Permissions in the Office 365 Security & Compliance Center

Permissions in the Office 365 Security & Compliance Center

Aplica-se a: Office 365 para Administradores

The Office 365 Security & Compliance Center lets you grant permissions to people who perform compliance tasks like device management, data loss prevention, eDiscovery, retention, and so on. These people can perform only the tasks that you explicitly grant them access to. To access the Security & Compliance Center, users need to be an Office 365 global administrator or a member of one or more Security & Compliance Center role groups.

Permissions in the Security & Compliance Center are based on the Role Based Access Control (RBAC) permissions model. This is the same permissions model that's used by Exchange, so if you're familiar with Exchange, granting permissions in the Security & Compliance Center will be very similar. It's important to remember, however, that Exchange role groups and Security & Compliance Center role groups don't share membership or permissions. While both have an Organization Management role group, they aren't the same. The permissions they grant, and the members of the role groups, are different. There's a list of Security & Compliance Center role groups below.

Relationship of members, roles, and role groups

A role grants permissions to do a set of tasks; for example, the Case Management role lets people work with eDiscovery cases.

A role group is a set of roles that lets people perform their job across the Security & Compliance Center; for example, the Compliance Administrator role group includes the roles for Case Management, Content Search, and Organization Configuration (plus others) because someone who’s a compliance admin will need the permissions for those tasks to do their job.

The Security & Compliance Center includes default role groups for the most common tasks and functions that you’ll need to assign people to. We recommend

simply adding people (individual users or groups) as members to the default role groups.

You can edit or delete the existing role groups, but we don’t recommend this. Instead of editing a default role group, you can copy it, modify it, and then save it with a different name.

Permissions needed to use features in the Security & Compliance Center

The following table lists the default role groups that are available in the Security & Compliance Center. To grant permissions to a user to perform a compliance task, add them to the appropriate Security & Compliance Center role group.

Managing permissions in the Security & Compliance Center only gives users access to the compliance features that are available within the Security & Compliance Center itself. If you want to grant permissions to other compliance features that aren't in the Security & Compliance Center, such as Exchange transport rules, you need to use the Exchange Admin Center.

To see how to grant access to the Security & Compliance Center, check out Give users access to Office 365 Compliance admin center.

Role group

Description

Compliance Administrator1

Members can manage settings for device management, data loss prevention, reports, and preservation.

eDiscovery Manager

Members can perform searches and place holds on mailboxes, SharePoint Online sites, and OneDrive for Business locations. Members can also create and manage eDiscovery cases, add and remove members to a case, create and edit Content Searches associated with a case.

An eDiscovery Administrator is a member of the eDiscovery Manager role group who has been assigned additional permissions. An eDiscovery Administrator can:

- View all eDiscovery cases in your organization.
- Manage any eDiscovery case after they add themself as a member of the case.
- Access Office 365 Advanced eDiscovery. This is because eDiscovery Administrators are automatically added as administrators in Advanced eDiscovery. Note that you have to be an eDiscovery Administrator in the Security & Compliance Center to access Advanced eDiscovery. For more information about making a user an eDiscovery Administrator, see eDiscovery cases in the Office 365 Security & Compliance Center.Note: If you want give a user administrative privileges in Advanced eDiscovery but don't want to make them an eDiscovery Administrator in the Security & Compliance Center, you can add them to the eDiscovery Manager role group and then add them as an administrator in Advanced eDiscovery. For instructions, see Setting up users and cases in Office 365 Advanced eDiscovery.

Organization Management1

Members can control permissions for accessing features in the Security & Compliance Center, and also manage settings for device management, data loss prevention, reports, and preservation.

Note that in order for a user who is not a global administrator to see the list of devices managed by MDM for Office 365 and perform actions on these devices, such as retiring a device from MDM for Office 365, the user must be an Exchange administrator.

Note: Office 365 global admins are automatically added as members of this role group.

Reviewer

Members can only view the list of cases on the eDiscovery cases page in the Security & Compliance Center. They can't create, open, or manage an eDiscovery case. The primary purpose of this role group is to allow members to view and access case data in Advanced eDiscovery.

This role group has the most restrictive eDiscovery-related permissions.

Security Administrator

Membership in this role group is synchronized across services and managed centrally. This role group is not manageable through the administrator portals. Members of this role group may include cross-service administrators, as well as external partner groups and Microsoft Support. By default, this group may not be assigned any roles. However, it will be a member of the Security Administrators role groups and will inherit the capabilities of that role group.

All of the read-only permissions of the Security reader role, plus a number of additional administrative permissions for the same services: Azure Information Protection, Identity Protection Center, Privileged Identity Management, Monitor Office 365 Service Health, and Office 365 Security & Compliance Center.

Security Reader

Members have read-only access to a number of security features of Identity Protection Center, Privileged Identity Management, Monitor Office 365 Service Health, and Office 365 Security & Compliance Center.

Membership in this role group is synchronized across services and managed centrally. This role group is not manageable through the administrator portals. Members of this role group may include cross-service administrators, as well as external partner groups and Microsoft Support. By default, this group may not be assigned any roles. However, it will be a member of the Security Reader role groups and will inherit the capabilities of that role group.

Service Assurance User

Members can access the Service assurance section in the Office 365Security & Compliance Center. Service assurance provides reports and documents that describe Microsoft’s security practices for customer data that's stored in Office 365. It also provides independent third-party audit reports on Office 365. For more information, see Service assurance in the Office 365 Security & Compliance Center.

Supervisory Review

Members can create and manage the policies that define which communications are subject to review in an organization. For more information, see Configure supervisory review policies for your organization.

Note: 1 This role group doesn't assign members the permissions necessary to search the Office 365 audit log or to use any reports that might include Exchange data, such as the DLP or ATP reports. To search the audit log or to view all reports, a user has to be assigned permissions in Exchange Online. This is because the underlying cmdlet used to search the audit log is an Exchange Online cmdlet. Office 365 global admins can search the audit log and view all reports because they're automatically added as members of the Organization Management role group in Exchange Online. For more information, see Search the audit log in the Office 365 Security & Compliance Center.

Fonte: support.office.com