

Microsoft 365Solutions and architecture ▾Apps and services ▾Training ▾Resources ▾Free Account

Version

Search

▸ policy-and-compliance-audit

▾ policy-and-compliance-content-search

Commands

Get-ComplianceSearch

Get-ComplianceSearchAction

Get-ComplianceSecurityFilter

Get-MailboxSearch

Invoke-ComplianceSearchActionStep

New-ComplianceSearch

New-ComplianceSearchAction

New-ComplianceSecurityFilter

New-MailboxSearch

Remove-ComplianceSearch

Remove-ComplianceSearchAction

Remove-ComplianceSecurityFilter

Remove-MailboxSearch

Set-ComplianceSearch

Set-ComplianceSearchAction

Set-ComplianceSecurityFilter

Set-MailboxSearch

Start-ComplianceSearch

Start-MailboxSearch

Stop-ComplianceSearch

Stop-MailboxSearch

▸ policy-and-compliance-dlp

▸ policy-and-compliance-ediscovery

▸ policy-and-compliance-retention

▸ powershell-v3-module

▸ reporting

▸ role-based-access-control


▸ server-health-and-performance

set-ExoSecOpsOverrideRule

▸ sharing-and-collaboration

▸ unified-messaging

▸ users-and-groups

 Download PDF

⋮ / policy-and-compliance-content-search /⊕✎⋮

New-ComplianceSearchAction

Feedback

Reference

Module: ExchangePowerShell

Applies to: Exchange Server 2016, Exchange Server 2019, Security & Compliance

In this article

Syntax

Description

Examples

Parameters

This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings may be exclusive to one environment or the other.

Use the New-ComplianceSearchAction cmdlet to create actions for content searches in Exchange Server and in the Microsoft Purview compliance portal.

For information about the parameter sets in the Syntax section below, see [Exchange cmdlet syntax](#).

PowerShellCopy

```
New-ComplianceSearchAction
  [-SearchName] <String[]>
  [-Export]
  [-ActionName <String>]
  [-ArchiveFormat <ComplianceExportArchiveFormat>]
  [-Confirm]
  [-FileTypeExclusionsForUnindexedItems <String[]>]
  [-EnableDedupe <Boolean>]
  [-ExchangeArchiveFormat <ComplianceExportArchiveFormat>]
  [-Force]
  [-Format <ComplianceDataTransferFormat>]
  [-IncludeCredential]
  [-IncludeSharePointDocumentVersions <Boolean>]
  [-JobOptions <Int32>]
  [-NotifyEmail <String>]
  [-NotifyEmailCC <String>]
  [-ReferenceActionName <String>]
  [-Region <String>]
  [-Report]
  [-RetentionReport]
  [-RetryOnError]
  [-Scenario <ComplianceSearchActionScenario>]
  [-Scope <ComplianceExportScope>]
  [-SearchNames <String[]>]
  [-SharePointArchiveFormat <ComplianceExportArchiveFormat>]
  [-ShareRootPath <String>]
  [-Version <String>]
  [-WhatIf]
  [<CommonParameters>]
```

PowerShellCopy

Page 1 of 15

```
New-ComplianceSearchAction
[-SearchName] <String[]>
[-Preview]
[-ActionName <String>]
[-Confirm]
[-Force]
[-Format <ComplianceDataTransferFormat>]
[-IncludeCredential]
[-JobOptions <Int32>]
[-ReferenceActionName <String>]
[-Region <String>]
[-RetryOnError]
[-Scenario <ComplianceSearchActionScenario>]
[-SearchNames <String[]>]
[-Version <String>]
[-WhatIf]
[<CommonParameters>]
```

PowerShell

 Copy

```
New-ComplianceSearchAction
[-SearchName] <String[]>
[-Purge]
[-PurgeType <ComplianceDestroyType>]
[-ActionName <String>]
[-Confirm]
[-Force]
[-Format <ComplianceDataTransferFormat>]
[-IncludeCredential]
[-JobOptions <Int32>]
[-Region <String>]
[-ReferenceActionName <String>]
[-RetryOnError]
[-Scenario <ComplianceSearchActionScenario>]
[-SearchNames <String[]>]
[-Version <String>]
[-WhatIf]
[<CommonParameters>]
```

Description

After you create a content search using the New-ComplianceSearch cmdlet and run it using the Start-ComplianceSearch cmdlet, you assign a search action to the search using the New-ComplianceSearchAction cmdlet.

In on-premises Exchange, this cmdlet is available in the Mailbox Search role. By default, this role is assigned only to the Discovery Management role group.

You need to be assigned permissions before you can run this cmdlet. Although this topic lists all parameters for the cmdlet, you may not have access to some parameters if they're not included in the permissions assigned to you. To find the permissions required to run any cmdlet or parameter in your organization, see [Find the permissions required to run any Exchange cmdlet](#).

In Microsoft 365, the account that you use to run this cmdlet must have a valid Microsoft 365 license assigned.

To use this cmdlet in Security & Compliance PowerShell, you need to be assigned permissions. For more information, see [Permissions in the Microsoft Purview compliance portal](#).

Examples

Example 1

PowerShell

 Copy

```
New-ComplianceSearchAction -SearchName "Project X" -Preview
```

This example creates a preview search action for the content search named Project X.

Example 2

PowerShellCopy

```
New-ComplianceSearchAction -SearchName "Project X" -Export
```

This example creates an export search action for the content search named Project X.

Example 3

PowerShellCopy

```
New-ComplianceSearchAction -SearchName "Remove Phishing Message" -Purge -PurgeType
```

This example deletes the search results returned by a content search named Remove Phishing Message. Note that unindexed items aren't deleted when you use the Purge parameter.

Example 4

PowerShellCopy

```
New-ComplianceSearchAction -SearchName "Case 321 All Sites" -Export -SharePoint/
```

This example exports the results returned by the content search named "Case 321 All Sites". The search results are compressed and exported to a single ZIP file. If the search included any Exchange locations, the search results are exported as one PST file per mailbox.

Parameters

-ActionName

This parameter is available only in the cloud-based service.

The ActionName parameter specifies a name for the content search action. You use this parameter only when you specify multiple content searches in the SearchName parameter.

Expand table

Type:	String
Position:	Named
Default value:	None
Required:	False
Accept pipeline input:	False
Accept wildcard characters:	False
Applies to:	Security & Compliance

-ArchiveFormat

This parameter has been deprecated and is no longer used.

To specify the format for Exchange search results, use the ExchangeArchiveFormat parameter. To specify the format for SharePoint and OneDrive search results, use the SharePointArchiveFormat parameter.

[Expand table](#)

Type:	ComplianceExportArchiveFormat
Position:	Named
Default value:	None
Required:	False
Accept pipeline input:	False
Accept wildcard characters:	False
Applies to:	Exchange Server 2016, Exchange Server 2019, Security & Compliance

-Confirm

The Confirm switch specifies whether to show or hide the confirmation prompt. How this switch affects the cmdlet depends on if the cmdlet requires confirmation before proceeding.

- Destructive cmdlets (for example, Remove-* cmdlets) have a built-in pause that forces you to acknowledge the command before proceeding. For these cmdlets, you can skip the confirmation prompt by using this exact syntax: `-Confirm:$false`.
- Most other cmdlets (for example, New-* and Set-* cmdlets) don't have a built-in pause. For these cmdlets, specifying the Confirm switch without a value introduces a pause that forces you acknowledge the command before proceeding.

This cmdlet has a built-in pause, so use `-Confirm:$false` to skip the confirmation.

[Expand table](#)

Type:	SwitchParameter
Aliases:	cf
Position:	Named
Default value:	None
Required:	False
Accept pipeline input:	False
Accept wildcard characters:	False
Applies to:	Exchange Server 2016, Exchange Server 2019, Security & Compliance

-EnableDedupe

This parameter is reserved for internal Microsoft use.

[Expand table](#)

Type:	Boolean
Position:	Named
Default value:	None
Required:	False
Accept pipeline input:	False

Accept wildcard characters:	False
Applies to:	Security & Compliance

-ExchangeArchiveFormat

This parameter is functional only in the cloud-based service.

This parameter requires the Export role in Security & Compliance PowerShell. By default, this role is assigned only to the eDiscovery Manager role group.

The ExchangeArchiveFormat parameter specifies how to export Exchange search results. Valid values are:

- PerUserPst: One PST file for each mailbox.
- SinglePst: One PST file that contains all exported messages.
- SingleFolderPst: One PST file with a single root folder for the entire export.
- IndividualMessage: Export each message as an .msg message file. This is the default value.
- PerUserZip: One ZIP file for each mailbox. Each ZIP file contains the exported .msg message files from the mailbox.
- SingleZip: One ZIP file for all mailboxes. The ZIP file contains all exported .msg message files from all mailboxes. This output setting is available only in PowerShell.

To specify the format for SharePoint and OneDrive search results, use the SharePointArchiveFormat parameter.

 Expand table

Type:	ComplianceExportArchiveFormat
Position:	Named
Default value:	None
Required:	False
Accept pipeline input:	False
Accept wildcard characters:	False
Applies to:	Exchange Server 2016, Exchange Server 2019, Security & Compliance

-Export

This parameter is functional only in the cloud-based service.

This parameter requires the Export role in Security & Compliance PowerShell. By default, this role is assigned only to the eDiscovery Manager role group.

The Export switch specifies the action for the content search is to export the full set of results that match the search criteria. You don't need to specify a value with this switch.

To only return the information about each detected item in a report, use the Report switch.

 Expand table

Type:	SwitchParameter
Position:	Named
Default value:	None
Required:	False
Accept pipeline input:	False

Accept wildcard characters:	False
Applies to:	Exchange Server 2016, Exchange Server 2019, Security & Compliance

-FileTypeExclusionsForUnindexedItems

The FileTypeExclusionsForUnindexedItems specifies the file types to exclude because they can't be indexed. You can specify multiple values separated by commas.


 Expand table

Type:	String[]
Position:	Named
Default value:	None
Required:	False
Accept pipeline input:	False
Accept wildcard characters:	False
Applies to:	Exchange Server 2016, Exchange Server 2019, Security & Compliance

-Force

The Force switch hides warning or confirmation messages. You don't need to specify a value with this switch.

You can use this switch to run tasks programmatically where prompting for administrative input is inappropriate.

 Expand table

Type:	SwitchParameter
Position:	Named
Default value:	None
Required:	False
Accept pipeline input:	False
Accept wildcard characters:	False
Applies to:	Exchange Server 2016, Exchange Server 2019, Security & Compliance

-Format

In Security & Compliance PowerShell, this parameter requires the Export role. By default, this role is assigned only to the eDiscovery Manager role group.

The Format parameter specifies the format of the search results when you use the Export switch. Valid values are:

- FxStream: Export to PST files. This is the only option that's available when you export search results from the Microsoft Purview compliance portal.
- Mime: Export to .eml message files. This the default value when you use cmdlets to export the search results.
- Msg: Export to .msg message files.

 Expand table

Type:	ComplianceDataTransferFormat
-------	------------------------------

Position:	Named
Default value:	None
Required:	False
Accept pipeline input:	False
Accept wildcard characters:	False
Applies to:	Exchange Server 2016, Exchange Server 2019, Security & Compliance

-IncludeCredential

The IncludeCredential switch specifies whether to include the credential in the results. You don't need to specify a value with this switch.

[Expand table](#)

Type:	SwitchParameter
Position:	Named
Default value:	None
Required:	False
Accept pipeline input:	False
Accept wildcard characters:	False
Applies to:	Exchange Server 2016, Exchange Server 2019, Security & Compliance

-IncludeSharePointDocumentVersions

This parameter is available only in the cloud-based service.

The IncludeSharePointDocumentVersions parameter specifies whether to export previous versions of the document when you use the Export switch. Valid values are:

- \$true: Export all versions of the document.
- \$false: Export only the current published version of the topic. This is the default value.

[Expand table](#)

Type:	Boolean
Position:	Named
Default value:	None
Required:	False
Accept pipeline input:	False
Accept wildcard characters:	False
Applies to:	Security & Compliance

-JobOptions

This parameter is reserved for internal Microsoft use.

[Expand table](#)

Type:	Int32
Position:	Named

Default value:	None
Required:	False
Accept pipeline input:	False
Accept wildcard characters:	False
Applies to:	Exchange Server 2016, Exchange Server 2019, Security & Compliance

-NotifyEmail

In Security & Compliance PowerShell, this parameter requires the Export role. By default, this is assigned only to the eDiscovery Manager role group.

The NotifyEmail parameter specifies the email address target for the search results when you use the Export switch.

The recipient you specify is in the To: field of the message.

 Expand table

Type:	String
Position:	Named
Default value:	None
Required:	False
Accept pipeline input:	False
Accept wildcard characters:	False
Applies to:	Exchange Server 2016, Exchange Server 2019, Security & Compliance

-NotifyEmailCC

In Security & Compliance PowerShell, this parameter requires the Export role. By default, this role is assigned only to the eDiscovery Manager role group.

The NotifyEmailCC parameter specifies the email address target for the search results when you use the Export switch.

The recipient you specify is in the Cc: field of the message.

 Expand table

Type:	String
Position:	Named
Default value:	None
Required:	False
Accept pipeline input:	False
Accept wildcard characters:	False
Applies to:	Exchange Server 2016, Exchange Server 2019, Security & Compliance

-Preview

In Security & Compliance PowerShell, this parameter requires the Preview role. By default, this role is assigned only to the eDiscovery Manager role group.

The Preview switch specifies the action for the content search is to preview the results that match the search criteria. You don't need to specify a value with this switch.

 Expand table

Type:	SwitchParameter
Position:	Named
Default value:	None
Required:	False
Accept pipeline input:	False
Accept wildcard characters:	False
Applies to:	Exchange Server 2016, Exchange Server 2019, Security & Compliance

-Purge

Note: In Security & Compliance PowerShell, this switch is available only in the Search and Purge role. By default, this role is assigned only to the Organization Management and Data Investigator role groups.

The Purge switch specifies the action for the content search is to remove items that match the search criteria. You don't need to specify a value with this switch.

- A maximum of 10 items per mailbox can be removed at one time. Because the capability to search for and remove messages is intended to be an incident-response tool, this limit helps ensure that messages are quickly removed from mailboxes. This action isn't intended to clean up user mailboxes.
- You can remove items from a maximum of 50,000 mailboxes using a single content search. To remove items from more than 50,000 mailboxes, you'll have to create separate content searches. For more information, see [Search for and delete email messages in your Microsoft 365 organization](#).
- Unindexed items aren't removed from mailboxes when you use this switch.
- The value of the PurgeType parameter controls how the items are removed.

 Expand table

Type:	SwitchParameter
Position:	Named
Default value:	None
Required:	False
Accept pipeline input:	False
Accept wildcard characters:	False
Applies to:	Exchange Server 2016, Exchange Server 2019, Security & Compliance

-PurgeType

Note: In Security & Compliance PowerShell, this parameter is available only in the Search and Purge role. By default, this role is assigned only to the Organization Management and Data Investigator role groups.

The PurgeType parameter specifies how to remove items when the action is Purge. Valid values are:

- SoftDelete: Purged items are recoverable by users until the deleted item retention period expires.

- HardDelete (cloud only): Purged items are marked for permanent removal from the mailbox and will be permanently removed the next time the mailbox is processed by the Managed Folder Assistant. If single item recovery is enabled on the mailbox, purged items will be permanently removed after the deleted item retention period expires.

[Expand table](#)

Type:	ComplianceDestroyType
Position:	Named
Default value:	None
Required:	False
Accept pipeline input:	False
Accept wildcard characters:	False
Applies to:	Exchange Server 2016, Exchange Server 2019, Security & Compliance

-ReferenceActionName

This parameter is reserved for internal Microsoft use.

[Expand table](#)

Type:	String
Position:	Named
Default value:	None
Required:	False
Accept pipeline input:	False
Accept wildcard characters:	False
Applies to:	Exchange Server 2016, Exchange Server 2019, Security & Compliance

-Region

This parameter is reserved for internal Microsoft use.

[Expand table](#)

Type:	String
Position:	Named
Default value:	None
Required:	False
Accept pipeline input:	False
Accept wildcard characters:	False
Applies to:	Exchange Server 2016, Exchange Server 2019, Security & Compliance

-Report

This parameter is functional only in the cloud-based service.

The Report switch specifies the action for the content search is to export a report about the results (information about each item instead of the full set of results) that match the search

criteria. You don't need to specify a value with this switch.

[Expand table](#)

Type:	SwitchParameter
Position:	Named
Default value:	None
Required:	False
Accept pipeline input:	False
Accept wildcard characters:	False
Applies to:	Exchange Server 2016, Exchange Server 2019, Security & Compliance

-RetentionReport

The RetentionReport switch specifies the action for the content search is to export a retention report. You don't need to specify a value with this switch.

[Expand table](#)

Type:	SwitchParameter
Position:	Named
Default value:	None
Required:	False
Accept pipeline input:	False
Accept wildcard characters:	False
Applies to:	Exchange Server 2016, Exchange Server 2019, Security & Compliance

-RetryOnError

The RetryOnError switch specifies whether to retry the action on any items that failed without re-running the entire action all over again. You don't need to specify a value with this switch.

[Expand table](#)

Type:	SwitchParameter
Position:	Named
Default value:	None
Required:	False
Accept pipeline input:	False
Accept wildcard characters:	False
Applies to:	Exchange Server 2016, Exchange Server 2019, Security & Compliance

-Scenario

In Security & Compliance PowerShell, this parameter requires the Preview role. By default, this role is assigned only to the eDiscovery Manager role group.

The Scenario parameter specifies the scenario type when you use the Export switch. Valid values are:

- AnalyzeWithZoom: Prepare the search results for processing in Microsoft Purview eDiscovery Premium.
- General: Exports the search results to the local computer. Emails are exported to .pst files. SharePoint and OneDrive for Business documents are exported in their native Office formats.
- GenerateReportsOnly:
- Inventory:
- RetentionReports:
- TriagePreview:

 Expand table

Type:	ComplianceSearchActionScenario
Position:	Named
Default value:	None
Required:	False
Accept pipeline input:	False
Accept wildcard characters:	False
Applies to:	Exchange Server 2016, Exchange Server 2019, Security & Compliance

-Scope

The Scope parameter specifies the items to include when the action is Export. Valid values are:

- IndexedItemsOnly
- UnindexedItemsOnly
- BothIndexedAndUnindexedItems

 Expand table

Type:	ComplianceExportScope
Position:	Named
Default value:	None
Required:	False
Accept pipeline input:	False
Accept wildcard characters:	False
Applies to:	Exchange Server 2016, Exchange Server 2019, Security & Compliance

-SearchName

The SearchName parameter specifies the name of the existing content search to associate with the content search action. You can specify multiple content searches separated by commas.

You can find the content search by running the command Get-ComplianceSearch | Format-Table -Auto Name,Status.

 Expand table

Type:	String[]
Position:	1

Default value:	None
Required:	True
Accept pipeline input:	False
Accept wildcard characters:	False
Applies to:	Exchange Server 2016, Exchange Server 2019, Security & Compliance

-SearchNames

This parameter is available only in the cloud-based service.

The SearchNames parameter specifies the names of the existing content searches to associate with the content search action. You separate the content search names by commas.

You can find content search names by running the command `Get-ComplianceSearch | Format-Table -Auto Name,Status`.

 Expand table

Type:	String[]
Position:	Named
Default value:	None
Required:	False
Accept pipeline input:	False
Accept wildcard characters:	False
Applies to:	Security & Compliance

-SharePointArchiveFormat

This parameter is functional only in the cloud-based service.

This parameter requires the Export role. By default, this role is assigned only to the eDiscovery Manager role group.

The SharePointArchiveFormat parameter specifies how to export SharePoint and OneDrive search results. Valid values are:

- IndividualMessage: Export the files uncompressed. This is the default value.
- PerUserZip: One ZIP file for each user. Each ZIP file contains the exported files for the user.
- SingleZip: One ZIP file for all users. The ZIP file contains all exported files from all users. This output setting is available only in PowerShell.

To specify the format for Exchange search results, use the ExchangeArchiveFormat parameter.

 Expand table

Type:	ComplianceExportArchiveFormat
Position:	Named
Default value:	None
Required:	False
Accept pipeline input:	False

Accept wildcard characters:	False
Applies to:	Exchange Server 2016, Exchange Server 2019, Security & Compliance

-ShareRootPath

{{ Fill ShareRootPath Description }}

[Expand table](#)

Type:	String
Position:	Named
Default value:	None
Required:	False
Accept pipeline input:	False
Accept wildcard characters:	False
Applies to:	Exchange Server 2016, Exchange Server 2019

-Version

This parameter is reserved for internal Microsoft use.

[Expand table](#)

Type:	String
Position:	Named
Default value:	None
Required:	False
Accept pipeline input:	False
Accept wildcard characters:	False
Applies to:	Exchange Server 2016, Exchange Server 2019, Security & Compliance

-WhatIf

The WhatIf switch doesn't work in Security & Compliance PowerShell.

The WhatIf switch simulates the actions of the command. You can use this switch to view the changes that would occur without actually applying those changes. You don't need to specify a value with this switch.

[Expand table](#)

Type:	SwitchParameter
Aliases:	wi
Position:	Named
Default value:	None
Required:	False
Accept pipeline input:	False
Accept wildcard characters:	False
Applies to:	Exchange Server 2016, Exchange Server 2019, Security & Compliance

Feedback

Was this page helpful?

👍 Yes

👎 No

[Provide product feedback](#) ↗