Configure supervision policies in Office 365

To view contributors to this article access the link below

https://docs.microsoft.com/en-us/microsoft-365/compliance/configure-supervision-policies?view=o365-worldwide

In this article

Important

This topic applies to configuring supervision policies in an Office 365 subscription. If you want to configure communications compliance for a Microsoft 365 subscription, see Configure communications compliance in Microsoft 365.

Use supervision policies to capture employee communications for examination by internal or external reviewers. For more information about how supervision policies can help you monitor communications in your organization, see Supervision policies in Office 365.

Note

Users monitored by supervision policies must have a Microsoft 365 E5 Compliance license, an Office 365 Enterprise E3 license with the Advanced Compliance add-on, or be included in an Office 365 Enterprise E5 subscription, or be included in a Microsoft 365 E5 subscription. If you don't have an existing Enterprise E5 plan and want to try supervision, you can sign up for a trial of Office 365 Enterprise E5.

Follow these steps to set up and use supervision in your Office 365 organization:

- **Step 1 (optional)**: Set up groups for supervision

  Before you start using supervision policies, determine who needs communications reviewed and who performs reviews. If you want to get started with just a few users to see how supervision works, you can skip setting up groups for now.

- **Step 2 (required)**: Make supervision available in your organization

  Add yourself to the Supervisory Review role group so you can set up policies. Anyone who has this role assigned can access the **Supervision** page in the Office 365 security and compliance center. If reviewable email is hosted on Exchange Online, each reviewer must have remote PowerShell access to Exchange Online.

- **Step 3 (optional)**: Create custom sensitive information types and custom keyword dictionaries

  If you need a custom sensitive info type or a custom keyword dictionary for your supervision policy, you need to create it before starting the supervision wizard.

- **Step 4 (required)**: Set up a supervision policy

  You create supervision policies in the Office 365 security and compliance center. These policies define which communications are subject to review in your organization and specifies who performs reviews. Communications include email and Microsoft Teams communications, and 3rd-party platform communications (such as Facebook, Twitter, etc.). Supervision policies created in Office 365 organizations are not supported in communication supervision in Microsoft 365 subscriptions.

- **Step 5 (optional)**: Test your communication supervision policy

  Test your supervision policy to make sure it functions as desired. It is important to ensure that your compliance strategy is meeting your standards.

Step 1: Set up groups for supervision (optional)

When you create a supervision policy, you define who has their communications scanned and who performs reviews. In the policy, you'll use email addresses to identify individuals or groups of people. To simplify your setup, you can create groups for people who have their communication scanned and groups for people who review those communications. If you're using groups, you may need several. For example, you want to monitor communications between two distinct groups of people or if you want to specify a group that isn't going to be supervised.

Use the following chart to help you configure groups in your organization for communication supervision policies:

Table 1

Policy Member	Supported Groups	Unsupported Groups
Supervised users Non-supervised users	Distribution groups Office 365 groups	Dynamic distribution groups
Reviewers	Mail-enabled security groups	Distribution groups Dynamic distribution groups

When you select an Office 365 group for supervised users, the policy monitors the content of the shared Office 365 mailbox and the Microsoft Teams channels associated with the group. When you select a distribution list, the policy monitors individual user mailboxes.

To manage supervised users in large enterprise organizations, you may need to monitor all users across large groups. You can use PowerShell to configure a distribution group for a global supervision policy for the assigned group. This enables you to monitor thousands of users with a single policy and keep the supervision policy updated as new employees join your organization.

1. Create a dedicated distribution group for your global supervision policy with the following properties: Make sure that this distribution group isn't used for other purposes or other Office 365 services.
    - **MemberDepartRestriction = Closed**. Ensures that users cannot remove themselves from the distribution group.
    - **MemberJoinRestriction = Closed**. Ensures that users cannot add themselves to the distribution group.
    - **ModerationEnabled = True**. Ensures that all messages sent to this group are subject to approval and that the group is not being used to communicate outside of the supervision policy configuration.

    PowerShell

```
New-DistributionGroup -Name <your group name> -Alias <your group alias> -
MemberDepartRestriction 'Closed' -MemberJoinRestriction 'Closed' -
ModerationEnabled $true
```

- Select an unused Exchange custom attribute to track users added to the supervision policy in your organization.

- Run the following PowerShell script on a recurring schedule to add users to the supervision policy:

PowerShell

```
$Mbx = (Get-Mailbox -RecipientTypeDetails UserMailbox -ResultSize
Unlimited -Filter {CustomAttribute9 -eq $Null})
$i = 0
ForEach ($M in $Mbx)
{
  Write-Host "Adding" $M.DisplayName
  Add-DistributionGroupMember -Identity <your group name> -Member
$M.DistinguishedName -ErrorAction SilentlyContinue
  Set-Mailbox -Identity $M.Alias -<your custom attribute name> SRAdded
    $i++
  }
Write-Host $i "Mailboxes added to supervisory review distribution
group."
```

For more information about setting up groups, see:

- Create and manage distribution groups
- Manage mail-enabled security groups
- Overview of Office 365 Groups

Step 2: Make supervision available in your organization (required)

To make **Supervision** available as a menu option in Office 365 security and compliance center, you must be assigned the Supervisory Review Administrator role.

To do this, you can either add yourself as a member of the Supervisory Review role group, or you can create a role group.

Add members to the Supervisory Review role group

1. Sign into https://protection.office.com using credentials for an admin account in your Office 365 organization.
2. In the Office 365 security and compliance center, go to **Permissions**.
3. Select the **Supervisory Review** role group and then click the Edit icon.
4. In the **Members** section, add the people who you want to manage communication supervision for your organization.

Create a new role group

1. Sign into https://protection.office.com/permissions using credentials for an admin account in your Office 365 organization.
2. In the Office 365 security and compliance center, go to **Permissions** and then click Add (+).
3. In the **Roles** section, click Add (+) and scroll down to **Supervisory Review Administrator**. Add this role to the role group.
4. In the **Members** section, add the people who you want to manage communication supervision for your organization.

For more information about role groups and permissions, see Permissions in the Compliance Center.

Enable remote PowerShell access for reviewers (if email is hosted on Exchange Online)

1. Follow the guidance in Enable or disable access to Exchange Online PowerShell.

Step 3: Create custom sensitive information types and custom keyword dictionaries (optional)

In order to pick from existing custom sensitive information types or custom keyword dictionaries in the supervision policy wizard, you first need to create these items if needed.

Create custom keyword dictionary/lexicon (optional)

Use a text editor (like Notepad), to create a file that includes the keyword terms you'd like to monitor in a supervision policy. Make sure that each term is on a separate line and save the file in the **Unicode/UTF-16 (Little Endian)** format.

Create custom sensitive information types

1. Create a new sensitive information type and add your custom dictionary in the Office 365 Security & Compliance Center. Navigate to **Classifications** > **Sensitive info types** and follow the steps in the **New sensitive info type wizard**. Here you will:
   - Define a name and description for the sensitive info type
   - Define the proximity, confidence level, and primary pattern elements
   - Import your custom dictionary as a requirement for the matching element
   - Review your selections and create the sensitive info type

   For more detailed information, see Create a custom sensitive information type and Create a keyword dictionary

   After the custom dictionary/lexicon is created, you can view the configured keywords with the Get-DlpKeywordDictionary cmdlet or add and remove terms using the Set-DlpKeywordDictionary cmdlet.

Step 4: Set up a supervision policy (required)

1. Sign into https://protection.office.com using credentials for an admin account in your Office 365 organization.
2. In the Office 365 security and compliance center, select **Supervision**.
3. Select **Create** and follow the wizard to set up the policy configuration. Using the wizard, you will:
   - Give the policy a name and description.
   - Choose the users or groups to supervise, including choosing users or groups you'd like to exclude.
   - Define the supervision policy conditions. You can choose from message address, keyword, file types, and size match conditions.
   - Choose if you'd like to include sensitive information types. This is where you can select default and custom sensitive info types.
   - Choose if you'd like to enable the offensive language model. This detects inappropriate language sent or received in the body of email messages.
   - Define the percentage of communications to review.
   - Choose the reviewers for the policy. Reviewers can be individual users or mail-enabled security groups. All reviewers must have mailboxes hosted on Exchange Online.
   - Review your policy selections and create the policy.

Step 5: Test your supervision policy (optional)

After you create a communication supervision policy, it's a good idea to test to make sure that the conditions you defined are being properly enforced by the policy. You may also want to test your data loss prevention (DLP) policies if your supervision policies include sensitive information types. Follow these steps to test your supervision policy:

1. Open an email client or Microsoft Teams logged in as a supervised user defined in the policy you want to test.
2. Send an email or Microsoft Teams chat that meets the criteria you've defined in the supervision policy. This can be a keyword, attachment size, domain, etc. Make sure that you determine if your configured conditional settings in the policy are too restrictive or too lenient.

   Note

   Emails subject to defined policies are processed in near real-time and can be tested immediately after the policy is configured. Chats in Microsoft Teams can take up to 24 hours to fully process in a policy.

3. Log into your Office 365 tenant as a reviewer designated in the communication supervision policy. Navigate to **Supervision** > *Your Custom Policy* > **Open** to view the report for the policy.