Rapid Deployment Guide for Azure Rights Management

Microsoft Corporation

Published: December 2015

Updated: February 2016

Version: 1.1

Abstract

The Rapid Deployment Guide helps you quickly deploy and use Azure Rights Management (Azure RMS) by choosing from a list of specific scenarios to implement.

This deployment guide contains both administrator instructions and accompanying end user documentation for Azure Rights Management. Before you give the documentation (instructions or announcements) to your end users, you will need to copy and paste it, and customize it for your business requirements and existing work flows. The guide includes instructions for how to customize the end user documentation with an example that shows how the final end user documentation might look.

Copyright Information

Contents

Rapid Deployment Guide for Azure Rights Management

Use this guide in addition to the technical documentation for Azure Rights Management, to help you deploy and use Azure Rights Management (Azure RMS) by choosing from a list of specific scenarios to implement.

These scenarios contain both administrator instructions and accompanying end user documentation. Before you give the documentation (instructions or announcements) to your end users, you will need to first customize this documentation for your business requirements and existing work flows. An example set of instructions or an announcement show how the final end user documentation might look.

Each scenario has a list of requirements with links to more information if needed, so that you can deploy these solutions independently and in any order.

The scenarios listed here are a sample of the most popular ones. Because Azure RMS can be used to protect information in a large number of scenarios both within an organization and across organizations, you can define your own scenarios and deploy them to your environment and to your users by using this same model. By focusing on specific scenarios, your Azure RMS deployment will more closely align to your business goals. In addition, our experience is that users tend to follow scenario-specific instructions much more closely and systematically than general guidance such as "protect sensitive documents".

Before you roll out these solutions, you might want to send a broad announcement to end users, letting them know that some changes are coming to help protect company data, and that it might require some changes from them. An example communication is included after the following table.

Note

If you have questions and comments about this guide, use the feedback mechanism on the Rapid Deployment Guide for Azure Rights Management page on TechNet, or send an email message to AskIPTeam@Microsoft.com.

Scenarios for Azure RMS

To help you more quickly deploy Azure RMS to address specific business problems, choose the scenarios that most closely match your business goals, and adapt them where necessary.

Scenario	Instructions and end user documentation
Safely email an Office file to users in another organization with the ability to track the resulting accesses (business-to-business collaboration). Examples: • Send a price list, roadmap, or release plans to a customer • Send a work order, or marketing specification to a vendor	Scenario - Share an Office File with Users in Another Organization

Scenario	Instructions and end user documentation
• Send a tender or request for quotation (RFQ) to a partner	
Ensure documents stored in a SharePoint library remain under your control. Examples: • Departmental spreadsheets and reports • Cross-team collaboration for design documents or other deliverables.	Scenario - Retain Control of Documents Stored in SharePoint
Executives can securely exchange privileged information over email. Examples: • Sharing acquisition plans • Discussing or disseminating legal issues • Information about potential layoffs or other sensitive subjects	Scenario - Executives Securely Exchange Privileged Information
Automatically protect all files on a file server. Examples: • CAD documents that must be kept in-house to prevent loss of intellectual property • Marketing promotion plans and dates that must be kept secret from public disclosure to maintain a competitive advantage	Scenario - Protect Files on a File Server Share
Tightly protect your most confidential, high-business impact documents. Examples: • Recipe or formula information that is unique to your company • Highly classified takeover or merger plans • Natural resources exploration data	Scenario - Secure Your Most (Few) Valuable Files
Securely send company-confidential emails and attachments. Examples: • Company vision statement • Organization charts, reorganization news, or promotion announcements • Company policy information	Scenario - Send a Company-Confidential Email

Scenario	Instructions and end user documentation
Apply persistent protection for Office files in Work Folders. Examples: • Locally edited Word documents for a company-confidential project • Locally created spreadsheets that contain sensitive data or high business impact data • Locally stored work-in-progress PowerPoint presentations that must not be leaked or accidentally shared with people outside the organization until the presentations are final	Scenario - Configure Work Folders for Persistent Protection

Announcement for users before rollout

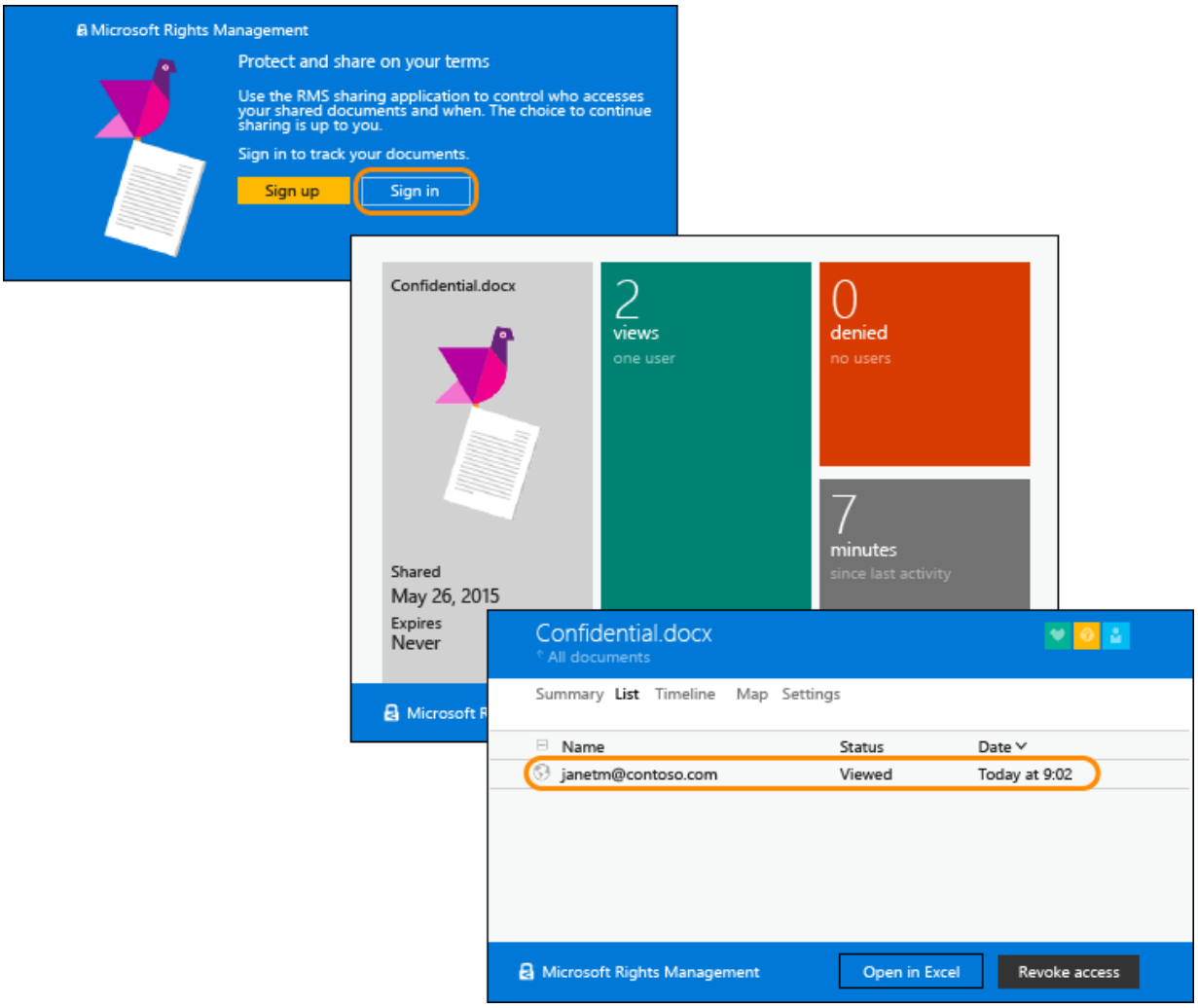
You can use the following example communication message to let users know that deploying Azure RMS means that some changes are on the way. Copy and paste the following text, to be sent by email to all users from somebody in your organization's leadership team, preferably your Chef Executive Officer. Consider making any changes to this text that will make the message more relevant to users and your organization.

Changes we're making to safeguard our data

Have you ever wanted to block access to that document you sent to your partners by mistake? Have you wondered if there’s a way to know which of your customers have read the latest product news you sent? Do you have a need to share confidential product information without concerns that it might be sent on to people who shouldn't see it?

You'll soon be able to do these things because the IT Department is rolling out some changes that implement Microsoft Azure Rights Management (Azure RMS) as an enterprise data protection solution. Many of these solutions will automatically apply the protection that we need, without you having to do anything different. But some changes might require you do some things differently and when this is the case, the IT Department will send you information and instructions, with support from the help desk if you have questions or problems.

For example, to track (and if necessary, revoke) the documents that you share, you'll be using the document tracking site:



For a sneak peak at how this works, have a look at this 2-minute video: [Azure RMS Document Tracking and Revocation]

One of this organization's most valuable assets is its data—the data that we generate, store, and use on a daily basis. It gives us our competitive advantage and helps us be successful. That's why it's so important that we remain in control of our data and ensure that people who should not access it, cannot access it.

The solutions that we're implementing will help us safeguard our valuable data, and give you the tools to keep control of that data. Thank you for your cooperation while we implement these changes.

Scenario - Share an Office File with Users in Another Organization

This scenario and supporting user documentation uses Azure Rights Management so that users can safely email an Office file with people in another organization. For example, the Office file might be a Word document, Excel spreadsheet, or PowerPoint presentation that contains price list information for a partner, a list of products for a reseller, or a list of delivery time lines with potential customers. When users follow the instructions, the file attached to the email message will be protected by Azure Rights Management.

This scenario is suitable for the following set of circumstances:

- The employee has to send information outside the organization, via email, in the form of an Office document attachment.
- The document contains information that is not public, but is not exclusively for internal use.
- The recipient users do not have a requirement to further share this information with others, print it, or use it as part of their own documentation. If this is not the case, you can change the user instructions from selecting view-only permissions to another option that permits the recipient to change the attachment.
- The employee is potentially interested in knowing when this document is opened by the external user.

Deployment Instructions

Make sure that the following requirements are in place before going on to the user documentation.

Requirements for this Scenario

For the user instructions for this scenario to work, the following must be in place:

Check	Requirement	If you need more information
☐	You have prepared accounts and groups for Office 365 or Azure Active Directory	Preparing for Azure Rights Management
☐	Azure Rights Management is activated	Activating Azure Rights Management
☐	The Rights Management sharing application is deployed to users'	Automatic deployment for the Microsoft Rights Management

Check	Requirement	If you need more information
	computers that run Windows	sharing application
☐	Users have Outlook from Office 2013	If users have Office 2010, replace the screen shot with an equivalent version so that the picture matches what users see.
☐	Your Azure RMS subscription includes document tracking	If your subscription for Azure RMS does not include document tracking and revocation, users will not be able to complete all steps in the user instructions. In this case, either purchase a subscription that does support these features, or modify the user instructions to remove the steps that use these features. To check your subscription support: Comparison of Rights Management Services (RMS) Offerings

User Documentation Instructions

Using the following template, copy and paste the user instructions into a communication for your end users, and make these modifications to reflect your environment:

1. Replace <*name of Office document type*> with the type of document that your users will be sending. Use wording that is specific and familiar to their work flows, such as "price list", "delivery times", and "bid proposal" rather than "Word document" and "Excel spreadsheet". This more specific wording helps to increases the likelihood that they will follow the instructions when working with those documents.
2. Replace <*contact details*> with instructions for how your users can contact the help desk, such as a website link, email address, or telephone number.
3. **Additional modifications you might want to make:**
   - In step 2, we suggest **Viewer - View Only** for the permissions, which makes the attached document (but not the original) read-only for the recipients. If this restriction is not suitable for your business requirement, change this option for another set of permissions, such as **Reviewer - View and Edit**.
   - In step 3, we suggest **Allow me to instantly revoke access to these documents** so that there is no delay if your users revoke the document later, but setting this option requires the recipient to always have an Internet connection to open the attachment. This step also requires you to have a subscription that supports document tracking and revocation. Delete this step if it is not suitable for your users.

- In step 4, we suggest the option **Email me when somebody tries to open this document**. If users track their documents by using the document tracking portal, you might decide that email notification is not necessary and delete this step.
- The steps do not include setting an expiration date. If the information should not be used after a specific date, add another step to set an appropriate expiration time, such as 90 days from sending the email message.

Note

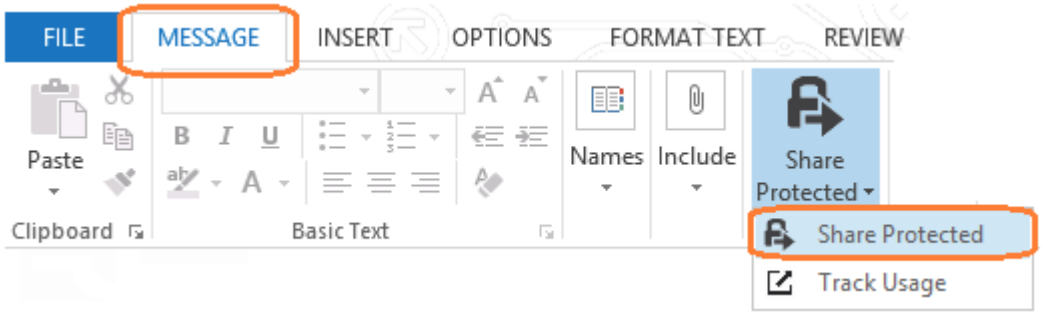
For more information about each of the options that users can select, see Dialog box options for the Rights Management sharing application

4. Make any other modifications that you want to this set of instructions, and then send it to these users.

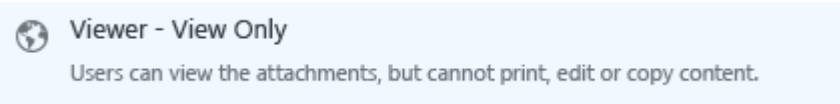
The example documentation shows how these instructions might look for users, after your customizations.

How to share a <name of Office document type>

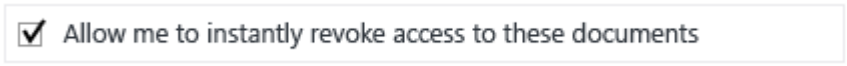
1. Create your email message by specifying the email address or addresses, type your message, and attach the *<name of Office document type>* to the email message. Then, on the **MESSAGE** tab, in the **RMS** group, click **Share Protected** and then click **Share Protected** again:



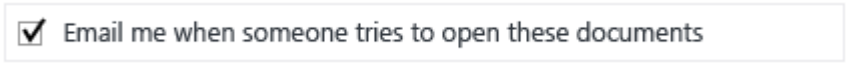
2. In the **share protected** dialog box, Select **Viewer – View Only**:



3. Select **Allow me to instantly revoke access to these documents**:



4. Select **Email me when somebody tries to open these documents**:



5. Click **Send Now**.

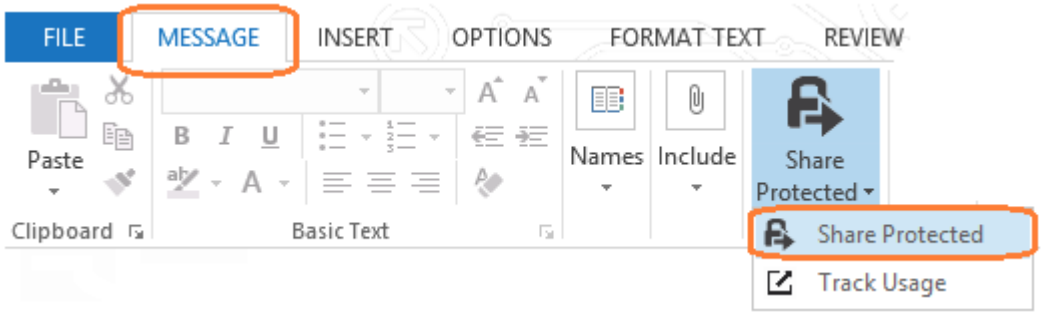
Need help?

- For additional information:
  - Protect a file that you share by email
  - Track and revoke your documents
- Contact the help desk:
  - *<contact details>*

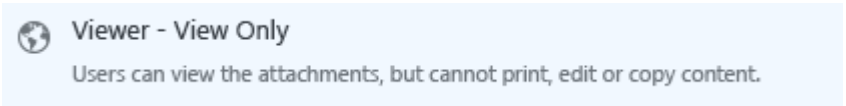
Example Customized User Documentation

How to share a price list with your customer

1. Create your email message by specifying the email address or addresses of your customer, type your message, and attach the latest price list to the email message. Then, on the **MESSAGE** tab, in the **RMS** group, click **Share Protected** and then click **Share Protected** again:

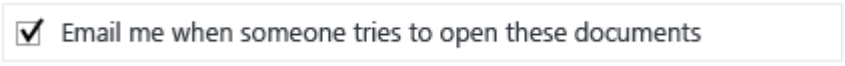


2. In the **share protected** dialog box, Select **Viewer – View Only**:



3. Select **Allow me to instantly revoke access to these documents**:

4. Select **Email me when somebody tries to open these documents**:



5. Click **Send Now**.

Need help?

- For additional information:
  - Protect a file that you share by email
  - Track and revoke your documents
- Contact the help desk:
  - Email: helpdesk@vanarsdelltd.com

Scenario - Retain Control of Documents Stored in SharePoint

This scenario and supporting user documentation uses Azure Rights Management to ensure that Office documents stored in SharePoint remain under your control by using protected libraries. For example, the documents are automatically protected from accidental or intended leakage by users and you can block access to content even after it is downloaded or synchronized. The files you want to protect might be for internal collaborating on design documents or plans, or for other deliverables. When you configure protected libraries for SharePoint, the Office files stored in them will be protected by Azure Rights Management.

The instructions are suitable for the following set of circumstances:

- Employees share and collaborate using Office documents that are on a SharePoint library.
- Employees do not need to set or change the permissions that an administrator sets at the library level.
- Employees do not need to share these documents with people outside your organization.

Deployment Instructions

Make sure that the following requirements and the supporting procedures are in place before you go on to the user documentation.

Requirements for this Scenario

For this scenario to work, the following must be in place:

Check	Requirement	If you need more information
☐	You have prepared accounts and groups for Office 365 or Azure Active Directory	Preparing for Azure Rights Management
☐	Azure Rights Management is activated	Activating Azure Rights Management
☐	If you will use SharePoint Server: Deploy the RMS connector and configure it for SharePoint	Deploying the Azure Rights Management Connector
☐	Configure permissions for the SharePoint site to protect	Manage permissions for a list, library, folder, document, or list

Check	Requirement	If you need more information
		item Apply Information Rights Management to a list or library
☐	Configure SharePoint for IRM and protected libraries	Set up Information Rights Management (IRM) in SharePoint admin center Apply Information Rights Management to a list or library

To configure the SharePoint library for IRM settings

1. After you have configured SharePoint to use the IRM service, navigate to your SharePoint library to protect with Azure RMS. In the **Settings** >**Information Rights Management (IRM)** page for the site, in addition to selecting **Restrict permissions on this library on download**, and specifying a policy title for administrators and a policy descriptions for users, click **SHOW OPTIONS**.
2. Select the following:
   - **Do not allow users to upload documents that do not support IRM**
   - Optional: **Allow group protection. Default group** and then specify the name of an additional group that might need to collaborate on documents stored in this library, but outside SharePoint. For example, the Sales group has Edit permissions to the site and somebody from this group downloads a document, saves it to disk, and emails it to a co-worker who is not in the Sales group. If the co-worker is in the group you specify here, she will automatically inherit the same permissions that are configured for the site and be able to edit the document.

     Without this option, only users that have access to the SharePoint library will be able to collaborate on these documents, and only by downloading the documents directly from SharePoint. In many cases, this restriction is appropriate.

User Documentation Instructions

There are no procedural instructions to give to users for this scenario because protected libraries require no special action from users. Documents are automatically protected on download, according to the permissions that a SharePoint administrator sets for the site. However, inform users about this change so that they know what to expect, and let your help desk know which libraries are protected and how this can restrict the use of the documents. For example, because of current limitations, these documents can be viewed but not edited with mobile devices. If you configured the group protection, let users know which groups can access and edit documents outside SharePoint.

Using the following template, copy and paste the announcement into a communication for your end users, and make these modifications to reflect your environment:

1. Replace each instance of *<name of SharePoint library>* with the name and link of the SharePoint library that you configured for Azure Rights Management. If this communication is for more than one protected library, change the instructions accordingly.

2. If you configured the **Allow group protection. Default group** option, replace <*group name*> with name of the group you configured and supply the reason for <reason why this group has access permissions to collaborate on the files but not by using the SharePoint library>. If you did not configure this option, delete this sentence.
3. Replace <*contact details*> with instructions for how your users can contact the help desk, such as a website link, email address, or telephone number.
4. Make any additional modifications that you want to the announcement, and then send it to these users.

The example documentation shows how this announcement might look for users, after your customizations.

IT Announcement: Changes to the <name of SharePoint library> site

The SharePoint site, **<name of SharePoint library>**, is now configured for secure collaboration. Now, only members of the <group name> can open these documents from this site, even if you save them locally or email them to somebody else. The exception is that you can share them with members of the <group name> after you have downloaded the documents, so that <reason why this group has access permissions to collaborate on the files but not by using the SharePoint library>. When you edit the files, you see a yellow information banner at the top of the document, to let you know that it has this protection and who can access them.

This change helps to keep our company-confidential data safe from people who should not see it. If you use a mobile device to access these protected documents, you can view them but you must use a desktop device to edit them.

You will not be able to upload documents to the <name of SharePoint site> site if they do not support secure collaboration.

Need help?

- Contact the help desk: <contact details>

Example User Documentation

IT Announcement: Changes to the Sales Forecasts and Reports site

The SharePoint site, **Sales Forecasts and Reports**, is now configured for secure collaboration. Now, only members of our Sales and Marketing team can open these documents from this site, even if you save them locally or email them to somebody else. The exception is that you can share them with members of the Finance team after you have downloaded the documents, so that they can extract the monthly forecast figures. When you edit the files, you see a yellow information banner at the top of the document, to let you know that it has this protection and who can access them.

This change helps to keep our company-confidential data safe from people who should not see it. If you use a mobile device to access these protected documents, you can view them but you must use a desktop device to edit them.

You will not be able to upload documents to the Sales Forecasts and Reports site if they do not support secure collaboration.

Need help?

- Contact the help desk: helpdesk@vanarsdelltd.com

Scenario - Executives Securely Exchange Privileged Information

This scenario and supporting user documentation uses Azure Rights Management so that executives can safely exchange emails and attachments by email with one another and policies automatically restrict access to the executives without requiring special action from them. The emails and any attachments will be automatically protected by Azure Rights Management.

If required, you can add an exception to the rule, such as the abbreviation of DNP (for "Do Not Protect") in the email message subject, so that executives can specify this if they need to send an unprotected email to other executives-for example, to review before forwarding to others.

The instructions are suitable for the following set of circumstances:

- Executives share confidential information with one another that should not be shared with others.
- Executives do not need to do anything different when they send these emails other than send them to a work email address rather than a personal email address.
- Executives have a way to override the rule themselves if they ever need to send an unprotected email message to other executives.

Deployment Instructions

Make sure that the following requirements are in place, and then follow the instructions for the supporting procedures before going on to the user documentation.

Requirements for this Scenario

For the instructions for this scenario to work, the following must be in place:

Check	Requirement	If you need more information
☐	You have prepared accounts and groups for Office 365 or Azure Active Directory: • A mail-enabled group named **Executives**, and all executives are members of this group • A mail-enabled group named **RMS administrators**, and all	Preparing for Azure Rights Management

Check	Requirement	If you need more information
	administrators that will configure Azure RMS are members of this group	
☐	Your Azure Rights Management tenant key is managed by Microsoft; you are not using BYOK	Planning and Implementing Your Azure Rights Management Tenant Key
☐	Azure Rights Management is activated	Activating Azure Rights Management
☐	Either: • Exchange Online is enabled for Azure Rights Management • The RMS connector is installed and configured for Exchange on-premises	• For Exchange Online: Expand the Exchange Online: IRM Configuration section in Configuring Applications for Azure Rights Management. • For Exchange on-premises: Deploying the Azure Rights Management Connector
☐	You have configured a custom template as described next	Configuring Custom Templates for Azure Rights Management
☐	You have configured a transport protection rule for IRM, as described later in this article	• For Exchange Online: Create a Transport Protection Rule • For Exchange 2013: Create a Transport Protection Rule • For Exchange 2010: Create a Transport Protection Rule

To configure the custom template for executives

1. In the Azure classic portal: Create a new custom template for Azure Rights Management, which contains these values and settings:
   - Name: **Executives**
   - Rights: Grant the **Executives** mail-enabled group **Co-Owner** rights
   - Scope: Select the **Executives** mail-enabled group, and the **RMS administrators** mail-enabled group.
2. Publish the new template.
3. For Exchange Online only: Refresh the templates by using the Windows PowerShell for Exchange Online command:

```
Import-RMSTrustedPublishingDomain -Name "RMS Online -1 " -RefreshTemplates -RMSOnline
```

To configure the transport rule for IRM

- Use the Exchange documentation referenced in the table for procedural information to create the transport rule with the following settings:
  - Name: **Apply the Executives templates to executive emails**
  - Specify the **Executives** group as the sender and recipient of the rule and additional condition.
  - For the action, select **Apply rights protection to the message with** and then select the **Executives** template that you configured.
  - Add the exception of **DNP** (as an abbreviation for "Do Not Protect"), or your choice of words to identify this exception, to be included in the subject.
  - Make sure the rule is configured for **Enforce**.

User Documentation Instructions

Unless you want to provide instructions of how to specify **DNP** or your choice of exception words or phrases in the email subject, there are no procedural instructions to give to users for this scenario because protecting emails from and to executives requires no special action from them. Email messages and any attachments are automatically protected so that only the members of the Executives group can access them.

However, you might need to inform the executives and your help desk that these emails will be automatically protected and how this can restrict their use of these emails. For example, they cannot successfully be read by other people if the emails or attachments are later forwarded to others. If you configured the DNP (or equivalent) exception, make sure that the help desk is aware of this configuration so that executives can override the rule themselves, without requiring action from an Exchange administrator.

Using the following template, copy and paste the announcement into a communication for your end users, and make these modifications to reflect your environment:

1. Replace the instances of <*organization name*>with the name of your organization.
2. If you chose a different string from DNP for the exemption, replace that value and the explanation accordingly.
3. Replace <*emaildomain*> with your organization's email domain name.
4. Replace <*contact details*> with instructions for how your users can contact the help desk, such as a website link, email address, or telephone number.
5. Make any additional modifications that you want to the announcement, and then send it to these users.

The example documentation shows how this announcement might look for users, after your customizations.

IT Announcement: <Organization name> executive emails are now automatically protected

From now on, whenever you send emails to another <organization name> executive in the company, the contents of the emails and any attachments will be automatically protected such that only another executive in the company can access them to read the information, print it, copy from it, and so on. This restriction applies even if you forward the email message to others, or save the attachments. This protection helps to prevent data loss of confidential and sensitive information.

Note that if you want others who are not a <organization name> executive to be able to read and edit the information that you send in these emails, you must email it to them separately. Or, to override the automatic protection, type the letters **DNP** (as an abbreviation for Do Not Protect) anywhere in the email message subject.

When sending company-confidential information to another <organization name> executive, please remember to send it to their work email address (*name*@<emaildomain>) and not to a personal email address.

Need help?

- Contact the help desk: <contact details>

Example User Documentation

IT Announcement: VanArsdel executive emails are now automatically protected

From now on, whenever you send emails to another VanArsdel executive in the company, the contents of the emails and any attachments will be automatically protected such that only another executive in the company can access them to read the information, print it, copy from it, and so on. This restriction applies even if you forward the email message to others, or save the attachments. This protection helps to prevent data loss of confidential and sensitive information.

Note that if you want others who are not a VanArsdel executive to be able to read and edit the information that you send in these emails, you must email it to them separately. Or, to override the automatic protection, type the letters **DNP** (as an abbreviation for Do Not Protect) anywhere in the email message subject.

When sending company-confidential information to another VanArsdel executive, please remember to send it to their work email address (*name*@vanarsdelltd.com) and not to a personal email address.

Need help?

- Contact the help desk: helpdesk@vanarsdelltd.com

Scenario - Protect Files on a File Server Share

This scenario and supporting user documentation uses Azure Rights Management to bulk-protect all files that you want to protect on a file server to ensure that only employees from your organization can access them, even if they are copied and saved to storage that is not under the control of your IT department, or emailed to others.

These instructions use one of the default templates, which restricts access to all employees with all usage rights. But if required, you can further restrict access and usage rights by configuring a custom template instead of using a default template.

The instructions are suitable for the following set of circumstances:

- You need to protect all file types and not just Office files. Files that cannot be natively protected by Azure RMS will be generically protected.
- All files in the specified path (including subfolders) will be protected.
- All files have protection reapplied on a schedule, to ensure that any changes to the rights policy templates are applied to the protected files.

Deployment Instructions

Make sure that the following requirements are in place, and then follow the instructions for the supporting procedures before going on to the user documentation.

Requirements for this Scenario

For the instructions for this scenario to work, the following must be in place:

Check	Requirement	If you need more information
☐	Azure Rights Management is activated	Activating Azure Rights Management
☐	You have synchronized your on-premises Active Directory user accounts with Azure Active Directory or Office 365, including their email address. This is required for all users that might need to access files after they are protected by FCI and Azure Rights Management.	Preparing for Azure Rights Management

Check	Requirement	If you need more information
☐	Either: • To use a default template for all users: You have not archived the default, <organization name> - Confidential • To use a custom template for specific users: You have created and published this custom template	Configuring Custom Templates for Azure Rights Management
☐	The Rights Management sharing application is deployed to users' computers that run Windows	Automatic deployment for the Microsoft Rights Management sharing application
☐	You have downloaded the RMS Protection tool and configured the prerequisites for Azure RMS	• For instructions to download the tool and prerequisites: RMS Protection Cmdlets • To configure additional prerequisites for Azure RMS, such as the service principal account: about_RMSProtection_AzureRMS

Configuring a file server to protect all files by using Azure RMS and File Server Resource Manager with file classification infrastructure

1. Start a Windows PowerShell session. You do not have to run this session as an administrator.
2. Authenticate to Azure RMS:

```
Set-RMSServerAuthentication
```

   When prompted, supply the values for the service principal account that you created as a prerequisite for the RMS Protection cmdlets.

3. Run the following to identify the template ID that will be used to protect the files:

```
Get-RMSTemplate
```

   To use the default template that restricts access to all employees with all usage rights, look for the template name of **<organization name> - Confidential**. For example, **VanArsdel, Ltd - Confidential**.

4. Follow the step-by-step instructions in RMS Protection with Windows Server File Classification Infrastructure (FCI).

These instructions include a Windows PowerShell script that you specify to run as a custom executable in File Server Resource Manager. The instructions also include how to verify that the files are protected by Azure Rights Management.

User Documentation Instructions

If the files you are protecting are Office files only, you might not have to provide users with any instructions about the protected files. When authorized users open these documents, they open as usual in Office, with the only difference being that users might be prompted to authenticate, and they will probably see an information bar at the top of the document that informs them that the document is protected.

If the protected files have a **.ppdf** file name extension or they are a protected text or image file (for example, they have a **.ptxt** or .**pjpg** file name extension), these files are now read-only and cannot be edited. Users can view them by using the RMS sharing application viewer, which loads automatically for these file types. These files are natively protected by Azure RMS and applies all policy settings from the template that you applied, with the exception of the usage rights, because the file itself is read-only. Unless you know that you will be protecting these file types, it is unlikely that you will need user instructions for this scenario but warn your help desk that they might need to explain to users why these files cannot be edited.

If the protected files have a **.pfile** file name extension, users can view these files but they must be saved to their original file name (remove the .pfile file name extension) if users want to edit and save their changes. These files are generically protected by Azure RMS and cannot enforce the usage rights from the template that you applied, which means that protection is lost if the file is saved with a new name. This scenario will need instructions for users.

Using the following template, copy and paste the instructions for your end users so that they know how to edit generically protected files. Make these modifications to reflect your environment:

- Replace <*type of file*> and <*file server share*> with the type of file that will be generically protected, and the name of the file server share.
- Replace <*organization name*> with the name of your organization, as it displays on your default Azure Rights Management templates.
- Replace <*organization name*> with the name of your organization.
- Replace <*Instructions how to save the file and remove the .pfile file name extension*> with application-specific instructions for this file type.
- Replace contact details with instructions for how your users can contact the help desk, such as a website link, email address, or telephone number.
- Make any additional modifications that you want to this set of instructions, and then sent it to these users.

The example documentation shows how these instructions might look for users, after your customizations.

How to edit <type of file> from the <file server share>

1. Double-click the file to open it. You might be prompted for your credentials.
2. You see a **protected file** dialog box from the Microsoft Rights Management sharing application, which tells you that you are expected to honor the permissions for **<organization name> - Confidential**. This means, do not share this document with other people if they do not work for <organization name>.
3. Click **Open**.
4. To edit the file, first save the file and remove the .pfile file name extension:
   - <Instructions how to save the file and remove the .pfile file name extension>
5. You can now edit and save file as usual.

Need help?

- For additional information:
  - View and use files that have been protected
- Contact the help desk:
  - *<contact details>*

Example Customized User Documentation

How to edit CAD drawings from the ProjectNextGen share

1. Double-click the file to open it. You might be prompted for your credentials.
2. You see a **protected file** dialog box from the Microsoft Rights Management sharing application, which tells you that you are expected to honor the permissions for **VanArsdel, Ltd - Confidential**. This means, do not share this document with other people if they do not work for VanArsdel, Ltd.
3. Click **Open**.

4. To edit the file, first save the file and remove the .pfile file name extension:
    - **File** > **Save As**
    - Delete **.pfile** from the end of the file name, and click **OK**.
5. You can now edit and save file as usual.

Need help?

- For additional information:
    - View and use files that have been protected
- Contact the help desk: helpdesk@vanarsdelltd.com

Scenario - Secure Your Most (Few) Valuable Files

This scenario and supporting user documentation uses Azure Rights Management to manually and custom-protect a handful of files that you have identified as being your most valuable, which warrant the highest level of protection from unauthorized access. These are usually files that only a few people should be able to access. For example, recipe instructions for your company's signature food product, or takeover plans that must not be public before a specified date.

The instructions are suitable for the following set of circumstances:

- You have identified the small set of files to protect .
- The files are in one of the Office file formats that support Rights Management. If the files are in other file formats (for example, CAD files) ensure that these formats support Azure RMS and that you deploy applications that natively support Azure RMS. For more information, see How Applications Support Azure Rights Management.
- The files contain highly confidential, sensitive information that should be accessible to only a few people.
- Requiring an Internet connection to authorize each individual access to a file is an acceptable tradeoff for these people, because it provides higher security.
- These people do not have a requirement to further share this information with others, but they can modify the information and save their changes.
- The administrator must be able to track who is accessing the files and when, and revoke access if necessary.

Deployment Instructions

Make sure that the following requirements are in place, and then follow the instructions for the supporting procedures before going on to the user documentation.

Requirements for this Scenario

For this scenario, the following must be in place:

Check	Requirement	If you need more information
☐	You have prepared accounts and groups for Office 365 or Azure	Preparing for Azure Rights Management

Check	Requirement	If you need more information
	Active Directory: • A mail-enabled group named **Privileged access**, which contains the few people who should have access to these highly confidential documents • A mail-enabled group named **IT Compliance managers**, which contains people whose job includes eDiscovery, monitoring and auditing • A mail-enabled group named **RMS administrators**, and all administrators that will configure Azure RMS are members of this group	
☐	Azure Rights Management is activated	Activating Azure Rights Management
☐	You have configured a custom template as described next	Configuring Custom Templates for Azure Rights Management
☐	The Rights Management sharing application is deployed to your Windows computer, so that you can protect these files in-place, as described in the next section	Download and install the Rights Management sharing application
☐	Authorized users have a minimum version of Office 2013	If users have Office 2010, they must also install the Rights Management sharing application.
☐	Your Azure RMS subscription includes document tracking	If your subscription for Azure RMS does not include document tracking and revocation, you will not be able to use the document tracking site to see who is accessing these document and revoke access if necessary. In this case, either purchase a subscription that does support document tracking, or accept this limitation. You might also consider the usage logging capabilities of Azure RMS, which can provide information such as

Check	Requirement	If you need more information
		who accessed each file and when, to help you detect potential suspicious behavior. To check your subscription support: Comparison of Rights Management Services (RMS) Offerings

To configure the custom template

1. In the Azure classic portal: Create a new custom template for Azure Rights Management, which contains these values and settings:
   - Name: **Privileged access**
   - Rights: Grant the **Privileged access** mail-enabled group **Co-author** rights
   - Scope: Select the **Privileged access** mail-enabled group, the **IT Compliance managers** mail-enabled group, and the **RMS administrators** mail-enabled group.
   - Offline access: **Content is available only with an Internet connection**
2. Publish the new template.

To protect the files in-place

1. In File Explorer, navigate to the first folder that contains the files to protect:
   - If you will protect all the files in the folder, select the folder.
   - If you will protect only some files in the folder, multi-select the files to protect.
2. Right-click, select **Protect with RMS**, and then select **Protect in-place**.
3. Select **Privileged access**.
4. You might be prompted for credentials. Wait for the files to be protected and then click **Close** when you see **the files have been protected** page.
5. If you have more files to protect in other folders, repeat steps 1 through 4 for each folder.

To monitor and if necessary, revoke access to the files

1. In File Explorer, right-click the protected file, select **Protect with RMS**, and then select **Track Usage**.
2. If prompted, sign in to access the document tracking site.
3. Check who has accessed the file and the other files that you protected, paying particular attention to failed attempts in case they indicate suspicious behavior. If deemed appropriate, you can revoke access to each file.

User Documentation Instructions

There are no specific instructions to give to users for this scenario because these files require no special action from users. The files have been protected by you and will be monitored by you. However, you might need to inform these users and your support channels which files are protected and how this can restrict use of the documents. For example, if an authorized user doesn't have an Internet connection, she will not be able to open the file.

Using the following template, copy and paste the announcement into a communication for your end users, and make these modifications:

1. Supply either the actual names of the files or use a clear reference that the authorized users will understand.
2. Replace <*contact details*> with instructions for how these users can contact the help desk or IT department with an escalated support channel that matches the importance of these documents. For example, provide a 24-hour telephone number for high severity support calls.
3. Make any additional modifications that you want to the announcement, and then send it to these users.

The example documentation shows how this announcement might look for users, after your customizations.

IT Announcement: Protecting <organization name>'s top secret documents

The following files now have a very high level of protection applied to them, so that only <restricted users> can access and change these files. To help safeguard them from unauthorized access, your application will automatically request authorization each time you open these files so you must now have an Internet connection to them and you might be prompted for your credentials:

- <top secret document, type or location 1>
- <top secret document, type or location 2>
- <top secret document, type or location 3>

Need help?

- If you cannot access these files or if you notice suspicious changes in the files <action and contact details>.

Example Customized User Documentation

IT Announcement: Protecting VanArsdel's top secret documents

The following files now have a very high level of protection applied to them, so that only the people on the To line of this email message can access and change these files. To help safeguard them from unauthorized access, your applications will automatically request authorization each time you open these files so you must now have an Internet connection to open them and you might be prompted for your credentials:

- Design specifications for code name "Mercury"
- Design specifications for code name "Jupiter"
- Design specifications for code name "Saturn"
- Design specifications for code name "Neptune"

Need help?

- If you cannot access these files or if you notice suspicious changes in the files, call the 24-hour support escalation line that has been sent to you in a protected email message from the IT Department.

Scenario - Send a Company-Confidential Email

This scenario and supporting user documentation uses Azure Rights Management so that any user in the organization can safely send email communications that cannot be read outside the organization. For example, if somebody forwards the email message to somebody in another organization or to a personal email account. The emails and any attachments will be protected by Azure Rights Management and a template that users select from the email client.

The simplest way to enable this scenario is to use one of the built-in, default templates that automatically restrict access to all users in your organization. But if required, you can make this more restrictive by creating a custom template that for example, restricts access to a subset of users, or has other restrictions such as read-only or an expiration date, or disables the Forward button in the email client.

Important

In this scenario, although you can remove the **Forward** right from a custom template that you configure, and this will disable the Forward button in the email client, this configuration doesn't prevent users from sharing the email with another authorized user. The recipient could save the email (and any attachments) and then share the information by using other sharing mechanisms.

For example, Bob sends an email to Alice using a custom template that applies the Save File and Edit Content custom rights to the Marketing group, and does not include the Forward right. Even though Alice cannot forward the email to others, she can save the email message and any attachments to a USB drive or file server share, which any member of the Marketing group can then read and edit if they can access these files. Users who are not in the Marketing group will not be able to open the content.

The instructions are suitable for the following set of circumstances:

- Any user within the organization wants to share information with others inside the organization, but that information should not be shared outside the organization.
- The information to be shared can be within the email message or attachment.
- Users must manually select the template from within their email client.

Deployment Instructions

Make sure that the following requirements are in place before going on to the user documentation.

Requirements for this Scenario

For the instructions for this scenario to work, the following must be in place:

Check	Requirement	If you need more information
☐	You have prepared accounts and groups for Office 365 or Azure Active Directory	Preparing for Azure Rights Management
☐	Your Azure Rights Management tenant key is managed by Microsoft; you are not using BYOK	Planning and Implementing Your Azure Rights Management Tenant Key
☐	Azure Rights Management is activated	Activating Azure Rights Management
☐	Either: • Exchange Online is enabled for Azure Rights Management • The RMS connector is installed and configured for Exchange on-premises	• For Exchange Online: Expand the Exchange Online: IRM Configuration section in Configuring Applications for Azure Rights Management. • For Exchange on-premises: Deploying the Azure Rights Management Connector
☐	You have not archived the default Azure Rights Management template **<organization> - Confidential**. Or, you have configured a custom template for this purpose because you need more restrictive settings or only a subset of users in the organization should be able to read the protected emails.	Configuring Custom Templates for Azure Rights Management **Tip** If you need more restrictive usage policy settings but for all users in the organization, copy and then edit one of the default templates, rather than create a template from scratch. Updated templates do not refresh immediately for the email clients in this scenario. Check the Refreshing templates for users section in the configuring templates article for information.
☐	Users that send the protected email have Outlook 2013 or Outlook 2016, or Outlook Web Access. Users that receive the email have an email client that supports Azure Rights Management.	You can use Outlook 2010, but you must install the Rights Management sharing application for Windows and adjust the user instructions accordingly. For a list of email clients that support Azure Rights Management, see the **Email** column in the Client devices

Check	Requirement	If you need more information
		capability table, from Requirements for Azure Rights Management

User Documentation Instructions

Using the following template, copy and paste the user instructions into a communication for your end users, and make these modifications to reflect your environment:

1. Replace all instances of <*organization name*> with the name of your organization.
2. Replace all instances of <*organization name - Confidential*> with the name of your default or custom template.
3. Replace the screenshots so that they show your organization template names.
4. Replace <*contact details*> with instructions for how your users can contact the help desk, such as a website link, email address, or telephone number.
5. **Additional modifications you might want to make:**
   - If it is practical to limit instructions to one email client only, consider doing this for simplicity and delete the other set of instructions.
   - If you use a custom template rather than the suggested default template, revise the wording in accordingly:
     - Make the title more specific.
     - Specify the users or groups to select in step 1.
     - Specify the name of the custom template in step 2.
     - Modify the final paragraph to explain the restrictions the recipients will have.
6. Make any other modifications that you want to this set of instructions, and then send it to these users.
7. Because some clients do not support Rights Management, you might need to provide guidance and recommendations for the recipients of these protected email messages. This information will be based on which devices and email applications are in use in your organization and any preferences that you have. For example, recommend that iOS users read protected emails with Outlook for iPad and iPhone rather than the native iOS mail client.

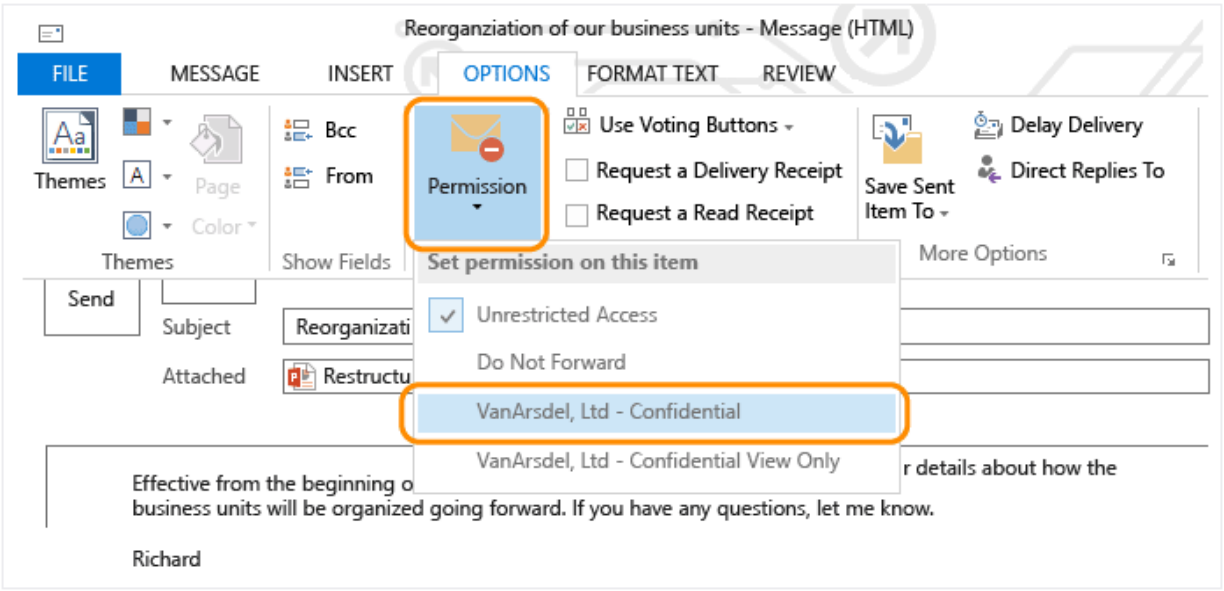
   For more information about the email clients, see the **Email** column in the Client devices capability table, from Requirements for Azure Rights Management.

The example documentation shows how these instructions might look for users, after your customizations.

TEMPLATE

How to send emails that contain company-confidential information using Outlook

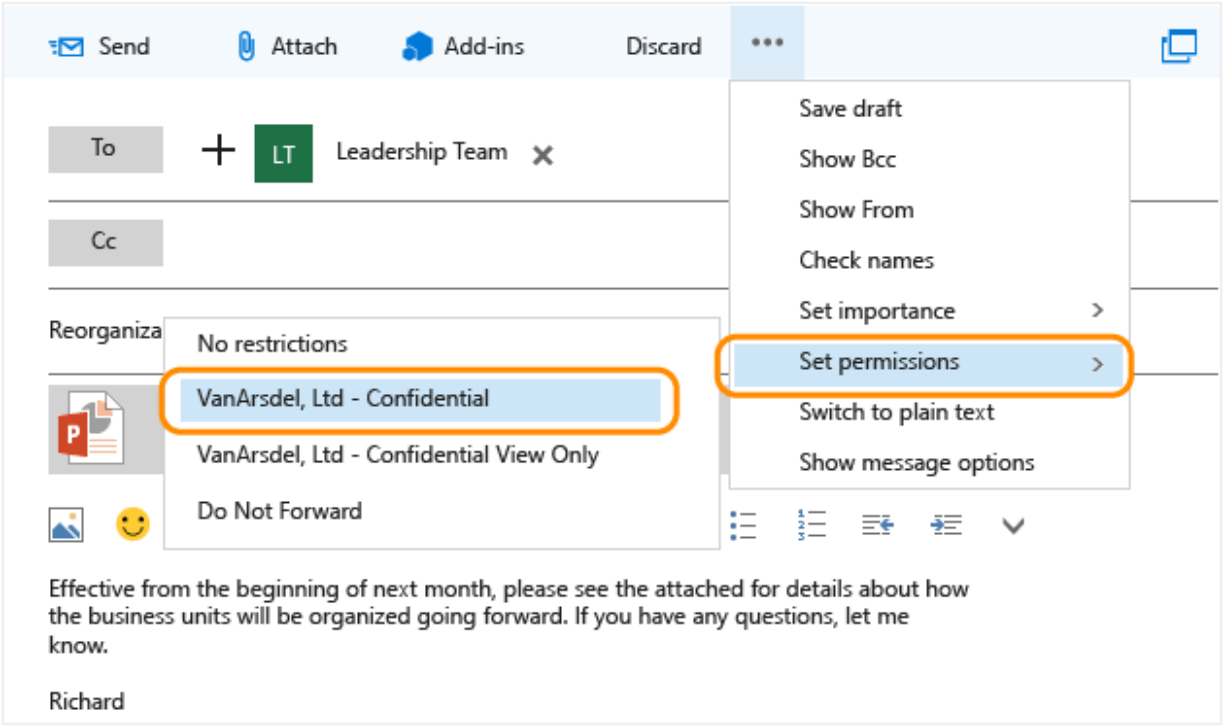
1. Within Outlook, create a new mail message, add any attachments that you want to include, and then select users or groups from *<organization name>*.
2. From the **OPTIONS** tab, click **Permission**, and then select **<organization name - Confidential>**:



3. Send the message.

How to send emails that contain company-confidential information using Outlook Web App

1. Within the Outlook Web App, create a new mail message, add any attachments that you want to include, and then select *<organization name>* users or groups from the address book.
2. Click **…**, click **Set permissions**, and then select **<organization name - Confidential>**:



3. Send the message.

When somebody on the **To**, **Cc**, or **Bcc** line receives this email, they might be asked to authenticate before they can read the message, to verify that they are a user from *<organization name>*. Other times, users are not prompted because they are already authenticated.

People that you send your email to will be able to forward it to other people, but only users from *<organization name>* will be able to read it. If you attach an Office document, it will have the same protection, even if that attachment is saved with a different name, to another location. However, successfully authenticated users can copy and paste from the email or attachment, or print from it. If you need more restrictive protection that prevents actions such as these, contact the help desk.

Need help?

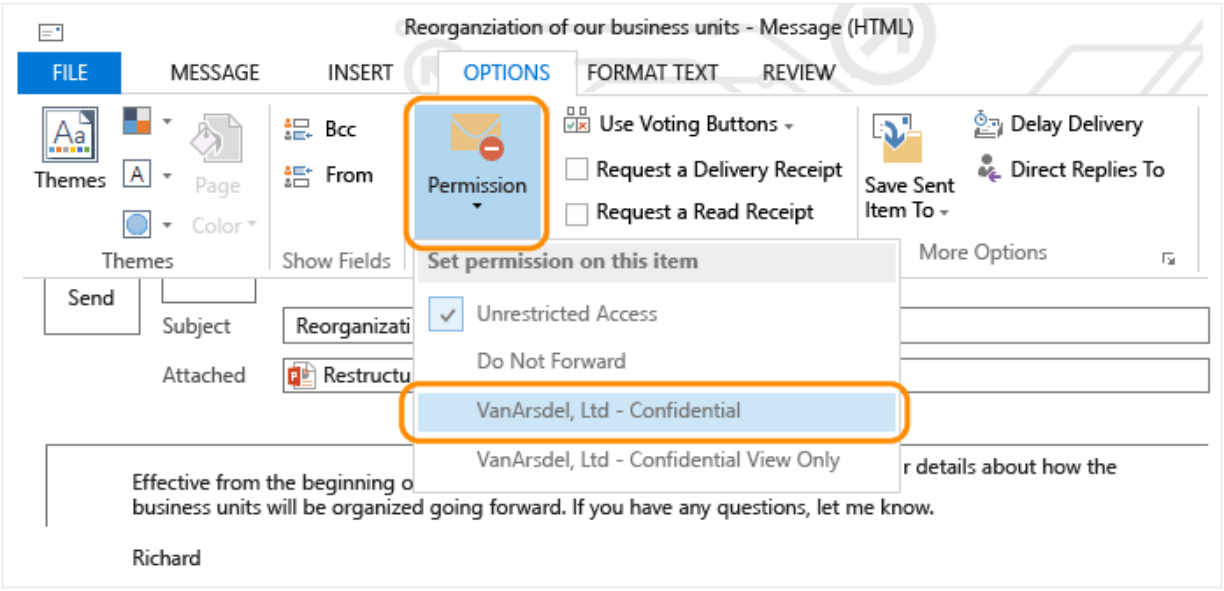
- Contact the help desk:
  - *<contact details>*

Example Customized User Documentation

EXAMPLE

How to send emails that contain company-confidential information using Outlook

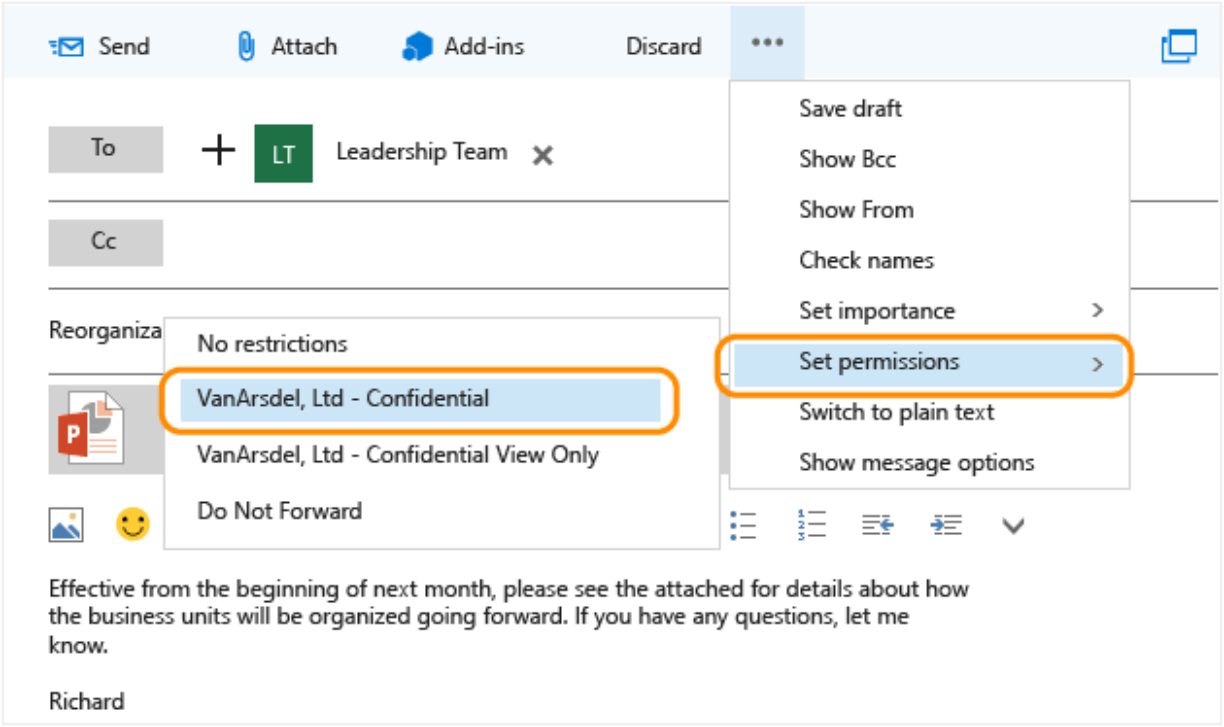
1. Within Outlook, create a new mail message, add any attachments that you want to include, and then select VanArsdel users or groups from the address book.
2. From the **OPTIONS** tab, click **Permission**, and then select **VanArsdel, Ltd - Confidential**:



3. Send the message.

How to send emails that contain company-confidential information using Outlook Web App

1. Within the Outlook Web App, create a new mail message, add any attachments that you want to include, and then select VanArsdel users or groups from the address book.
2. Click **…**, click **Set permissions**, and then select **VanArsdel, Ltd - Confidential**:



3. Send the message.

When somebody on the **To**, **Cc**, or **Bcc** line receives this email, they might be asked to authenticate before they can read the message, to verify that they are a user from VanArsdel, Ltd. Other times, users are not prompted because they are already authenticated.

People that you send your email to will be able to forward it to other people, but only users from VanArsdel will be able to read it. If you attach an Office document, it will have the same protection, even if that attachment is saved with a different name, to another location. However, successfully authenticated users can copy and paste from the email or attachment, or print from it. If you need more restrictive protection that prevents actions such as these, contact the help desk.

Need help?

- Contact the help desk:
  - Email: helpdesk@vanarsdelltd.com

Scenario - Configure Work Folders for Persistent Protection

This scenario and supporting user documentation uses Azure Rights Management to apply persistent protection to Office documents in Work Folders. Work Folders uses a role service for file servers running Windows Server that provides a consistent way for users to access their work files from their PCs and devices. Although Work Folders provides its own encryption to protect the files, this protection is lost if the files are then moved outside the Work Folders environment. For example, users copy the synchronized files and save them to storage that is not under the control of your IT department, or the files are emailed to others.

The additional protection that Azure Rights Management provides helps to prevent accidental data loss by preventing the files from being viewed by people outside your organization. To do this, you can use one of the built-in, default rights policy templates. However, before you deploy this scenario, consider whether users might need to legitimately share any of these files with people outside the organization. For example, after working on a draft price list, a user then emails the final version to their customer in another organization. When you use the default Rights Management template for Work Folders, that customer in the other organization couldn't be able to read this emailed document. You can accommodate this requirement by creating a custom template that lets users apply a new rights policy to the file, which replaces the original restriction of all employees to the people that they specify in the email.

Note

When you use the custom template that is documented for this scenario, although users can intentionally share files with people that you didn't define in the template, the additional protection that you're applying with Azure Rights Management provides a lot of benefits. This additional protection prevents accidental data loss if the content is moved outside the Work Folders boundary, because the content remains protected from unauthorized users, whether it is at rest or transmitted. For example, a user loses a device that is using Work Folders, or this device is stolen, or the content synchronized to and from this device is transferred over unsecured infrastructure.

If a user shares the content with somebody in another organization, by using the Share Protected functionality from the Rights Management sharing application, that user replaces the original protection with their own protection policy. As a result, the content is still protected from unauthorized access and only the people that the user specifies can access the content.

You can apply this persistent protection to all Office documents in users' Work Folders, or only to files that contain sensitive or high-business-impact data.

The instructions are suitable for the following set of circumstances:

- The Work Folder files that you want to protect with persistent protection are Office files. These files can be natively protected by Azure Right Management and do not change their file name extension or require a different work flow to open them.
- You want to apply the persistent protection to all Office files in users' Work Folders, or to selective files that have been identified by using File Classification Infrastructure from File Server Resource Manager in Windows Server.

- For files that must be shared with people that are not specified in the rights policy template (for example, users in another organization), users must apply a new rights policy to replace the original rights policy protection.

Deployment Instructions

Make sure that the following requirements are in place, and then follow the instructions for the supporting procedures before going on to the user documentation.

Requirements for this Scenario

For the instructions for this scenario to work, the following must be in place:

Check	Requirement	If you need more information
☐	Azure Rights Management is activated	Activating Azure Rights Management
☐	You have synchronized your on-premises Active Directory user accounts with Azure Active Directory or Office 365, including their email address. This is required for all users that use Work Folders.	Preparing for Azure Rights Management
☐	Either: • To use a default template for all users that does not allow users to apply a new rights policy: You have not archived the default template, **<organization name> - Confidential** • To use a custom template that is suitable for users to apply a new rights policy: You use the instructions that follow to create a custom template	Configuring Custom Templates for Azure Rights Management

Check	Requirement	If you need more information
☐	The Rights Management connector is installed, authorized for the Windows Server computer, and configured for the **FCI Server** role.	Deploying the Azure Rights Management Connector
☐	The Rights Management sharing application is deployed to users' computers that run Windows	Automatic deployment for the Microsoft Rights Management sharing application

Configuring the custom rights policy template so that users can share Work Folders files outside the organization

1. Sign into the Azure classic portal, and navigate to the Azure Rights Management templates.
2. Copy the **<organization name> - Confidential** template, and supply a name and description for this Work Folders scenario. We suggest the following:
   - Name: **Content protected by Work Folders**
   - Description: **This content is protected by Work Folders and is restricted to company employees only. To share this content with people outside the organization, attach the document to an email message and use the Share Protected function.**
3. On the **RIGHTS** page:
   - Change the existing rights from **Custom** to **Co-Owner**.
4. On the **CONFIGURE** page:
   - Make sure the **STATUS** is set to **PUBLISH**
   - For the **name and description**, delete the entries for the languages that you do not use. For the languages that you do use, update the **NAME** and **DESCRIPTION** so that these match the name and description that you gave this template, using the specified language.
5. Save the template.

Configuring Work Folders to apply persistent protection to Office file

1. Implement Work Folders for your users so that locally saved files are synchronized to a file server folder, known as a sync share. The sync share on the file server must not be on the same server that runs the Rights Management connector.

   This solution requires the Work Folders role service in Server Manager, for the File and Storage Services role. The file server must be running a minimum version of Windows Server 2012 R2, and this file server can be on-premises, or in a virtual machine in Azure. For more information about Work Folders, see Work Folders Overview.

   For deployment instructions, see Deploying Work Folders. Make sure that you select the built-in encryption (the option **Encrypt Work Folders**), which will be applied in addition to Azure Rights Management encryption. In addition:

- When you bind the SSL certificate on the sync server (step 4): Use the netsh command (rather than the IIS management console) to bind the certificate to the Default Web Site HTTPS interface.
- To avoid users getting the Work Folders setup error **There was a problem applying security policies** and the requirement that they must be a local administrator on their domain-joined computers: Use the Set-SyncShare cmdlet with the PasswordAutolockExcludeDomain parameter, and specify the domain names that these computers reside in (for example, contoso.com).

2. To complete the configuration for the Rights Management connector:
   a. Using File Server Resource Manager, create a file management task that identifies the sync share folder as the scope.
   b. For the action, choose **RMS encryption**, and select a template:
      - If you did not create a custom template because you do not want users to be able to share files with others outside the organization, select the template name of **<organization name> - Confidential**. For example, **VanArsdel, Ltd - Confidential**.
      - If you created a custom template by using the preceding instructions, select this template. For example, **Content protected by Work Folders**.
   c. Specify a schedule that allows plenty of time for all the Office files to be encrypted by Azure Rights Management, and specify the option to **Run continuously on new files**.
3. To manually test this configuration, make sure that the folder contains some Office files, and then use the **Run File Management Task Now** option, and select **Wait for the task to complete**.

   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 Azure Rights Management. For example, open a file and confirm that you see the information banner at the top of the document that displays the name and description of the Rights Management template.
4. If you decided to selectively protect files by using File Classification Infrastructure, configure your classification rule and schedule, and then modify the file management task to include this classification property as a condition.

User Documentation Instructions

If the files you are protecting with Azure Rights Management do not need to be shared with people outside your organization, you might not have to provide users with any additional instructions than those you provide for using Work Folders. When users open the files that are protected by Azure Rights Management and the default template, the files open as usual in Office, with the only difference being that users might be prompted to authenticate, and they will see an information bar at the top of the document that informs them that the content contains proprietary information intended for internal users only.

If you configured the custom template as documented for this scenario, users will see the template description in the information bar: **This content is protected by Work Folders and is restricted to company employees only. To share this content with people outside the organization, attach the document to an email message and use the Share Protected function.**. Although this description

provides a summary of how to share the file outside the organization, users will probably need detailed instructions how to do this, especially for the first few times they do this. To support this follow-on scenario, use the administrator and end-user instructions from Scenario - Share an Office File with Users in Another Organization.

Tip

If you decided not to use the custom template in these instructions, because you do not want users to be able to share these files outside the organization without IT oversight, let your help desk know so that if the sharing requirement is legitimate, it can be accommodated by using whatever mechanism is most appropriate for your business. For example, somebody who is a super user could apply a new template to the content that grants the requesting user Full Control rights, so that this user can then use the Share Protected function.

After a period of time, if you discover there are many such requests, you might decide to define your own custom template for this scenario that grants only specific users (such as managers or the help desk) the Co-Owner option while standard users are granted Co-Author or whatever rights you decide are suitable.