

Module 3: Managing role delegation, security, and compliance in Microsoft 365

In this module, you'll learn how to configure role delegation to maintain administrative tasks and how to use administrative units in Microsoft 365 to delegate administration. You'll also learn about the Microsoft Defender and Microsoft Purview platforms and how you can use them to provide security and compliance to Microsoft 365 services.

By completing this module, you'll achieve the knowledge and skills to:

- Implement roles and role assignments.
- Implement administrative units.
- Manage Microsoft 365 security and compliance.

Lesson 1: Roles and role assignments

In an on-premises Active Directory environment, an administrator uses security groups to implement delegated management. They add a user to a security group, and by using the Delegate Control wizard in Active Directory Domain Services (AD DS), they specify a level of administrative permissions on an organizational unit (OU). Microsoft 365 uses a slightly different process known as role-based access control (RBAC), which we'll discuss in this lesson.

By completing this lesson, you'll achieve the knowledge and skills to:

- Describe roles and role groups.
- Manage role assignments.
- Apply the principle of least privilege.

Roles and role groups

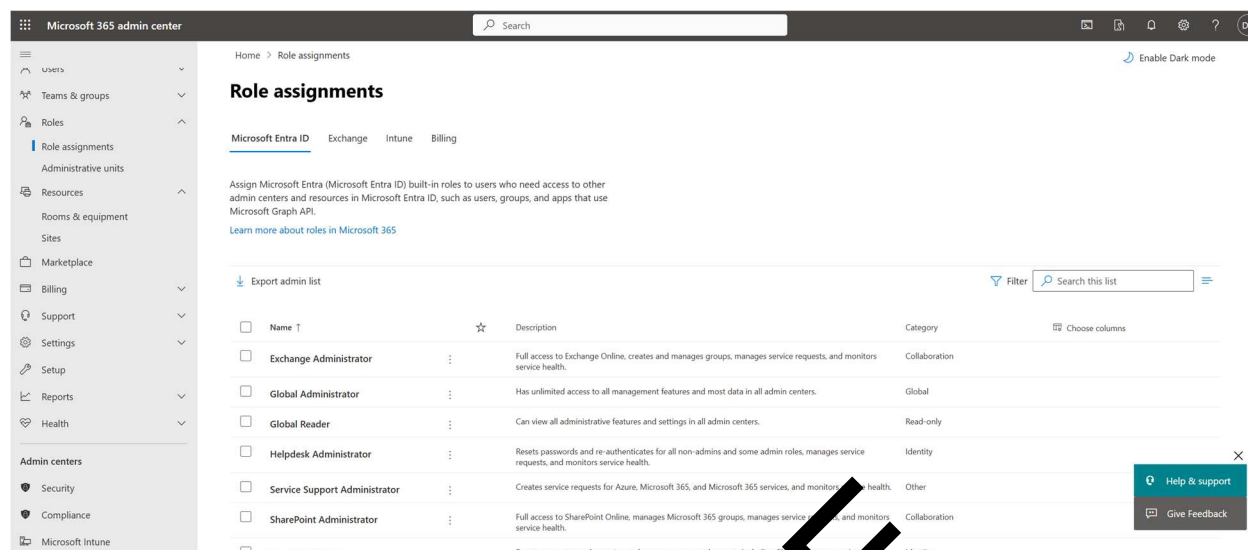


Figure 1: Reviewing the role assignments in Microsoft 365 admin center

Your Microsoft 365 tenant contains a number of built-in roles, which are assigned predetermined permissions on the objects within your tenant. You can assign a role to a user, thereby enabling that user to perform the administrative function defined by the role's permissions. You can review and manage these roles in the Microsoft 365 admin center. The Microsoft 365 admin center displays the roles in four categories:

- **Entra ID.** Enables you to assign roles to users that require access to other admin centers or resources, such as users, groups, and apps.
- **Exchange.** Enables you to assign specialist messaging management roles to your users, so that they can manage email services, recipients, and related services and objects.
- **Intune.** Contains the built-in roles used to manage devices and their properties in your organization.
- **Billing.** Contains three roles that enable you to delegate aspects of billing management for your organization.

Built-in Roles

You'll primarily rely on the roles defined on the **Entra ID** tab. There are numerous built-in Entra ID roles, and some of the more important roles are described in the following table.

Table 1: Overview of important built-in Entra ID roles in Microsoft 365

Role	Description
Billing Administrator	Purchases products, manages subscriptions, and monitors service health.

Cloud Device Administrator	Enables, disables, and deletes devices. Can also read BitLocker recovery keys.
Compliance Administrator	Manages regulatory compliance and maintains data governance.
Exchange Administrator	Has full access to Exchange Online and can perform all management and administrative tasks in Exchange Online.
Global Administrator	Has unlimited administrative access to Microsoft 365 apps and data.
Helpdesk Administrator	Can reset passwords for all non-admin users (and some admin roles), manages service requests, and monitors service health.
License Administrator	Assigns and manages user licenses.
Password Administrator	Can reset passwords for all non-admin users and some admin roles.
SharePoint Administrator	Provides full administrative access to SharePoint Online.
Teams Administrator	Provides full administrative access to Microsoft Teams.
User Administrator	Has the same permissions as the Helpdesk Administrator, but can also create and manage users and groups.
Windows 365 Administrator	Provisions and manages all aspect of cloud PCs.

Reviewing a role's details

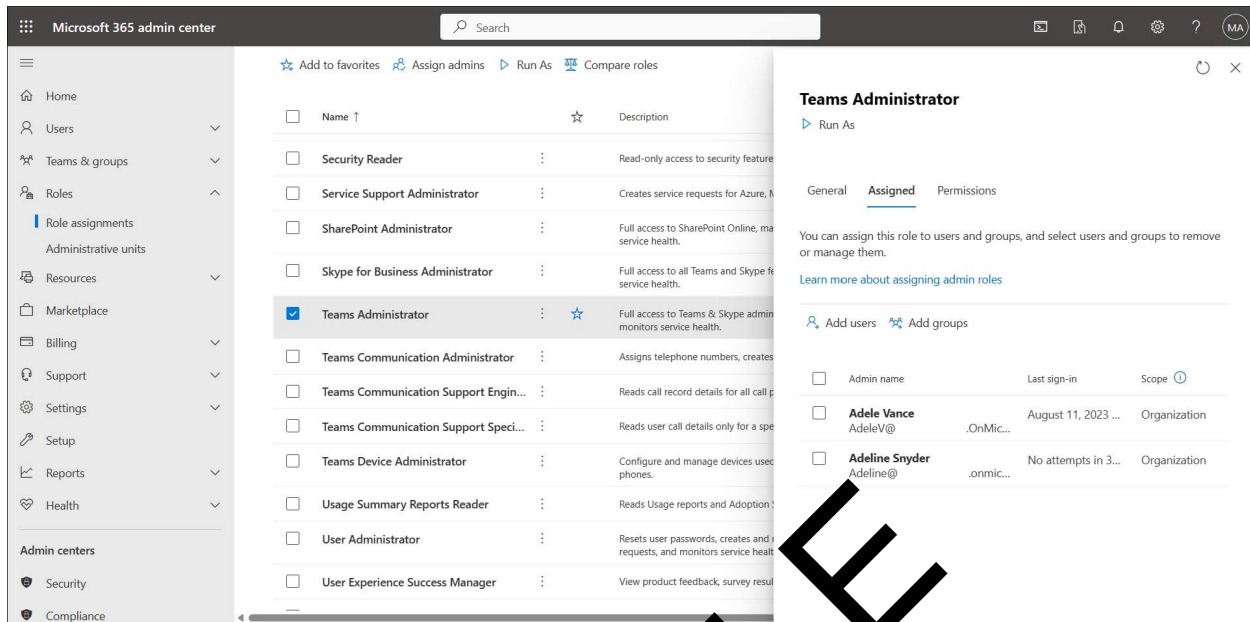


Figure 2: Reviewing the details of a built-in role

To review details about a role from the Microsoft 365 admin center:

1. Open the **Microsoft 365 admin center**.
2. In the navigation pane, expand **Roles**, and then select **Role assignments**.
3. Select the required role, and in the details pane on the right, review the information displayed on the following tabs:
 - **General**. Describes how to use the role.
 - **Assigned**. Lists the users and groups that have been assigned the role. Enables you to add additional assignments.
 - **Permissions**. Displays the permissions the role has.

To retrieve a list of Entra ID roles, you can also use the Windows PowerShell **Get-MgDirectoryRole** cmdlet. For example, the following command displays the output in Figure 3.

```
Get-MgDirectoryRole | ft DisplayName, Description
```

```
Administrator: Windows Powe x + v
PS C:\Users> get-MgDirectoryRole | ft DisplayName, Description

DisplayName      Description
-----
Teams Administrator Can manage the Microsoft Teams service.
Authentication Administrator Allowed to view, set and reset authentication method information fo...
Compliance Administrator Can read and manage compliance configuration and reports in Azure A...
Message Center Reader Can read messages and updates for their organization in Office 365 ...
Exchange Administrator Can manage all aspects of the Exchange product.
Directory Readers Can read basic directory information. Commonly used to grant direct...
Global Administrator Can manage all aspects of Azure AD and Microsoft services that use ...
Azure AD Joined Device Local Administrator Users assigned to this role are added to the local administrators g...
Security Administrator Security Administrator allows ability to read and manage security c...
Directory Synchronization Accounts Only used by Azure AD Connect service.
Billing Administrator Can perform common billing related tasks like updating payment info...
Helpdesk Administrator Can reset passwords for non-administrators and Helpdesk Administrat...
Intune Administrator Can manage all aspects of the Intune product.
Teams Communications Administrator Can manage calling and meetings features within the Microsoft Teams...
Desktop Analytics Administrator Can access and manage Desktop management tools and services.
Exchange Recipient Administrator Can create or update Exchange Online recipients within the Exchange...
Message Center Privacy Reader Can read security messages and updates in Office 365 Message Center...
Hybrid Identity Administrator Can manage AD to Azure AD cloud provisioning, Azure AD Connect, and...
```

Figure 3: Displaying the list of Entra ID roles

Adding custom roles

Although there are many built-in roles, you might want to create your own roles with particular permissions. Although you cannot currently add a custom role in the Microsoft 365 admin center, you can do so by using the Microsoft Entra admin center.

To create a custom role:

1. Open the **Microsoft Entra admin center**.
2. Expand **Identity** and then select **Show more**.
3. In the navigation pane, select **Roles & admins**.
4. Select **Roles & admins** again.
5. On the **Roles and administrators | All roles** page, select **+ New custom role**.
6. On the **New custom role** page, on the **Basics** tab, enter the following information and then select **Next**:
 - A name for your role.
 - A meaningful description.
 - The baseline permissions, and you can choose start from scratch, or close from a previously created custom role.
7. On the **Permissions** tab, select the required permissions, and then select **Next**.
8. On the **Review + create** tab, review the details, and then select **Create**.

Managing role assignments

To enable delegated administration of your Microsoft 365 tenant, you'll need to assign the required roles to the appropriate users. You can assign roles by using the Microsoft 365 admin center and Windows PowerShell.

Tip: You should always assign roles to groups rather than to users directly, because this makes ongoing role management simpler and more secure. For example, if you want to assign Adele the Helpdesk Administrator role, you should create a group (perhaps called Helpdesk-Admins) and add Adele to the group. You can then assign the Helpdesk Administrator role to the Helpdesk-Admins group. If Adele moves to a new job in your organization, and is replaced by Simon, you only need to remove Adele from the Helpdesk-Admins group. To add Simon to that group; you won't need to unassign the Helpdesk Administrator role from Adele, nor assign that role to Simon's account.

To assign a role using the Microsoft 365 admin center:

1. In the navigation pane, select **Teams & groups**, and then select **Active teams & groups**.
2. On the **Active teams and groups** page, select the **Security groups** tab.
3. Select **+ Add a security group**.
4. On the **Set up the basics** page, enter a **Name** and **Description**, and then select **Next**.
5. On the **Edit settings** page, select the **Role assignment** check box, and then select **Next**.
6. On the **Review and finish adding group** page, select **Create group**.
7. When prompted, select **Close**.
8. Search for and select your newly created group.
9. On the details page for the selected group, on the **General** tab, in the **Roles** section, select **Manage roles**.
10. On the **Manage admin roles** page, select **Admin center access** and then select the appropriate roles from the displayed list. When you're done, select **Save changes**.

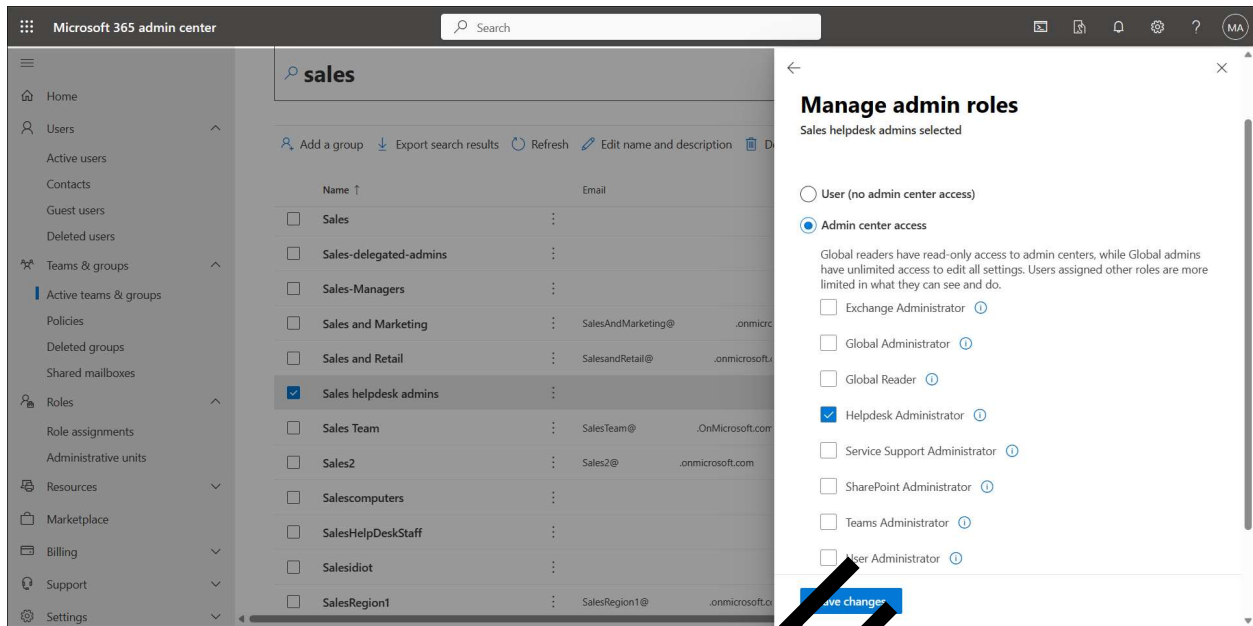


Figure 4: Adding a role to a group

11. Select the back button, and select the **Members** tab.
12. Select the **View all and manage members** link.
13. Select **Add members** and then select the required user(s).
14. Select **Add**.
15. Close the group details page.

To review the roles assigned to a user in the Microsoft 365 admin center:

1. Locate and select the required user account.
2. On the user's detail page, on the **Account** tab, select the **Manage roles** link in the **Roles** section.
3. You can review all assigned roles, and those assigned via a group are indicated with the relevant group name. Make any changes required, and then select **Save changes**.

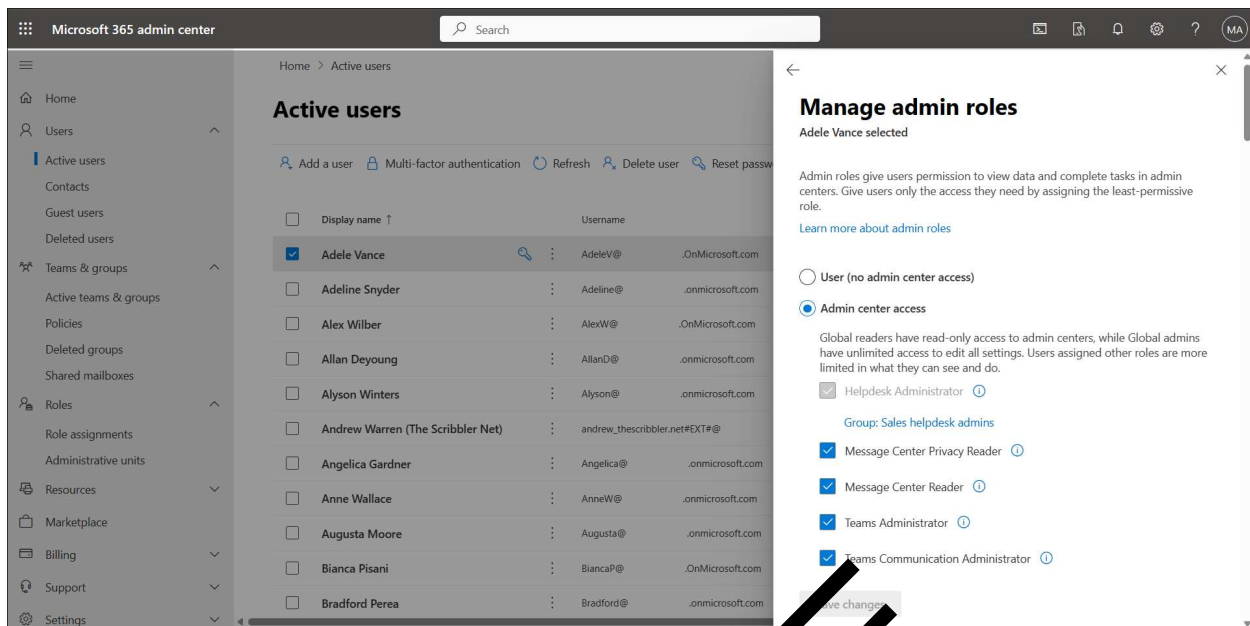


Figure 5: Reviewing a user's assigned roles

Applying the least privilege concept

When considering how to assign roles within your organization, it's important that you remember to only assign the permissions that are specifically required to perform a job role, and no more. This is known as the principle of applying least privilege.

For example, if a user is assigned the responsibility of resetting user passwords, don't assign the User Administrator or Global Administrator role. Instead, assign the Helpdesk Administrator role. Better yet, create a custom role with only the permissions required to reset passwords. In addition, consider only assigning the role when the user needs to exercise that role. In Microsoft 365, this is known as just-in-time access.

Note: Just-in-time access is a feature of Privileged Identity Management and is only available in premium versions of Microsoft Entra ID.

Tip: You manage Privileged Identity Management in the Microsoft Entra admin center.

Assigning a just-in-time role

To assign a role that implements just-in-time access:

1. Open the **Microsoft Entra admin center**.
2. Locate and select the group (or user) account you want to assign a just in time role to.
3. On the navigation page for the user or group, select **Assigned roles**.
4. On the **Active assignments** tab, select **+ Add assignments**.

5. On the **Add assignments** page, in the **Search role** list, select the relevant role, and then select **Next**.
6. On the **Setting** tab, in the **Assignment type** section, choose:
 - **Eligible**. Requires confirmation before the assigned role can be exercised.
 - **Active**. Means that the role is immediately available for use. If you choose **Active**, you must enter a justification in the text box that subsequently appears on the **Setting** page.
 - **Permanently eligible / Permanently assigned**. You can make the role permanently eligible / permanently assigned, or specify a start and end date and time. This is useful for scenarios where you want to make the role assigned for a short period, such as when the usual administrator is on vacation. If you cleared this check box, then enter the relevant date period.
7. For our purposes, choose **Eligible**, and then select **Assign**.

You can verify the assignment of the eligible role by reviewing the properties of a user account that belongs to the configured group. On the **Assigned roles** page for the selected user account, select the **Eligible assignments** tab.

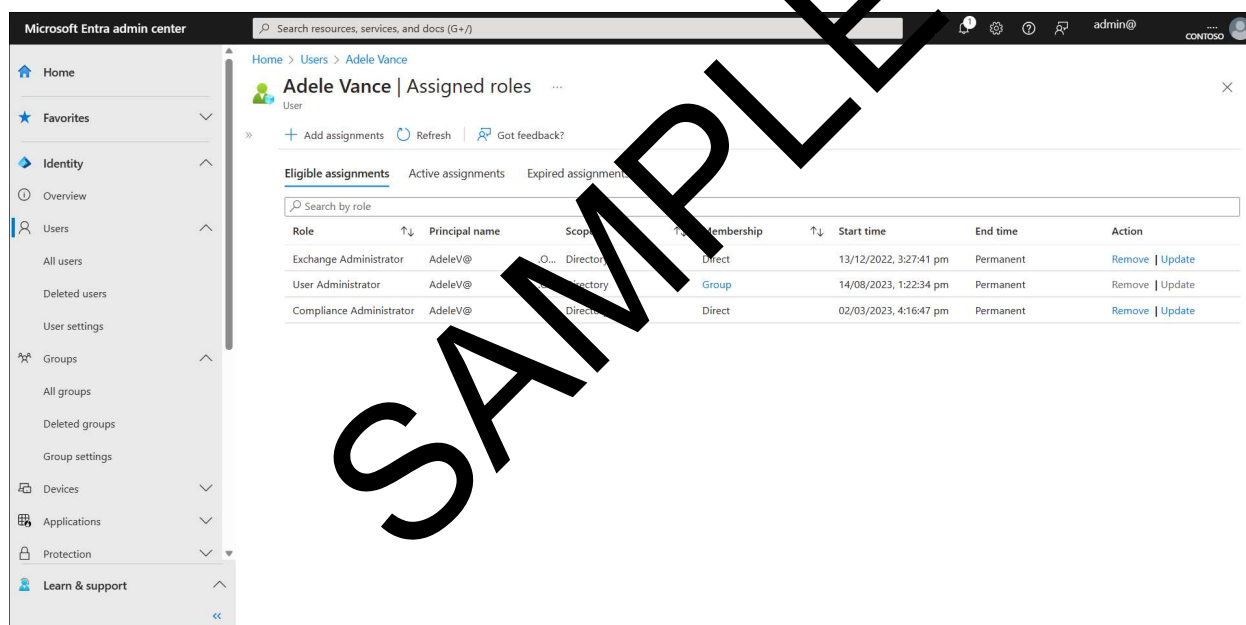


Figure 6: Reviewing a user's eligible roles

When a user attempts to exercise a right to perform a management task from a role that they hold as eligible, they must activate the role. This requires that they complete a form stating the reason for activation. The role is then activated. This helps reduce the security exposure for your organization as the role is only assigned when being used.

You can configure the settings so that a user's request to activate the role requires approval. This process generates a pending approval to which a delegated approver can respond. Until approved, the user cannot exercise the permissions granted by the role assignment. Delegated approvers receive an email notification.

To configure the notification settings for a role:

1. Open **Microsoft Entra admin center**.
2. In the navigation pane, select **Show more**, and then expand **Roles & admins**.
3. Select **Roles & admins**.
4. Select the relevant role; for example, Helpdesk Administrator.
5. On the **Assignments** page, select **Settings**.
6. On the **Role settings details** page for the role, select **Edit**.
7. There are three tabs:
 - **Activation**. Update the required activation settings, such as, on activation, require:
 - **None**
 - **Azure MFA**
 - **Microsoft Entra Conditional Access authentication context**
 - **Assignment**. Update the assignment settings, such as:
 - **Allow permanent assignment**
 - **Require Azure Multi-Factor Authentication on active assignment**
 - **Notification**. Update details that relate to who receives notifications on the following actions:
 - **Send notifications when members are assigned as eligible to this role**
 - **Send notifications when members are assigned as active to this role**
 - **Send notifications when eligible members activate this role**
8. When you've made the required changes, select **Update**.

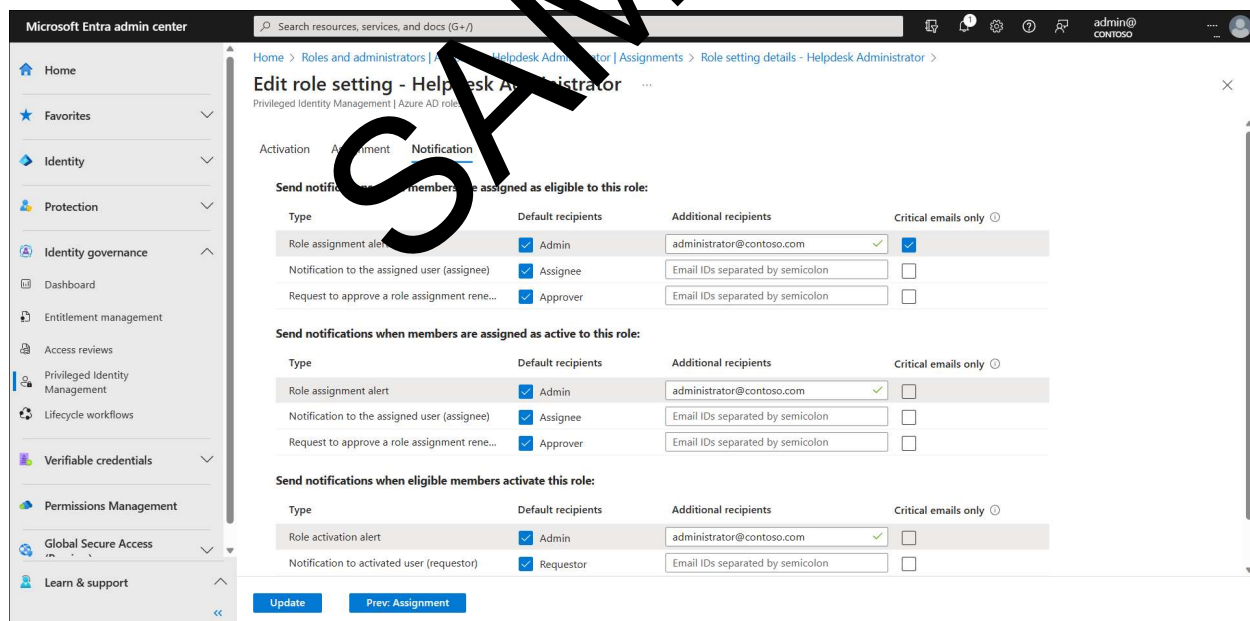


Figure 7: Updating notifications for an assigned role

Periodically, it's a good idea to review the roles that are being used within your organization. You can do this within the **Privileged Identity Management** folder in the Microsoft Entra admin center:

1. Expand **Identity governance**, and then select **Privileged Identity Management**.
2. In the details pane, select the **Manage** button in the **Manage access** section.
3. On the **Roles** page, you can review the **Active** and **Eligible** assignments for all listed roles.

Reviewing the assigned roles

It's also worth reviewing the assigned roles. You can do this by selecting **Privileged Identity Management** in **Identity governance**. Then:

1. In the **Discover and monitor** section, select **Discover**.
2. On the **Assignments** page, review the **Eligible assignments**, **Active assignments**, and **Expired assignments** tabs to review the details about role holders.
3. Select **Discovery and insights** in the **Manage** section of the navigation pane. This page displays recommendations that can help reduce your security exposure, such as:
 - The number of global administrator assignments.
 - The number of accounts with highly privileged roles.
 - The service principals with privileged role assignments.

You can then choose to reduce the instances of these privileged role assignments.

Lesson 2: Administrative units

It's important that a delegated administrator—that is, one assigned a specific role or roles, can exercise their administrative control over specific resources. In large organizations, it can be beneficial to target that administrative control to specific parts of the directory.

In on-premises AD DS, administrative control is delegated to a domain, or to an OU within that domain. In Microsoft 365, you assign a role to a security principal, and scope that assignment to the whole directory, or to only a part of the directory referred to as an *administrative unit*.

By completing this lesson, you'll achieve the knowledge and skills to:

- Describe administrative units.
- Create and manage administrative units.
- Delegate role assignments on administrative units.

Overview of administrative units

Administrative units enable you to target your delegated administration. Typically, you might create administrative units that represent:

- Departments.
- Geographical regions.
- Specific projects within your organization.

You can then add the following objects to the administrative units:

- Users
- Groups
- Devices

Tip: You can add groups to administrative units, but that doesn't add the members of the group to the administrative unit. It merely brings the group into the management scope of the administrative unit.

Finally, you would implement a delegated administrative model that meant that specific roles are scoped to the administrative units.

A typical scenario might be as follows:

1. Create an administrative unit for the research department.
2. Add research department users, groups, and their devices to the Research administrative unit.

Tip: A resource can belong to a maximum of 30 administrative units.

3. Create a role with appropriate administrative permissions and scope it to the Research administrative unit.
4. Assign the role and its scope to an appropriate administrative group.

Creating and managing administrative units

You can use the Microsoft 365 admin center, the Microsoft Entra admin center, and Windows PowerShell to create and manage your administrative units.

Warning: Administrative units cannot be nested.

By using the Microsoft 365 admin center, you're guided through the process with a wizard:

1. In the Microsoft 365 admin center, in the navigation pane, select **Show all**.
2. Expand **Roles**, and then select **Administrative units**.
3. On the **Administrative units** page, select **+ Add unit**.
4. In the **Add administrative units** wizard, on the **Basics** page, enter a **Name** and **Description** for your administrative unit, and then select **Next**.
5. On the **Add members** page, select one of the following, and then select **Next**:
 - **Add up to 20 users and groups**. Displays an area on the page with options to **Add users** and **Add groups**.
 - **Upload users**. Enables you to browse and select a CSV file that contains the details for up to 200 users. You can download a sample file to use for populating with your user details.

Tip: You can select **Next** without adding users or groups and perform that task later, when you've created the administrative unit.

- On the **Assign admins to scoped roles** page, you can select a role and then assign admins to that role. If you choose a role, you can then select **Assign admins** to choose the user or group that will be assigned the role in the scope of the administrative unit. You can also just select **Next**, and complete this process later.

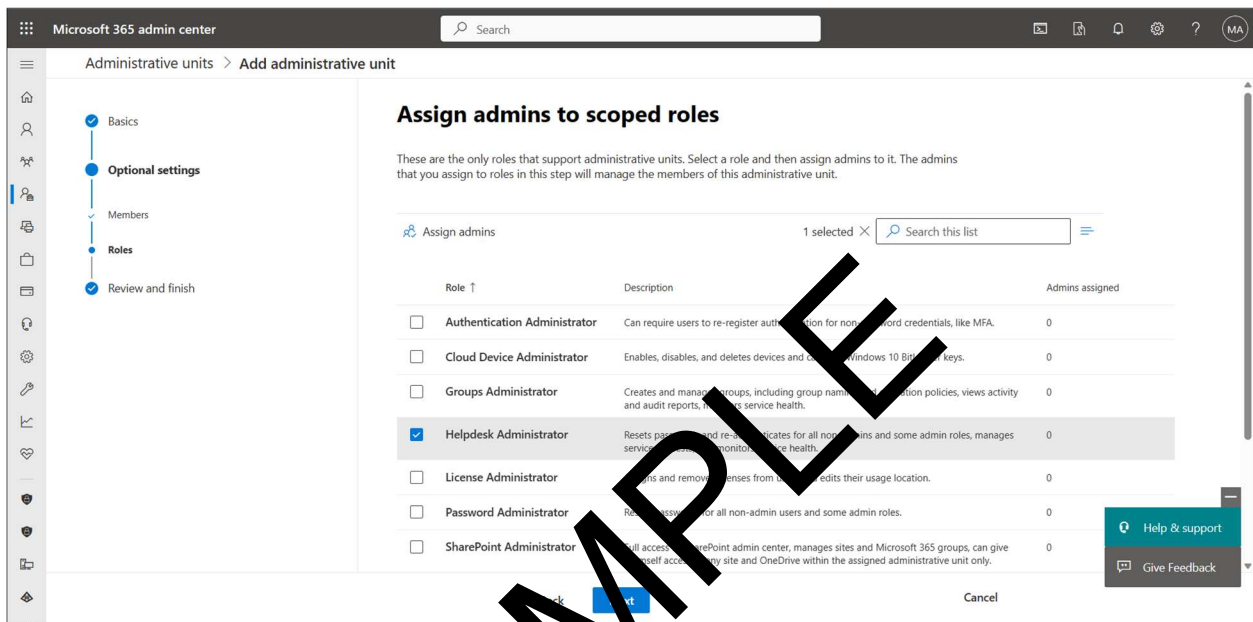


Figure 8: Assigning a scoped admin role during creation of the administrative unit

- On the **Review and finish** page, select **Add**.

Note: There are only 11 roles that support scoped delegation. These are described in the following topic.

To manage an administrative unit, select it within the Microsoft 365 admin center. You can then:

- Add members, such as users, groups, and devices.
- Manage role assignments.

To add devices to an administrative unit, you must use the Microsoft Entra admin center:

- Open **Microsoft Entra admin center**.
- In the navigation pane, select **Show more**.
- Expand **Devices** and then select **All devices**.
- Select the appropriate device.
- In the device details, select the **Administrative Units** page.
- On the **Administrative Units** page, select **Assign to administrative unit**.

7. Choose the relevant administrative unit, and then click **Select**.

To use Windows PowerShell, you must first connect to the administrative unit context. You can achieve this by using the **Connect-MgGraph** cmdlet. Next, you'll need to use the **New-MgDirectoryAdministrativeUnit** cmdlet to create your administrative unit. For example:

```
Connect-MgGraph -Scopes "AdministrativeUnit.ReadWrite.All"
$params = @{
    DisplayName = "Research Department"
    Description = "Research Department administrative unit"
    Visibility = "HiddenMembership"
}
$adminUnitObj = New-MgDirectoryAdministrativeUnit -BodyParameter $params
```

Managing role assignments on administrative units

As discussed earlier, you can assign the necessary roles on your administrative units during their creation. You can also configure these roles subsequently.

Available roles

Currently, there are only ten roles that can be assigned to administrative units:

- Authentication Administrator
- Cloud Device Administrator
- Groups Administrator
- Helpdesk Administrator
- License Administrator
- Password Administrator
- SharePoint Administrator
- Teams Administrator
- Teams Device Administrator
- User Administrator

Tip: An additional role displays in Microsoft Entra admin center: Printer Administrator.

Assigning a role to the scope of an administrative unit

To use the Microsoft 365 admin center to assign roles to your administrative units after they've been created:

1. Open the **Microsoft 365 admin center**.
2. In the navigation pane, select **Show all**.

3. Expand **Roles**, and then select **Administrative units**.
4. Select the relevant administrative unit.
5. Select the **Role assignments** tab.
6. In the list of roles, select the relevant role, and then select **Assign admins**.
7. On the **Assigned admins** page, select either **Add users** or **Add groups**. You can choose up to 20 users or groups at a time to assign to the role.
8. Select **Add**. Close the open window.

Tip: You can also set up role assignments and scope to an administrative unit with Windows PowerShell by using the **New-MgRoleManagementDirectoryRoleAssignment** cmdlet.

Lesson 3: Security and compliance

When your organization moves its data to the cloud, your security focus shifts. You're far less concerned with server hardening, or firewall zone security. Instead, your attention switches to endpoint security, and to the management and movement of your organizational data between the cloud repositories (such as Exchange Online, SharePoint, and OneDrive) and your users' devices.

Microsoft 365 provides numerous security features, including Microsoft 365 Defender and Microsoft Purview, which help you secure your organizational data and devices. They also enable you to maintain data compliance with both organizational and governmental requirements.

In this lesson, we'll explore the functions and features of both Microsoft 365 Defender and Microsoft Purview to learn how they can help you manage security and compliance in your organization.

By completing this lesson, you'll achieve the knowledge and skills to:

- Describe Microsoft 365 Defender.
- Review Secure Score for your organization.
- Describe compliance in Microsoft Purview.
- Explain Microsoft 365 information governance.

Overview of the Microsoft 365 Defender platform

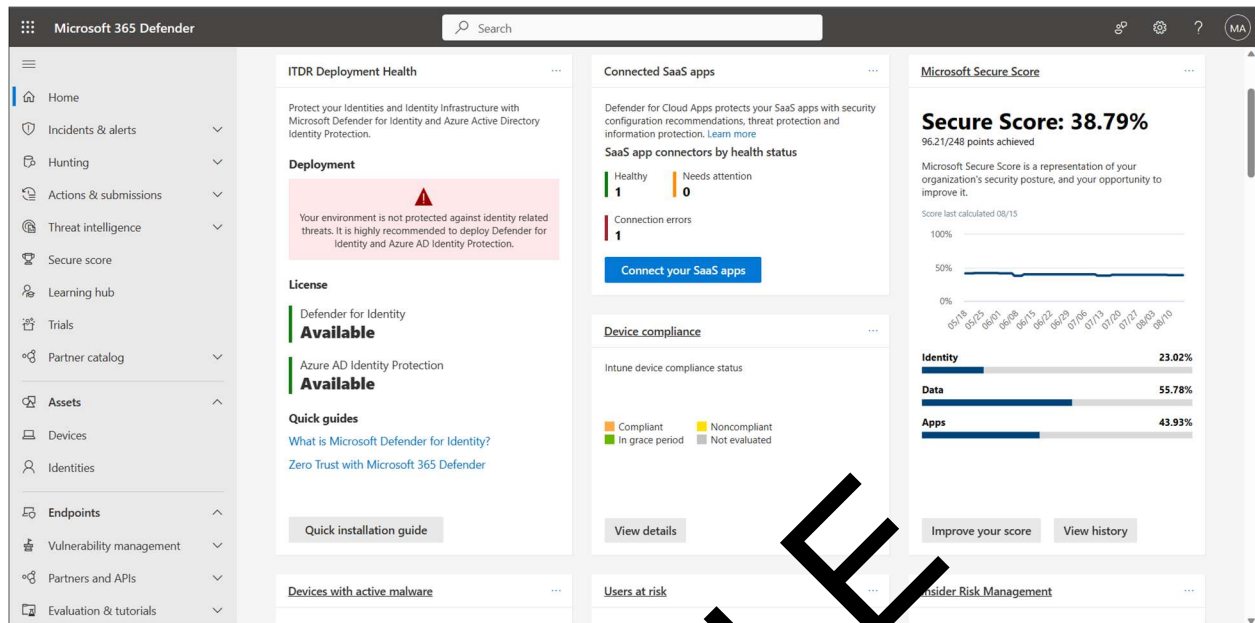


Figure 9: Reviewing an overview of your organization's security posture

You can access Microsoft 365 Defender from the **Admin centers** section in the Microsoft 365 admin center. Select **Security** to launch **Microsoft 365 Defender** on a new browser tab. Microsoft 365 Defender provides a single point of contact for you to analyze and configure the security posture of your organization.

The following table describes the available functionality in Microsoft 365 Defender.

Table 2: Functionality of Microsoft 365 Defender

Component	Description
Incidents & alerts	Contains: - Incidents. Displays and describes recent security incidents. Includes severity information and impacted assets. - Alerts. Displays and describes recent security alerts. Includes severity information and impacted assets.
Hunting	Provides both advanced hunting and custom detection rules that enable you to search for evidence of security issues. You can search on alerts and behaviors, apps and identities, email and collaboration, devices, and other factors.
Actions & submissions	Provides access to the action center and to submissions. If auditing is enabled, lets you review data returned by auditing features.

Threat intelligence	Contains Threat analytics , which displays possible threats and where available, makes suggestions for threat mitigations and actions. Threats include ransomware, extortion, and phishing. Summary displays latest threats, high-impact threats, and highest exposure threats,
Secure Score	Displays your organization's security score. Includes suggested actions for improving the score.
Trials	Displays upcoming security features that you can trial within your organization.
Assets	Contains: ▪ Devices. Provides a device inventory: computers & mobile, network devices, IoT devices, and others. Provides details about possible risks. ▪ Identities. Displays detailed information about your organization's identities, such as users, groups, and apps. You can select an item, such as a user, to review more detailed information about that security principal.
Endpoints	Provides access to: ▪ Vulnerability management. Displays options for a vulnerability dashboard, recommendations for vulnerability mitigations, remediations, inventories, weaknesses, and more. ▪ Partners and APIs. Displays connected apps and the API Explorer. ▪ Evaluation & tutorials. Provides access to the evaluation lab and to both tutorials and simulations of upcoming features. ▪ Configuration Management. The dashboard displays connected SaaS apps, your security score, device information, and users at risk.
Email & collaboration	Provides access to: ▪ Investigations. Displays automated investigation and response (AIR) capabilities and enables you to run automated investigation processes in response to well-known threats. ▪ Explorer. Displays details about emails, malware, phishing, campaigns, content malware, and URL clicks. ▪ Review. Enables you to access the Action Center, Quarantine, Restricted Entities, and Malware trends. ▪ Campaigns. Displays security campaign data. ▪ Threat tracker. Displays saved queries, tracked queries, and trending campaigns. ▪ Exchange message trace. Opens a new tab for the message trace center in Exchange admin center. ▪ Attack simulation training. Provides information about how to perform attack simulations for your organization. ▪ Policies & rules. Enables you to set up policies to manage devices, protect against threats, and receive alerts about various activities in your organization. ▪ Policy types. Enables you to access threat policies, alert policies, advanced alert policies, and activity alert policies.

Cloud apps	Enables you to configure and access cloud app security features, such as cloud discovery, your cloud app catalog, OAuth apps, cloud app policies, and others.
Reports	Provides links to standard reports that enable you to generate and review security-related information. Reports include Threat protection , Web protection , Device health , Device control , and Attack surface reduction rules .
Audit	Enables you to audit your organization's security posture.
Health	Displays links for service health and message center.
Permissions	Displays links that enable you to review and configure security-related roles, including: ▪ Microsoft 365 Defender ▪ Entra ID ▪ Endpoints roles & groups ▪ Email & collaboration roles ▪ Cloud Apps
Settings	Displays links to the settings for: ▪ Security center ▪ Microsoft 365 Defender ▪ Endpoints ▪ Email & collaboration ▪ Identities ▪ Device discovery ▪ Cloud Apps

What is Secure Score?

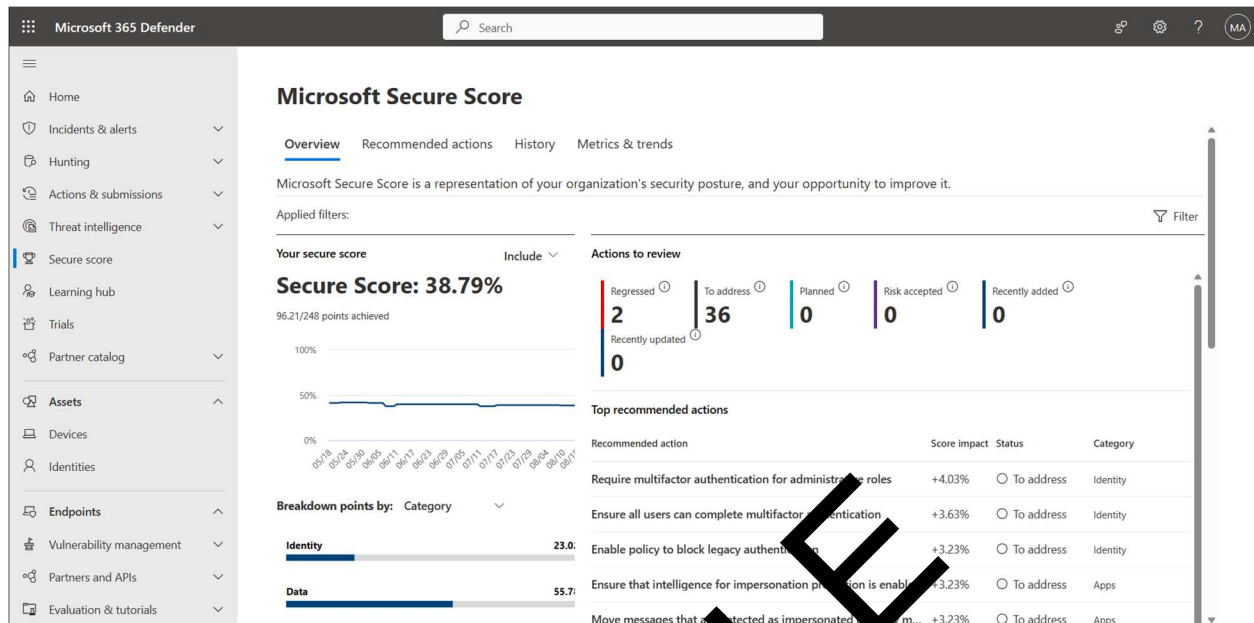


Figure 10: Reviewing the Secure Score in Microsoft 365 Defender

You can use Secure Score to gain an insight into your organization's overall security posture. This is a good place to start reviewing and improving the security of your organization. Secure Score measures the following main categories:

- Apps
- Data
- Identities

When you review the security score for your organization, it's important to remember that the score is indicative only, and based on metrics. Which is to say that a score that is beneath 100% isn't necessarily a bad thing, nor does such a score indicate that action must be taken.

It's important to remember that when reviewing security, and particularly when implementing security features, you must strike a balance between security and usability. The more secure a system is, generally, the less usable it becomes. So, when you review the score, what you're probably aiming for is a score as high as you can achieve without hindering your users' abilities to get their jobs done.

For example, when reviewing the score, if you notice a recommendation that you should implement multifactor authentication for users with high privilege, such as administrators, that would seem to be an easy win because it won't impair your users in any way. However, disabling access to Microsoft 365 resources from apps that don't support modern authentication, while ultimately desirable, might well prevent some users from being able to complete their day-to-day tasks. Therefore, you should perform a trial of such a change to help ensure that you can mitigate any possible inconvenience for your users.

Review your organization's secure score periodically as part of your regular security processes. Where new threats are identified, and your score is impacted, review recommendations and consider the impact of their implementation. It's probably worth considering planning a pilot for the implementation of security settings that you suspect might seriously impact your users.

Overview of Microsoft Purview

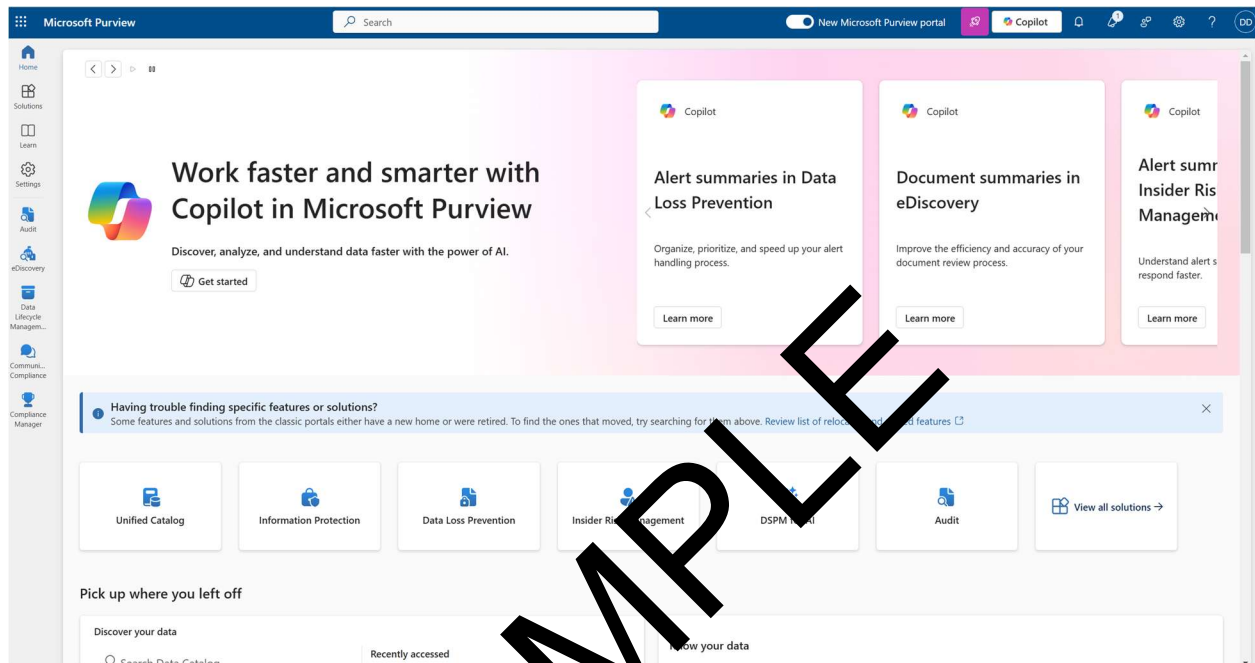


Figure 11: Microsoft Purview portal

It's often a requirement that certain types of data, whether electronically stored, or stuffed in a filing cabinet, are retained for compliance purposes. These purposes might be because of governmental or legal reasons.

For example, you must retain data because the data relates to accounting records, and your government requires their retention for five years. Or perhaps you have data that you are storing, but the data is sensitive and must only be accessed by authorized people.

Part of the problem with data compliance is knowing what data you have and where it's stored, and what rules and regulations apply to its retention. In addition, it's important to know where your organization's sensitive data resides, and how you can control access to that data.

Another major issue with data compliance is the specialist knowledge that is required around electronically stored data. Data stored in European datacenters, for example, is impacted by numerous governmental data retention and access regulations (both regional and country-specific). And the fact that you don't know what those regulations are doesn't allow you to be non-conformant with them.

Microsoft Purview is a comprehensive set of solutions that can help your organization govern, protect, and manage data, wherever it is. Microsoft Purview solutions provide integrated coverage

and help address the fragmentation of data across organizations, the lack of visibility that hampers data protection and governance, and the blurring of traditional IT management roles.

Microsoft Purview combines solutions and services together into a unified platform to help your organization:

- Gain visibility into data across the organization.
- Safeguard and manage sensitive data across its lifecycle, wherever it is.
- Govern data seamlessly in new, comprehensive ways.
- Manage critical data risks and regulatory requirements.

Microsoft Purview provides a centralized portal where you can manage all aspects of data compliance, both governmental and organizational, and manage both data retention and sensitivity.

Microsoft Purview provides a coordinated set of data-security solutions to help you discover and protect sensitive information. The solutions include:

- Microsoft Purview Data Loss Prevention
- Microsoft Purview Information Barriers
- Microsoft Purview Information Protection
- Microsoft Purview Insider Risk Management
- Microsoft Purview Privileged Access Management
-

You can launch the Microsoft Purview console from Microsoft 365 admin center by selecting **Compliance** in the **Admin centers** section to open a new tab. The Purview portal provides access to the components described in the following table.

Table 3: Microsoft Purview components

Component	Description
Compliance Manager	Displays an organizational compliance status summary, including recommendations for improvement. Details include Overview , Improvement actions , Solutions , Assessments , Regulations , Alerts , and Alert policies .
Data classification	Contains: ▪ Overview. Displays summary of the information types used in your organization's data. ▪ Classifiers. Provides options enabling you to define data classification within your organization. Classifiers include retention or sensitivity types. ▪ Content explorer. Enables you to explore email and documents in your organization that contain sensitive information or have retention or sensitivity labels applied.

	▪ Activity explorer. Enables you to review content-related activity for sensitive data or data that has labels applied. Also displays information such as whether labels were changed, or files were modified.
Data connectors	Displays the connectors used by your organization. These connectors enable movement of data to and from the Microsoft 365 environment to or from other data repositories. By understanding this data movement, you can help to identify noncompliance.
Alerts	Displays information about recent compliance issues, including severity, status, and last occurrence.
Policies	Enables you to create policies that help manage organizational compliance, including: ▪ Alert (3): ○ Alert ○ Defender for Cloud Apps ○ Alert policies ▪ Data (2): ○ Data loss prevention ○ Retention ○ Access (1), which defines terms of use
Roles & scopes	Contains: ▪ Permissions: ○ Entra ID roles. Displays available roles and number of role holders, including Global administrator, Compliance data administrator, Compliance administrator, Security reader, and Global reader. ○ Microsoft Purview. Displays available roles and number of role holders, including Organization Management, Compliance administrator, eDiscovery manager, Insider risk management. ▪ Adaptive scopes. These define the attributes and properties that define the users, groups, or sites in your organization.
Solutions	Displays a list of available compliance solutions, including catalog, audit, content search, communication compliance, data loss prevention, eDiscovery, data lifecycle management, information protection, and information barriers.
Settings	Displays: ▪ Device onboarding. Review and onboard devices that can be included in your compliance solutions. ▪ Co-authoring for files with sensitivity labels . Allow users in your organization to co-author in Office desktop documents that are encrypted by using sensitivity labels. ▪ Compliance Manager. Set up automated testing of actions, and manage the privacy of your users' data.

	▪ Information protection scanner . Review and onboard repositories to be scanned by the information protection scanner. ▪ Just-in-time protection . Monitor and evaluate content shared from devices to dynamically help prevent sensitive data from inappropriately leaving your organization.
--	--

Purview also provides a summary Compliance Score. This is accessible on the **Compliance Manager** page.



Figure 12: Reviewing the compliance score

Solutions that can impact your compliance score are:

- **Protect information**
- **Govern information**
- **Control access**
- **Manage devices**
- **Protect against threats**
- **Discover and respond**
- **Manage internal risks**
- **Manage compliance**
- **Privacy Management**
- **Infrastructure Cloud**

For each of these solutions, you can review the percentage score, and access a link that provides detailed improvement actions that you can consider.

Information governance

Microsoft supports many governmental data compliance requirements, including:

- Health Insurance Portability and Accountability Act (HIPAA)
- Health Information Technology for Economic and Clinical Health (HITECH) Act
- ISO/IEC 27017:2015 Code of Practice for Information Security Controls
- ISO 9001:2015
- ISO/IEC 27001:2013 Information Security Management Standards
- Gramm-Leach-Bliley Act (GLBA)
- Family Educational Rights and Privacy Act (FERPA)
- Federation Against Copyright Theft (FACT)
- General Data Protection Regulation (GDPR)
- European Standards EN 301 549
- Canada privacy laws

These data compliance requirements deal with data retention and appropriate access. Microsoft Purview provides a means for you to implement these requirements by using labelling of data, and data-related policies.

Overview of data retention

You can use retention labels to identify data that must be retained. You can create these labels centrally, and assign them to data by using policies. You can configure policies that enable users to assign appropriate retention labels, or else you can apply such labels automatically by using policies. Your data retention policies can be fairly generalized, and impact data anywhere in your organization, but they can also be targeted at particular repositories, such as SharePoint sites, specific mailboxes in Exchange, or within a particular Teams channel.

Implementing retention policies

Retention policies are created in the Microsoft Purview portal. When you define a retention policy, you must configure:

- A name and description.
- Scope of the policy, which is either the full directory, or an administrative unit.
- The policy type. You can choose static or adaptive. With static, you define the data locations for retention. With adaptive, the policy automatically updates criteria.
- Locations where the data resides, which can include Exchange mailboxes, SharePoint sites, OneDrive accounts, Microsoft 365 Group mailboxes and sites, Exchange public folders, Teams chats and channel messages, and Yammer.
- Retention details, such as retention period, and actions to take after that period expires (such as delete, or do nothing).

After you've created the policy, you can test it before enabling it properly in your organization.

Overview of data sensitivity

A typical user in a typical organization is likely to share organizational data. They might share this data with colleagues within your organization, or they might share the data with people outside your organization. The sharing of data is a necessity of the modern workplace, and often, if not mostly, this sharing is legitimate and necessary. Occasionally, however, users in organizations inadvertently share data with recipients that should not be able to review that data.

By using sensitivity labeling and policies, you can help to manage and, where necessary, restrict that inappropriate sharing. By classifying your data into sensitivity types, and defining policies about the decryption and movement of such data, you can begin to control this sharing.

Tip: Many catalogs and templates of predefined sensitive information are accessible in Microsoft Purview.

Implementing DLP policies

A common way to manage the sharing of sensitive data is the use of DLP policies. DLP policies in Microsoft 365 enable you to:

- Identify sensitive information in on-premises, third-party app, and Microsoft 365 repositories. Microsoft 365 repositories include:
 - Exchange distribution lists.
 - OneDrive and SharePoint.
 - Microsoft Teams channels and chat messages.
- Prevent sharing of sensitive information, whether intentional or accidental.
- Educate your users on how to remain compliant while not disrupting their workflow.
- Access reports that display content matching your organization's DLP policies.

When you create a DLP policy, you must define:

- An initial template for the type of data, or else manually define that data.
- A name and description.
- Scope of the policy, which is either the full directory, or an administrative unit.
- Locations where the data resides, which can include Exchange email, SharePoint sites, OneDrive accounts, Teams chats and channel messages, Microsoft Defender for Cloud Apps, On-premises repositories, and Microsoft Power BI.
- Confidence level required to prevent sharing.
- Sharing audience: internal or external to the organization.
- Protection actions, such as notifications, policy tips, and content-sharing restrictions.
- Permitted overrides, such as identifying as false positive, or require business justification.

After you create the policy, you can enable it immediately, or you can test it out first (with or without policy tips).

Lab 3: Managing roles and permissions in Microsoft 365

Please refer to the online lab to supplement your learning experience with exercises.

Knowledge check

Check your knowledge by answering these questions:

1. Which built-in role can perform the following tasks and only these tasks:
 - Reset passwords for all non-admin users (and some admin roles)
 - Manage service requests
 - Monitor service health
2. When creating a custom role, can you clone the initial permissions from an existing built-in role?
3. How many roles can be scoped to an administrative unit by using the Microsoft 365 admin center?
4. True or false? When creating a DLP policy, you can scope it to an administrative unit.

Note: To find the answers, refer to the knowledge check slides in the PowerPoint presentation.