a [UserPolicy](#) using the first template in the list.

Source: *MsipcTaskFragment.java*

```

CreationCallback<UserPolicy> userPolicyCreationCallback = new CreationCallback<UserPolicy>()
{
 @Override
 public Context getContext()
 {
 ...
 }

 @Override
 public void onCancel()
 {
 ...
 }

 @Override
 public void onFailure(ProtectionException e)
 {
 ...
 }

 @Override
 public void onSuccess(final UserPolicy item)
 {
 ...
 }
};

try
{
 ...
 mIAyncControl = UserPolicy.create((TemplateDescriptor)selectedDescriptor, mEmailId,
mRmsAuthCallback,
 UserPolicyCreationFlags.NONE, userPolicyCreationCallback);
 ...
}
catch (InvalidParameterException e)
{
 ...
}

```

- **Step 3:** Create a [ProtectedFileOutputStream](#) and write content to it.

Source: *MsipcTaskFragment.java*

```

private void createPTxt(final byte[] contentToProtect)
{
 ...
 CreationCallback<ProtectedFileOutputStream> protectedFileOutputStreamCreationCallback = new
CreationCallback<ProtectedFileOutputStream>()
{
 ...
 @Override
 public Context getContext()
 {
 ...
 }

 @Override
 public void onCancel()
 {
 ...
 }

 @Override
 public void onFailure(ProtectionException e)
 {
 ...
 }

 @Override
 public void onSuccess(ProtectedFileOutputStream protectedFileOutputStream)
 {
 try
 {
 // write to this stream
 protectedFileOutputStream.write(contentToProtect);
 protectedFileOutputStream.flush();
 protectedFileOutputStream.close();
 ...
 }
 catch (IOException e)
 {
 ...
 }
 ...
 }
 };
 try
 {
 File file = new File(filePath);
 outputStream = new FileOutputStream(file);
 mIAyncControl = ProtectedFileOutputStream.create(outputStream, mUserPolicy,
originalFileExtension,
 protectedFileOutputStreamCreationCallback);
 }
 catch (FileNotFoundException e)
 {
 ...
 }
 catch (InvalidParameterException e)
 {
 ...
 }
}
}

```

### Scenario: Open a custom protected file

- Step 1: Create a [UserPolicy](#) from a *serializedContentPolicy*.

Source: *MsicTaskFragment.java*

```

CreationCallback<UserPolicy> userPolicyCreationCallbackFromSerializedContentPolicy = new
CreationCallback<UserPolicy>()
{
 @Override
 public void onSuccess(UserPolicy userPolicy)
 {
 ...
 }

 @Override
 public void onFailure(ProtectionException e)
 {
 ...
 }

 @Override
 public void onCancel()
 {
 ...
 }

 @Override
 public Context getContext()
 {
 ...
 }
};

try
{
 ...

 // Read the serializedContentPolicyLength from the inputStream.
 long serializedContentPolicyLength = readUnsignedInt(inputStream);

 // Read the PL bytes from the input stream using the PL size.
 byte[] serializedContentPolicy = new byte[(int)serializedContentPolicyLength];
 inputStream.read(serializedContentPolicy);

 ...

 UserPolicy.acquire(serializedContentPolicy, null, mRmsAuthCallback,
PolicyAcquisitionFlags.NONE,
 userPolicyCreationCallbackFromSerializedContentPolicy);
}
catch (com.microsoft.rightsmanagement.exceptions.InvalidParameterException e)
{
 ...
}
catch (IOException e)
{
 ...
}

```

- Step 2: Create a [CustomProtectedInputStream](#) using the [UserPolicy](#) from Step 1.

Source: *MsicTaskFragment.java*

```

CreationCallback<CustomProtectedInputStream> customProtectedInputStreamCreationCallback = new
CreationCallback<CustomProtectedInputStream>()
{
 ...
 @Override
 public Context getContext()
 {
 ...
 }

 @Override
 public void onCancel()
 {
 ...
 }

 @Override
 public void onFailure(ProtectionException e)
 {
 ...
 }

 @Override
 public void onSuccess(CustomProtectedInputStream customProtectedInputStream)
 {
 ...

 byte[] dataChunk = new byte[16384];
 try
 {
 while ((nRead = customProtectedInputStream.read(dataChunk, 0, dataChunk.length)) != -1)
 {
 ...
 }
 ...
 customProtectedInputStream.close();
 }
 catch (IOException e)
 {
 ...
 }
 ...
 }
};

try
{
 ...
 // Retrieve the encrypted content size.
 long encryptedContentLength = readUnsignedInt(inputStream);

 updateTaskStatus(new TaskStatus(TaskState.Starting, "Consuming content", true));

 CustomProtectedInputStream.create(userPolicy, inputStream,
 encryptedContentLength,
 customProtectedInputStreamCreationCallback);
}
catch (com.microsoft.rightsmanagement.exceptions.InvalidParameterException e)
{
 ...
}
catch (IOException e)
{
 ...
}

```

- Step 3: Read content from the `CustomProtectedInputStream` into `mDecryptedContent` then close.

Source: `MsipcTaskFragment.java`

```

@Override
public void onSuccess(CustomProtectedInputStream customProtectedInputStream)
{
 mUserPolicy = customProtectedInputStream.getUserPolicy();
 ByteArrayOutputStream buffer = new ByteArrayOutputStream();

 int nRead;
 byte[] dataChunk = new byte[16384];

 try
 {
 while ((nRead = customProtectedInputStream.read(dataChunk, 0,
 dataChunk.length)) != -1)
 {
 buffer.write(dataChunk, 0, nRead);
 }

 buffer.flush();
 mDecryptedContent = new String(buffer.toByteArray(), Charset.forName("UTF-8"));

 buffer.close();
 customProtectedInputStream.close();
 }
 catch (IOException e)
 {
 ...
 }
}

```

### Scenario: Create a custom protected file using a custom policy

- Step 1: With an email address provided by the user, create a policy descriptor.

Source: `MsipcTaskFragment.java`

Description: In practice, the following objects would be created by using user inputs from the device interface; `UserRights` and `PolicyDescriptor`.

```

// create userRights list
UserRights userRights = new UserRights(Arrays.asList("consumer@domain.com"),
 Arrays.asList(CommonRights.View, EditableDocumentRights.Print));
ArrayList<UserRights> usersRigthsList = new ArrayList<UserRights>();
usersRigthsList.add(userRights);

// Create PolicyDescriptor using userRights list
PolicyDescriptor policyDescriptor = PolicyDescriptor.createPolicyDescriptorFromUserRights(
 usersRigthsList);
policyDescriptor.setOfflineCacheLifetimeInDays(10);
policyDescriptor.setContentValidUntil(new Date());

```

- Step 2: Create a custom `UserPolicy` from the policy descriptor, `selectedDescriptor`.

Source: `MsipcTaskFragment.java`

```

mIAyncControl = UserPolicy.create((PolicyDescriptor)selectedDescriptor,
 mEmailId, mRmsAuthCallback, UserPolicyCreationFlags.NONE, userPolicyCreationCallback);

```

- Step 3: Create and write content to the `CustomProtectedOutputStream` and then close.

Source: *MsipcTaskFragment.java*

```

File file = new File(filePath);
final OutputStream outputStream = new FileOutputStream(file);
CreationCallback<CustomProtectedOutputStream> customProtectedOutputStreamCreationCallback = new
CreationCallback<CustomProtectedOutputStream>()
{
 @Override
 public Context getContext()
 {
 ...
 }

 @Override
 public void onCancel()
 {
 ...
 }

 @Override
 public void onFailure(ProtectionException e)
 {
 ...
 }

 @Override
 public void onSuccess(CustomProtectedOutputStream protectedOutputStream)
 {
 try
 {
 // write serializedContentPolicy
 byte[] serializedContentPolicy = mUserPolicy.getSerializedContentPolicy();
 writeLongAsUnsignedIntToStream(outputStream, serializedContentPolicy.length);
 outputStream.write(serializedContentPolicy);
 // write encrypted content
 if (contentToProtect != null)
 {
 writeLongAsUnsignedIntToStream(outputStream,
 CustomProtectedOutputStream.getEncryptedContentLength(contentToProtect.length,
 protectedOutputStream.getUserPolicy()));
 protectedOutputStream.write(contentToProtect);
 protectedOutputStream.flush();
 protectedOutputStream.close();
 }
 else
 {
 outputStream.flush();
 outputStream.close();
 }
 ...
 }
 catch (IOException e)
 {
 ...
 }
 }
};

try
{
 mIAsyncControl = CustomProtectedOutputStream.create(outputStream, mUserPolicy,
 customProtectedOutputStreamCreationCallback);
}
catch (InvalidParameterException e)
{
 ...
}

```

# Linux code examples

3/17/2020 • 8 minutes to read • [Edit Online](#)

## IMPORTANT

Versions of the Microsoft Rights Management Service SDK released prior to March 2020 are deprecated; applications using earlier versions must be updated to use the March 2020 release. For full details, see the [deprecation notice](#).

No further enhancements are planned for the Microsoft Rights Management Service SDK. We strongly recommend adoption of the [Microsoft Information Protection SDK](#) for classification, labeling, and protection services.

This topic introduces you to important scenarios and code elements for the Linux version of the RMS SDK.

The code snippets below are from the sample applications, *rms\_sample* and *rmsauth\_sample*. For more information, see [samples](#) at the GitHub repository.

## Scenario: Access protection policy information from a protected file

**Opens and reads an RMS protected file** Source: [rms\\_sample/mainwindow.cpp](#)

**Description:** After getting a file name from the user, reading the certificates (see *MainWindow::addCertificates*), setting up the authorization callback with Client ID and Redirect URL, calling *ConvertFromPFile* (see following code example), then reading out the protection policy name, description and content validity date.

C++:

```

void MainWindow::ConvertFromPFILE(const string& fileIn,
 const string& clientId,
 const string& redirectUrl,
 const string& clientEmail)
{
// add trusted certificates using HttpHelpers of RMS and Auth SDKs
addCertificates();

// create shared in/out streams
auto inFile = make_shared<ifstream>(
fileIn, ios_base::in | ios_base::binary);

if (!inFile->is_open()) {
 AddLog("ERROR: Failed to open ", fileIn.c_str());
 return;
}

string fileOut;

// generate output filename
auto pos = fileIn.find_last_of('.');

if (pos != string::npos) {
 fileOut = fileIn.substr(0, pos);
}

// create streams
auto outFile = make_shared<fstream>(
fileOut, ios_base::in | ios_base::out | ios_base::trunc | ios_base::binary);

if (!outFile->is_open()) {
 AddLog("ERROR: Failed to open ", fileOut.c_str());
 return;
}

try
{
// create authentication context
AuthCallback auth(clientId, redirectUrl);

// process conversion
auto pfs = PFileConverter::ConvertFromPFile(
 clientEmail,
 inFile,
 outFile,
 auth,
 this->consent);

AddLog("Successfully converted to ", fileOut.c_str());
}
catch (const rmsauth::Exception& e)
{
AddLog("ERROR: ", e.error().c_str());
}
catch (const rmscore::exceptions::RMSErrorException& e) {
AddLog("ERROR: ", e.what());
}
inFile->close();
outFile->close();
}

```

Create a protected file stream Source: [rms\\_sample/pfileconverter.cpp](#)

**Description:** This method creates a protected file stream from the passed in backing stream through the SDK method, *ProtectedFileStream::Acquire*, which is then returned to the caller.

C++:

```
shared_ptr<GetProtectedFileStreamResult> PFileConverter::ConvertFromPFile(
 const string& userId,
 shared_ptr<istream> inStream,
 shared_ptr<iostream> outStream,
 IAuthenticationCallback& auth,
 IConsentCallback& consent)
{
 auto inIStream = rmscrypto::api::CreateStreamFromStdStream(inStream);

 auto fsResult = ProtectedFileStream::Acquire(
 inIStream,
 userId,
 auth,
 consent,
 POL_None,
 static_cast<ResponseCacheFlags>(RESPONSE_CACHE_INMEMORY
 | RESPONSE_CACHE_ONDISK));

 if ((fsResult.get() != nullptr) && (fsResult->m_status == Success) &&
 (fsResult->m_stream != nullptr)) {
 auto pfs = fsResult->m_stream;

 // preparing
 readPosition = 0;
 writePosition = 0;
 totalSize = pfs->Size();

 // start threads
 for (size_t i = 0; i < THREADS_NUM; ++i) {
 threadPool.push_back(thread(WorkerThread,
 static_pointer_cast<iostream>(outStream), pfs,
 false));
 }

 for (thread& t: threadPool) {
 if (t.joinable()) {
 t.join();
 }
 }
 }
 return fsResult;
}
```

## Scenario: Create a new protected file using a template

Protects a file with a user selected template Source: [rms\\_sample/mainwindow.cpp](#)

**Description:** After getting a file name from the user, reading the certificates (see *MainWindow::addCertificates*) and setting up the authorization callback with Client ID and Redirect URL, the selected file is protected by calling *ConvertToPFileTemplates* (see following code example).

C++:

```

void MainWindow::ConvertToPFILEUsingTemplates(const string& fileIn,
 const string& clientId,
 const string& redirectUrl,
 const string& clientEmail)
{
 // generate output filename
 string fileOut = fileIn + ".pfile";

 // add trusted certificates using HttpHelpers of RMS and Auth SDKs
 addCertificates();

 // create shared in/out streams
 auto inFile = make_shared<ifstream>(
 fileIn, ios_base::in | ios_base::binary);
 auto outFile = make_shared<fstream>(
 fileOut, ios_base::in | ios_base::out | ios_base::trunc | ios_base::binary);

 if (!inFile->is_open()) {
 AddLog("ERROR: Failed to open ", fileIn.c_str());
 return;
 }

 if (!outFile->is_open()) {
 AddLog("ERROR: Failed to open ", fileOut.c_str());
 return;
 }

 // find file extension
 string fileExt;
 auto pos = fileIn.find_last_of('.');
 if (pos != string::npos) {
 fileExt = fileIn.substr(pos);
 }

 try {
 // create authentication callback
 AuthCallback auth(clientId, redirectUrl);

 // process conversion
 PFileConverter::ConvertToPFileTemplates(
 clientEmail, inFile, fileExt, outFile, auth,
 this->consent, this->templates);

 AddLog("Successfully converted to ", fileOut.c_str());
 }
}

```

```

catch (const rmsauth::Exception& e) { AddLog("ERROR: ", e.error().c_str()); outFile->close(); remove(fileOut.c_str()); }
catch (const rmscore::exceptions::RMSErrorException& e) { AddLog("ERROR: ", e.what()); }

```

```

 outFile->close();
 remove(fileOut.c_str());
}
inFile->close();
outFile->close();
}

```

**Protects a file using a policy created from a template** Source: [rms\\_sample/pfileconverter.cpp](#)

**Description:** A list of templates associated with the user is fetched and selected template is then used to create a policy which in turn is used to protect the file.

C++:

```

void PFileConverter::ConvertToPFileTemplates(const string & userId,
 shared_ptr<iostream> inStream,
 const string & fileExt,
 std::shared_ptr<iostream> outStream,
 IAuthenticationCallback& auth,
 IConsentCallback& /*consent*/,
 ITemplatesCallback & templ)
{
 auto templates = TemplateDescriptor::GetTemplateList(userId, auth);

 rmscore::modernapi::AppDataHashMap signedData;

 size_t pos = templ.SelectTemplate(templates);

 if (pos < templates.size()) {
 auto policy = UserPolicy::CreateFromTemplateDescriptor(
 templates[pos],
 userId,
 auth,
 USER_AllowAuditedExtraction,
 signedData);

 ConvertToPFileUsingPolicy(policy, inStream, fileExt, outStream);
 }
}

```

**Protects a file given a policy** Source: [rms\\_sample/pfileconverter.cpp](#)

**Description:** Create a protected file stream using the given policy then protect that file.

**C++:**

```

void PFileConverter::ConvertToPFileUsingPolicy(shared_ptr<UserPolicy> policy,
 shared_ptr<iostream> inStream,
 const string & fileExt,
 std::shared_ptr<iostream> outStream)
{
 if (policy.get() != nullptr) {
 auto outIStream = rmscrypto::api::CreateStreamFromStdStream(outStream);
 auto pStream = ProtectedFileStream::Create(policy, outIStream, fileExt);

 // preparing
 readPosition = 0;
 writePosition = pStream->Size();

 inStream->seekg(0, ios::end);
 totalSize = inStream->tellg();

 // start threads
 for (size_t i = 0; i < THREADS_NUM; ++i) {
 threadPool.push_back(thread(WorkerThread,
 static_pointer_cast<iostream>(inStream),
 pStream,
 true));
 }

 for (thread& t: threadPool) {
 if (t.joinable()) {
 t.join();
 }
 }

 pStream->Flush();
 }
}

```

## Scenario: Protect a file using custom protection

Protects a file using custom protection Source: [rms\\_sample/mainwindow.cpp](#)

**Description:** After getting a file name from the user, reading the certificates (see *MainWindow::addCertificates*), collecting rights information from the user, and setting up the authorization callback with Client ID and Redirect URL, the selected file is projected by calling *ConvertToPFilePredefinedRights* (see following code example).

C++:

```
void MainWindow::ConvertToPFILEUsingRights(const string & fileIn,
 const vector<UserRights>& userRights,
 const string & clientId,
 const string & redirectUrl,
 const string & clientEmail)

{
 // generate output filename
 string fileOut = fileIn + ".pfile";

 // add trusted certificates using HttpHelpers of RMS and Auth SDKs
 addCertificates();

 // create shared in/out streams
 auto inFile = make_shared<ifstream>(
 fileIn, ios_base::in | ios_base::binary);
 auto outFile = make_shared<fstream>(
 fileOut, ios_base::in | ios_base::out | ios_base::trunc | ios_base::binary);

 if (!inFile->is_open()) {
 AddLog("ERROR: Failed to open ", fileIn.c_str());
 return;
 }

 if (!outFile->is_open()) {
 AddLog("ERROR: Failed to open ", fileOut.c_str());
 return;
 }

 // find file extension
 string fileExt;
 auto pos = fileIn.find_last_of('.');

 if (pos != string::npos) {
 fileExt = fileIn.substr(pos);
 }

 // is anything to add
 if (userRights.size() == 0) {
 AddLog("ERROR: ", "Please fill email and check rights");
 return;
 }

 try {
 // create authentication callback
 AuthCallback auth(clientId, redirectUrl);

 // process conversion
 PFileConverter::ConvertToPFilePredefinedRights(
 clientEmail,
 inFile,
 fileExt,
 outFile,
 auth,
 this->consent,
 userRights);
 }
}
```

```

AddLog("Successfully converted to ", fileOut.c_str());
}
catch (const rmsauth::Exception& e) {
AddLog("ERROR: ", e.error().c_str());

outFile->close();
remove(fileOut.c_str());
}
catch (const rmscore::exceptions::RMSErrorException& e) {
AddLog("ERROR: ", e.what());

outFile->close();
remove(fileOut.c_str());
}
inFile->close();
outFile->close();
}

```

**Creates a protection policy give user selected rights** Source: [rms\\_sample/pfileconverter.cpp](#)

**Description:** Create a policy descriptor and fill it with the user's rights information then, use the policy descriptor to create a user policy. This policy is used to protect the selected file via a call to *ConvertToPFileUsingPolicy* (see this described in a previous section of this topic).

C++:

```

void PFileConverter::ConvertToPFilePredefinedRights(
 const string & userId,
 shared_ptr<iostream> inStream,
 const string & fileExt,
 shared_ptr<iostream> outStream,
 IAuthenticationCallback & auth,
 IConsentCallback& /*consent*/,
 const vector<UserRights>& userRights)
{
 auto endValidation = chrono::system_clock::now() + chrono::hours(48);

 PolicyDescriptor desc(userRights);

 desc.Referrer(make_shared<string>("https://client.test.app"));
 desc.ContentValidUntil(endValidation);
 desc.AllowOfflineAccess(false);
 desc.Name("Test Name");
 desc.Description("Test Description");

 auto policy = UserPolicy::Create(desc, userId, auth,
 USER_AllowAuditedExtraction);
 ConvertToPFileUsingPolicy(policy, inStream, fileExt, outStream);
}

```

## WorkerThread - a supporting method

The *WorkerThread()* method is called by two of the previous example scenarios; **Create a protected file stream** and **Protects a file given a policy** in the following manner:

C++:

```

threadPool.push_back(thread(WorkerThread,
 static_pointer_cast<iostream>(outStream), pfs,
 false));

```

## Supporting method, WorkerThread()

C++:

```
static mutex threadLocker;
static int64_t totalSize = 0;
static int64_t readPosition = 0;
static int64_t writePosition = 0;
static vector<thread> threadPool;

static void WorkerThread(shared_ptr<iostream> stdStream,
 shared_ptr<ProtectedFileStream>pStream,
 bool modeWrite) {
vector<uint8_t> buffer(4096);
int64_t bufferSize = static_cast<int64_t>(buffer.size());

while (totalSize - readPosition > 0) {
// lock
threadLocker.lock();

// check remain
if (totalSize - readPosition <= 0) {
 threadLocker.unlock();
 return;
}

// get read/write offset
int64_t offsetRead = readPosition;
int64_t offsetWrite = writePosition;
int64_t toProcess = min(bufferSize, totalSize - readPosition);
readPosition += toProcess;
writePosition += toProcess;

// no need to lock more
threadLocker.unlock();

if (modeWrite) {
 // stdStream is not thread safe!!!
 try {
 threadLocker.lock();

 stdStream->seekg(offsetRead);
 stdStream->read(reinterpret_cast<char*>(&buffer[0]), toProcess);
 threadLocker.unlock();
 auto written =
 pStream->WriteAsync(
 buffer.data(), toProcess, offsetWrite, std::launch::deferred).get();

 if (written != toProcess) {
 throw rmscore::exceptions::RMSStreamException("Error while writing data");
 }
 }
 catch (exception& e) {
 qDebug() << "Exception: " << e.what();
 }
} else {
 auto read =
 pStream->ReadAsync(&buffer[0],
 toProcess,
 offsetRead,
 std::launch::deferred).get();

 if (read == 0) {
 break;
 }

 try {
 // stdStream is not thread safe!!!

```

```

 // ... code here to write the buffer...
 threadLocker.lock();

 // seek to write
 stdStream->seekp(offsetWrite);
 stdStream->write(reinterpret_cast<const char *>(buffer.data()), read);
 threadLocker.unlock();
}

catch (exception& e) {
 qDebug() << "Exception: " << e.what();
}
}
}
}

```

## Scenario: RMS authentication

The following examples show two different authentication approaches; obtaining Azure Authentication oAuth2 token using UI and without UI. **Acquiring oAuth2 Authentication Token with UI Source:**

[rmsauth\\_sample/mainwindow.cpp](#)

**Step 1:** Create a shared point of **rmsauth::FileCache** object. Description: You can set cache path or use default.

**C++:**

```
auto FileCachePtr = std::make_shared< rmsauth::FileCache>();
```

**Step 2:** Create **rmsauth::AuthenticationContext** object Description: Specify Azure *authority URI* and *FileCache* object.

**C++:**

```
AuthenticationContext authContext(
 std::string("https://sts.aadrm.com/_sts/oauth/authorize"),
 AuthorityValidationType::False,
 FileCachePtr);
```

**Step 3:** Call **acquireToken** method of **authContext** object and specify next parameters: Description:

- *Requested resource* - protected resource you want to access
- *Client unique ID* - usually a GUID
- *Redirection URI* - the URL which will be readdressed after authentication token fetched
- *Authentication prompt behavior* - if you set **PromptBehavior::Auto** the library tries to use cache and refresh token if necessary
- *User ID* - User name displayed in the prompt window

**C++:**

```
auto result = authContext.acquireToken(
 std::string("api.aadrm.com"),
 std::string("4a63455a-cfa1-4ac6-bd2e-0d046cf1c3f7"),
 std::string("https://client.test.app"),
 PromptBehavior::Auto,
 std::string("john.smith@msopentechtest01.onmicrosoft.com"));
```

**Step 4:** Get access token from result Description: Call **result-> accessToken()** method

**Note** Any of the authentication library methods may raise **rmsauth::Exception**

## Acquiring oAuth2 Authentication Token without UI Source: [rmsauth\\_sample/mainwindow.cpp](#)

**Step 1:** Create a shared point of **rmsauth::FileCache** object Description: You can set cache path or use default

C++:

```
auto FileCachePtr = std::make_shared< rmsauth::FileCache>();
```

**Step 2:** Create **UserCredential** object Description: Specify *user login* and *password*

C++:

```
auto userCred = std::make_shared<UserCredential>("john.smith@msopentechtest01.onmicrosoft.com",
 "SomePass");
```

**Step 3:** Create **rmsauth::AuthenticationContext** object Description: Specify Azure authority *URI* and *FileCache* object

C++:

```
AuthenticationContext authContext(
 std::string("https://sts.aadrm.com/_sts/oauth/authorize"),
 AuthorityValidationType::False,
 FileCachePtr);
```

**Step 4:** Call the **acquireToken** method of **authContext** and specify parameters:

- *Requested resource* - protected resource you want to access
- *Client unique ID* - usually a GUID
- *User credentials* - pass the created object

C++:

```
auto result = authContext.acquireToken(
 std::string("api.aadrm.com"),
 std::string("4a63455a-cfa1-4ac6-bd2e-0d046cf1c3f7"),
 userCred);
```

**Step 5:** Get access token from result Description: Call **result-> accessToken()** method

**Note** Any of the authentication library methods may raise **rmsauth::Exception**

# iOS/OS X code examples

5/8/2020 • 5 minutes to read • [Edit Online](#)

## IMPORTANT

Versions of the Microsoft Rights Management Service SDK released prior to March 2020 are deprecated; applications using earlier versions must be updated to use the March 2020 release. For full details, see the [deprecation notice](#).

No further enhancements are planned for the Microsoft Rights Management Service SDK. We strongly recommend adoption of the [Microsoft Information Protection SDK](#) for classification, labeling, and protection services.

This topic will introduce you to important code elements for the iOS/OS X version of the RMS SDK.

**Note** In the example code and descriptions that follow, we use the term MSIPC (Microsoft Information Protection and Control) to reference the client process.

## Using the Microsoft Rights Management SDK 4.2 - key scenarios

Following are **Objective C** code examples from a larger sample application representing development scenarios important to your orientation to this SDK. These demonstrate: use of Microsoft Protected File format referred to as protected file , use of custom protected file formats, and use of custom UI controls.

### Scenario: Consume an RMS protected file

- **Step 1:** Create an [MSProtectedData](#) object

**Description:** Instantiate an [MSProtectedData](#) object, through its create method which implements service authentication using the [MSAuthenticationCallback](#) to get a token by passing an instance of [MSAuthenticationCallback](#), as the parameter *authenticationCallback*, to the MSIPC API. See the call to [MSProtectedData protectedDataWithProtectedFile](#) in the following example code section.

```
+ (void)consumePtxtFile:(NSString *)path authenticationCallback:
 (id<MSAuthenticationCallback>)authenticationCallback
{
 // userId can be provided as a hint for authentication
 [MSProtectedData protectedDataWithProtectedFile:path
 userId:nil
 authenticationCallback:authenticationCallback
 options:Default
 completionBlock:^(MSProtectedData *data, NSError *error)
 {
 //Read the content from the ProtectedData, this will decrypt the data
 NSData *content = [data retrieveData];
 }];
}
```

- **Step 2:** Setup authentication using the Active Directory Authentication Library (ADAL).

**Description:** In this step you will see ADAL used to implement an [MSAuthenticationCallback](#) with example authentication parameters. For more information on using ADAL, see the Azure AD Authentication Library (ADAL).

```

// AuthenticationCallback holds the necessary information to retrieve an access token.
@interface MsipcAuthenticationCallback : NSObject<MSAuthenticationCallback>

@end

@implementation MsipcAuthenticationCallback

- (void)accessTokenWithAuthenticationParameters:
 (MSAuthenticationParameters *)authenticationParameters
 completionBlock:
 (void(^)(NSString *accessToken, NSError *error))completionBlock
{
 ADAAuthenticationError *error;
 ADAAuthenticationContext* context = [
 ADAAuthenticationContext authenticationContextWithAuthority:authenticationParameters.authority
 error:&error
];
 NSString *appClientId = @"com.microsoft.sampleapp";
 NSURL *redirectURI = [NSURL URLWithString:@"local://authorize"];
 // Retrieve token using ADAL
 [context acquireTokenWithResource:authenticationParameters.resource
 clientId:appClientId
 redirectUri:redirectURI
 userId:authenticationParameters.userId
 completionBlock:^(ADAuthenticationResult *result) {
 if (result.status != AD_SUCCEEDED)
 {
 NSLog(@"Auth Failed");
 completionBlock(nil, result.error);
 }
 else
 {
 completionBlock(result.accessToken, result.error);
 }
 }];
}

```

- **Step 3:** Check if the Edit right exists for this user with this content via the [MSUserPolicy accessCheck](#) method of a [MSUserPolicy](#) object.

```

- (void)accessCheckWithProtectedData:(MSProtectedData *)protectedData
{
 //check if user has edit rights and apply enforcements
 if (!protectedData.userPolicy.accessCheck(EditableDocumentRights.Edit))
 {
 // enforce on the UI
 textEditor.focusableInTouchMode = NO;
 textEditor.focusable = NO;
 textEditor.enabled = NO;
 }
}

```

### Scenario: Create a new protected file using a template

This scenario begins with getting a list of templates, [MSTemplateDescriptor](#), selecting the first one to create a policy, then creating and writing to the new protected file.

- **Step 1:** Get list of templates

```

+ (void)templateListUsageWithAuthenticationCallback:(id<MSAuthenticationCallback>)authenticationCallback
{
 [MSTemplateDescriptor templateListWithUserId:@"user@domain.com"
 authenticationCallback:authenticationCallback
 completionBlock:^(NSArray/*MSTemplateDescriptor*/ *templates, NSError *error)
 {
 // use templates array of MSTemplateDescriptor (Note: will be nil on error)
 }];
}

```

- Step 2: Create a [MSUserPolicy](#) using the first template in the list.

```

+ (void)userPolicyCreationFromTemplateWithAuthenticationCallback:
(id<MSAuthenticationCallback>)authenticationCallback
{
 [MSUserPolicy userPolicyWithTemplateDescriptor:[templates objectAtIndex:0]
 userId:@"user@domain.com"
 signedAppData:nil
 authenticationCallback:authenticationCallback
 options:None
 completionBlock:^(MSUserPolicy *userPolicy, NSError *error)
 {
 // use userPolicy (Note: will be nil on error)
 }];
}

```

- Step 3: Create a [NSMutableProtectedData](#) and write content to it.

```

+ (void)createPtxtWithUserPolicy:(MSUserPolicy *)userPolicy contentToProtect:(NSData *)contentToProtect
{
 // create an NSMutableProtectedData to write content
 [contentToProtect protectedDataInFile:filePath
 originalFileExtension:kDefaultTextFileExtension
 withUserPolicy:userPolicy
 completionBlock:^(NSMutableProtectedData *data, NSError *error)
 {
 // use data (Note: will be nil on error)
 }];
}

```

### Scenario: Open a custom protected file

- Step 1: Create a [MSUserPolicy](#) from a *serializedContentPolicy*.

```

+ (void)userPolicyWith:(NSData *)protectedData
authenticationCallback:(id<MSAuthenticationCallback>)authenticationCallback
{
 // Read header information from protectedData and extract the PL
 /*-----|
 | PL length | PL | ContentSizeLength |
 -----*/
 NSUInteger serializedPolicySize;
 NSMutableData *serializedPolicy;
 [protectedData getBytes:&serializedPolicySize length:sizeof(serializedPolicySize)];
 [protectedData getBytes:[serializedPolicy mutableBytes] length:serializedPolicySize];

 // Get the user policy , this is an async method as it hits the REST service
 // for content key and usage restrictions
 // userId provided as a hint for authentication
 [MSUserPolicy userPolicyWithSerializedPolicy:serializedPolicy
 userId:@"user@domain.com"
 authenticationCallback:authenticationCallback
 options:Default
 completionBlock:^(MSUserPolicy *userPolicy,
 NSError *error)
 {
 }];
}

```

- **Step 2:** Create a [MSCustomProtectedData](#) using the [MSUserPolicy](#) from **Step 1** and read from it.

```

+ (void)customProtectedDataWith:(NSData *)protectedData
{
 // Read header information from protectedData and extract the protectedContentSize
 /*-----|
 | PL length | PL | ContentSizeLength |
 -----*/
 NSUInteger protectedContentSize;
 [protectedData getBytes:&protectedContentSize
 length:sizeof(protectedContentSize)];

 // Create the MSCustomProtector used for decrypting the content
 // The content start position is the header length
 [MSCustomProtectedData customProtectedDataWithPolicy:userPolicy
 protectedData:protectedData
 contentStartPosition:sizeof(NSUInteger) + serializedPolicySize
 contentSize:protectedContentSize
 completionBlock:^(MSCustomProtectedData *customProtector,
 NSError *error)
 {
 //Read the content from the custom protector, this will decrypt the data
 NSData *content = [customProtector retrieveData];
 NSLog(@"%@", content);
 }];
}

```

### Scenario: Create a custom protected file using a custom (ad-hoc) policy

- **Step 1:** With an email address provided by the user, create a policy descriptor.

**Description:** In practice the following objects would be created by using user inputs from the device interface: [MSUserRights](#) and [MSPolicyDescriptor](#).

```

+ (void)policyDescriptor
{
 MSUserRights *userRights = [[MSUserRights alloc] initWithUsers:[NSArray arrayWithObjects:@"user1@domain.com", @"user2@domain.com", nil] rights:[MSEmailRights all]];

 MSPolicyDescriptor *policyDescriptor = [[MSPolicyDescriptor alloc] initWithUserRights:[NSArray arrayWithObjects:userRights, nil]];
 policyDescriptor.contentValidUntil = [[NSDate alloc]
initWithTimeIntervalSinceNow:NSTimeIntervalSince1970 + 3600.0];
 policyDescriptor.offlineCacheLifetimeInDays = 10;
}

```

- **Step 2:** Create a custom [MSUserPolicy](#) from the policy descriptor, *selectedDescriptor*.

```

+ (void)userPolicyWithPolicyDescriptor:(MSPolicyDescriptor *)policyDescriptor
{
 [MSUserPolicy userPolicyWithPolicyDescriptor:policyDescriptor
 userId:@"user@domain.com"
 authenticationCallback:authenticationCallback
 options:None
 completionBlock:^(MSUserPolicy *userPolicy, NSError *error)
 {
 // use userPolicy (Note: will be nil on error)
 }];
}

```

- **Step 3:** Create and write content to the [NSMutableCustomProtectedData](#) and then close.

```

+ (void)mutableCustomProtectedData:(NSMutableData *)backingData policy:(MSUserPolicy *)policy
contentToProtect:(NSString *)contentToProtect
{
 //Get the serializedPolicy from a given policy
 NSData *serializedPolicy = [policy serializedPolicy];

 // Write header information to backing data including the PL
 // -----
 // | PL length | PL | ContentSizeLength |
 // -----
 NSUInteger serializedPolicyLength = [serializedPolicy length];
 [backingData appendData:[NSData dataWithBytes:&serializedPolicyLength
length:sizeof(serializedPolicyLength)]];
 [backingData appendData:serializedPolicy];
 NSUInteger protectedContentLength = [MSCustomProtectedData
getEncryptedContentLengthWithPolicy:policy contentLength:unprotectedData.length];
 [backingData appendData:[NSData dataWithBytes:&protectedContentLength
length:sizeof(protectedContentLength)]];

 NSUInteger headerLength = sizeof(serializedPolicyLength) + serializedPolicyLength +
sizeof(protectedContentLength);

 // Create the NSMutableCustomProtector used for encrypting content
 // The content start position is the current length of the backing data
 // The encryptedContentSize content size is 0 since there is no content yet
 [MSCustomProtectedData customProtectorWithUserPolicy:policy
 backingData:backingData
 protectedContentOffset:headerLength
 completionBlock:^(NSMutableCustomProtectedData
*customProtector,
 NSError *error)
 {
 //Append data to the custom protector, this will encrypt the data and write it to the backing
 data
 [customProtector appendData:[contentToProtect dataUsingEncoding:NSUTF8StringEncoding]
error:&error];

 //close the custom protector so it will flush and finalise encryption
 [customProtector close:&error];
 }];
}

```

# Community resources

8/5/2019 • 2 minutes to read • [Edit Online](#)

Active Directory Rights Management Services is well supported by a growing community of developers on multiple platforms.

## Developer's Blog

[Microsoft RMS Cloud TechNet forum](#). [Stack Overflow Azure RMS](#)

## Microsoft Connect

The Rights Management Services section on the Connect site is where you can find current deliverables and have the opportunity to offer feedback.

### NOTE

If you haven't registered on Microsoft Connect, do the following:

- Navigate to [Microsoft Connect](https://connect.microsoft.com) (<https://connect.microsoft.com>)
- Sign in by using your Microsoft account
- Click **Directory** on the command bar
- Search for "Rights Management Services"
- Click **Join** to register

# Developer guidance

8/5/2019 • 2 minutes to read • [Edit Online](#)

The focus of Microsoft Rights Management SDK 4.2 is to help you build AD RMS-enabled applications that leverage Active Directory Right Management Services (AD RMS), as simply as possible.

The following topics are intended to support your design process for developing RMS-enabled applications.

- [How to register and RMS enable your app with Azure AD](#) - Describes the basics of user authentication for your RMS-enabled app.
- [How to enable error and performance logging](#) - RMS SDK 4.2 manages diagnosis and performance logs upload through a single device property.
- [How to use built-in rights](#) - Outlines the built-in rights that the RMS SDK 4.2 provides and usage restrictions that an app should enforce in honoring those restrictions.
- [How to use document tracking](#) - Using the document tracking feature requires some simple understandings about managing the associated metadata and registration with the service.

# How to register and RMS enable your app with Azure AD

5/8/2020 • 5 minutes to read • [Edit Online](#)

This topic will guide you through the basics of app registration and RMS enablement through the Azure portal followed by user authentication with the Azure Active Directory Authentication Library (ADAL).

## What is user authentication

User authentication is an essential step to establish communication between your device app and the RMS infrastructure. This authentication process uses the standard OAuth 2.0 protocol which requires key pieces of information about the current user and the authentication request.

## Registration via Azure portal

Begin by following this guide for configuring your app's registration through the Azure portal, [Configure Azure RMS for ADAL authentication](#). Be sure to copy and save the **Client ID** and **Redirect Uri** from this process for use later.

## Complete your Information Protection Integration Agreement (IPIA)

Before you can deploy your application, you must complete an IPIA with the Microsoft Information Protection team. For complete details, see the first section of the topic, [Deploy into production](#).

## Implement user authentication for your app

Each RMS API has a callback that must be implemented in order to enable the user's authentication. The RMS SDK 4.2 will then use your implementation of the callback when you do not provide an access token, when your access token needs to be refreshed or when the access token is expired.

- Android - [AuthenticationRequestCallback](#) and [AuthenticationCompletionCallback](#) interfaces.
- iOS / OS X - [MSAuthenticationCallback](#) protocol.
- Windows Phone / Window RT - [IAuthenticationCallback](#) interface.
- Linux - [IAuthenticationCallback](#) interface.

### What library to use for authentication

In order to implement your authentication callback you will need to download an appropriate library and configure your development environment to use it. You will find the ADAL libraries on GitHub for these platforms.

Each of the following resources contains guidance to setup your environment and use the library.

- [Windows Azure Active Directory Authentication Library \(ADAL\) for iOS](#)
- [Windows Azure Active Directory Authentication Library \(ADAL\) for Mac](#)
- [Windows Azure Active Directory Authentication Library \(ADAL\) for Android](#)
- [Windows Azure Active Directory Authentication Library \(ADAL\) for dotnet](#)
- For Linux SDK, the ADAL library is packaged with the SDK source, available via [Github](#).

#### **NOTE**

We recommend that you use one of the ADAL although you may use other authentication libraries.

### **Authentication parameters**

ADAL requires several pieces of information to successfully authenticate a user to Azure RMS (or AD RMS). These are standard OAuth 2.0 parameters and are generally required of any Azure AD app. You will find the current guidelines for ADAL usage in the README file of the corresponding Github repositories, listed previously.

- **Authority** – the URL for the authentication end-point, usually AAD or ADFS.
- **Resource** - the URL/URI of the service application you are trying to access, usually Azure RMS or AD RMS.
- **User Id** – the UPN, usually email address, of the user who wants to access the app. This parameter can be empty if the user is not yet known, and is also used for caching the user token or requesting a token from the cache. It is also generally used as a *hint* for user prompting.
- **Client Id** – the ID of your client app. This must be a valid Azure AD application ID. and comes from the previous registration step via the Azure portal.
- **Redirect Uri** – provides the authentication library with a URI target for the authentication code. Specific formats are required for iOS and Android. These are explained in the README files of the corresponding GitHub repositories of ADAL. This value comes from the previous registration step via the Azure portal.

#### **NOTE**

Scope is not currently used but may be and is therefore reserved for future use.

Android: `msauth://packagename/Base64UrlencodedSignature`

iOS: `<app-scheme>://<bundle-id>`

#### **NOTE**

If your app does not follow these guidelines, Azure RMS and Azure AD workflows are likely to fail and will not be supported by Microsoft.com. Further, the Rights Management License Agreement (RMLA) may be violated if an invalid Client Id is used in a production app.

### **What should an authentication callback implementation look like**

**Authentication Code Examples** - This SDK has example code showing the use of authentication callbacks. For your convenience, these code examples are represented here as well as in each of the follow linked topics.

**Android user authentication** - for more information, see [Android code examples](#), Step 2 of the first scenario, "Consuming an RMS protected file".

```
class MsipcAuthenticationCallback implements AuthenticationRequestCallback
{
 ...
 @Override
 public void getToken(Map<String, String> authenticationParametersMap,
 final AuthenticationCompletionCallback authenticationCompletionCallbackToMsipc)
 {
 String authority = authenticationParametersMap.get("oauth2.authority");
 String resource = authenticationParametersMap.get("oauth2.resource");
 String userId = authenticationParametersMap.get("userId");
 mClientId = "12345678-ABCD-ABCD-ABCD-ABCDEFHGIJ"; // get your registered Azure AD application ID here
 mEndpointUrl = "https://login.microsoftonline.com";
 }
}
```

```

mRedirectURI = urn:ietf:wg:oauth:2.0:zero;
final String userHint = (userId == null)? "" : userId;
AuthenticationContext authenticationContext = App.getInstance().getAuthenticationContext();
if (authenticationContext == null || !authenticationContext.getAuthority().equalsIgnoreCase(authority))
{
 try
 {
 authenticationContext = new AuthenticationContext(App.getInstance().getApplicationContext(),
authority, ...);
 App.getInstance().setAuthenticationContext(authenticationContext);
 }
 catch (NoSuchAlgorithmException e)
 {
 ...
 authenticationCompletionCallbackToMsipc.onFailure();
 }
 catch (NoSuchPaddingException e)
 {
 ...
 authenticationCompletionCallbackToMsipc.onFailure();
 }
}
App.getInstance().getAuthenticationContext().acquireToken(mParentActivity, resource, mClientId,
mRedirectURI, userId, mPromptBehavior,
"&USERNAME=" + userHint, new AuthenticationCallback<AuthenticationResult>()
{
 @Override
 public void onError(Exception exc)
 {
 ...
 if (exc instanceof AuthenticationCancelError)
 {
 ...
 authenticationCompletionCallbackToMsipc.onCancel();
 }
 else
 {
 ...
 authenticationCompletionCallbackToMsipc.onFailure();
 }
 }

 @Override
 public void onSuccess(AuthenticationResult result)
 {
 ...
 if (result == null || result.getAccessToken() == null
 || result.getAccessToken().isEmpty())
 {
 ...
 }
 else
 {
 // request is successful
 ...
 authenticationCompletionCallbackToMsipc.onSuccess(result.getAccessToken());
 }
 }
});
}

```

**iOS/OS X user authentication** - for more information, see [iOS/OS X code examples](#), *Step 2 of the first scenario, "Consuming an RMS protected file"*.

```

// AuthenticationCallback holds the necessary information to retrieve an access token.
@interface MsipcAuthenticationCallback : NSObject<MSAuthenticationCallback>

@end

@implementation MsipcAuthenticationCallback

- (void)accessTokenWithAuthenticationParameters:
 (MSAuthenticationParameters *)authenticationParameters
 completionBlock:
 (void(^)(NSString *accessToken, NSError *error))completionBlock
{
 ADAuthenticationError *error;
 ADAuthenticationContext* context = [ADAuditontext
 authenticationContextWithAuthority:authenticationParameters.authority error:&error];

 NSString *appClientId = @”12345678-ABCD-ABCD-ABCD-ABCDEFHIJ”;

 // get your registered Azure AD application ID here

 NSURL *redirectURI = [NSURL URLWithString:@”ms-sample://com.microsoft.sampleapp”];

 // get your <app-scheme>://<bundle-id> here
 // Retrieve token using ADAL
 [context acquireTokenWithResource:authenticationParameters.resource
 clientId:appClientId
 redirectUri:redirectURI
 userId:authenticationParameters.userId
 completionBlock:^(ADAuthenticationResult *result)
 {
 if (result.status != AD_SUCCEEDED)
 {
 NSLog(@”Auth Failed”);
 completionBlock(nil, result.error);
 }
 else
 {
 completionBlock(result.accessToken, result.error);
 }
 }];
}

```

**Linux user authentication** - for more information, see [Linux code examples](#).

```

// Class Header
class AuthCallback : public IAuthenticationCallback {
private:

 std::shared_ptr<rmsauth::FileCache> FileCachePtr;
 std::string clientId_;
 std::string redirectUrl_;

public:

 AuthCallback(const std::string& clientId,
 const std::string& redirectUrl);
 virtual std::string GetToken(shared_ptr<AuthenticationParameters>& ap) override;
};

class ConsentCallback : public IConsentCallback {
public:

 virtual ConsentList Consents(ConsentList& consents) override;
};

// Class Implementation
AuthCallback::AuthCallback(const string& clientId, const string& redirectUrl)
: clientId_(clientId), redirectUrl_(redirectUrl) {
 FileCachePtr = std::make_shared<FileCache>();
}

string AuthCallback::GetToken(shared_ptr<AuthenticationParameters>& ap)
{
 string redirect =
 ap->Scope().empty() ? redirectUrl_ : ap->Scope();

 try
 {
 if (redirect.empty()) {
 throw rmscore::exceptions::RMSInvalidArgumentException(
 "redirect Url is empty");
 }

 if (clientId_.empty()) {
 throw rmscore::exceptions::RMSInvalidArgumentException("client Id is empty");
 }

 AuthenticationContext authContext(
 ap->Authority(), AuthorityValidationType::False, FileCachePtr);

 auto result = authContext.acquireToken(ap->Resource(),
 clientId_, redirect,
 PromptBehavior::Auto,
 ap->UserId());
 return result->accessToken();
 }

 catch (const rmsauth::Exception& ex)
 {
 // out logs
 throw;
 }
}

```

# How to: Enable error and performance logging

8/5/2019 • 2 minutes to read • [Edit Online](#)

The Microsoft Rights Management SDK 4.2 manages diagnosis and performance logs upload through a single device property.

## Overview

You can improve your users' experience and troubleshooting by enabling automatic diagnostics, performance, and telemetry logging data upload to Microsoft.

### IMPORTANT

In order to honor user privacy, you as the app developer, must ask the user to consent before enabling the automatic logging.

### NOTE

As example, here is a standard message Microsoft uses for logging notification:

*By turning on Error and Performance Logging, you are agreeing to send Error and Performance Data to Microsoft. Microsoft will collect error and performance data over the internet ("Data"). Microsoft uses this Data to provide and improve the quality, security and integrity of Microsoft products and services. For example, we analyze performance and reliability, such as what features you use, how quickly the features respond, device performance, user interface interactions, and any problems you experience with the product. Data will also include information about the configuration of your software like the software you are currently running, and the IP address.*

You will manager logging control through two properties.

- Enable logging through the **IpcCustomerExperienceDataCollectionEnabled** property. The setting is persistent across device resets.
- Control the logging level through the **IpcLogLevel** property using the following settings.
  - 1 - Verbose
  - 2 - Informational
  - 3 - Warning
  - 4 - Error
  - 5 - Critical

In each of the example code snippets following, the calling application can set or query the property.

### Android

Enable automatic logging

```
SharedPreferences preferences = PreferenceManager.getDefaultSharedPreferences(context);
SharedPreferences.Editor editor = preferences.edit();
editor.putBoolean("IpcCustomerExperienceDataCollectionEnabled", true);
editor.commit();
```

Get current logging control flag setting

```
SharedPreferences preferences = PreferenceManager.getDefaultSharedPreferences(context);
Boolean isLogUploadEnabled = preferences.getBoolean("IpcCustomerExperienceDataCollectionEnabled", false);
```

## iOS

Enable automatic logging

```
NSUserDefaults *prefs = [NSUserDefaults standardUserDefaults];
[prefs setBool:FALSE forKey:@"IpcCustomerExperienceDataCollectionEnabled"];
[[NSUserDefaults standardUserDefaults] synchronize];
```

Get current logging control flag setting

```
[[NSUserDefaults standardUserDefaults] boolForKey:@"IpcCustomerExperienceDataCollectionEnabled"];
```

Set log level control

```
NSUserDefaults *prefs = [NSUserDefaults standardUserDefaults];
[prefs setInteger:1 forKey:@"IpcLogLevel"];
[[NSUserDefaults standardUserDefaults] synchronize];
```

Get log level control setting

```
[[NSUserDefaults standardUserDefaults] boolForKey:@"IpcLogLevel"];
```

## Windows

Enable automatic logging

```
CustomerExperienceConfiguration::Option = CustomerExperienceOptions::LoggingEnabledNow;
```

For more information on optional settings, see [CustomerExperienceOptions](#).

Get current logging control flag setting

```
CustomerExperienceOptions loggingOption = CustomerExperienceConfiguration::Option;
```

**Note** - The Windows code snips above are in C++. For C#, update the syntax with '.' in place of '::'.

**Linux / C++** - This SDK has some basic logging that is not as extensive as that of the other platforms. For more information see the **Troubleshooting** section of the "README.md" at [RMS SDK for portable C++](#).

# How to: Use built-in rights

8/5/2019 • 4 minutes to read • [Edit Online](#)

This topic outlines the built-in rights that the Microsoft Rights Management SDK 4.2 provides and usage restrictions that an app should enforce in honoring those restrictions. The following shows the built-in rights; common rights, editable document rights and email rights followed by a description and their values by operating system.

**Note** - For the Linux SDK, see the *rights.h* source file for details.

## Common Rights

**All** - A collection of all common rights.

- Android: [CommonRights.All](#)
- iOS and OS X: [MSCommonRights](#) - user owner and view to implement All
- Windows Store and Windows Phone: [CommonRights.All](#)
- Linux: [CommonRights::All](#)

**Owner** - The Owner right grants full control over the protected content.

- Android: [CommonRights.Owner](#)
- iOS and OS X: [MSCommonRights owner](#)
- Windows Store and Windows Phone: [CommonRights.Owner](#)
- Linux: [CommonRights::Owner](#)

**View** - The right to view protected content. Typically, when this right is granted, the application enables the user to open and view protected content; however, additional rights are required to modify, extract, forward, or save the content.

- Android: [CommonRights.View](#)
- iOS and OS X: [MSCommonRights view](#)
- Windows Store and Windows Phone: [CommonRights.View](#)
- Linux: [CommonRights::View](#)

## Editable Document Rights

**All** - A collection that contains all of the editable document rights.

- Android: [EditableDocumentRights.All](#)
- iOS and OS X: [MSEditableDocumentRights all](#)
- Windows Store and Windows Phone: [EditableDocumentRights.All](#)
- Linux: [EditableDocumentRights::All](#)

**Comment** - The right to make comments on the document.

- Android: [EditableDocumentRights.Comment](#)
- iOS and OS X: [MSEditableDocumentRights comment](#)
- Windows Store and Windows Phone: [EditableDocumentRights.Comment](#)

- Linux: [EditableDocumentRights::Comment](#)

**Edit** - The right to edit protected content and save it in the same protected format. Typically, when this right is granted, the app enables the user to change protected content and then save it to the same file.

- Android: [EditableDocumentRights.Edit](#)
- iOS and OS X: [MSEditableDocumentRights.edit](#)
- Windows Store and Windows Phone: [EditableDocumentRights.Edit](#)
- Linux: [EditableDocumentRights::Edit](#)

**Export** - The right to extract content from a protected format and place it in a different AD RMS-protected format. Typically, when this right is granted, the app enables the user to save protected content to other AD RMS-protected formats; for example, if the application implements a *Save As* functionality.

- Android: [EditableDocumentRights.Export](#)
- iOS and OS X: [MSEditableDocumentRights.exportable](#)
- Windows Store and Windows Phone: [EditableDocumentRights.Export](#)
- Linux: [EditableDocumentRights::Export](#)

**Extract** - The right to extract content from a protected format and place it in an unprotected format. Typically, when this right is granted, the app enables the user to copy and paste information from protected content. If the app implements a *Save As* functionality, the application might also enable the user to save protected content to unprotected formats and other protected formats. This right has the same value as the Extract right for email.

- Android: [EditableDocumentRights.Extract](#)
- iOS and OS X: [MSEditableDocumentRights.extract](#)
- Windows Store and Windows Phone: [EditableDocumentRights.Extract](#)
- Linux: [EditableDocumentRights::Extract](#)

**Print** - The right to print protected content. Typically, when this right is granted, the app enables the user to print protected content. This right has the same value as the Print right for email.

- Android: [EditableDocumentRights.Print](#)
- iOS and OS X: [MSEditableDocumentRights.print](#)
- Windows Store and Windows Phone: [EditableDocumentRights.Print](#)
- Linux: [EditableDocumentRights::Print](#)

## Email Rights

**All** - A collection that contains all of the email rights.

- Android: [EmailRights.All](#)
- iOS and OS X: [MSEmailRights.all](#)
- Windows Store and Windows Phone: [EmailRights.All](#)
- Linux: [EmailRights::All](#)

**Extract** - The right to extract content from a protected format and place it in an unprotected format. Typically, when this right is granted, the app enables an email recipient to copy and paste information from a protected message. If the app implements a *Save As* functionality, the application might also enable the recipient to save protected content to unprotected formats and other protected formats. This right has the same value as the Extract right for editable documents.

- Android: [EmailRights.Extract](#)

- iOS and OS X: [MSEmailRights extract](#)
- Windows Store and Windows Phone: [EmailRights.Extract](#)
- Linux: [EmailRights::Extract](#)

**Forward** - The right to forward a protected message. Typically, when this right is granted, the app enables an email recipient to forward a protected message.

- Android: [EmailRights.Forward](#)
- iOS and OS X: [MSEmailRights forward](#)
- Windows Store and Windows Phone: [EmailRights.Forward](#)
- Linux: [EmailRights::Forward](#)

**Print** - The right to print protected content. Typically, when this right is granted, the app enables an email recipient to print a protected message. This right has the same value as the Print right for editable documents.

- Android: [EmailRights.Print](#)
- iOS and OS X: [MSEmailRights print](#)
- Windows Store and Windows Phone: [EmailRights.Print](#)
- Linux: [EmailRights::Print](#)

**Reply** - Typically, when this right is granted, the app enables an email recipient to reply to a protected message and include a copy of the original message.

- Android: [EmailRights.Reply](#)
- iOS and OS X: [MSEmailRights reply](#)
- Windows Store and Windows Phone: [EmailRights.Reply](#)
- Linux: [EmailRights::Reply](#)

**ReplyAll** - Typically, when this right is granted, the app enables an email recipient to reply to all recipients of a protected message and include a copy of the original message.

- Android: [EmailRights ReplyAll](#)
- iOS and OS X: [MSEmailRights replyAll](#)
- Windows Store and Windows Phone: [EmailRights ReplyAll](#)
- Linux: [EmailRights::ReplyAll](#)

# How to: Use document tracking

3/17/2020 • 2 minutes to read • [Edit Online](#)

## IMPORTANT

Versions of the Microsoft Rights Management Service SDK released prior to March 2020 are deprecated; applications using earlier versions must be updated to use the March 2020 release. For full details, see the [deprecation notice](#).

No further enhancements are planned for the Microsoft Rights Management Service SDK. We strongly recommend adoption of the [Microsoft Information Protection SDK](#) for classification, labeling, and protection services.

Using the document tracking feature requires some simple understandings about managing the associated metadata and registration with the service.

## Managing document tracking metadata

Each of the operating systems supporting document tracking have similar implementations. These include as set of properties that represent the metadata, a new parameter added to the user policy creation methods and a method for registering the policy to be tracked with the document tracking service.

Operationally, only the **content name** and the **notification type** properties are required for document tracking.

The sequence of steps you will use to setup document tracking for a given piece of content is:

- Create a **license metadata** object then set the **content name** and **notification type**. These are the only required properties.
  - Android - [LicenseMetadata](#)
  - iOS - [MSLicenseMetadata](#)

Choose policy type; template or ad-hoc:

- For template based document tracking, create a **user policy** object passing the license metadata as a parameter.
  - Android - [UserPolicy.create](#)
  - iOS - [MSUserPolicy.userPolicyWithTemplateDescriptor](#)
- For ad-hoc based document tracking, set the **license metadata** property on the **policy descriptor** object.
  - Android - [PolicyDescriptor.setLicenseMetadata](#)
  - iOS - [MSPolicyDescriptor.licenseMetadata](#).

**Note** The license metadata object is only directly accessible during the process of setting up document tracking for the given user policy. Once the user policy object is created, the associated license metadata is not accessible i.e. changing the values of license metadata has no effect.

- Finally, call the platform registration method for document tracking
  - Android - [UserPolicy.registerForDocTracking asynchronous](#) or [UserPolicy.registerForDocTracking synchronous](#)
  - iOS - [MSUserPolicy.registerForDocTracking](#)

# API SDK 4.2 reference

8/5/2019 • 2 minutes to read • [Edit Online](#)

The Azure Information Protection SDK 4.2 supports several operating systems. For more information on specifics, see [What's new](#).

## Apple

- [iOS / OS X API reference](#) - API reference for the Apple iOS and OS X operating systems.

## Google

- [Android namespaces](#)

## Linux

- [Linux API reference](#) - API reference for our Linux flavored operating system support is hosted on Github - [RMS SDK for C++](#).

## Microsoft

- [Windows API Reference](#) - API reference for the Windows Phone and Windows Store Applications SDKs.

## Related topics

- [Get started](#)

# Linux API reference

3/17/2020 • 2 minutes to read • [Edit Online](#)

## IMPORTANT

Versions of the Microsoft Rights Management Service SDK released prior to March 2020 are deprecated; applications using earlier versions must be updated to use the March 2020 release. For full details, see the [deprecation notice](#).

No further enhancements are planned for the Microsoft Rights Management Service SDK. We strongly recommend adoption of the [Microsoft Information Protection SDK](#) for classification, labeling, and protection services.

API reference for our Linux flavored operating system support is hosted on Github - [RMS SDK for C++](#). For more information, see [Get started](#).

# Rights Management Services SDK 2.1

8/5/2019 • 2 minutes to read • [Edit Online](#)

## Purpose

The Rights Management Services SDK 2.1 platform enables developers to build applications that leverage Rights Management Services (RMS) or Azure Rights Management to provide information protection. The RMS SDK 2.1 handles complex security practices such as key management, encryption and decryption processing and offers a simplified API for easy application development.

### Developer audience

The RMS SDK 2.1, available from the [RMS SDK 2.1 download page](#) on the Microsoft download center, is used to create custom applications that enable rights management on digital assets and enforce terms-of-use for those assets. Knowledge of the C++ programming language is required.

For answers to frequently asked questions, see the developers section of our [RMS FAQ](#)

### Run-time requirements

For information about the run-time requirements for a particular programming element, see the Requirements section of the reference topic for that element.

TOPIC	DESCRIPTION
<a href="#">Overview</a>	Rights Management Services (RMS) is an information protection technology that helps safeguard digital information from unauthorized use.
<a href="#">Getting started</a>	The RMS SDK 2.1 platform enables developers to build applications that leverage RMS information protection.
<a href="#">Release notes</a>	This topic contains important information about this and previous releases of the RMS SDK 2.1.
<a href="#">Developer notes</a>	This section covers specific guidance for several important development scenarios.
<a href="#">API reference</a>	This section contains topics covering reference material for all of the API elements.

## Related topics

- [RMS SDK 2.1 download page](#)
- [RMS FAQ](#)

# Overview

8/5/2019 • 2 minutes to read • [Edit Online](#)

Rights Management Services SDK 2.1 is an information protection technology that helps safeguard digital information from unauthorized use. Through your rights-enabled application, content owners will be able to define who can open, modify, print, forward, or take other actions with the content.

AD RMS consists of both [server](#) and [client](#) components. The server, running on Azure or Windows Server, consists of multiple web services.

The [client](#) component can be run on either a client or server operating system and contains functions that enable an application to encrypt and decrypt content, retrieve templates and revocation lists, acquire licenses and certificates from a server, and other related rights management tasks.

For more information, see [Application types](#).

The following are just a few of the scenarios to which applications built on the Rights Management Services SDK 2.1 can be applied.

- A law firm wants to prevent sensitive email messages from being printed or forwarded.
- The developers of computer-aided design and manufacturing software want to limit drawing access to a small group of users within the research division without requiring the use of passwords.
- The owners of a graphic design website want to use a single license that allows free viewing of low-resolution copies of their images but requires payment for access to the high-resolution versions.
- The owners of an online document library want to enable rights to view, print, or edit documents based on the identity of the user.
- A corporation wants to publish sensitive employee information to an internal website that restricts viewing and editing privileges to certain users.

For more information on AD RMS server, AD RMS client and their functionality, see the TechNet content for [IT Pro documentation for AD RMS](#).

The remaining topics in this section cover the RMS Architecture and its implementations.

## In this section

TOPIC	DESCRIPTION
<a href="#">Client</a>	This topic describes the purpose and function of the Rights Management Service Client 2.1
<a href="#">Server</a>	This topic describes the purpose and functions of the RMS Server; for Azure and Windows Server.

## Related topics

- [RMS Concepts](#)
- [Get started](#)
- [IT Pro documentation for AD RMS](#)

# Client

8/5/2019 • 2 minutes to read • [Edit Online](#)

This topic describes the purpose and function of the Rights Management Service Client 2.1.

The RMS Client 2.1 is software designed for your client computers to help protect access to and usage of information flowing through applications that use RMS whether installed on your premises or in a Microsoft datacenter. It ships as an optional download which can be, with acknowledgment and acceptance of its license agreement, freely distributed with your third-party software to enable client access to content that has been rights-protected by use and deployment of RMS servers in your environment.

The RMS Client 2.1, exposes functionality that enables users to create, publish, and consume protected (encrypted) content. Specifically, an RMS-enabled applications leverage the client installed on the end-user machine to perform tasks that it was built to perform in the context of rights management.

The Rights Management Services SDK 2.1 works with RMS Client 2.1. Rights enabled applications built on the RMS SDK 2.1 must use the RMS Client 2.1.

For more information, see the [TechNet documentation on the RMS Client 2.1](#).

## Related topics

- [Overview](#)
- [Enable your service application to work with cloud based RMS](#)
- [TechNet documentation on the RMS Client 2.1](#)

# Server

8/5/2019 • 2 minutes to read • [Edit Online](#)

This topic describes the purpose and functions of the RMS Server; for Azure and Windows Server.

**Azure RMS** - For information on using the Azure Rights Management service, see [Enable your service application to work with cloud based RMS](#).

## IMPORTANT

We recommend developing and testing your application via Azure RMS.

**Windows Server** - For RMS on premise servers, beginning with Windows Server 2008, you can install and configure the RMS service by adding it as a role. To install the service on prior operating systems, download it from the Microsoft download center at [Microsoft Windows Rights Management Services with Service Pack 2](#).

Of the many web services installed, the following are important for application development for RMS Server on Windows Server.

SERVICE	DESCRIPTION
Administration	Hosts the Administration website that enables you to manage RMS. The service runs on root certification servers and on licensing servers. You can use the Active Directory Rights Management Services Scripting API to write administration scripts.
Account Certification	Creates machine certificates that identify computers in the RMS certificate hierarchy and rights account certificates that associate users with specific computers. For more information, see Activating a Computer and Activating a User.  This service runs on the root certification server.
Licensing	Issues an <i>end-user license</i> . The service runs on root certification servers and on licensing servers.
Publishing	Creates an <i>issuance license</i> which define the policies that can be enumerated in an end-user license. For more information, see <a href="#">Creating an Issuance License</a> .  The service runs on root certification servers and on licensing servers.
Pre-certification	Enables a server to request a <i>rights account certificate</i> on behalf of a user. The service runs on root certification servers and on licensing servers.
Service Locator	Provides the URL of the account certification, licensing, and publishing services to Active Directory so that they can be discovered by RMS clients. The service runs on root certification servers and on licensing servers.

## Related topics

- [Overview](#)
- [Microsoft Internet Information Services](#)
- [Enable your service application to work with cloud based RMS](#)
- [Microsoft Windows Rights Management Services with Service Pack 2](#)
- [Active Directory Rights Management Services Scripting API](#)
- [Activating a Computer](#)
- [Activating a User](#)
- [Creating an Issuance License](#)

# Getting started

12/19/2019 • 2 minutes to read • [Edit Online](#)

The Rights Management Services SDK 2.1 platform enables developers to build applications that leverage RMS information protection via an RMS Server or Azure RMS. The platform handles complex security practices such as key management, encryption and decryption processing and, offers a simplified API for easy application development.

## Get started with RMS SDK 2.1

This topic will guide you through the process of setting up and running your rights-enabled application in a testing environment. The following topics discuss how to set up your development environment and are listed such that they suggest an order that you could perform the tasks.

### In this sections

TOPIC	DESCRIPTION
<a href="#">Release Notes</a>	This topic contains important information about this and previous releases of the RMS SDK 2.1.
<a href="#">Install the SDK</a>	This topic guides you through installing the developer tools.
<a href="#">Configure Visual Studio</a>	This topic contains instructions about how to configure a Visual Studio project to use the RMS SDK 2.1.
<a href="#">Developing your application</a>	This topic contains essential guidance on the core aspects of an RMS enabled application and can serve as the foundation of your own application development.
<a href="#">Testing your application</a>	This topic contains instructions about how to setup for your application testing.
<a href="#">Deploy into production</a>	This topic guides you through deployment options for your rights-enabled application.

Try using RMS SDK 2.1 by following the guidance in these topics:

- [Install the SDK](#)
- [Configure Visual Studio](#)
- [Developing your application](#)
- [Testing your application](#)
- [Deploy into production](#)

### Why use RMS SDK 2.1 for protecting your content

For developers who want to add RMS support to their new and existing applications, the RMS SDK 2.1 helps make it easier to:

- Author manageable, compliant and robust RMS-aware applications.
- Encrypt user data persistently. The data remains encrypted regardless of the environment, device, or operating system.

- Enforce a rich set of usage restrictions, such as preventing screen captures of your sensitive data.
- Support enterprise-managed protection policies.
- Support new authentication mechanisms and encryption algorithms as they become available.

The RMS SDK 2.1 supports a range of important client and server platforms. For more information see, [Supported platforms](#).

## Core principles

**Simplicity**—Feedback and usage patterns for the AD RMS SDK 1.0 were analyzed, and that data used to simplify or automate the most difficult programming tasks. RMS applications authored using the RMS SDK 2.1 typically require 5–10 times fewer lines of RMS code than RMS applications written using AD RMS SDK 1.0. **Write once**—RMS SDK 2.1 applications do not need a code change or a recompile to work with the newest RMS features. New RMS features will become available in your existing application as they get added to the RMS server.

**Consistency**—RMS SDK 2.1 helps make it easy to write applications that consistently honor different RMS configurations. It also significantly reduces the amount of RMS user interface you, as the application developer, needs to author, encouraging a consistent look and feel and reducing the need for user education.

## Related topics

- [RMS Developers Guide](#)

# Release notes

5/8/2020 • 7 minutes to read • [Edit Online](#)

This article contains important information about this and previous releases of the RMS SDK 2.1.

## October 2019 - update

- Under some circumstances, using symmetric key authentication fails to authenticate the user with Azure RMS which prevents protecting and unprotecting content.
- The RMS client may crash when trying to check whether some PDF documents that have been previously protected and unprotected are currently protected.
- Using DNS redirection for AD RMS servers that have been configured on special ports will not work correctly.

## September 2019 - update

- Fixed a deadlock that may occur when trying to call the initialization methods at the same time as some other RMS client methods.
- Fixed an issue with determining whether password protected Office files are RMS protected.
- Update licensing validation for special purpose licenses.
- Updates to the PDF protector.
- Other bug fixes.
- Update to link statically against the C runtime libraries.

## April 2019 - update

- Bug fixes in the File API.
- File API updated to check the EXPORT right rather than the EXTRACT right when decrypting content.
- Installer fix to ensure that the new PDF v2 protector is installed upon upgrade.
- Telemetry changes. This change required an update to the installation package that installs the C runtime libraries.
- Service backend authentication changes, **please update to this SDK version to minimize disruption if you use symmetric key authentication for your applications**
- Support for VC 15.9

## October 2017 - update

- Addition of two new APIs for environment initialization and uninitialization. For information, see [IpcInitializeEnvironment](#) and [IpcUninitializeEnvironment](#).
- Visio file types are now supported. For more information, see [File API configuration](#).

## February 2016 - SDK documentation update

### NOTE

The feature documentation updates in this section apply to the SDK download dated 12/11/2015.

- Improved authentication flow - using OAuth2 token-based authentication via the [Azure Active](#)

[Directory Authentication Library \(ADAL\)](#). For more information on this process and the API extensions for it, see [ADAL authentication for your RMS enabled application](#).

- **Update to ADAL** - By updating your application to use ADAL authentication rather than the Microsoft Online Sign-in Assistant, you and your customers will be able to:
  - Utilize multi-factor authentication
  - Install the RMS 2.1 client without requiring administrative privileges to the machine
  - Certify your application for Windows 10
- **Support for Microsoft Online Sign-in Assistant (SIA) with the RMS SDK is being removed.** We will continue to support the use of SIA for six months after which time support will stop.

## December 2015 update

- Performance improvements have been implemented in several areas including:
  - Publish from primary licensing server when using license-only servers.
  - RMS SDK 2.1 fails faster when there is no network connection.
- Many updates to improve error messaging and troubleshooting experience.
- Note also that the [Supported platforms](#) listing is also updated.
- The need for the pre-production environment and the use of an application manifest has been removed from the RMS SDK 2.1. These sections of this developer documentation set have been removed and the overall documentation simplified and reorganized.

## May 2015 update

- **Service apps and cloud based RMS** - [IPC\\_CREDENTIAL\\_SYMMETRIC\\_KEY](#) needs three pieces of information; symmetric key, [AppPrincipalId](#), and [TenantBposId](#). The article for this has been updated to provide guidance on processing this information. For this update, see the revised version of [Enable your service application to work with cloud based RMS](#).

## April 2015 update

- **Document tracking** is now possible through a set of new APIs. For more information, see [Tracking Content](#).
- **Encryption type** - We now support API level control for selection of the encryption package. For more information, see [Working with encryption](#).

**Note** We will no longer be exposing the `IPC_LI_DEPRECATED_ENCRYPTION_ALGORITHMS` flag in our API. This means that future apps will no longer compile if they reference this flag, but apps already built will continue to work since we will honor the flag privately in the API code. Getting the benefit of the old deprecated encryption algorithms flag can still be achieved simply by changing a flag. For more information, see [Working with encryption](#).

- **Server Mode Applications**, those using an [API mode values](#) of `IPC_API_MODE_SERVER`, no longer require an application manifest. You can test your application against a production RMS server and are not required to obtain a production license when switching to production environment. For more information on server mode applications, see [Application types](#).
- **Logging** is now implemented through both file and Event Tracing for Windows methods.
- If you're running on a **Windows 7 SP1 or Windows Server 2008 R2** machine, see the note following under "Important developer notes".

## January 2015 update

- **Supported protected file (pfile) size increase** - Now supports pfile sizes greater than one gigabyte (1 GB). For more information on pfiles, see [Supported File Formats](#).
- **Improved logging for better diagnostics** - Logging levels will show **ERROR** or **WARNING** for messages that should be reviewed. All other messages, including exceptions, which are still displayed, will be logged as **INFO**.

We chose this approach so that you won't lose any details. Now, only the important messages are shown with level as **WARNING**.

- **Acquiring Company templates** – substantial fixes to the template acquire code, based on customer reports and feedback.
- Improved localization consistency

## October 2014 update

- Default behaviors for the File API component of SDK have been updated. For more information, see [File API configuration](#).
- Email notification, a new feature, is described in the Developer notes article, [Enabling email notification](#).

## July 2014 update

The File API component of SDK has been extended and offers the following features:

- Identifies which protector to use.
- Provides RMS protection at the granularity level of a file.

Functions added in this release:

**Note** - Further supporting data types and structures, not listed here, have been added for the File API extensions. All articles that have been updated for this release are marked as **preliminary and subject to change**.

- [IpcfOpenFileOnHandle](#)
- [IpcfOpenFileOnILockBytes](#)
- [IpcfGetProperty](#)
- [IpcfLogicalFileRangeToRawFileRange](#)
- [IpcfReadFile](#)
- [IpcfSetEndOfFile](#)
- [IpcfWriteFile](#)

## April 2014 update

- **File API memory usage**, especially for large PFiles has been improved significantly.
- **Content ID** is now writable via the property **IPC\_LI\_CONTENT\_ID**. For more information, see [License property types](#).
- **Production manifest requirement** - When your RMS enabled application/service is being run in server mode, we will not require a manifest anymore. For more information, see [Application types](#).
- **Documentation updates**

**Testing best practice** - guidance added for use of on-premise server before testing with Azure RMS. For

more information, see [Enable your service application to work with cloud based RMS](#).

## Important developer notes

- **Native support for all file types**

Native support can be added for any file type (extension) with this release of Rights Management Services SDK 2.1. For instance, for any extension <ext> (non-office and pdf), \*.p<ext> will be used if the admin configuration for that extension is "NATIVE".

For more information on supported file types, see [File API configuration](#).

- **Windows 7 SP1 and Windows Server 2008 R2 SP1 machines** without the update, [KB2533623](#), may have the following error protecting any office file "The parameter is incorrect. Error code 0x80070057". If you see this, please install the update and try again. If you're still seeing issues, please contact RMS SDK Beta Feedback alias [rmcstbeta@microsoft.com](mailto:rmcstbeta@microsoft.com).

**Note** As of the April 2015 release, a check has been added to the installation process for this KB.

- **File API integration**

The Active Directory Rights Management Services File API , with the addition of File API, provides the following benefits and capabilities.

- You can protect confidential data in an automated way without having to know the details of the Information Rights Management (IRM) implementation used by various file formats.
- Microsoft Office files, Portable Document Format (PDF) files, and selected other file types can be protected using native protection. For a complete list of file types that can be protected with native protection, see [File API configuration](#).
- All files, except system files and Office files can be protected using RMS Protected File format (PFile).

The file API is implemented via the following four new functions: [IpcfDecryptFile](#), [IpcfEncryptFile](#), [IpcfGetSerializedLicenseFromFile](#), and [IpcflsFileEncrypted](#).

The File API requires that the Rights Management Service Client 2.1 be installed on the client computer and that the computer have connectivity to an RMS server. For more information on RMS server, RMS client, and their functionality, see the TechNet content for [IT Pro documentation for RMS](#).

- **Issue:** When creating a license from scratch, ownership rights must be granted explicitly.

**Solution:** Your application must explicitly add **Owner** rights to the license owner when creating a license from scratch using [IpcCreateLicenseFromScratch](#). For more information, see [Add explicit owner rights](#).

- **Issue:** If an application calls [IpcProtectWindow](#) or [IpcUnprotectWindow](#) twice for the same window by using its handle, RMS SDK 2.1 will return a failure in the **HRESULT**.

**Solution:** For specific guidance on this, see the Remarks section in [IpcProtectWindow](#) and [IpcUnprotectWindow](#).

- **Issue:** When building for multiple architectures, you must use this guidance.

**Solution:** If you want to use the Ipcsecproc\*isv.dll for a different architecture (for example, you have installed the 64-bit SDK on a 64-bit computer but now want to deploy on a 32-bit computer that requires Ipcsecproc\*isv.dll), you must install the 32-bit SDK on a different computer and copy the Ipcsecproc\*isv.dll files to there from the "%PROGRAMFILES%\Microsoft Information Protection And Control" folder (the default location or wherever you chose to install the SDK).

## Frequently asked questions

**Q:** How does the default language behavior work with functions that take an LCID parameter?

**A:** Use 0 for the default locale. In this case, AD RMS Client 2.1 looks up names and descriptions in the following sequence and retrieves the first available one:

- 1 - User preferred LCID.
- 2 - System locale LCID.
- 3 - The first available language specified in the Rights Management Server (RMS) template.

If no name and description can be retrieved, an error is returned. There can be only one name and description for a specific LCID.

# Install the SDK

8/5/2019 • 2 minutes to read • [Edit Online](#)

This topic guides you through installing the developer tools.

## Instructions

### Install the developer tools

1. Download the [Rights Management Services SDK 2.1](#) from the Microsoft Download Center, being careful to choose the correct architecture version for your computer.
2. Run the installer package from your install location:

`...\\setup_sdk.exe`

The Setup\_sdk.exe file will install both the RMS SDK 2.1 and Active Directory Rights Management Services Client 2.1.

For more information on the files installed on your system by "setup\_sdk.exe", see [Development environment files](#)

## Related topics

- [Development environment files](#)

# Configure Visual Studio

8/5/2019 • 2 minutes to read • [Edit Online](#)

This topic contains instructions about how to configure a Visual Studio project to use the Rights Management Services SDK 2.1.

## Prerequisites

- [Install the SDK](#)

### Instructions

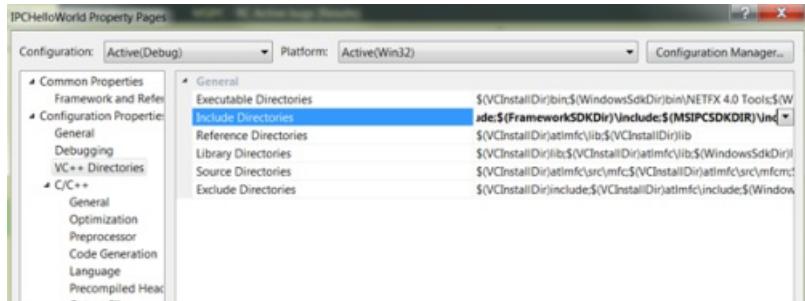
#### Step 1: Configure a Visual Studio project to use RMS SDK 2.1

These instructions are specific to Microsoft Visual Studio 2010. If you are using a different version of Microsoft Visual Studio, your settings dialog boxes may appear slightly different.

These instructions apply to building a native 32-bit application.

1. Add the RMS SDK 2.1 include directory to your Visual Studio 2010 project.

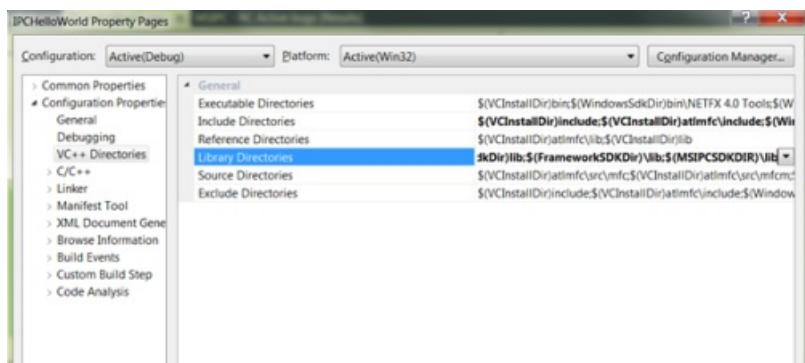
Under **Configuration Properties** select **VC++ Directories** and add the RMS SDK 2.1 include directory, **\$(MSIPCSDKDIR)\inc**, to the **Include Directories** field.



2. Add the RMS SDK 2.1 library directory to your Visual Studio 2010 project.

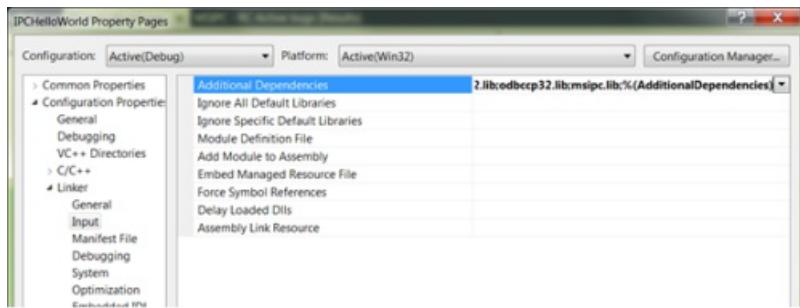
Under **Configuration Properties** select **VC++ Directories** and add the RMS SDK 2.1 library directory, to the **Library Directories** field for your platform.

- For Win32, use **\$(MSIPCSDKDIR)\lib**
- For x64, use **\$(MSIPCSDKDIR)\lib\x64**



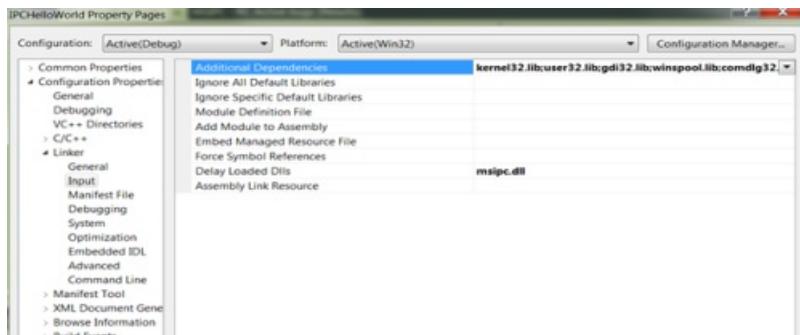
3. Add the RMS SDK 2.1 library files as Visual Studio 2010 dependencies.

Under **Linker**, select **Input** and add the RMS SDK 2.1 library files; **Msicpc.lib** and **Msicpc\_s.lib**, to the **Additional Dependencies** field.



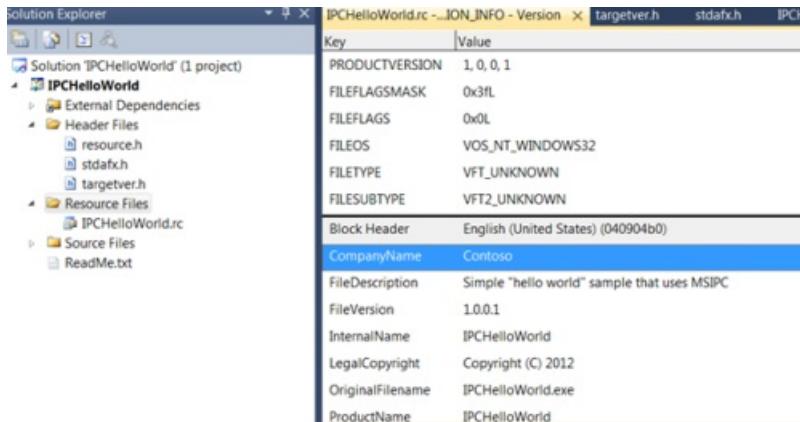
4. Add the RMS SDK 2.1 Dynamic Link Library (DLL) as a delay-loaded DLL.

Under **Linker**, select **Input**, and add the RMS SDK 2.1 DLL file, **Msicp.dll**, to the **Delay Loaded DLLs** field.



5. Create version information for your resulting binary.

Under **Solution Explorer** select **Resource Files** and add your binary name to the **OriginalFileName** field.



## Related topics

- [Install the SDK](#)

# Developing your application

5/8/2020 • 5 minutes to read • [Edit Online](#)

In this example you are going to build a simple console application that interacts with the Azure Information Protection service (AIP). It will take as input the path of a document to protect, then protect it with an ad-hoc policy or an Azure template. The application will then apply the correct policies according to the inputs, creating a information protected document. The sample code you will be using is [Azure IP test application](#) and is on Github.

## Sample app prerequisites

- **Operating System:** Windows 10, Windows 8, Windows 7, Windows Server 2008, Windows Server 2008 R2, or Windows Server 2012
- **Programming Language:** C# (.NET Framework 3.0 and above)
- **Development environment:** Visual Studio 2015 (and later)

## Setting up your Azure Configuration

Getting Azure set up for this app requires you to create a Tenant ID, a Symmetric Key, and an Application Principal ID.

### Azure AD Tenant configuration

To configure the Azure AD environment for Azure Information Protection, follow the guidance in [Activating the protection service from Azure Information Protection](#).

Once the service is activated you will need PowerShell components for the next steps. Follow [Administering protection from Azure Information Protection by using PowerShell](#) to accomplish this.

### Getting your Tenant ID

- As an administrator, run PowerShell.
- Import the RMS module: `Import-Module AIPService`
- Connect to the service with the assigned user credentials: `Connect-AipService -Verbose`
- Ensure RMS is enabled: `enable-aipservice`
- Get your tenant ID by running: `Get-AipServiceConfiguration`

Record the BPOSId (tenant ID) value. You will need it in future steps.

### Example output

```
PS C:\windows\system32> Get-AipServiceConfiguration
BPOSId : 86d2a9b2-d939-495b-9d40-cec2cc43ad59
RightsManagementServiceId : da48c84c-b62c-4652-b7f7-9189061a1c4f
LicensingIntranetDistributionPointUrl : https://da48c84c-b62c-4652-b7f7-9189061a1c4f.rms.na.aadrm.com/_wmcs/licensi
ng
LicensingExtranetDistributionPointUrl : https://da48c84c-b62c-4652-b7f7-9189061a1c4f.rms.na.aadrm.com/_wmcs/licensi
ng
CertificationIntranetDistributionPointUrl : https://da48c84c-b62c-4652-b7f7-9189061a1c4f.rms.na.aadrm.com/_wmcs/certifi
cation
CertificationExtranetDistributionPointUrl : https://da48c84c-b62c-4652-b7f7-9189061a1c4f.rms.na.aadrm.com/_wmcs/certifi
cation
```

- Disconnect from the service: `Disconnect-AipServiceService`

### Create a service Principal

Follow these steps to create a Service Principal:

A service principal is credentials configured globally for access control that allow a service to authenticate with Microsoft Azure AD and to protect information using Microsoft Azure AD Rights Management

- As an administrator, run PowerShell
- Import the Microsoft Azure AD module using: `Import-Module MSOnline`
- Connect to your online service with the assigned user credentials: `Connect-MsolService`
- Create a new service principal by running: `New-MsolServicePrincipal`
- Provide a name for your service principal

Record the symmetric key and application principal id for future use.

#### Example output

```
PS C:\windows\system32> New-MsolServicePrincipal
cmdlet New-MsolServicePrincipal at command pipeline position 1
Supply values for the following parameters:
DisplayName: examplePrincipal
The following symmetric key was created as one was not supplied [w3g+wcyclSmMD3szEKj+4xo/t1nnWwys3M8i8hf/M8IU=]

DisplayName : examplePrincipal
ServicePrincipalNames : {21049c0e-749b-47fc-bd1f-d8cd85a9fbc2}
ObjectId : 62a46635-65ec-44ea-8b54-61a2ab186c2f
AppPrincipalId : 21049c0e-749b-47fc-bd1f-d8cd85a9fbc2
TrustedForDelegation : False
AccountEnabled : True
Addresses : {}
KeyType : Symmetric
KeyId : 2d907cb3-928a-4f10-8f8c-0370c52df076
StartDate : 10/24/2016 8:56:21 PM
EndDate : 10/24/2017 8:56:21 PM
Usage : Verify
```

- Add your application principal id, symmetric key, and tenant ID to the application's App.config file.

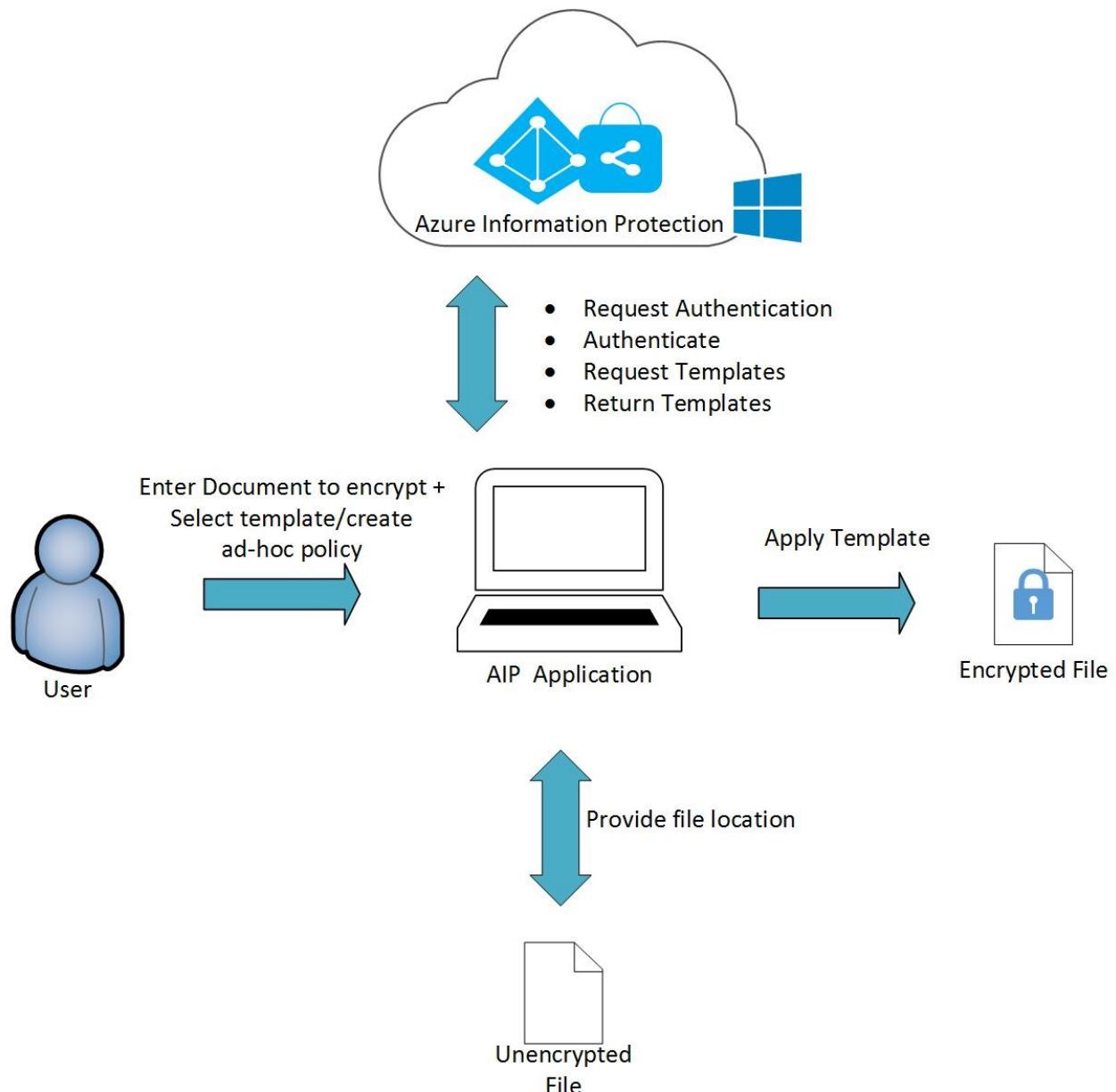
#### Example App.config file

```
<appSettings>
 <add key="ida:Tenant" value="XXXXXXXXXX" />
 <add key="ida:ClientId" value="XXXXXXXXXX" />
 <add key="ida:RedirectUri" value="XXXXXXXXXX" />
 <add key="ida:AADInstance" value="XXXXXXXXXX" />
 <add key="todo:TodoListBaseAddress" value="XXXXXXXXXX" />
 <add key="AppPrincipalId" value="21049c0e-749b-47fc-bd1f-d8cd85a9fbc2" />
 <add key="Base64Key" value="w3g+wcyclSmMD3szEKj+4xo/t1nnWwys3M8i8hf/M8IU=" />
 <add key="BposTenantId" value="86d2a9b2-d939-495b-9d40-cec2cc43ad59" />
</appSettings>
```

- The *ClientId* and *RedirectUri* will be available to you from when you registered your application in Azure. For more information on how to register your application in Azure and to acquire a *ClientId* and *RedirectUri* see, [Configure Azure RMS for ADAL authentication](#).

## Design summary

The following diagram depicts an architecture and process flow for the app you're creating, steps outlined below.



1. The user inputs:
  - The path of the file to be protected
  - Selects a template or creates an ad-hoc policy
2. The application requests authentication with AIP.
3. AIP confirms authentication
4. The application requests templates from the AIP.
5. AIP returns pre-defined templates.
6. The application locates the specified file with given location.
7. The application applies the AIP protection policy to the file.

## How the code works

In the sample, Azure IP Test, the solution begins up with the file `Iprotect.cs`. This is a C# console application and, like with any other AIP enabled application, you begin with loading the `MSIPC.dll` as shown in the `main()` method.

```
//Loads MSIPC.dll
SafeNativeMethods.IpcInitialize();
SafeNativeMethods.IpcSetAPIMode(APIMode.Server);
```

Load the parameters needed to connect to Azure

```
//Loads credentials for the service principal from App.Config
SymmetricKeyCredential symmetricKeyCred = new SymmetricKeyCredential();
symmetricKeyCred.AppPrincipalId = ConfigurationManager.AppSettings["AppPrincipalId"];
symmetricKeyCred.Base64Key = ConfigurationManager.AppSettings["Base64Key"];
symmetricKeyCred.BposTenantId = ConfigurationManager.AppSettings["BposTenantId"];
```

When you provide the file path in the console application, the application checks if the document is already encrypted. The method is of the **SafeFileApiNativeMethods** class.

```
var checkEncryptionStatus = SafeFileApiNativeMethods.IpcfIsFileEncrypted(filePath);
```

If the document is not encrypted, then it proceeds to encrypt the document with the selection provided on the prompt.

```
if (!checkEncryptionStatus.ToString().ToLower().Contains(alreadyEncrypted))
{
 if (method == EncryptionMethod1)
 {
 //Encrypt a file via AIP template
 ProtectWithTemplate(symmetricKeyCred, filePath);

 }
 else if (method == EncryptionMethod2)
 {
 //Encrypt a file using ad-hoc policy
 ProtectWithAdHocPolicy(symmetricKeyCred, filePath);
 }
}
```

The protect with template option proceeds to get the template list from the server and provides the user the option to select.

If you did not Modify templates then you will get default templates from AIP

```

public static void ProtectWithTemplate(SymmetricKeyCredential symmetricKeyCredential, string filePath)
{
 // Gets the available templates for this tenant
 Collection<TemplateInfo> templates = SafeNativeMethods.IpcGetTemplateList(null, false, true,
 false, true, null, null, symmetricKeyCredential);

 //Requests tenant template to use for encryption
 Console.WriteLine("Please select the template you would like to use to encrypt the file.");

 //Outputs templates available for selection
 int counter = 0;
 for (int i = 0; i < templates.Count; i++)
 {
 counter++;
 Console.WriteLine(counter + ". " + templates.ElementAt(i).Name + "\n" +
 templates.ElementAt(i).Description);
 }

 //Parses template selection
 string input = Console.ReadLine();
 int templateSelection;
 bool parseResult = Int32.TryParse(input, out templateSelection);

 //Returns error if no template selection is entered
 if (parseResult)
 {
 //Ensures template value entered is valid
 if (0 < templateSelection && templateSelection <= counter)
 {
 templateSelection -= templateSelection;

 // Encrypts the file using the selected template
 TemplateInfo selectedTemplateInfo = templates.ElementAt(templateSelection);

 string encryptedFilePath = SafeFileApiNativeMethods.IpcfEncryptFile(filePath,
 selectedTemplateInfo.TemplateId,
 SafeFileApiNativeMethods.EncryptFlags.IPCF_EF_FLAG_KEY_NO_PERSIST, true, false, true, null,
 symmetricKeyCredential);
 }
 }
}

```

If you select ad-hoc policy, the user of the application has to provide emails of the people that would have rights. In this section the license is created using the `IpcCreateLicenseFromScratch()` method and applying the new policy on the template.

```

if (issuerDisplayName.Trim() != "")
{
 // Gets the available issuers of rights policy templates.
 // The available issuers is a list of RMS servers that this user has already contacted.
 try
 {
 Collection<TemplateIssuer> templateIssuers = SafeNativeMethods.IpcGetTemplateIssuerList(
 null,
 true,
 false,
 false, true, null, symmetricKeyCredential);

 // Creates the policy and associates the chosen user rights with it
 SafeInformationProtectionLicenseHandle handle = SafeNativeMethods.IpcCreateLicenseFromScratch(
 templateIssuers.ElementAt(0));
 SafeNativeMethods.IpcSetLicenseOwner(handle, owner);
 SafeNativeMethods.IpcSetLicenseUserRightsList(handle, userRights);
 SafeNativeMethods.IpcSetLicenseDescriptor(handle, new TemplateInfo(null, CultureInfo.CurrentCulture,
 policyName,
 policyDescription,
 issuerDisplayName,
 false));

 //Encrypts the file using the ad hoc policy
 string encryptedFilePath = SafeFileApiNativeMethods.IpcfEncryptFile(
 filePath,
 handle,
 SafeFileApiNativeMethods.EncryptFlags.IPCF_EF_FLAG_KEY_NO_PERSIST,
 true,
 false,
 true,
 null,
 symmetricKeyCredential);
 }
}

```

## User interaction example

Once you get everything built and executing, the outputs of the application should look like the following:

1. You are prompted to select an encryption method.

```
Please select the desired encryption method (Enter 1 or 2)
1. Protect via Azure Template
2. Protect via Ad Hoc Policy
2
```

2. You are asked to provide the path to the file to be protected.

```
Please enter the path to the file to be encrypted.
C:\src\Test.docx
```

3. You are prompted to enter a license owner's email (this owner must have Global Administrator privileges on the Azure AD Tenant).

```
Please enter the license owner's email.
sampleowner@sampletenant.onmicrosoft.com
```

4. You enter email addresses of users who will have rights to access the file (emails must be separated by

spaces).

Please enter the email(s) of user(s) you would like to have rights to the file.

Separate emails with spaces.

sampleuser1@sampletenant.onmicrosoft.com sampleuser2@sampletenant.onmicrosoft.com

5. You select from a list of rights to be given to the authorized users.

Please select the rights you would like user(s) to have.  
Separate rights with spaces.

OWNER  
VIEW  
EDIT  
EXTRACT  
EXPORT  
PRINT  
COMMENT  
VIEWRIGHTSDATA  
EDITRIGHTSDATA  
FORWARD  
REPLY  
REPLYALL  
**VIEW EDIT**

6. Finally, you enter some policy metadata: policy name, description, and issuer (Azure AD Tenant) display name

Please enter a name for this license.  
**Example License**  
Please enter a description for this license.  
Gives authorized users VIEW and EDIT rights  
Please enter a display name for the license issuer.  
**Azure AD Tenant**

# Testing your application

5/8/2020 • 2 minutes to read • [Edit Online](#)

Here, you learn how to prepare for application testing.

## Instructions

You can test with either Azure RMS or an RMS server running on Windows Server. Begin testing with Azure RMS and test with RMS Server (if required for your deployment).

- For testing with Azure RMS, see [How-to: use ADAL authentication](#).
- For testing with RMS Server, see [How-to: install and configure an RMS server](#).
- To install the developer runtime:

You must have the Rights Management Service Client 2.1 installed on the computer on which you will be testing your application.

- To test your application on a computer other than your development computer, install the RMS Client 2.1 on that computer from the [AD RMS Client download page](#).
- Your development computer should have the Rights Management Services SDK 2.1, which was previously installed.

For help installing RMS SDK 2.1, see [Install the SDK](#).

## Remarks

This guidance is not comprehensive. To learn how to configure the RMS Client 2.1, see [RMS Client 2.1 Deployment Notes](#).

## Related topics

- [How-to install and configure an RMS server](#)
- [How-to: use ADAL authentication](#)
- [Install the SDK](#)
- [RMS Client 2.1 Deployment Notes](#)

# Deploy into production

5/8/2020 • 4 minutes to read • [Edit Online](#)

This topic guides you through the deployment process for your Azure Information Protection (AIP) / Rights Management Services (RMS) enabled application.

## Request an Information Protection Integration Agreement (IPIA)

Before you can release an application developed with AIP/RMS, you must apply for and complete a formal agreement with Microsoft.

### Begin the process

Obtain your IPIA by sending an email to [IPIA@microsoft.com](mailto:IPIA@microsoft.com) with the following information:

**Subject:** Requesting IPIA for *Company Name*

In the body of the email, include:

- Application and product name
- First and last name of the requester
- Email address of the requester

### Next steps

Upon receipt of your IPIA request, we will send you a form (as a Word document). Review the terms and conditions of the IPIA, and return the form to [IPIA@microsoft.com](mailto:IPIA@microsoft.com) with the following information:

- Legal name of the Company
- State/Province (US/Canada) or Country of Incorporation
- Company URL
- Email address of the contact person
- Additional addresses of the company (optional)
- Name of the Company Application
- Brief Description of the Application
- *Azure Tenant ID*
- *App ID* for the application
- Company contacts, email, and phone for Critical Situation Correspondence

### Completing the agreement

When we receive your form, we'll send you the final IPIA link to digitally sign. After your signing, it will be signed by the appropriate Microsoft representative, completing the agreement.

### Already have a signed IPIA?

If you already have a signed IPIA and want to add a new *App ID* for an application you are releasing, send an email to [IPIA@microsoft.com](mailto:IPIA@microsoft.com) and provide us with the following information:

- Name of the Company Application
- Brief Description of the Application
- Azure Tenant ID (even if it the same one as before)
- App ID for the application
- Company contacts, email, and phone for Critical Situation Correspondence

Upon the sending of the email, please allow up to 72 hours for an acknowledgement of the receipt.

## Deploying to the client environment

In order to deploy your application, built with Azure Information Protection (AIP) / Rights Management Services (RMS) tools, you will need to deploy the RMS Client 2.1 on the end-user's machine.

### RMS Client 2.1

The RMS Client 2.1 is designed to protect access to and usage of information flowing through AIP/RMS enabled applications, whether installed on your premises or in a Microsoft datacenter.

The RMS Client 2.1 is not a Windows operating system component. The client ships as an optional download which can be, with acknowledgment and acceptance of its license agreement, freely distributed with your application.

#### IMPORTANT

The RMS Client 2.1 is architecture specific and must match the architecture of your target operating system.

## RMS Client 2.1 installation options

### Creating your deployment package

We recommend that you bundle the RMS Client installer package with your application or solution using your preferred installation technology. The RMS Client can be freely redistributed with other applications and solutions.

You can choose to install the RMS Client 2.1 interactively by starting the RMS Client 2.1 installer or silently installing it. The integration steps will be:

- Download RMS Client 2.1 installer
- Integrate the RMS Client 2.1 installer to run with your application installer

An example of integrating the RMS Client 2.1 with your application is the [Rights Protected Folder Explorer](#) package. Try installing it yourself to understand the approach.

### Make RMS Client 2.1 a pre-requisite for your application install

In this case, you will create a pre-requisite such that your application install will fail if RMS Client 2.1 is not present on the end-user machine.

If the client is not present, provide an error message informing the user where they can download a copy of the RMS Client 2.1.

If the client is present, proceed with your application installation.

## Enabling Azure Information Protection Services with your application

#### NOTE

If you have migrated to the new ADAL model for authentication, you don't have to install SIA. For more information, see [ADAL authentication for your RMS enabled application](#). Also, you can [Certify your application for Windows 10](#) - By updating your application to use ADAL authentication rather than the Microsoft Online Sign-in Assistant, you and your customers will be able to: Utilize multi-factor authentication Install the RMS Client 2.1 without requiring administrative privileges to the machine

In order for your end-user to take advantage of Information Protection services, you must deploy the *Online*

*Services Sign-in Assistant (SIA)*. As the application developer, you do not know whether the end-user will use Information Protection through RMS (on premises) or through Azure Information Protection.

#### **IMPORTANT**

If you will be running your client application with Azure based RMS, you'll need to create your own tenants. For more information, see [Azure RMS requirements: Cloud subscriptions that support Azure RMS](#). For more information on running with Azure RMS see, [Enable your service application to work with cloud based RMS](#).

- Download the [Microsoft Online Services Sign-In Assistant](#) from the Microsoft Download Center.
- Ensure that your deployment of a rights-enabled application includes a pre-requisites check for this service selection.
- For your own testing and for your end-users use of the on-line service see the TechNet topic, [Configuring Rights Management](#).

You will also need to use this guide to configure your app - [How to configure your App Service application to use Azure Active Directory login](#).

For more on enabling your application to use RMS for Azure Rights Management services see, [Enable your application to work with cloud based RMS](#).

## Related topics

- [Microsoft Online Services Sign-In Assistant](#)
- [Configuring Rights Management](#)
- [Enable your application to work with cloud based RMS](#)

# Developer guidance

5/8/2020 • 2 minutes to read • [Edit Online](#)

This section covers specific guidance for several important development scenarios as well as general information about developing with this SDK. The scenarios in this section are specific to this release of the Rights Management Services SDK 2.1 and may be altered in subsequent releases.

- [How-to: use ADAL authentication](#) - Authentication with Azure RMS for your app using Azure Active Directory Authentication Library (ADAL).
- [How-to: Add explicit owner rights](#) - Your application should explicitly add "Owner" rights when creating a license from scratch (`IpcCreateLicenseFromScratch`).
- [How-to: debug a rights-enabled application](#) - This topic shows how to debug your application and use the Windows Event Log.
- [How-to: deploy an app into a customer's tenant](#) - Outlines the steps for deploying an app from its development Azure AD tenant to a production Azure AD tenant.
- [How-to: enable document tracking and revocation](#) - This topic covers the basic guidance for implementing document tracking of content as well as example code for metadata updates and for creating a **Track Usage** button for your app.
- [How-to: enable email notification](#) - Email notification allows for a protected content owner to be notified when his or her content is accessed.
- [How-to: enable your service application to work with cloud based RMS](#) - This topic outlines steps for setting up your service application to use Azure Rights Management.
- [How-to: install and configure an RMS server](#) - This topic covers the steps to connect to an RMS Server or Azure RMS for testing your rights-enabled application.
- [How-to: set the API security mode](#) - You can choose which security mode your File API application runs in by using the `IpcSetGlobalProperty` function.
- [How-to: work with encryption settings](#) - This topic orients you to our encryption packages and shows some code snips for their use.
- [Application types](#) - This topic covers types of applications that you might choose to create as rights-enabled.
- [File API configuration](#) - The File API's behavior can be configured through settings in the registry.
- [Security guidelines](#) - provides orientation and direction to application developers for working well within the AIP ecosystem.
- [Supported file formats](#) - The File API supports native and Pfile formats
- [Supported platforms](#) - This topic identifies the RMS SDK 2.1 supported client and server platforms.
- [Understanding usage restrictions](#) - All RMS enabled applications must enforce usage restrictions which are defined by the constants listed in this topic.

## Related topics

- [Overview](#)

# How-to: use ADAL authentication

5/8/2020 • 2 minutes to read • [Edit Online](#)

Authentication with Azure RMS for your app using Azure Active Directory Authentication Library (ADAL).

By updating your application to use ADAL authentication rather than the Microsoft Online Sign-in Assistant, you and your customers will be able to:

- Utilize multi-factor authentication
- Install the RMS 2.1 client without requiring administrative privileges to the machine
- Certify your application for Windows 10

## Two approaches to authentication

This topic contains two approaches to authentication with corresponding code examples.

- **Internal authentication** - OAuth authentication managed by the RMS SDK.

Use this approach if you want the RMS client to display an ADAL authentication prompt when authentication is necessary. For details on how to configure your application, see the section, "Internal authentication".

### NOTE

If your application currently uses AD RMS SDK 2.1 with the sign-in assistant, we recommend that you use the internal authentication method as your application migration path.

- **External authentication** - OAuth authentication managed by your application.

Use this approach if you want your application to manage its own OAuth authentication. With this approach, the RMS client will exercise an application defined callback when authentication is necessary. For a detailed example, see "External authentication" at the end of this topic.

### NOTE

External authentication does not imply the ability to change users; the RMS client always uses the default user for a given RMS tenant.

## Internal authentication

1. Follow the Azure configuration steps in [Configure Azure RMS for ADAL authentication](#) then return to the following app initialization step.
2. You are now ready to configure your application to use the internal ADAL authentication provided by the RMS SDK 2.1.

To configure your RMS client, add a call to [IpcSetGlobalProperty](#) right after calling [IpcInitialize](#) to configure the RMS client. Use the following code snippet as an example.

```

C++
IpcInitialize();

IPC_AAD_APPLICATION_ID applicationId = { 0 };
applicationId.cbSize = sizeof(IPC_AAD_APPLICATION_ID);
applicationId.wszClientId = L"GUID-provided-by-AAD-for-your-app-(no-brackets)";
applicationId.wszRedirectUri = L"RedirectionUriWeProvidedAADForOurApp://authorize";
HRESULT hr = IpcSetGlobalProperty(IPC_EI_APPLICATION_ID, &applicationId);
if (FAILED(hr)) {
 //Handle the error
}

```

## External Authentication

Use this code as an example of how to manage your own authentication tokens. C++ extern HRESULT  
GetADALToken(LPVOID pContext, const IPC\_NAME\_VALUE\_LIST& Parameters, \_\_out wstring wstrToken) throw();

```

HRESULT GetLicenseKey(PCIPC_BUFFER pvLicense, __in LPVOID pContextForAdal, __out IPC_KEY_HANDLE &hKey)
{
 IPC_OAUTH2_CALLBACK pfGetADALToken =
 [] (LPVOID pvContext, PIPC_NAME_VALUE_LIST pParameters, IPC_AUTH_TOKEN_HANDLE* phAuthToken) -> HRESULT
 {
 wstring wstrToken;
 HRESULT hr = GetADALToken(pvContext, *pParameters, wstrToken);
 return SUCCEEDED(hr) ? IpcCreateOAuth2Token(wstrToken.c_str(), OUT phAuthToken) : hr;
 };

 IPC_OAUTH2_CALLBACK_INFO callbackCredentialContext =
 {
 sizeof(IPC_OAUTH2_CALLBACK_INFO),
 pfGetADALToken,
 pContextForAdal
 };

 IPC_CREDENTIAL credentialContext =
 {
 IPC_CREDENTIAL_TYPE_OAUTH2,
 NULL
 };
 credentialContext.pcOAuth2 = &callbackCredentialContext;

 IPC_PROMPT_CTX promptContext =
 {
 sizeof(IPC_PROMPT_CTX),
 NULL,
 IPC_PROMPT_FLAG_SILENT | IPC_PROMPT_FLAG_HAS_USER_CONSENT,
 NULL,
 &credentialContext
 };

 hKey = 0L;
 return IpcGetKey(pvLicense, 0, &promptContext, NULL, &hKey);
}

```

## Related topics

- [Data types](#)
- [Environment properties](#)
- [IpcCreateOAuth2Token](#)
- [IpcGetKey](#)

- [IpcInitialize](#)
- [IPC\\_CREDENTIAL](#)
- [IPC\\_NAME\\_VALUE\\_LIST](#)
- [IPC\\_OAUTH2\\_CALLBACK\\_INFO](#)
- [IPC\\_PROMPT\\_CTX](#)
- [IPC\\_AAD\\_APPLICATION\\_ID](#)

# Configure your app for ADAL authentication

5/8/2020 • 2 minutes to read • [Edit Online](#)

This topic describes the steps for configuring your app for Azure Active Directory Authentication Library (ADAL) based authentication.

## Azure authentication setup

You will need the following:

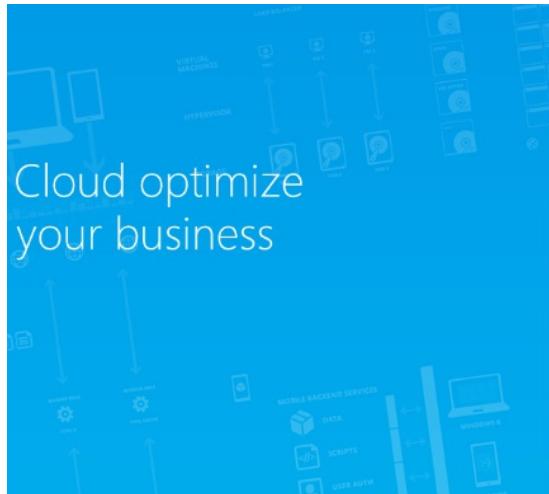
- A [subscription for Microsoft Azure](#) (a free trial is sufficient). For more information, see [How users sign up for RMS for individuals](#)
- A subscription for Microsoft Azure Rights Management (a free [RMS for Individuals](#) account is sufficient).

### NOTE

Ask your IT Admin whether or not you have a subscription for Microsoft Azure Rights Management and, have your IT Admin perform the steps below. If your organization does not have a subscription, you should have your IT admin create one. Also, your IT Admin should subscribe with a *Work or school account*, rather than a *Microsoft account* (i.e. Hotmail).

After signing up for Microsoft Azure:

- Login to the [Azure Management Portal](#) for your organization using an account with administrative privileges.



### Microsoft Azure

Type the email address or phone number of the account you want to sign in with.

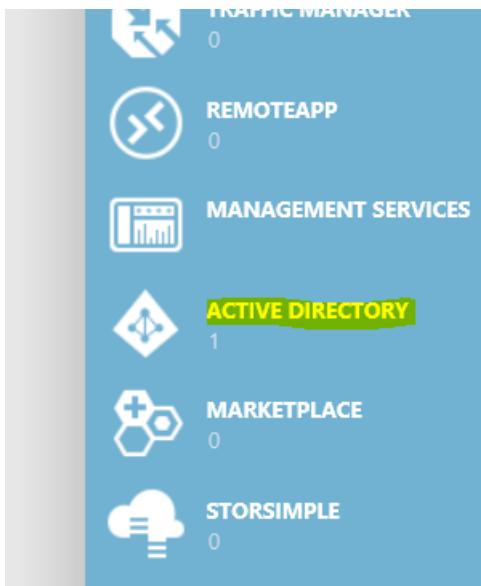
[Continue](#)

© 2016 Microsoft

[Terms of use](#) [Privacy & Cookies](#)



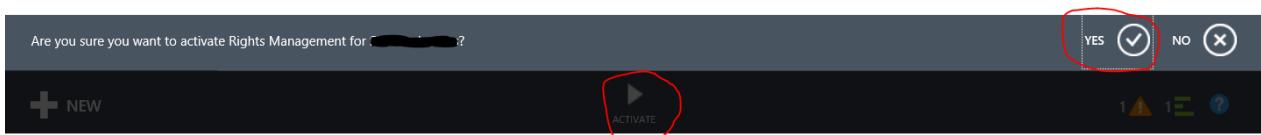
- Browse down to the **Active Directory** application on the left side of the portal.



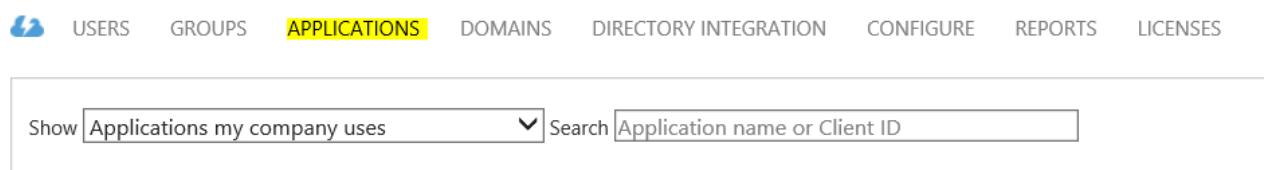
- If you haven't created a directory already, choose the **New** button located in the bottom left corner of the portal.



- Select the **Rights Management** tab and ensure that the **Rights Management Status** is either **Active**, **Unknown** or **Unauthorized**. If the status is **Inactive**, choose the **Activate** button at the bottom, center portion of the portal and confirm your selection.



- Now, create a new *Native Application* in your directory by selecting your directory, choosing Applications.



- Then choose the **Add** button located in the bottom, center portion of the portal.



- At the prompt choose **Add an application my organization is developing**.

# What do you want to do?

④ Add an application my organization is developing

④ Add an application from the gallery

- Name your application by selecting **NATIVE CLIENT APPLICATION** and choosing the **Next** button.

ADD APPLICATION ×

Tell us about your application

NAME

my app x

Type

WEB APPLICATION AND/OR WEB API ?  
 NATIVE CLIENT APPLICATION ?



- Add a redirection URI and choose next. The redirection URI needs to be a valid URI and unique to your directory. For example, you could use something like `https://contoso.azurewebsites.net/.auth/login/done`.

ADD APPLICATION

## Application information

**REDIRECT URI**

The URI to which Microsoft Azure AD will redirect in response to an OAuth 2.0 request. The value does not need to be a physical endpoint, but must be a valid URI.

[Learn more](#)

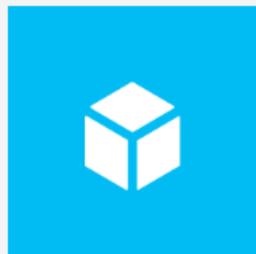
1

← ✓

- Select your application in the directory and choose **CONFIGURE**.

my app

 DASHBOARD **CONFIGURE**



Your native

Integrate you

Skip Quick Start

**NOTE**

Copy the **CLIENT ID** and **REDIRECT URI** and store them for future use when configuring the RMS client.

- Browse to the bottom of your application settings and choose the **Add application** button under **permissions to other applications**.

**NOTE**

The **Delegated Permissions** that are shown for Windows Azure Active Directory are correct by default – only one option should be selected and that option is **Sign in and read user profile**.

permissions to other applications



Windows Azure Active Directory      Delegated Permissions: 1

Add application

- Choose the plus button next to **Microsoft Rights Management**.

## Permissions to other applications

SHOW	All Apps	STARTING WITH	Delegated Permissions	Selected
NAME	APPLICATION PERMISSIONS	DELEGATED PERMISSIONS	P	
Microsoft Rights Manage...	(+)	1		None

- Now, choose the check mark located on the bottom left corner of the dialog.

## Permissions to other applications

SHOW	Microsoft Apps	Delegated Permissions	Selected
NAME	APPLICATION ...	DELEGATED PERMISSIONS	P
Microsoft Graph	18	40	
Microsoft Intune API	3	0	
Microsoft Rights Management Services	(+)	1	Microsoft Rights Management Serv
Office 365 Exchange Online	9	30	
Office 365 Management APIs	7	7	
Office 365 SharePoint Online	8	11	
Power BI Service	0	9	
Skype for Business Online	4	5	
Windows Azure Active Directory	(+)	8	
Windows Azure Service Management API	0	1	

- You're now ready to add a dependency to your application for Azure RMS. To add the dependency, select the new **Microsoft Rights Management Services** entry under permissions to other applications and choose the **Create and access protected content for users** checkbox under the Delegated Permissions: drop box.

permissions to other applications



Windows Azure Active Directory      Delegated Permissions: 1

Microsoft Rights Management Services      Delegated Permissions: 1

Create and access protected content for users

Add application

- Save your application to persist the changes by choosing the **Save** icon located on the bottom, center of the portal.

permissions to other applications



Windows Azure Active Directory      Delegated Permissions: 1

Microsoft Rights Management Services      Delegated Permissions: 1

Create and access protected content for users

Add application



# How-to: add explicit owner rights

8/5/2019 • 2 minutes to read • [Edit Online](#)

Your application should explicitly add "Owner" rights when creating a license from scratch using [IpcCreateLicenseFromScratch](#).

## Prerequisites

When your application is creating a license handle using [IpcCreateLicenseFromScratch](#), it must also grant the owner full rights (permissions) explicitly.

### NOTE

Setting a user as "owner" using [IpcSetLicenseProperty](#) with the IPC\_LI\_OWNER property does not grant the owner full permissions.

The following example code only represents the steps involved in creating and adding the specific rights to a given license.

## Instructions

### Step 1: Example scenario

In this example, needed rights are added to a license created with [IpcCreateLicenseFromScratch](#). The example shows the creation and assignment of the rights to the license through a rights list.

The following two rights are added to these users:

- *Read* permissions assigned to joe@contoso.com
- *Full* permissions assigned to mary\_kay@contoso.com

```

// Create User Rights structure
IPC_USER_RIGHTS ownerRightForOwner = {0};

// Create rights
LPCWSTR rgwszOwnerRights[1] = {IPC_GENERIC_ALL};

// Assign values to members of Rights structure
ownerRightForOwner.User.dwType = IPC_USER_TYPE_IPC;
ownerRightForOwner.User.wszID = IPC_USER_ID_OWNER;
ownerRightForOwner.rgwszRights = rgwszOwnerRights;
ownerRightForOwner.cRights = 1;

// Create User Rights structure for Joe with Read permissions
IPC_USER_RIGHTS joeReadRight = {0};
LPCWSTR rgwszReadRights[1] = {IPC_GENERIC_READ};

// Assign values to members of Rights structure for Joe
joeReadRight.User.dwType = IPC_USER_TYPE_EMAIL;
joeReadRight.User.wszID = "joe@contoso.com";
joeReadRight.rgwszRights = rgwszReadRights;
joeReadRight.cRights = 1;

// Create User Rights structure for Mary Kay with Full permissions
IPC_USER_RIGHTS mary_kayFullRight = {0};
LPCWSTR rgwszFullRights[1] = {IPC_GENERIC_ALL};

// Assign values to members of Rights structure for Mary Kay
mary_kayFullRight.User.dwType = IPC_USER_TYPE_EMAIL;
mary_kayFullRight.User.wszID = L"mary_kay@contoso.com";
mary_kayFullRight.rgwszRights = rgwszFullRights;
mary_kayFullRight.cRights = 1;

// Create User Rights List and assign the above rights
size_t uNoOfUserRights = 3;
PIPC_USER_RIGHTS_LIST pUserRightsList = NULL;
pUserRightsList = reinterpret_cast<PIPC_USER_RIGHTS_LIST>
(new BYTE[sizeof(IPC_USER_RIGHTS_LIST) + uNoOfUserRights * sizeof(IPC_USER_RIGHTS)]);

if(pUserRightsList == NULL)
{
 // Handle error
}

// Assign values to members of Rights List structure for Joe and Mary Kay
(*pUserRightsList).cbSize = sizeof(IPC_USER_RIGHTS_LIST);
(*pUserRightsList).cUserRights = uNoOfUserRights;
(*pUserRightsList).rgUserRights[0] = ownerRightForOwner;
(*pUserRightsList).rgUserRights[1] = joeReadRight;
(*pUserRightsList).rgUserRights[2] = mary_kayFullRight;

// Set the Rights List property on the license via its handle
// hLicense is a license handle created with IpcCreateLicenseFromScratch
hr = IpcSetLicenseProperty(hLicense, FALSE, IPC_LI_USER_RIGHTS_LIST, pUserRightsList);

if(FAILED(hr))
{
 // Handle the error
}

```

## Related topics

- [Developer notes](#)
- [IpcSetLicenseProperty](#)
- [IpcCreateLicenseFromScratch](#)



# How-to: debug a rights-enabled application

8/5/2019 • 2 minutes to read • [Edit Online](#)

The following topic shows how to debug your application and use the Windows Event Log.

## Debugging your application

In Rights Management Services SDK 2.1, the anti-debugging checks in the developer version of our runtime are disabled.

You can turn on debug tracing by using the following registry key. (To turn debug tracing off, change the value to 0.) Nothing else is required for debugging in this release.

```
HKEY_LOCAL_MACHINE
 SOFTWARE
 Microsoft
 MSIPC
 "Trace" = 00000001
 Data type
 dword
```

## Application logging by using the Windows Event Log

The name of the event log is "Microsoft-RMS-MSIPC/Debug". This means that in the Windows Event Viewer, your log appears as "Application and Services Logs\Microsoft\RMS\MSIPC\Debug".

**Note** The log is enabled by default and set to verbosity level 3.

To change the settings of the logging feature, you can use either the UI for the Windows Event Viewer or Wevtutil, a command line tool built into Windows.

Through the Wevtutil interface, you can control the level of verbosity of your log.

At this time, we support 3 levels of logging:

- Level 2—Error
- Level 3—Warning
- Level 4—Information

For example, the following command will enable the MSIPC event log and set the level of verbosity to information.

```
wevtutil sl Microsoft-RMS-MSIPC/Debug /e:true /l:4
```

**Note** In the Windows Event Viewer on the **View** menu, select **Show Analytic and Debug Logs** to make the MSIPC Debug log visible.

# Deploying a service application into a different tenant

8/5/2019 • 2 minutes to read • [Edit Online](#)

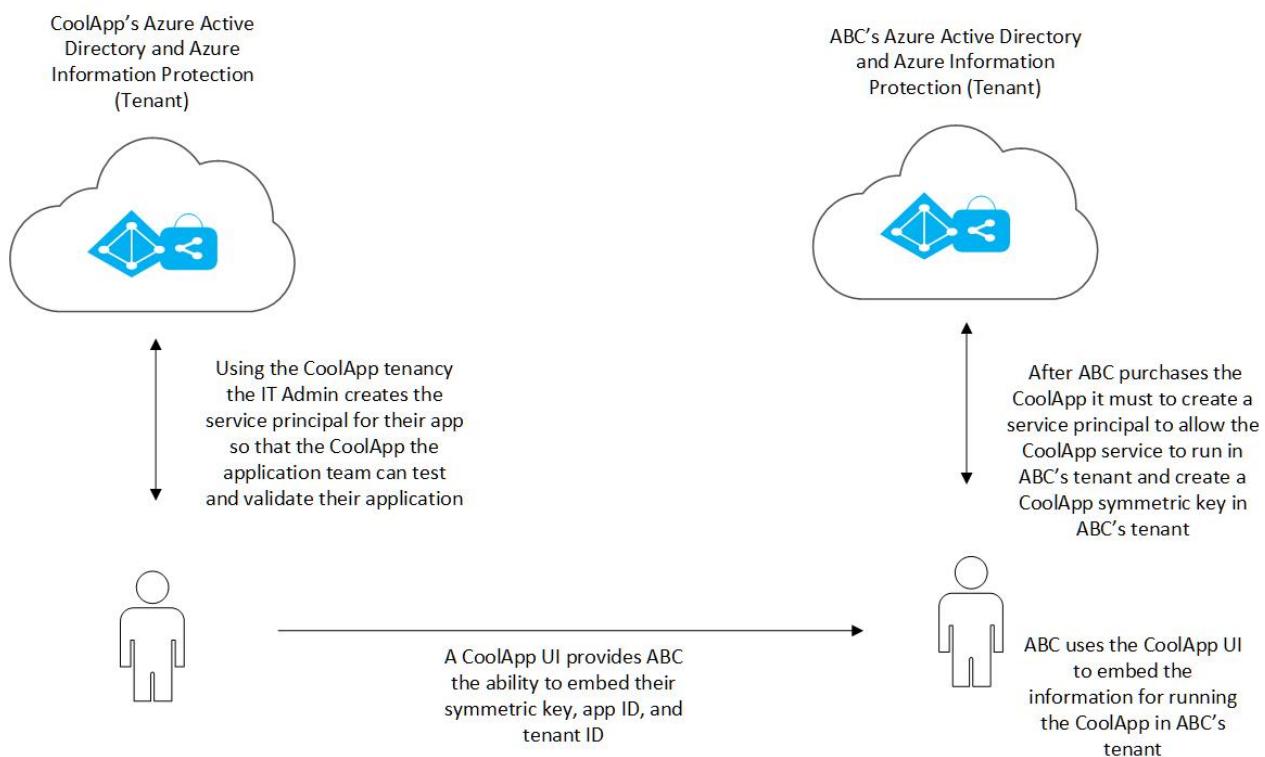
This article describes the process of deploying a service application. In this scenario we are transitioning the application from being registered with its initial development AD tenant to being registered with a different company's production AD tenant.

## NOTE

This scenario is only relevant if the service application uses symmetric key authentication.

## Scenario

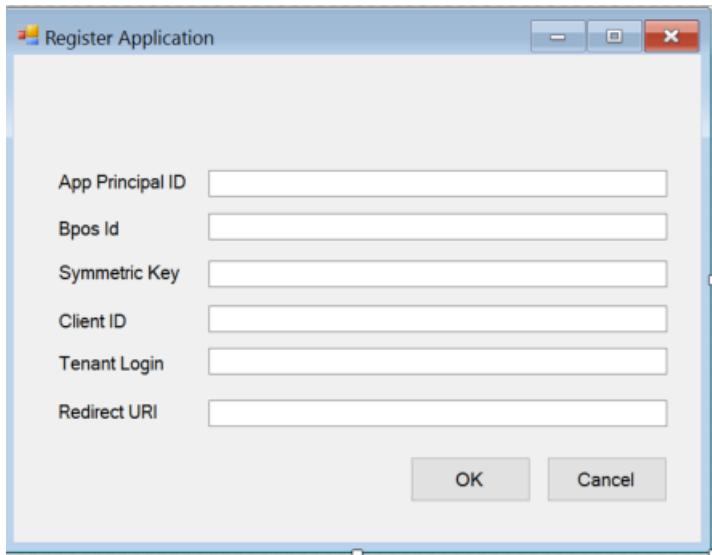
Company *CoolApp* has developed a service application using Azure Information Protection (AIP) that encrypts, labels, and, protects documents when users are exporting from a business application such as Dynamics, SAP, or, Salesforce. For this scenario, large enterprise *ABC* buys *CoolApp*'s new application so, the *CoolApp* team needs to deploy their solution into *ABC*'s environment.



## Flow 1: *CoolApp* provides a UI dialog to *ABC* to implement the deployment

Once *ABC* purchases *CoolApp*'s solution, the IT administrator at *ABC* must create the *CoolApp* service principal and register the application in *ABC*'s Azure AD tenant.

The steps for this are outlined in the [Create a service Principal](#) section of [Developing your application](#).



#### NOTE

To create Service Principal in a tenant you need tenant admin rights

ABC's IT administrator then launches *CoolApp*'s application as a service in their environment and embeds the details for the *CoolApp* application to work such as; application ID, tenant ID, and, the symmetric key.

If the desired experience is to not provide the IT administrator of ABC with a UI dialog for the service principal information, then **Flow 2** is the method to follow.

## Flow 2: ABC IT Administrator provides the key to the *CoolApp* team

Once ABC's IT Administrator creates the service principal, as shown in **Figure 1**, ABC provides the information to the *CoolApp* team. The *CoolApp* team then proceeds to embed the information in the *CoolApp* application for use in ABC's tenant.

# How-to: enable document tracking and revocation

8/5/2019 • 2 minutes to read • [Edit Online](#)

This topic covers the basic guidance for implementing document tracking of content as well as example code for metadata updates and for creating a **Track Usage button** for your app.

## Steps to implement document tracking

Steps 1 and 2 enable the document to be tracked. Step 3 enables your app users to reach the document tracking site in order to track and revoke your protected documents.

1. Add document tracking metadata
2. Register the document with the RMS service
3. Add Track Usage button to your app

The implementation details for these steps follow.

### 1. Add document tracking metadata

Document tracking is a feature of the Rights Management system. By adding specific metadata during the document protection process, a document can be registered with the tracking service portal which then provides several options for tracking.

Use these APIs to add/update a content license with document tracking metadata.

Operationally, only the **content name** and the **notification type** properties are required for document tracking.

- [IpcCreateLicenseMetadataHandle](#)
- [IpcSetLicenseMetadataProperty](#)

We expect that you will set all of the metadata properties. Here they are, listed by type.

For more information, see [License metadata property types](#).

- **IPC\_MD\_CONTENT\_PATH**

Use to identify the tracked document. In cases where a full path is not possible, just provide the file name.

- **IPC\_MD\_CONTENT\_NAME**

Use to identify the tracked document name.

- **IPC\_MD\_NOTIFICATION\_TYPE**

Use to specify when notification will be sent. For more information, see [Notification type](#).

- **IPC\_MD\_NOTIFICATION\_PREFERENCE**

Use to specify the type of notification. For more information, see [Notification preference](#).

- **IPC\_MD\_DATE\_MODIFIED**

We suggest that you set this date each time the user clicks Save.

- **IPC\_MD\_DATE\_CREATED**

Use to set the origination date of the file

- [IpcSerializeLicenseWithMetadata](#)

Use the appropriate one of these APIs to add the metadata to your file or stream.

- [IpcfEncryptFileWithMetadata](#)
- [IpcfEncryptFileStreamWithMetadata](#)

Lastly, use this API to register your tracked document with the tracking system.

- [IpcRegisterLicense](#)

## 2. Register the document with the RMS service

Here's a code snippet showing an example of setting document tracking metadata and the call to register with the tracking system.

```
C++
HRESULT hr = S_OK;
LPCWSTR wszOutputFile = NULL;
wstring wszWorkingFile;
IPC_LICENSE_METADATA md = {0};

md.cbSize = sizeof(IPC_LICENSE_METADATA);
md.dwNotificationType = IPCD_CT_NOTIFICATION_TYPE_ENABLED;
md.dwNotificationPreference = IPCD_CT_NOTIFICATION_PREF_DIGEST;
//file origination date, current time for this example
md.ftDateCreated = GetCurrentTime();
md.ftDateModified = GetCurrentTime();

LOGSTATUS_EX(L"Encrypt file with official template...");

hr = IpcfEncryptFileWithMetadata(wszWorkingFile.c_str(),
 m_wszTestTemplateID.c_str(),
 IPCF_EF_TEMPLATE_ID,
 0,
 NULL,
 NULL,
 &md,
 &wszOutputFile);

/* This will contain the serialized license */
PIPC_BUFFER pSerializedLicense;

/* the context to use for the call */
PCIPC_PROMPT_CTX pContext;

wstring wstrContentName("MyDocument.txt");
bool sendLicenseRegistrationNotificationEmail = FALSE;

hr = IpcRegisterLicense(pSerializedLicense,
 0,
 pContext,
 wstrContentName.c_str(),
 sendLicenseRegistrationNotificationEmail);
```

## Add a Track Usage button to your app

Adding a **Track Usage** UI item to your app is as simple as using one of the following URL formats:

- Using Content ID

- Get the content ID by using [IpcGetLicenseProperty](#) or [IpcGetSerializedLicenseProperty](#) if the license is serialized and use the license property **IPC\_LI\_CONTENT\_ID**. For more information, see [License property types](#).
- With the **ContentId** and **Issuer** metadata, use the following format:

<https://track.azurerms.com/#/{ContentId}/{Issuer}>

Example -

<https://track.azurerms.com/#/summary/05405df5-8ad6-4905-9f15-fc2ecbd8d0f7/janedoe@microsoft.com>
- If you don't have access to that metadata (i.e. you are examining the unprotected version of the document), you can use the **Content\_Name** in the following format: 

<https://track.azurerms.com/#/?q={ContentName}>

Example - <https://track.azurerms.com/#/?q=Secret!.txt>

The client simply needs to open a browser with the appropriate URL. The RMS Document Tracking portal will handle authentication and any required redirection.

## Related topics

- [License metadata property types](#)
- [Notification preference](#)
- [Notification type](#)
- [IpcCreateLicenseMetadataHandle](#)
- [IpcSetLicenseMetadataProperty](#)
- [IpcSerializeLicenseWithMetadata](#)
- [IpcfEncryptFileWithMetadata](#)
- [IpcfEncryptFileStreamWithMetadata](#)
- [IpcRegisterLicense](#)

# How-to: enable email notification

8/5/2019 • 2 minutes to read • [Edit Online](#)

Email notification allows for a protected content owner to be notified when his or her content is accessed.

To setup your email notification for a given license, use [IpcSetLicenseProperty](#) with the property type parameter, *dwPropID*, as [IPC\\_LI\\_APP\\_SPECIFIC\\_DATA](#) and the application data fields formatted as an [IPC\\_NAME\\_VALUE\\_LIST](#).

C++

```
int numDataPairs = 3;

IPC_NAME_VALUE propertyValuePairs [numDataPairs];

// lcid field set to 0 causes the default lcid to be used

propertyValuePairs[0] = {"MS.Content.Name", 0, "FinancialReport.docx"};
propertyValuePairs[1] = {"MS.Notify.Enabled",0 , "true"};
propertyValuePairs[2] = {"MS.Notify.Culture",0 , "en-US"};

IPC_NAME_VALUE_LIST emailNotificationAppData = {numDataPairs, propertyValuePairs};

result = IpcSetLicenseProperty(licenseHandle, FALSE, IPC_LI_APP_SPECIFIC_DATA, emailNotificationAppData);
```

The following table contains the application data fields, property name and value pairs, for RMS email notification.

PROPERTY NAME	DATA TYPE	EXAMPLE VALUE	NOTES
MS.Content.Name	string	"FinancialReport.docx"	This is an identifier associated with the protected content.  For protected files this value should be the name of the file without any path information.  For other types of content such as an email message it might be the subject of the email or it might be empty.
MS.Notify.Enabled	string	"true"   "false"	If this value is set to "true" a notification email will be sent to the owner of the publishing license when someone attempts to use it to obtain an end user license.

PROPERTY NAME	DATA TYPE	EXAMPLE VALUE	NOTES
MS.Notify.Culture	string	"en-US"	<p><b>Source:</b> System.Globalization.CultureInfo.CurrentUICulture.Name</p> <p>This value is used to determine the localized language of the notification email and the date/time and number formatting that should be used in the email message.</p> <p>It should be set based on user settings of the machine that the publish license is created on, or based on the preferred culture of the owner of the publish license.</p>
MS.Notify.TZID	string	"Pacific Standard Time"	<p><b>Source:</b> TimeZoneInfo.Local.Id - Windows time zone ID.</p> <p>This value is the Microsoft Windows OS time zone identifier describing a particular time zone and its characteristics.</p>

PROPERTY NAME	DATA TYPE	EXAMPLE VALUE	NOTES
MS.Notify.TZO	string	"-480"	<p>This is the publish license owner's time zone offset in terms of minutes from UTC time.</p> <p>If a valid TZID value is provided the offset of the time zone specified by it will be used and this value will be ignored.</p> <p>This value will more than likely be used by non-windows based publishing platforms that do not have access to the list of Windows OS time zone ID values.</p> <p>If a TZID value is not provided this value will be used to calculate the time offset in notification messages, and the TZSN will be used (regardless of the time zone value) to indicate the name of the time zone. This will result time zone being fixed and not updating for daylight savings when it is applicable.</p> <p>For example:</p> <p>If TXID is blank and TZ0 is set to "-420" and the TZSN is set to "Pacific Daylight Time" all values shown in the notification email will be adjusted to "Pacific Daylight Time" and displayed as such even if daylight savings is no longer in affect currently.</p> <p>On the other hand if a TZID is supplied along with both TZSN and TZDN, then the times specified in the notification email will be adjusted and displayed based on whether the date and time should be displayed in Daylight mode or Standard mode.</p>

PROPERTY NAME	DATA TYPE	EXAMPLE VALUE	NOTES
MS.Notify.TZSN	string	"Pacific Standard Time"	<p><b>Source:</b> TimeZoneInfo.Local.StandardName - Standard Time Zone name.</p> <p>This should be the localized name of the time zone's standard time zone name.</p>
MS.Notify.TZDN	string	"Pacific Daylight Time"	<p><b>Source:</b> TimeZoneInfo.Local.DaylightName - Daylight Time Zone name.</p> <p>This should be the localized name of the time zone's daylight savings name. It can be the same as the standard name if the time zone does not support daylight savings.</p>

## Related topics

- [IpcSetLicenseProperty](#)
- [IPC\\_LI\\_APP\\_SPECIFIC\\_DATA](#)
- [IPC\\_NAME\\_VALUE\\_LIST](#).

# How-to: enable your service application to work with cloud based RMS

3/17/2020 • 3 minutes to read • [Edit Online](#)

## IMPORTANT

Versions of the Microsoft Rights Management Service SDK released prior to March 2020 are deprecated; applications using earlier versions must be updated to use the March 2020 release. For full details, see the [deprecation notice](#).

No further enhancements are planned for the Microsoft Rights Management Service SDK. We strongly recommend adoption of the [Microsoft Information Protection SDK](#) for classification, labeling, and protection services.

This topic outlines steps for setting up your service application to use Azure Rights Management. For more information, see [Getting started with Azure Rights Management](#).

### Important

In order to use your Rights Management Services SDK 2.1 service application with Azure RMS, you'll need to create your own tenants. For more information, see [Azure RMS requirements: Cloud subscriptions that support Azure RMS](#)

## Prerequisites

- RMS SDK 2.1 must be installed and configured. For more information, see [Getting started with RMS SDK 2.1](#).
- You must [create a service identity via ACS](#) by using the symmetric key option, or through other means, and record the key information from that process.

## Connecting to the Azure Rights Management Service

- Call [IpcInitialize](#).
- Set [IpcSetGlobalProperty](#).

```
C++
int mode = IPC_API_MODE_SERVER;
IpcSetGlobalProperty(IPC_EI_API_MODE, &(mode));
```

**Note** For more information, see [Setting the API security mode](#)

- The following steps are the setup for creating an instance of an [IPC\\_PROMPT\\_CTX](#) structure with the *pcCredential* ([IPC\\_CREDENTIAL](#)) member populated with connection information from the Azure Rights Management Service.
- Use the information from your symmetric key service identity creation (see the prerequisites listed earlier in this topic) to set the *wszServicePrincipal*, *wszBposTenantId*, and *cbKey* parameters when you create an instance of an [IPC\\_CREDENTIAL\\_SYMMETRIC\\_KEY](#) structure.

**Note** - Due to an existing condition with our discovery service, if you are not in North America, symmetric key credentials are not accepted from other regions therefore, you must specify your tenant URLs directly. This is done through the *pConnectionInfo* parameter, type [IPC\\_CONNECTION\\_INFO](#), on functions [IpcGetTemplateList](#) or [IpcGetTemplateIssuerList](#).

# Generate a symmetric key and collect the needed information

## Instructions to generate a symmetric key

- Install [Microsoft Online Sign-in Assistant](#)
- Install [Azure AD Powershell Module](#).

**Note** - You must be a tenant administrator to use the Powershell cmdlets.

- Start Powershell and run the following commands to generate a key

```
Import-Module MSOnline
```

```
Connect-MsolService
```

 (type-in your admin credentials)

```
New-MsolServicePrincipal
```

 (type-in a display name)

- After it generates a symmetric key, it will output information about the key including the key itself and an *AppPrincipalId*.

```
The following symmetric key was created as one was not supplied
ZYbF/1TtwE28qplQofCpi2syWd11D83+A3DRlb2Jnv8=
```

```
DisplayName : RMSTestApp
ServicePrincipalNames : {7d9c1f38-600c-4b4d-8249-22427f016963}
ObjectId : 0ee53770-ec86-409e-8939-6d8239880518
AppPrincipalId : 7d9c1f38-600c-4b4d-8249-22427f016963
```

## Instructions to find out TenantBposId and Urls

- Install [Azure RMS powershell module](#).
- Start Powershell and run the following commands to get the RMS configuration of the tenant.

```
Import-Module AIPService
```

```
Connect-AipService
```

 (type-in your admin credentials)

```
Get-AipServiceConfiguration
```

- Create an instance of an [IPC\\_CREDENTIAL\\_SYMMETRIC\\_KEY](#) and set a few members.

```
// Create a key structure.
IPC_CREDENTIAL_SYMMETRIC_KEY symKey = {0};

// Set each member with information from service creation.
symKey.wszBase64Key = "your service principal key";
symKey.wszAppPrincipalId = "your app principal identifier";
symKey.wszBposTenantId = "your tenant identifier";
```

For more information see, [IPC\\_CREDENTIAL\\_SYMMETRIC\\_KEY](#).

- Create an instance of an [IPC\\_CREDENTIAL](#) structure containing your [IPC\\_CREDENTIAL\\_SYMMETRIC\\_KEY](#) instance.

**Note** - The *connectionInfo* members are set with URLs from the previous call to [Get-AipServiceConfiguration](#) and noted here with those field names.

```

// Create a credential structure.
IPC_CREDENTIAL cred = {0};

IPC_CONNECTION_INFO connectionInfo = {0};
connectionInfo.wszIntranetUrl = LicensingIntranetDistributionPointUrl;
connectionInfo.wszExtranetUrl = LicensingExtranetDistributionPointUrl;

// Set each member.
cred.dwType = IPC_CREDENTIAL_TYPE_SYMMETRIC_KEY;
cred.pcCertContext = (PCCERT_CONTEXT)&symKey;

// Create your prompt control.
IPC_PROMPT_CTX promptCtx = {0};

// Set each member.
promptCtx.cbSize = sizeof(IPC_PROMPT_CTX);
promptCtx.hwndParent = NULL;
promptCtx.dwFlags = IPC_PROMPT_FLAG_SILENT;
promptCtx.hCancelEvent = NULL;
promptCtx.pcCredential = &cred;

```

## Identify a template and then encrypt

- Select a template to use for your encryption. Call [IpcGetTemplateList](#) passing in the same instance of [IPC\\_PROMPT\\_CTX](#).

```

PCIPC_TIL pTemplates = NULL;
IPC_TEMPLATE_ISSUER templateIssuer = (pTemplateIssuerList->aTi)[0];

hr = IpcGetTemplateList(&(templateIssuer.connectionInfo),
 IPC_GTL_FLAG_FORCE_DOWNLOAD,
 0,
 &promptCtx,
 NULL,
 &pTemplates);

```

- With the template from earlier in this topic, call [IpcfEncryptFile](#), passing in the same instance of [IPC\\_PROMPT\\_CTX](#).

### Example use of [IpcfEncryptFile](#):

```

LPCWSTR wszContentTemplateId = pTemplates->aTi[0].wszID;
hr = IpcfEncryptFile(wszInputFilePath,
 wszContentTemplateId,
 IPCF_EF_TEMPLATE_ID,
 IPC_EF_FLAG_KEY_NO_PERSIST,
 &promptCtx,
 NULL,
 &wszOutputFilePath);

```

### Example use of [IpcfDecryptFile](#):

```

hr = IpcfDecryptFile(wszInputFilePath,
 IPCF_DF_FLAG_DEFAULT,
 &promptCtx,
 NULL,
 &wszOutputFilePath);

```

You have now completed the steps needed to enable your application to use Azure Rights Management.

## Related topics

- [Getting started with Azure Rights Management](#)
- [Getting started with RMS SDK 2.1](#)
- [Create a service identity via ACS](#)
- [IpcSetGlobalProperty](#)
- [IpcInitialize](#)
- [IPC\\_PROMPT\\_CTX](#)
- [IPC\\_CREDENTIAL](#)
- [IPC\\_CREDENTIAL\\_SYMMETRIC\\_KEY](#)
- [IpcGetTemplateIssuerList](#)
- [IpcGetTemplateList](#)
- [IpcfDecryptFile](#)
- [IpcfEncryptFile](#)
- [IpcCreateLicenseFromScratch](#)
- [IpcCreateLicenseFromTemplateID](#)

# How-to: install, configure and test with an RMS server

8/5/2019 • 2 minutes to read • [Edit Online](#)

This topic covers the steps to connect to an RMS Server or Azure RMS for testing your rights-enabled application.

## Instructions

### Step 1: Setup your RMS server

The following steps guide you in setting up your RMS server and include:

- Install the server
- Enroll the server

#### 1. Install the server

Active Directory Rights Management Services (AD RMS) consists of separate client and server components. The server component is implemented as a set of web services that can be used to administer an RMS infrastructure, issue licenses to content consumers and publishers, and issue certificates to computers and users.

Beginning with Windows Server 2008, both the client and the server components are included in the operating system. You can download the server components for prior operating systems from the following location.

- [RMS Server v1.0 SP2](#)

To configure the server component on Windows Server 2008, you must install the AD RMS role. If you are developing applications against a prior server operating system, configure the registry after installing RMS server v1.0 SP2 but before provisioning the RMS service.

#### 2. Enroll the server

You must enroll an Rights Management Services (RMS) server to identify it in the Pre-Production or Production hierarchy. The enrollment process leaves a server licensor certificate on the server computer. This certificate chains back to a Microsoft root of trust. How you enroll the server depends on which RMS version you are using.

- **Self enrollment**

Beginning with Windows Server 2008, you can enroll an RMS server in the appropriate hierarchy without sending information to Microsoft. When you install the RMS role, a self-enrollment certificate and private key are also installed. These are used to automatically create the server licensor certificate. No information is exchanged with Microsoft.

- **Online enrollment**

If you are using AD RMS v1.0 SP2, you can enroll the server online. Enrollment takes place behind the scenes during the provisioning process, but you must have an Internet connection.

`HKEY_LOCAL_MACHINE\Software\Microsoft\DRMS\1.0\UddiProvider = 0e3d9bb8-b765-4a68-a329-51548685fed3`

#### 3. Test with RMS Server

For testing with an RMS server, configure either server-side discovery or client-side discovery to enable the Rights Management Service Client 2.1 to discover and establish communication with your RMS server.

**NOTE**

Testing with Azure RMS does not require discovery configuration.

- In server-side discovery, an administrator registers a service connection point (SCP) for the RMS root cluster with Active Directory, and the client queries Active Directory to discover the SCP and establish a connection with the server.
- In client-side discovery, you configure RMS Service Discovery settings in the registry on the computer where the RMS Client 2.1 is running. These settings point the RMS Client 2.1 to the RMS server to use. When they are present, server-side discovery is not performed.

To configure client-side discovery, you can set the following registry keys to point to your RMS server. For information about how to configure service-side discovery, see [RMS Client 2.0 Deployment Notes](#).

#### 4. EnterpriseCertification

```
HKEY_LOCAL_MACHINE
 SOFTWARE
 Microsoft
 MSIPC
 ServiceLocation
 EnterpriseCertification
```

**Value:** (Default): [[http](#)|[https](#)]://RMSClusterName/\_wmcs/Certification

#### 5. EnterprisePublishing

```
HKEY_LOCAL_MACHINE
 SOFTWARE
 Microsoft
 MSIPC
 ServiceLocation
 EnterprisePublishing
```

**Value:** (Default): [[http](#)|[https](#)]://RMSClusterName/\_wmcs/Licensing

**NOTE**

By default, these keys do not exist in the registry and must be created.

**IMPORTANT**

If you are running a 32-bit application on a 64-bit version of Windows, you must set these keys in the following key location:

```
HKEY_LOCAL_MACHINE
 SOFTWARE
 Wow6432Node
 Microsoft
 MSIPC
 ...
```

# How-to: set the API security mode

8/5/2019 • 2 minutes to read • [Edit Online](#)

You can choose which security mode your File API application runs in by using the [IpcSetGlobalProperty](#) function.

To initialize your application to run in *server mode*, call the [IpcSetGlobalProperty](#) function and set the security mode to [IPC\\_API\\_MODE\\_SERVER](#). By default, your application will run in *client mode*, [IPC\\_API\\_MODE\\_CLIENT](#).

For more information on *server mode*, see [Application types](#).

**Important** The security mode should be set before any other Rights Management Services SDK 2.1 function is called. After the security mode has been set, it cannot be changed for the current process.

## Related topics

- [Application types](#)
- [API mode values](#)
- [IpcSetGlobalProperty](#)

# How-to: work with encryption settings

8/5/2019 • 2 minutes to read • [Edit Online](#)

This topic orients you to our encryption packages and shows some code snips for their use.

## Support for AES 256, the new default

No additional code is required to use *AES 256* based encryption as it is the new default, assuming you build against the RMS SDK 2.1 March 2015 update or later. We encourage you to seriously consider updating your applications with this release for the additional security benefits of *AES 256*.

### IMPORTANT

Support for consumption of *AES 256* protected files has existed since the [October 2014 release](#). If you are running applications built with a version of the SDK from before October 2014, this update will break your application. Please make sure that customers of the applications you are building, are either using the updated SDK, or are willing to immediately update to the most recent version of your application.

## API encryption support

Beginning with the [March 2015 update](#), we have incorporated the following three flags into our API and their associated encryption packages:

- `IPC_ENCRYPTION_PACKAGE_AES256_CBC4K`
- `IPC_ENCRYPTION_PACKAGE_AES128_CBC4K`
- `IPC_ENCRYPTION_PACKAGE_AES128_ECB` (Also known as, Deprecated Algorithms)

The encryption package flags, see [Preferred encryption](#), can be used in conjunction with the, License Property flag - `IPC_LL_PREFERRED_ENCRYPTION_PACKAGE`.

Following are some simple code snippets that demonstrates how to use the new license property.

## Deprecated Algorithms

We are no longer exposing the `IPC_LL_DEPRECATED_ENCRYPTION_ALGORITHMS` flag in our API. This means that future applications will no longer compile if they reference this flag, but applications already built using it will continue to work since we honor the flag privately in the API code.

Getting the benefit of the old deprecated encryption algorithms flag can still be achieved simply by changing one flag. See the following code snippets for an examples.

## Protect Files with AES 256 CBC4K

No change in code needed, *AES 256* *CBC4K* is the default.

C++

```
hr = IpcCreateLicenseFromTemplateID(pcTil->aTi[0].wszID,
 0,
 NULL,
 &pLicenseHandle);
```

## Protect Files with AES-128 CBC4K

C++

```
hr = IpcCreateLicenseFromTemplateID(pcTil->aTi[0].wszID,
 0,
 NULL,
 &pLicenseHandle);

DWORD dwEncryptionMode = IPC_ENCRYPTION_PACKAGE_AES128_CBC4K;

hr = IpcSetLicenseProperty(pLicenseHandle,
 false,
 IPC_LI_PREFERRED_ENCRYPTION_PACKAGE,
 &dwEncryptionMode);
```

## Protect Files with AES-128 ECB (Deprecated Algorithms)

This sample also shows the new way of supporting *deprecated algorithms*.

C++

```
hr = IpcCreateLicenseFromTemplateID(pcTil->aTi[0].wszID,
 0,
 NULL,
 &pLicenseHandle);

DWORD dwEncryptionMode = IPC_ENCRYPTION_PACKAGE_AES128_ECB;

hr = IpcSetLicenseProperty(pLicenseHandle,
 false,
 IPC_LI_PREFERRED_ENCRYPTION_PACKAGE,
 &dwEncryptionMode);
```

# Application types

8/5/2019 • 2 minutes to read • [Edit Online](#)

This topic covers types of applications that you might choose to create as rights-enabled.

The following application types are currently supported by Rights Management Services SDK 2.1

## Simple applications

A simple application could be a command line tool built to encrypt a provided file. For an example of a simple, rights-enabled application see our implementation of *IPCHelloWorld*, described in [Developing your application](#).

### Server mode applications

*Server mode* is meant for non-interactive applications that consume, protect or process RMS-protected content. An example would be a *Data Loss Prevention* application that runs as a service on a file server and automatically protects sensitive documents. See the [IpcDlp sample](#) for an example of this application type.

If your application uses the *server mode*, it should authenticate to the RMS server silently. Unlike the *client mode*, the RMS SDK 2.1 will not open a credential prompt when it fails to authenticate silently. Also, when running in *server mode*, no application manifest is needed.

For more information on setting the API security mode see, [Setting the API security mode](#).

### Rich client applications

A rich client application allows users to view and manipulate data through a graphical user interface (GUI). Often, the data presented in this GUI is high-value and sensitive to theft or accidental exposure. Information protection support typically enhances existing scenarios but, is not the primary motivation for developing the application.

Using RMS SDK 2.1 with rich client applications helps you:

- Ensure that this data is always encrypted.
- Prevent users from extracting data to an unprotected format (for example, prevent using the clipboard to copy and paste).

Microsoft Notepad is a simple rich client application. Microsoft Office is a more complex rich client application.

For more information on protecting your application, see [Understanding usage restrictions](#).

## Related topics

- [IpcDlp sample](#)
- [Developing your application](#)
- [Setting the API security mode](#)
- [Understanding usage restrictions](#)

# File API configuration

3/4/2019 • 4 minutes to read • [Edit Online](#)

The File API's behavior can be configured through settings in the registry.

The File API provides two kinds of protection; native protection and Pfile protection.

- **Native protection** - the file is protected to an AD RMS format based on its MIME type (file name extension).
- **Pfile protection** - the file is protected to the AD RMS Protected File (Pfile) format.

For more information about supported file formats, see [File API File Support Details](#) in this article.

## Key/Key Value types and descriptions

The following sections describe the keys and key values that control encryption.

`HKEY_LOCAL_MACHINE\Software\Microsoft\MSIPC\FileProtection`

Type: Key

Description: Contains general configuration for the File API.

`HKEY_LOCAL_MACHINE\Software\Microsoft\MSIPC\FileProtection\<EXT>`

Type: Key

Description: Specifies configuration information for a specific file extension; for example, TXT, JPG, and so on.

- The wildcard character, '\*', is allowed; however, a setting for a specific extension takes precedence over the wildcard setting. The wildcard character does not affect settings for Microsoft Office files; these must be explicitly disabled by file type.
- To specify files that do not have an extension, use '.'.
- Do not specify the '.' character when specifying the key for a specific file extension; for example, use `HKEY_LOCAL_MACHINE\Software\Microsoft\MSIPC\FileProtection\TXT` to specify settings for .txt files. (Do not use `HKEY_LOCAL_MACHINE\Software\Microsoft\MSIPC\FileProtection\.TXT`).

To specify the protection behavior, set the **Encryption** value in the key. If the **Encryption** value is not set, the default behavior for the file type is observed.

`HKEY_LOCAL_MACHINE\Software\Microsoft\MSIPC\FileProtection\<EXT>\Encryption*`

Type: REG\_SZ

Description: Contains one of three values:

- Off: Encryption is disabled.

### NOTE

This setting has no bearing on decryption. Any encrypted file, whether encrypted using Native or Pfile protection, can be decrypted, as long as the user has the EXTRACT right.

- **Native:** Native encryption is used. For Office files the encrypted file will have the same extension as the original file. For example, a file with the .docx file extension will be encrypted to a file with an extension of .docx. For other files that can have native protection applied, the file will be encrypted to a file with an

extension of the format pzzz, where zzz is the original file extension. For example, .txt files will be encrypted to a file with an extension of .ptxt. A list of file extensions that can have native protection applied follows.

- **Pfile:** PFile encryption is used. The encrypted file will have .pfile appended to the original extension. For example, after encryption, a .txt file, will have an extension of .txt.pfile.

#### NOTE

This setting has no bearing on Office file formats. For example, if the

`HKEY_LOCAL_MACHINE\Software\Microsoft\MSIPC\FileProtection\DOCX\Encryption` value is set to "Pfile", .docx files will still be encrypted using native protection, and the encrypted file will still have a file extension of .docx.

Setting any other value or setting no value results in default behavior.

## Default behavior for different file formats

- **Office files** Native encryption is enabled.
- **txt, xml, jpg, jpeg, pdf, png, tiff, bmp, gif, giff, jpe, jfif, jif files** Native encryption is enabled (xxx becomes pxxx)
- **All other files** Encryption is protected file (pfile) enabled (xxx become xxx.pfile)

If encryption is attempted on a file type that is blocked, an [IPCERROR\\_FILE\\_ENCRYPT\\_BLOCKED](#) error occurs.

### File API - File Support Details

Native support can be added for any file type (extension). For instance, any extension <ext> (non-office), \*.p<ext> will be used if the admin configuration for that extension is "NATIVE".

### Office files

- File extensions: doc, dot, xla, xls, xlt, pps, ppt, docm, docx, dotm, dotx, xlam, xlsb, xlsm, xlsx, xltx, xps, potm, potx, ppsx, ppsm, pptm, pptx, thmx, vsdx, vsdm, vssx, vssm, vstx, and vstm.
- Protection type = Native (default): sample.docx is encrypted to sample.docx
- Protection type = Pfile: For Office files, has the same effect as Native.
- Off: Disables encryption.

### PDF files

- Protection type = Native: sample.pdf is encrypted and named sample.ppdf
- Protection type = Pfile: sample.pdf is encrypted and named sample.pdf.pfile.
- Off: Disables encryption.

### All other file formats

- Protection type = Pfile: sample.zzz is encrypted and named sample.zzz.pfile; where zzz is the original file extension.
- Off: Disables encryption.

### Examples

The following settings enable PFile encryption for txt files. Office files will have native protection applied (by default), txt files will have PFile protection applied, and all other files will have protection blocked (by default).

```
HKEY_LOCAL_MACHINE
 Software
 Microsoft
 MSIPC
 FileProtection
 txt
 Encryption = Pfile
```

The following settings enable PFile encryption for all non-Office files except txt files. Office files will have native protection applied (by default), txt files will have protection blocked, and all other files will have PFile protection applied.

```
HKEY_LOCAL_MACHINE
 Software
 Microsoft
 MSIPC
 FileProtection
 *
 Encryption = Pfile
 txt
 Encryption = Off
```

The following settings disable native encryption for docx files. Office files, except for docx files, will have native protection applied (by default) and all other files will have protection blocked (by default).

```
HKEY_LOCAL_MACHINE
 Software
 Microsoft
 MSIPC
 FileProtection
 docx
 Encryption = Off
```

## Related articles

- [Developer notes](#)
- [IPCERROR\\_FILE\\_ENCRYPT\\_BLOCKED](#)

# Security best practices for Information Protection

7/2/2019 • 6 minutes to read • [Edit Online](#)

Information Protection Software Development Kits (SDKs) provide a robust system for publishing and consuming protected information of all types. To help a system be as strong as possible, information protection-enabled applications must be built using best practices. Applications share responsibility in helping maintain the security of this ecosystem. Identifying security risks and providing mitigations for those risks introduced during application development helps to minimize the likelihood of a less secure software implementation.

This information supplements the legal agreement that must be signed, to obtain digital certificates for applications using the SDKs.

## Subjects not covered

Although the following subjects are important considerations for creating a development environment and secure applications, they're out of scope for this article:

- **Software development process management** — Configuration management, securing source code, minimizing access to debugged code, and assigning priority to bugs. For some customers, having a more secure software development process is of paramount importance to them. Some customers even prescribe a development process.
- **Common coding errors** — Information for avoiding buffer overruns. We recommend the latest version of Writing Secure Code by Michael Howard and David LeBlanc (Microsoft Press, 2002) to review these generic threats and mitigations.
- **Social engineering** — Includes information about procedural and structural safeguards, to help protect code against exploitation by developers or others within the manufacturer's organization.
- **Physical security** — Includes information about locking down access to your code base and signing certificates.
- **Deployment or distribution of prerelease software** — Includes information about distributing your beta software.
- **Network management** — Includes information about intrusion-detection systems on your physical networks.

## Threat models and mitigations

Digital information owners need the ability to evaluate the environments in which their assets will be decrypted. A statement of minimum security standards provides information owners with a framework for understanding and assessing the security level of the applications.

Some industries, such as government and health care, have certification and accreditation processes and standards that may apply to your product. Meeting these minimum security recommendations isn't a substitute for the unique accreditation needs of your customers. However, the intent of the security standards is to help you prepare for current and future customer requirements, and any investment you make early in the development cycle will benefit your application. These guidelines are recommendations, not a formal Microsoft certification program.

There are several major categories of vulnerabilities in a rights management services system including:

- **Leakage** — Information appears in unauthorized locations.
- **Corruption** — Software or data is modified in an unauthorized manner.

- **Denial** — A computing resource isn't available for use.

These topics focus primarily on leakage issues. The integrity of an API system depends upon its ability, over time, to protect information, enabling access only to designated entities. These topics also touch upon corruption issues. Denial issues aren't covered.

Microsoft doesn't test or review test results related to meeting the minimum standard. The partner is responsible for ensuring the minimum standards are met. Microsoft provides two additional levels of recommendations to help mitigate common threats. In general, these suggestions are additive. For example, meeting preferred recommendations assumes that you have met minimum standards, where applicable, unless otherwise specified.

STANDARD LEVEL	DESCRIPTION
Minimum standard	An application that handles protected information must meet the minimum standard, before it can be signed with the production certificate received from Microsoft. Partners generally use the production hierarchy certificate, at the time of final release of the software. A partner's own internal tests are used to verify whether the application meets this minimum standard. Meeting the minimum standard isn't, and shouldn't be construed as, a guarantee of security by Microsoft. Microsoft doesn't test or review test results related to meeting the minimum standard. The partner is responsible for ensuring the minimum is met.
Recommended standard	Recommended guidelines both chart a path to improved application security, and provide an indication of how the SDK may evolve as more security criteria are implemented. Vendors may differentiate their applications by building to this higher level of security guidelines.
Preferred standard	This standard is the highest category of security currently defined. Vendors who develop applications marketed as highly secure should aim for this standard. Applications that adhere to this standard are likely to be the least vulnerable to attack.

## Malicious software

Microsoft has defined minimum required standards that your application must meet to protect content from malicious software.

### Importing malicious software by using address tables

The information protection SDK doesn't support code modification at run time or modification of the import address table (IAT). An import address table is created for every DLL loaded in your process space. It specifies the addresses of all functions that your application imports. One common attack is to modify the IAT entries within an application to, for example, point to malicious software. The SDK stops the application when it detects this type of attack.

### Minimum standard

- You can't modify the import address table in the application process during execution. Your application specifies many of the functions called at run time by using address tables. These tables can't be altered during or after run time. Among other things, this restriction means you can't perform code-profiling on an application signed by using the production certificate.
- You can't call the `DebugBreak` function from within any DLL specified in the manifest.
- You can't call `LoadLibrary` with the `DONT_RESOLVE_DLL_REFERENCES` flag set. This flag tells the loader to skip binding to the imported modules, thereby modifying the import address table.

- You can't alter delayed loading by making run-time or subsequent changes to the /DELAYLOAD linker switch.
- You can't alter delayed loading by providing your own version of the Delayimp.lib helper function.
- You can't unload modules that are delay-loaded by authenticated modules, while the information protection SDK environment exists.
- You can't use the `/DELAY:UNLOAD` linker switch to enable unloading of delayed modules.

## Incorrectly interpreting license rights

If your application doesn't correctly interpret and enforce the rights expressed in the SDK issuance license, you may make information available in ways that the information owner didn't intend. For example, when an application allows a user to save unencrypted information to new media, when the issuance license only confers the right to view the information.

### Azure Information Protection (AIP)

The information protection system organizes rights a few groupings. For more information, see [Configuring usage rights for Azure Information Protection](#).

AIP allows a user to either decrypt information or not. The information doesn't have any inherent protection. If a user has the right to decrypt, the API permits it. The application is responsible for managing or protecting that information after it is in the clear. An application is responsible for managing its environment and interface to prevent the unauthorized use of information. For example, disabling the **Print** and **Copy** buttons if a license only grants the **VIEW** right. Your test suite should verify that your application acts correctly on all the license rights that it recognizes.

### Minimum standard

- The customer implementation of XrML v.1.2 rights should be consistent with the definitions of these rights, as described in the XrML specifications, which are available at the XrML Web site (<http://www.xrml.org>). Any rights that are specific to your application must be defined for all entities that have an interest in your application.
- Your test suite and test process should verify that your application executes properly against the rights that the application supports. It should also verify that it **doesn't** act upon unsupported rights.
- If you're building a publishing application, you must make information available that explains the intrinsic rights used. This includes those that are, and aren't, supported by the publishing application, and how these rights should be interpreted. In addition, the user interface should make clear to the end user what the implications are of each right granted or denied an individual piece of information.
- Any rights that are abstracted, by inclusion in new rights implemented by an application, must be mapped to the new terminology. For example, a new right called **MANAGER** might include as abstracted rights the **PRINT**, **COPY**, and **EDIT** rights.

### Recommended standard

None at this time.

### Preferred standard

None at this time.

## Next steps

Best practices for implementing applications by using the AIP SDK include the following articles:

- [Threat Models and Mitigations](#)
- [Security Attacks](#)

# Supported file formats

8/5/2019 • 2 minutes to read • [Edit Online](#)

The File API supports native and Pfile formats.

## Supported File Formats

The current version of the File API supports native protection for Microsoft Office files, Portable Document Files (PDF) and PFile protection for all other file formats. PDF files can optionally have PFile protection applied.

- **Native protection.** In native protection, the file is encrypted to an AD RMS file format that is based its MIME type (file name extension). Files that are natively protected using File API are consistent with the format expected by AD RMS enabled applications that use native protection; for example, Office 2013, Office 2010, and FoxIt PDF reader. Native protection is supported only on Office files, PDF files, and a select number of other file types. For more information about the file types on which native protection is supported, see [File API configuration](#).
- **PFile protection.** In PFile protection, files are encrypted using AD RMS Protected File (PFile) format. The file is encrypted to a file with an extension of .pfile. PFile protection is supported for all file formats except Office files.

Administrators can set registry keys to configure whether and how files should be protected based on their file name extension. For more information about how to configure file protection when using File API, see [File API configuration](#).

## Related topics

- [Developer notes](#)
- [File API configuration](#)

# Supported platforms

8/5/2019 • 2 minutes to read • [Edit Online](#)

This topic identifies the Rights Management Services SDK 2.1 supported client and server platforms.

## Supported platforms

- Windows 10
- Windows Server 2012 R2
- Windows Server 2012
- Windows 8
- Windows Server 2008 R2 SP1
- Windows 7 + SP1

**Note** Use of the templates feature is supported beginning with Windows Server 2008.

# Understanding usage restrictions

8/5/2019 • 5 minutes to read • [Edit Online](#)

All RMS enabled applications must enforce usage restrictions. A usage restriction is a condition that results when a user tries to take an action (ex. printing a document), but the RMS policy for that document does not grant them permission or right to perform that action (ex. the PRINT right).

A user's permissions for a document can be queried by using the [IpcAccessCheck](#) function.

## Designing with usage restrictions

- Familiarize yourself with standard RMS rights

For the full set of RMS rights your application may enforce, see [Usage restriction reference](#).

Note that application defined rights specific to your situation and that go beyond the standard RMS rights may be created.

- Identify usage restriction enforcement points

A *usage restriction enforcement point* is a place in your application's control flow where you need to enforce a usage restriction. The [Usage restriction reference](#) topic gives several examples of common enforcement points.

Evaluate your own application to determine which usage restriction enforcement points apply.

Your application may not need all enforcement points described in [Usage restriction reference](#). For example, if your application does not allow users to print content, it does not need to check for the **IPC\_GENERIC\_PRINT** right.

- Update your code to perform an access check at each enforcement point

For guidance about how to enforce specific rights, see [Usage restriction reference](#).

## Usage restriction reference

Usage restrictions are defined by the following constants.

Each user right, listed in the AD RMS right column, has a description, an enforcement point, and suggested methods for enforcement.

AD RMS RIGHT/DESCRIPTION	HOW TO ENFORCE
<b>IPC_GENERIC_ALL</b>  Grants all rights to the user.  <b>Common Enforcement Points:</b> None	This right is used by the system and generally should not be checked directly.  <b>IpcAccessCheck</b> uses this right to determine whether to grant the user other rights as in this example.  <pre>/* fAccessGranted is set to TRUE if either the IPC_GENERIC_WRITE or the IPC_GENERIC_ALL right is granted */</pre> <pre>IpcAccessCheck(hKey, IPC_GENERIC_WRITE, &amp;fAccessGranted);</pre>

AD RMS RIGHT/DESCRIPTION	HOW TO ENFORCE
<p><b>IPC_GENERIC_READ</b></p> <p>The right to read document contents.</p> <p><b>Common Enforcement Points:</b> Document load</p>	Don't load or present document contents
<p><b>IPC_GENERIC_WRITE</b></p> <p>The right to edit document contents</p> <p><b>Common Enforcement Points:</b> Document modification</p>	<p>Make any UI controls that can be used to modify document contents non-editable.</p> <p>Disable any menu items that trigger document changes. <b>Edit &gt; Cut</b>, <b>Edit &gt; Paste</b>, and <b>Insert</b> are typical examples.</p> <p>Disable any shortcut menu items that trigger document changes.</p>
<p>No AD RMS right</p> <p>No description</p> <p><b>Common Enforcement Points:</b> Save</p>	<p>Disable the <b>File &gt; Save</b> menu.</p> <p><b>Note</b> This right does not control <b>File &gt; Save As</b> because that right does not represent a change to the original document.</p> <p>Disable any keyboard shortcut that can be used to trigger a save (for example, Ctrl+S).</p> <p><b>Tip</b> A best practice is to update your core <b>File &gt; Save</b> code to fail if the user doesn't have this right. This acts as a safety net if you miss any UX mechanisms that can be used to trigger a save.</p>
<p><b>IPC_GENERIC_EXTRACT</b></p> <p>The right to extract content from a protected format and place it in an unprotected format.</p> <p><b>Common Enforcement Points:</b> Copy-to-clipboard</p>	<p>Disable the <b>Edit &gt; Copy</b> menu. Disable the <b>Edit &gt; Cut</b> menu.</p> <p>Disable <b>Copy</b> and <b>Cut</b> from any shortcut menus.</p> <p>Disable any keyboard shortcut that can be used to trigger a copy (for example, Ctrl+C or Ctrl+X).</p> <p>Update window message handlers for <b>WM_CUT</b> to reject copying of data if the user does not have this right. If the window is using the default Windows-provided message handler, subclass this window and provide your own handlers for <b>WM_COPY</b> and <b>WM_CUT</b>.</p>
<p>No AD RMS right</p> <p>No description</p> <p><b>Common Enforcement Points:</b> Save As</p>	In your <b>Save As</b> dialog box, disable any file formats that would result in the document being saved without RMS protection.
<p>No AD RMS right</p> <p>No description</p> <p><b>Common Enforcement Points:</b> Alt+PrtScn</p>	Call <b>IpcProtectWindow</b> on any windows that render document contents.

AD RMS RIGHT/DESCRIPTION	HOW TO ENFORCE
<p><b>IPC_GENERIC_EXPORT</b></p> <p>The right to extract content from a protected format and place it in a different AD RMS-protected format.</p> <p><b>Common Enforcement Points:</b> Save As</p>	<p>In your <b>Save As</b> dialog box, disable the ability to save to any other file formats.</p> <p><b>Tip</b> A best practice is to update your core <b>File &gt; Save As</b> code to fail if the user attempts to save this file to a different format and doesn't have this right. This acts as a safety net if you miss any UX mechanisms that can be used to trigger a save as.</p>
<p><b>IPC_GENERIC_PRINT</b></p> <p>The right to print document contents.</p> <p><b>Common Enforcement Points:</b> Print</p>	<p>Disable the <b>File &gt; Print</b> menu.</p> <p>Disable any keyboard shortcut that could be used to trigger a print (for example, Ctrl+P).</p> <p>Disable shortcut menu items that could be used to trigger a print.</p> <p><b>Tip</b> A best practice is to update your core <b>File &gt; Print</b> code to fail if the user doesn't have this right. This acts as a safety net if you miss any UX mechanisms that can be used to trigger a print.</p>
<p><b>IPC_GENERIC_COMMENT</b></p> <p>Some applications support the ability to add comments and annotations to the document without updating core document contents.</p> <p>This right grants the user access to this capability.</p> <p><b>Common Enforcement Points:</b></p> <ul style="list-style-type: none"> <li>Review &gt; Insert comment</li> <li>Review &gt; Delete Comment</li> </ul>	<p>Disable any menu items that can be used to modify document comments or annotations. <b>Review &gt; Insert comment</b> and <b>Review &gt; Delete Comment</b> are examples.</p> <p>Disable any keyboard shortcut that could trigger modification of document comments.</p> <p><b>Note</b> A default implementation requires both <b>IPC_GENERIC_COMMENT</b> and <b>IPC_GENERIC_WRITE</b> to persist new comments to a file. Applications may choose to add support for the case where the <b>IPC_GENERIC_COMMENT</b> right is granted and the <b>IPC_GENERIC_WRITE</b> right is not. In this case, it is permitted to allow Save, as long as document modifications are restricted to comments only.</p>
<p><b>IPC_VIEW_RIGHTS</b></p> <p>No description</p> <p><b>Common Enforcement Points:</b> N/A</p>	<p>Enforced by the system. The system will not allow the developer to query the <b>user rights list</b> from a license unless this right is granted.</p>
<p><b>IPC_EDIT_RIGHTS</b></p> <p>Some applications allow users to modify the set of users and rights for AD RMS-protected content.</p> <p>This right grants the user access to this capability.</p> <p><b>Common Enforcement Points:</b> Application rights editing UI control</p>	<p>Disable user access to any UI that can be used to edit the RMS policy for a document.</p>

## Related topics

- [IpcAccessCheck](#)

# API reference

8/5/2019 • 2 minutes to read • [Edit Online](#)

The Microsoft Rights Management SDK 2.1 supports RMS enablement of Windows clients. For more information on specifics, see [Release notes](#).

- [Constants](#)
- [Data types](#)
- [Functions](#)
- [Structures](#)
- [Error codes](#)

## Related topics

- [Release notes](#)

# Frequently asked questions for Azure Information Protection

7/20/2020 • 18 minutes to read • [Edit Online](#)

Applies to: [Azure Information Protection](#), [Office 365](#)

## NOTE

To provide a unified and streamlined customer experience, **Azure Information Protection client (classic)** and **Label Management** in the Azure Portal are being **deprecated** as of **March 31, 2021**. This time-frame allows all current Azure Information Protection customers to transition to our unified labeling solution using the Microsoft Information Protection Unified Labeling platform. Learn more in the official [deprecation notice](#).

Have a question about Azure Information Protection, or about the Azure Rights Management service (Azure RMS)? See if it's answered here.

## What's the difference between Azure Information Protection and Microsoft Information Protection?

Unlike Azure Information Protection, [Microsoft Information Protection](#) isn't a subscription or product that you can buy. Instead, it's a framework for products and integrated capabilities that help you protect your organization's sensitive information.

**Microsoft Information Protection products include:**

- Azure Information Protection
- Office 365 Information Protection, such as Office 365 DLP
- Windows Information Protection
- Microsoft Cloud App Security

**Microsoft Information Protection capabilities include:**

- Unified label management
- End-user labeling experiences built into Office apps
- The ability for Windows to understand unified labels and apply protection to data
- The Microsoft Information Protection SDK
- Functionality in Adobe Acrobat Reader to view labeled and protected PDFs

For more information, see [Information protection capabilities to help protect your sensitive data](#).

## What's the difference between labels in Azure Information Protection and labels in Office 365?

Originally, Office 365 had just [retention labels](#) that enabled you to classify documents and emails for auditing and retention when that content was stored in Office 365 services.

In contrast, Azure Information Protection labels enabled you apply a consistent classification and protection policy for documents and emails whether they were stored on-premises or in the cloud.

Announced at Microsoft Ignite 2018 in Orlando, Office 365 now has the option to create and configure [sensitivity labels](#), in addition to retention labels. Sensitivity labels can be created and configured in the following admin centers:

- Office 365 Security & Compliance Center
- Microsoft 365 security center
- Microsoft 365 compliance center

Use Azure Information Protection labels as sensitivity labels with Office 365 apps by [migrating your AIP labels to the unified labeling store](#).

For more information about unified labeling management and support, see [Announcing availability of information protection capabilities to help protect your sensitive data](#).

## How can I determine if my tenant is on the unified labeling platform?

When your tenant is on the unified labeling platform, it supports sensitivity labels that can be used by [clients and services that support unified labeling](#). If you obtained your subscription for Azure Information Protection in June 2019 or later, your tenant is automatically on the unified labeling platform and no further action is needed. Your tenant might also be on this platform because somebody migrated your Azure Information Protection labels.

If your tenant is not on the unified labeling platform, you'll see the following information banner in the Azure portal, on the **Azure Information Protection** panes:

 Unified labeling is not activated in this tenant. Labels and policies are limited to the Azure Information Protection client (classic). Activate unified labeling now →

You can also check by going to **Azure Information Protection > Manage > Unified labeling**, and view the **Unified labeling** status:

STATUS	DESCRIPTION
Activated	Your tenant is on the unified labeling platform. You can <a href="#">create, configure, and publish labels</a> from the Microsoft 365 compliance center.
Not activated	Your tenant is not on the unified labeling platform. For migration instructions and guidance, see <a href="#">How to migrate Azure Information Protection labels to unified sensitivity labels</a> .

## What's the difference between the Azure Information Protection classic and unified labeling clients?

The original client, referred to as the *Azure Information client* or the *classic* client, downloads labels and policy settings from Azure and enables you to configure the [AIP policy](#) from the Azure portal.

The *unified labeling client* is a more recent addition and supports the unified labeling store used by multiple applications and services. The unified labeling client downloads [sensitivity labels](#) and policy settings from the following admin centers:

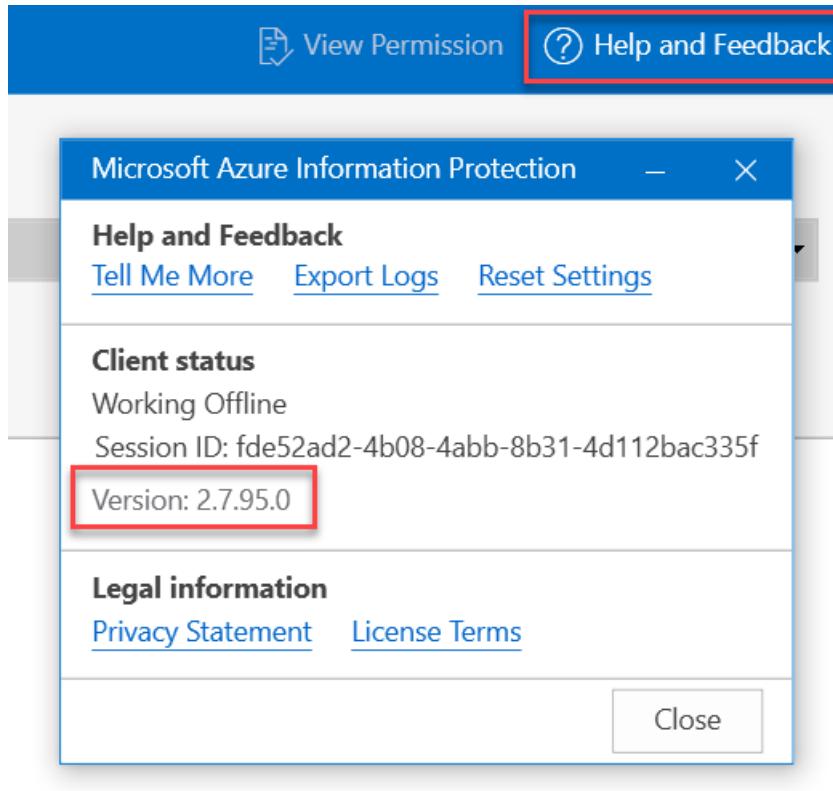
- Office 365 Security & Compliance Center
- Microsoft 365 security center
- Microsoft 365 compliance center

If you're an admin and aren't sure which client to use, see [Choose which Azure Information Protection client to use](#).

## Identify the client you have installed

If you are a user who wants to understand verify whether you have the classic or unified labeling client installed, select **Help and Feedback** to show the **Microsoft Azure Information Protection** dialog box.

For example:



The version number indicates the client, as follows:

- Versions 1.x indicate that you have the classic client. Example: 1.54.59.0
- Versions 2.x indicate that you have the unified labeling client. Example: 2.6.111.0

Access this dialog using one of the following methods:

- In the File Explorer, right-click a file, files, or folder, select **Classify and protect > Help and Feedback**.
- In Office applications, the classic client has a **Protect** button, and the unified labeling client has a **Sensitivity** button. Select either of these buttons and then select **Help and Feedback**.

## When is the right time to migrate my labels?

We recommend that you migrate your Azure Information Protection labels to the unified labeling platform so that you can use them as sensitivity labels with other [clients and services that support unified labeling](#).

For more information and instructions, see [How to migrate Azure Information Protection labels to unified sensitivity labels](#).

## After I've migrated my labels, which management portal do I use?

After you've migrated your labels in the Azure portal, continue managing them in one of the following locations, depending on the clients you have installed:

CLIENT

COLUMN2

CLIENT	COLUMN2
Unified labeling clients and services only	If you only have unified labeling clients installed, manage your labels in one of the admin centers: Office 365 Security & Compliance Center, Microsoft 365 security center, or Microsoft 365 compliance center. Unified labeling clients download the labels and policy settings from these admin centers. For instructions, see <a href="#">Create and configure sensitivity labels and their policies</a> .
Classic client only	If you've migrated your labels, but still have the classic client installed, continue to use the Azure portal to edit labels and policy settings. The classic client continues to download labels and policy settings from Azure.
Both the AIP <a href="#">classic client</a> and <a href="#">unified labeling</a> clients	If you have both of the clients installed, use the admin centers or the Azure portal to make label changes. For the classic clients to pick up label changes made in the admin centers, return to the Azure portal to publish them. In the Azure portal > <b>Azure Information Protection - Unified labeling</b> pane, select <b>Publish</b> .  Continue to use the Azure portal for <a href="#">central reporting</a> and the <a href="#">scanner</a> .

## What's the difference between Azure Information Protection and Azure Rights Management?

Azure Information Protection (AIP) provides classification, labeling, and protection for an organization's documents and emails.

Content is protected using the Azure Rights Management service, which is now a component of AIP.

For more information, see [How data is protected](#) and [What is Azure Rights Management?](#).

## What's the role of identity management for Azure Information Protection?

Identity management is an important component of AIP, as users must have a valid user name and password to access protected content.

To read more about how Azure Information Protection helps to secure your data, see [The role of Azure Information Protection in securing data](#).

## What subscription do I need for Azure Information Protection and what features are included?

To understand more about AIP subscriptions, see the subscription information and feature list on the [Azure Information Protection pricing](#) page.

If you have an Office 365 subscription that includes Azure Rights Management data protection, download the [Azure Information Protection licensing datasheet](#) for more details about integrating with AIP.

Still have questions about licensing? See if they are answered in the [frequently asked questions for licensing](#) section.

## Is the Azure Information Protection client only for subscriptions that include classification and labeling?

No. The classic AIP client can also be used with subscriptions that include just the Azure Rights Management service, for data protection only.

When the classic client is installed without an Azure Information Protection policy, the client automatically operates in [protection-only mode](#), which enables users to apply Rights Management templates and custom permissions.

If you later purchase a subscription that does include classification and labeling, the client automatically switches to standard mode when it downloads the Azure Information Protection policy.

## Do you need to be a global admin to configure Azure Information Protection, or can I delegate to other administrators?

Global administrators for an Office 365 tenant or Azure AD tenant can obviously run all administrative tasks for Azure Information Protection.

However, if you want to assign administrative permissions to other users, do so using the following roles:

- [Azure Information Protection administrator](#)
- [Compliance administrator or Compliance data administrator](#)
- [Security reader or Global reader](#)
- [Security administrator](#)
- [Azure Rights Management Global Administrator and Connector Administrator](#)

Additionally, note the following when managing administrative tasks and roles:

TOPIC	DETAILS
<b>Supported account types</b>	Microsoft accounts are not supported for delegated administration of Azure Information Protection, even if these accounts are assigned to one of the administrative roles listed.
<b>Onboarding controls</b>	If you have configured <a href="#">onboarding controls</a> , this configuration does not affect the ability to administer Azure Information Protection, except the RMS connector. For example, if you have configured onboarding controls so that the ability to protect content is restricted to the <i>IT department</i> group, the account used to install and configure the RMS connector must be a member of that group.
<b>Removing protection</b>	Administrators cannot automatically remove protection from documents or emails that were protected by Azure Information Protection. Only users who are assigned as super users can do remove protection, and only when the super user feature is enabled.  Any user with administrative permissions to Azure Information Protection can enable the super user feature, and assign users as super users, including their own account.  These actions are recorded in an administrator log.  For more information, see the security best practices section in <a href="#">Configuring super users for Azure Information Protection and discovery services or data recovery</a> .

Topic	Details
<b>Migrating to the unified labeling store</b>	If you are migrating your Azure Information Protection labels to the unified labeling store, be sure to read the following section from the label migration documentation: <a href="#">Administrative roles that support the unified labeling platform</a> .

## Azure Information Protection administrator

This Azure Active Directory administrator role lets an administrator configure Azure Information Protection but not other services.

Administrators with this role can:

- Activate and deactivate the Azure Rights Management protection service
- Configure protection settings and labels
- Configure the Azure Information Protection policy
- Run all the PowerShell cmdlets for the [Azure Information Protection client](#) and from the [AIPService module](#)

To assign a user to this administrative role, see [Assign a user to administrator roles in Azure Active Directory](#).

### NOTE

This role doesn't support tracking and revoking documents for users, and is not supported in the Azure portal if your tenant is on the [unified labeling platform](#).

## Compliance administrator or Compliance data administrator

These Azure Active Directory administrator roles enable administrators to:

- Configure Azure Information Protection, including activating and deactivating the Azure Rights Management protection service
- Configure protection settings and labels
- Configure the Azure Information Protection policy
- Run all the PowerShell cmdlets for the [Azure Information Protection client](#) and from the [AIPService module](#).

To assign a user to this administrative role, see [Assign a user to administrator roles in Azure Active Directory](#).

To see what other permissions a user with these roles have, see the [Available roles](#) section from the Azure Active Directory documentation.

### NOTE

These roles don't support tracking and revoking documents for users.

## Security reader or Global reader

These roles are used for [Azure Information Protection analytics](#) only, and enable administrators to:

- View how your labels are being used
- Monitor user access to labeled documents and emails
- View changes made to classification
- Identify documents that contain sensitive information that must be protected

Because this feature uses Azure Monitor, you must also have a supporting [RBAC role](#).

### Security administrator

This Azure Active Directory administrator role enables administrators to configure Azure Information Protection in the Azure portal as well as some aspects of other Azure services.

Administrators with this role cannot run any of the [PowerShell cmdlets from the AIPService module](#), or track and revoke documents for users.

To assign a user to this administrative role, see [Assign a user to administrator roles in Azure Active Directory](#).

To see what other permissions a user with this role has, see the [Available roles](#) section from the Azure Active Directory documentation.

### Azure Rights Management Global Administrator and Connector Administrator

The Global Administrator role enables users to run all [PowerShell cmdlets from the AIPService module](#) without making them a global administrator for other cloud services.

The Connector Administrator role enables users to run only the Rights Management (RMS) connector.

These administrative roles don't grant permissions to management consoles, or support tracking and revoking documents for users.

To assign either of these administrative roles, use the AIPService PowerShell cmdlet, [Add-AipServiceRoleBasedAdministrator](#).

## Does Azure Information Protection support on-premises and hybrid scenarios?

Yes. Although Azure Information Protection is a cloud-based solution, it can classify, label, and protect documents and emails that are stored on-premises, as well as in the cloud.

If you have Exchange Server, SharePoint Server, and Windows file servers, use one or both of the following methods:

- Deploy the [Rights Management connector](#) so that these on-premises servers can use the Azure Rights Management service to protect your emails and documents
- Synchronize and federate your Active Directory domain controllers with Azure AD for a more seamless authentication experience for users. For example, use [Azure AD Connect](#).

The Azure Rights Management service automatically generates and manages XrML certificates as required, so it doesn't use an on-premises PKI.

For more information about how Azure Rights Management uses certificates, see the [Walkthrough of how Azure RMS works: First use, content protection, content consumption](#).

## What types of data can Azure Information Protection classify and protect?

Azure Information Protection can classify and protect email messages and documents, whether they are located on-premises or in the cloud. These documents include Word documents, Excel spreadsheets, PowerPoint presentations, PDF documents, text-based files, and image files.

For more information, see the full list [file types supported](#).

**NOTE**

Azure Information Protection cannot classify and protect structured data such as database files, calendar items, Yammer posts, Sway content, and OneNote notebooks.

**TIP**

Power BI now supports classification by using sensitivity labels and can apply protection from those labels to data that is exported to the following file formats: .pdf, .xls, and .ppt. For more information, see [Data protection in Power BI \(preview\)](#).

## I see Azure Information Protection is listed as an available cloud app for conditional access—how does this work?

Yes, as a preview offering, you can now configure Azure AD conditional access for Azure Information Protection.

When a user opens a document that is protected by Azure Information Protection, administrators can now block or grant access to users in their tenant, based on the standard conditional access controls. Requiring multi-factor authentication (MFA) is one of the most commonly requested conditions. Another one is that devices must be [compliant with your Intune policies](#) so that for example, mobile devices meet your password requirements and a minimum operating system version, and computers must be domain-joined.

For more information and some walk-through examples, see the following blog post: [Conditional Access policies for Azure Information Protection](#).

Additional information:

TOPIC	DETAILS
Evaluation frequency	For Windows computers, and the current preview release, the conditional access policies for Azure Information Protection are evaluated when the <a href="#">user environment is initialized</a> (this process is also known as bootstrapping), and then every 30 days. To fine-tune how often your conditional access policies get evaluated, <a href="#">configure the token lifetime</a> .
Administrator accounts	We recommend that you do not add administrator accounts to your conditional access policies because these accounts will not be able to access the Azure Information Protection pane in the Azure portal.
MFA and B2B collaboration	If you use MFA in your conditional access policies for collaborating with other organizations (B2B), you must use <a href="#">Azure AD B2B collaboration</a> and create guest accounts for the users you want to share with in the other organization.
Terms of Use prompts	With the Azure AD December 2018 preview release, you can now <a href="#">prompt users to accept a terms of use</a> before they open a protected document for the first time.

TOPIC	DETAILS
Cloud apps	If you use many cloud apps for conditional access, you might not see <b>Microsoft Azure Information Protection</b> displayed in the list to select. In this case, use the search box at the top of the list. Start typing "Microsoft Azure Information Protection" to filter the available apps. Providing you have a supported subscription, you'll then see <b>Microsoft Azure Information Protection</b> to select.

## I see Azure Information Protection is listed as a security provider for Microsoft Graph Security—how does this work and what alerts will I receive?

Yes, as a public preview offering, you can now receive an alert for **Azure Information Protection anomalous data access**. This alert is triggered when there are unusual attempts to access data that is protected by Azure Information Protection. For example, accessing an unusually high volume of data, at an unusual time of day, or access from an unknown location.

Such alerts can help you to detect advanced data-related attacks and insider threats in your environment. These alerts use machine learning to profile the behavior of users who access your protected data.

The Azure Information Protection alerts can be accessed by [using the Microsoft Graph Security API](#), or you can [stream alerts](#) to SIEM solutions, such as Splunk and IBM QRadar, by using Azure Monitor.

For more information about the Microsoft Graph Security API, see [Microsoft Graph Security API overview](#).

## What's the difference between Windows Server FCI and the Azure Information Protection scanner?

Windows Server File Classification Infrastructure has historically been an option to classify documents and then protect them by using the [Rights Management connector](#) (Office documents only) or a [PowerShell script](#) (all file types).

We now recommend you use the [Azure Information Protection scanner](#). The scanner uses the Azure Information Protection client and your Azure Information Protection policy to label documents (all file types) so that these documents are then classified and optionally, protected.

The main differences between these two solutions:

	WINDOWS SERVER FCI	AZURE INFORMATION PROTECTION SCANNER
Supported data stores	Local folders on Windows Server	- Windows file shares and network-attached storage - SharePoint Server 2016 and SharePoint Server 2013. SharePoint Server 2010 is also supported for customers who have <a href="#">extended support for this version of SharePoint</a> .
Operational mode	Real time	Systematically crawls the data stores once or repeatedly

	WINDOWS SERVER FCI	AZURE INFORMATION PROTECTION SCANNER
Supported file types	<ul style="list-style-type: none"> <li>- All file types are protected by default</li> <li>- Specific file types can be excluded from protection by editing the registry</li> </ul>	<p>Support for file types:</p> <ul style="list-style-type: none"> <li>- Office file types and PDF documents are protected by default</li> <li>- Additional file types can be included for protection by editing the registry</li> </ul>

## Setting Rights Management owners

By default, for both Windows Server FCI and the Azure Information Protection scanner, the [Rights Management owner](#) is set to the account that protects the file.

Override the default settings as follows:

- **Windows Server FCI:** Set the Rights Management owner to be a single account for all files, or dynamically set the Rights Management owner for each file.

To dynamically set the Rights Management owner, use the **-OwnerMail [Source File Owner Email]** parameter and value. This configuration retrieves the user's email address from Active Directory by using the user account name in the file's Owner property.

- **Azure Information Protection scanner:** For newly protected files, set the Rights Management owner to be a single account for all files on a specified data store, by specifying the **-Default owner** setting in the scanner profile.

Dynamically setting the Rights Management owner for each file is not supported, and the Rights Management owner is not changed for previously protected files.

### NOTE

When the scanner protects files on SharePoint sites and libraries, the Rights Management owner is dynamically set for each file by using the SharePoint Editor value.

## I've heard a new release is going to be available soon, for Azure Information Protection—when will it be released?

The technical documentation does not contain information about upcoming releases. For this type of information, use the [Microsoft 365 Roadmap](#), check the [Enterprise Mobility + Security Blog](#).

## Is Azure Information Protection suitable for my country?

Different countries have different requirements and regulations. To help you answer this question for your organization, see [Suitability for different countries](#).

## How can Azure Information Protection help with GDPR?

To see how Azure Information Protection can help you meet the General Data Protection Regulation (GDPR), see the following blog post announcement, with video:

[Microsoft 365 provides an information protection strategy to help with the GDPR](#)

## Where can I find supporting information for Azure Information

## Protection—such as legal, compliance, and SLAs?

See [Compliance and supporting information for Azure Information Protection](#).

## How can I report a problem or send feedback for Azure Information Protection?

For technical support, use your standard support channels or [contact Microsoft Support](#).

We also invite you to engage with our engineering team, on their [Azure Information Protection Yammer site](#).

## What do I do if my question isn't here?

First, review the frequently asked questions listed below, which are specific to classification and labeling, or specific to data protection. The [Azure Rights Management service \(Azure RMS\)](#) provides the data protection technology for Azure Information Protection. Azure RMS can be used with classification and labeling, or by itself.

- [FAQs for classification and labeling](#)
- [FAQs for data protection](#)

If your question isn't answered, see the links and resources listed in [Information and support for Azure Information Protection](#).

In addition, there are FAQs designed for end users:

- [FAQ for Azure Information Protection app for iOS and Android](#)
- [FAQ for RMS sharing app for Mac computers](#)

# Frequently asked questions about classification and labeling in Azure Information Protection

3/16/2020 • 5 minutes to read • [Edit Online](#)

Applies to: [Azure Information Protection](#), [Office 365](#)

## NOTE

To provide a unified and streamlined customer experience, **Azure Information Protection client (classic)** and **Label Management** in the Azure Portal are being **deprecated** as of **March 31, 2021**. This time-frame allows all current Azure Information Protection customers to transition to our unified labeling solution using the Microsoft Information Protection Unified Labeling platform. Learn more in the official [deprecation notice](#).

Have a question about Azure Information Protection that is specifically about classification and labeling? See if it's answered here.

## Which client do I install for testing new functionality?

Currently, there are two Azure Information Protection clients for Windows:

- The **Azure Information Protection unified labeling client** that downloads labels and policy settings from one of the following admin centers: Office 365 Security & Compliance Center, Microsoft 365 security center, Microsoft 365 compliance center. This client is now in general availability, and might have a preview version for you to test additional functionality for a future release.
- The **Azure Information Protection client (classic)** that downloads labels and policy settings from the Azure portal. This client builds on previous general availability versions of the client.

We recommend you test with the unified labeling client if its current feature set and functionality meet your business requirements. If not, or if you have configured labels in the Azure portal that you haven't yet [migrated to the unified labeling store](#), use the classic client.

For more information, including a feature and functionality comparison table, see [Choose which Azure Information Protection client to use](#).

## Where can I find information about using sensitivity labels for Office apps?

See the following documentation resources:

- [Learn about sensitivity labels](#)
- [Sensitivity labels in Office apps](#)
- [Apply sensitivity labels to your documents and email within Office](#)

## Can a file have more than one classification?

Users can select just one label at a time for each document or email, which often results in just one classification. However, if users select a sublabel, this actually applies two labels at the same time; a primary label and a

secondary label. By using sublabels, a file can have two classifications that denote a parent\child relationship for an additional level of control.

For example, the label **Confidential** might contain sublabels such as **Legal** and **Finance**. You can apply different classification visual markings and different Rights Management templates to these sublabels. A user cannot select the **Confidential** label by itself; only one of its sublabels, such as **Legal**. As a result, the label that they see set is **Confidential \ Legal**. The metadata for that file includes one custom text property for **Confidential**, one custom text property for **Legal**, and another that contains both values (**Confidential Legal**).

When you use sublabels, don't configure visual markings, protection, and conditions at the primary label. When you use sublevels, configure these setting on the sublabel only. If you configure these settings on the primary label and its sublabel, the settings at the sublabel take precedence.

## How do I prevent somebody from removing or changing a label?

Although there's a [policy setting](#) that requires users to state why they are lowering a classification label, removing a label, or removing protection, this setting does not prevent these actions. To prevent users from removing or changing a label, the content must already be protected and the protection permissions do not grant the user the Export or Full Control [usage right](#).

## When an email is labeled, do any attachments automatically get the same labeling?

No. When you label an email message that has attachments, those attachments do not inherit the same label. The attachments remain either without a label or retain a separately applied label. However, if the label for the email applies protection, that protection is applied to Office attachments.

## How can DLP solutions and other applications integrate with Azure Information Protection?

Because Azure Information Protection uses persistent metadata for classification, which includes a clear-text label, this information can be read by DLP solutions and other applications.

For more information about this metadata, see [Label information stored in emails and documents](#).

For examples of using this metadata with Exchange Online mail flow rules, see [Configuring Exchange Online mail flow rules for Azure Information Protection labels](#).

## Can I create a document template that automatically includes the classification?

Yes. You can configure a label to [apply a header or footer that includes the label name](#). But if that doesn't meet your requirements, for the Azure Information Protection client (classic) only, you can create a document template that has the formatting you want and add the classification as a field code.

As an example, you might have a table in your document's header that displays the classification. Or, you use specific wording for an introduction that references the document's classification.

To add this field code in your document:

1. Label the document and save it. This action creates new metadata fields that you can now use for your field code.
2. In the document, position the cursor where you want to add the label's classification and then, from the **Insert** tab, select **Text > Quick Parts > Field**.

3. In the **Field** dialog box, from the **Categories** dropdown, select **Document Information**. Then, from the **Fields names** dropdown, select **DocProperty**.
4. From the **Property** dropdown, select **Sensitivity**, and select **OK**.

The current label's classification is displayed in the document and this value will be refreshed automatically whenever you open the document or use the template. So if the label changes, the classification that is displayed for this field code is automatically updated in the document.

## How is classification for emails using Azure Information Protection different from Exchange message classification?

Exchange message classification is an older feature that can classify emails and it is implemented independently from Azure Information Protection labels or sensitivity labels that apply classification.

However, you can integrate this older feature with labels, so that when users classify an email by using Outlook on the web and by using some mobile mail applications, the label classification and corresponding label markings are automatically added.

You can use this same technique to use your labels with Outlook on the web and these mobile mail applications.

Note that there's no need to do this if you're using Outlook on the web with Exchange Online, because this combination supports built-in labeling when you publish sensitivity labels from the Office 365 Security & Compliance Center, Microsoft 365 security center, or Microsoft compliance center.

If you cannot use built-in labeling with Outlook on the web, see the configuration steps for this workaround: [Integrate Exchange message classification with Azure Information Protection for a mobile device labeling solution](#).

# Frequently asked questions about data protection in Azure Information Protection

7/20/2020 • 19 minutes to read • [Edit Online](#)

Applies to: [Azure Information Protection](#), [Office 365](#)

## NOTE

To provide a unified and streamlined customer experience, **Azure Information Protection client (classic)** and **Label Management** in the Azure Portal are being **deprecated** as of **March 31, 2021**. This time-frame allows all current Azure Information Protection customers to transition to our unified labeling solution using the Microsoft Information Protection Unified Labeling platform. Learn more in the official [deprecation notice](#).

Have a question about the data protection service, Azure Rights Management, from Azure Information Protection? See if it's answered here.

## Do files have to be in the cloud to be protected by Azure Rights Management?

No, this is a common misconception. The Azure Rights Management service (and Microsoft) does not see or store your data as part of the information protection process. Information that you protect is never sent to or stored in Azure unless you explicitly store it in Azure or use another cloud service that stores it in Azure.

For more information, see [How does Azure RMS work? Under the hood](#) to understand how a secret key formula that is created and stored on-premises is protected by the Azure Rights Management service but remains on-premises.

## What's the difference between Azure Rights Management encryption and encryption in other Microsoft cloud services?

Microsoft provides multiple encryption technologies that enable you to protect your data for different, and often complementary scenarios. For example, while Office 365 offers encryption at-rest for data stored in Office 365, the Azure Rights Management service from Azure Information Protection independently encrypts your data so that it is protected regardless of where it is located or how it is transmitted.

These encryption technologies are complementary and using them requires enabling and configuring them independently. When you do so, you might have the option to bring your own key for the encryption, a scenario also known as "BYOK." Enabling BYOK for one of these technologies does not affect the others. For example, you can use BYOK for Azure Information Protection and not use BYOK for other encryption technologies, and vice versa. The keys used by these different technologies might be the same or different, depending on how you configure the encryption options for each service.

## What's the difference between BYOK and HYOK and when should I use them?

**Bring your own key (BYOK)** in the context of Azure Information Protection, is when you create your own key on-premises for Azure Rights Management protection. You then transfer that key to a hardware security module

(HSM) in Azure Key Vault where you continue to own and manage your key. If you didn't do this, Azure Rights Management protection would use a key that is automatically created and managed for you in Azure. This default configuration is referred to as "Microsoft-managed" rather than "customer-managed" (the BYOK option).

For more information about BYOK and whether you should choose this key topology for your organization, see [Planning and implementing your Azure Information Protection tenant key](#).

**Hold your own key** (HYOK) in the context of Azure Information Protection, is for a few organizations that have a subset of documents or emails that cannot be protected by a key that is stored in the cloud. For these organizations, this restriction applies even if they created the key and manage it, using BYOK. The restriction can often be because of regulatory or compliance reasons and the HYOK configuration should be applied to "Top Secret" information only, that will never be shared outside the organization, will only be consumed on the internal network, and does not need to be accessed from mobile devices.

For these exceptions (typically less than 10% of all the content that needs to be protected), organizations can use an on-premises solution, Active Directory Rights Management Services, to create the key that remains on-premises. With this solution, computers get their Azure Information Protection policy from the cloud, but this identified content can be protected by using the on-premises key.

For more information about HYOK and to make sure that you understand its limitations and restrictions, and guidance when to use it, see [Hold your own key \(HYOK\) requirements and restrictions for AD RMS protection](#).

## Can I now use BYOK with Exchange Online?

Yes, you can now use BYOK with Exchange Online when you follow the instructions in [Set up new Office 365 Message Encryption capabilities built on top of Azure Information Protection](#). These instructions enable the new capabilities in Exchange Online that support using BYOK for Azure Information Protection, as well as the new Office 365 Message Encryption.

For more information about this change, see the blog announcement: [Office 365 Message Encryption with the new capabilities](#)

## Where can I find information about third-party solutions that integrate with Azure RMS?

Many software vendors already have solutions or are implementing solutions that integrate with Azure Rights Management—and the list is growing rapidly. You might find it useful to check the [RMS-enchanted solutions](#) list and get the latest updates from [Microsoft Mobility@MSFTMobility](#) on Twitter. Also check the [developer's guide](#) and post any specific integration questions on the Azure Information Protection [Yammer site](#).

## Is there a management pack or similar monitoring mechanism for the RMS connector?

Although the Rights Management connector logs information, warning, and error messages to the event log, there isn't a management pack that includes monitoring for these events. However, the list of events and their descriptions, with more information to help you take corrective action is documented in [Monitor the Azure Rights Management connector](#).

## How do I create a new custom template in the Azure portal?

Custom templates have moved to the Azure portal where you can continue to manage them as templates, or convert them to labels. To create a new template, create a new label and configure the data protection settings for Azure RMS. Under the covers, this creates a new template that can then be accessed by services and applications that integrate with Rights Management templates.

For more information about templates in the Azure portal, see [Configuring and managing templates for Azure Information Protection](#).

## I've protected a document and now want to change the usage rights or add users—do I need to reprotect the document?

If the document was protected by using a label or template, there's no need to reprotect the document. Modify the label or template by making your changes to the usage rights or add new groups (or users), and then save these changes:

- When a user hasn't accessed the document before you made the changes, the changes take effect as soon as the user opens the document.
- When a user has already accessed the document, these changes take effect when their [use license](#) expires. Reprotect the document only if you cannot wait for the use license to expire. Reprotecting effectively creates a new version of the document, and therefore a new use license for the user.

Alternatively, if you have already configured a group for the required permissions, you can change the group membership to include or exclude users and there is no need to change the label or template. There might be a small delay before the changes take effect because group membership is [cached](#) by the Azure Rights Management service.

If the document was protected by using custom permissions, you cannot change the permissions for the existing document. You must protect the document again and specify all the users and all the usage rights that are required for this new version of the document. To reprotect a protected document, you must have the Full Control usage right.

Tip: To check whether a document was protected by a template or by using custom permission, use the [Get-AIPFileStatus](#) PowerShell cmdlet. You always see a template description of **Restricted Access** for custom permissions, with a unique template ID that is not displayed when you run [Get-RMSTemplate](#).

## I have a hybrid deployment of Exchange with some users on Exchange Online and others on Exchange Server—is this supported by Azure RMS?

Absolutely, and the nice thing is, users are able to seamlessly protect and consume protected emails and attachments across the two Exchange deployments. For this configuration, [activate Azure RMS](#) and [enable IRM for Exchange Online](#), then [deploy and configure the RMS connector](#) for Exchange Server.

## If I use this protection for my production environment, is my company then locked into the solution or risk losing access to content that we protected with Azure RMS?

No, you always remain in control of your data and can continue to access it, even if you decide to no longer use the Azure Rights Management service. For more information, see [Decommissioning and deactivating Azure Rights Management](#).

## Can I control which of my users can use Azure RMS to protect content?

Yes, the Azure Rights Management service has user onboarding controls for this scenario. For more information, see the [Configuring onboarding controls for a phased deployment](#) section in the [Activating the protection service from Azure Information Protection](#) article.

## Can I prevent users from sharing protected documents with specific organizations?

One of the biggest benefits of using the Azure Rights Management service for data protection is that it supports business-to-business collaboration without you having to configure explicit trusts for each partner organization, because Azure AD takes care of the authentication for you.

There is no administration option to prevent users from securely sharing documents with specific organizations. For example, you want to block an organization that you don't trust or that has a competing business. Preventing the Azure Rights Management service from sending protected documents to users in these organizations wouldn't make sense because your users would then share their documents unprotected, which is probably the last thing you want to happen in this scenario. For example, you wouldn't be able to identify who is sharing company-confidential documents with which users in these organizations, which you can do when the document (or email) is protected by the Azure Rights Management service.

## When I share a protected document with somebody outside my company, how does that user get authenticated?

By default, the Azure Rights Management service uses an Azure Active Directory account and an associated email address for user authentication, which makes business-to-business collaboration seamless for administrators. If the other organization uses Azure services, users already have accounts in Azure Active Directory, even if these accounts are created and managed on-premises and then synchronized to Azure. If the organization has Office 365, under the covers, this service also uses Azure Active Directory for the user accounts. If the user's organization doesn't have managed accounts in Azure, users can sign up for [RMS for individuals](#), which creates an unmanaged Azure tenant and directory for the organization with an account for the user, so that this user (and subsequent users) can then be authenticated for the Azure Rights Management service.

The authentication method for these accounts can vary, depending on how the administrator in the other organization has configured the Azure Active Directory accounts. For example, they could use passwords that were created for these accounts, federation, or passwords that were created in Active Directory Domain Services and then synchronized to Azure Active Directory.

Other authentication methods:

- If you protect an email with an Office document attachment to a user who doesn't have an account in Azure AD, the authentication method changes. The Azure Rights Management service is federated with some popular social identity providers, such as Gmail. If the user's email provider is supported, the user can sign in to that service and their email provider is responsible for authenticating them. If the user's email provider is not supported, or as a preference, the user can apply for a one-time passcode that authenticates them and displays the email with the protected document in a web browser.
- Azure Information Protection can use Microsoft accounts for supported applications. Currently, not all applications can open protected content when a Microsoft account is used for authentication. [More information](#)

## Can I add external users (people from outside my company) to custom templates?

Yes. The [protection settings](#) that you can configure in the Azure portal let you add permissions to users and groups from outside your organization, and even all users in another organization. You might find it useful to reference the step-by-step example, [Secure document collaboration by using Azure Information Protection](#).

Note that if you have Azure Information Protection labels, you must first convert your custom template to a label before you can configure these protection settings in the Azure portal. For more information, see [Configuring and](#)

managing templates for Azure Information Protection.

Alternatively, you can add external users to custom templates (and labels) by using PowerShell. This configuration requires you to use a rights definition object that you use to update your template:

1. Specify the external email addresses and their rights in a rights definition object, by using the [New-AipServiceRightsDefinition](#) cmdlet to create a variable.
2. Supply this variable to the RightsDefinition parameter with the [Set-AipServiceTemplateProperty](#) cmdlet.

When you add users to an existing template, you must define rights definition objects for the existing users in the templates, in addition to the new users. For this scenario, you might find helpful [Example 3: Add new users and rights to a custom template](#) from the [Examples](#) section for the cmdlet.

## What type of groups can I use with Azure RMS?

For most scenarios, you can use any group type in Azure AD that has an email address. This rule of thumb always applies when you assign usage rights but there are some exceptions for administering the Azure Rights Management service. For more information, see [Azure Information Protection requirements for group accounts](#).

## How do I send a protected email to a Gmail or Hotmail account?

When you use Exchange Online and the Azure Rights Management service, you just send the email to the user as a protected message. For example, you can select the new **Protect** button in the command bar in Outlook on the Web, use the Outlook **Do Not Forward** button or menu option. Or, you can select an Azure Information Protection label that automatically applies Do Not Forward for you, and classifies the email.

The recipient sees an option to sign in to their Gmail, Yahoo, or Microsoft account, and then they can read the protected email. Alternatively, they can choose the option for a one-time passcode to read the email in a browser.

To support this scenario, Exchange Online must be enabled for the Azure Rights Management service and the new capabilities in Office 365 Message Encryption. For more information about this configuration, see [Exchange Online: IRM Configuration](#).

For more information about the new capabilities that include supporting all email accounts on all devices, see the following blog post: [Announcing new capabilities available in Office 365 Message Encryption](#).

## What devices and which file types are supported by Azure RMS?

For a list of devices that support the Azure Rights Management service, see [Client devices that support Azure Rights Management data protection](#). Because not all supported devices can currently support all Rights Management capabilities, be sure to also check the table for [RMS-enlighted applications](#).

The Azure Rights Management service can support all file types. For text, image, Microsoft Office (Word, Excel, PowerPoint) files, .pdf files, and some other application file types, Azure Rights Management provides native protection that includes both encryption and enforcement of rights (permissions). For all other applications and file types, generic protection provides file encapsulation and authentication to verify if a user is authorized to open the file.

For a list of file name extensions that are natively supported by Azure Rights Management, see [File types supported by the Azure Information Protection client](#). File name extensions not listed are supported by using the Azure Information Protection client that automatically applies generic protection to these files.

## How do I configure a Mac computer to protect and track documents?

First, make sure that you have installed Office for Mac by using the software installation link from <https://admin.microsoft.com>. For full instructions, see [Download and install or reinstall Office 365 or Office 2019](#)

on a PC or Mac.

Open Outlook and create a profile by using your Office 365 work or school account. Then, create a new message and do the following to configure Office so that it can protect documents and emails by using the Azure Rights Management service:

1. In the new message, on the **Options** tab, click **Permissions**, and then click **Verify Credentials**.
2. When prompted, specify your Office 365 work or school account details again, and select **Sign in**.

This downloads the Azure Rights Management templates and **Verify Credentials** is now replaced with options that include **No Restrictions**, **Do Not Forward**, and any Azure Rights Management templates that are published for your tenant. You can now cancel this new message.

To protect an email message or a document: On the **Options** tab, click **Permissions** and choose an option or template that protects your email or document.

To track a document after you have protected it: From a Windows computer that has the Azure Information Protection client installed, register the document with the document tracking site by using either an Office application or File Explorer. For instructions, see [Track and revoke your documents](#). From your Mac computer, you can now use your web browser to go to the document tracking site (<https://track.azurerms.com>) to track and revoke this document.

## When I open an RMS-protected Office document, does the associated temporary file become RMS-protected as well?

No. In this scenario, the associated temporary file doesn't contain data from the original document but instead, only what the user enters while the file is open. Unlike the original file, the temporary file is obviously not designed for sharing and would remain on the device, protected by local security controls, such as BitLocker and EFS.

## A feature I am looking for doesn't seem to work with SharePoint protected libraries—is support for my feature planned?

Currently, Microsoft SharePoint supports RMS-protected documents by using IRM protected libraries, which do not support Rights Management templates, document tracking, and some other capabilities. For more information, see the [SharePoint in Microsoft 365 and SharePoint Server](#) section in the [Office applications and services](#) article.

If you are interested in a specific capability that isn't yet supported, be sure to keep an eye on announcements on the [Enterprise Mobility and Security Blog](#).

## How do I configure One Drive in SharePoint, so that users can safely share their files with people inside and outside the company?

By default, as an Office 365 administrator, you don't configure this; users do.

Just as a SharePoint site administrator enables and configures IRM for a SharePoint library that they own, OneDrive is designed for users to enable and configure IRM for their own OneDrive library. However, by using PowerShell, you can do this for them. For instructions, see the [SharePoint in Microsoft 365 and OneDrive: IRM Configuration](#) section in the [Office 365: Configuration for clients and online services](#) article.

## Do you have any tips or tricks for a successful deployment?

After overseeing many deployments and listening to our customers, partners, consultants, and support engineers – one of the biggest tips we can pass on from experience: **Design and deploy simple policies**.

Because Azure Information Protection supports sharing securely with anyone, you can afford to be ambitious with

your data protection reach. But be conservative when you configure rights usage restrictions. For many organizations, the biggest business impact comes from preventing data leakage by restricting access to people in your organization. Of course, you can get much more granular than that if you need to – prevent people from printing, editing etc. But keep the more granular restrictions as the exception for documents that really need high-level security, and don't implement these more restrictive usage rights on day one, but plan for a more phased approach.

## How do we regain access to files that were protected by an employee who has now left the organization?

Use the [super user feature](#), which grants the Full Control usage rights to authorized users for all documents and emails that are protected by your tenant. Super users can always read this protected content, and if necessary, remove the protection or reprotect it for different users. This same feature lets authorized services index and inspect files, as needed.

## When I test revocation in the document tracking site, I see a message that says people can still access the document for up to 30 days—is this time period configurable?

Yes. This message reflects the [use license](#) for that specific file.

If you revoke a file, that action can be enforced only when the user authenticates to the Azure Rights Management service. So if a file has a use license validity period of 30 days and the user has already opened the document, that user continues to have access to the document for the duration of the use license. When the use license expires, the user must reauthenticate, at which point the user is denied access because the document is now revoked.

The user who protected the document, the [Rights Management issuer](#) is exempt from this revocation and is always able to access their documents.

The default value for the use license validity period for a tenant is 30 days and this setting can be overridden by a more restrictive setting in a label or template. For more information about the use license and how to configure it, see the [Rights Management use license](#) documentation.

## Can Rights Management prevent screen captures?

By not granting the [Copy usage right](#), Rights Management can prevent screen captures from many of the commonly used screen capture tools on Windows platforms (Windows 7, Windows 8.1, Windows 10, Windows 10 Mobile) and Android. However, iOS and Mac devices do not allow any app to prevent screen captures. In addition, browsers on any device cannot prevent screen captures. Browser use includes Outlook on the web and Office for the web.

Preventing screen captures can help to avoid accidental or negligent disclosure of confidential or sensitive information. But there are many ways that a user can share data that is displayed on a screen, and taking a screenshot is only one method. For example, a user intent on sharing displayed information can take a picture of it using their camera phone, retype the data, or simply verbally relay it to somebody.

As these examples demonstrate, even if all platforms and all software supported the Rights Management APIs to block screen captures, technology alone cannot always prevent users from sharing data that they should not. Rights Management can help to safeguard your important data by using authorization and usage policies, but this enterprise rights management solution should be used with other controls. For example, implement physical security, carefully screen and monitor people who have authorized access to your organization's data, and invest in user education so users understand what data should not be shared.

## What's the difference between a user protecting an email with Do Not Forward and a template that doesn't include the Forward right?

Despite its name and appearance, **Do Not Forward** is not the opposite of the Forward right, or a template. It is actually a set of rights that include restricting copying, printing, and saving the email outside the mailbox, in addition to restricting the forwarding of emails. The rights are dynamically applied to users via the chosen recipients, and not statically assigned by the administrator. For more information, see the [Do Not Forward option for emails](#) section in [Configuring usage rights for Azure Information Protection](#).

# Information and support for Azure Information Protection

7/20/2020 • 5 minutes to read • [Edit Online](#)

Applies to: [Azure Information Protection](#), [Office 365](#)

## NOTE

To provide a unified and streamlined customer experience, **Azure Information Protection client (classic)** and **Label Management** in the Azure Portal are being **deprecated** as of **March 31, 2021**. This time-frame allows all current Azure Information Protection customers to transition to our unified labeling solution using the Microsoft Information Protection Unified Labeling platform. Learn more in the official [deprecation notice](#).

Use the following resources to help you learn about, deploy, and support Azure Information Protection for your organization.

TO DO THIS ...	...DO THIS:
Learn about new and upcoming releases	See the <a href="#">Information about new releases and updates</a> section on this page.
Get help with the product	See the <a href="#">Support options and community resources</a> section on this page.
Check subscription information and what features are supported	Use the subscription information and feature list from the <a href="#">Azure Information Protection Pricing</a> page.
See commonly asked questions about licensing answered	Read through the <a href="#">frequently asked questions</a> for licensing.
Request a new feature or change of functionality	Visit the <a href="#">UserVoice</a> site for Azure Information Protection, and use your company email address to sign in.
Engage with the product team and your peers	Visit the <a href="#">Yammer site</a> for Azure Information Protection.
Understand a specific Azure Information Protection term	Search for the term or abbreviation on the <a href="#">terminology</a> page.

## Information about new releases and updates

The official roadmap for Azure Information Protection is now on the [Microsoft 365 Roadmap](#).

The Azure Information Protection product team posts announcements about major new releases on the [Enterprise Mobility + Security blog](#). Smaller releases are announced on the Azure Information Protection [Yammer site](#), and you might also find it useful to check the [UserVoice site](#) for the status of requested features.

You'll find additional and more detailed information on the [Azure Information Protection technical blog](#).

## What's new in the documentation

The Azure Information Protection technical blog also has a summary of [documentation changes each month](#).

These changes can include new and updated documentation for new release, changes to support statements, and also corrections and clarifications for existing releases.

These doc updates posts are titled: "Azure Information Protection Documentation Update for <month year>".

## Support options and community resources

The following sections provide information about support and troubleshooting options, and community resources.

### To contact Microsoft Support

If you have Premier Support, visit the [Microsoft Services Hub](#) to submit incidents, browse solutions, and get help.

You might be eligible for **FastTrack**: You can use the FastTrack Center Benefit when you purchase at least 150 licenses in an eligible plan for Azure Information Protection. The FastTrack Center Benefit lets you work with Microsoft specialists to assess, remediate, and enable eligible services. For more information, see [FastTrack Center Benefit for Enterprise Mobility + Security \(EMS\)](#).

For other customers, use the support channels in the following table, depending on your subscription for Azure Information Protection.

SUBSCRIPTION	INSTRUCTIONS
Azure Information Protection (standalone)	<ol style="list-style-type: none"><li>1. Select <b>New support request</b> from <a href="#">Help + support</a> in the Azure portal.</li><li>2. When you are prompted, on the <b>Basics</b> pane, choose <b>Technical</b> for the <b>Issue type</b> and <b>Information Protection</b> for the service.</li><li>3. In addition, make sure that one of the following options is selected:<ul style="list-style-type: none"><li>- <b>Subscription with technical support included:</b> You see this option if you have a paid or trial subscription for Azure.</li><li>- <b>Technical support - Included:</b> You see this option if you don't have an Azure subscription.</li></ul></li></ol>
Azure Information Protection and an Office 365 subscription Azure Rights Management with an Office 365 subscription	See <a href="#">Contact support for business products - Admin Help</a> for information about how to contact Support by using the Microsoft 365 admin center, and for contact telephone numbers.
Azure Information Protection with Enterprise Mobility + Security (EMS)	<ol style="list-style-type: none"><li>1. Select <b>New support request</b> from <a href="#">Help + support</a> in the Azure portal.</li><li>2. When you are prompted, on the <b>Basics</b> pane, choose <b>Technical</b> for the <b>Issue type</b> and <b>Information Protection</b> for the service.</li><li>3. In addition, make sure that one of the following options is selected:<ul style="list-style-type: none"><li>- <b>Subscription with technical support included:</b> You see this option if you have a paid or trial subscription for Azure.</li><li>- <b>Technical support - Included:</b> You see this option if you don't have an Azure subscription.</li></ul></li></ol>

SUBSCRIPTION	INSTRUCTIONS
Azure Information Protection with Microsoft 365 Enterprise	Use the <a href="#">Office 365 support channels</a> .

For additional support options, ask your Microsoft contact.

## Self-help

Hands-on labs: See [Azure Information Protection Hands On Lab](#)

On-demand videos:

- Tech Community recorded webinars for [Azure Information Protection](#).
- Microsoft Virtual Academy sessions that include [Azure Information Protection](#).

Troubleshooting:

- If you have a question about how something works: Check whether your question is already answered as a [frequently asked question](#).
- If you have a question about a support statement for Azure Information Protection: See the [Requirements](#) information, which is regularly updated.
- For information to support your end users, help desk, and administrators who are configuring services and applications that use the protection service from Azure Information Protection: See [Helping users to protect files](#).
- If you have deployed the Rights Management connector for your on-premises servers: See the [monitoring](#) information, which includes details about event log entries, performance counters, and logging.
- For the Azure Information Protection client:
  - Unified labeling client: See the [Installation checks and troubleshooting](#) section from this client's administrator guide, and confirm that you're using a [supported version](#). If there's a preview version available, try that to see if it fixes the issue—not all fixes are listed in the version history.
  - Classic client: See the [Installation checks and troubleshooting](#) section from this client's administrator guide, and confirm that you're using a [supported version](#). If there's a preview version available, try that to see if it fixes the issue—not all fixes are listed in the version history.

## Community resources

We recommend the [Yammer site for Azure Information Protection](#). This resource provides direct responses from the Azure Information Protection team in addition to the benefit of shared experience and knowledge from other admins and consultants.

If you don't have access to this site, try the [Tech Community space for Azure Information Protection](#), or the [TechNet forum for Microsoft RMS \(Cloud\)](#).

# Compliance and supporting information for Azure Information Protection

12/8/2019 • 2 minutes to read • [Edit Online](#)

Azure Information Protection supports other services and also relies on other services. If you're looking for information that is related to Azure Information Protection but not about how to use the Azure Information Protection service, check the following resources:

## Suitability for different countries

Given the variability between laws and regulations in different countries, different use cases and scenarios, and the varying requirements between different business sectors, you will need to consult your legal adviser to help you answer whether Azure Information Protection is suitable for your country.

However, some relevant information that can help your legal adviser make a determination:

- Azure Information Protection uses AES 256 and AES 128 to encrypt documents. [More information](#)
- All encryption keys used by Azure Information Protection are protected with a customer-specific root key that uses RSA 2048 bits. RSA 1024 bits is also supported for backwards compatibility. [More information](#)
- Customer-specific root keys are either managed by Microsoft or provisioned by the customer in a nCipher HSM by using "bring your own key" (BYOK). Azure Information Protection also supports limited functionality with an on-premises key by using "hold your own key" (HYOK) for content that is affected by requirements that indicate that it should not be protected with a cloud-based key.
- The Azure Information Protection service is hosted in regional data centers across the globe. Azure Information Protection keys and policies always remain within the region in which is originally deployed.
- Azure Information Protection does not transmit document contents from clients to the Azure Information Protection service. Content encryption and decryption operations are performed in-place in the client device. Or, for service-based rendering, these operations are performed within the service that's rendering the content. [More information](#)

## Legal and privacy

- For Microsoft Azure agreement information: [Microsoft Azure Agreement](#)
- For Microsoft Azure privacy information: [Microsoft Azure Privacy Statement](#)

## Security, compliance, and auditing

See the [Security, compliance, and regulatory requirements](#) section in the [What problems does Azure RMS solve?](#) article, for information about specific certifications for the Azure Rights Management service. In addition:

- For external certifications for Azure Information Protection: [Microsoft Azure Trust Center](#)
- For FIPS 140 information: [FIPS 140 Validation](#)

For in-depth technical information about how the protection technology works, see [How does Azure RMS work?](#)

## Service level agreements

- [SLA for Azure Information Protection](#)
- [SLA for Azure Active Directory](#)
- [SLA for Azure Key Vault](#)

## Documentation

- Azure Active Directory documentation: [Azure Active Directory](#)
- Office 365 Enterprise documentation: [Office 365](#)

# Azure Information Protection audit log reference (public preview)

7/20/2020 • 5 minutes to read • [Edit Online](#)

Applies to: [Azure Information Protection](#), [Office 365](#)

Microsoft Azure Information Protection generates audit logs at the following activity events:

- [Access](#)
- [Access denied](#)
- [Change protection](#)
- [Discover](#)
- [Downgrade label](#)
- [File removed](#)
- [New label](#)
- [New protection](#)
- [Remove label](#)
- [Remove protection](#)
- [Upgrade label](#)

## Access audit logs

Access audit logs are generated for the following activities:

REPORTED BY	PLATFORM	APPLICATION	ACTION / DESCRIPTION
Azure Information Protection: - Classic client - Unified labeling client	Windows	Office	Generated for the first time in each session that a labeled or protected file is saved. The log includes any information type matches.
Azure Information Protection: - Classic client - Unified labeling client	Windows	Office	Generated each time a labeled or protected file is created.

REPORTED BY	PLATFORM	APPLICATION	ACTION / DESCRIPTION
Azure Information Protection: - Classic client - Unified labeling client	Windows, SharePoint, OneDrive	Office	Generated each time a labeled or protected file is opened. <b>Note:</b> For protected files, Access audit logs are generated only when the file is opened and the content is successfully decrypted and exposed to the user. For protected emails in Outlook, Access audit logs are also generated each time the user attempts to open an encrypted email, even if the decryption is blocked due to a lack of permissions.
Microsoft Information Protection (MIP) SDK	Any	Third-party applications	Generated each time a labeled or protected file is accessed by a third-party application that supports it.
RMS service	Windows	Office	Generated each time a labeled or protected document is accessed.

## Access denied audit logs

**Access denied** audit logs are generated for the following activities:

REPORTED BY	PLATFORM	APPLICATION	ACTION / DESCRIPTION
RMS service	Windows	Office	Generated each time a user attempts to access a protected document for which they have no permissions.

## Change protection audit logs

**Change protection** audit logs are generated for the following activities:

REPORTED BY	PLATFORM	APPLICATION	ACTION / DESCRIPTION
Azure Information Protection: - Classic client - Unified labeling client	Windows, SharePoint, OneDrive	Office	Generated each time the protection on an unlabeled document is changed manually.
Microsoft Information Protection (MIP) SDK	Any	Third-party applications	Generated each time the protection on an unlabeled document is changed manually. Generated only if supported by the third-party application.

## Discover audit logs

Discover audit logs are generated for the following activities:

REPORTED BY	PLATFORM	APPLICATION	ACTION / DESCRIPTION
Azure Information Protection: - Classic scanner - Unified labeling scanner	Windows	Office	Generated each time a file is scanned by the AIP scanner. The log includes the following details: - Matched information types - Labels
Microsoft Information Protection (MIP) SDK	Any	Third-party applications	Generated each time a file is scanned by a third-party application that supports it. The log includes the following details: - Matched information types - Labels

## Downgrade label audit logs

Downgrade label audit logs are generated for the following activities:

REPORTED BY	PLATFORM	APPLICATION	ACTION / DESCRIPTION
Azure Information Protection: - Classic scanner and client - Unified labeling scanner and client	Windows, SharePoint, One Drive	Office	Generated each time a document label is updated with a less sensitive label.
Microsoft Defender ATP	Windows	OS	Generated each time a document label is updated with a less sensitive label.
Microsoft Information Protection (MIP) SDK	Any	Third-party applications	Generated each time a document label is updated with a less sensitive label. Generated only if supported by the third-party application.

## File removed audit logs

### NOTE

File removed audit logs are supported only in Azure Information Protection scanner version [2.7.96.0](#) and later.

File removed audit logs are generated for the following activities:

REPORTED BY	PLATFORM	APPLICATION	ACTION / DESCRIPTION
Azure Information Protection scanner, Unified labeling client	Windows	Office and supported file types	Generated each time the AIP scanner detects that a previously scanned file has been removed.

## New label audit logs

New label audit logs are generated for the following activities:

REPORTED BY	PLATFORM	APPLICATION	ACTION / DESCRIPTION
Azure Information Protection: - Classic scanner and client - Unified labeling scanner and client	Windows, SharePoint, One Drive	Office	Generated each time new label is applied.
Microsoft Defender ATP	Windows	OS	Generated each time a new document label is applied.
Microsoft Information Protection (MIP) SDK	Any	Third-party applications	Generated each time a new document label is applied. Generated only when supported by the third-party application.

## New protection audit logs

New protection audit logs are generated for the following activities:

REPORTED BY	PLATFORM	APPLICATION	ACTION / DESCRIPTION
Azure Information Protection: - Classic client - Unified labeling client	Windows, SharePoint, One Drive	Office	Generated each time protection is newly added manually, without a label.
Microsoft Information Protection (MIP) SDK	Any	Third-party applications	Generated each time protection is newly added manually, without a label. Generated only when supported by the third-party application.

## Remove label audit logs

Remove label audit logs are generated for the following activities:

REPORTED BY	PLATFORM	APPLICATION	ACTION / DESCRIPTION
Azure Information Protection: - Classic scanner and client - Unified labeling scanner and client	Windows, SharePoint, One Drive	Office	Generated each time a label is removed.
Microsoft Defender ATP	Windows	OS	Generated each time a label is removed.
Microsoft Information Protection (MIP) SDK	Any	Third-party applications	Generated each time a label is removed. Generated only when supported by the third-party application.

## Remove protection audit logs

Remove protection audit logs are generated for the following activities:

REPORTED BY	PLATFORM	APPLICATION	ACTION / DESCRIPTION
Azure Information Protection: - Classic client - Unified labeling client	Windows, SharePoint, One Drive	Office	Generated each time protection is manually removed, without a label.
Microsoft Information Protection (MIP) SDK	Any	Third-party applications	Generated each time protection is manually removed, without a label. Generated only when supported by the third-party application.

## Upgrade label audit logs

Upgrade label audit logs are generated for the following activities:

REPORTED BY	PLATFORM	APPLICATION	ACTION / DESCRIPTION
Azure Information Protection: - Classic scanner and client - Unified labeling scanner and client	Windows, SharePoint, One Drive	Office	Generated each time a document label is updated with a more sensitive label.
Microsoft Defender ATP	Windows	OS	Generated each time a document label is updated with a more sensitive label.
Microsoft Information Protection (MIP) SDK	Any	Third-party applications	Generated each time a document label is updated with a more sensitive label. Generated only when supported by the third-party application.



# Terminology for Azure Information Protection

7/20/2020 • 9 minutes to read • [Edit Online](#)

Applies to: [Azure Information Protection](#), [Office 365](#)

Confused by a word, phrase, or acronym that's related to Microsoft Azure Information Protection? Find the definition here for terms and abbreviations that are either specific to Azure Information Protection or have a specific meaning when used in the context of this service.

## Word, phrase, or acronym

TERM	DEFINITION
AADRM	The name of the first PowerShell module for the protection service (Azure Rights Management), which was derived from the unofficial abbreviation for Azure Rights Management when it was previously named (Windows) Azure Active Directory Rights Management. This PowerShell module is now replaced with the AIPService module.
activate	To enable the protection service (Azure Rights Management) so that an organization can protect their documents and email. This action also enables IRM features in Exchange Online and Microsoft SharePoint.
Active Directory Rights Management Services	Frequently abbreviated to <i>AD RMS</i> .  A Windows Server role that provides rights management protection by using encryption and policy to help secure documents, files, and email.
AD RMS	See <i>Active Directory Rights Management Services</i> .
AIPService	The current name of the PowerShell module for the protection service, which replaces with the older, AADRM module.
AzureInformationProtection	The name of the PowerShell module for the Azure Information Protection client (classic) and the Azure Information Protection unified labeling client.
Azure Information Protection	A cloud-based service that uses labels to classify and protect documents and emails. Azure Rights Management provides the protection by using encryption, identity, and authorization policies.
Azure Information Protection client (classic)	Sometimes abbreviated to <i>classic client</i> .  The original client side of Azure Information Protection that lets users, administrators, and services use the labels and settings from your Azure Information Protection policy. Now being replaced with the Azure Information Protection unified labeling client.

TERM	DEFINITION
Azure Information Protection label	An item that always applies a classification value to documents and emails, and can also protect them. When a label is applied, the label information is stored in the metadata for applications and services to read and optionally, act on it.
Azure Information Protection policy	Administrator-defined configuration for clients and services that use Azure Information Protection labels and policy settings.
Azure Information Protection scanner	A service that runs on Windows Server and lets you discover, classify, and protect documents on network shares, and SharePoint Server sites and libraries.
Azure Information Protection unified labeling client	<p>Sometimes abbreviated to <i>unified labeling client</i>.</p> <p>The client for Windows computers that lets users, administrators, and services use the sensitivity labels and label policy settings from the Office 365 Security &amp; Compliance Center, the Microsoft 365 security center, and the Microsoft 365 compliance center. Replaces the Azure Information Protection client (classic).</p>
Azure RMS	See <i>Azure Rights Management</i> .
Azure Information Protection viewer	An app that runs on Windows computers and mobile devices, to display protected files.
Azure Rights Management	<p>Frequently abbreviated to <i>Azure RMS</i>.</p> <p>An Azure service used by Azure Information Protection that uses encryption and policy to help secure documents, files, and email. Also known as <i>Azure Rights Management service</i>. Previous names have included:</p> <ul style="list-style-type: none"> <li>- <i>Windows Azure Active Directory Rights Management</i>: Frequently abbreviated to Windows Azure AD Rights Management Service.</li> <li>- <i>RMS Online</i>: The original, proposed name, which you might sometimes see in error messages and log file entries.</li> </ul>
default template	A protection template that is automatically created for you when you obtain a subscription for Azure Information Protection, so that you can immediately start protecting documents and emails that contain sensitive information.
BYOK	See <i>bring your own key</i> .
bring your own key	<p>Frequently abbreviated to <i>BYOK</i>.</p> <p>A configuration and topology option chosen by an organization that wants to generate and manage their own tenant key for Azure Information Protection.</p>

TERM	DEFINITION
built-in labeling	An Office 365 app or service capability to support sensitivity labels without the requirement to install an additional labeling client. Also known as <i>native labeling</i> .
content key	A unique key that is created by RMS-enlightened applications for each document or email that is protected by using Rights Management and that helps to limit the risk of information disclosure.
consume	<p>In the context of protection only: To open a document or email to read or use it when that content has been protected by a rights management service. For a document, consuming includes editing and adding new content to a protected document. For an email message, consuming includes replying to a protected message.</p> <p>In the context of labeling (with or without protection): To read and potentially act on the label information stored in the metadata of files and emails.</p>
deactivate	To disable the Rights Management service so that the organization can no longer use Azure Information Protection.
departmental template	A protection template that you create and that is configured to be visible for selected users rather than all users in your organization. Also known as a <i>scoped template</i> .
enlightened applications	Applications that natively support Rights Management, which includes Office applications, such as Word and Excel. Independent software vendors (ISVs) and developers can also write applications that natively support Rights Management.
enterprise rights management	An industry-standard, generic term that is often used to describe products and solutions that help organizations protect sensitive or valuable information by using a combination of encryption and policy authorization tools. Azure Information Protection is an example of an enterprise rights management (ERM) solution.
ERM	See <i>enterprise rights management</i> .
generic protection	A level of protection that encrypts any file type and prevents unauthorized people from opening the file. After the file is opened, the file is now unencrypted and usable in an application that doesn't natively support Rights Management.
HYOK	See <i>hold your own key</i> .
hold your own key	<p>Frequently abbreviated to <i>HYOK</i>.</p> <p>A configuration and topology option for an organization that wants to generate and store their own key on-premises, typically for regulatory or compliance reasons.</p>

TERM	DEFINITION
key object	In the context of the tenant key, an entity that contains metadata that is required by the Azure Rights Management service for cryptographic operations.
label	See <i>Azure Information Protection label</i> .
information protection	<p>Sometimes abbreviated to <i>IP</i>.</p> <p>An industry-standard, generic term that refers to protecting data and files from unauthorized access, even after the data and files leave the organizational boundaries by using email or document sharing. Microsoft Azure Information Protection is an example of an information protection (IP) solution.</p>
Information Rights Management	<p>Frequently abbreviated to <i>I/RM</i>.</p> <p>A term used in conjunction with Office services, such as Exchange Server, Word, and SharePoint, to describe the ability to support the Microsoft Rights Management services.</p>
IRM	See <i>Information Rights Management</i> .
Office Message Encryption	<p>Frequently abbreviated to <i>OME</i>.</p> <p>The new Office 365 Message Encryption capabilities have native integration with the Azure Rights Management service to provide the same email protection for internal and external users, automatic refresh of templates, and support for the bring your own key (BYOK) scenario. The previous OME implementation was designed for external recipients only, required a mail flow rule, and did not support BYOK.</p>
Microsoft Information Protection	<p>Sometimes abbreviated to <i>MIP</i>.</p> <p>A framework for products and integrated capabilities that use the same labeling store ("unified labels") and help you protect your organization's sensitive information.</p>
MIP	See <i>Microsoft Information Protection</i>
MSDRM	Sometimes seen as references for the RMS client 1.0, which is replaced with the newer client, MSIPC. This older client supports applications that are developed with the RMS SDK 1.0 and supports Office 2010 and Office 2007, Exchange 2010 and Exchange 2013, and SharePoint 2010 and SharePoint 2007.
MSIPC	Sometimes seen as references for the RMS client 2.0, which replaced the older RMS client, MSDRM. This later client supports applications that are developed with the RMS SDK 2.0 and supports Office 365 ProPlus, Office 2019, Office 2016, Office 2013, SharePoint 2013, and the Azure Information Protection client.

TERM	DEFINITION
native protection	A level of protection available in all enlightened applications that prevents unauthorized people from opening a file and that can also enforce more stringent policies, such as read-only, and do not print. In addition, this protection stays with the file, even when the file is forwarded to other people or saved in a public location that others can access.
.pfile	The file name extension that is appended to all files that a rights management service generically protects.
permissions level	A logical grouping of usage rights that make it easier for end-users and administrators to choose configuration options that are role-based. For example, Reviewer and Co-Author.
protect	Apply rights management controls to files or email messages by using encryption, identity, and access control policies to help secure your data.
protection template	<p>Also known as a <i>rights policy template</i>, <i>Rights Management template</i>, and <i>RMS template</i>.</p> <p>A group of protection settings that are managed by an administrator and that include the defined usage rights for authorized users, and access controls for expiry and offline access.</p>
publish	To protect a file in order to safeguard it from unauthorized access and use. Also used as a term in conjunction with protection templates and the Azure Information Protection policy, to make these items available for use by clients and services.
Rights Management connector	An outbound proxy relay that you can deploy for on-premises services such as Exchange Server and SharePoint, to protect data by using the Azure Rights Management service.
Rights Management issuer	The account that protected a document or email.
Rights Management owner	The account that retains full control of a protected document or email by being automatically granted the Rights Management Full Control usage right and is exempt from any expiry date or offline setting.
Rights Management services	The generic term that applies to both the cloud version of Rights Management (Azure Rights Management) and the on-premises version of Rights Management (AD RMS).
Rights Management sharing application	Now replaced by the Azure Information Protection client.
RMS	See <i>Rights Management services</i> .
RMS connector	See <i>Rights Management connector</i> .

TERM	DEFINITION
RMS for individuals	A free subscription for a user to use Rights Management when their organization does not have a subscription to Office 365 or Azure Active Directory.
RMS sharing app	See <i>Rights Management sharing application</i> .
RMS template	See <i>protection template</i> .
protection-only mode	An operational mode for the Azure Information Protection client when there is no Azure Information Protection policy to apply labels. In this mode, classification labels are not displayed but users can still apply Rights Management protection.
scanner	See <i>Azure Information Protection scanner</i> .
super user	A group of highly trusted administrators who can decrypt and access files that the organization has protected by using a rights management service. Typically, this level of access is required for legal eDiscovery and by auditing teams.
tenant key	<p>Also known as the <i>server licensor certificate (SLC) key</i>.</p> <p>The key that is unique to an organization and ultimately secures all Rights Management cryptographic functions that chain to this tenant key.</p>
unified label	<p>Also known as <i>unified sensitivity label</i>.</p> <p>A label that can be applied by apps, clients, and services that support the Microsoft Information Protection framework, to apply classification and optionally, protection. In Office apps and services, unified labels are implemented as sensitivity labels.</p>
unprotect	Remove protection controls from files or email messages, which used encryption, identity, usage rights, and access control policies to help secure your data.
use license	A per-document certificate that is granted to a user who opens a file or email message that has been protected by a rights management service. This certificate contains that user's rights for the file or email message and the encryption key that was used to encrypt the content, as well as additional access restrictions defined in the document's policy.