Filename: microsoft-ms101-13-1-1-search-content-using-security-and-compliance-center-overview
ShowName: Microsoft 365 Mobility and Security
SubTitle: Exam MS-101
Topic: Manage eDiscovery
EpisodeName: Search Content Using Security & Compliance Center Overview
Description: Adam and Wes discuss the steps necessary to help you successfully search content by using the Security & Compliance Center.

Search Content Using Security & Compliance Center - Overview

Manage Microsoft 365 Governance and Compliance (35-40%)

Manage eDiscovery
• Search Content Using Security & Compliance Center - Overview
• Search Content Using Security & Compliance Center - Roles
• Plan for in-place and legal hold
• Configure eDiscovery

==========

Search Content Using Security & Compliance Center - Overview

Microsoft 365 admin centers and dashboards

Configure your security and compliance settings in these admin centers and dashboards to protect your Office 365 environment:

Office 365: https://admin.microsoft.com

Enterprise Mobility + Security: https://portal.azure.com

Enterprise Mobility + Security: https://portal.cloudappsecurity.com

Licensing for content search in O365 is tied to eDiscovery. The key licensing types that include eDiscovery are:

```
E1 | F1 | Business Essentials | Business Premium:

E1 provides the lowest eDiscovery/content search capability, allowing for
```

searching across O365 services, as well as searching across multiple mailboxes or sites in a single search. You CANNOT use content holds or export results from searches.

```
NOTE: F1 plans used to be "K" plans. F plans are designated for
```

"Firstline Workers"

https://www.microsoft.com/en-us/microsoft-365/business/office-365-f1?activetab=pivot:faqtab

```
E3: All of the E1 functionality plus the ability to export data from the
```

searches and the use of content holds. In addition, you can use eDiscovery cases, which allow you to organize and segment searches.

```
E5: All of the E3 functionality plus access to the Advanced eDiscovery feature
```

set, which uses cloud based analytics to assess searches.

NOTE: If you have an E3 license and want to use the Advanced eDiscovery capability, you can purchase the Advanced Compliance add-on instead of upgrading to an E5 license. Any users targeted by Advanced eDiscovery must have an E5 license.

What permissions are necessary to perform eDiscovery or content searches?

BY DEFAULT, NOBODY HAS PERMISSION !!! EVEN o365 ADMINS.

The primary eDiscovery-related role group in Security & Compliance Center is called eDiscovery Manager.

There are two subgroups within this role group:

```
eDiscovery Managers - can use the Content Search tool in the Security &
```

Compliance Center to search content locations in the organization, and perform various search-related actions such as preview and export search results.

Members can also create and manage eDiscovery cases, add and remove members to a case, create case holds, and run Content Searches associated with a case, and access case data in Office 365 Advanced eDiscovery.

An eDiscovery Managers can only access and manage the cases they create.

```
eDiscovery Administrators - member of the eDiscovery Manager role group, and
```

can perform the same Content Search and case management-related tasks that an eDiscovery Manager can perform. Additionally, an eDiscovery Administrator can:

```
• Access all cases that are listed on the eDiscovery cases page in the
```

Security & Compliance Center

```
• Access case data in Advanced eDiscovery for any case in the organization

• Manage any eDiscovery case after they add themselves as a member of the case
```

You have to be a member of the Organization Management role group (or be assigned the Role Management role) to assign eDiscovery permissions in the Security & Compliance Center.

You can use the Add-RoleGroupMember cmdlet in Security & Compliance Center PowerShell to add a mail-enabled security group as a member of the eDiscovery Managers subgroup in the eDiscovery Manager role group.

However, you cannot add a mail-enabled security group to the eDiscovery Administrators subgroup.

You can also use the Add-eDiscoveryCaseAdmin cmdlet to make a user an eDiscovery Administrator. However, the user must be assigned the Case Management role before you can use this cmdlet to make them an eDiscovery Administrator.