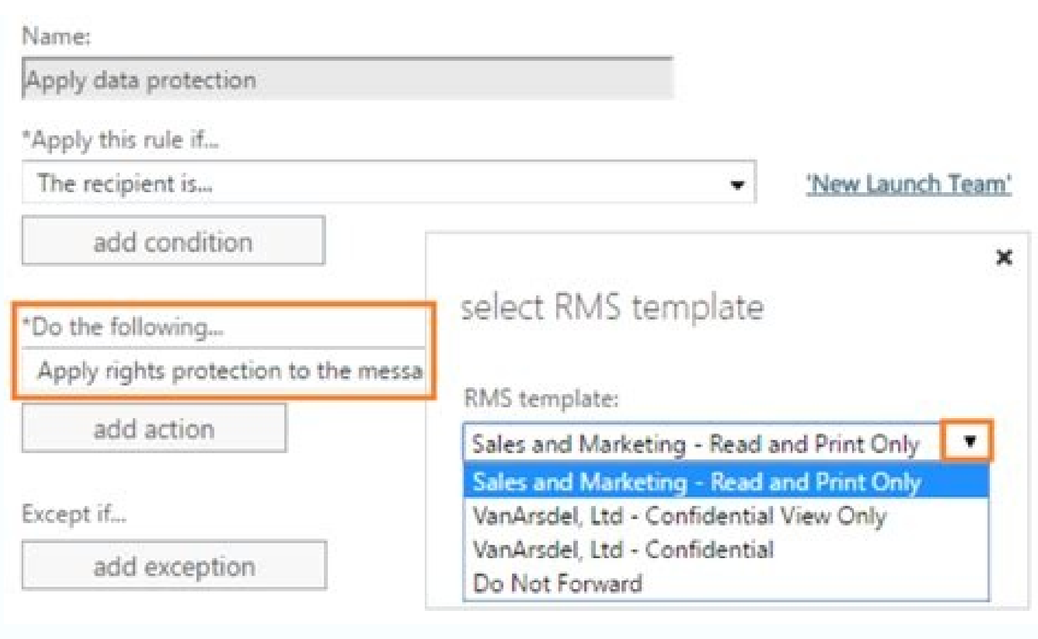
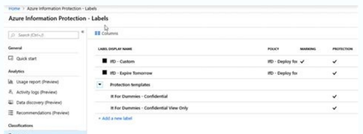
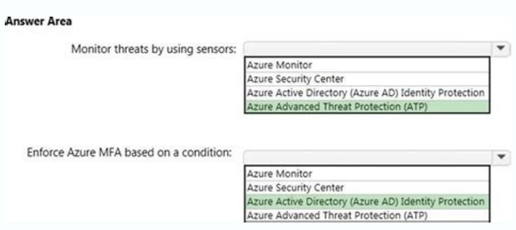
Azure information protection service excel

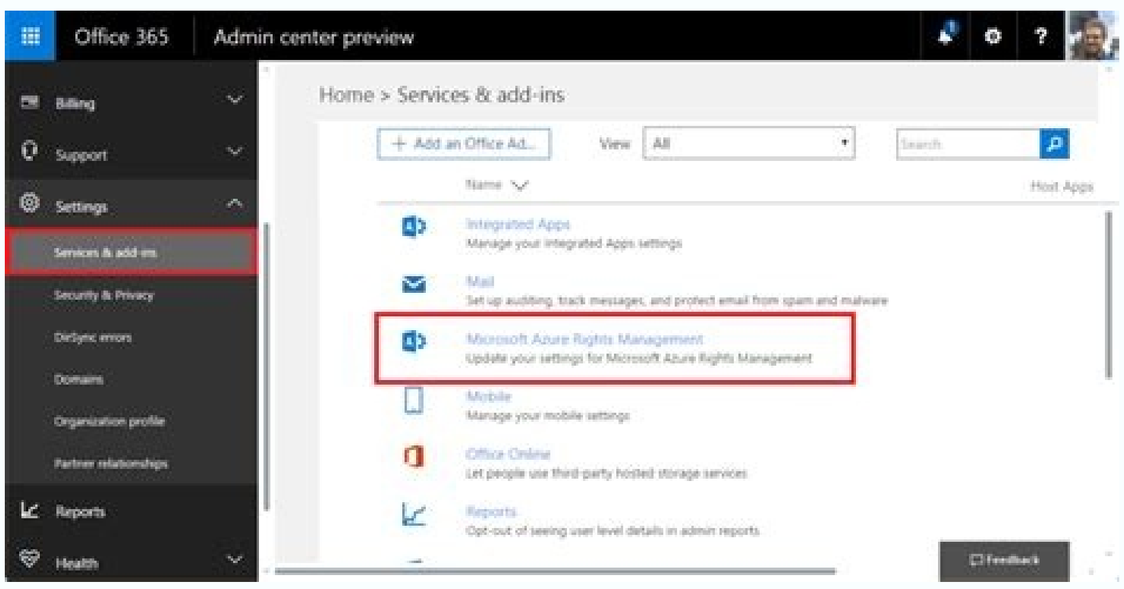
Continue





Answer Area





Included with our Microsoft license is Azure Information Protection (AIP). AIP is a Windows plugin that classifies, protects and encrypts documents before sending them in email or posting them on a website. If you do not have a Windows computer you can still view protected files by installing the AIP Viewer App. If you need to protect email messages before sending them, both Mac and Windows machines may use Google Mail's Confidential Mode. Please note Confidential Mode is not an encryption service. AIP ensures that only specific people can open documents even when these files are accidentally forwarded as buried attachments in email. Microsoft AIP also lets you revoke access, lets you see who opened your files and provides email notifications when someone accesses them or can't open a file. AIP works like a plugin in your Word, Excel, PowerPoint or Outlook menus. Microsoft overview of Azure Information Protection (AIP) Ensure that files you send over email are only opened by intended recipients regardless if the email is forwarded to others. Let your recipients know how sensitive this document is and protect it from being printed or copied. Many types of files can be protected. If you are sending a file to someone who does not have a Microsoft account they may download a viewer to look at the file. Includes Windows OS, Surface Pro, and Windows Phones. Windows devices can protect as well as access protected files. Recipients of protected, non-Microsoft files (PDF, TXT, Images) may not be able to open the file unless they have the Azure Information Protection client (plugin) or Azure Information Protection Viewer app installed. Recipients should be instructed to download the AIP Viewer app when being sent a protected file. There are no additional resources available for this service. The Division of Information Technology provides support on all of our services. If you require assistance please submit a support ticket through the IT Service Management system. Submit A Quick Ticket Electronic record management, especially documents and emails, is often one of the biggest pain points for both large and small organizations. Think about how many emails you send and receive throughout the course of a day. Your job role may require you to reference various documents housed within the organization. Proper categorization and security are significant concerns, especially when it comes to improper password protection or other human errors that can lead to a data breach. That's what Azure Information Protection works to address. What is Azure Information Protection? Azure Information Protection (AIP) is a subscription-based cloud product from Microsoft that assists organizations by applying labels to documents and emails to help with categorizing, discovering, classifying, and protecting those electronic records. AIP is one piece of the overall Microsoft Information Protection (MIP) framework. You can use AIP directly within Office 365 to provide encryption security to an outgoing message. The solution protects documents created using Office products like Excel, Word, and PowerPoint. AIP protects electronic records kept on your desktop or in the cloud. How Does Azure Information Protection Work? Many organizations find themselves shifting to a model where a large part of their workforce requires remote access to the company network. It's common for businesses to store a lot of their information in the cloud. AIP protects documents throughout their entire lifecycle, regardless of the point of creation. Organizations need a way of protecting sensitive information from getting into the wrong hands. If an employee accidentally leaves a company thumbnail at a coffee shop, you don't want hackers gaining access to information that could compromise your company's security infrastructure. AIP lets organizations set up role-based access to sensitive information. You control everything from which users can view specific documents to who can send them out via email transmission. If someone leaves the company or moves into a different role, AIP lets you revoke that user's document permissions. With AIP, organizations can stop individuals from illegally modifying, storing, and distributing documents and emails containing critical business data. It also keeps unauthorized users from viewing content meant for others in specific company roles. AIP helps companies meet any regulatory data protection obligations and compliance standards required by their industry. What Do I Need to Work with Azure Information Protection? To get started, you need to sign up for an AIP plan to take advantage of the solution's labeling, classification, and protection features. Organizations must have Azure Active Directory (AD) set up. Client devices must run an operating system capable of supporting Azure Information Protection. Clients capable of running AIP Include: Windows 10 Windows 8.1 Windows 8 Windows Server 2019 Windows Server 2016 Windows Server 2012 R2 Windows Server 2012 If you plan on using AIP on a virtual machine, verify whether any software installed on the virtual desktop has additional configuration requirements for AIP unified labeling or the client. Citrix solutions may require you to disable API hooks for AIP components that use files like: Winword.exe Excel.exe Outlook.exe Powerpnt.exe Msip.app.exe Msip.viewer.exe You can use API clients to label and protect document and emails for Word, PowerPoint, Outlook, and Excel from the following Office editions: Office 365 Business Office 365 for Enterprise Office Professional Plus 2019 Office Professional Plus 2016 Office Professional Plus 2013 SP 1 Office Professional Plus 2010 SP 2 How Do I Label Documents and Emails for Tracking? With AIP, you can add a classification and protect documents at the time of creation or when editing them inside Word, Excel, PowerPoint, or Outlook. File Explorer lets you classify and protect additional file types and work with multiple files at once. Keep in mind that you may not be able to save protected documents to SharePoint or OneDrive. Check with admins to confirm if they've enabled sensitivity labels for those solutions. AIP lets you create labels specifically for sending protected documents to people outside of your organization. That feature becomes useful when you need to send communications to regular B2B customers. Any documents sent via restricted emails receive the same level of protection. How Do I Track and Revoke Access with Azure Information Protection? The document tracking feature in AIP tells administrators who accessed protected documents. It's possible to give both admins and users the right to revoke access to tracked documents. You can do this even if you don't label the documents. Users can revoke access to a document from Word, Excel, and PowerPoint by clicking the Sensitivity button, then selecting Revoke Access. However, they may still be able to view the document if you've made it available for offline viewing. Incorporate Azure Information Protection into Your Organization Azure Information Protection gives organizations more control over the security of company emails and documents. Internet eBusiness Solutions can help you configure AIP within your Office 36 installation. Set up a consultation with us today and learn more about the benefits of Azure Information Protection. This superbly located eatery sits by the entrance of Buža II and quickly went to number one on TripAdvisor in its very first season. Here you can tuck into a reasonably priced, Med-and-Asian-influenced main here – fragrant meatballs in a chicken-coconut broth, perhaps, or Adriatic prawn pouches on grilled aubergine in a red-curry-and-coconut sauce – before an afternoon's sunbathing or nightcap overlooking the waves. Starters include mussels in beer butter and chilli and Dalmatian tom yum soup. Microsoft's Azure Information Protection is a cloud solution (referred to as AIP) that gives an organization the power to classify and protect documents, data, and emails with labels. AIP client helps to keep important documents and emails safe from unauthorized parties who shouldn't see them, even if the email is forwarded or documents are saved to another location. The AIP solution is used to classify documents and open documents that other people have protected by using the "Rights Management Protection" technology from Azure. Classifications and policies are defined at the organization level and are enforced by AIP clients. The client checks for any changes whenever a supported Microsoft Office application starts and downloads the changes as its latest Azure Information Protection policy. Users must have Azure Information Protection clients installed on their machines to define classifications and open protected documents. Under Microsoft's Azure Rights Management, documents can be protected even when not in the organization's system. A file can be set to be viewable only to specific individuals even if the file is taken out of the system and distributed elsewhere, thereby keeping the data protected and encrypted even if the document is copied or removed. In this implementation guide, we cover the following four phases of the Information Protection life cycle and provide guidance on how to approach each of these phases.How does Azure Information Protection work?Azure Information Protection is a 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.At a high level, Azure Information Protection protects your data in three key steps:1. First, data is classified and labeled. For example, if a document is classified as confidential and should be available only to the recipients of the email, the label might be "Confidential — Recipients Only."2. Next, data is protected through encryption, access control, and policies based on the label. Continuing with the preceding example, a document marked with the Confidential — Recipients Only label will be encrypted so that only the recipients can read it.3. Finally, documents can be tracked, and access can be revoked if necessary. From the preceding example, the sender of the email may decide that one of the recipients should no longer have access to the document. In that case, the sender can revoke access for a specific user.4. At a high level, 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. 5. Throughout the protection process when Azure RMS is encrypting and decrypting, authorizing, and enforcing restrictions, the secret formula is never sent to Azure. Office 365 Message Encryption, or OME, is one of the features of Azure Information Protection. If you have the AIP Premium P2 license, you can avail yourself of additional functionalities, such as automatic classification for cloud and on-premises data. Here, you discover the features available in the AIP Premium P1 license.What all can be achieved by Azure Information Protection?Azure Information Protection is a cloud-based solution that helps an organization to classify, and optionally protect, its documents and emails by applying labels. Labels can be applied automatically by administrators who define rules and conditions, manually by users, or a combination where users are given recommendations.A number of technologies are behind Azure Information Protection and the classification is achieved through the use of labels, which are now unified across Office 365.Applying protection is achieved either by applying a label that has protection, or by a user choosing to protect certain data.As an example, a user can choose to protect an email by clicking the "Do Not Forward" option.The result is that for the email recipients:· Copy and paste is disabled on protected content· Screenshots do not work· Screen sharing will result in black where the application window would be· Printing is disabled· The forward button does nothing· When replying, you cannot add new recipients to the repliesThis kind of protection can be achieved because the encryption technology is baked into the Office applications. It is not, like a password-protected Zip file, a wrapper around the files. The actual content is protected. Office files such as Word, Excel, and PowerPoint can all be protected using AIP.What are the requirements for Azure Information Protection?1) Licensing Requirements : · Standalone· As part of an Enterprise Mobility + Security (EMS) suite· As part of a Microsoft 365 Enterprise E3 license.You will also need an Office application version that supports the Azure Information Protection features, and that means either:· Office 365 Enterprise E3; or· Office 365 Enterprise E5.2) Azure Active Directory Your organization must have an Azure Active Directory (Azure AD) to support user authentication and authorization for Azure Information Protection. Configuring Single Sign-On (SSO) for Azure AD is also highly recommended for a seamless user experience. Additional details on requirements for Azure AD can be found in our documentation. 3) Network Connectivity A common stumbling block for many AIP deployments are the Firewall and Network Requirements. Azure Information Protection uses a subset of the Office 365 URLs and IP address ranges. We recommend following the guidance in the Office 365 documentation and opening all Required URLs and IP addresses listed under the Microsoft 365 Common and Office Online12 section. One additional callout is that termination of TLS client-to-service connections (for example, packet-level inspection) to the aadrm.com URL will break certificate pinning required by AIP to ensure secure communications with the Microsoft Root Certificate Authority. For those consuming contentIf you are an external recipient, you would need a suitable email address:· Users of Hotmail, Yahoo, or Gmail will be able to log in using those accounts and access content· If the recipient or their company uses Office 365, their email address will be supported without further action· If they use other email addresses (e.g. email provided by their company but not through Office 365), they will need to sign up for an account at a Windows PCOne of the following versions of Microsoft Office:· Office 2013 or later (all editions)· Office 365 ProPlus applications (as included in Office 365 E3, for example)· Office 365 Business applications (as included in Office 365 Business Premium, for example)· Excel Online (supported, but we expect most people will want to use our data in the full desktop applications)· Office 365 Home and PersonalThe recipient or their IT department may have already installed the Azure Information Protection Client, but this is no longer essential for consuming content.Using macOSYou will need one of the following versions of Office:· Office 365 ProPlus: Office 2016· Office Standard 2016 for MacUsing an Android device or an Apple iOS deviceWith Office Mobile or Outlook installed, users should be able to open protected documents without trouble.Using web applicationsSupport for consumption and protection of content using web apps is rolling out across tenants and some features are still in development.How to install Azure Information Protection Client?You can have the greatest policies and labels for Azure Information Protection in Azure, but they'll be no good if your end-users can't see and apply them. The AIP client, a program that is run on the end users' devices, solves this problem.Before you install the AIP client, make sure Office ProPlus is already installed but not running on the device. When you're ready to install the AIP client, do the following:1. Navigate to the Azure Information Protection client download page.The Microsoft Download Center appears.2. Click the Download button.The Choose the Download You Want window is displayed.3. Select AzInfoProtection.exe by selecting the box and then click Next.Downloading the Azure Information Protection client.1. From the notification that pops up at the bottom of your screen, click (or double-click) Run.The system performs a security check on the download. When the check is complete, the Microsoft Azure Information Protection window pops up.Installation window for Azure Information Protection.1. Click the I Agree the button.You can opt to install a demo policy (not recommended because it will clutter your user interface) or send usage statistics to Microsoft or both.2. In the User Account Control window that displays, click Yes to start the installation.You see the progress of the installation.3. When the Microsoft Azure Information Protection window displays Completed Successfully, click the Close button.The installation window disappears, and you're now ready to check that the Azure Information Protection client was successfully installed. To verify the installation, open a blank document in Word. You see the labels below the ribbon.Azure Information Protection labels displayed in Word.How to apply a Label to a Document?Now that the Azure Information Protection client is installed, and the labels are displayed in the Office applications, it's time to put it to the test.1. Create a Word document and pretend that it's highly confidential.2. On the Sensitivity bar, click Highly Confidential and select All Employees.Applying the Highly Confidential/All Employees label.The label is applied, and the other labels will disappear.1. Run Outlook, start a new email and attach the Word document.Note that Outlook displays the Sensitivity bar with the same labels you saw in Word.2. Enter the email address of a user in your organization.Outlook sends the email to the recipients with the Highly Confidential/All Employees label. In this exercise, the email will still go out to both internal and external users. The internal user will be able to open and read the document from the sharing invitation.The external user, however, will be blocked from opening the document and will be presented with the message shown here.An external user blocked from a sensitive document.What are labels in Azure Information Protection?The following is a list of classifications that were defined for CRIF Highmark Depending on Celcom's security requirements, data classification was defined as shown below.Public: The lowest level of data classification that applies to any of the official documents or emails. Users can select the "External" label if the document or email doesn't belong to Internal or Restricted. Proprietor: Internal classification applies for the documents and emails if the information should only be shared within "celcom.com.my" and "axiata.com" domains. Company Confidential: The highest level of classification that applies to highly confidential cooperate information. This classification can be applied to emails or documents if it contains the organization's sensitive information. How to create a new Label in Azure Information Protection?Open a new browser window and sign in to Protection.office.com Then navigate to the Azure Information Protection pane. Revoking access to information in Azure Information ProtectionRevoking access to informationAzure Information Protection protects your company information from falling into the wrong hands — even after it has fallen into the wrong hands.For example, suppose you realize that you accidentally sent a document to the wrong people and want to remedy the situation by revoking all access to the document. Here's what you can do, continuing from the example above:1. Open the protected Word document from the preceding exercise.A yellow bar appears, indicating the sensitivity of the document and containing a button to view the permissions for the document.2. On the Ribbon, click Home and then click the Protect button.A submenu appears below the Protect button.Accessing the document-tracking site.3. On the submenu, click Track and Revoke to launch the document-tracking site.Your browser launches to take you to the document-tracking site.4. If this is the first time you've visited the site, log in with your Microsoft 365 Business credentials.After a successful login, the document-tracking site displays a summary of views of your document. Explore the tabs to see the robust features in Azure Information Protection.The document-tracking site.5. At the bottom of the document-tracking site, click the Revoke access button.The Revoke access page is displayed.6. Click the Confirm button at the bottom of the page.The

Revoke Complete window is displayed.7. Click Continue to go back to the document-tracking page.In the Summary view, the document displays the Revoked stamp.One of the features that are most amazing in this solution is that in the Map tab, you can see where around the world users tried to access your document! So, if you ever find that someone from, say, Russia or Timbuktu tried to open your document even though all your users are in the United States, you'll know that access to the document should be revoked.Is AIP free?AIP can come with certain plans of M365 licenses incorporated. AIP can also be purchased separately as an add-on with a Basic M365 license. Refer to the below image for more clarity.