Communication compliance in Microsoft 365

Use the following guide to learn more about the latest communication compliance policies and how to configure these policies for your organization. Getting started is easy, and this guide will help you prioritize your first steps in meeting internal policy, reducing risk, and engaging in regulatory compliance using Microsoft 365.

Prepared by:
Microsoft 365 Security & Compliance team

Communication compliance in Microsoft 365 (preview)

Communication compliance is part of the new insider risk solution set in Microsoft 365 that helps minimize communication risks by helping you detect, capture, and take remediation actions for inappropriate messages in your organization. Pre-defined and custom policies allow you to scan internal and external communications for policy matches so they can be examined by designated reviewers. Reviewers can investigate scanned email, Microsoft Teams, or third-party communications in your organization and take appropriate remediation actions to make sure that they are compliant with your organization's message standards.

Communication compliance policies in Microsoft 365 help you overcome many modern challenges associated with compliance and internal and external communications, including:

- Scanning increasing types of communication channels
- The increasing volume of message data
- Regulatory enforcement & the risk of fines

Scenarios

Corporate policies: Communication compliance policies can detect policy matches and help you take corrective actions to help mitigate these types of incidents.
Risk management: Using communications supervision policies to help identify and manage potential legal exposure and risk can help minimize risks before they can damage corporate operations.
Regulatory compliance: Communication compliance policies can help your organization meet regulatory compliance standards by providing a process to both scan and report on corporate communications.

New enhancements

Communication compliance in Microsoft 365 builds on the features of Supervision policies in Office 365 with several new enhancements:

Intelligent customizable templates: Intelligent customizable templates in communication compliance allow you to apply machine learning to intelligently detect communication violations in your organization.
Flexible remediation workflows: Built-in remediation workflows allow you to quickly identify and take action on messages with policy matches in your organization.

Actionable insights: New interactive dashboards for alerts, policy matches, actions, and trends help you quickly view the status of pending and resolved alerts in your organization.

Integration with Microsoft 365 services

Communication compliance policies scan and capture messages across several communication channels to help you quickly review and remediate compliance issues:

- Microsoft Teams: Policies now automatically scan all Microsoft Teams channels and teams for specific users defined in a policy, eliminating the need to keep a separate mapping list for Microsoft Teams assignments.
- Exchange Online: Emails and attachments matching communication compliance policy conditions are instantly available for monitoring and in supervision reports.
- Skype for Business Online: Communication compliance policies support scanning chat communications and associated attachments in Skype for Business Online.
- Third-party sources: Communication compliance supports connections to several popular platforms, including Instant Bloomberg, Facebook, Twitter, and others.

Workflow

Communication compliance helps you address common pain points associated with complying with internal policies and regulatory compliance requirements. With focused policy templates and a flexible workflow, you can use actionable insights to quickly resolve detected compliance issues.

Configure: In this workflow step, you identify your compliance requirements and configure applicable communication compliance policies. You can choose from the following policy templates in the Microsoft 365 compliance center:

- **Offensive language and anti-harassment**: Quickly create a policy that uses the built-in classifier to automatically detect content that may be considered abusive or offensive.
- **Sensitive information**: Create a policy to scan communications containing defined sensitive information types or keywords to help make sure that important data isn't shared with people that shouldn't have access.
- **Regulatory compliance**: Create a policy to scan communications for references to standard financial terms associated with regulatory standards.
- **Custom policy**: Configure specific communication channels, individual detection conditions, and the amount of content to review for supervision in your organization.

Investigate: In this step, you look deeper into the issues detected as matching your communication compliance policies. This step includes the following actions available in the Microsoft 365 compliance center:

- **Alerts**: When a message matches a supervision policy, an alert is automatically generated. For each alert, you can see the status, the severity, the time detected, and if a case is assigned and its status.
- **Issue management**: For each alert, you can take investigative actions to help remediate the issue detected in the message.
- **Document review**: During the investigation of an issue, you can use several views of the message to help properly evaluate the detected issue.
- **Reviewing user activity history**: View the history of user message activities and remediation actions, such as past notifications and escalations for policy matches.
- **Filters**: Use filters such as sender, recipient, date, and subject to quickly narrow down the message alerts that you want to review.

Remediate: The next step is to remediate communication compliance issues you've investigated using the following options:

- **Resolve**: After reviewing an issue, you can remediate by resolving the alert. Alerts are automatically resolved after marking the alert as a false positive, sending a notice to an employee about the alert, or opening a new case for the alert.
- **Tag a message**: As part of the resolution of an issue, you can tag the detected message as compliant, non-compliant, or as questionable as it relates to the policies and standards for your organization.
- **Notify the user**: Often, users accidentally or inadvertently violate a communication compliance policy. You can use the notify feature to provide a warning notice to the user and to resolve the issue.
- **Escalate to another reviewer**: You can easily escalate message issues to reviewers in other areas of your organization as part of the resolution process.
- **Mark as a false positive**: Messages incorrectly detected as matches of compliance policies will occasionally slip through to the review process. You can mark these types of alerts as false positives and automatically resolve the issue.

Monitor

Keeping track and managing compliance issues identified by communication compliance policies spans the entire workflow process. As alerts are generated and investigation and remediation actions are implemented, existing policies may need review and updates, and new policies may need to be created.

- **Monitor and report**: Use communication compliance dashboards, reports, export logs, and events recorded in the unified Office 365 audit logs to continually evaluate and improve your compliance posture.

Configure communication compliance for Microsoft 365 (preview)

Use communication compliance policies to capture employee communications for examination by internal or external reviewers.

***NOTE**: Users monitored by communication compliance policies must have either 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. If you don't have an existing Enterprise E5 plan and want to try communication compliance, you can sign up for a trial of Office 365 Enterprise E5.*

Step 1 (optional): Set up groups for communication compliance
Before you start using communication compliance, determine who needs communications reviewed and who performs reviews. If you want to get started with just a few users to see how communication compliance works, you can skip setting up groups for now.

Step 2 (required): Make communication compliance available in your organization
Add yourself to the **Supervisory Review Administrator** role so you can set up policies. If reviewable email is hosted on Exchange Online, each reviewer must have remote PowerShell access to Exchange Online.

Step 3 (required): Set up a communication compliance policy
You create communication compliance policies in the Microsoft 365 compliance center. Communications include email, Microsoft Teams, Skype for Business, and 3rd-party platform communications (such as Facebook, Twitter, etc.).

Step 4 (optional): Create employee notice templates
Create custom notice templates to send email notifications to employees as a remediation option for policy matches.

Step 5 (optional): Test your communication compliance policy
Test your communication compliance policy to make sure it functions as desired. It is important to ensure that your compliance strategy is meeting your standards.

Investigate and remediate communication compliance alerts (preview)

After you've configured your communication compliance policies, you'll start to receive alerts in the Microsoft 365 compliance center for message issues that match your policy conditions. Follow the workflow instructions here to investigate and remediate alert issues.

Investigate alerts

The first step to investigate issues detected by your policies is to review generated alerts in the Microsoft 365 compliance center. There are several areas in the compliance center to help you to quickly investigate alerts, depending on how you prefer to view alert grouping:

- Communication compliance home page: Here you'll see:
  - Alerts needing review listed from high to low severity. Select an alert to launch the alert details page and to start remediation actions.
  - Recent policy matches listed by policy name.
  - Resolved items listed by policy name.
  - Escalations listed by policy name.
  - Users with the most policy matches, listed from the most to the least number of matches.
- **Alerts tab**: Display alerts grouped by matched communication compliance policy. This view allows you to quickly see which communication compliance policies are generating the most alerts ordered by severity.
- **Policies tab**: Each policy listed includes the count of alerts that need review. Selecting a policy displays all the pending alerts for matches to the policy, select a specific alert to launch the policy details page and to start remediation actions.

Using filters

The next step is to sort the messages so that it's easier for you to investigate alerts. Communication compliance supports multi-level filtering for several message fields to help you quickly investigate and review messages with policy matches. For a complete list of filters and field details, see Filters in the feature reference topic.

Using near and exact duplicate analysis

Communication compliance policies automatically scan and pre-group near and exact message duplicates without any additional configuration steps. This allows you to

quickly remediate similar messages one-by-one or as a group, reducing the message investigation burden for reviewers. As duplicates are detected, the **Near Duplicates** and/or the **Exact Duplicates** controls are displayed in the remediation action toolbar.

Remediate alerts

No matter where you start to review alerts or the filtering you configure, the next step is to take action to remediate the alert. Start your alert remediation using the following workflow on the **Policy** or **Alerts** pages:

1. **Examine the message basics**: Sometimes it's obvious from the source or subject that a message can be immediately remediated. It may be that the message is spurious or incorrectly matched to a policy and it should be resolved as a false positive. Consider using the **Tag as** or **Escalate** controls to assign a tag to applicable messages or to send messages to a designated reviewer.
2. **Examine the message details**: After reviewing the message basics, it's time to open a message to examine the details and to determine further remediation actions. Several different views are available to help you decide the proper course of action, including source view, text view, annotate view and user history.
3. **Decide on a remediation action**: Now that you've reviewed the details of the message for the alert, you can choose several remediation actions:
    - **Resolve**: Selecting the **Resolve** control immediately removes the message from the **Pending alerts** queue and no further action can be taken on the message. By selecting **Resolve**, you've essentially closed the alert without further classification and it cannot be reopened for further actions.
    - **False Positive**: You can always resolve a message as a false positive at any point during the message review workflow.
    - **Tag as**: Tag the message as *compliant*, *non-compliant*, or as *questionable* as it relates to the policies and standards for your organization.
    - **Notify**: You can use the **Notify** control to assign a custom notice template to the alert and to send a warning notice to the user.
    - **Escalate**: Using the **Escalate** control, you can choose who else in your organization should review the message.
4. **Determine if message details should be archived outside of communication compliance**

Communication compliance feature reference (preview)

Policies

You create communication compliance policies for Microsoft 365 organizations in the Microsoft 365 compliance center. If you have an Office 365 organization, you'll configure Supervision policies in the Office 365 security and compliance center. Communication compliance policies define which communications and users are subject to review in your organization, define custom conditions that the communications must meet, and specifies who should perform reviews.

Policy templates

Policy templates are pre-defined policy settings that you can use to quickly create policies to address common compliance scenarios. You can choose from the following policy templates:

- Offensive language and anti-harassment
- Sensitive information
- Regulatory compliance

Supervised users

Before you start using communication compliance, you must determine who needs their communications reviewed. In the policy, user email addresses identify individuals or groups of people to supervise. Some examples of these groups are Office 365 Groups, Exchange-based distribution lists, and Microsoft Teams channels. You also can exclude specific users or groups from scanning with a specific exclusion group or a list of groups.

***NOTE**: Users covered by communication compliance policies must have either 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. If you don't have an existing Enterprise E5 plan and want to try communication compliance, you can sign up for a trial of Office 365 Enterprise E5.*

Reviewers

When you create a communication compliance policy, you must determine who performs reviews of the messages of the supervised users. In the policy, user email addresses identify individuals or groups of people to review supervised communications. All reviewers must have mailboxes hosted on Exchange Online and must be assigned the **Case Management** and **Review** roles.

Groups for supervised users and reviewers

To simplify your setup, create groups for people who need their communications reviewed and groups for people who review those communications. If you're using groups, you might need several. For example, if you want to scan communications between two distinct groups of people, or if you want to specify a group that isn't supervised.

Supported communication types

With communication compliance policies, you can choose to scan messages in one or more of the following communication platforms as a group or as standalone sources. Communications captured across these platforms are retained for seven years for each policy by default, even if users leave your organization and their mailbox is deleted.

- Microsoft Teams: chat or channel communications
- Exchange email
- Skype for Business Online
- Third-party sources

Policy settings

- **Direction**: By default, the **Direction is** condition is displayed and can't be removed. Communication direction settings in a policy are chosen individually or together.
- **Sensitive information types:** You have the option of including sensitive information types as part of your communication compliance policy. Sensitive information types are either pre-defined or custom data types that can help identify and protect credit card numbers, bank account numbers, passport numbers, and more.
- **Custom keyword dictionaries:** Configure custom keyword dictionaries (or lexicons) to provide simple management of keywords specific to your organization or industry.
- **Classifiers**: Built-in classifiers scan sent or received messages across all communication channels in your organization for different types of compliance issues. Classifiers use a combination of artificial intelligence and keywords to identify language in messages likely to violate anti-harassment policies.
- **Conditional settings:** The conditions you choose for the policy apply to communications from both email and 3rd-party sources in your organization (like from Facebook or DropBox). The table here explains more about each condition.

Notices

You can create notice templates if you want to send users an email reminder notice for policy matches as part of the issue resolution process. Notices can only be sent to the employee email address associated with the policy match that generated the specific alert for remediation.

- **HTML for notices:** If you'd like to create more than a simple text-based email message for notifications, you can create a more detailed message by using HTML in the message body field of a notice template.

Filters

Communication compliance filters allow you to filter and sort alert messages for quicker investigation and remediation actions. Filtering is available on the **Pending** and **Resolved** tabs for each policy. To save a filter or filter set as a saved filter query, one or more values must be configured as filter selections.

Alert policies

After configuring a policy, a corresponding alert policy is automatically created and alerts are generated for messages that match conditions defined in the policy. By default, all policy matches alert triggers are assigned a severity level of medium in the associated alert policy. Alerts are generated for a communication compliance policy once the aggregation trigger threshold level is met in the associated Office 365 alert policy.

Audit

In some instances, you must provide information to regulatory or compliance auditors to prove supervision of employee activities and communications. Communication compliance policies have built-in audit trails for complete readiness for internal or external audits. Detailed audit histories of every create, edit, and delete action are captured by your communication policies to provide proof of supervisory procedures.