Filename: microsoft-ms101-12-1-1-configuring-audit-logging
ShowName: Microsoft 365 Mobility and Security
SubTitle: Exam MS-101
Topic: Manage Auditing
EpisodeName: Configuring Audit Logging
Description: Adam and Wes discuss the steps necessary to help you successfully configure audit logging.

Configuring Audit Logging

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

Manage Auditing
• Configure Audit Log Retention
• Configure Audit Policy
• Monitor Unified Audit Logs

==========

Configure Audit Log Retention | Configure Audit Policy

While auditing is now enabled by default, you need to ensure that permissions and licensing are set properly:

```
Permissions - For complete control over auditing, you need any of the following:

    • Organization Management Role
    • Compliance Management Role
    • Global Administrator
```

For searching and viewing audit logs, you need:

```
    • View-Only Audit Logs Role
    • Audit Logs Role


Licensing -

    • E3 offers up to 90 days of log retention
    • E5 offers up to 365 days of log retention
```

You can also use ANY o365 subscription and add on the Advanced Compliance license to get up to 365 days of log retention.

You can get the Advanced Compliance license bundled with Azure Information Protection - it is called the Information Protection & Compliance bundle.

What do I get with Default Auditing?

```
• User activity in SharePoint Online and OneDrive for Business
• User activity in Exchange Online (Exchange mailbox audit logging)
• Admin activity in SharePoint Online
• Admin activity in Azure Active Directory (the directory service for Office 365)
• Admin activity in Exchange Online (Exchange admin audit logging)
• User and admin activity in Sway
• eDiscovery activities in the security and compliance center
• User and admin activity in Power BI
• User and admin activity in Microsoft Teams
• User and admin activity in Dynamics 365
• User and admin activity in Yammer
• User and admin activity in Microsoft Flow
• User and admin activity in Microsoft Stream
• Analyst and admin activity in Microsoft Workplace Analytics
• User and admin activity in Microsoft PowerApps
```

How do I enable additional auditing in Exchange?

Why, PowerShell of course !!!

```
Set-Mailbox "name of mailbox goes here" -AuditEnabled $True
```

How about to enable for ALL mailboxes at once?

```
Get-Mailbox -ResultSize Unlimited -Filter {RecipientTypeDetails -eq "UserMailbox"} | Set-Mailbox -AuditEnabled $True
```

Monitor Unified Audit Logs:

How do I know if logging is enabled?

PowerShell to the rescue !!

```
Get-AdminAuditLogConfig | FL *unified*
```

Want to turn on/off logging?

```
Set-AdminAuditLogConfig -UnifiedAuditLogIngestionEnabled $True

Set-AdminAuditLogConfig -UnifiedAuditLogIngestionEnabled $False
```