

Exchange PowerShell

By chrisda

Archived: 2026-04-05 21:11:28 UTC

In this article

1. [active-directory](#)
2. [antispam-antimalware](#)
3. [client-access](#)
4. [client-access-servers](#)
5. [database-availability-groups](#)
6. [defender-for-office-365](#)
7. [devices](#)
8. [email-addresses-and-address-books](#)
9. [encryption-and-certificates](#)
10. [federation-and-hybrid](#)
11. [mail-flow](#)
12. [mailbox-databases-and-servers](#)
13. [mailboxes](#)
14. [move-and-migration](#)
15. [organization](#)
16. [policy-and-compliance](#)
17. [policy-and-compliance-audit](#)
18. [policy-and-compliance-content-search](#)
19. [policy-and-compliance-dlp](#)
20. [policy-and-compliance-ediscovery](#)
21. [policy-and-compliance-retention](#)
22. [powershell-v3-module](#)
23. [reporting](#)
24. [role-based-access-control](#)
25. [server-health-and-performance](#)
26. [sharing-and-collaboration](#)
27. [unified-messaging](#)
28. [users-and-groups](#)
29. [ExchangePowerShell](#)

Cmdlet	Description
Add-ADPermission	This cmdlet is available only in on-premises Exchange.

Cmdlet	Description
	<p>Use the Add-ADPermission cmdlet to add permissions to an Active Directory object.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Dump-ProvisioningCache</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Dump-ProvisioningCache cmdlet to return a list of the cached keys and values for the specified server and Windows PowerShell application.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-ADPermission</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Get-ADPermission cmdlet to get permissions on an Active Directory object.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-ADServerSettings</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Get-ADServerSettings cmdlet to view the Active Directory Domain Services (AD DS) environment settings in the current Exchange Management Shell session. The Get-ADServerSettings cmdlet replaces the AdminSessionADSettings session variable that was used in Exchange Server 2007.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-ADSite</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Get-ADSite cmdlet to display configuration information about one or more Active Directory sites.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
Get-DomainController	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Get-DomainController cmdlet to view a list of domain controllers that exist in your organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Get-OrganizationalUnit	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Get-OrganizationalUnit cmdlet to view a list of organizational units (OUs) that exist in your organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Get-Trust	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Get-Trust cmdlet to return external and forest trusts.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Get-UserPrincipalNamesSuffix	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Get-UserPrincipalNamesSuffix cmdlet to view the user principal name (UPN) suffixes in the Active Directory forest. The UPN suffixes are created in Active Directory Domains and Trusts.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Remove-ADPermission	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Remove-ADPermission cmdlet to remove permissions from an Active Directory object.</p>

Cmdlet	Description
	<p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Reset-ProvisioningCache</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>The Reset-ProvisioningCache cmdlet clears the Windows PowerShell provisioning cache of frequently used Active Directory objects. This cmdlet is only used for diagnostic purposes.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-ADServerSettings</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Set-ADServerSettings cmdlet to manage the Active Directory Domain Services (AD DS) environment in the current Exchange Management Shell session. The Set-ADServerSettings cmdlet replaces the AdminSessionADSettings session variable that was used in Exchange Server 2007.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-ADSite</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Set-ADSite cmdlet to configure the Exchange settings of Active Directory sites.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Cmdlet	Description
<p>Add-AttachmentFilterEntry</p>	<p>This cmdlet is available or effective only on Edge Transport servers in on-premises Exchange.</p> <p>Use the Add-AttachmentFilterEntry cmdlet to add an entry to the attachment filter list that's used by the Attachment Filtering agent on Edge Transport servers.</p>

Cmdlet	Description
	<p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Add-ContentFilterPhrase</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Add-ContentFilterPhrase cmdlet to define custom words for the Content Filter agent. A custom word is a word or phrase that the administrator sets for the Content Filter agent to evaluate the content of an message and apply appropriate filter processing.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Add-IPAllowListEntry</p>	<p>This cmdlet is available or effective only on Edge Transport servers in on-premises Exchange.</p> <p>Use the Add-IPAllowListEntry cmdlet to add IP Allow list entries to the IP Allow list that's used by the Connection Filtering agent on Edge Transport servers.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Add-IPAllowListProvider</p>	<p>This cmdlet is available or effective only on Edge Transport servers in on-premises Exchange.</p> <p>Use the Add-IPAllowListProvider cmdlet to create IP Allow list providers that are used by the Connection Filtering agent on Edge Transport servers.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Add-IPBlockListEntry</p>	<p>This cmdlet is available or effective only on Edge Transport servers in on-premises Exchange.</p> <p>Use the Add-IPBlockListEntry cmdlet to add IP Block list entries to the IP Block list that's used by the Connection Filtering agent on Edge Transport servers.</p>

Cmdlet	Description
	<p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Add-IPBlockListProvider</p>	<p>This cmdlet is available or effective only on Edge Transport servers in on-premises Exchange.</p> <p>Use the Add-IPBlockListProvider cmdlet to create IP Block list providers that are used by the Connection Filtering agent on Edge Transport servers.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Delete-QuarantineMessage</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Delete-QuarantineMessage cmdlet to delete quarantine messages from your cloud-based organization</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Disable-EOPProtectionPolicyRule</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Disable-EOPProtectionPolicyRule cmdlet to turn off the Standard preset security policy or the Strict preset security policy. If your organization has Defender for Office 365, you also need to use the Disable-ATPProtectionPolicyRule cmdlet to turn off the policy.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Disable-HostedContentFilterRule</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Disable-HostedContentFilterRule cmdlet to disable spam filter rules (content filter rules) in your cloud-based organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
Disable-HostedOutboundSpamFilterRule	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Disable-HostedOutboundSpamFilterRule cmdlet to disable outbound spam filter rules in your cloud-based organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Disable-MalwareFilterRule	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Disable-MalwareFilterRule cmdlet to disable malware filter rules in your organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Disable-ReportSubmissionRule	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Disable-ReportSubmissionRule cmdlet to disable the report submission rule in your cloud-based organization. The report submission rule identifies the reporting mailbox where user reported messages are delivered.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Enable-AntispamUpdates	<p>The Enable-AntispamUpdates cmdlet was deprecated in Microsoft Exchange Server 2010 Service Pack 1 and is no longer used.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Enable-EOPProtectionPolicyRule	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Enable-EOPProtectionPolicyRule cmdlet to turn on the Standard preset security policy or the Strict preset security policy.</p>

Cmdlet	Description
	<p>If your organization has Defender for Office 365, you also need to use the Enable-ATPProtectionPolicyRule cmdlet to turn on the policy.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Enable-HostedContentFilterRule</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Enable-HostedContentFilterRule cmdlet to enable spam filter rules (content filter rules) in your cloud-based organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Enable-HostedOutboundSpamFilterRule</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Enable-HostedOutboundSpamFilterRule cmdlet to enable outbound spam filter rules in your cloud-based organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Enable-MalwareFilterRule</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Enable-MalwareFilterRule cmdlet to enable malware filter rules in your organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Enable-ReportSubmissionRule</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Enable-ReportSubmissionRule cmdlet to enable the report submission rule in your cloud-based organization. The report submission rule identifies the reporting mailbox where user reported messages are delivered.</p>

Cmdlet	Description
	<p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Export-QuarantineMessage</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Export-QuarantineMessage cmdlet to export quarantined messages and files from your cloud-based organization. Messages are exported to .eml message files so you can open them in Outlook.</p> <p>For files that were quarantined by Safe Attachments for SharePoint, OneDrive, and Microsoft Teams, the files are exported in Base64 format.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-AgentLog</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Get-AgentLog cmdlet to parse log files that you specify as parameters and collect raw statistics from the filtering that anti-spam agents apply during a time period that you specify.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-AggregateZapReport</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Get-AggregateZapReport cmdlet to view aggregate information about zero-hour auto purge (ZAP) activity. By default, the cmdlet shows the last three days of activity, but you can specify up to ten days.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-ArcConfig</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Get-ArcConfig cmdlet to view the list of trusted Authenticated Received Chain (ARC) sealers that are configured</p>

Cmdlet	Description
	<p>in the cloud-based organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-AttachmentFilterEntry</p>	<p>This cmdlet is available or effective only on Edge Transport servers in on-premises Exchange.</p> <p>Use the Get-AttachmentFilterEntry cmdlet to view the list of attachment filter entries that are used by the Attachment Filtering agent on Edge Transport servers.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-AttachmentFilterListConfig</p>	<p>This cmdlet is available or effective only on Edge Transport servers in on-premises Exchange.</p> <p>Use the Get-AttachmentFilterListConfig cmdlet to view the configuration of the Attachment Filtering agent on Edge Transport servers.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-BlockedConnector</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Get-BlockedConnector cmdlet to view inbound connectors that have been detected as potentially compromised. Blocked connectors are prevented from sending email.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-BlockedSenderAddress</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Get-BlockedSenderAddress cmdlet to view users in your Microsoft 365 organization that are affected by the protection system. These users sent multiple messages that were classified as spam, so they're blocked from sending messages.</p>

Cmdlet	Description
	<p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-ConfigAnalyzerPolicyRecommendation</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Get-ConfigAnalyzerPolicyRecommendation cmdlet to compare the settings in your existing security policies to the settings that are used in the Standard or Strict preset security policies. Settings that are below the recommend value are returned in the results.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-ContentFilterConfig</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Get-ContentFilterConfig cmdlet to view the content filter configuration for the computer on which the cmdlet is run.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-ContentFilterPhrase</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Get-ContentFilterPhrase cmdlet to view one or all custom words that the Content Filter agent processes.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-DetailZapReport</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Get-DetailZapReport cmdlet to view details about zero-hour auto purge (ZAP) activity. By default, the cmdlet shows the last three days of activity, but you can specify up to ten days.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
Get-DkimSigningConfig	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Get-DkimSigningConfig cmdlet to view the DomainKeys Identified Mail (DKIM) signing policy settings for domains in a cloud-based organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Get-EOPProtectionPolicyRule	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Get-EOPProtectionPolicyRule cmdlet to view rules for the built-in security features for all cloud mailboxes in preset security policies. The rules specify recipient conditions and exceptions for the protection, and also allow you to turn on and turn off the associated preset security policies.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Get-ExoPhishSimOverrideRule	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Get-ExoPhishSimOverrideRule cmdlet to view non-Microsoft phishing simulation override rules that bypass filtering. For more information, see Configure the advanced delivery policy for non-Microsoft phishing simulations and email delivery to SecOps mailboxes.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
Get-ExoSecOpsOverrideRule	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Get-ExoSecOpsOverrideRule cmdlet to view SecOps mailbox override rules that bypass filtering. For more information, see Configure the advanced delivery policy for non-Microsoft phishing simulations and email delivery to SecOps mailboxes.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Get-HostedConnectionFilterPolicy	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Get-HostedConnectionFilterPolicy cmdlet to view the settings of connection filter policies in your cloud-based organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Get-HostedContentFilterPolicy	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Get-HostedContentFilterPolicy cmdlet to view the settings of spam filter policies (content filter policies) in your cloud-based organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Get-HostedContentFilterRule	<p>This cmdlet is functional only in the cloud-based service.</p> <p>Use the Get-HostedContentFilterRule cmdlet to view spam filter rules (content filter rules) in your cloud-based organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Get-HostedOutboundSpamFilterPolicy	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Get-HostedOutboundSpamFilterPolicy cmdlet to view outbound spam filter policies in your cloud-based organization.</p>

Cmdlet	Description
	<p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-HostedOutboundSpamFilterRule</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Get-HostedOutboundSpamFilterRule cmdlet to view outbound spam filter rules in your cloud-based organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-IPAllowListConfig</p>	<p>This cmdlet is available or effective only on Edge Transport servers in on-premises Exchange.</p> <p>Use the Get-IPAllowListConfig cmdlet to view the configuration information for the IP Allow list that's used by the Connection Filtering agent on Edge Transport servers.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-IPAllowListEntry</p>	<p>This cmdlet is available or effective only on Edge Transport servers in on-premises Exchange.</p> <p>Use the Get-IPAllowListEntry cmdlet to view the IP address entries in the IP Allow list that's used by the Connection Filtering agent on Edge Transport servers.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
<p>Get-IPAllowListProvider</p>	<p>This cmdlet is available or effective only on Edge Transport servers in on-premises Exchange.</p> <p>Use the Get-IPAllowListProvider cmdlet to view IP Allow list providers that are used by the Connection Filtering agent on Edge Transport servers.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-IPAllowListProvidersConfig</p>	<p>This cmdlet is available or effective only on Edge Transport servers in on-premises Exchange.</p> <p>Use the Get-IPAllowListProvidersConfig cmdlet to view the settings that affect all IP Allow list providers that are configured on an Edge Transport server.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-IPBlockListConfig</p>	<p>This cmdlet is available or effective only on Edge Transport servers in on-premises Exchange.</p> <p>Use the Get-IPBlockListConfig cmdlet to view the IP Block list configuration information that's used by the Connection Filtering agent on Edge Transport servers.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-IPBlockListEntry</p>	<p>This cmdlet is available or effective only on Edge Transport servers in on-premises Exchange.</p> <p>Use the Get-IPBlockListEntry cmdlet to view the IP Block list entries that are used by the Connection Filtering agent on Edge Transport servers.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
<p>Get-IPBlockListProvider</p>	<p>This cmdlet is available or effective only on Edge Transport servers in on-premises Exchange.</p> <p>Use the Get-IPBlockListProvider cmdlet to view IP Block list providers that are used by the Connection Filtering agent on Edge Transport servers.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-IPBlockListProvidersConfig</p>	<p>This cmdlet is available or effective only on Edge Transport servers in on-premises Exchange.</p> <p>Use the Get-IPBlockListProvidersConfig cmdlet to view the settings that affect all IP Block list providers that are configured on an Edge Transport server.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-MailboxJunkEmailConfiguration</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Get-MailboxJunkEmailConfiguration cmdlet to view the junk email settings on mailboxes.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-MalwareFilteringServer</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Get-MalwareFilteringServer cmdlet to view the Malware agent settings in the Transport service on a Mailbox server.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
<p>Get-MalwareFilterPolicy</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Get-MalwareFilterPolicy cmdlet to view the malware filter policies in your organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-MalwareFilterRule</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Enable-MalwareFilterRule cmdlet to view malware filter rules in your organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-PhishSimOverridePolicy</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Get-PhishSimOverridePolicy cmdlet to view non-Microsoft phishing simulation override policies that bypass filtering. For more information, see Configure the advanced delivery policy for non-Microsoft phishing simulations and email delivery to SecOps mailboxes.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
Get-QuarantineMessage	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Get-QuarantineMessage cmdlet to view quarantined messages and files in your cloud-based organization. Files are quarantined by Safe Attachments for SharePoint, OneDrive, and Microsoft Teams.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Get-QuarantineMessageHeader	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Get-QuarantineMessageHeader cmdlet to view the message header of a quarantined message. The command fails if the specified message is not in quarantine.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Get-QuarantinePolicy	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Get-QuarantinePolicy cmdlet to view quarantine policies in your cloud-based organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Get-RecipientFilterConfig	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Get-RecipientFilterConfig cmdlet to view the recipient filter configuration information for the Exchange server.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Get-ReportSubmissionPolicy	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Get-ReportSubmissionPolicy cmdlet to view the report submission policy in your cloud-based organization. The report</p>

Cmdlet	Description
	<p>submission policy controls most of the user reported message settings in the organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-ReportSubmissionRule</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Get-ReportSubmissionRule cmdlet to view the report submission rule in your cloud-based organization. The report submission rule identifies the reporting mailbox where user reported messages are delivered.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-SecOpsOverridePolicy</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Get-SecOpsOverridePolicy cmdlet to view SecOps mailbox override policies that bypass filtering. For more information, see Configure the advanced delivery policy for non-Microsoft phishing simulations and email delivery to SecOps mailboxes.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-SenderFilterConfig</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Get-SenderFilterConfig cmdlet to view the Sender Filter configuration information for the Exchange server.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-SenderIdConfig</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Get-SenderIdConfig cmdlet to view the Sender ID configuration information for the Exchange server.</p>

Cmdlet	Description
	<p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-SenderReputationConfig</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Get-SenderReputationConfig cmdlet to view the configuration information for sender reputation on the computer on which the command is run.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-TeamsProtectionPolicy</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Get-TeamsProtectionPolicy cmdlet to view Microsoft Teams protection policies.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-TeamsProtectionPolicyRule</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Get-TeamsProtectionPolicyRule cmdlet to view Microsoft Teams protection policy rules.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-TenantAllowBlockListItems</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Get-TenantAllowBlockListItems cmdlet to view entries in the Tenant Allow/Block List in the Microsoft Defender portal.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-TenantAllowBlockListSpoofItems</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Get-TenantAllowBlockListSpoofItems cmdlet to view spoofed sender entries in the Tenant Allow/Block List.</p>

Cmdlet	Description
	<p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-DkimSigningConfig</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the New-DkimSigningConfig cmdlet to create the DomainKeys Identified Mail (DKIM) signing policy settings for domains in a cloud-based organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-EOPProtectionPolicyRule</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the New-EOPProtectionPolicyRule cmdlet to create rules for the built-in security features for all cloud mailboxes in preset security policies. The rules specify recipient conditions and exceptions for the protection, and also allow you to turn on and turn off the associated preset security policies.</p> <p>Note: Unless you manually removed a rule using the Remove-EOPProtectionPolicyRule cmdlet, we don't recommend using this cmdlet to create rules. To create the rule, you need to specify the existing individual security policies that are associated with the preset security policy. We never recommend creating these required individual security policies manually. Turning on the preset security policy for the first time in the Microsoft Defender portal automatically creates the required individual security policies, but also creates the associated rules using this cmdlet. So, if the rules already exist, you don't need to use this cmdlet to create them.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-ExoPhishSimOverrideRule</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the New-ExoPhishSimOverrideRule cmdlet to create non-Microsoft phishing simulation override rules that bypass filtering. For more information, see Configure the advanced delivery policy.</p>

Cmdlet	Description
	<p>for non-Microsoft phishing simulations and email delivery to SecOps mailboxes.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-ExoSecOpsOverrideRule</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the New-ExoSecOpsOverrideRule cmdlet to create SecOps mailbox override rules that bypass filtering. For more information, see Configure the advanced delivery policy for non-Microsoft phishing simulations and email delivery to SecOps mailboxes.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-HostedContentFilterPolicy</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the New-HostedContentFilterPolicy cmdlet to create spam filter policies (content filter policies) in your cloud-based organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-HostedContentFilterRule</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the New-HostedContentFilterRule cmdlet to create spam filter rules (content filter rules) in your cloud-based organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-HostedOutboundSpamFilterPolicy</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the New-HostedOutboundSpamFilterPolicy cmdlet to create outbound spam filter policies in your cloud-based organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
New-HostedOutboundSpamFilterRule	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the New-HostedOutboundSpamFilterRule cmdlet to create outbound spam filter rules in your cloud-based organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
New-MalwareFilterPolicy	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the New-MalwareFilterPolicy cmdlet to create malware filter policies in your organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
New-MalwareFilterRule	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the New-MalwareFilterRule cmdlet to create malware filter rules in your organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
New-PhishSimOverridePolicy	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the New-PhishSimOverridePolicy cmdlet to create non-Microsoft phishing simulation override policies that bypass filtering. For more information, see Configure the advanced delivery policy for non-Microsoft phishing simulations and email delivery to SecOps mailboxes.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
<p>New-QuarantinePermissions</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Note: Instead of using this cmdlet to set quarantine policy permissions, we recommend using the <code>EndUserQuarantinePermissionsValue</code> parameter on the <code>New-QuarantinePolicy</code> and <code>Set-QuarantinePolicy</code> cmdlets.</p> <p>Use the <code>New-QuarantinePermissions</code> cmdlet to create a variable that contains a quarantine permissions object to use with the <code>EndUserQuarantinePermission</code> parameter on the <code>New-QuarantinePolicy</code> or <code>Set-QuarantinePolicy</code> cmdlets in the same PowerShell session.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-QuarantinePolicy</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the <code>New-QuarantinePolicy</code> cmdlet to create quarantine policies in your cloud-based organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-ReportSubmissionPolicy</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the <code>New-ReportSubmissionPolicy</code> cmdlet to create the report submission policy in your cloud-based organization. The report submission policy controls most of the user reported message settings in the organization.</p> <p>Note: If the policy already exists (the <code>Get-ReportSubmissionPolicy</code> cmdlet returns output), you can't use this cmdlet. To delete the existing policy and start over with the default settings, use the <code>Remove-ReportSubmissionPolicy</code> cmdlet first.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
New-ReportSubmissionRule	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the New-ReportSubmissionRule cmdlet to create the report submission rule in your cloud-based organization. The report submission rule identifies the reporting mailbox where user reported messages are delivered.</p> <p>Note: If the rule already exists (the Get-ReportSubmissionRule cmdlet returns output), you can't use this cmdlet. To delete the existing rule and start over, use the Remove-ReportSubmissionRule cmdlet first.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
New-SecOpsOverridePolicy	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the New-SecOpsOverridePolicy cmdlet to create SecOps mailbox override policies that bypass filtering. For more information, see Configure the advanced delivery policy for non-Microsoft phishing simulations and email delivery to SecOps mailboxes.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
New-TeamsProtectionPolicy	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the New-TeamsProtectionPolicy cmdlet to create Microsoft Teams protection policies.</p> <p>Note: If the policy already exists (the Get-TeamsProtectionPolicy cmdlet returns output), you can't use this cmdlet.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
New-TeamsProtectionPolicyRule	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the New-TeamsProtectionPolicyRule cmdlet to create Microsoft Teams protection policy rules.</p>

Cmdlet	Description
	<p>Note: If the rule already exists (the Get-TeamsProtectionPolicyRule cmdlet returns output), you can't use this cmdlet.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-TenantAllowBlockListItems</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the New-TenantAllowBlockListItems cmdlet to add entries to the Tenant Allow/Block List in the Microsoft Defender portal.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-TenantAllowBlockListSpoofItems</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the New-TenantAllowBlockListSpoofItems cmdlet to create spoofed sender entries in the Tenant Allow/Block List.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Preview-QuarantineMessage</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Preview-QuarantineMessage cmdlet to preview the contents of quarantined messages in your cloud-based organization. This cmdlet doesn't work on files that were quarantined by Safe Attachments for SharePoint, OneDrive, and Microsoft Teams.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Release-QuarantineMessage</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Release-QuarantineMessage cmdlet to release messages from quarantine in your cloud-based organization. You can release messages to all original recipients, or to specific recipients.</p>

Cmdlet	Description
	<p>For files that were quarantined by Safe Attachments for SharePoint, OneDrive, and Microsoft Teams, you can unblock the files in the respective team sites and document libraries by using the Release-QuarantineMessage cmdlet so users can access, share, and download the files.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-AttachmentFilterEntry</p>	<p>This cmdlet is available or effective only on Edge Transport servers in on-premises Exchange.</p> <p>Use the Remove-AttachmentFilterEntry cmdlet to remove an entry from the attachment filter list that's used by the Attachment Filtering agent on Edge Transport servers.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-BlockedConnector</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Remove-BlockedConnector cmdlet to unblock inbound connectors that have been detected as potentially compromised. Blocked connectors are prevented from sending email.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-BlockedSenderAddress</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Remove-BlockedSenderAddress cmdlet to unblock users in your Microsoft 365 organization that were affected by the protection system. These users sent multiple messages that were classified as spam, so they were blocked from sending messages.</p> <p>Note: There's a limit to the number of times you can unblock a Microsoft 365 account. If you exceed the unblock limit for a user, you get an error, and you need to contact Microsoft Support to unblock the user.</p>

Cmdlet	Description
	<p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-ContentFilterPhrase</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Remove-ContentFilterPhrase cmdlet to remove one or all custom words that the Content Filter agent processes.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-DkimSigningConfig</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Remove-DkimSigningConfig cmdlet to remove the DomainKeys Identified Mail (DKIM) signing policy settings for domains in a cloud-based organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-EOPProtectionPolicyRule</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Remove-EOPProtectionPolicyRule cmdlet to remove rules for the built-in security features for all cloud mailboxes in preset security policies. The rules specify recipient conditions and exceptions for the protection, and also allow you to turn on and turn off the associated preset security policies.</p> <p>Note: Use this cmdlet to remove a rule only if you plan to immediately recreate the rule using the New-EOPProtectionPolicyRule cmdlet. The affected preset security policy can't function without a corresponding rule.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-ExoPhishSimOverrideRule</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Remove-ExoPhishSimOverrideRule cmdlet to remove non-Microsoft phishing simulation override rules that bypass</p>

Cmdlet	Description
	<p>filtering. For more information, see Configure the advanced delivery policy for non-Microsoft phishing simulations and email delivery to SecOps mailboxes.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-ExoSecOpsOverrideRule</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Remove-ExoSecOpsOverrideRule cmdlet to remove SecOps mailbox override rules that bypass filtering. For more information, see Configure the advanced delivery policy for non-Microsoft phishing simulations and email delivery to SecOps mailboxes.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-HostedContentFilterPolicy</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Remove-HostedContentFilterPolicy cmdlet to remove spam filter policies (content filter policies) from your cloud-based organization.</p> <p>When a policy is removed and there are rules associated with it, the rules are not removed when the policy is removed. This is by design. If you want to remove the associated rules, you need to do this separately via the Remove-HostedContentFilterRule cmdlet.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-HostedContentFilterRule</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Remove-HostedContentFilterRule cmdlet to remove spam filter rules (content filter rules) in your cloud-based organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
<p>Remove-HostedOutboundSpamFilterPolicy</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Remove-HostedOutboundSpamFilterPolicy cmdlet to remove outbound spam filter policies from your cloud-based organization.</p> <p>When a policy is removed and there are rules associated with it, the rules are not removed when the policy is removed. This is by design. If you want to remove the associated rules, you need to do this separately via the Remove-HostedOutboundSpamFilterRule cmdlet.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-HostedOutboundSpamFilterRule</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Remove-HostedOutboundSpamFilterRule cmdlet to remove outbound spam filter rules in your cloud-based organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-IPAllowListEntry</p>	<p>This cmdlet is available or effective only on Edge Transport servers in on-premises Exchange.</p> <p>Use the Remove-IPAllowListEntry cmdlet to remove IP address entries from the IP Allow list that's used by the Connection Filtering agent on Edge Transport servers.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-IPAllowListProvider</p>	<p>This cmdlet is available or effective only on Edge Transport servers in on-premises Exchange.</p> <p>Use the Remove-IPAllowListProvider cmdlet to remove IP Allow list providers that are used by the Connection Filtering agent on Edge Transport servers.</p>

Cmdlet	Description
	<p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-IPBlockListEntry</p>	<p>This cmdlet is available or effective only on Edge Transport servers in on-premises Exchange.</p> <p>Use the Remove-IPBlockListEntry cmdlet to remove IP block list entries that are used by the Connection Filtering agent on Edge Transport servers.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-IPBlockListProvider</p>	<p>This cmdlet is available or effective only on Edge Transport servers in on-premises Exchange.</p> <p>Use the Remove-IPBlockListProvider cmdlet to remove IP Block list providers that are used by the Connection Filtering agent on Edge Transport server.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-MalwareFilterPolicy</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Remove-MalwareFilterPolicy cmdlet to remove malware filter policies from your organization.</p> <p>When a policy is removed and there are rules associated with it, the rules are not removed when the policy is removed. This is by design. If you want to remove the associated rules, you need to do this separately via the Remove-MalwareFilterRule cmdlet.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-MalwareFilterRule</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be</p>

Cmdlet	Description
	<p>exclusive to one environment or the other.</p> <p>Use the Remove-MalwareFilterRule cmdlet to remove malware filter rules from your organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-PhishSimOverridePolicy</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Remove-PhishSimOverridePolicy cmdlet to remove non-Microsoft phishing simulation override policies that bypass filtering. For more information, see Configure the advanced delivery policy for non-Microsoft phishing simulations and email delivery to SecOps mailboxes.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-QuarantinePolicy</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Remove-QuarantinePolicy cmdlet to remove quarantine policies from your cloud-based organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-ReportSubmissionPolicy</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Remove-ReportSubmissionPolicy cmdlet to remove the report submission policy from your cloud-based organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-ReportSubmissionRule</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Remove-ReportSubmissionRule cmdlet to remove the report submission rule from your cloud-based organization. The report submission rule identifies the reporting mailbox where user reported messages are delivered.</p>

Cmdlet	Description
	<p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-SecOpsOverridePolicy</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Remove-SecOpsOverridePolicy cmdlet to remove SecOps mailbox override policies that bypass filtering. For more information, see Configure the advanced delivery policy for non-Microsoft phishing simulations and email delivery to SecOps mailboxes.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-TenantAllowBlockListItems</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Remove-TenantAllowBlockListItems cmdlet to remove entries from the Tenant Allow/Block List in the Microsoft Defender portal.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-TenantAllowBlockListSpoofItems</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Remove-TenantAllowBlockListSpoofItems cmdlet to remove spoofed sender entries from the Tenant Allow/Block List.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
Rotate-DkimSigningConfig	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Rotate-DkimSigningConfig cmdlet to rotate the public and private DomainKeys Identified Mail (DKIM) signing policy keys for domains in a cloud-based organization. This cmdlet creates new DKIM keys and uses the alternate DKIM selector.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Set-ArcConfig	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Set-ArcConfig cmdlet to modify the list of trusted Authenticated Received Chain (ARC) sealers that are configured in the cloud-based organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Set-AttachmentFilterListConfig	<p>This cmdlet is available or effective only on Edge Transport servers in on-premises Exchange.</p> <p>Use the Set-AttachmentFilterListConfig cmdlet to modify the configuration of the Attachment Filtering agent on Edge Transport servers.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Set-ContentFilterConfig	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Set-ContentFilterConfig cmdlet to modify the content filter configuration on a Mailbox server or an Edge Transport server.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Set-DkimSigningConfig	<p>This cmdlet is available only in the cloud-based service.</p>

Cmdlet	Description
	<p>Use the Set-DkimSigningConfig cmdlet to modify the DomainKeys Identified Mail (DKIM) signing policy settings for domains in a cloud-based organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-EOPProtectionPolicyRule</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Set-EOPProtectionPolicyRule cmdlet to modify rules associated with the built-in security features for all cloud mailboxes in preset security policies.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-ExoPhishSimOverrideRule</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Set-ExoPhishSimOverrideRule cmdlet to modify non-Microsoft phishing simulation override rules that bypass filtering. For more information, see Configure the advanced delivery policy for non-Microsoft phishing simulations and email delivery to SecOps mailboxes.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-ExoSecOpsOverrideRule</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Set-ExoSecOpsOverrideRule cmdlet to modify SecOps mailbox override rules that bypass filtering. For more information, see Configure the advanced delivery policy for non-Microsoft phishing simulations and email delivery to SecOps mailboxes.</p> <p>Tip: This cmdlet doesn't modify email addresses in the SecOps override rule. To modify the email addresses in the SecOps override rule, use the Set-SecOpsOverridePolicy cmdlet.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
Set-HostedConnectionFilterPolicy	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Set-HostedConnectionFilterPolicy cmdlet to modify the settings of connection filter policies in your cloud-based organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Set-HostedContentFilterPolicy	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Set-HostedContentFilterPolicy cmdlet to modify spam filter policies (content filter policies) in your cloud-based organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Set-HostedContentFilterRule	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Set-HostedContentFilterRule cmdlet to modify spam filter rules (content filter rules) in your cloud-based organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Set-HostedOutboundSpamFilterPolicy	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Set-HostedOutboundSpamFilterPolicy cmdlet to modify outbound spam filter policies in your cloud-based organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Set-HostedOutboundSpamFilterRule	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Set-HostedOutboundSpamFilterRule cmdlet to modify the settings of outbound spam filter rules in your cloud-based organization.</p>

Cmdlet	Description
	<p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-IPAllowListConfig</p>	<p>This cmdlet is available or effective only on Edge Transport servers in on-premises Exchange.</p> <p>Use the Set-IPAllowListConfig cmdlet to modify the IP Allow list configuration that's used by the Connection Filtering agent on Edge Transport servers.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-IPAllowListProvider</p>	<p>This cmdlet is available or effective only on Edge Transport servers in on-premises Exchange.</p> <p>Use the Set-IPAllowListProvider cmdlet to modify IP Allow list providers that are used by the Connection Filtering agent on Edge Transport servers.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-IPAllowListProvidersConfig</p>	<p>This cmdlet is available or effective only on Edge Transport servers in on-premises Exchange.</p> <p>Use the Set-IPAllowListProvidersConfig cmdlet to modify the settings that affect all IP Allow list providers that are configured on an Edge Transport server.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-IPBlockListConfig</p>	<p>This cmdlet is available or effective only on Edge Transport servers in on-premises Exchange.</p> <p>Use the Set-IPBlockListConfig cmdlet to modify the IP Block list configuration that's used by the Connection Filtering agent on Edge Transport servers.</p>

Cmdlet	Description
	<p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-IPBlockListProvider</p>	<p>This cmdlet is available or effective only on Edge Transport servers in on-premises Exchange.</p> <p>Use the Set-IPBlockListProvider cmdlet to modify IP Block list providers that are used by the Connection Filtering agent on Edge Transport servers.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-IPBlockListProvidersConfig</p>	<p>This cmdlet is available or effective only on Edge Transport servers in on-premises Exchange.</p> <p>Use the Set-IPBlockListProvidersConfig cmdlet to modify the settings that affect all IP Block list providers that are configured on an Edge Transport server.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-MailboxJunkEmailConfiguration</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Set-MailboxJunkEmailConfiguration cmdlet to configure the junk email settings on mailboxes.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-MalwareFilteringServer</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Set-MalwareFilteringServer cmdlet to configure the Malware agent settings in the Transport service on a Mailbox server.</p>

Cmdlet	Description
	<p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-MalwareFilterPolicy</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Set-MalwareFilterPolicy cmdlet to modify malware filter policies in your organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-MalwareFilterRule</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Set-MalwareFilterRule cmdlet to modify malware filter rules in your organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-PhishSimOverridePolicy</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Set-PhishSimOverridePolicy cmdlet to modify non-Microsoft phishing simulation override policies that bypass filtering. For more information, see Configure the advanced delivery policy for non-Microsoft phishing simulations and email delivery to SecOps mailboxes.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-QuarantinePermissions</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Note: Instead of using this cmdlet to set quarantine policy permissions, we recommend using the EndUserQuarantinePermissionsValue parameter on the New-QuarantinePolicy and Set-QuarantinePolicy cmdlets.</p>

Cmdlet	Description
	<p>Use the Set-QuarantinePermissions cmdlet to modify quarantine permissions objects that were created by the New-QuarantinePermissions and stored as a variable in the current PowerShell session. You use the variable as a value for the EndUserQuarantinePermission parameter on the New-QuarantinePolicy or Set-QuarantinePolicy cmdlets in the same PowerShell session.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-QuarantinePolicy</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Set-QuarantinePolicy cmdlet to modify quarantine policies in your cloud-based organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-RecipientFilterConfig</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Set-RecipientFilterConfig cmdlet to enable and configure the Recipient Filter agent.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-ReportSubmissionPolicy</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Set-ReportSubmissionPolicy cmdlet to modify the report submission policy in your cloud-based organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-ReportSubmissionRule</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Set-ReportSubmissionRule cmdlet to modify the report submission rule in your cloud-based organization. The report</p>

Cmdlet	Description
	<p>submission rule identifies the reporting mailbox where user reported messages are delivered.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-SecOpsOverridePolicy</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Set-SecOpsOverridePolicy cmdlet to modify SecOps mailbox override policies that bypass filtering. For more information, see Configure the advanced delivery policy for non-Microsoft phishing simulations and email delivery to SecOps mailboxes.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-SenderFilterConfig</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Set-SenderFilterConfig cmdlet to modify the Sender Filter agent configuration.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-SenderIdConfig</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Set-SenderIdConfig cmdlet to modify the configuration of the Sender ID agent.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
Set-SenderReputationConfig	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Set-SenderReputationConfig cmdlet to modify the sender reputation configuration on Mailbox servers or Edge Transport servers.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Set-TeamsProtectionPolicy	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Set-TeamsProtectionPolicy cmdlet to modify Microsoft Teams protection policies.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Set-TeamsProtectionPolicyRule	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Set-TeamsProtectionPolicyRule cmdlet to modify Microsoft Teams protection policy rules.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Set-TenantAllowBlockListItems	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Set-TenantAllowBlockListItems cmdlet to modify entries in the Tenant Allow/Block List in the Microsoft Defender portal.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
Set-TenantAllowBlockListSpoofItems	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Set-TenantAllowBlockListSpoofItems cmdlet to modify spoofed sender entries in the Tenant Allow/Block List.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Test-IPAllowListProvider	<p>This cmdlet is available or effective only on Edge Transport servers in on-premises Exchange.</p> <p>Use the Test-IPAllowListProvider cmdlet to test IP Allow list providers on Edge Transport servers.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Test-IPBlockListProvider	<p>This cmdlet is available or effective only on Edge Transport servers in on-premises Exchange.</p> <p>Use the Test-IPBlockListProvider cmdlet to test IP Block list providers on Edge Transport servers.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Test-SenderId	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Test-SenderId cmdlet to test whether a specified IP address is the legitimate sending address for a specified SMTP address.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Update-SafeList	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Update-SafeList cmdlet to update the safelist aggregation data in Active Directory. Safelist aggregation data is used in the built-in anti-spam filtering in Microsoft Exchange. EdgeSync</p>

Cmdlet	Description
	<p>replicates safelist aggregation data to Edge Transport servers in the perimeter network.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Cmdlet	Description
<p>Clear-TextMessagingAccount</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>The Clear-TextMessagingAccount cmdlet allows a user to remove the text messaging settings from their own mailbox. An administrator can't use this cmdlet to remove the text messaging settings from another user's mailbox.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Compare-TextMessagingVerificationCode</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Compare-TextMessagingVerificationCode cmdlet to verify the text messaging verification code that the user specified as part of configuring text message notifications on the mailbox.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Disable-PushNotificationProxy</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Disable-PushNotificationProxy cmdlet to disable the push notification proxy that's configured between an on-premises Microsoft Exchange organization and a Microsoft 365 organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
Enable-PushNotificationProxy	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Enable-PushNotificationProxy cmdlet to enable a push notification proxy between an on-premises Microsoft Exchange organization and a Microsoft 365 organization.</p> <p>In order for event notifications to be successfully delivered, you also need to configure OAuth authentication between your on-premises Exchange organization and your Microsoft 365 organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Export-AutoDiscoverConfig	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Export-AutoDiscoverConfig cmdlet to create or update a service connection point for an Autodiscover service pointer in a target Exchange forest.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Get-CASMailbox	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Get-CASMailbox cmdlet to view the Client Access settings that are configured on mailboxes.</p> <p>Note: In Exchange Online PowerShell, we recommend that you use the Get-EXOCASMailbox cmdlet instead of this cmdlet. For more information, see Connect to Exchange Online PowerShell.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Get-CASMailboxPlan	<p>This cmdlet is functional only in the cloud-based service.</p> <p>Use the Get-CASMailboxPlan cmdlet to view Client Access services (CAS) mailbox plans in cloud-based organizations.</p>

Cmdlet	Description
	<p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-ClientAccessRule</p>	<p>Note</p> <p>Client access rules were deprecated for all Exchange Online organizations in September 2025. For more information, see Update on Client Access Rules Deprecation in Exchange Online.</p> <p>This cmdlet is functional only in Exchange Server 2019 or later.</p> <p>Use the Get-ClientAccessRule cmdlet to view client access rules. Client access rules help you control access to your organization based on the properties of the connection.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-ImapSettings</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Get-ImapSettings cmdlet to view the settings of the Microsoft Exchange IMAP4 service on Exchange servers. This is the client access (frontend) IMAP4 service that clients connect to.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-MailboxCalendarConfiguration</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Get-MailboxCalendarConfiguration cmdlet to show the calendar settings for a specified mailbox.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-MailboxMessageConfiguration</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p>

Cmdlet	Description
	<p>Use the Get-MailboxMessageConfiguration cmdlet to view the Outlook on the web settings that are applied to specific mailboxes.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-MailboxRegionalConfiguration</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Get-MailboxRegionalConfiguration cmdlet to view the regional settings of a mailbox. You can view the date format, time format, time zone, and language of the mailbox.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-MailboxSpellingConfiguration</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Get-MailboxSpellingConfiguration cmdlet to retrieve the Outlook on the web spelling checker settings of a specified user. For example, users can set their dictionary language and configure the spelling checker to ignore mixed digits and words in all uppercase.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-OutlookProvider</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Get-OutlookProvider cmdlet to obtain the global settings from the AutoDiscoverConfig object under the Global Settings object in Active Directory.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-OwaMailboxPolicy</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one</p>

Cmdlet	Description
	<p>environment or the other.</p> <p>Use the Get-OwaMailboxPolicy cmdlet to view Outlook on the web mailbox policies in the organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-PopSettings</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Get-POPSettings cmdlet to view the configuration of the Microsoft Exchange POP3 service. This service exists on Exchange servers that have the Client Access server role installed and is used by POP3 clients to connect to Exchange.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-TextMessagingAccount</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Get-TextMessagingAccount cmdlet to view the text notification settings on mailboxes.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
New-ClientAccessRule	<p>Note</p> <p>Client access rules were deprecated for all Exchange Online organizations in September 2025. For more information, see Update on Client Access Rules Deprecation in Exchange Online.</p> <p>This cmdlet is functional only in Exchange Server 2019 or later.</p> <p>Use the New-ClientAccessRule cmdlet to create client access rules. Client access rules help you control access to your organization based on the properties of the connection.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
New-OutlookProvider	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the New-OutlookProvider cmdlet to create the AutoDiscoverConfig object and then populate the object with relevant settings.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
New-OwaMailboxPolicy	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the New-OwaMailboxPolicy cmdlet to create Outlook on the web mailbox policies.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Remove-ClientAccessRule	<p>Note</p> <p>Client access rules were deprecated for all Exchange Online organizations in September 2025. For more information, see Update on Client Access Rules Deprecation in Exchange Online.</p> <p>This cmdlet is functional only in Exchange Server 2019 or later.</p>

Cmdlet	Description
	<p>Use the Remove-ClientAccessRule cmdlet to remove client access rules. Client access rules help you control access to your organization based on the properties of the connection.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-OutlookProvider</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Remove-OutlookProvider cmdlet to delete the AutoDiscoverConfig object from Active Directory.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-OwaMailboxPolicy</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Remove-OwaMailboxPolicy cmdlet to remove Outlook on the web mailbox policies from the organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Send-TextMessagingVerificationCode</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Send-TextMessagingVerificationCode cmdlet to send a text messaging verification as part of configuring text message notifications on the mailbox.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-CASMailbox</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p>

Cmdlet	Description
	<p>Use the Set-CASMailbox cmdlet to configure client access settings on a mailbox. For example, you can configure settings for Exchange ActiveSync, Outlook, Outlook on the web, POP3, and IMAP4.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-CASMailboxPlan</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Set-CASMailboxPlan cmdlet to modify Client Access services (CAS) mailbox plans in cloud-based organizations.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-ClientAccessRule</p>	<p>Note</p> <p>Client access rules were deprecated for all Exchange Online organizations in September 2025. For more information, see Update on Client Access Rules Deprecation in Exchange Online.</p> <p>This cmdlet is functional only in Exchange Server 2019 or later.</p> <p>Use the Set-ClientAccessRule cmdlet to modify existing client access rules. Client access rules help you control access to your organization based on the properties of the connection.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-ImapSettings</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Set-ImapSettings cmdlet to modify the settings of the Microsoft Exchange IMAP4 service on Exchange servers. This service exists on Exchange servers that have the Client Access server role installed, and is used by IMAP4 clients to connect to Exchange.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
Set-MailboxCalendarConfiguration	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Set-MailboxCalendarConfiguration cmdlet to modify mailbox calendar settings for Outlook on the web. This affects how the user's calendar looks and how reminders work in Outlook on the web. This also affects settings that define how meeting invitations, responses, and notifications are sent to the user.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Set-MailboxMessageConfiguration	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Set-MailboxMessageConfiguration cmdlet to configure the Outlook on the web settings that are applied to specific mailboxes.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Set-MailboxRegionalConfiguration	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Set-MailboxRegionalConfiguration cmdlet to modify the regional settings of a mailbox. You can modify the date format, time format, time zone and language of the mailbox.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Set-MailboxSpellingConfiguration	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Set-MailboxSpellingConfiguration cmdlet to modify Outlook on the web spelling checker options for a specified user. For example, you</p>

Cmdlet	Description
	<p>can set the dictionary language and configure the spelling checker to ignore mixed digits or words in all uppercase.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-OutlookProvider</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Set-OutlookProvider cmdlet to set specific global settings using the msExchOutlookProvider attribute on the msExchAutoDiscoverConfig object in Active Directory.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-OwaMailboxPolicy</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Set-OwaMailboxPolicy cmdlet to configure existing Outlook on the web mailbox policies.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-PopSettings</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Set-PopSettings cmdlet to modify the configuration of the Microsoft Exchange POP3 service. This service exists on Exchange servers that have the Client Access server role installed, and is used by POP3 clients to connect to Exchange.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-TextMessagingAccount</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p>

Cmdlet	Description
	<p>The Set-TextMessagingAccount cmdlet allows a user to configure the text messaging settings on their own mailbox. An administrator can't use this cmdlet to configure the text messaging settings on another user's mailbox.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Test-CalendarConnectivity</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Test-CalendarConnectivity cmdlet to verify that anonymous calendar sharing is enabled and working properly. The Calendar virtual directory is a subdirectory of the Microsoft Outlook on the web virtual directories. When you run this command without any parameters, the command tests calendar connectivity against all Outlook on the web virtual directories.</p> <p>Note: This cmdlet works best in Exchange 2010. In later versions of Exchange, the functionality of this cmdlet is replaced by Managed Availability. For the best results, use the Invoke-MonitoringProbe cmdlet and specify the relevant active monitor probe instead of using this cmdlet.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Test-ClientAccessRule</p>	<p>Note</p> <p>Client access rules were deprecated for all Exchange Online organizations in September 2025. For more information, see Update on Client Access Rules Deprecation in Exchange Online.</p> <p>This cmdlet is functional only in Exchange Server 2019 or later.</p> <p>Use the Test-ClientAccessRule cmdlet to test how client access rules affect access to your organization. If any of the client properties you specify for this cmdlet match any client access rules, the rules are returned in the results.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
Test-EcpConnectivity	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Test-EcpConnectivity cmdlet to test connectivity to Exchange Control Panel (ECP) virtual directories.</p> <p>Note: This cmdlet works best in Exchange 2010. In later versions of Exchange, the functionality of this cmdlet is replaced by Managed Availability. For the best results, use the Invoke-MonitoringProbe cmdlet and specify the relevant active monitor probe instead of using this cmdlet.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Test-ImapConnectivity	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Test-ImapConnectivity cmdlet to verify that connectivity to the Microsoft Exchange IMAP4 service is working as expected.</p> <p>Note: This cmdlet works best in Exchange 2010. In later versions of Exchange, the functionality of this cmdlet is replaced by Managed Availability. For the best results, use the Invoke-MonitoringProbe cmdlet and specify the relevant active monitor probe instead of using this cmdlet.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Test-OutlookConnectivity	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Test-OutlookConnectivity cmdlet to test end-to-end Microsoft Outlook client connectivity in the Microsoft Exchange organization. This includes testing for both Outlook Anywhere (RPC over HTTP) and MAPI over HTTP connections.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Test-OutlookWebServices	<p>This cmdlet is functional only in Exchange Server 2010.</p>

Cmdlet	Description
	<p>Use the Test-OutlookWebServices cmdlet to verify the Autodiscover service settings for Microsoft Outlook on a computer running Microsoft Exchange Server 2010 that has the Client Access server role installed.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Test-OwaConnectivity</p>	<p>This cmdlet is available only in Exchange Server 2010.</p> <p>Use the Test-OwaConnectivity cmdlet to verify that Microsoft Office Outlook Web App is running as expected. The Test-OwaConnectivity cmdlet can be used to test Outlook Web App connectivity for all Microsoft Exchange Server 2010 virtual directories on a specified Client Access server for all mailboxes on servers running Exchange that are in the same Active Directory site. The Test-OwaConnectivity cmdlet can also be used to test the connectivity for an individual Exchange Outlook Web App URL.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Test-PopConnectivity</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Test-PopConnectivity cmdlet to verify that the Microsoft Exchange POP3 service is working as expected.</p> <p>Note: This cmdlet works best in Exchange 2010. In later versions of Exchange, the functionality of this cmdlet is replaced by Managed Availability. For the best results, use the Invoke-MonitoringProbe cmdlet and specify the relevant active monitor probe instead of using this cmdlet.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Test-PowerShellConnectivity</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Test-PowerShellConnectivity cmdlet to test client connectivity to Exchange remote PowerShell virtual directories.</p>

Cmdlet	Description
	<p>Note: This cmdlet works best in Exchange 2010. In later versions of Exchange, the functionality of this cmdlet is replaced by Managed Availability. For the best results, use the Invoke-MonitoringProbe cmdlet and specify the relevant active monitor probe instead of using this cmdlet.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Test-WebServicesConnectivity</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Test-WebServicesConnectivity cmdlet to test client connectivity to Exchange Web Services virtual directories.</p> <p>Note: This cmdlet works best in Exchange 2010. In later versions of Exchange, the functionality of this cmdlet is replaced by Managed Availability. For the best results, use the Invoke-MonitoringProbe cmdlet and specify the relevant active monitor probe instead of using this cmdlet.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Cmdlet	Description
<p>Disable-OutlookAnywhere</p>	<p>This cmdlet is available only in Exchange Server 2010.</p> <p>Use the Disable-OutlookAnywhere cmdlet to disable Outlook Anywhere on Exchange Server 2010 Client Access servers.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Enable-OutlookAnywhere</p>	<p>This cmdlet is available only in Exchange Server 2010.</p> <p>Use the Enable-OutlookAnywhere cmdlet to enable Outlook Anywhere on a computer running Microsoft Exchange Server 2010 that has the Client Access server role installed. Running the Enable-OutlookAnywhere cmdlet enables the server to accept requests from Microsoft Office Outlook 2007 and Outlook 2003 client computers from the Internet by using Outlook Anywhere, also known as RPC over HTTP.</p>

Cmdlet	Description
	<p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-ActiveSyncVirtualDirectory</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Get-ActiveSyncVirtualDirectory cmdlet to view Exchange ActiveSync virtual directories that are used in Internet Information Services (IIS) on Microsoft Exchange servers.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-AuthRedirect</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Get-AuthRedirect cmdlet to view OAuth redirection objects that are used for legacy Microsoft Exchange 2010 Client Access servers in your organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-AutodiscoverVirtualDirectory</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Get-AutodiscoverVirtualDirectory cmdlet to view Autodiscover virtual directories that are used in Internet Information Services (IIS) on Microsoft Exchange servers.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-ClientAccessArray</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Get-ClientAccessArray cmdlet to view legacy RPC Client Access arrays (load-balanced arrays of Client Access servers within a single Active Directory site) that exist in your Exchange organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
Get-ClientAccessServer	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Get-ClientAccessServer cmdlet to view settings that are associated with the Client Access server role.</p> <p>Note: In Exchange 2013 or later, use the Get-ClientAccessService cmdlet instead. If you have scripts that use Get-ClientAccessServer, update them to use Get-ClientAccessService.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Get-ClientAccessService	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Get-ClientAccessService cmdlet to view settings that are associated with the Client Access server role.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Get-EcpVirtualDirectory	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Get-EcpVirtualDirectory cmdlet to view Exchange Control Panel (ECP) virtual directories that are used in Internet Information Services (IIS) on Microsoft Exchange servers. The Exchange admin center (EAC) uses the ECP virtual directories.</p> <p>The ECP web management interface was introduced in Exchange Server 2010. In Exchange Server 2013 and Exchange Server 2016, the EAC virtual directories and the corresponding management cmdlets still use ECP in the name. You can use these cmdlets to manage ECP virtual directories on Exchange 2010, Exchange 2013 and Exchange 2016 servers.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Get-MapiVirtualDirectory	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Get-MapiVirtualDirectory cmdlet to view Message Application Programming Interface (MAPI) virtual directories that are used in Internet Information Services (IIS) on Microsoft Exchange servers. A MAPI virtual</p>

Cmdlet	Description
	<p>directory is used by supported versions of Microsoft Outlook to connect to mailboxes by using the MAPIHTTP protocol.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-OutlookAnywhere</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Get-OutlookAnywhere cmdlet to view Outlook Anywhere virtual directories that are used in Internet Information Services (IIS) on Microsoft Exchange servers.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-OwaVirtualDirectory</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Get-OwaVirtualDirectory cmdlet to view Outlook on the web virtual directories that are used in Internet Information Services (IIS) on Microsoft Exchange servers.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-PowerShellVirtualDirectory</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Get-PowerShellVirtualDirectory cmdlet to view Windows PowerShell virtual directories that are used in Internet Information Services (IIS) on Microsoft Exchange servers.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-RpcClientAccess</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Get-RpcClientAccess cmdlet to view the settings of the Microsoft Exchange RPC Client Access service on Exchange servers that have the Client Access server role installed. These settings affect Outlook clients that connect by using Outlook Anywhere (RPC over HTTP).</p>

Cmdlet	Description
	<p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-WebServicesVirtualDirectory</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Get-WebServicesVirtualDirectory cmdlet to view Exchange Web Services (EWS) virtual directories that are used in Internet Information Services (IIS) on Microsoft Exchange servers.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-ActiveSyncVirtualDirectory</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the New-ActiveSyncVirtualDirectory cmdlet to create Exchange ActiveSync virtual directories that are used in Internet Information Services (IIS) on Microsoft Exchange servers.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-AuthRedirect</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the New-AuthRedirect cmdlet to create OAuth redirection objects that are used for legacy Microsoft Exchange 2010 Client Access servers in your organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-AutodiscoverVirtualDirectory</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the New-AutodiscoverVirtualDirectory cmdlet to create Autodiscover virtual directories that are used in Internet Information Services (IIS) on Microsoft Exchange servers.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
New-ClientAccessArray	<p>This cmdlet is available only in Exchange Server 2010.</p> <p>Use the New-ClientAccessArray cmdlet to create an object that represents a load balanced array of Client Access servers within a single Active Directory site.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
New-EcpVirtualDirectory	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the New-EcpVirtualDirectory cmdlet to create Exchange Control Panel (ECP) virtual directories that are used in Internet Information Services (IIS) on Microsoft Exchange servers. This is a command that Microsoft Exchange Server Setup runs when you install Exchange in your organization. The ECP virtual directory manages the Exchange admin center.</p> <p>The ECP web management interface was introduced in Exchange Server 2010. In Exchange Server 2013 and Exchange Server 2016, the EAC virtual directories and the corresponding management cmdlets still use ECP in the name. You can use these cmdlets to manage ECP virtual directories on Exchange 2010, Exchange 2013, and Exchange 2016 servers.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
New-MapiVirtualDirectory	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the New-MapiVirtualDirectory cmdlet to create Messaging Application Programming Interface (MAPI) virtual directories that are used in Internet Information Services (IIS) on Microsoft Exchange servers. A MAPI virtual directory is used by supported versions of Microsoft Outlook to connect to mailboxes by using the MAPIHTTP protocol.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
New-OwaVirtualDirectory	<p>This cmdlet is available only in on-premises Exchange.</p>

Cmdlet	Description
	<p>Use the New-OwaVirtualDirectory cmdlet to create Outlook on the web virtual directories that are used in Internet Information Services on Exchange servers. Typically, you create virtual directories on Exchange servers that have the Client Access server role installed.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-PowerShellVirtualDirectory</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the New-PowerShellVirtualDirectory cmdlet to create Windows PowerShell virtual directories that are used in Internet Information Services (IIS) on Microsoft Exchange servers.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-RpcClientAccess</p>	<p>This cmdlet is available only in Exchange Server 2010.</p> <p>Use the New-RpcClientAccess cmdlet to create configuration information for the Exchange RPC Client Access service on a Client Access server. This set up task is performed by default on new installations of the Client Access server role on Microsoft Exchange Server 2010.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-WebServicesVirtualDirectory</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the New-WebServicesVirtualDirectory cmdlet to create Exchange Web Services virtual directories that are used in Internet Information Services (IIS) on Microsoft Exchange servers.</p> <p>You can create multiple virtual directories by using this cmdlet. However, you can create only one Exchange Web Services virtual directory for each website.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
Remove-ActiveSyncVirtualDirectory	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Remove-ActiveSyncVirtualDirectory cmdlet to remove existing Exchange ActiveSync virtual directories from Internet Information Services (IIS) virtual directories on Exchange servers.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Remove-AuthRedirect	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Remove-AuthRedirect cmdlet to remove OAuth redirection objects that are used for legacy Microsoft Exchange 2010 Client Access servers in your organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Remove-AutodiscoverVirtualDirectory	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Remove-AutodiscoverVirtualDirectory cmdlet to remove an existing Autodiscover virtual directory from Internet Information Services (IIS).</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Remove-ClientAccessArray	<p>This cmdlet is available only in Exchange Server 2010.</p> <p>Use the Remove-ClientAccessArray cmdlet to remove RPC Client Access arrays (load-balanced arrays of Client Access servers within a single Active Directory site).</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Remove-EcpVirtualDirectory	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Remove-EcpVirtualDirectory cmdlet to remove Exchange Control Panel (ECP) virtual directories from Internet Information Services (IIS) on</p>

Cmdlet	Description
	<p>Microsoft Exchange servers. The ECP virtual directory manages the Exchange admin center.</p> <p>The ECP web management interface was introduced in Exchange Server 2010. In Exchange Server 2013 and Exchange Server 2016, the EAC virtual directories and the corresponding management cmdlets still use ECP in the name. You can use these cmdlets to manage ECP virtual directories on Exchange 2010, Exchange 2013 and Exchange 2016 servers.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-MapiVirtualDirectory</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Remove-MapiVirtualDirectory cmdlet to remove Message Application Programming Interface (MAPI) virtual directories from Exchange servers. A MAPI virtual directory is used by supported versions of Microsoft Outlook to connect to mailboxes by using the MAPIHTTP protocol.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-OwaVirtualDirectory</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Remove-OwaVirtualDirectory cmdlet to remove Outlook on the web virtual directories from Internet Information Services (IIS) on Exchange servers.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-PowerShellVirtualDirectory</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Remove-PowerShellVirtualDirectory cmdlet to remove existing Windows PowerShell virtual directories from Internet Information Services (IIS) on Exchange servers.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
Remove-RpcClientAccess	<p>This cmdlet is available only in Exchange Server 2010.</p> <p>Use the Remove-RpcClientAccess cmdlet to remove the configuration information that allows RPC access through the Client Access server role on Microsoft Exchange Server 2010. After you remove the configuration information, the Exchange RPC Client Access service stops and no longer starts.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Remove-WebServicesVirtualDirectory	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Remove-WebServicesVirtualDirectory cmdlet to remove existing Exchange Web Services virtual directories from Internet Information Services (IIS) on Microsoft Exchange servers.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Set-ActiveSyncVirtualDirectory	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Set-ActiveSyncVirtualDirectory cmdlet to modify existing Microsoft Exchange ActiveSync virtual directories that are used in Internet Information Services (IIS) on Exchange servers.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Set-AuthRedirect	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Set-AuthRedirect cmdlet to modify the existing OAuth redirection settings for Microsoft Exchange 2010 Client Access servers in your Microsoft Exchange 2013 organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Set-AutodiscoverVirtualDirectory	<p>This cmdlet is available only in on-premises Exchange.</p>

Cmdlet	Description
	<p>Use the Set-AutodiscoverVirtualDirectory cmdlet to configure Autodiscover virtual directories that are used in Internet Information Services (IIS) on Exchange servers.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-ClientAccessArray</p>	<p>This cmdlet is available only in Exchange Server 2010.</p> <p>Use the Set-ClientAccessArray cmdlet to modify RPC Client Access arrays (load-balanced arrays of Client Access servers within a single Active Directory site).</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-ClientAccessServer</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Set-ClientAccessServer cmdlet to modify settings that are associated with the Client Access server role.</p> <p>Note: In Exchange 2013 or later, use the Set-ClientAccessService cmdlet instead. If you have scripts that use Set-ClientAccessServer, update them to use Set-ClientAccessService.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-ClientAccessService</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Set-ClientAccessService cmdlet to modify settings that are associated with the Client Access server role.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-EcpVirtualDirectory</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Set-EcpVirtualDirectory cmdlet to modify Exchange Control Panel (ECP) virtual directories that are used in Internet Information Services (IIS)</p>

Cmdlet	Description
	<p>on Microsoft Exchange servers. The ECP virtual directory manages the Exchange admin center.</p> <p>The ECP web management interface was introduced in Exchange Server 2010. In Exchange Server 2013 and Exchange Server 2016, the EAC virtual directories and the corresponding management cmdlets still use ECP in the name. You can use these cmdlets to manage ECP virtual directories on Exchange 2010, Exchange 2013, and Exchange 2016 servers.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-MapiVirtualDirectory</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Set-MapiVirtualDirectory cmdlet to modify Messaging Application Programming Interface (MAPI) virtual directories that are used in Internet Information Services (IIS) on Microsoft Exchange servers. A MAPI virtual directory is used by supported versions of Microsoft Outlook to connect to mailboxes by using the MAPIHTTP protocol.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-OutlookAnywhere</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Set-OutlookAnywhere cmdlet to modify Outlook Anywhere virtual directories that are used in Internet Information Services (IIS) on Microsoft Exchange servers. Outlook Anywhere uses virtual directories that contain "rpc" in the name.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
Set-OwaVirtualDirectory	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Set-OwaVirtualDirectory cmdlet to modify existing Outlook on the web virtual directories that are used in Internet Information Services (IIS) on Exchange servers.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Set-PowerShellVirtualDirectory	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Set-PowerShellVirtualDirectory cmdlet to modify existing Windows PowerShell virtual directories that are used in Internet Information Services (IIS) on Exchange servers.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Set-RpcClientAccess	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Set-RpcClientAccess cmdlet to modify the settings of the Microsoft Exchange RPC Client Access service on Exchange servers that have the Client Access server role installed. These settings affect Outlook clients that connect by using Outlook Anywhere (RPC over HTTP).</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Set-WebServicesVirtualDirectory	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Set-WebServicesVirtualDirectory cmdlet to modify existing Exchange Web Services virtual directories that are used in Internet Information Services (IIS) on Microsoft Exchange servers.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
Add-DatabaseAvailabilityGroupServer	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Add-DatabaseAvailabilityGroupServer cmdlet to add a Mailbox server to a database availability group (DAG). A DAG is a set of Mailbox servers that use continuous replication and managed availability to provide automatic database-level recovery from database, server, or network failures.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Add-MailboxDatabaseCopy	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Add-MailboxDatabaseCopy cmdlet to create a passive copy of an existing active mailbox database.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Get-DatabaseAvailabilityGroup	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Get-DatabaseAvailabilityGroup cmdlet to obtain a variety of configuration settings, status and other information about a database availability group (DAG).</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Get-DatabaseAvailabilityGroupNetwork	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Get-DatabaseAvailabilityGroupNetwork cmdlet to display configuration and state information for a database availability group (DAG) network.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Get-MailboxDatabaseCopyStatus	<p>This cmdlet is available only in on-premises Exchange.</p>

Cmdlet	Description
	<p>Use the Get-MailboxDatabaseCopyStatus cmdlet to view health and status information about one or more mailbox database copies.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Move-ActiveMailboxDatabase</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Move-ActiveMailboxDatabase cmdlet to perform a database or server switchover.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-DatabaseAvailabilityGroup</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the New-DatabaseAvailabilityGroup cmdlet to create a database availability group (DAG).</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-DatabaseAvailabilityGroupNetwork</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the New-DatabaseAvailabilityGroupNetwork cmdlet to create a database availability group (DAG) network.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-DatabaseAvailabilityGroup</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Remove-DatabaseAvailabilityGroup cmdlet to delete an empty database availability group (DAG). Before you can delete a DAG, you must first remove all Mailbox servers from the DAG.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
Remove-DatabaseAvailabilityGroupNetwork	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Remove-DatabaseAvailabilityGroupNetwork cmdlet to remove a database availability group (DAG) network.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Remove-DatabaseAvailabilityGroupServer	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Remove-DatabaseAvailabilityGroupServer cmdlet to remove a Mailbox server from a database availability group (DAG). To remove a Mailbox server from a DAG, the Mailbox server must not host any replicated databases.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Remove-MailboxDatabaseCopy	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Remove-MailboxDatabaseCopy cmdlet to remove a passive copy of a mailbox database.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Restore-DatabaseAvailabilityGroup	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Restore-DatabaseAvailabilityGroup cmdlet as part of a datacenter switchover of a database availability group (DAG).</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Resume-MailboxDatabaseCopy	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Resume-MailboxDatabaseCopy cmdlet to unblock activation or resume log copying and replay for a passive mailbox database copy.</p>

Cmdlet	Description
	<p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-DatabaseAvailabilityGroup</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Set-DatabaseAvailabilityGroup cmdlet to configure properties of a database availability group (DAG).</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-DatabaseAvailabilityGroupNetwork</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Set-DatabaseAvailabilityGroupNetwork cmdlet to configure a network for a database availability group (DAG).</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-MailboxDatabaseCopy</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Set-MailboxDatabaseCopy cmdlet to configure the properties of a database copy.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Start-DatabaseAvailabilityGroup</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Start-DatabaseAvailabilityGroup cmdlet to reincorporate one or more previously failed members of a database availability group (DAG).</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Stop-DatabaseAvailabilityGroup</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Stop-DatabaseAvailabilityGroup cmdlet to mark a member of a database availability group (DAG) as failed, or to mark all DAG</p>

Cmdlet	Description
	<p>members in a specific Active Directory site as failed.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Suspend-MailboxDatabaseCopy</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Suspend-MailboxDatabaseCopy cmdlet to block replication and replay activities (log copying and replay) or activation for a database configured with two or more database copies.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Test-ReplicationHealth</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Test-ReplicationHealth cmdlet to check all aspects of replication and replay, or to provide status for a specific Mailbox server in a database availability group (DAG).</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Update-MailboxDatabaseCopy</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Update-MailboxDatabaseCopy cmdlet to seed or reseed a mailbox database copy.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Cmdlet	Description
<p>Disable-AntiPhishRule</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Disable-AntiPhishRule cmdlet to disable antiphish rules in your cloud-based organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
Disable-ATPProtectionPolicyRule	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Disable-ATPProtectionPolicyRule and Disable-EOPProtectionPolicyRule cmdlets together to turn off the Standard preset security policy or the Strict preset security policy in organizations with Microsoft Defender for Office 365.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Disable-SafeAttachmentRule	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Disable-SafeAttachmentRule cmdlet to disable safe attachment rules in your cloud-based organization. This cmdlet is also responsible for disabling complete Safe Attachments policies in the admin center, which consist of the safe attachment rule and the corresponding assigned safe attachment policy in PowerShell.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Disable-SafeLinksRule	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Disable-SafeLinksRule cmdlet to disable enabled Safe Links rules in your cloud-based organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Enable-AntiPhishRule	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Enable-AntiPhishRule cmdlet to enable antiphish rules in your cloud-based organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Enable-ATPProtectionPolicyRule	<p>This cmdlet is available only in the cloud-based service.</p>

Cmdlet	Description
	<p>Use the Enable-ATPProtectionPolicyRule and Enable-EOPProtectionPolicyRule cmdlets together to turn on the Standard preset security policy or the Strict preset security policy in organizations with Microsoft Defender for Office 365.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Enable-SafeAttachmentRule</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Enable-SafeAttachmentRule cmdlet to enable safe attachment rules in your cloud-based organization. This cmdlet is also responsible for disabling complete Safe Attachments policies in the admin center, which consist of the safe attachment rule and the corresponding assigned safe attachment policy in PowerShell.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Enable-SafeLinksRule</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Enable-SafeLinksRule cmdlet to enable disabled Safe Links rules in your cloud-based organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-AntiPhishPolicy</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Get-AntiPhishPolicy cmdlet to view antiphish policies in your cloud-based organization. This cmdlet returns results only in Exchange Online PowerShell.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-AntiPhishRule</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Get-AntiPhishRule cmdlet to view antiphish rules in your cloud-based organization.</p>

Cmdlet	Description
	<p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-ATPBuiltInProtectionRule</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Get-ATPBuiltInProtectionRule cmdlet to view the rule for the Built-in protection preset security policy that effectively provides default policies for Safe Links and Safe Attachments in Microsoft Defender for Office 365. The rule specifies exceptions to the policy.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-AtpPolicyForO365</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Get-AtpPolicyForO365 cmdlet to view the settings for the following features in Microsoft Defender for Office 365:</p> <ul style="list-style-type: none"> • Safe Links protection for supported Office 365 apps. • Safe Documents: Uses Microsoft Defender for Endpoint to scan documents and files that are opened in Protected View in Microsoft 365 apps for enterprise. • Safe Attachments for SharePoint, OneDrive, and Microsoft Teams. <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-ATPProtectionPolicyRule</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Get-ATPProtectionPolicyRule cmdlet to view rules for Microsoft Defender for Office 365 protections in preset security policies. The rules specify recipient conditions and exceptions for the protection, and also allow you to turn on and turn off the associated preset security policies.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
Get-ATPTotalTrafficReport	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Get-ATPTotalTrafficReport to view details about message traffic in your Microsoft Defender for Office 365 organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Get-ContentMalwareMdoAggregateReport	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Get-ContentMalwareMdoAggregateReport cmdlet to view a summary detections by Safe Attachments for SharePoint, OneDrive, and Microsoft Teams in Microsoft Defender for Office 365.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Get-ContentMalwareMdoDetailReport	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the ContentMalwareMdoDetailReport cmdlet to view detection details by Safe Attachments for SharePoint, OneDrive, and Microsoft Teams in Microsoft Defender for Office 365.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Get-EmailTenantSettings	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Get-EmailTenantSettings cmdlet to view whether priority account protection is enabled or disabled in your Microsoft Defender for Office 365 organization. For more information about priority accounts, see Manage and monitor priority accounts.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Get-MailDetailATPReport	<p>This cmdlet is available only in the cloud-based service.</p>

Cmdlet	Description
	<p>Use the Get-MailDetailATPReport cmdlet to list details about Microsoft Defender for Office 365 detections in your cloud-based organization for the last 10 days.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-MailTrafficATPReport</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Get-MailTrafficATPReport cmdlet to view the results of Microsoft Defender for Office 365 detections in your cloud-based organization for the last 90 days.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-SafeAttachmentPolicy</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Get-SafeAttachmentPolicy cmdlet to view safe attachment policies in your cloud-based organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-SafeAttachmentRule</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Get-SafeAttachmentRule cmdlet to view safe attachment rules in your cloud-based organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-SafeLinksAggregateReport</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Get-SafeLinksAggregateReport cmdlet to return general information about Safe Links results for the last 90 days. Yesterday is the most recent date that you can specify.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
Get-SafeLinksDetailReport	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Get-SafeLinksDetailReport cmdlet to return detailed information about Safe Links results for the last 7 days. Yesterday is the most recent date that you can specify.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Get-SafeLinksPolicy	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Get-SafeLinksPolicy cmdlet to view Safe Links policies in your cloud-based organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Get-SafeLinksRule	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Get-SafeLinksRule cmdlet to view Safe Links rules in your cloud-based organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Get-SpoofIntelligenceInsight	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Get-SpoofIntelligenceInsight cmdlet to view spoofed senders that were allowed or blocked by spoof intelligence during the last 30 days.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Get-SpoofMailReport	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Get-SpoofMailReport cmdlet to view information about spoofed senders in your cloud-based organization for the past 90 days. Spoofing is where the sender of the inbound message is different than the actual source of the message (for example, the</p>

Cmdlet	Description
	<p>sender is lila@contoso.com, but the message was sent from the email infrastructure of fabrikam.com).</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-AntiPhishPolicy</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the New-AntiPhishPolicy cmdlet to create antiphish policies in your cloud-based organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-AntiPhishRule</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the New-AntiPhishRule cmdlet to create antiphish rules in your cloud-based organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-ATPBuiltInProtectionRule</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Note: Don't use this cmdlet. This cmdlet is used by the system to create the one and only rule for the Built-in protection preset security policy during the creation of the organization. You can't use this cmdlet if a rule for the Built-in protection preset security policy already exists. The Remove-ATPBuiltInProtectionRule cmdlet is not available to remove rules.</p> <p>Use the New-ATPBuiltInProtectionRule cmdlet to create the rule for the Built-in protection preset security policy that effectively provides default policies for Safe Links and Safe Attachments in Microsoft Defender for Office 365. The rule specifies exceptions to the policy.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
<p>New-ATPProtectionPolicyRule</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the New-ATPProtectionPolicyRule cmdlet to create rules for Microsoft Defender for Office 365 protections in preset security policies. The rules specify recipient conditions and exceptions for the protection, and also allow you to turn on and turn off the associated preset security policies.</p> <p>Note: Unless you manually removed a rule using the Remove-ATPProtectionPolicyRule cmdlet, we don't recommend using this cmdlet to create rules. To create the rule, you need to specify the existing individual security policies that are associated with the preset security policy. We never recommend creating these required individual security policies manually. Turning on the preset security policy for the first time in the Microsoft Defender portal automatically creates the required individual security policies, but also creates the associated rules using this cmdlet. So, if the rules already exist, you don't need to use this cmdlet to create them.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-SafeAttachmentPolicy</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the New-SafeAttachmentPolicy cmdlet to create safe attachment policies in your cloud-based organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-SafeAttachmentRule</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the New-SafeAttachmentRule cmdlet to create safe attachment rules in your cloud-based organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-SafeLinksPolicy</p>	<p>This cmdlet is available only in the cloud-based service.</p>

Cmdlet	Description
	<p>Use the New-SafeLinksPolicy cmdlet to create Safe Links policies in your cloud-based organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-SafeLinksRule</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the New-SafeLinksRule cmdlet to create Safe Links rules in your cloud-based organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-AntiPhishPolicy</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Remove-AntiPhishPolicy cmdlet to remove antiphish policies from your cloud-based organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-AntiPhishRule</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Remove-AntiPhishRule cmdlet to remove antiphish rules from your cloud-based organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-ATPProtectionPolicyRule</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Remove-ATPProtectionPolicyRule cmdlet to remove rules from Microsoft Defender for Office 365 protections in preset security policies. The rules specify recipient conditions and exceptions for the protection, and also allow you to turn on and turn off the associated preset security policies.</p> <p>Note: Use this cmdlet to remove a rule only if you plan to immediately recreate the rule using the New-</p>

Cmdlet	Description
	<p>ATPProtectionPolicyRule cmdlet. The affected preset security policy doesn't function without a corresponding rule.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-SafeAttachmentPolicy</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Remove-SafeAttachmentPolicy cmdlet to remove safe attachment policies from your cloud-based organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-SafeAttachmentRule</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Remove-SafeAttachmentRule cmdlet to remove safe attachment rules from your cloud-based organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-SafeLinksPolicy</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Remove-SafeLinksPolicy cmdlet to remove Safe Links policies from your cloud-based organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-SafeLinksRule</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Remove-SafeLinksRule cmdlet to remove Safe Links rules from your cloud-based organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-AntiPhishPolicy</p>	<p>This cmdlet is available only in the cloud-based service.</p>

Cmdlet	Description
	<p>Use the Set-AntiPhishPolicy cmdlet to modify antiphish policies in your cloud-based organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-AntiPhishRule</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Set-AntiPhishRule cmdlet to modify antiphish rules in your cloud-based organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-ATPBuiltInProtectionRule</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Set-ATPBuiltInProtectionRule cmdlet to modify the rule for the Built-in protection preset security policy that effectively provides default policies for Safe Links and Safe Attachments in Microsoft Defender for Office 365. The rule specifies exceptions to the policy.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-AtpPolicyForO365</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Set-AtpPolicyForO365 cmdlet to modify the settings for the following features in Microsoft Defender for Office 365:</p> <ul style="list-style-type: none"> • Safe Links protection for supported Office 365 apps. • Safe Documents: Uses Microsoft Defender for Endpoint to scan documents and files that are opened in Protected View in Microsoft 365 apps for enterprise. • Safe Attachments for SharePoint, OneDrive, and Microsoft Teams. <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
Set-ATPProtectionPolicyRule	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Set-ATPProtectionPolicyRule cmdlet to modify rules that are associated with Microsoft Defender for Office 365 protections in preset security policies.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Set-EmailTenantSettings	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Set-EmailTenantSettings cmdlet to enable or disable priority account protection in your Microsoft Defender for Office 365 organization. For more information about priority accounts, see Manage and monitor priority accounts.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Set-SafeAttachmentPolicy	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Set-SafeAttachmentPolicy cmdlet to modify safe attachment policies in your cloud-based organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Set-SafeAttachmentRule	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Set-SafeAttachmentRule cmdlet to modify safe attachment rules in your cloud-based organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Set-SafeLinksPolicy	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Set-SafeLinksPolicy cmdlet to modify Safe Links policies in your cloud-based organization.</p>

Cmdlet	Description
	<p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-SafeLinksRule</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Set-SafeLinksRule cmdlet to create Safe Links rules in your cloud-based organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Cmdlet	Description
<p>Clear-ActiveSyncDevice</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Clear-ActiveSyncDevice cmdlet to delete all data from a mobile device.</p> <p>Note: In Exchange 2013 or later, use the Clear-MobileDevice cmdlet instead. If you have scripts that use Clear-ActiveSyncDevice, update them to use Clear-MobileDevice.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Clear-MobileDevice</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Clear-MobileDevice cmdlet to delete all data from a mobile phone. This action is often called a remote device wipe.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Export-ActiveSyncLog</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Export-ActiveSyncLog cmdlet to parse the Internet Information Services (IIS) logs and return information about</p>

Cmdlet	Description
	<p>Microsoft Exchange ActiveSync usage, either on the screen or in an output file.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-ActiveSyncDevice</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Get-ActiveSyncDevice cmdlet to retrieve the list of devices in your organization that have active Exchange ActiveSync partnerships.</p> <p>Note: In Exchange 2013 or later, use the Get-MobileDevice cmdlet instead. If you have scripts that use Get-ActiveSyncDevice, update them to use Get-MobileDevice.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-ActiveSyncDeviceAccessRule</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Get-ActiveSyncDeviceAccessRule cmdlet to retrieve an access group of Exchange mobile devices along with their access level.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-ActiveSyncDeviceAutoblockThreshold</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Get-ActiveSyncDeviceAutoblockThreshold cmdlet to obtain the Autoblock settings for Microsoft Exchange ActiveSync mobile devices.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
<p>Get-ActiveSyncDeviceClass</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Get-ActiveSyncDeviceClass cmdlet to retrieve a list of ActiveSync devices that have connected to your organization. The cmdlet returns the mobile device type and model information.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-ActiveSyncDeviceStatistics</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Get-ActiveSyncDeviceStatistics cmdlet to retrieve the list of mobile devices configured to synchronize with a specified user's mailbox and return a list of statistics about the mobile devices.</p> <p>Note: This cmdlet works best in Exchange 2010. In later versions of Exchange or Exchange Online, use the Get-MobileDeviceStatistics cmdlet instead. If you have scripts that use Get-ActiveSyncDeviceStatistics, update them to use Get-MobileDeviceStatistics.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-ActiveSyncMailboxPolicy</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Get-ActiveSyncMailboxPolicy cmdlet to retrieve the Mobile Device mailbox policy settings for a specific Mobile Device mailbox policy.</p> <p>Note: In Exchange 2013 or later, use the Get-MobileDeviceMailboxPolicy cmdlet instead. If you have scripts that use Get-ActiveSyncMailboxPolicy, update them to use Get-MobileDeviceMailboxPolicy.</p>

Cmdlet	Description
	<p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-ActiveSyncOrganizationSettings</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Get-ActiveSyncOrganizationSettings cmdlet to view the Microsoft Exchange ActiveSync settings for your organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-DeviceConditionalAccessPolicy</p>	<p>This cmdlet is functional only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Get-DeviceConditionalAccessPolicy cmdlet to view mobile device conditional access policies in Basic Mobility and Security in Microsoft 365.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-DeviceConditionalAccessRule</p>	<p>This cmdlet is functional only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Get-DeviceConditionalAccessRule cmdlet to view mobile device conditional access rules in Basic Mobility and Security in Microsoft 365.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-DeviceConfigurationPolicy</p>	<p>This cmdlet is functional only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p>

Cmdlet	Description
	<p>Use the Get-DeviceConfigurationPolicy cmdlet to view mobile device configuration policies in Basic Mobility and Security in Microsoft 365.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-DeviceConfigurationRule</p>	<p>This cmdlet is functional only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Get-DeviceConfigurationRule cmdlet to view mobile device configuration rules in Basic Mobility and Security in Microsoft 365.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-DevicePolicy</p>	<p>This cmdlet is functional only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Get-DevicePolicy cmdlet to view all types of Basic Mobility and Security policies in Microsoft 365.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-DeviceTenantPolicy</p>	<p>This cmdlet is functional only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Get-DeviceTenantPolicy cmdlet to view your organization's mobile device tenant policy in Basic Mobility and Security in Microsoft 365.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
<p>Get-DeviceTenantRule</p>	<p>This cmdlet is functional only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Get-DeviceTenantRule cmdlet to view your organization's mobile device tenant rule in Basic Mobility and Security in Microsoft 365.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-MobileDevice</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Get-MobileDevice cmdlet to get the list of devices in your organization that have active partnerships.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-MobileDeviceMailboxPolicy</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Get-MobileDeviceMailboxPolicy cmdlet to retrieve the Mobile Device mailbox policy settings for a specific Mobile Device mailbox policy.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-MobileDeviceStatistics</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Get-MobileDeviceStatistics cmdlet to retrieve the list of mobile devices configured to synchronize with a specified user's mailbox and return a list of statistics about the mobile devices.</p>

Cmdlet	Description
	<p>Note: In Exchange Online PowerShell, we recommend that you use the Get-EXOMobileDeviceStatistics cmdlet instead of this cmdlet. For more information, see Connect to Exchange Online PowerShell.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-ActiveSyncDeviceAccessRule</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the New-ActiveSyncDeviceAccessRule cmdlet to define the access levels for Exchange ActiveSync devices based on the identity of the device.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-ActiveSyncMailboxPolicy</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the New-ActiveSyncMailboxPolicy cmdlet to create a Microsoft Mobile Device mailbox policy object.</p> <p>Note: In Exchange 2013 or later, use the New-MobileDeviceMailboxPolicy cmdlet instead. If you have scripts that use New-ActiveSyncMailboxPolicy, update them to use New-MobileDeviceMailboxPolicy.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-DeviceConditionalAccessPolicy</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the New-DeviceConditionalAccessPolicy cmdlet to create mobile device conditional access policies in Basic Mobility and Security in Microsoft 365.</p>

Cmdlet	Description
	<p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-DeviceConditionalAccessRule</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the New-DeviceConditionalAccessRule cmdlet to create mobile device conditional access rules in Basic Mobility and Security in Microsoft 365.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-DeviceConfigurationPolicy</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the New-DeviceConfigurationPolicy cmdlet to create mobile device configuration policies in Basic Mobility and Security in Microsoft 365.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-DeviceConfigurationRule</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the New-DeviceConfigurationRule cmdlet to create mobile device configuration rules in Basic Mobility and Security in Microsoft 365.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-DeviceTenantPolicy</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p>

Cmdlet	Description
	<p>Use the New-DeviceTenantPolicy cmdlet to create your organization's mobile device tenant policy in Basic Mobility and Security in Microsoft 365.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-DeviceTenantRule</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the New-DeviceTenantRule cmdlet to create your organization's mobile device tenant rule in Basic Mobility and Security in Microsoft 365.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-MobileDeviceMailboxPolicy</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the New-MobileDeviceMailboxPolicy cmdlet to create mobile device mailbox policies.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-ActiveSyncDevice</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Remove-ActiveSyncDevice cmdlet to remove mobile device partnerships that identify the devices that are configured to synchronize with user mailboxes.</p> <p>Note: In Exchange 2013 or later, use the Remove-MobileDevice cmdlet instead. If you have scripts that use Remove-ActiveSyncDevice, update them to use Remove-MobileDevice.</p>

Cmdlet	Description
	<p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-ActiveSyncDeviceAccessRule</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Remove-ActiveSyncDeviceAccessRule cmdlet to remove any existing device access rule.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-ActiveSyncDeviceClass</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Remove-ActiveSyncDeviceClass cmdlet to clean up the list of mobile devices synchronizing with Microsoft Exchange.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-ActiveSyncMailboxPolicy</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Remove-ActiveSyncMailboxPolicy cmdlet to remove mobile device mailbox policies.</p> <p>Note: In Exchange 2013 or later, use the Remove-MobileDeviceMailboxPolicy cmdlet instead. If you have scripts that use Remove-ActiveSyncMailboxPolicy, update them to use Remove-MobileDeviceMailboxPolicy.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-DeviceConditionalAccessPolicy</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p>

Cmdlet	Description
	<p>Use the Remove-DeviceConditionalAccessPolicy cmdlet to remove mobile device conditional access policies from Basic Mobility and Security in Microsoft 365.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-DeviceConditionalAccessRule</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Remove-DeviceConditionalAccessRule cmdlet to remove mobile device conditional access rules from Basic Mobility and Security in Microsoft 365.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-DeviceConfigurationPolicy</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Remove-DeviceConfigurationPolicy cmdlet to remove mobile device configuration policies from Basic Mobility and Security in Microsoft 365.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-DeviceConfigurationRule</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Remove-DeviceConfigurationRule cmdlet to remove mobile device configuration rules from Basic Mobility and Security in Microsoft 365.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-DeviceTenantPolicy</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance</p>

Cmdlet	Description
	<p>PowerShell.</p> <p>Use the Remove-DeviceTenantPolicy cmdlet to remove your organization's mobile device tenant policy from Basic Mobility and Security in Microsoft 365.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-DeviceTenantRule</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Remove-DeviceTenantRule cmdlet to remove your organization's mobile device tenant rule from Basic Mobility and Security in Microsoft 365.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-MobileDevice</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Remove-MobileDevice cmdlet to remove mobile device partnerships that identify the devices that are configured to synchronize with user mailboxes.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-MobileDeviceMailboxPolicy</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Remove-MobileDeviceMailboxPolicy cmdlet to remove mobile device mailbox policies from Exchange servers.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
Set-ActiveSyncDeviceAccessRule	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Set-ActiveSyncDeviceAccessRule cmdlet to set the level of access for the rule.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Set-ActiveSyncDeviceAutoblockThreshold	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Set-ActiveSyncDeviceAutoblockThreshold cmdlet to change settings for autoblocking mobile devices.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Set-ActiveSyncMailboxPolicy	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Set-ActiveSyncMailboxPolicy cmdlet to apply a variety of Mobile Device mailbox policy settings to a server. You can set any of the parameters by using one command.</p> <p>Note: In Exchange 2013 or later, use the Set-MobileDeviceMailboxPolicy cmdlet instead. If you have scripts that use Set-ActiveSyncMailboxPolicy, update them to use Set-MobileDeviceMailboxPolicy.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Set-ActiveSyncOrganizationSettings	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Set-ActiveSyncOrganizationSettings cmdlet to set the Exchange ActiveSync settings for the organization.</p>

Cmdlet	Description
	<p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-DeviceConditionalAccessPolicy</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Set-DeviceConditionalAccessPolicy cmdlet to modify mobile device conditional access policies in Basic Mobility and Security in Microsoft 365.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-DeviceConditionalAccessRule</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Set-DeviceConditionalAccessRule cmdlet to modify mobile device conditional access rules in Basic Mobility and Security in Microsoft 365.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-DeviceConfigurationPolicy</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Set-DeviceConfigurationPolicy cmdlet to modify mobile device configuration policies in Basic Mobility and Security in Microsoft 365.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-DeviceConfigurationRule</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p>

Cmdlet	Description
	<p>Use the Set-DeviceConfigurationRule cmdlet to modify mobile device configuration rules in Basic Mobility and Security in Microsoft 365.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-DeviceTenantPolicy</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Set-DeviceTenantPolicy cmdlet to modify your organization's mobile device tenant policy in Basic Mobility and Security in Microsoft 365.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-DeviceTenantRule</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Set-DeviceTenantRule cmdlet to modify your organization's mobile device tenant rule in Basic Mobility and Security in Microsoft 365.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-MobileDeviceMailboxPolicy</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Set-MobileDeviceMailboxPolicy cmdlet to modify mobile device mailbox policies.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Test-ActiveSyncConnectivity</p>	<p>This cmdlet is available only in on-premises Exchange.</p>

Cmdlet	Description
	<p>Use the Test-ActiveSyncConnectivity cmdlet to test connectivity to Microsoft Exchange ActiveSync virtual directories.</p> <p>Note: This cmdlet works best in Exchange 2010. In later versions of Exchange, the functionality of this cmdlet is replaced by Managed Availability. For the best results, use the Invoke-MonitoringProbe cmdlet and specify the relevant active monitor probe instead of using this cmdlet.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Cmdlet	Description
<p>Disable-AddressListPaging</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Disable-AddressListPaging cmdlet to disable Active Directory virtual list view for address lists. Virtual list view displays address lists in your organization as pages instead of loading and viewing the entire directory.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Enable-AddressListPaging</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Enable-AddressListPaging cmdlet to enable Active Directory virtual list view for address lists. Virtual list view allows you to display the address lists in your organization as pages instead of loading and viewing the entire directory.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-AddressBookPolicy</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Get-AddressBookPolicy cmdlet to return address book policies that match the specified conditions.</p> <p>In Exchange Online, this cmdlet is available only in the Address Lists role, and by default, the role isn't assigned to any role groups. To use this cmdlet, you need to</p>

Cmdlet	Description
	<p>add the Address Lists role to a role group (for example, to the Organization Management role group). For more information, see Add a role to a role group.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Get-AddressList	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Get-AddressList cmdlet to view address lists.</p> <p>In Exchange Online, this cmdlet is available only in the Address Lists role, and by default, the role isn't assigned to any role groups. To use this cmdlet, you need to add the Address Lists role to a role group (for example, to the Organization Management role group). For more information, see Add a role to a role group.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Get-DetailsTemplate	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Get-DetailsTemplate cmdlet to retrieve the attributes for details templates.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Get-EmailAddressPolicy	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Get-EmailAddressPolicy cmdlet to view email address policies. In Exchange Online, email address policies are available only for Microsoft 365 Groups.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Get-GlobalAddressList	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Get-GlobalAddressList cmdlet to view a global address list (GAL) or a set of GALs.</p>

Cmdlet	Description
	<p>In Exchange Online, this cmdlet is available only in the Address Lists role, and by default, the role isn't assigned to any role groups. To use this cmdlet, you need to add the Address Lists role to a role group (for example, to the Organization Management role group). For more information, see Add a role to a role group.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-OabVirtualDirectory</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Get-OabVirtualDirectory cmdlet to view offline address book (OAB) virtual directories(OAB distribution points) that are used in Internet Information Services (IIS) on Microsoft Exchange servers.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-OfflineAddressBook</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Get-OfflineAddressBook cmdlet to view offline address books (OABs).</p> <p>In Exchange Online, this cmdlet is available only in the Address Lists role, and by default, the role isn't assigned to any role groups. To use this cmdlet, you need to add the Address Lists role to a role group (for example, to the Organization Management role group). For more information, see Add a role to a role group.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Move-AddressList</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Move-AddressList cmdlet to move an existing address list to a new container under the root address list.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Move-OfflineAddressBook</p>	<p>This cmdlet is available only in on-premises Exchange.</p>

Cmdlet	Description
	<p>Use the Move-OfflineAddressBook cmdlet to designate a new server that's responsible for generating the offline address book (OAB) in Exchange Server 2010. This cmdlet isn't used on OABs in Exchange Server 2016 or Exchange Server 2013. To perform this task in Exchange 2016 or Exchange 2013, use the Set-OfflineAddressBook cmdlet with the GeneratingMailbox parameter.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-AddressBookPolicy</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the New-AddressBookPolicy cmdlet to create an address book policy. Address book policies define the global address list (GAL), offline address book (OAB), room list, and address lists shown to mailbox users who are assigned the policy.</p> <p>In Exchange Online, this cmdlet is available only in the Address Lists role, and by default, the role isn't assigned to any role groups. To use this cmdlet, you need to add the Address Lists role to a role group (for example, to the Organization Management role group). For more information, see Add a role to a role group.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-AddressList</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the New-AddressList cmdlet to create address lists and apply them to recipients.</p> <p>In Exchange Online, this cmdlet is available only in the Address Lists role, and by default, the role isn't assigned to any role groups. To use this cmdlet, you need to add the Address Lists role to a role group (for example, to the Organization Management role group). For more information, see Add a role to a role group.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-EmailAddressPolicy</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p>

Cmdlet	Description
	<p>Use the New-EmailAddressPolicy cmdlet to create email address policies. In Exchange Online, email address policies are available only for Microsoft 365 Groups.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-GlobalAddressList</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the New-GlobalAddressList cmdlet to create a global address list (GAL).</p> <p>In Exchange Online, this cmdlet is available only in the Address Lists role, and by default, the role isn't assigned to any role groups. To use this cmdlet, you need to add the Address Lists role to a role group (for example, to the Organization Management role group). For more information, see Add a role to a role group.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-OabVirtualDirectory</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the New-OABVirtualDirectory cmdlet to create offline address book (OAB) virtual directories that are used in Internet Information Services (IIS) on Microsoft Exchange servers. The OAB virtual directory configures the server as a web distribution point for an offline address book (OAB). Typically, you create virtual directories on Exchange servers that have the Client Access server role installed.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-OfflineAddressBook</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the New-OfflineAddressBook cmdlet to create offline address books (OABs).</p> <p>In Exchange Online, this cmdlet is available only in the Address Lists role, and by default, the role isn't assigned to any role groups. To use this cmdlet, you need to add the Address Lists role to a role group (for example, to the Organization Management role group). For more information, see Add a role to a role group.</p>

Cmdlet	Description
	<p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-AddressBookPolicy</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Remove-AddressBookPolicy cmdlet to delete an address book policy. You can't remove the address book policy if it's still assigned to a user's mailbox.</p> <p>In Exchange Online, this cmdlet is available only in the Address Lists role, and by default, the role isn't assigned to any role groups. To use this cmdlet, you need to add the Address Lists role to a role group (for example, to the Organization Management role group). For more information, see Add a role to a role group.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-AddressList</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Remove-AddressList cmdlet to remove existing address lists.</p> <p>In Exchange Online, this cmdlet is available only in the Address Lists role, and by default, the role isn't assigned to any role groups. To use this cmdlet, you need to add the Address Lists role to a role group (for example, to the Organization Management role group). For more information, see Add a role to a role group.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-EmailAddressPolicy</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Remove-EmailAddressPolicy cmdlet to remove existing email address policies and update the affected recipients. In Exchange Online, email address policies are available only for Microsoft 365 Groups.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
Remove-GlobalAddressList	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Remove-GlobalAddressList cmdlet to remove an existing global address list (GAL).</p> <p>In Exchange Online, this cmdlet is available only in the Address Lists role, and by default, the role isn't assigned to any role groups. To use this cmdlet, you need to add the Address Lists role to a role group (for example, to the Organization Management role group). For more information, see Add a role to a role group.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Remove-OabVirtualDirectory	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Remove-OabVirtualDirectory cmdlet to remove offline address book (OAB) virtual directories from Internet Information Services (IIS) on Exchange servers.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Remove-OfflineAddressBook	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Remove-OfflineAddressBook cmdlet to remove (delete) offline address books (OABs).</p> <p>In Exchange Online, this cmdlet is available only in the Address Lists role, and by default, the role isn't assigned to any role groups. To use this cmdlet, you need to add the Address Lists role to a role group (for example, to the Organization Management role group). For more information, see Add a role to a role group.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Restore-DetailsTemplate	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Restore-DetailsTemplate cmdlet to restore the specified template to its default state.</p>

Cmdlet	Description
	<p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-AddressBookPolicy</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Set-AddressBookPolicy cmdlet to change the settings of an address book policy.</p> <p>In Exchange Online, this cmdlet is available only in the Address Lists role, and by default, the role isn't assigned to any role groups. To use this cmdlet, you need to add the Address Lists role to a role group (for example, to the Organization Management role group). For more information, see Add a role to a role group.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-AddressList</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Set-AddressList cmdlet to modify existing address lists.</p> <p>In Exchange Online, this cmdlet is available only in the Address Lists role, and by default, the role isn't assigned to any role groups. To use this cmdlet, you need to add the Address Lists role to a role group (for example, to the Organization Management role group). For more information, see Add a role to a role group.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-DetailsTemplate</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Set-DetailsTemplate cmdlet to modify the attributes of a details template. To make changes to the details template format and layout, you need to use the Details Templates Editor in the Exchange Toolbox.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
Set-EmailAddressPolicy	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Set-EmailAddressPolicy cmdlet to modify email address policies. In Exchange Online, email address policies are available only for Microsoft 365 Groups.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Set-GlobalAddressList	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Set-GlobalAddressList cmdlet to modify an existing global address list (GAL).</p> <p>In Exchange Online, this cmdlet is available only in the Address Lists role, and by default, the role isn't assigned to any role groups. To use this cmdlet, you need to add the Address Lists role to a role group (for example, to the Organization Management role group). For more information, see Add a role to a role group.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Set-OabVirtualDirectory	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Set-OabVirtualDirectory cmdlet to modify offline address book (OAB) virtual directories that are used in Internet Information Services (IIS) on Exchange servers.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Set-OfflineAddressBook	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Set-OfflineAddressBook cmdlet to modify offline address book (OAB) settings.</p> <p>In Exchange Online, this cmdlet is available only in the Address Lists role, and by default, the role isn't assigned to any role groups. To use this cmdlet, you need to</p>

Cmdlet	Description
	<p>add the Address Lists role to a role group (for example, to the Organization Management role group). For more information, see Add a role to a role group.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Update-AddressList	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Update-AddressList cmdlet to update the recipients included in address lists.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Update-EmailAddressPolicy	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Update-EmailAddressPolicy cmdlet to apply new or updated email address policies to the affected recipients in an on-premises Exchange organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Update-GlobalAddressList	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Update-GlobalAddressList cmdlet to update the recipients included in a global address list (GAL).</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Update-OfflineAddressBook	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Update-OfflineAddressBook cmdlet to update the offline address books (OABs) used by Microsoft Outlook clients.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Cmdlet	Description
Enable-ExchangeCertificate	<p>This cmdlet is available only in on-premises Exchange.</p>

Cmdlet	Description
	<p>Use the Enable-ExchangeCertificate cmdlet to enable an existing certificate on the Exchange server for Exchange services such as Internet Information Services (IIS), SMTP, POP, IMAP and Unified Messaging (UM). Once you enable a certificate for a service, you can't disable it.</p> <p>To see the existing certificates that are used for Exchange services, use Get-ExchangeCertificate.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Export-ExchangeCertificate</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Export-ExchangeCertificate cmdlet to export existing certificates and pending certificate requests (also known as certificate signing requests or CSRs) from Exchange servers.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-DataEncryptionPolicy</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Get-DataEncryptionPolicy cmdlet to view data encryption policies in Exchange Online.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
<p>Get-ExchangeCertificate</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Get-ExchangeCertificate cmdlet to view Exchange certificates that are installed on Exchange servers. This cmdlet returns Exchange self-signed certificates, certificates that were issued by a certification authority and pending certificate requests (also known as certificate signing requests or CSRs).</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-IRMConfiguration</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Get-IRMConfiguration cmdlet to view the Information Rights Management (IRM) configuration in your organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-M365DataAtRestEncryptionPolicy</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Get-M365DataAtRestEncryptionPolicy cmdlet to view existing Microsoft 365 data-at-rest encryption policies.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
<p>Get-M365DataAtRestEncryptionPolicyAssignment</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Get-M365DataAtRestEncryptionPolicyAssignment cmdlet to view the currently assigned Microsoft 365 data-at-rest encryption policy.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-MailboxIRMAccess</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Get-MailboxIRMAccess cmdlet to view delegate access to IRM-protected messages in other mailboxes (shared mailboxes or user mailboxes where delegates have Full Access permission).</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-OMEConfiguration</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Get-OMEConfiguration cmdlet to view Microsoft Purview Message Encryption configurations.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-OMEMessageStatus</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Get-OMEMessageStatus cmdlet to view the Microsoft Purview Message Encryption revocation status for a specific message.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-RMSTemplate</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p>

Cmdlet	Description
	<p>Use the Get-RMSTemplate cmdlet to retrieve the current list of active rights policy templates from the Active Directory Rights Management Services (AD RMS) deployment for the organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-SmimeConfig</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Get-SmimeConfig cmdlet to view the S/MIME configuration for Outlook on the web (formerly known as Outlook Web App).</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Import-ExchangeCertificate</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Import-ExchangeCertificate cmdlet to import certificates on Exchange servers. You use this cmdlet to install certificates that were exported from other servers, and to complete pending certification requests (also known as certificate signing requests or CSRs) from certification authorities (CAs).</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-DataEncryptionPolicy</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the New-DataEncryptionPolicy cmdlet to create data encryption policies in Exchange Online.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-ExchangeCertificate</p>	<p>This cmdlet is available only in on-premises Exchange.</p>

Cmdlet	Description
	<p>Use the New-ExchangeCertificate cmdlet to create and renew self-signed certificates, and to create certificate requests (also known as certificate signing requests or CSRs) for new certificates and certificate renewals from a certification authority (CA).</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-M365DataAtRestEncryptionPolicy</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the New-M365DataAtRestEncryptionPolicy cmdlet to create a new Microsoft 365 data-at-rest encryption policy.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-OMEConfiguration</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the New-OMEConfiguration cmdlet to create a Microsoft Purview Message Encryption configuration.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-ExchangeCertificate</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Remove-ExchangeCertificate cmdlet to remove existing Exchange certificates or pending certificate requests (also known as certificate signing requests or CSRs) from Exchange servers.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-MailboxIRMAccess</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Remove-MailboxIRMAccess cmdlet to allow (unblock) delegate access to IRM-protected messages in</p>

Cmdlet	Description
	<p>other mailboxes (shared mailboxes or user mailboxes where delegates have Full Access permission).</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-OMEConfiguration</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Remove-OMEConfiguration cmdlet to remove custom Microsoft Purview Message Encryption configurations. You can't use this cmdlet to remove the default OME configuration.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-DataEncryptionPolicy</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Set-DataEncryptionPolicy cmdlet to modify data encryption policies in Exchange Online.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-IRMConfiguration</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Set-IRMConfiguration cmdlet to configure Information Rights Management (IRM) features on your organization.</p> <p>Configuring and using IRM features in an on-premises Exchange organization requires Active Directory Rights Management Services (AD RMS).</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-M365DataAtRestEncryptionPolicy</p>	<p>This cmdlet is available only in the cloud-based service.</p>

Cmdlet	Description
	<p>Use the Set-M365DataAtRestEncryptionPolicy cmdlet to modify Microsoft 365 data-at-rest encryption policies in Exchange Online.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-M365DataAtRestEncryptionPolicyAssignment</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Set-M365DataAtRestEncryptionPolicyAssignment cmdlet to assign a Microsoft 365 data-at-rest encryption policy at the tenant level.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-MailboxIRMAccess</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Set-MailboxIRMAccess cmdlet to block delegate access to IRM-protected messages in other mailboxes (shared mailboxes or user mailboxes where delegates have Full Access permission).</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-OMEConfiguration</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Set-OMEConfiguration cmdlet to configure Microsoft Purview Message Encryption.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-OMEMessageRevocation</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Set-OMEMessageRevocation cmdlet to revoke Microsoft Purview Message Encryption for a message. Revoking encryption prevents the recipient from viewing the message in the OME portal.</p>

Cmdlet	Description
	<p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-RMSTemplate</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Note</p> <p>This cmdlet is deprecated. If you use AD RMS with Exchange Online, you need to migrate to Azure Information Protection before you can use message encryption. For more information, see Verify that Azure Rights Management is active.</p> <p>Use the Set-RMSTemplate cmdlet to modify the properties of an existing Active Directory Rights Management Services (AD RMS) template in your organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-SmimeConfig</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Set-SmimeConfig cmdlet to modify the S/MIME configuration for Outlook on the web (formerly known as Outlook Web App or OWA) and new Outlook for Windows.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
<p>Test-IRMConfiguration</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Test-IRMConfiguration cmdlet to test Information Rights Management (IRM) configuration and functionality.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Test-M365DataAtRestEncryptionPolicy</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Test-M365DataAtRestEncryptionPolicy cmdlet to test an existing Microsoft 365 data-at-rest encryption policy.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Cmdlet	Description
<p>Add-FederatedDomain</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Add-FederatedDomain cmdlet to configure a secondary domain with the federated organization identifier in the federation trust for the Exchange organization.</p> <p>The domains being added to the federation trust must exist as accepted domains in the Exchange organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
Disable-RemoteMailbox	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Disable-RemoteMailbox cmdlet to remove user mailboxes from the cloud-based service but keep the associated user objects in the on-premises Active Directory.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Enable-RemoteMailbox	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Enable-RemoteMailbox cmdlet to create a mailbox in the cloud-based service for an existing user in the on-premises Active Directory.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Get-FederatedDomainProof	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Get-FederatedDomainProof cmdlet to generate a cryptographically secure string for the domain used for federated sharing in your Exchange organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Get-FederatedOrganizationIdentifier	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Get-FederatedOrganizationIdentifier cmdlet to retrieve the Exchange organization's federated organization identifier and related details, such as federated domains, organization contact and status.</p> <p>For more information, see Federation.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
Get-FederationInformation	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Get-FederationInformation cmdlet to get federation information from an external Exchange organization.</p> <p>Tip</p> <p>For information about changes made to the Get-FederationInformation cmdlet to improve security and privacy, see Important Update to the Get-FederationInformation Cmdlet in Exchange Online.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Get-FederationTrust	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Get-FederationTrust cmdlet to view the federation trust configured for the Exchange organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Get-HybridConfiguration	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Get-HybridConfiguration cmdlet to view the hybrid configuration for the Microsoft Exchange organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Get-HybridMailflowDatacenterIPs	<p>This cmdlet is available only in the cloud-based service.</p> <p>This cmdlet is deprecated and is no longer used.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
Get-IntraOrganizationConfiguration	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Get-IntraOrganizationConfiguration cmdlet to view the component settings of a hybrid Exchange deployment.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Get-IntraOrganizationConnector	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Get-IntraOrganizationConnector cmdlet to view the settings of Intra-Organization connectors.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Get-OnPremisesOrganization	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Get-OnPremisesOrganization cmdlet to retrieve settings for the OnPremisesOrganization object that is created for a hybrid deployment.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Get-PendingFederatedDomain	<p>This cmdlet is available only in on-premises Exchange.</p> <p>The Get-PendingFederatedDomain cmdlet is used by the Exchange admin center to display a list of pending federated domains for the federation trust for your Exchange organization. You shouldn't use this cmdlet to attempt to manually configure a federation trust.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Get-RemoteMailbox	<p>This cmdlet is available only in on-premises Exchange.</p>

Cmdlet	Description
	<p>Use the Get-RemoteMailbox cmdlet to retrieve the mail-related attributes of users in the on-premises organization that have associated mailboxes in the cloud-based service.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-FederationTrust</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the New-FederationTrust cmdlet to set up a federation trust between your Exchange organization and the Microsoft Federation Gateway.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-HybridConfiguration</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the New-HybridConfiguration cmdlet to manually create the HybridConfiguration object and manually set up a hybrid deployment between your on-premises Exchange organization and Exchange Online in Microsoft 365 for enterprises.</p> <p>Note</p> <p>We strongly recommend that you use the Hybrid Configuration wizard to create the HybridConfiguration object and configure your hybrid deployment with Exchange Online.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-IntraOrganizationConnector</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the New-IntraOrganizationConnector cmdlet to create an Intra-Organization connector between two on-premises Exchange forests in an organization, between an Exchange on-premises organization and an Exchange Online organization, or between two Exchange Online organizations. This connector enables feature availability and service</p>

Cmdlet	Description
	<p>connectivity across the organizations using a common connector and connection endpoints.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-OnPremisesOrganization</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the New-OnPremisesOrganization cmdlet to create an OnPremisesOrganization object in a Microsoft 365 organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-RemoteMailbox</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the New-RemoteMailbox cmdlet to create a mail user in the on-premises Active Directory and also create an associated mailbox in the cloud-based service.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-FederatedDomain</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Remove-FederatedDomain cmdlet to remove a federated domain from the federated organization identifier in the federation trust for the Exchange organization.</p> <p>If you remove a domain configured for federated sharing, federated sharing for that domain is disabled.</p> <p>For more information, see Federation.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-FederationTrust</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Remove-FederationTrust cmdlet to remove an existing federation trust from an Exchange organization.</p>

Cmdlet	Description
	<p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-HybridConfiguration</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Remove-HybridConfiguration cmdlet to delete the HybridConfigurationActive Directory object for your on-premises Exchange organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-IntraOrganizationConnector</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Remove-IntraOrganizationConnector cmdlet to remove existing Intra-Organization connectors.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-OnPremisesOrganization</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Remove-OnPremisesOrganization cmdlet to remove an OnPremisesOrganization object in a Microsoft 365 tenant.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
Remove-RemoteMailbox	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Remove-RemoteMailbox cmdlet to remove a mail-enabled user in the on-premises Active Directory and the associated mailbox in the cloud-based service.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Set-FederatedOrganizationIdentifier	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Set-FederatedOrganizationIdentifier cmdlet to configure the federated organization identifier for the Exchange organization.</p> <p>For more details, see Federation.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Set-FederationTrust	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Set-FederationTrust cmdlet to modify an existing federation trust.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Set-HybridConfiguration	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Set-HybridConfiguration cmdlet to modify the hybrid deployment between your on-premises Exchange organization and Exchange Online in Microsoft 365 for enterprises.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Set-IntraOrganizationConnector	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p>

Cmdlet	Description
	<p>Use the Set-IntraOrganizationConnector cmdlet to modify an existing Intra-Organization connector between two on-premises Exchange forests in an organization, between an on-premises Exchange organization and an Exchange Online organization or between two Exchange Online organizations.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-OnPremisesOrganization</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Set-OnPremisesOrganization cmdlet to modify the parameters of the OnPremisesOrganization object on the Microsoft 365 tenant.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-PendingFederatedDomain</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>The Set-PendingFederatedDomain cmdlet is used by the Exchange admin center to configure pending domains with the federated organization identifier in the federation trust for the Exchange organization. You shouldn't use this cmdlet to attempt to manually configure a federation trust.</p> <p>The domains being added to the federation trust must exist as accepted domains in the Exchange organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-RemoteMailbox</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Set-RemoteMailbox cmdlet to modify remote mailboxes. A remote mailbox is a mail user in Active Directory that's associated with a mailbox in the cloud-based service.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
Test-FederationTrust	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Test-FederationTrust cmdlet to verify that the federation trust is properly configured and functioning as expected.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Test-FederationTrustCertificate	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Test-FederationTrustCertificate cmdlet to check the status of certificates that are used for federation on all Exchange servers.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Update-HybridConfiguration	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Update-HybridConfiguration cmdlet to define the credentials that are used to update the hybrid configuration object.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Update-Recipient	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Update-Recipient cmdlet to add Exchange attributes to recipient objects.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Cmdlet	Description
Add-ResubmitRequest	<p>This cmdlet is available only in on-premises Exchange.</p>

Cmdlet	Description
	<p>Use the Add-ResubmitRequest cmdlet to add requests to replay redundant copies of messages from Safety Net after a mailbox database recovery.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Disable-DnssecForVerifiedDomain</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Disable-DnssecForVerifiedDomain cmdlet to disable Domain Name System Security (DNSSEC) for inbound mail to accepted domains in Exchange Online.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Disable-IPv6ForAcceptedDomain</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Disable-IPv6ForAcceptedDomain cmdlet to disable or opt-out of support for mail delivery to accepted domains in Exchange Online using IPv6.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Disable-SmtpDaneInbound</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Disable-SMTPDaneInbound cmdlet to disable SMTP DNS-based Authentication of Named Entities (DANE) for inbound mail to accepted domains in Exchange Online.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Disable-TransportAgent</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Disable-TransportAgent cmdlet to disable a transport agent.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
Enable-DnssecForVerifiedDomain	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Enable-DnssecForVerifiedDomain cmdlet to enable Domain Name System Security (DNSSEC) for inbound mail to accepted domains in Exchange Online.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Enable-IPv6ForAcceptedDomain	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Enable-IPv6ForAcceptedDomain cmdlet to enable support for mail delivery to accepted domains in Exchange Online using IPv6.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Enable-SmtpDaneInbound	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Enable-SMTPDaneInbound cmdlet to enable SMTP DNS-based Authentication of Named Entities (DANE) for inbound mail to accepted domains in Exchange Online.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Enable-TransportAgent	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Enable-TransportAgent cmdlet to enable a transport agent.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Export-Message	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Export-Message cmdlet to copy a message from a queue on a Mailbox server or an Edge Transport server to a specified file path in your organization.</p>

Cmdlet	Description
	<p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-AcceptedDomain</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Get-AcceptedDomain cmdlet to view the configuration information for the accepted domains in your organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-AddressRewriteEntry</p>	<p>This cmdlet is available or effective only on Edge Transport servers in on-premises Exchange.</p> <p>Use the Get-AddressRewriteEntry cmdlet to view an existing address rewrite entry that rewrites sender and recipient email addresses in messages sent to or sent from your organization through an Edge Transport server.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-DeliveryAgentConnector</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Get-DeliveryAgentConnector cmdlet to retrieve information about a specific delivery agent connector in your organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
Get-DnssecStatusForVerifiedDomain	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Get-DnssecStatusForVerifiedDomain cmdlet to view information about Domain Name System Security (DNSSEC) for accepted domains in Exchange Online.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Get-EdgeSubscription	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Get-EdgeSubscription cmdlet to retrieve information about Edge Subscriptions in your organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Get-EdgeSyncServiceConfig	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Get-EdgeSyncServiceConfig cmdlet to retrieve the edge synchronization services settings that control the general synchronization behavior shared by all Microsoft Exchange EdgeSync services.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Get-ForeignConnector	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Get-ForeignConnector cmdlet to view the configuration information for a Foreign connector in the Transport service of a Mailbox server.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Get-FrontendTransportService	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Get-FrontEndTransportService cmdlet to view the configuration of the Front End Transport service on Exchange 2013 or later servers that have the Client Access server role installed.</p>

Cmdlet	Description
	<p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-InboundConnector</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Get-InboundConnector cmdlet to view the settings for an Inbound connector in your cloud-based organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-IPv6StatusForAcceptedDomain</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Get-IPv6StatusForAcceptedDomain cmdlet to view the status of support for mail delivery to accepted domains in Exchange Online using IPv6.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-MailboxTransportService</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Get-MailboxTransportService cmdlet to view the configuration of the Mailbox Transport service on Exchange 2013 or later Mailbox servers.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-Message</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Get-Message cmdlet to view the details of one or more messages in queues on Mailbox servers or Edge Transport servers.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-MessageTrace</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Note</p>

Cmdlet	Description
	<p>This cmdlet is replaced by the Get-MessageTraceV2 cmdlet and will eventually be deprecated.</p> <p>Use the Get-MessageTrace cmdlet to trace messages as they pass through the cloud-based organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-MessageTraceDetail</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Note</p> <p>This cmdlet is replaced by the Get-MessageTraceDetailV2 cmdlet and will eventually be deprecated.</p> <p>Use the Get-MessageTraceDetail cmdlet to view the message trace event details for a specific message. These detailed results are returned less quickly than the Get-MessageTrace results.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-MessageTrackingLog</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Get-MessageTrackingLog cmdlet to search for message delivery information stored in the message tracking log.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
Get-MessageTrackingReport	<p>This cmdlet is functional only in on-premises Exchange.</p> <p>Use the Get-MessageTrackingReport cmdlet to return data for a specific message tracking report. This cmdlet is used by the delivery reports feature.</p> <p>In Exchange Online, delivery reports are replaced by message trace (the Get-MessageTraceV2 and Get-MessageTraceDetailV2 cmdlets).</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Get-NetworkConnectionInfo	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Get-NetworkConnectionInfo cmdlet to view the network configuration information for all network adapters configured on the local server.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Get-OutboundConnector	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Get-OutboundConnector cmdlet to view the configuration information for an Outbound connector in your cloud-based organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Get-Queue	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Get-Queue cmdlet to view configuration information for queues on Mailbox servers or Edge Transport servers.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Get-QueueDigest	<p>This cmdlet is available only in on-premises Exchange.</p>

Cmdlet	Description
	<p>Use the Get-QueueDigest cmdlet to view information about message delivery queues across database availability groups (DAGs) Active Directory sites, or Active Directory forests in your organization.</p> <p>By default, the Get-QueueDigest cmdlet displays delivery queues that contain ten or more messages, and the results are between one and two minutes old. For instructions on how to change these default values, see Configure Get-QueueDigest.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-ReceiveConnector</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Get-ReceiveConnector cmdlet to view Receive connectors on Mailbox servers and Edge Transport servers. Receive connectors listen for inbound SMTP connections on the Exchange server.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-RemoteDomain</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Get-RemoteDomain cmdlet to view the configuration information for the remote domains configured in your organization. You can view the remote domain configuration from inside the Exchange organization or from an Edge Transport server in the perimeter network.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
Get-ResubmitRequest	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Get-ResubmitRequest cmdlet to view requests to replay redundant copies of messages from Safety Net after a mailbox database recovery.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Get-RoutingGroupConnector	<p>This cmdlet is available only in Exchange Server 2010.</p> <p>Use the Get-RoutingGroupConnector cmdlet to view the configuration details of the routing group connectors in a Microsoft Exchange Server 2010 organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Get-SendConnector	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Get-SendConnector cmdlet to view the settings for a Send connector.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Get-SmtpDaneInboundStatus	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Get-SmtpDaneInboundStatus cmdlet to view information about SMTP DNS-based Authentication of Named Entities (DANE) for inbound mail to accepted domains in Exchange Online.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Get-SystemMessage	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Get-SystemMessage cmdlet to view default or custom system messages. System messages are delivery status notifications (also known</p>

Cmdlet	Description
	<p>as DSNs, non-delivery reports, NDRs or bounce messages) and quota messages.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-TransportAgent</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Get-TransportAgent cmdlet to view the configuration of a transport agent.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-TransportConfig</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Get-TransportConfig cmdlet to view organization-wide transport configuration settings.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-TransportPipeline</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Get-TransportPipeline cmdlet to view transport agents and the SMTP event where the transport agent is registered.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-TransportServer</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Get-TransportServer cmdlet to view settings that are associated with the Hub Transport server role or the Edge Transport server role.</p> <p>Note: In Exchange 2013 or later, use the Get-TransportService cmdlet instead. If you have scripts that use Get-TransportServer, update them to use Get-TransportService.</p>

Cmdlet	Description
	<p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-TransportService</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Get-TransportService cmdlet to view the settings of the Transport service on Exchange 2013 or later Mailbox servers or Edge Transport servers.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-X400AuthoritativeDomain</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Get-X400AuthoritativeDomain cmdlet to view the configuration information for the X.400 authoritative domains configured in your organization. For more information about how to configure an X.400 authoritative domain, see Set-X400AuthoritativeDomain.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Install-TransportAgent</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Install-TransportAgent cmdlet to register transport agents on Exchange servers.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-AcceptedDomain</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the New-AcceptedDomain cmdlet to create an accepted domain in your organization. An accepted domain is any SMTP namespace for which an Exchange organization sends and receives email.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
New-AddressRewriteEntry	<p>This cmdlet is available or effective only on Edge Transport servers in on-premises Exchange.</p> <p>Use the New-AddressRewriteEntry cmdlet to create an address rewrite entry that rewrites sender and recipient email addresses in messages sent to or sent from your organization through an Edge Transport server.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
New-DeliveryAgentConnector	<p>This cmdlet is available only in on-premises Exchange.</p> <p>The New-DeliveryAgentConnector cmdlet creates a delivery agent connector in your organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
New-EdgeSubscription	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the New-EdgeSubscription cmdlet to export an Edge Subscription file from an Edge Transport server and to import the Edge Subscription file to a Mailbox server.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
New-EdgeSyncServiceConfig	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the New-EdgeSyncServiceConfig cmdlet to create edge synchronization service settings that control the general synchronization behavior shared by all EdgeSync services.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
New-ForeignConnector	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the New-ForeignConnector cmdlet to create a new Foreign connector in the Transport service of a Mailbox server.</p>

Cmdlet	Description
	<p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-InboundConnector</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the New-InboundConnector cmdlet to create a new Inbound connector in your cloud-based organization.</p> <p>Note: Creation of inbound connectors is restricted in Microsoft 365 E5 developer subscriptions. Opening a support ticket in affected organizations won't help.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-OutboundConnector</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the New-OutboundConnector cmdlet to create a new Outbound connector in your cloud-based organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-ReceiveConnector</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the New-ReceiveConnector cmdlet to create Receive connectors on Mailbox servers and Edge Transport servers. Receive connectors listen for inbound SMTP connections on the Exchange server.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-RemoteDomain</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the New-RemoteDomain cmdlet to create a managed connection for a remote domain. When you create a remote domain, you can control mail flow with more precision, apply message formatting and messaging</p>

Cmdlet	Description
	<p>policies and specify acceptable character sets for messages sent to and received from the remote domain.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-RoutingGroupConnector</p>	<p>This cmdlet is available only in Exchange Server 2010.</p> <p>Use the New-RoutingGroupConnector cmdlet to establish a connection between a Microsoft Exchange Server 2010 routing group and an Exchange Server 2003 routing group when the organization is running more than one version of Exchange.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-SendConnector</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the New-SendConnector cmdlet to create a new Send connector.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-SystemMessage</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the New-SystemMessage cmdlet to create custom system messages. System messages are delivery status notifications (also known as DSNs, non-delivery reports, NDRs or bounce messages) and quota messages.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
New-X400AuthoritativeDomain	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the New-X400AuthoritativeDomain cmdlet to create and specify the X.400 authoritative domain for the organization. The X.400 authoritative domain defines the standard fields for the namespace appended to the recipient identity for all mailboxes assigned an X.400 address.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Redirect-Message	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Redirect-Message cmdlet to drain the active messages from all the delivery queues on a Mailbox server, and transfer those messages to another Mailbox server.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Remove-AcceptedDomain	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Remove-AcceptedDomain cmdlet to remove an accepted domain. When you remove an accepted domain, the accepted domain object is deleted.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Remove-AddressRewriteEntry	<p>This cmdlet is available or effective only on Edge Transport servers in on-premises Exchange.</p> <p>Use the Remove-AddressRewriteEntry cmdlet to remove an existing address rewrite entry that's no longer needed on an Edge Transport server.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Remove-DeliveryAgentConnector	<p>This cmdlet is available only in on-premises Exchange.</p>

Cmdlet	Description
	<p>The Remove-DeliveryAgentConnector cmdlet removes a specific delivery agent connector configured in your organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-EdgeSubscription</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Remove-EdgeSubscription cmdlet to remove Edge Subscription from the Exchange organization and from the subscribed Edge Transport server.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-ForeignConnector</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Remove-ForeignConnector cmdlet to delete a Foreign connector in the Transport service of a Mailbox server.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-InboundConnector</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Remove-InboundConnector cmdlet to delete an Inbound connector from your cloud-based organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-Message</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Remove-Message cmdlet to delete a message from a queue on a Mailbox server or an Edge Transport server.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-OutboundConnector</p>	<p>This cmdlet is available only in the cloud-based service.</p>

Cmdlet	Description
	<p>Use the Remove-OutboundConnector cmdlet to delete an Outbound connector from your cloud-based organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-ReceiveConnector</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Remove-ReceiveConnector cmdlet to remove Receive connectors from Mailbox servers and Edge Transport servers.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-RemoteDomain</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Remove-RemoteDomain cmdlet to remove a remote domain. When you remove a remote domain, the remote domain object is deleted. Removing a remote domain doesn't disable mail flow to that domain.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-ResubmitRequest</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Remove-ResubmitRequest cmdlet to remove requests to replay redundant copies of messages from Safety Net after a mailbox database recovery.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-RoutingGroupConnector</p>	<p>This cmdlet is available only in Exchange Server 2010.</p> <p>Use the Remove-RoutingGroupConnector cmdlet to remove a routing group connector between a Microsoft Exchange Server 2010 routing group and an Exchange Server 2003 routing group.</p>

Cmdlet	Description
	<p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-SendConnector</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Remove-SendConnector cmdlet to delete a Send connector.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-SystemMessage</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Remove-SystemMessage cmdlet to remove custom system messages. System messages are delivery status notifications (also known as DSNs, non-delivery reports, NDRs or bounce messages) and quota messages.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-X400AuthoritativeDomain</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Remove-X400AuthoritativeDomain cmdlet to remove an X.400 authoritative domain. When you remove an X.400 authoritative domain, the X.400 authoritative domain object is deleted from Active Directory.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Resume-Message</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Resume-Message cmdlet to enable delivery of a previously suspended message in a queue on a Mailbox server or Edge Transport server.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Resume-Queue</p>	<p>This cmdlet is available only in on-premises Exchange.</p>

Cmdlet	Description
	<p>Use the Resume-Queue cmdlet to restart processing for a suspended queue on a Mailbox server or an Edge Transport server.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Retry-Queue</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Retry-Queue cmdlet to force a connection attempt for a queue on a Mailbox server or an Edge Transport server.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Search-MessageTrackingReport</p>	<p>This cmdlet is functional only in on-premises Exchange.</p> <p>Use the Search-MessageTrackingReport cmdlet to find the unique message tracking report based on the search criteria provided. You can then pass this message tracking report ID to the Get-MessageTrackingReport cmdlet to get full message tracking information. For more information, see Get-MessageTrackingReport. The message tracking report cmdlets are used by the delivery reports feature.</p> <p>In Exchange Online, delivery reports are replaced by message trace (the Get-MessageTraceV2 and Get-MessageTraceDetailV2 cmdlets).</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-AcceptedDomain</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Set-AcceptedDomain cmdlet to modify existing accepted domains in your organization. An accepted domain is any SMTP namespace for which an Exchange organization sends and receives email.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
Set-AddressRewriteEntry	<p>This cmdlet is available or effective only on Edge Transport servers in on-premises Exchange.</p> <p>Use the Set-AddressRewriteEntry cmdlet to modify an existing address rewrite entry that rewrites sender and recipient email addresses in messages sent to or sent from your organization through an Edge Transport server.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Set-DeliveryAgentConnector	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Set-DeliveryAgentConnector cmdlet to configure a specific delivery agent connector in your organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Set-EdgeSyncServiceConfig	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Set-EdgeSyncServiceConfig cmdlet to modify the configuration of edge synchronization service settings that control the general synchronization behavior shared by all EdgeSync services.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Set-ForeignConnector	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Set-ForeignConnector cmdlet to modify an existing Foreign connector in the Transport service of a Mailbox server.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Set-FrontendTransportService	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Get-FrontEndTransportService cmdlet to modify the configuration of the Front End Transport service on Exchange 2013 or</p>

Cmdlet	Description
	<p>later servers that have the Client Access server role installed.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-InboundConnector</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Set-InboundConnector cmdlet to change an existing Inbound connector in your cloud-based organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-MailboxTransportService</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Set-MailboxTransportService cmdlet to modify the configuration of the Mailbox Transport service on Exchange 2013 or later Mailbox servers.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-OutboundConnector</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Set-OutboundConnector cmdlet to modify an existing Outbound connector in your cloud-based organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-ReceiveConnector</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Set-ReceiveConnector cmdlet to modify Receive connectors on Mailbox servers and Edge Transport servers.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-RemoteDomain</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one</p>

Cmdlet	Description
	<p>environment or the other.</p> <p>Use the Set-RemoteDomain cmdlet to configure a managed connection for a remote domain.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Set-ResubmitRequest	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Set-ResubmitRequest cmdlet to enable or disable requests to replay redundant copies of messages from Safety Net after a mailbox database recovery.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Set-RoutingGroupConnector	<p>This cmdlet is available only in Exchange Server 2010.</p> <p>Use the Set-RoutingGroupConnector cmdlet to modify the properties of an existing routing group connector between a Microsoft Exchange Server 2010 routing group and an Exchange Server 2003 routing group. You can also use this cmdlet to configure the maximum message size that can pass across a routing group connector.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Set-SendConnector	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Set-SendConnector cmdlet to modify a Send connector.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Set-SystemMessage	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Set-SystemMessage cmdlet to modify custom system messages. System messages are delivery status notifications (also known as DSNs, non-delivery reports, NDRs or bounce messages) and quota messages.</p>

Cmdlet	Description
	<p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-TransportAgent</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Set-TransportAgent cmdlet to modify existing transport agents.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-TransportConfig</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Set-TransportConfig cmdlet to modify the transport configuration settings for the whole Exchange organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-TransportServer</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Set-TransportServer cmdlet to modify settings that are associated with the Hub Transport server role or the Edge Transport server role.</p> <p>Note: In Exchange 2013 or later, use the Set-TransportService cmdlet instead. If you have scripts that use Set-TransportServer, update them to use Set-TransportService.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-TransportService</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Set-TransportService cmdlet to modify the settings of the Transport service on Exchange 2013 or later Mailbox servers or Edge Transport servers.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
Set-X400AuthoritativeDomain	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Set-X400AuthoritativeDomain cmdlet to edit an existing X.400 authoritative domain for your organization. The X.400 authoritative domain defines the standard fields for the namespace appended to the recipient identity for all mailboxes assigned an X.400 address.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Start-EdgeSynchronization	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Start-EdgeSynchronization cmdlet to immediately start synchronization of configuration data from Active Directory to the subscribed Edge Transport servers.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Start-HistoricalSearch	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Start-HistoricalSearch cmdlet to start a new historical search.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Stop-HistoricalSearch	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Stop-HistoricalSearch cmdlet to stop an existing historical search that has a status value of NotStarted.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Suspend-Message	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Suspend-Message cmdlet to prevent delivery of a particular message in a queue on a Mailbox server or an Edge Transport server.</p>

Cmdlet	Description
	<p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Suspend-Queue</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Suspend-Queue cmdlet to stop processing for a queue on a Mailbox server or an Edge Transport server.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Test-EdgeSynchronization</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Test-EdgeSynchronization cmdlet to diagnose whether the subscribed Edge Transport servers have a current and accurate synchronization status.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Test-Mailflow</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Test-Mailflow cmdlet to diagnose whether mail can be successfully sent from and delivered to the system mailbox on a Mailbox server. You can also use this cmdlet to verify that email is sent between Mailbox servers within a defined latency threshold.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Test-SmtpConnectivity</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Test-SmtpConnectivity cmdlet to diagnose whether an SMTP connection can successfully be established to the Receive connectors on a specific server. Although you can run this cmdlet manually to verify SMTP connectivity for a specified server, it's primarily used by Microsoft System Center Operations Manager 2007 to test your transport servers' ability to receive SMTP connections to each of the bindings on all the Receive connectors on those servers.</p>

Cmdlet	Description
	<p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Uninstall-TransportAgent</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Uninstall-TransportAgent cmdlet to unregister transport agents from Exchange servers.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Validate-OutboundConnector</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Validate-OutboundConnector cmdlet to test the settings of Outbound connectors in Microsoft 365.</p> <p>Note: This cmdlet does not set the validation status or timestamp on the connector. To set these values, run the following command: <code>Set-OutboundConnector -Identity "<ConnectorName>" -IsValidated \$true -LastValidationTimestamp (Get-Date).ToUniversalTime() .</code></p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Cmdlet	Description
<p>Clean-MailboxDatabase</p>	<p>This cmdlet is available only in Exchange Server 2010.</p> <p>Use the Clean-MailboxDatabase cmdlet to scan Active Directory for disconnected mailboxes that aren't yet marked as disconnected in the Microsoft Exchange store and update the status of those mailboxes in the Exchange store. This cmdlet isn't able to update the Exchange store unless the Microsoft Exchange Information Store service is running and the database is mounted.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Disable-MailboxQuarantine</p>	<p>This cmdlet is available only in on-premises Exchange.</p>

Cmdlet	Description
	<p>Use the Disable-MailboxQuarantine cmdlet to release quarantined mailboxes.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Disable-MetaCacheDatabase</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Disable-MetaCacheDatabase cmdlet to disable the metacache database on Exchange 2019 Mailbox servers. The metacache database stores mailbox database indexes and secondary copies of metadata on solid state drives (SSDs) to improve search latency and user logons.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Dismount-Database</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Dismount-Database cmdlet to dismount databases. You can run this command only if the Microsoft Exchange Information Store service is running.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Enable-MailboxQuarantine</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Enable-MailboxQuarantine cmdlet to quarantine mailboxes that affect the availability of the mailbox database.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Enable-MetaCacheDatabase</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Enable-MetaCacheDatabase cmdlet to enable the metacache database on Exchange 2019 Mailbox servers. The metacache database stores mailbox database indexes and secondary copies of metadata on solid state drives (SSDs) to improve search latency and user logons.</p>

Cmdlet	Description
	<p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-FailedContentIndexDocuments</p>	<p>This cmdlet is available only in Exchange Server 2016 or earlier.</p> <p>Use the Get-FailedContentIndexDocuments cmdlet to retrieve a list of documents for a mailbox, mailbox database, or Mailbox server that couldn't be indexed by Exchange Search.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-MailboxDatabase</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Get-MailboxDatabase cmdlet to retrieve one or more mailbox database objects from a server or organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-MailboxRepairRequest</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Get-MailboxRepairRequest cmdlet to display information about current mailbox repair requests. Mailbox repair requests are created using the New-MailboxRepairRequest cmdlet to detect and fix mailbox corruptions.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-MailboxServer</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Get-MailboxServer cmdlet to view information about Mailbox servers in your organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-SearchDocumentFormat</p>	<p>This cmdlet is available only in on-premises Exchange.</p>

Cmdlet	Description
	<p>Use the Get-SearchDocumentFormat cmdlet to retrieve details of file formats supported by Exchange Search.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-StoreUsageStatistics</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Get-StoreUsageStatistics cmdlet to aid in diagnosing performance issues with your servers or databases.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Mount-Database</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Mount-Database cmdlet to mount mailbox databases on Exchange servers. The cmdlet mounts the database only if the Microsoft Exchange Information Store service and the Microsoft Exchange Replication service are running.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Move-DatabasePath</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Move-DatabasePath cmdlet to set a new path to the location of a database on the specified Mailbox server and to move the related files to that location.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
New-MailboxDatabase	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the New-MailboxDatabase cmdlet to create a mailbox database, or a recovery database. Each database you create must have a unique name in the organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
New-MailboxRepairRequest	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the New-MailboxRepairRequest cmdlet to detect and fix mailbox corruption issues.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
New-SearchDocumentFormat	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the New-SearchDocumentFormat cmdlet to add a format-specific filter to those used by Exchange search.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Remove-MailboxDatabase	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Remove-MailboxDatabase cmdlet to delete a mailbox database object.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Remove-MailboxRepairRequest	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Remove-MailboxRepairRequest cmdlet to remove mailbox repair requests from a mailbox database that were created using the New-MailboxRepairRequest cmdlet.</p>

Cmdlet	Description
	<p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-SearchDocumentFormat</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Remove-SearchDocumentFormat cmdlet to remove a format-specific filter from those used by Exchange search. Only filters added with New-SearchDocumentFormat can be removed.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-StoreMailbox</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Remove-StoreMailbox cmdlet to purge the mailbox and all of its message content from the mailbox database. This results in permanent data loss for the mailbox being purged. You can only run this cmdlet against disconnected or soft-deleted mailboxes. Running this command against an active mailbox fails, and you receive an error.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-MailboxDatabase</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Set-MailboxDatabase cmdlet to configure a variety of properties for a mailbox database.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-MailboxServer</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Set-MailboxServer cmdlet to modify the mailbox configuration settings and attributes of Mailbox servers.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
Set-SearchDocumentFormat	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Set-SearchDocumentFormat cmdlet to enable or disable the file format for Exchange Search.</p> <p>When you disable a file format for content indexing by Exchange Search, contents of the file become unsearchable by Exchange Search clients such as Outlook on the web, Microsoft Outlook in online mode and In-Place eDiscovery.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Start-MailboxAssistant	<p>This cmdlet is available only in Exchange Server 2019 in Cumulative Update 11 (CU11) or later.</p> <p>Use the Start-MailboxAssistant cmdlet to start processing of a mailbox by the specified assistant.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Test-AssistantHealth	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Test-AssistantHealth cmdlet to verify that the Microsoft Exchange Mailbox Assistants service (MSEExchangeMailboxAssistants) is healthy, to recover from health issues, and to report the status of the diagnosis or recovery action.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Test-ExchangeSearch	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Test-ExchangeSearch cmdlet to test that Exchange Search is currently enabled and is indexing new email messages in a timely manner.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
Test-MRSHealth	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Test-MRSHealth cmdlet to test the health of an instance of the Microsoft Exchange Mailbox Replication service.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Update-DatabaseSchema	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Update-DatabaseSchema cmdlet to upgrade the database schema for one or more databases after an Exchange software update that includes database schema updates is installed on Mailbox servers in a database availability group (DAG). Some software updates for Exchange might include database schema updates. After such an update is installed on all members of a DAG, the administrator must run the Update-DatabaseSchema cmdlet for each database in the DAG and dismount/mount or failover the database to trigger the database schema update. The in-place database schema upgrade engine ensures that no schema updates occur until all members of the DAG have compatible versions of the software.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Update-FileDistributionService	<p>This cmdlet is available only in Exchange Server 2010.</p> <p>Use the Update-FileDistributionService cmdlet to access the Microsoft Exchange File Distribution service to poll for offline address book (OAB), Group Metrics, and Unified Messaging (UM) configuration and data.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Update-StoreMailboxState	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Update-StoreMailboxState cmdlet to synchronize the mailbox state for a mailbox in the Exchange mailbox store with the state of the corresponding Active Directory user account.</p>

Cmdlet	Description
	<p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Cmdlet	Description
<p>Add-MailboxFolderPermission</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Add-MailboxFolderPermission cmdlet to add folder-level permissions for users in mailboxes.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Add-MailboxPermission</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Add-MailboxPermission cmdlet to add permissions to a mailbox or to an Exchange Server 2016, Exchange Server 2019, or Exchange Online mail user.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Add-RecipientPermission</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Add-RecipientPermission cmdlet to add SendAs permission to users in a cloud-based organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
<p>Connect-Mailbox</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Connect-Mailbox cmdlet to connect disconnected mailboxes to existing user accounts that don't already have mailboxes.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Disable-App</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Disable-App cmdlet to disable (turn off) a specific app for a specific user.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Disable-InboxRule</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Disable-InboxRule cmdlet to disable existing Inbox rules in mailboxes.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
Disable-Mailbox	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Disable-Mailbox cmdlet to disable the mailbox of existing users who already have mailboxes. For this cmdlet, a user could also be a public folder mailbox or an InetOrgPerson object. The user account that's associated with the mailbox remains, but it's no longer associated with a mailbox.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Disable-ServiceEmailChannel	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Disable-ServiceEmailChannel cmdlet to disable the .NET service channel for a specific user. The .NET service channel enables Microsoft Exchange to store information that it later forwards to applications or devices that aren't permanently connected to the server running Exchange.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Disable-SweepRule	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Disable-SweepRule cmdlet to disable Sweep rules in mailboxes.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Enable-App	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Enable-App cmdlet to enable (turn on) a specific app for a specific user.</p>

Cmdlet	Description
	<p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Enable-InboxRule</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Enable-InboxRule cmdlet to enable an Inbox rule. Inbox rules are used to process messages in the Inbox based on conditions specified and take actions such as moving a message to a specified folder or deleting a message.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Enable-Mailbox</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Enable-Mailbox cmdlet to create mailboxes for existing users who don't already have mailboxes. You can also use this cmdlet to create In-Place archives for existing mailboxes.</p> <p>Note: In Exchange Online, you use this cmdlet to add archive mailboxes for existing users and to enable auto-expanding archives. To add a mailbox for an existing Microsoft Entra account, you need to add a license to the account as described in Assign licenses to user accounts.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Enable-ServiceEmailChannel</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Enable-ServiceEmailChannel cmdlet to enable the .NET service channel for a specific user.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
Enable-SweepRule	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Enable-SweepRule cmdlet to enable Sweep rules in mailboxes.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Expedite-Delicensing	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Expedite-Delicensing cmdlet to end the delay for removing mailbox licenses from users. After you remove the delay, the licenses are removed from mailboxes within 24 hours. You configure delayed mailbox license removal using the DelayedDelicensingEnabled parameter on the Set-OrganizationConfig cmdlet.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Export-MailboxDiagnosticLogs	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Export-MailboxDiagnosticLogs cmdlet to export diagnostic data from user and system mailboxes in your organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Export-RecipientDataProperty	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Export-RecipientDataProperty cmdlet to download the picture or spoken name audio file of a mailbox or mail contact.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
Get-App	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Get-App cmdlet to view installed apps.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Get-CalendarDiagnosticAnalysis	<p>Although this cmdlet is available in on-premises Exchange and in the cloud-based service, it only works in on-premises Exchange.</p> <p>Use the Get-CalendarDiagnosticAnalysis cmdlet to troubleshoot calendar-related reliability issues. You can use this cmdlet to analyze calendar item data that's recorded in the Calendar Diagnostic logs. You provide the calendar item data to this cmdlet by using the Get-CalendarDiagnosticLog cmdlet.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Get-CalendarDiagnosticLog	<p>Although this cmdlet is available in on-premises Exchange and in the cloud-based service, it only works in on-premises Exchange. In cloud-based service, use the Get-CalendarDiagnosticObjects cmdlet instead.</p> <p>Use the Get-CalendarDiagnosticLog cmdlet to collect a range of calendar logs. The Calendar Diagnostic logs track all calendar items and meeting requests in mailboxes. You can use this information to troubleshoot calendar issues that occur in mailboxes.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Get-CalendarDiagnosticObjects	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Get-CalendarDiagnosticObjects cmdlet to collect a range of calendar logs. The calendar diagnostic logs track important calendar-related event data for each mailbox, and can be used to troubleshoot calendar issues that occur in mailboxes. The logs track all calendar items and meeting messages.</p>

Cmdlet	Description
	<p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-CalendarNotification</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Get-CalendarNotification cmdlet to view calendar text message notification settings for a mailbox.</p> <p>Note: This cmdlet is deprecated in Exchange Online PowerShell. The text message notification service is discontinued in Microsoft 365.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-CalendarProcessing</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Get-CalendarProcessing cmdlet to view the calendar processing options for resource mailboxes, which include the Calendar Attendant, resource booking assistant and calendar configuration. The settings returned by this cmdlet are editable only on resource mailboxes.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-Clutter</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Get-Clutter cmdlet to view Clutter settings for mailboxes in your organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-EventsFromEmailConfiguration</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Get-EventsFromEmailConfiguration cmdlet to view the events from email settings on a mailbox. These settings define whether Outlook or Outlook on the web (formerly known as Outlook Web App)</p>

Cmdlet	Description
	<p>automatically discovers events from email messages and adds them to the user's calendar.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-ExternalInOutlook</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Get-ExternalInOutlook cmdlet to view the configuration of external sender identification that's available in Outlook, Outlook for Mac, Outlook on the web, and Outlook for iOS and Android.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-FocusedInbox</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Get-FocusedInbox cmdlet to view the Focused Inbox configuration for mailboxes in your organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-InboxRule</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Get-InboxRule cmdlet to view Inbox rule properties. Inbox rules are used to process messages in the Inbox based on conditions specified and take actions such as moving a message to a specified folder or deleting a message.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-Mailbox</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p>

Cmdlet	Description
	<p>Use the Get-Mailbox cmdlet to view mailbox objects and attributes, populate property pages, or supply mailbox information to other tasks.</p> <p>Note: In Exchange Online PowerShell, we recommend that you use the Get-EXOMailbox cmdlet instead of this cmdlet. For more information, see Connect to Exchange Online PowerShell.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-MailboxAutoReplyConfiguration</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Get-MailboxAutoReplyConfiguration cmdlet to retrieve Automatic Replies settings for a specific mailbox.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-MailboxCalendarFolder</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Get-MailboxCalendarFolder cmdlet to retrieve the publishing or sharing settings for a specified mailbox calendar folder.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-MailboxExportRequest</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Get-MailboxExportRequest cmdlet to view the detailed status of an ongoing export request that was initiated by using the New-MailboxExportRequest cmdlet.</p> <p>This cmdlet is available only in the Mailbox Import Export role, and by default, the role isn't assigned to any role groups. To use this cmdlet, you need to add the Mailbox Import Export role to a role group (for example, to the Organization Management role group). For more information, see Add a role to a role group.</p>

Cmdlet	Description
	<p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-MailboxExportRequestStatistics</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Get-MailboxExportRequestStatistics cmdlet to view detailed information about export requests.</p> <p>This cmdlet is available only in the Mailbox Import Export role, and by default, the role isn't assigned to any role groups. To use this cmdlet, you need to add the Mailbox Import Export role to a role group (for example, to the Organization Management role group). For more information, see Add a role to a role group.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-MailboxFolder</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Get-MailboxFolder cmdlet to view folders in your own mailbox. Administrators can't use this cmdlet to view folders in other mailboxes (the cmdlet is available only from the MyBaseOptions user role).</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
Get-MailboxFolderPermission	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Get-MailboxFolderPermission cmdlet to view folder-level permissions in mailboxes.</p> <p>Note: In Exchange Online PowerShell, we recommend that you use the Get-EXOMailboxFolderPermission cmdlet instead of this cmdlet. For more information, see Connect to Exchange Online PowerShell.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Get-MailboxFolderStatistics	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Get-MailboxFolderStatistics cmdlet to retrieve information about the folders in a specified mailbox, including the number and size of items in the folder, the folder name and ID, and other information.</p> <p>Note: In Exchange Online PowerShell, we recommend that you use the Get-EXOMailboxFolderStatistics cmdlet instead of this cmdlet. For more information, see Connect to Exchange Online PowerShell.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Get-MailboxImportRequest	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Get-MailboxImportRequest cmdlet to view the detailed status of an ongoing import request that was initiated using the New-MailboxImportRequest cmdlet.</p> <p>This cmdlet is available only in the Mailbox Import Export role, and by default, the role isn't assigned to any role groups. To use this cmdlet, you need to add the Mailbox Import Export role to a role group (for example,</p>

Cmdlet	Description
	<p>to the Organization Management role group). For more information, see Add a role to a role group.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-MailboxImportRequestStatistics</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Get-MailboxImportRequestStatistics cmdlet to view detailed information about import requests.</p> <p>This cmdlet is available only in the Mailbox Import Export role, and by default, the role isn't assigned to any role groups. To use this cmdlet, you need to add the Mailbox Import Export role to a role group (for example, to the Organization Management role group). For more information, see Add a role to a role group.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-MailboxLocation</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Get-MailboxLocation cmdlet to view mailbox location information in Exchange Online.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-MailboxPermission</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Get-MailboxPermission cmdlet to retrieve permissions on a mailbox.</p> <p>Note: In Exchange Online PowerShell, we recommend that you use the Get-EXOMailboxPermission cmdlet instead of this cmdlet. For more</p>

Cmdlet	Description
	<p>information, see Connect to Exchange Online PowerShell.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-MailboxPlan</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Get-MailboxPlan cmdlet to view information about mailbox plans in the cloud-based service.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-MailboxRestoreRequest</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Get-MailboxRestoreRequest cmdlet to view detailed status of an ongoing restore request that was initiated by using the New-MailboxRestoreRequest cmdlet.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-MailboxRestoreRequestStatistics</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Get-MailboxRestoreRequestStatistics cmdlet to view detailed information about restore requests.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
Get-MailboxSentItemsConfiguration	<p>This cmdlet is available only in Exchange Server 2010.</p> <p>Use the Get-MailboxSentItemsConfiguration cmdlet to view the Sent Items settings on mailboxes.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Get-MailboxStatistics	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Get-MailboxStatistics cmdlet to return information about a mailbox, such as the size of the mailbox, the number of messages it contains, and the last time it was accessed. In addition, you can get the move history or a move report of a completed move request.</p> <p>Note: In Exchange Online PowerShell, we recommend that you use the Get-EXOMailboxStatistics cmdlet instead of this cmdlet. For more information, see Connect to Exchange Online PowerShell.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Get-MailboxUserConfiguration	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Get-MailboxUserConfiguration cmdlet to view user configuration items in mailboxes.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Get-MessageCategory	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Get-MessageCategory cmdlet to retrieve a message category from the specified mailbox.</p>

Cmdlet	Description
	<p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-PendingDelicenseUser</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Get-PendingDelicenseUser cmdlet to view information about mailboxes that have delayed mailbox license removal requests. You configure delayed mailbox license removal using the DelayedDelicensingEnabled parameter on the Set-OrganizationConfig cmdlet.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-Place</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Get-Place cmdlet to view the additional metadata that was configured on room mailboxes by using the Set-Place cmdlet. The additional metadata provides a better search and room suggestion experience.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-RecipientPermission</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Get-RecipientPermission cmdlet to view information about SendAs permissions that are configured for users in a cloud-based organization.</p> <p>Note: In Exchange Online PowerShell, we recommend that you use the Get-EXORecipientPermission cmdlet instead of this cmdlet. For more information, see Connect to Exchange Online PowerShell.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-RecoverableItems</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p>

Cmdlet	Description
	<p>Use the <code>Get-RecoverableItems</code> cmdlet to view deleted items in mailboxes. After you find the deleted items, you use the <code>Restore-RecoverableItems</code> cmdlet to restore them.</p> <p>This cmdlet is available only in the Mailbox Import Export role, and by default, the role isn't assigned to any role groups. To use this cmdlet, you need to add the Mailbox Import Export role to a role group (for example, to the Organization Management role group). For more information, see Add a role to a role group.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-ResourceConfig</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the <code>Get-ResourceConfig</code> cmdlet to view custom room and equipment mailbox properties that you've configured by using the <code>Set-ResourceConfig</code> cmdlet.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-SweepRule</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the <code>Get-SweepRule</code> cmdlet to view Sweep rules in mailboxes. Sweep rules run at regular intervals to help keep your Inbox clean.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-UserPhoto</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the <code>Get-UserPhoto</code> cmdlet to view information about the user photos feature that allows users to associate a picture with their account. User photos appear in client applications, such as Outlook, Microsoft Teams, and SharePoint.</p>

Cmdlet	Description
	<p>Note: In Microsoft 365, you can manage user photos in Microsoft Graph PowerShell. For instructions, see Manage user photos in Microsoft Graph PowerShell.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Import-RecipientDataProperty</p>	<p>Use the Import-RecipientDataProperty cmdlet to add a picture or a spoken name audio file to a mailbox or mail contact.</p> <p>Note: Profile cards across Microsoft apps and services don't support imported pictures for mail contacts.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-App</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the New-App cmdlet to install apps for Outlook.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-InboxRule</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the New-InboxRule cmdlet to create Inbox rules in mailboxes. Inbox rules process messages in the Inbox based on conditions and take actions such as moving a message to a specified folder or deleting a message.</p> <p>You must have adequate permissions on the mailbox to create an Inbox rule.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
<p>New-Mailbox</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the New-Mailbox cmdlet to create mailboxes and user accounts at the same time.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-MailboxExportRequest</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the New-MailboxExportRequest cmdlet to begin the process of exporting contents of a primary mailbox or archive to a .pst file.</p> <p>This cmdlet is available only in the Mailbox Import Export role, and by default, the role isn't assigned to any role groups. To use this cmdlet, you need to add the Mailbox Import Export role to a role group (for example, to the Organization Management role group). For more information, see Add a role to a role group.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-MailboxFolder</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the New-MailboxFolder cmdlet to create folders in your own mailbox. Administrators can't use this cmdlet to create folders in other mailboxes (the cmdlet is available only from the MyBaseOptions user role).</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-MailboxImportRequest</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p>

Cmdlet	Description
	<p>Use the New-MailboxImportRequest cmdlet to begin the process of importing a .pst file to a mailbox or archive.</p> <p>Note: This cmdlet is no longer supported in Exchange Online. To import a .pst file in Exchange Online, see Use network upload to import PST files.</p> <p>This cmdlet is available only in the Mailbox Import Export role, and by default, the role isn't assigned to any role groups. To use this cmdlet, you need to add the Mailbox Import Export role to a role group (for example, to the Organization Management role group). For more information, see Add a role to a role group.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-MailboxRestoreRequest</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the New-MailboxRestoreRequest cmdlet to restore a soft-deleted or disconnected mailbox. This cmdlet starts the process of moving content from the soft-deleted mailbox, disabled mailbox, or any mailbox in a recovery database into a connected primary or archive mailbox.</p> <p>The properties used to find disconnected mailboxes and restore a mailbox are different in Exchange Server and Exchange Online. For more information about Exchange Online, see Restore an inactive mailbox.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-MailMessage</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the New-MailMessage cmdlet to create an email message for the specified user mailbox and place the email message in the Drafts folder of the user's mailbox.</p>

Cmdlet	Description
	<p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-SiteMailbox</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>The New-SiteMailbox cmdlet is used by the Microsoft SharePoint and Microsoft Exchange user interfaces to create site mailboxes. We recommend that you don't use this cmdlet; instead use SharePoint to create the site mailbox. This cmdlet should only be used for diagnostic and troubleshooting purposes.</p> <p>Site mailboxes were deprecated in Exchange Online and SharePoint Online in 2017. For more information, see Deprecation of Site Mailboxes.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-SweepRule</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the New-SweepRule cmdlet to create Sweep rules in mailboxes. Sweep rules run at regular intervals to help keep your Inbox clean.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-App</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Remove-App cmdlet to uninstall an app.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-CalendarEvents</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p>

Cmdlet	Description
	<p>Use the Remove-CalendarEvents cmdlet to cancel future meetings in user or resource mailboxes. Cancelling future meetings removes them from attendee and resource calendars (for example, you're going to remove the mailbox, or the user is going on a leave of absence).</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-InboxRule</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Remove-InboxRule cmdlet to remove an Inbox rule.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-Mailbox</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Remove-Mailbox cmdlet to delete mailboxes and the associated user accounts.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-MailboxExportRequest</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Remove-MailboxExportRequest cmdlet to remove fully or partially completed export requests. You can create multiple export requests for a specified mailbox provided that you specify a distinct name. Completed export requests aren't cleared automatically; they need to be removed by using this cmdlet.</p> <p>This cmdlet is available only in the Mailbox Import Export role, and by default, the role isn't assigned to any role groups. To use this cmdlet, you need to add the Mailbox Import Export role to a role group (for example, to the Organization Management role group). For more information, see Add a role to a role group.</p>

Cmdlet	Description
	<p>When a partially completed export request is removed, content already exported isn't removed from the PST file. If you want to start a new export request to the same file name and start with an empty PST file, you need to rename or delete the previous PST file.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-MailboxFolderPermission</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Remove-MailboxFolderPermission cmdlet to remove folder-level permissions for users in mailboxes.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-MailboxImportRequest</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Remove-MailboxImportRequest cmdlet to remove fully or partially completed import requests. Completed import requests aren't automatically cleared. Requests need to be removed by using the Remove-MailboxImportRequest cmdlet. Multiple import requests can exist against the same mailbox if you provide a distinct import request name.</p> <p>NOTE: This cmdlet is no longer supported in Exchange Online. To import a .pst file in Exchange Online, see Use network upload to import PST files.</p> <p>This cmdlet is available only in the Mailbox Import Export role, and by default, the role isn't assigned to any role groups. To use this cmdlet, you need to add the Mailbox Import Export role to a role group (for example, to the Organization Management role group). For more information, see Add a role to a role group.</p> <p>Removing a partially completed import request removes the request from the Microsoft Exchange Mailbox Replication service (MRS) job queue. Any import progress made before the removal isn't reverted.</p>

Cmdlet	Description
	<p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-MailboxPermission</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Remove-MailboxPermission cmdlet to remove permissions from a user's mailbox or from an Exchange Server 2016, Exchange Server 2019 or Exchange Online mail user.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-MailboxRestoreRequest</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Remove-MailboxRestoreRequest cmdlet to remove fully or partially completed restore requests.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-MailboxUserConfiguration</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Remove-MailboxUserConfiguration cmdlet to remove user configuration items from mailboxes. Typically, after you delete a user configuration item, it's automatically recreated the next time the user uses that feature in their mailbox.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-RecipientPermission</p>	<p>This cmdlet is available only in the cloud-based service.</p>

Cmdlet	Description
	<p>Use the Remove-RecipientPermission cmdlet to remove SendAs permission from users in a cloud-based organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-SweepRule</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Remove-SweepRule cmdlet to remove Sweep rules from mailboxes.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-UserPhoto</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Remove-UserPhoto cmdlet to delete the photo associated with a user's account. The user photo feature allows users to associate a picture with their account. User photos appear in client applications, such as Outlook, Microsoft Teams, and SharePoint.</p> <p>Note: In Microsoft 365, you can manage user photos in Microsoft Graph PowerShell. For instructions, see Manage user photos in Microsoft Graph PowerShell.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Restore-Mailbox</p>	<p>This cmdlet is available only in Exchange Server 2010.</p> <p>Use the Restore-Mailbox cmdlet to extract mailbox content from a restored database.</p> <p>Note: In Exchange Server 2010 Service Pack 1 (SP1) or later, use the New-MailboxRestoreRequest cmdlet instead of the Restore-Mailbox cmdlet to extract mailbox content from a restored database.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
<p>Restore-RecoverableItems</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Restore-RecoverableItems items cmdlet to restore deleted items in mailboxes. You use the Get-RecoverableItems cmdlet to find the deleted items to recover.</p> <p>This cmdlet is available only in the Mailbox Import Export role, and by default, the role isn't assigned to any role groups. To use this cmdlet, you need to add the Mailbox Import Export role to a role group (for example, to the Organization Management role group). For more information, see Add a role to a role group.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Resume-MailboxExportRequest</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Resume-MailboxExportRequest cmdlet to resume an export request that was suspended or failed.</p> <p>This cmdlet is available only in the Mailbox Import Export role and by default, the role isn't assigned to any role groups. To use this cmdlet, you need to add the Mailbox Import Export role to a role group (for example, to the Organization Management role group). For more information, see Add a role to a role group.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Resume-MailboxImportRequest</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Resume-MailboxImportRequest cmdlet to resume an import request that was suspended or failed.</p> <p>NOTE: This cmdlet is no longer supported in Exchange Online. To import a .pst file in Exchange Online, see Use network upload to import PST files.</p>

Cmdlet	Description
	<p>This cmdlet is available only in the Mailbox Import Export role and by default, the role isn't assigned to any role groups. To use this cmdlet, you need to add the Mailbox Import Export role to a role group (for example, to the Organization Management role group). For more information, see Add a role to a role group.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Resume-MailboxRestoreRequest</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Resume-MailboxRestoreRequest cmdlet to resume a restore request that was suspended or failed.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Search-Mailbox</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Search-Mailbox cmdlet to search a mailbox and copy the results to a specified target mailbox, delete messages from the source mailbox, or both.</p> <p>Note: In cloud-based environments, the Search-Mailbox cmdlet was deprecated in favor of New-ComplianceSearch and related eDiscovery cmdlets.</p> <p>By default, Search-Mailbox is available only in the Mailbox Search or Mailbox Import Export roles, and these roles aren't assigned to <i>any</i> role groups. To use this cmdlet, you need to add one or both of the roles to a role group (for example, the Organization Management role group). Only the Mailbox Import Export role gives you access to the DeleteContent parameter. For more information about adding roles to role groups, see Add a role to a role group.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
Set-App	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Set-App cmdlet to modify the availability of organization apps.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Set-CalendarNotification	<p>This cmdlet is available only in on-premises Exchange.</p> <p>The Set-CalendarNotification cmdlet allows users to set text message notification options for calendar events in their own calendar. By default, the MyTextMessaging end-user role gives access to this cmdlet, so admins can't configure text messaging notification for calendar events in user calendars.</p> <p>Note: This cmdlet is deprecated in Exchange Online PowerShell. The text message notification service is discontinued in Microsoft 365.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Set-CalendarProcessing	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Set-CalendarProcessing cmdlet to modify calendar processing options for resource mailboxes, which include the Calendar Attendant, resource booking assistant, and calendar configuration. This cmdlet is effective only on resource mailboxes.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Set-Clutter	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Set-Clutter cmdlet to configure Clutter settings for mailboxes in your organization.</p>

Cmdlet	Description
	<p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-EventsFromEmailConfiguration</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Set-EventsFromEmailConfiguration cmdlet to modify the events from email settings on a mailbox. on Outlook clients and Outlook on the web. These settings define whether Outlook or Outlook on the web (formerly known as Outlook Web App) automatically discovers events from email messages and adds them to the user's calendar.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-ExternalInOutlook</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Set-ExternalInOutlook cmdlet to modify the configuration of external sender identification that's available in Outlook, Outlook for Mac, Outlook on the web, and Outlook for iOS and Android.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-FocusedInbox</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Set-FocusedInbox cmdlet to enable or disable Focused Inbox for mailboxes in your organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-InboxRule</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Set-InboxRule cmdlet to modify existing Inbox rules in mailboxes. Inbox rules process messages in the Inbox based on conditions specified and take actions such as moving a message to a specified folder or deleting a message.</p>

Cmdlet	Description
	<p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-Mailbox</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Set-Mailbox cmdlet to modify the settings of existing mailboxes.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-MailboxAutoReplyConfiguration</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Set-MailboxAutoReplyConfiguration cmdlet to configure Automatic Replies settings for a specific mailbox.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-MailboxCalendarFolder</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Set-MailboxCalendarFolder cmdlet to configure calendar publishing or sharing settings on a mailbox for the visibility of calendar information to external users. To add or modify the permissions so internal users can access the calendar, use the Add-MailboxFolderPermission or Set-MailboxFolderPermission cmdlets.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-MailboxExportRequest</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Set-MailboxExportRequest cmdlet to change export request options after the request is created. You can use the Set-MailboxExportRequest cmdlet to recover from failed export requests.</p>

Cmdlet	Description
	<p>This cmdlet is available only in the Mailbox Import Export role, and by default, the role isn't assigned to any role groups. To use this cmdlet, you need to add the Mailbox Import Export role to a role group (for example, to the Organization Management role group). For more information, see Add a role to a role group.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-MailboxFolderPermission</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Set-MailboxFolderPermission cmdlet to modify folder-level permissions for users in mailboxes. This cmdlet differs from the Add-MailboxFolderPermission cmdlet in that it modifies existing permission entries. To configure calendar publishing or sharing settings for a mailbox so calendar information is visible to external users, use the Set-MailboxCalendarFolder cmdlet.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-MailboxImportRequest</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Set-MailboxImportRequest cmdlet to change import request options after the request is created. You can use the Set-MailboxImportRequest cmdlet to recover from failed import requests.</p> <p>This cmdlet is available only in the Mailbox Import Export role, and by default, the role isn't assigned to any role groups. To use this cmdlet, you need to add the Mailbox Import Export role to a role group (for example, to the Organization Management role group). For more information, see Add a role to a role group.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
Set-MailboxPlan	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Set-MailboxPlan cmdlet to modify the settings of mailbox plans in the cloud-based service.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Set-MailboxRestoreRequest	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Set-MailboxRestoreRequest cmdlet to change restore request options after the request is created. You can use this cmdlet to recover from failed restore requests.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Set-MailboxSentItemsConfiguration	<p>This cmdlet is available only in Exchange Server 2010.</p> <p>Use the Set-MailboxSentItemsConfiguration cmdlet to modify the Sent Items settings for mailboxes in your organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Set-Place	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Set-Place cmdlet to update room mailboxes with additional metadata, which provides a better search and room suggestion experience.</p> <p>Note: In hybrid environments, this cmdlet doesn't work on the following properties on synchronized room mailboxes: City, CountryOrRegion, GeoCoordinates, Phone, PostalCode, State, or Street. To modify these properties (except GeoCoordinates on synchronized room mailboxes), use the Set-User or Set-Mailbox cmdlets in on-premises Exchange.</p> <p>Note: We recommend using this cmdlet with the EXO V3 module.</p> <p>Commands using Set-Place to change certain combinations of properties</p>

Cmdlet	Description
	<p>together can fail in older versions of the module. For more information about the EXO V3 module, see About the Exchange Online PowerShell module.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-ResourceConfig</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Set-ResourceConfig cmdlet to create custom resource properties that you can add to room and equipment mailboxes.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-SweepRule</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Set-SweepRule cmdlet to modify Sweep rules in mailboxes.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-UserPhoto</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Set-UserPhoto cmdlet to configure the user photos feature that allows users to associate a picture with their account. User photos appear in client applications, such as Outlook, Microsoft Teams, and SharePoint.</p> <p>Note: In Microsoft 365, you can manage user photos in Microsoft Graph PowerShell. For instructions, see Manage user photos in Microsoft Graph PowerShell.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
Suspend-MailboxExportRequest	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Suspend-MailboxExportRequest cmdlet to suspend an export request any time after the request was created, but before the request reaches the status of Completed. You can resume the request by using the Resume-MailboxExportRequest cmdlet.</p> <p>This cmdlet is available only in the Mailbox Import Export role, and by default, the role isn't assigned to any role groups. To use this cmdlet, you need to add the Mailbox Import Export role to a role group (for example, to the Organization Management role group). For more information, see Add a role to a role group.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Suspend-MailboxImportRequest	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Suspend-MailboxImportRequest cmdlet to suspend an import request any time after the request was created, but before the request reaches the status of Completed. You can resume the move request by using the Resume-MailboxImportRequest cmdlet.</p> <p>NOTE: This cmdlet is no longer supported in Exchange Online. To import a .pst file in Exchange Online, see Use network upload to import PST files.</p> <p>This cmdlet is available only in the Mailbox Import Export role, and by default, the role isn't assigned to any role groups. To use this cmdlet, you need to add the Mailbox Import Export role to a role group (for example, to the Organization Management role group). For more information, see Add a role to a role group.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Suspend-MailboxRestoreRequest	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p>

Cmdlet	Description
	<p>Use the Suspend-MailboxRestoreRequest cmdlet to suspend a restore request any time after the request was created, but before the request reaches the status of Completed. You can resume the restore request by using the Resume-MailboxRestoreRequest cmdlet.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Test-MAPIConnectivity</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Test-MapiConnectivity cmdlet to verify server functionality by logging on to the mailbox that you specify. If you don't specify a mailbox, the cmdlet logs on to the SystemMailbox on the database that you specify.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Undo-SoftDeletedMailbox</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Undo-SoftDeletedMailbox cmdlet to recover a mailbox that is deleted. Mailboxes can be recovered within 30 days of being deleted.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Cmdlet	Description
<p>Complete-MigrationBatch</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Complete-MigrationBatch cmdlet to finalize a migration batch that has successfully finished initial synchronization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
<p>Export-MigrationReport</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>The Export-MigrationReport is used by the Exchange migration process to enable an administrator to download a CSV file that contains migration errors for a selected migration batch. This cmdlet isn't run by an administrator in Windows PowerShell.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-MigrationBatch</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Get-MigrationBatch cmdlet to retrieve status information about the current migration batch.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-MigrationConfig</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Get-MigrationConfig cmdlet to retrieve migration configuration settings on Exchange servers.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-MigrationEndpoint</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Get-MigrationEndpoint cmdlet to retrieve migration endpoint settings for source or destination</p>

Cmdlet	Description
	<p>servers for cutover or staged Exchange migrations, IMAP migrations, and remote moves.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-MigrationStatistics</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Get-MigrationStatistics cmdlet to view detailed information about migration requests.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-MigrationUser</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Get-MigrationUser cmdlet to view information about move and migration users.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-MigrationUserStatistics</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Get-MigrationUserStatistics cmdlet to view detailed information about the migration requested for a specific user.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-MoveRequest</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p>

Cmdlet	Description
	<p>Use the Get-MoveRequest cmdlet to view the detailed status of an ongoing asynchronous mailbox move that was initiated by using the New-MoveRequest cmdlet.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-MoveRequestStatistics</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Get-MoveRequestStatistics cmdlet to view detailed information about move requests.</p> <p>Some of the failure messages that are returned by this cmdlet are temporary and don't indicate that a request has actually failed. If the Status value is Queued or InProgress, then the request is proceeding normally.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-PublicFolderMailboxMigrationRequest</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Get-PublicFolderMailboxMigrationRequest cmdlet to view the status of individual jobs in public folder migration batches that were created by using the New-MigrationBatch cmdlet.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-PublicFolderMailboxMigrationRequestStatistics</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Get-PublicFolderMailboxMigrationRequestStatistics cmdlet to view the detailed status of individual jobs in a public</p>

Cmdlet	Description
	<p>folder migration batch created using New-MigrationBatch cmdlet.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-PublicFolderMigrationRequest</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Get-PublicFolderMigrationRequest cmdlet to view information about serial public folder migration requests (requests created by the New-PublicFolderMigrationRequest cmdlet).</p> <p>Note: Support for serial migration of public folders ended in Exchange 2013 Cumulative Update 8 (CU8), and the cmdlets are no longer available in Exchange Online. Instead, use the corresponding *-MigrationBatch and *-PublicFolderMailboxMigration* cmdlets.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-PublicFolderMigrationRequestStatistics</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Get-PublicFolderMigrationRequestStatistics cmdlet to view detailed information about serial public folder migration requests (requests created by the New-PublicFolderMigrationRequest cmdlet).</p> <p>Note: Support for serial migration of public folders ended in Exchange 2013 Cumulative Update 8 (CU8), and the cmdlets are no longer available in Exchange Online. Instead, use the corresponding *-MigrationBatch and *-PublicFolderMailboxMigration* cmdlets.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-PublicFolderMoveRequest</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p>

Cmdlet	Description
	<p>Use the Get-PublicFolderMoveRequest cmdlet to view the detailed status of an ongoing public folder move that was initiated using the New-PublicFolderMoveRequest cmdlet.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-PublicFolderMoveRequestStatistics</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Get-PublicFolderMoveRequestStatistics cmdlet to view detailed information about public folder move requests.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-MigrationBatch</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the New-MigrationBatch cmdlet to submit a new migration request for a batch of users.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-MigrationEndpoint</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the New-MigrationEndpoint cmdlet to configure the connection settings for cross-forests moves, remote move migrations, cutover or staged Exchange migrations, IMAP migrations, and Google Workspace (formerly G Suite) migrations.</p>

Cmdlet	Description
	<p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-MoveRequest</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the New-MoveRequest cmdlet to begin the process of an asynchronous mailbox or personal archive move. You can also check mailbox readiness to be moved by using the WhatIf parameter.</p> <p>Note: After April 15, 2020, you shouldn't use this cmdlet to manually move mailboxes within an Exchange Online organization. You can only use this cmdlet for migrating to and from Exchange Online. If you have issues with a mailbox and want to fix it by moving the mailbox within your Exchange Online organization, please open a Microsoft Support request instead.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-PublicFolderMigrationRequest</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the New-PublicFolderMigrationRequest cmdlet to start a serial public folder migration from Exchange Server 2010.</p> <p>Note: Support for serial migration of public folders ended in Exchange 2013 Cumulative Update 8 (CU8), and the cmdlets are no longer available in Exchange Online. Instead, use the corresponding *-MigrationBatch and *-PublicFolderMailboxMigration* cmdlets.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-PublicFolderMoveRequest</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings</p>

Cmdlet	Description
	<p>might be exclusive to one environment or the other.</p> <p>Use the <code>New-PublicFolderMoveRequest</code> cmdlet to begin the process of moving public folder contents between public folder mailboxes. Moving public folders only moves the physical contents of the public folder; it doesn't change the logical hierarchy. When the move request is completed, you must run the <code>Remove-PublicFolderMoveRequest</code> cmdlet to remove the request or wait until the time specified in the <code>CompletedRequestAgeLimit</code> parameter has passed. The request must be removed before you can run another move request.</p> <p>Be aware that the target public folder mailbox was locked while the move request is active. For more information, see the Description section.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-MigrationBatch</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the <code>Remove-MigrationBatch</code> cmdlet to delete a migration batch that either isn't running or is completed. If necessary, you can run the <code>Get-MigrationBatch</code> cmdlet to determine the status of a migration batch before you remove it.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-MigrationEndpoint</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the <code>Remove-MigrationEndpoint</code> cmdlet to remove existing migration endpoints for source or destination</p>

Cmdlet	Description
	<p>servers for cutover or staged Exchange migrations, IMAP migrations and remote moves.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-MigrationUser</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Remove-MigrationUser cmdlet to remove a migration user from a batch.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-MoveRequest</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Remove-MoveRequest cmdlet to cancel a mailbox move initiated using the New-MoveRequest cmdlet.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-PublicFolderMailboxMigrationRequest</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Remove-PublicFolderMailboxMigrationRequest cmdlet to remove individual jobs from public folder migration batches that were created by using the New-MigrationBatch cmdlet.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-PublicFolderMigrationRequest</p>	<p>This cmdlet is available only in on-premises Exchange.</p>

Cmdlet	Description
	<p>Use the Remove-PublicFolderMigrationRequest cmdlet to cancel or complete serial public folder migration requests (requests created by the New-PublicFolderMigrationRequest cmdlet). You need to use this cmdlet to remove an existing serial public folder migration request before you can create another one.</p> <p>Note: Support for serial migration of public folders ended in Exchange 2013 Cumulative Update 8 (CU8), and the cmdlets are no longer available in Exchange Online. Instead, use the corresponding *-MigrationBatch and *-PublicFolderMailboxMigration* cmdlets.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-PublicFolderMoveRequest</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Remove-PublicFolderMoveRequest cmdlet to cancel a mailbox move initiated using the New-MoveRequest cmdlet. After the move is finalized, you can't undo the move request.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Resume-MoveRequest</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Resume-MoveRequest cmdlet to resume a move request that is suspended or has failed.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Resume-PublicFolderMigrationRequest</p>	<p>This cmdlet is available only in on-premises Exchange.</p>

Cmdlet	Description
	<p>Use the Resume-PublicFolderMigrationRequest cmdlet to resume serial public folder migration requests (requests created by the New-PublicFolderMigrationRequest cmdlet) that have failed or have been suspended (manually or automatically).</p> <p>Note: Support for serial migration of public folders ended in Exchange 2013 Cumulative Update 8 (CU8), and the cmdlets are no longer available in Exchange Online. Instead, use the corresponding *-MigrationBatch and *-PublicFolderMailboxMigration* cmdlets.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Resume-PublicFolderMoveRequest</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Resume-PublicFolderMoveRequest cmdlet to resume a public folder move request that is suspended or has failed.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-MigrationBatch</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Set-MigrationBatch cmdlet to update a migration request for a batch of users. For more information, see New-MigrationBatch.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-MigrationConfig</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Set-MigrationConfig cmdlet to edit migration configurations on Exchange servers.</p>

Cmdlet	Description
	<p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-MigrationEndpoint</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Set-MigrationEndpoint cmdlet to edit settings for cutover or staged Exchange migrations, IMAP migrations, Google Workspace (formerly G Suite) migrations, and remote moves.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-MigrationUser</p>	<p>This cmdlet is functional only in the cloud-based service.</p> <p>Use the Set-MigrationUser cmdlet to modify the migration settings of a user in an existing migration batch.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-MoveRequest</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Set-MoveRequest cmdlet to change move request options after the move request is created. You can use the Set-MoveRequest cmdlet to recover from failed move requests.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-PublicFolderMigrationRequest</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Set-PublicFolderMigrationRequest cmdlet to modify serial public folder migration requests (requests created by the New-PublicFolderMigrationRequest</p>

Cmdlet	Description
	<p>cmdlet). You can use this cmdlet to recover from failed migration requests.</p> <p>Note: Support for serial migration of public folders ended in Exchange 2013 Cumulative Update 8 (CU8), and the cmdlets are no longer available in Exchange Online. Instead, use the corresponding *-MigrationBatch and *-PublicFolderMailboxMigration* cmdlets.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-PublicFolderMoveRequest</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Set-PublicFolderMoveRequest cmdlet to change a public folder move request after the move request is created. You can use the Set-PublicFolderMoveRequest cmdlet to recover from a failed move request.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Start-MigrationBatch</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Start-MigrationBatch cmdlet to start a move request or migration batch that was created with the New-MigrationBatch cmdlet.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Start-MigrationUser</p>	<p>This cmdlet is functional only in the cloud-based service.</p> <p>Use the Start-MigrationUser cmdlet to start the migration of a user in an existing migration batch.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
<p>Stop-MigrationBatch</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Stop-MigrationBatch cmdlet to stop the processing of a migration batch that's in progress.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Stop-MigrationUser</p>	<p>This cmdlet is functional only in the cloud-based service.</p> <p>Use the Stop-MigrationUser cmdlet to stop the migration of a user in an existing migration batch.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Suspend-MoveRequest</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Suspend-MoveRequest cmdlet to suspend a move request any time after the move request was created, but before it reaches the status of CompletionInProgress. You can resume the move request by using the Resume-MoveRequest cmdlet.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Suspend-PublicFolderMailboxMigrationRequest</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Suspend-PublicFolderMailboxMigrationRequest cmdlet to suspend individual jobs in public folder migration batches that were created by using the New-MigrationBatch cmdlet.</p>

Cmdlet	Description
	<p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Suspend-PublicFolderMigrationRequest</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Suspend-PublicFolderMigrationRequest cmdlet to suspend serial public folder migration requests (requests created by the New-PublicFolderMigrationRequest cmdlet). You can suspend active requests before they reach the status CompletionInProgress. You resume suspended requests by using the Resume-PublicFolderMigrationRequest cmdlet.</p> <p>Note: Support for serial migration of public folders ended in Exchange 2013 Cumulative Update 8 (CU8), and the cmdlets are no longer available in Exchange Online. Instead, use the corresponding *-MigrationBatch and *-PublicFolderMailboxMigration* cmdlets.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Suspend-PublicFolderMoveRequest</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Suspend-PublicFolderMoveRequest cmdlet to suspend a move request any time after the move request was created, but before it reaches the status of CompletionInProgress. You can resume the move request by using the Resume-PublicFolderMoveRequest cmdlet.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Test-MigrationServerAvailability</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Test-MigrationServerAvailability cmdlet to test the availability of the target server in preparation to perform cross-forest mailbox moves, migration of on-</p>

Cmdlet	Description
	<p>premises mailboxes to Exchange Online, or to migrate on-premises mailbox data from an IMAP server to Exchange Online mailboxes. For all migration types, the cmdlet attempts to verify the connection settings used to connect to the target server.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Cmdlet	Description
<p>Add-HVEAppAccess</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Add-HVEAppAccess cmdlet to add applications to the Allowed Apps list of a High Volume Email (HVE) account.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Disable-CmdletExtensionAgent</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Disable-CmdletExtensionAgent cmdlet to disable existing cmdlet extension agents.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Enable-CmdletExtensionAgent</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Enable-CmdletExtensionAgent cmdlet to enable existing cmdlet extension agents.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Enable-OrganizationCustomization</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>You might be prompted to run the EnableOrganizationCustomization cmdlet before you create or modify objects in your Exchange Online organization.</p>

Cmdlet	Description
	<p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-AccessToCustomerDataRequest</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Get-AccessToCustomerDataRequest cmdlet to view Microsoft 365 Customer Lockbox requests that control access to your data by Microsoft support engineers.</p> <p>Note: Customer Lockbox is included in Microsoft 365 E5, or you can buy a separate Customer Lockbox subscription with any Microsoft 365 Enterprise plan.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-ApplicationAccessPolicy</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Get-ApplicationAccessPolicy cmdlet to view the list of application access policies.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-AuthConfig</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Get-AuthConfig cmdlet to get the authorization configuration for partner applications.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
<p>Get-AuthenticationPolicy</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Get-AuthenticationPolicy cmdlet to view authentication policies in your organization. For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-AuthServer</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Get-AuthServer cmdlet to view the settings of authorization servers in the Exchange organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-CmdletExtensionAgent</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Get-CmdletExtensionAgent cmdlet to view cmdlet extension agents.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-ExchangeAssistanceConfig</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Get-ExchangeAssistanceConfig cmdlet to view the configuration information for the URLs that Microsoft Exchange Help uses to connect to the source of the documentation.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-ExchangeDiagnosticInfo</p>	<p>This cmdlet is available only in on-premises Exchange.</p>

Cmdlet	Description
	<p>Use the Get-ExchangeDiagnosticInfo cmdlet to return information about processes that are running on Exchange servers.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-ExchangeFeature</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Get-ExchangeFeature cmdlet to return information about features that are flighted on Exchange servers.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-ExchangeServer</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Get-ExchangeServer cmdlet to view the properties of Exchange servers.</p> <p>When you run the Get-ExchangeServer cmdlet with no parameters, it returns the attributes of all the servers in the Exchange organization. To return specific server properties (including domain controller information) where the Get-ExchangeServer cmdlet has to contact servers directly or perform a complex or slow calculation, make sure you use the Status parameter.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
Get-ExchangeServerAccessLicense	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Get-ExchangeServerAccessLicense cmdlet to return a list of licenses in use in your Exchange organization. This refers to the specific legal name of the license, as defined in the Microsoft Product List and is representative of your licenses when you run this cmdlet.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Get-ExchangeServerAccessLicenseUser	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Get-ExchangeServerAccessLicenseUser cmdlet to return a list of unique users for the specified license name. Each object contains the FQDN or primary SMTP address of the mailbox and the license that's associated with it.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Get-ExchangeSettings	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Get-ExchangeSettings cmdlet to view customized Exchange setting objects that are stored in Active Directory. Use the New-ExchangeSettings to create the settings object, and the Set-ExchangeSettings cmdlet to define the actual settings.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Get-FeatureConfiguration	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Note</p> <p>This cmdlet is currently available in Public Preview, isn't available in all organizations, and is subject to change.</p>

Cmdlet	Description
	<p>Use the Get-FeatureConfiguration cmdlet to view Microsoft Purview feature configurations within your organization, including:</p> <ul style="list-style-type: none"> • Collection policies. • Advanced label based protection. <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-HVEAccountSettings</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Get-HVEAccountSettings cmdlet to view the account settings of a High Volume Email (HVE) account.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-Notification</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Note</p> <p>This cmdlet will be deprecated in the cloud-based service. The classic Exchange admin center was deprecated in the cloud-based service in 2023.</p> <p>Use the Get-Notification cmdlet to view notification events that are shown in the notification viewer in the Exchange admin center (EAC). These notifications are related to the following events:</p> <ul style="list-style-type: none"> • Mailbox moves and migrations. • Expiring and expired certificates. • Exporting mailbox content to .pst files. • Importing mailbox content from .pst files. • Restoring deleted mailboxes. <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
<p>Get-OrganizationConfig</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Get-OrganizationConfig cmdlet to get configuration data for an Exchange organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-PartnerApplication</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Get-PartnerApplication cmdlet to retrieve settings for a partner application.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-PerimeterConfig</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Get-PerimeterConfig cmdlet to view the list of gateway server and internal mail server IP addresses that have been added to the cloud-based safelists.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-ServicePrincipal</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Get-ServicePrincipal cmdlet to view information about service principals in your cloud-based organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-SettingOverride</p>	<p>This cmdlet is available only in on-premises Exchange.</p>

Cmdlet	Description
	<p>Caution: Incorrect usage of the setting override cmdlets can cause serious damage to your Exchange organization. This damage could require you to reinstall Exchange. Only use these cmdlets as instructed by product documentation or under the direction of Microsoft Customer Service and Support.</p> <p>Use the Get-SettingOverride cmdlet to view existing setting overrides that store Exchange customizations in Active Directory instead of in text files on the server.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Invoke-ProvisioningAcceptedDomainDiagnostic</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Invoke-ProvisioningAcceptedDomainDiagnostic cmdlet to validate and repair accepted domain configurations in cloud-based organizations.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Invoke-ProvisioningCompanyObjectDiagnostic</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Invoke-ProvisioningCompanyObjectDiagnostic cmdlet to validate and fix core Microsoft 365 tenant information and service plan configuration in cloud-based organizations.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Invoke-ProvisioningRecipientDiagnostic</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Invoke-ProvisioningRecipientDiagnostic cmdlet to identify and repair recipient provisioning failures in cloud-based organizations. Recipients include mailboxes, mail contacts, mail users, and groups.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
<p>Invoke-ProvisioningVerifyRbacDiagnostic</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Invoke-ProvisioningVerifyRbacDiagnostic cmdlet to analyze and repair role-based access control (RBAC) configurations in cloud-based organizations.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-ApplicationAccessPolicy</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Important</p> <p>App Access Policies are replaced by Role Based Access Control for Applications. To learn more, see Role Based Access Control for Exchange Applications. Don't create new App Access Policies as these policies will eventually require migration to Role Based Access Control for Applications.</p> <p>Use the New-ApplicationAccessPolicy cmdlet to restrict or deny access to a specific set of mailboxes by an application that uses APIs (Outlook REST, Microsoft Graph, or Exchange Web Services (EWS)). These policies are complementary to the permission scopes that are declared by the application.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-AuthenticationPolicy</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the New-AuthenticationPolicy cmdlet to create authentication policies in your organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-AuthServer</p>	<p>This cmdlet is available only in on-premises Exchange.</p>

Cmdlet	Description
	<p>Use the New-AuthServer cmdlet to create an authorization server object in Microsoft Exchange and specify its AuthMetadataUrl. Exchange honors tokens issued by the authorization server for access by a partner application.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-ExchangeSettings</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the New-ExchangeSettings cmdlet to create customized Exchange setting objects that are stored in Active Directory. Use the Set-ExchangeSettings cmdlet to configure the actual settings.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-FeatureConfiguration</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Note</p> <p>This cmdlet is currently available in Public Preview, isn't available in all organizations, and is subject to change.</p> <p>Use the New-FeatureConfiguration cmdlet to create Microsoft Purview feature configurations within your organization, including:</p> <ul style="list-style-type: none"> • Collection policies. • Advanced label based protection. <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-PartnerApplication</p>	<p>This cmdlet is functional only in on-premises Exchange.</p> <p>Use the New-PartnerApplication cmdlet to create partner application configurations in on-premises Exchange organizations.</p>

Cmdlet	Description
	<p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-ServicePrincipal</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the New-ServicePrincipal cmdlet to create service principals in your cloud-based organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-SettingOverride</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Caution: Incorrect usage of the setting override cmdlets can cause serious damage to your Exchange organization. This damage could require you to reinstall Exchange. Only use these cmdlets as instructed by product documentation or under the direction of Microsoft Customer Service and Support.</p> <p>Use the New-SettingOverride cmdlet to create setting overrides that store Exchange customizations in Active Directory instead of in text files on the server.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-ApplicationAccessPolicy</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Remove-ApplicationAccessPolicy cmdlet to remove application access policies. These changes might take up to 30 minutes to go live.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-AuthenticationPolicy</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p>

Cmdlet	Description
	<p>Use the Remove-AuthenticationPolicy cmdlet to remove authentication policies from your organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-AuthServer</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Remove-AuthServer cmdlet to remove an authorization server.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-FeatureConfiguration</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Note</p> <p>This cmdlet is currently available in Public Preview, isn't available in all organizations, and is subject to change.</p> <p>Use the Remove-FeatureConfiguration cmdlet to remove Microsoft Purview feature configurations within your organization, including:</p> <ul style="list-style-type: none"> • Collection policies. • Advanced label based protection. <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-HVEAppAccess</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Remove-HVEAppAccess cmdlet to remove applications from the Allowed Apps list of a High Volume Email (HVE) account.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
<p>Remove-PartnerApplication</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Remove-PartnerApplication cmdlet to remove a partner application configuration.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-ServicePrincipal</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Remove-ServicePrincipal cmdlet to remove service principals from your cloud-based organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-SettingOverride</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Caution: Incorrect usage of the setting override cmdlets can cause serious damage to your Exchange organization. This damage could require you to reinstall Exchange. Only use these cmdlets as instructed by product documentation or under the direction of Microsoft Customer Service and Support.</p> <p>Use the Remove-SettingOverride cmdlet to remove setting overrides from Active Directory.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-AccessToCustomerDataRequest</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Set-AccessToCustomerDataRequest cmdlet to approve, deny, or cancel Microsoft 365 customer lockbox requests that control access to your data by Microsoft support engineers.</p> <p>Note: Customer Lockbox is included in Microsoft 365 E5, or you can buy a separate Customer Lockbox subscription with any Microsoft 365 Enterprise plan.</p>

Cmdlet	Description
	<p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-ApplicationAccessPolicy</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Set-ApplicationAccessPolicy cmdlet to modify the description of an application access policy.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-AuthConfig</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Set-AuthConfig cmdlet to modify the authorization configuration for your Exchange organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-AuthenticationPolicy</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Set-AuthenticationPolicy cmdlet to modify authentication policies in your organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-AuthServer</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Set-AuthServer cmdlet to configure an authorization server that partner applications can use to obtain tokens recognized by Microsoft Exchange.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-CmdletExtensionAgent</p>	<p>This cmdlet is available only in on-premises Exchange.</p>

Cmdlet	Description
	<p>Use the Set-CmdletExtensionAgent cmdlet to modify cmdlet extension agents. To enable or disable cmdlet extension agents, use the Enable-CmdletExtensionAgent and Disable-CmdletExtensionAgent cmdlets.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-ExchangeAssistanceConfig</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Set-ExchangeAssistanceConfig cmdlet to modify the Microsoft Exchange Help configurations for your organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-ExchangeFeature</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Set-ExchangeFeature cmdlet to approve or block features flighted via Feature Flighting on Exchange Server.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-ExchangeServer</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Set-ExchangeServer cmdlet to set Exchange attributes in Active Directory for a specified server.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-ExchangeSettings</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Set-ExchangeSettings cmdlet to configure Exchange setting objects that you created with the New-ExchangeSettings cmdlet.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
<p>Set-FeatureConfiguration</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Note</p> <p>This cmdlet is currently available in Public Preview, isn't available in all organizations, and is subject to change.</p> <p>Use the Set-FeatureConfiguration cmdlet to modify Microsoft Purview feature configurations within your organization, including:</p> <ul style="list-style-type: none"> • Collection policies. • Advanced label based protection. <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-HVEAccountSettings</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Set-HVEAccountSettings cmdlet to modify the account settings of a High Volume Email (HVE) account.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-Notification</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Note</p> <p>This cmdlet will be deprecated in the cloud-based service. The classic Exchange admin center was deprecated in the cloud-based service in 2023.</p> <p>Use the Set-Notification cmdlet to modify notification events that are shown in the notification viewer in the Exchange admin center (EAC). These notifications are related to the following events:</p>

Cmdlet	Description
	<ul style="list-style-type: none"> • Mailbox moves and migrations. • Expiring and expired certificates. • Exporting mailbox content to .pst files. • Importing mailbox content from .pst files. • Restoring deleted mailboxes. <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-OrganizationConfig</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Set-OrganizationConfig cmdlet to configure various settings of an Exchange organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-PartnerApplication</p>	<p>This cmdlet is functional only in on-premises Exchange.</p> <p>Use the Set-PartnerApplication cmdlet to configure partner application configurations in on-premises Exchange organizations.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-PerimeterConfig</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Set-PerimeterConfig cmdlet to modify the list of gateway server IP addresses that have been added to the cloud-based safelists.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-ServicePrincipal</p>	<p>This cmdlet is available only in the cloud-based service.</p>

Cmdlet	Description
	<p>Use the Set-ServicePrincipal cmdlet to change service principals in your cloud-based organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-SettingOverride</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Caution: Incorrect usage of the setting override cmdlets can cause serious damage to your Exchange organization. This damage could require you to reinstall Exchange. Only use these cmdlets as instructed by product documentation or under the direction of Microsoft Customer Service and Support.</p> <p>Use the Set-SettingOverride cmdlet to modify setting overrides that store Exchange customizations in Active Directory instead of in text files on the server.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Test-ApplicationAccessPolicy</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Test-ApplicationAccessPolicy cmdlet to test access right of an application to a specific user/mailbox.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Test-OAuthConnectivity</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Test-OAuthConnectivity cmdlet to test OAuth authentication to partner applications for a user.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Test-ServicePrincipalAuthorization</p>	<p>This cmdlet is available only in the cloud-based service.</p>

Cmdlet	Description
	<p>Use the Test-ServicePrincipalAuthorization cmdlet to test the access granted by role-based access control (RBAC) for Applications. For more information, see Role Based Access Control for Applications in Exchange Online.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Test-SystemHealth</p>	<p>This cmdlet is available only in Exchange Server 2010.</p> <p>Use the Test-SystemHealth cmdlet to gather data about your Microsoft Exchange system and to analyze the data according to best practices.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Update-ExchangeHelp</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Update-ExchangeHelp cmdlet to find, download and install the latest available help articles for the Exchange Management Shell on the local computer. If an available version is found based your installed version and languages of Exchange, the cmdlet downloads and integrates the updated version of Help in the Exchange Management Shell. This cmdlet is a required substitute for the Update-Help cmdlet that's available in Windows PowerShell.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Cmdlet	Description
<p>Cancel-SensitiveInformationScan</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Cancel-SensitiveInformationScan cmdlet to cancel sensitive information scans.</p>

Cmdlet	Description
	<p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Check-PurviewConfig</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Check-PurviewConfig cmdlet to validate and review your organization's configuration settings in Microsoft Purview.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Disable-JournalArchiving</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Disable-JournalArchiving cmdlet to disable journal archiving for specific users. Microsoft 365 journal archiving uses mailboxes in Exchange Online to record or journal messages for mailboxes in on-premises organizations.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Disable-JournalRule</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Disable-JournalRule cmdlet to disable a journal rule on a Mailbox server.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Disable-OutlookProtectionRule</p>	<p>Note: This cmdlet is no longer supported in the cloud-based service.</p> <p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p>

Cmdlet	Description
	<p>Use the Disable-OutlookProtectionRule cmdlet to disable an existing Microsoft Outlook protection rule.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Disable-TransportRule</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Disable-TransportRule cmdlet to disable transport rules (mail flow rules) in your organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Enable-JournalRule</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Enable-JournalRule cmdlet to enable an existing journal rule on a Mailbox server.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Enable-OutlookProtectionRule</p>	<p>Note: This cmdlet is no longer supported in the cloud-based service.</p> <p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Enable-OutlookProtectionRule cmdlet to enable an existing Outlook protection rule.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
<p>Enable-TransportRule</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Enable-TransportRule cmdlet to enable transport rules (mail flow rules) in your organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Execute-AzureADLabelSync</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Execute-AzureADLabelSync cmdlet to start the synchronization of sensitivity labels into Microsoft Entra ID. This allows the application of sensitivity labels to Microsoft Teams sites, Microsoft 365 Groups, and SharePoint sites. This cmdlet is required if you were using sensitivity labels before September 2019.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Export-JournalRuleCollection</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Export-JournalRuleCollection cmdlet to export the journal rules in your organization to an XML file.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Export-TransportRuleCollection</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Export-TransportRuleCollection cmdlet to export the transport rules in your organization.</p>

Cmdlet	Description
	<p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-AdministrativeUnit</p>	<p>This cmdlet is functional only in the cloud-based service.</p> <p>Use the Get-AdministrativeUnit cmdlet to view administrative units, which are Microsoft Entra containers of resources. You can use administrative units to delegate administrative permissions and apply policies to different groups of users.</p> <p>Note: Administrative units are available only in Microsoft Entra ID P1 or P2. You create and manage administrative units in Microsoft Graph PowerShell.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-AutoSensitivityLabelPolicy</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Get-AutoSensitivityLabelPolicy cmdlet to view auto-labeling policies in your organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-AutoSensitivityLabelRule</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Get-AutoSensitivityLabelPolicy cmdlet to view auto-labeling policy rules in your organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-EtrLimits</p>	<p>This cmdlet is available only in the cloud-based service.</p>

Cmdlet	Description
	<p>Use the Get-EtrLimits cmdlet to show information about mail flow rule (also known as transport rule) limits in Exchange Online, as well the current usage and the largest rule IDs in terms of size and regular expression character count.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-ExoInformationBarrierPolicy</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Get-ExoInformationBarrierPolicy cmdlet to view information barrier policies in your Exchange Online organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-ExoInformationBarrierRelationship</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Get-ExoInformationBarrierRelationship cmdlet to view information barrier relationships in your Exchange Online organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-ExoInformationBarrierSegment</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Get-ExoInformationBarrierSegment to view information barrier segments in your Exchange Online organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-InformationBarrierPoliciesApplicationStatus</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p>

Cmdlet	Description
	<p>Use the <code>Get-InformationBarrierPoliciesApplicationStatus</code> cmdlet to view the application status of information barrier policies.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-InformationBarrierPolicy</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the <code>Get-InformationBarrierPolicy</code> cmdlet to view information barrier policies in the Microsoft Purview compliance portal.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-InformationBarrierRecipientStatus</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the <code>Get-InformationBarrierRecipientStatus</code> cmdlet to return information about recipients and their relationship to information barrier policies.</p> <p>Note: This cmdlet doesn't work with information barriers in non-legacy mode. To determine your current mode, see Check the IB mode for your organization. If you're in non-legacy mode, run the following command to get information about a single recipient: <code>Get-Recipient -Identity <IdentityValue> Format-List Name,*segment*</code>. Similarly, to get the relationship information between two recipients, use the Get-ExoInformationBarrierRelationship cmdlet.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-JournalRule</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be</p>

Cmdlet	Description
	<p>exclusive to one environment or the other.</p> <p>Use the Get-JournalRule cmdlet to view the journal rules in your organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-Label</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Get-Label cmdlet to view sensitivity labels in your organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-LabelPolicy</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Get-LabelPolicy cmdlet to view sensitivity label policies in your organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-MessageClassification</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Get-MessageClassification cmdlet to view existing message classifications in your organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-OrganizationSegment</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security &</p>

Cmdlet	Description
	<p>Compliance PowerShell.</p> <p>Use the Get-OrganizationSegment cmdlet to view organization segments in the Microsoft Purview compliance portal.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-OutlookProtectionRule</p>	<p>Note: This cmdlet is no longer supported in the cloud-based service.</p> <p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Get-OutlookProtectionRule cmdlet to retrieve Microsoft Outlook protection rules configured in an organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-ProtectionAlert</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Get-ProtectionAlert cmdlet to view alert policies in the Microsoft Purview compliance portal.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-ReviewItems</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Get-ReviewItems to retrieve a list of disposition review items that are either pending review or already disposed for a specific retention label. It can also be used to retrieve a list of disposed items for a specific record label.</p> <p>This cmdlet is available only in the Mailbox Import Export role, and by default, the role isn't assigned to any role groups.</p>

Cmdlet	Description
	<p>To use this cmdlet, you need to add the Mailbox Import Export role to a role group (for example, to the Organization Management role group). For more information, see Add a role to a role group.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-SensitiveInformationScan</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Get-SensitiveInformationScan cmdlet to view the properties of sensitive information scans.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-SensitiveInformationScanRule</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Get-SensitiveInformationScanRule cmdlet to view sensitive information scan rules.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-SupervisoryReviewPolicyV2</p>	<p>This cmdlet is functional only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Get-SupervisoryReviewPolicyV2 cmdlet to view supervisory review policies in the Microsoft Purview compliance portal. Supervisory review lets you define policies that capture communications in your organization so they can be examined by internal or external reviewers.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
<p>Get-SupervisoryReviewRule</p>	<p>This cmdlet is functional only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Get-SupervisoryReviewRule cmdlet to modify supervisory review rules in the Microsoft Purview compliance portal. Supervisory review lets you define policies that capture communications in your organization so they can be examined by internal or external reviewers.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-TransportRule</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Get-TransportRule cmdlet to view transport rules (mail flow rules) in your organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-TransportRuleAction</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Get-TransportRuleAction cmdlet to view the actions that are available for transport rules (mail flow rules).</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-TransportRulePredicate</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Get-TransportRulePredicate cmdlet to view the predicates (conditions and exceptions) that are available for transport rules (mal flow rules).</p>

Cmdlet	Description
	<p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Import-JournalRuleCollection</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Import-JournalRuleCollection cmdlet to import journal rules from an XML file. You can import a journal rule collection you previously exported as a backup, or import rules you exported from an older version of Exchange.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Import-TransportRuleCollection</p>	<p>This cmdlet is functional only in on-premises Exchange.</p> <p>Use the Import-TransportRuleCollection cmdlet to import a transport rule collection. You can import a rule collection you previously exported as a backup, or import rules that you've exported from an older version of Exchange.</p> <p>Note: For replacement import functionality in Exchange Online using a PowerShell script, see Import or export a mail flow rule collection in Exchange Online.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Install-UnifiedCompliancePrerequisite</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Install-UnifiedCompliancePrerequisite cmdlet to view, create, or configure the Compliance Policy Center in Microsoft SharePoint. The Compliance Policy Center is a site collection that's used by the Microsoft Purview compliance portal to store preservation policies that act on content in SharePoint sites.</p> <p>Typically, you don't need to run this cmdlet. You use this cmdlet for troubleshooting and diagnostics.</p>

Cmdlet	Description
	<p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Invoke-ComplianceSecurityFilterAction</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Invoke-ComplianceSecurityFilterAction cmdlet to view and set compliance boundaries for Microsoft OneDrive sites in cloud-based organizations.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-AutoSensitivityLabelPolicy</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the New-AutoSensitivityLabelPolicy cmdlet to create auto-labeling policies in your organization. Create auto-labeling policy rules using the New-AutoSensitivityLabelRule cmdlet and associate them with the policy to complete the policy creation.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-AutoSensitivityLabelRule</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the New-AutoSensitivityLabelRule cmdlet to create auto-labeling rules and associate them with auto-labeling policies in your organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-InformationBarrierPolicy</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security &</p>

Cmdlet	Description
	<p>Compliance PowerShell.</p> <p>Use the New-InformationBarrierPolicy cmdlet to create information barrier policies in the Microsoft Purview compliance portal.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-JournalRule</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the New-JournalRule cmdlet to create a journal rule in your organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-Label</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the New-Label cmdlet to create sensitivity labels in your organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-LabelPolicy</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the New-LabelPolicy cmdlet to create sensitivity label policies in your organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
<p>New-MessageClassification</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the New-MessageClassification cmdlet to create a message classification instance in your organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-OrganizationSegment</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the New-OrganizationSegment cmdlet to create organization segments for use with information barrier policies in the Microsoft Purview compliance portal. Organization Segments are not in effect until you apply information barrier policies.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-OutlookProtectionRule</p>	<p>Note: This cmdlet is no longer supported in the cloud-based service.</p> <p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the New-OutlookProtectionRule cmdlet to create a Microsoft Outlook protection rule.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-ProtectionAlert</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p>

Cmdlet	Description
	<p>Use the New-ProtectionAlert cmdlet to create alert policies in the Microsoft Purview compliance portal and the Microsoft Defender portal. Alert policies contain conditions that define the user activities to monitor, and the notification options for email alerts and entries.</p> <p>Note</p> <p>Although the cmdlet is available, you receive the following error if you don't have an enterprise license:</p> <p><i>Creating advanced alert policies requires an Office 365 E5 subscription or Office 365 E3 subscription with an Office 365 Threat Intelligence or Office 365 EquivioAnalytics add-on subscription for your organization. With your current subscription, only single event alerts can be created.</i></p> <p>You can bypass this error by specifying <code>-AggregationType None</code> and an <code>-Operation</code> within the command.</p> <p>For more information, see Alert policies in Microsoft 365.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-SensitiveInformationScan</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the New-SensitiveInformationScan cmdlet to create new on-demand classification scans. Learn more about on-demand classifications at On-demand classification.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-SensitiveInformationScanRule</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the New-SensitiveInformationScan cmdlet to create sensitive information scan rules.</p>

Cmdlet	Description
	<p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-SupervisoryReviewPolicyV2</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the New-SupervisoryReviewPolicyV2 cmdlet to create supervisory review policies in the Microsoft Purview compliance portal. Supervisory review lets you define policies that capture communications in your organization so they can be examined by internal or external reviewers.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-SupervisoryReviewRule</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the New-SupervisoryReviewRule cmdlet to create supervisory review rules in the Microsoft Purview compliance portal. Supervisory review lets you define policies that capture communications in your organization so they can be examined by internal or external reviewers.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-TransportRule</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the New-TransportRule cmdlet to create transport rules (mail flow rules) in your organization.</p> <p>Note:</p> <ul style="list-style-type: none"> The action of a rule without conditions or exceptions is applied to all messages, which could have unintended consequences. For example, if the rule

Cmdlet	Description
	<p>action deletes messages, the rule without conditions or exceptions might delete all inbound and outbound messages for the entire organization.</p> <ul style="list-style-type: none"> Rules that use Active Directory or Microsoft Entra ID properties as conditions or exceptions work only on senders or recipients in the organization. <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-AutoSensitivityLabelPolicy</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Remove-AutoSensitivityLabelPolicy cmdlet to remove auto-labeling policies from your organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-AutoSensitivityLabelRule</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Remove-AutoSensitivityLabelPolicy cmdlet to remove auto-labeling policy rules from your organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
<p>Remove-InformationBarrierPolicy</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Remove-InformationBarrierPolicy cmdlet to remove information barrier policies from the Microsoft Purview compliance portal.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-JournalRule</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Remove-JournalRule cmdlet to remove an existing journal rule.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-Label</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Remove-Label cmdlet to remove sensitivity labels from your organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
<p>Remove-LabelPolicy</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Remove-LabelPolicies cmdlet to remove sensitivity label policies from your organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-MessageClassification</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Remove-MessageClassification cmdlet to delete an existing message classification instance from your organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-OrganizationSegment</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Remove-OrganizationSegment cmdlet to remove organization segments from the Microsoft Purview compliance portal.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-OutlookProtectionRule</p>	<p>Note: This cmdlet is no longer supported in the cloud-based service.</p> <p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p>

Cmdlet	Description
	<p>Use the Remove-OutlookProtectionRule cmdlet to remove Outlook protection rules.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-ProtectionAlert</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Remove-ProtectionAlert cmdlet to remove alert policies from the Microsoft Purview compliance portal.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-SensitiveInformationScan</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Remove-SensitiveInformationScan cmdlet to delete on-demand classification scans. You can't delete a scan if estimation or classification is in progress.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-SensitiveInformationScanRule</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Remove-SensitiveInformationScanRule cmdlet to delete on-demand classification scan rules. You can't delete a rule when a parent scan is in the ClassificationInProgress or ClassificationComplete state.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
<p>Remove-SupervisoryReviewPolicyV2</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Remove-SupervisoryReviewPolicyV2 cmdlet to remove supervisory review policies from the Microsoft Purview compliance portal.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-TransportRule</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Remove-TransportRule cmdlet to remove transport rules (mail flow rules) from your organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-AutoSensitivityLabelPolicy</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Set-AutoSensitivityLabelPolicy cmdlet to modify auto-labeling policies in your organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
<p>Set-AutoSensitivityLabelRule</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Set-AutoSensitivityLabelPolicy cmdlet to modify auto-labeling policy rules in your organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-InformationBarrierPolicy</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Set-InformationBarrierPolicy cmdlet to modify information barrier policies in the Microsoft Purview compliance portal.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-JournalRule</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Set-JournalRule cmdlet to modify an existing journal rule in your organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
<p>Set-Label</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Set-Label cmdlet to modify sensitivity labels in your organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-LabelPolicy</p>	<p>This cmdlet is functional only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Set-Label cmdlet to modify sensitivity label policies in your organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-MessageClassification</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Set-MessageClassification cmdlet to configure an existing message classification instance in your organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-OrganizationSegment</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Set-OrganizationSegment cmdlet to modify organization segments in the Microsoft Purview compliance portal. Organization Segments are not in effect until you apply information barrier policies.</p>

Cmdlet	Description
	<p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-OutlookProtectionRule</p>	<p>Note: This cmdlet is no longer supported in the cloud-based service.</p> <p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Set-OutlookProtectionRule cmdlet to modify an existing Microsoft Outlook protection rule.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-ProtectionAlert</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Set-ProtectionAlert cmdlet to modify alert policies in the Microsoft Purview compliance portal.</p> <p>Note: You can't use this cmdlet to edit default alert policies. You can only modify alerts that you created using the New-ProtectionAlert cmdlet.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-SensitiveInformationScan</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Set-SensitiveInformationScan cmdlet to modify on-demand classification scans.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
<p>Set-SensitiveInformationScanRule</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Set-SensitiveInformationScan cmdlet to modify sensitive information scan rules.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-SupervisoryReviewPolicyV2</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Set-SupervisoryReviewPolicyV2 cmdlet to modify supervisory review policies in the Microsoft Purview compliance portal.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-SupervisoryReviewRule</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Set-SupervisoryReviewRule cmdlet to modify supervisory review rules in the Microsoft Purview compliance portal.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-TransportRule</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Set-TransportRule cmdlet to modify existing transport rules (mail flow rules) in your organization.</p> <p>Note:</p>

Cmdlet	Description
	<ul style="list-style-type: none"> • The action of a rule without conditions or exceptions is applied to all messages, which could have unintended consequences. For example, if the rule action deletes messages, the rule without conditions or exceptions might delete all inbound and outbound messages for the entire organization. • Rules that use Active Directory or Microsoft Entra ID properties as conditions or exceptions work only on senders or recipients in the organization. <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Start-InformationBarrierPoliciesApplication</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Start-InformationBarrierPoliciesApplication cmdlet to apply active information barrier policies in the Microsoft Purview compliance portal.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Stop-InformationBarrierPoliciesApplication</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Stop-InformationBarrierPoliciesApplication cmdlet to stop the process of applying information barrier policies in the Microsoft Purview compliance portal.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Test-ArchiveConnectivity</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p>

Cmdlet	Description
	<p>Use the Test-ArchiveConnectivity cmdlet to verify archive functionality for a mailbox user.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Cmdlet	Description
<p>Get-AdminAuditLogConfig</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Get-AdminAuditLogConfig cmdlet to view the administrator audit logging configuration settings.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-AuditConfig</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Get-AuditConfig cmdlet to view the auditing configuration in the Microsoft Purview compliance portal.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-AuditLogSearch</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Get-AuditLogSearch cmdlet to return a list of current audit log searches that were created with the New-AdminAuditLogSearch or New-MailboxAuditLogSearch cmdlets. The Get-AuditLogSearch cmdlet also returns audit log searches that are initiated whenever an administrator uses the Exchange admin center (EAC) to export audit logs.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
<p>Get-MailboxAuditBypassAssociation</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Get-MailboxAuditBypassAssociation cmdlet to retrieve information about the AuditBypassEnabled property value for user accounts (on-premises Exchange and the cloud) and computer accounts (on-premises Exchange only). You use the Set-MailboxAuditBypassAssociation cmdlet to enable this property to bypass mailbox audit logging.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-UnifiedAuditLogRetentionPolicy</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Get-UnifiedAuditLogRetentionPolicy cmdlet to view the properties of the audit log retention policies in the Microsoft Defender portal or the Microsoft Purview compliance portal.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-AdminAuditLogSearch</p>	<p>Note</p> <p>This cmdlet will be deprecated in the cloud-based service. To access audit log data, use the Search-UnifiedAuditLog cmdlet. For more information, see this blog post: https://aka.ms/AdminAuditCmdletBlog.</p> <p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the New-AdminAuditLogSearch cmdlet to search the contents of the administrator audit log and send the results to one or more mailboxes that you specify.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
New-MailboxAuditLogSearch	<p>Note</p> <p>This cmdlet will be deprecated in the cloud-based service. To access audit log data, use the Search-UnifiedAuditLog cmdlet. For more information, see this blog post: https://aka.ms/AuditCmdletBlog.</p> <p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the New-MailboxAuditLogSearch cmdlet to search mailbox audit logs and have search results sent via email to specified recipients.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
New-UnifiedAuditLogRetentionPolicy	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the New-UnifiedAuditLogRetentionPolicy cmdlet to create audit log retention policies in the Microsoft Defender portal or the Microsoft Purview compliance portal.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Remove-UnifiedAuditLogRetentionPolicy	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Remove-UnifiedAuditLogRetentionPolicy cmdlet to delete audit log retention policies from the Microsoft Defender portal or the Microsoft Purview compliance portal.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Search-AdminAuditLog	<p>Note</p> <p>This cmdlet will be deprecated in the cloud-based service. To access audit log data, use the Search-UnifiedAuditLog cmdlet. For more information, see this blog post: https://aka.ms/AdminAuditCmdletBlog.</p>

Cmdlet	Description
	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Search-AdminAuditLog cmdlet to search the contents of the administrator audit log. Administrator audit logging records when a user or administrator makes a change in your organization (in the Exchange admin center or by using cmdlets).</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Search-MailboxAuditLog</p>	<p>Note</p> <p>This cmdlet will be deprecated in the cloud-based service. To access audit log data, use the Search-UnifiedAuditLog cmdlet. For more information, see this blog post: https://aka.ms/AuditCmdletBlog.</p> <p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Search-MailboxAuditLog cmdlet to search mailbox audit log entries matching the specified search terms.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Search-UnifiedAuditLog</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Search-UnifiedAuditLog cmdlet to search the unified audit log. This log contains events from Exchange Online, SharePoint, OneDrive, Microsoft Entra ID, Microsoft Teams, Power BI, and other Microsoft 365 services. You can search for all events in a specified date range, or you can filter the results based on specific criteria, such as the user who performed the action, the action, or the target object.</p> <p>Note: By default, this cmdlet returns a subset of results containing up to 100 records. Use SessionCommand parameter with the ReturnLargeSet value to exhaustively search up to 50,000 results. The SessionCommand parameter causes the cmdlet to return unsorted data.</p>

Cmdlet	Description
	<p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-AdminAuditLogConfig</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Set-AdminAuditLogConfig cmdlet to configure the administrator audit logging configuration settings.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-AuditConfig</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Set-AuditConfig cmdlet to configure the auditing configuration in the Microsoft Purview compliance portal.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-MailboxAuditBypassAssociation</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Set-MailboxAuditBypassAssociation cmdlet to configure mailbox audit logging bypass for user or computer accounts such as service accounts for applications that access mailboxes frequently.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-UnifiedAuditLogRetentionPolicy</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Set-UnifiedAuditLogRetentionPolicy cmdlet to modify audit log retention policies in the Microsoft Defender portal or the Microsoft Purview compliance portal.</p>

Cmdlet	Description
	<p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Write-AdminAuditLog</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Write-AdminAuditLog cmdlet to write a comment to the administrator audit log.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Cmdlet	Description
<p>Get-ComplianceSearch</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Get-ComplianceSearch cmdlet to view estimate compliance searches in Exchange Server 2016 or later and in the Microsoft Purview compliance portal. After you use the New-ComplianceSearchAction cmdlet to define a preview action for the compliance search, use the Get-ComplianceSearchAction cmdlet to view the results of the compliance search.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-ComplianceSearchAction</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Get-ComplianceSearchAction cmdlet to view information about compliance search actions.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
Get-ComplianceSecurityFilter	<p>This cmdlet is functional only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Get-ComplianceSecurityFilter cmdlet to view compliance security filters in the Microsoft Purview compliance portal. These filters allow specified users to search only a subset of mailboxes and SharePoint or OneDrive sites in your Microsoft 365 organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Get-MailboxSearch	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Get-MailboxSearch cmdlet to view mailbox searches that are in progress, complete or stopped.</p> <p>Note: As of October 2020, the *-MailboxSearch cmdlets are retired in Exchange Online PowerShell. Use the *-ComplianceSearch cmdlets in Security & Compliance PowerShell instead. For more information, see Retirement of legacy eDiscovery tools.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Invoke-ComplianceSearchActionStep	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>This cmdlet is reserved for internal Microsoft use.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
New-ComplianceSearch	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p>

Cmdlet	Description
	<p>Use the New-ComplianceSearch cmdlet to create compliance searches in Exchange Server 2016 or later and in the Microsoft Purview compliance portal. You use this cmdlet to define the search criteria.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-ComplianceSearchAction</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the New-ComplianceSearchAction cmdlet to create actions for content searches in Exchange Server and in Microsoft Purview.</p> <p>Note: Several of the parameters on this cmdlet are functional only in on-premises Exchange. For more information, see May 2025 changes to Microsoft Purview eDiscovery.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-ComplianceSecurityFilter</p>	<p>This cmdlet is functional only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the New-ComplianceSecurityFilter cmdlet to create compliance security filters in the Microsoft Purview compliance portal. These filters allow specified users to search only a subset of mailboxes and SharePoint or OneDrive sites in your Microsoft 365 organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-MailboxSearch</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the New-MailboxSearch cmdlet to create a mailbox search and either get an estimate of search results, place search results on In-Place Hold or copy them to a Discovery mailbox. You can also place all contents in a mailbox on hold by not specifying a search query, which accomplishes similar results as Litigation Hold.</p>

Cmdlet	Description
	<p>Note: As of October 2020, the *-MailboxSearch cmdlets are retired in Exchange Online PowerShell. Use the *-ComplianceSearch cmdlets in Security & Compliance PowerShell instead. For more information, see Retirement of legacy eDiscovery tools.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-ComplianceSearch</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Remove-ComplianceSearch cmdlet to remove compliance searches from Exchange Server 2016 and from the Microsoft Purview compliance portal. The searches must be stopped or completed.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-ComplianceSearchAction</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Remove-ComplianceSearch cmdlet to remove compliance search actions from the Microsoft Purview compliance portal.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-ComplianceSecurityFilter</p>	<p>This cmdlet is functional only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Remove-ComplianceSecurityFilter cmdlet to remove compliance security filters from the Microsoft Purview compliance portal.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-MailboxSearch</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p>

Cmdlet	Description
	<p>Use the Remove-MailboxSearch cmdlet to remove a mailbox search.</p> <p>Note: As of October 2020, the *-MailboxSearch cmdlets are retired in Exchange Online PowerShell. Use the *-ComplianceSearch cmdlets in Security & Compliance PowerShell instead. For more information, see Retirement of legacy eDiscovery tools.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-ComplianceSearch</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Set-ComplianceSearch cmdlet to modify non-running compliance searches in Exchange Server 2016 or later and in the Microsoft Purview compliance portal.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-ComplianceSearchAction</p>	<p>This cmdlet is functional only in on-premises Exchange. For more information, see May 2025 changes to Microsoft Purview eDiscovery.</p> <p>Use the Set-ComplianceSearchAction cmdlet to change the export key on export compliance search actions in on-premises Exchange.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-ComplianceSecurityFilter</p>	<p>This cmdlet is functional only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Set-ComplianceSecurityFilter cmdlet to modify compliance security filters in the Microsoft Purview compliance portal.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
Set-MailboxSearch	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Set-MailboxSearch cmdlet to modify an existing mailbox search.</p> <p>Note: As of October 2020, the *-MailboxSearch cmdlets are retired in Exchange Online PowerShell. Use the *-ComplianceSearch cmdlets in Security & Compliance PowerShell instead. For more information, see Retirement of legacy eDiscovery tools.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Start-ComplianceSearch	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Start-ComplianceSearch cmdlet to start stopped, completed or not started compliance searches in Exchange Server 2016 or later and in the Microsoft Purview compliance portal.</p> <p>Note</p> <p>In the cloud, this cmdlet has the following requirements:</p> <ul style="list-style-type: none"> • Version 3.9.0 or later of the Exchange Online PowerShell module (August 2025). • Use the <i>EnableSearchOnlySession</i> parameter when you run the Connect-IPPSSession command to connect to Security & Compliance PowerShell. <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Start-MailboxSearch	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Start-MailboxSearch cmdlet to restart or resume a mailbox search that's been stopped.</p>

Cmdlet	Description
	<p>Note: As of October 2020, the *-MailboxSearch cmdlets are retired in Exchange Online PowerShell. Use the *-ComplianceSearch cmdlets in Security & Compliance PowerShell instead. For more information, see Retirement of legacy eDiscovery tools.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Stop-ComplianceSearch</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Stop-ComplianceSearch cmdlet to stop running compliance searches in Exchange Server 2016 or later and in the Microsoft Purview compliance portal.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Stop-MailboxSearch</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Stop-MailboxSearch cmdlet to stop a mailbox search that's in progress.</p> <p>Note: As of October 2020, the *-MailboxSearch cmdlets are retired in Exchange Online PowerShell. Use the *-ComplianceSearch cmdlets in Security & Compliance PowerShell instead. For more information, see Retirement of legacy eDiscovery tools.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Cmdlet	Description
<p>Export-ActivityExplorerData</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p>

Cmdlet	Description
	<p>Use the Export-ActivityExplorerData cmdlet to export activities from Data classification > Activity Explorer in the Microsoft 365 Purview compliance portal. Activity explorer reports on up to 30 days worth of data.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Export-DlpPolicyCollection</p>	<p>Note: This cmdlet is retired from the cloud-based service. For more information, see this blog post.</p> <p>This cmdlet is functional only in on-premises Exchange.</p> <p>Use the Export-DlpPolicyCollection cmdlet to export data loss prevention (DLP) policy collections that are based on transport rules (mail flow rules) from your organization to a file.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-ClassificationRuleCollection</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Get-ClassificationRuleCollection cmdlet to view the classification rule collections in your organization.</p> <p>In the Microsoft Purview compliance portal, use the Get-DlpSensitiveInformationTypeRulePackage cmdlet.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-DataClassification</p>	<p>This cmdlet is functional only in on-premises Exchange.</p> <p>In Exchange Online, this cmdlet is replaced by the Get-DlpSensitiveInformationType cmdlet in Security & Compliance PowerShell.</p> <p>Use the Get-DataClassification cmdlet to view the data classification rules in your organization. This cmdlet shows</p>

Cmdlet	Description
	<p>built-in data classification rules and rules that you created that use document fingerprints.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-DataClassificationConfig</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Get-DataClassificationConfig cmdlet to view the data classification configuration for your organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-DlpCompliancePolicy</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Get-DlpCompliancePolicy to view data loss prevention (DLP) policies in the Microsoft Purview compliance portal.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-DlpComplianceRule</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Get-DlpComplianceRule to view data loss prevention (DLP) rules in the Microsoft Purview compliance portal. DLP rules identify and protect sensitive information.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-DlpDetailReport</p>	<p>Note: This cmdlet is retired. Use the Export-ActivityExplorerData cmdlet to view DLP information. Data from Export-ActivityExplorerData is the same as the retired Get-DlpIncidentDetailReport cmdlet.</p>

Cmdlet	Description
	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Get-DlpDetailReport cmdlet to list details about data loss prevention (DLP) rule matches for Exchange Online, SharePoint, and OneDrive in your cloud-based organization for the last 30 days.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-DlpDetectionsReport</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Note: This cmdlet will be retired. Use the Export-ActivityExplorerData cmdlet to view DLP information. Data from Export-ActivityExplorerData is the same as the retired Get-DlpIncidentDetailReport cmdlet.</p> <p>Use the Get-DlpDetectionsReport cmdlet to list a summary of data loss prevention (DLP) rule matches for Exchange Online, SharePoint and OneDrive in your cloud-based organization for the last 30 days.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-DlpEdmSchema</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Get-DlpEdmSchema cmdlet to view exact data match (EDM) data loss prevention (DLP) schemas in the Microsoft Purview compliance portal.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-DlpIncidentDetailReport</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Note: This cmdlet will be retired. Use the Export-ActivityExplorerData instead.</p>

Cmdlet	Description
	<p>Use the Get-DlpIncidentDetailReport cmdlet to view the details of incidents that happened in the last 30 days.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-DlpKeywordDictionary</p>	<p>This cmdlet is functional only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Get-DlpKeywordDictionary cmdlet to view data loss prevention (DLP) keyword dictionaries in the Microsoft Purview compliance portal.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-DlpPolicy</p>	<p>Note: This cmdlet is retired from the cloud-based service. For more information, see this blog post. Use the Get-DlpCompliancePolicy and Get-DlpComplianceRule cmdlets instead.</p> <p>This cmdlet is functional only in on-premises Exchange.</p> <p>Use the Get-DlpPolicy cmdlet to view existing data loss prevention (DLP) policies that are based on transport rules (mail flow rules) in your organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
Get-DlpPolicyTemplate	<p>Note: This cmdlet is retired from the cloud-based service. For more information, see this blog post.</p> <p>This cmdlet is functional only in on-premises Exchange.</p> <p>Use the Get-DlpPolicyTemplate cmdlet to view existing data loss prevention (DLP) policy templates that are based on transport rules (mail flow rules) in your Exchange organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Get-DlpSensitiveInformationType	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Get-DlpSensitiveInformationType cmdlet to list the sensitive information types that are defined for your organization in the Microsoft Purview compliance portal. Sensitive information types are used by data loss prevention (DLP) rules to check for sensitive information such as social security, passport, or credit card numbers.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Get-DlpSensitiveInformationTypeRulePackage	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Get-DlpSensitiveInformationTypeRulePackage cmdlet to view data loss prevention (DLP) sensitive information type rule packages in the Microsoft Purview compliance portal.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Get-DlpSiDetectionsReport	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p>

Cmdlet	Description
	<p>Note: This cmdlet will be retired. Use the Export-ActivityExplorerData cmdlet to view DLP information. Data from Export-ActivityExplorerData is the same as the retired Get-DlpIncidentDetailReport cmdlet.</p> <p>Use the Get-DlpSiDetectionsReport cmdlet to view information about data loss prevention (DLP) sensitive information type detections in the Microsoft Purview compliance portal for the last 90 days.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-PolicyConfig</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Get-PolicyConfig cmdlet to view the endpoint restrictions that are configured in the organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-PolicyTipConfig</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Get-PolicyTipConfig cmdlet to view the data loss prevention (DLP) Policy Tips in your organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Import-DlpPolicyCollection</p>	<p>Note: This cmdlet is retired from the cloud-based service. For more information, see this blog post.</p> <p>This cmdlet is functional only in on-premises Exchange.</p> <p>Use the Import-DlpPolicyCollection cmdlet to import data loss prevention (DLP) policy collections that are based on transport rules (mail flow rules) into your organization.</p>

Cmdlet	Description
	<p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Import-DlpPolicyTemplate</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Import-DlpPolicyTemplate cmdlet to import data loss prevention (DLP) policy template files that are based on transport rules (mail flow rules) into your Exchange organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-ClassificationRuleCollection</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the New-ClassificationRuleCollection cmdlet to import new classification rule collections into your organization.</p> <p>In tSecurity & Compliance PowerShell, use the New-DlpSensitiveInformationTypeRulePackage cmdlet.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-DataClassification</p>	<p>This cmdlet is functional only in on-premises Exchange.</p> <p>In Exchange Online, this cmdlet is replaced by the New-DlpSensitiveInformationType cmdlet in Security & Compliance PowerShell.</p> <p>Use the New-DataClassification cmdlet to create data classification rules that use document fingerprints.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-DlpCompliancePolicy</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance</p>

Cmdlet	Description
	<p>PowerShell.</p> <p>Use the New-DlpCompliancePolicy cmdlet to create data loss prevention (DLP) policies in the Microsoft Purview compliance portal. DLP policies contain DLP rules that identify, monitor, and protect sensitive information.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-DlpComplianceRule</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the New-DlpComplianceRule to create data loss prevention (DLP) rules in the Microsoft Purview compliance portal. DLP rules define sensitive information to be protected and the actions to take on rule matches.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-DlpEdmSchema</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the New-DlpEdmSchema cmdlet to create exact data match (EDM)-based classification schemas in the Microsoft Purview compliance portal. Such schemas can be used with data loss prevention (DLP) policies.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-DlpFingerprint</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the New-DlpFingerprint cmdlet to create document fingerprints that are used with data loss prevention (DLP) sensitive information types in the Microsoft Purview</p>

Cmdlet	Description
	<p>compliance portal. Because the results of New-DlpFingerprint aren't stored outside of the sensitive information type, you always run New-DlpFingerprint and New-DlpSensitiveInformationType or Set-DlpSensitiveInformationType in the same PowerShell session.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-DlpKeywordDictionary</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the New-DlpKeywordDictionary cmdlet to create data loss prevention (DLP) keyword dictionaries in the Microsoft Purview compliance portal.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-DlpPolicy</p>	<p>Note: This cmdlet is retired from the cloud-based service. For more information, see this blog post. Use the New-DlpCompliancePolicy and New-DlpComplianceRule cmdlets instead.</p> <p>This cmdlet is functional only in on-premises Exchange.</p> <p>Use the New-DlpPolicy cmdlet to create data loss prevention (DLP) policies that are based on transport rules (mail flow rules) in your organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-DlpSensitiveInformationType</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the New-DlpSensitiveInformationType cmdlet to create sensitive information type rules that use document fingerprints.</p>

Cmdlet	Description
	<p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-DlpSensitiveInformationTypeRulePackage</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the New-DlpSensitiveInformationTypeConfig cmdlet to import data loss prevention (DLP) sensitive information type rule packages in the Microsoft Purview compliance portal.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-Fingerprint</p>	<p>This cmdlet is functional only in on-premises Exchange.</p> <p>Note: In Exchange Online, this cmdlet is replaced by the New-DlpFingerPrint cmdlet in Security & Compliance PowerShell.</p> <p>Use the New-Fingerprint cmdlet to create document fingerprints that are used with data classification rules. Because the results of New-Fingerprint are not stored outside of the data classification rule, you always run New-Fingerprint and New-DataClassification or Set-DataClassification in the same PowerShell session.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-PolicyTipConfig</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Set-PolicyTipConfig cmdlet to create custom Policy Tips in your organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
<p>Remove-ClassificationRuleCollection</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Remove-ClassificationRuleCollection to remove classification rule collections from your organization.</p> <p>In Security & Compliance PowerShell, use the Remove-DlpSensitiveInformationTypeRulePackage cmdlet.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-DataClassification</p>	<p>This cmdlet is functional only in on-premises Exchange.</p> <p>In Exchange Online, this cmdlet is replaced by the Remove-DlpSensitiveInformationType cmdlet in Security & Compliance PowerShell.</p> <p>Use the Remove-DataClassification cmdlet to remove data classification rules that use document fingerprints. You can't use this cmdlet to remove built-in data classification rules.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-DlpCompliancePolicy</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Remove-DlpCompliancePolicy cmdlet to remove data loss prevention (DLP) policies from the Microsoft Purview compliance portal.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-DlpComplianceRule</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p>

Cmdlet	Description
	<p>Use the Remove-DlpComplianceRule cmdlet to remove Data Loss Prevention (DLP) rules from the Microsoft Purview compliance portal.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-DlpEdmSchema</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Remove-DlpEdmSchema cmdlet to remove exact data match (EDM) data loss prevention (DLP) schemas from the Microsoft Purview compliance portal.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-DlpKeywordDictionary</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Remove-DlpKeywordDictionary cmdlet to remove data loss prevention (DLP) keyword dictionaries from the Microsoft Purview compliance portal.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-DlpPolicy</p>	<p>Note: This cmdlet is retired from the cloud-based service. For more information, see this blog post. Use the Remove-DlpCompliancePolicy and Remove-DlpComplianceRule cmdlets instead.</p> <p>This cmdlet is functional only in on-premises Exchange.</p> <p>Use the Remove-DlpPolicy cmdlet to remove existing data loss prevention (DLP) policies that are based on transport rules (mail flow rules) from your organization.</p>

Cmdlet	Description
	<p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-DlpPolicyTemplate</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Remove-DlpPolicyTemplate cmdlet to remove data loss prevention (DLP) policy templates that are based on transport rules (mail flow rules) from your organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-DlpSensitiveInformationType</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Remove-DlpSensitiveInformationType cmdlet to remove sensitive information type rules that use document fingerprints. You can't use this cmdlet to remove built-in sensitive information type rules.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-DlpSensitiveInformationTypeRulePackage</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Remove-DlpSensitiveInformationTypeConfig cmdlet to remove data loss prevention (DLP) sensitive information type rule packages from the Microsoft Purview compliance portal.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-PolicyTipConfig</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p>

Cmdlet	Description
	<p>Use the Remove-PolicyTipConfig cmdlet to remove custom data loss prevention (DLP) Policy Tips from your organization. You can't remove built-in Policy Tips.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-ClassificationRuleCollection</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Set-ClassificationRuleCollection cmdlet to update existing classification rule collections in your organization.</p> <p>In the Microsoft Purview compliance portal, use the Set-DlpSensitiveInformationTypeRulePackage cmdlet.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-DataClassification</p>	<p>This cmdlet is functional only in on-premises Exchange.</p> <p>In Exchange Online, this cmdlet is replaced by the Set-DlpSensitiveInformationType cmdlet in Security & Compliance PowerShell.</p> <p>Use the Set-DataClassification cmdlet to modify data classification rules that use document fingerprints.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
Set-DlpCompliancePolicy	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Set-DlpCompliancePolicy cmdlet to modify data loss prevention (DLP) policies in the Microsoft Purview compliance portal.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Set-DlpComplianceRule	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Set-DlpComplianceRule to modify data loss prevention (DLP) rules in the Microsoft Purview compliance portal. DLP rules define sensitive information to be protected and the actions to take on rule violations.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Set-DlpEdmSchema	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Set-DlpEdmSchema cmdlet to modify exact data match (EDM) data loss prevention (DLP) schemas in the Microsoft Purview compliance portal.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Set-DlpKeywordDictionary	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Set-DlpKeywordDictionary cmdlet to modify data loss prevention (DLP) keyword dictionaries in the Microsoft</p>

Cmdlet	Description
	<p>Purview compliance portal.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-DlpPolicy</p>	<p>Note: This cmdlet is retired from the cloud-based service. For more information, see this blog post. Use the Set-DlpCompliancePolicy and Set-DlpComplianceRule cmdlets instead.</p> <p>This cmdlet is functional only in on-premises Exchange.</p> <p>Use the Set-DlpPolicy cmdlet to modify data loss prevention (DLP) policies that are based on transport rules (mail flow rules) in your organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-DlpSensitiveInformationType</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Set-DlpSensitiveInformationType cmdlet to modify sensitive information type rules that use document fingerprints.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-DlpSensitiveInformationTypeRulePackage</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Set-DlpSensitiveInformationTypeRulePackage cmdlet to update existing data loss prevention (DLP) sensitive information type rule packages in the Microsoft Purview compliance portal.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
<p>Set-PolicyConfig</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Set-PolicyConfig cmdlet to modify the endpoint restrictions that are configured in the organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-PolicyTipConfig</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Set-PolicyTipConfig cmdlet to modify custom Policy Tips in your organization. You can't modify built-in Policy Tips.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Test-DataClassification</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Test-DataClassification cmdlet to find the confidence and count of a sensitive information type that's found in a specified text string.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Test-TextExtraction</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Test-TextExtraction cmdlet to return the text from unencrypted email message files.</p>

Cmdlet	Description
	<p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Cmdlet	Description
<p>Add-ComplianceCaseMember</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Add-ComplianceCaseMember cmdlet to add an individual member to an eDiscovery case in the Microsoft Purview compliance portal. To replace all existing members, use the Update-ComplianceCaseMember cmdlet.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Add-eDiscoveryCaseAdmin</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Add-eDiscoveryCaseAdmin cmdlet to add an eDiscovery Administrator in the Microsoft Purview compliance portal. To replace all existing eDiscovery Administrators, use the Update-eDiscoveryCaseAdmin cmdlet.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-CaseHoldPolicy</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Get-CaseHoldPolicy to view existing case hold policies in the Microsoft Purview compliance portal. To get relevant information about how the hold was applied and the affected locations, you need to include the DistributionDetail switch.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-CaseHoldRule</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p>

Cmdlet	Description
	<p>Use the Get-CaseHoldRule to view case hold rules in the Microsoft Purview compliance portal.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-ComplianceCase</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Get-ComplianceCase cmdlet to different types of compliance cases in the Microsoft Purview compliance portal. See the CaseType parameter for a list of these case types.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-ComplianceCaseMember</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Get-ComplianceCaseMember cmdlet to view the members of eDiscovery cases in the Microsoft Purview compliance portal.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-eDiscoveryCaseAdmin</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Get-eDiscoveryCaseAdmin cmdlet to view eDiscovery Administrators in the Microsoft Purview compliance portal. An eDiscovery Administrator is member of the eDiscovery Manager role group who can also view and access all eDiscovery cases in your organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-CaseHoldPolicy</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p>

Cmdlet	Description
	<p>Use the New-CaseHoldPolicy cmdlet to create new case hold policies in the Microsoft Purview compliance portal.</p> <p>Note</p> <p>This cmdlet causes a full synchronization across your organization, which is a significant operation. If you need to create multiple policies, wait until the policy distribution is successful before running the cmdlet again for the next policy. For information about the distribution status, see Get-CaseHoldPolicy.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-CaseHoldRule</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the New-CaseHoldRule cmdlet to create new case hold rules in the Microsoft Purview compliance portal.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-ComplianceCase</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the New-ComplianceCase cmdlet to create eDiscovery cases in the Microsoft Purview compliance portal. You use eDiscovery cases to place content locations on hold, perform Content Searches associated with the case, and export search results.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-CaseHoldPolicy</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Remove-CaseHoldPolicy cmdlet to remove case hold policies from the Microsoft Purview compliance portal.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
Remove-CaseHoldRule	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Remove-CaseHoldRule cmdlet to remove case hold rules from the Microsoft Purview compliance portal.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Remove-ComplianceCase	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Remove-ComplianceCase cmdlet to remove compliance cases from the Microsoft Purview compliance portal or the Microsoft Purview compliance portal.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Remove-ComplianceCaseMember	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Remove-ComplianceCaseMember cmdlet to remove a single member from an eDiscovery search in Security & Compliance. To replace all existing members, use the Update-ComplianceCaseMember cmdlet.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Remove-eDiscoveryCaseAdmin	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Remove-eDiscoveryCaseAdmin cmdlet to remove an eDiscovery Administrator from the Microsoft Purview compliance portal. To replace all eDiscovery Administrators, use the Update-eDiscoveryCaseAdmin cmdlet.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
Set-CaseHoldPolicy	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Set-CaseHoldPolicy cmdlet to modify existing case hold policies in the Microsoft Purview compliance portal.</p> <p>Note: Running this cmdlet causes a full synchronization across your organization, which is a significant operation. If you need to update multiple policies, wait until the policy distribution is successful before running the cmdlet again for the next policy. If you need to update a policy multiple times, make all changes in a single call of the cmdlet. For information about the distribution status, see Get-CaseHoldPolicy.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Set-CaseHoldRule	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Set-CaseHoldRule cmdlet to modify existing case hold rules in the Microsoft Purview compliance portal.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Set-ComplianceCase	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Set-ComplianceCase cmdlet to modify eDiscovery cases in the Microsoft Purview compliance portal.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Update-ComplianceCaseMember	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Update-ComplianceCaseMember cmdlet to replace all members of eDiscovery cases in the Microsoft Purview compliance portal. To add or remove</p>

Cmdlet	Description
	<p>existing members, use the Add-ComplianceCaseMember and Remove-ComplianceCaseMember cmdlets.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Update-eDiscoveryCaseAdmin</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Update-eDiscoveryCaseAdmin cmdlet to replace all existing eDiscovery Administrators in the Microsoft Purview compliance portal. To add or remove individual eDiscovery Administrators, use the Add-eDiscoveryCaseAdmin and Remove-eDiscoveryCaseAdmin cmdlets.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Cmdlet	Description
<p>Enable-ComplianceTagStorage</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Enable-ComplianceTagStorage cmdlet to create the retention label policy in the Microsoft Purview compliance portal. This is a one-time operation. Retention labels apply retention settings to content.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Export-ContentExplorerData</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Export-ContentExplorerData cmdlet to export data classification file details in Microsoft Purview compliance.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
<p>Export-FilePlanProperty</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Export-FilePlanProperty cmdlet to export file plan properties.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-AdaptiveScope</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Get-AdaptiveScope cmdlet to view adaptive scopes in your organization. Adaptive scopes (or static scopes) are used in retention policies and retention label policies.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-AdaptiveScopeMembers</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Get-AdaptiveScopeMembers cmdlet to retrieve current and past members of adaptive scopes in your organization. Adaptive scopes are used in retention policies, Insider Risk Management policies and retention label policies.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-AppRetentionCompliancePolicy</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Get-AppRetentionCompliancePolicy to view app retention compliance policies. App retention & labeling policies target new ways to scope and manage policies.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
<p>Get-AppRetentionComplianceRule</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Get-AppRetentionComplianceRule to view app retention compliance rules.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-ComplianceRetentionEvent</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Get-ComplianceRetentionEvent cmdlet to view compliance retention events in the Microsoft Purview compliance portal.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-ComplianceRetentionEventType</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Get-ComplianceRetentionEventType cmdlet to view retention event types in the Microsoft Purview compliance portal.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-ComplianceTag</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Get-ComplianceTag cmdlet to view retention labels in the Microsoft Purview compliance portal. Retention labels apply retention settings to content.</p>

Cmdlet	Description
	<p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-ComplianceTagStorage</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Get-ComplianceTagStorage cmdlet to confirm that you've created the retention label policy by using the Enable-ComplianceTagStorage cmdlet. Retention labels apply retention settings to content.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-DataRetentionReport</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Get-DataRetentionReport cmdlet to view information about data retention in the Microsoft Purview compliance portal.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-FilePlanPropertyAuthority</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Get-FilePlanPropertyAuthority cmdlet to view file plan property authorities.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-FilePlanPropertyCategory</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p>

Cmdlet	Description
	<p>Use the Fet-FilePlanPropertyCategory cmdlet to view file plan property categories.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-FilePlanPropertyCitation</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Get-FilePlanPropertyCitation cmdlet to view file plan property citations.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-FilePlanPropertyDepartment</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Get-FilePlanPropertyDepartment cmdlet to view file plan property departments.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-FilePlanPropertyReferenceId</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Get-FilePlanPropertyReferenceId cmdlet to view file plan property reference IDs.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-FilePlanPropertyStructure</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p>

Cmdlet	Description
	<p>Use the Get-FilePlanPropertyStructure cmdlet to view the file plan property structure in your organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-FilePlanPropertySubCategory</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Get-FilePlanPropertySubCategory cmdlet to view file plan property subcategories.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-HoldCompliancePolicy</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Get-HoldCompliancePolicy to view existing preservation policies in the Microsoft Purview compliance portal.</p> <p>Note: The Get-HoldCompliancePolicy cmdlet is replaced by the Get-RetentionCompliancePolicy cmdlet. If you have scripts that use Get-HoldCompliancePolicy, update them to use Get-RetentionCompliancePolicy.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-HoldComplianceRule</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Get-HoldComplianceRule to view preservation rules in the Microsoft Purview compliance portal.</p> <p>Note: The Get-HoldComplianceRule cmdlet is replaced by the Get-RetentionComplianceRule cmdlet. If you have scripts that</p>

Cmdlet	Description
	<p>use Get-HoldComplianceRule, update them to use Get-RetentionComplianceRule.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-ManagedContentSettings</p>	<p>This cmdlet is available only in Exchange Server 2010.</p> <p>Use the Get-ManagedContentSettings cmdlet to retrieve managed content settings associated with managed folders.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-ManagedFolder</p>	<p>This cmdlet is available only in Exchange Server 2010.</p> <p>Use the Get-ManagedFolder cmdlet to retrieve the attributes of one or more managed folders.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-ManagedFolderMailboxPolicy</p>	<p>This cmdlet is available only in Exchange Server 2010.</p> <p>Use the Get-ManagedFolderMailboxPolicy cmdlet to return all attributes of one or more managed folder mailbox policies.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-RecordReviewNotificationTemplateConfig</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Get-RecordReviewNotificationTemplateConfig cmdlet to view the record review notification and reminder settings.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-RegulatoryComplianceUI</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance</p>

Cmdlet	Description
	<p>PowerShell .</p> <p>Use the Get-RegulatoryComplianceUI cmdlet to view the status of the regulatory compliance UI in the Microsoft Purview compliance portal (whether the preservation lock checkbox is displayed for retention policies and the immutable label checkbox is displayed for retention labels).</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-RetentionCompliancePolicy</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Get-RetentionCompliancePolicy to view existing retention policies in the Microsoft Purview compliance portal.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-RetentionComplianceRule</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Get-RetentionComplianceRule to view retention rules in the Microsoft Purview compliance portal.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-RetentionEvent</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Get-RetentionEvent cmdlet to view retention events in your organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
<p>Get-RetentionPolicy</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Get-RetentionPolicy cmdlet to retrieve the settings for retention policies.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-RetentionPolicyTag</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Get-RetentionPolicyTag cmdlet to retrieve settings for a retention tag.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Import-FilePlanProperty</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Import-FilePlanProperty cmdlet to import file plan properties.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
<p>Invoke-HoldRemovalAction</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Invoke-HoldRemovalAction cmdlet to view and remove holds on mailboxes and SharePoint sites. You can also see holds that were previously removed by using this cmdlet.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-AdaptiveScope</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the New-AdaptiveScope cmdlet to create adaptive scopes in your organization. Adaptive scopes (or static scopes) are used in retention policies and retention label policies.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-AppRetentionCompliancePolicy</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the New-AppRetentionCompliancePolicy to create app retention compliance policies. App retention & labeling policies target new ways to scope and manage policies.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-AppRetentionComplianceRule</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the New-AppRetentionComplianceRule to create app retention compliance rules.</p>

Cmdlet	Description
	<p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-ComplianceRetentionEvent</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the New-ComplianceRetentionEvent cmdlet to create compliance retention events in your organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-ComplianceRetentionEventType</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the New-ComplianceRetentionEventType cmdlet to create retention event types in the Microsoft Purview compliance portal.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-ComplianceTag</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the New-ComplianceTag cmdlet to create retention labels in the Microsoft Purview compliance portal. Retention labels apply retention settings to content.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-FilePlanPropertyAuthority</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p>

Cmdlet	Description
	<p>Use the New-FilePlanPropertyAuthority cmdlet to create file plan property authorities.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-FilePlanPropertyCategory</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the New-FilePlanPropertyCategory cmdlet to create file plan property categories.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-FilePlanPropertyCitation</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the New-FilePlanPropertyCitation cmdlet to create file plan property citations.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-FilePlanPropertyDepartment</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the New-FilePlanPropertyDepartment cmdlet to create file plan property departments.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-FilePlanPropertyReferenceId</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p>

Cmdlet	Description
	<p>Use the New-FilePlanPropertyReferenceId cmdlet to create file plan property reference IDs.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-FilePlanPropertySubCategory</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the New-FilePlanPropertySubCategory cmdlet to create file plan property subcategories.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-HoldCompliancePolicy</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the New-HoldCompliancePolicy cmdlet to create new preservation policies in the Microsoft Purview compliance portal.</p> <p>Note: The New-HoldCompliancePolicy cmdlet is replaced by the New-RetentionCompliancePolicy cmdlet. If you have scripts that use New-HoldCompliancePolicy, update them to use New-RetentionCompliancePolicy.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-HoldComplianceRule</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the New-HoldComplianceRule cmdlet to create new preservation rules in the Microsoft Purview compliance portal.</p> <p>Note: The New-HoldComplianceRule cmdlet is replaced by the New-RetentionComplianceRule cmdlet. If you have scripts</p>

Cmdlet	Description
	<p>that use New-HoldComplianceRule, update them to use New-RetentionComplianceRule.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-ManagedContentSettings</p>	<p>This cmdlet is available only in Exchange Server 2010.</p> <p>Use the New-ManagedContentSettings cmdlet to create managed content settings for managed folders.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-ManagedFolder</p>	<p>This cmdlet is available only in Exchange Server 2010.</p> <p>Use the New-ManagedFolder cmdlet to create a managed folder object for messaging records management (MRM).</p> <p>This command doesn't accept pipelined input.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-ManagedFolderMailboxPolicy</p>	<p>This cmdlet is available only in Exchange Server 2010.</p> <p>Use the New-ManagedFolderMailboxPolicy cmdlet to create a managed folder mailbox policy.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-RetentionCompliancePolicy</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the New-RetentionCompliancePolicy cmdlet to create new retention policies and new retention label policies in the Microsoft Purview compliance portal. Creating a new policy also requires use of the New-RetentionComplianceRule cmdlet.</p>

Cmdlet	Description
	<p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-RetentionComplianceRule</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the New-RetentionComplianceRule cmdlet to create new retention rules in the Microsoft Purview compliance portal.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-RetentionPolicy</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the New-RetentionPolicy cmdlet to create a retention policy.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-RetentionPolicyTag</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the New-RetentionPolicyTag cmdlet to create a retention tag.</p> <p>For more information about retention tags, see Retention tags and retention policies in Exchange Server.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-AdaptiveScope</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p>

Cmdlet	Description
	<p>Use the Remove-AdaptiveScope cmdlet to remove adaptive scopes from your organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-AppRetentionCompliancePolicy</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Remove-AppRetentionCompliancePolicy to remove app retention compliance policies.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-AppRetentionComplianceRule</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Remove-AppRetentionComplianceRule to remove app retention compliance rules.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-ComplianceRetentionEventType</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Remove-ComplianceRetentionEventType cmdlet to remove retention event types in the Microsoft Purview compliance portal.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-ComplianceTag</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p>

Cmdlet	Description
	<p>Use the Remove-ComplianceTag cmdlet to remove retention labels from the Microsoft Purview compliance portal. Retention labels apply retention settings to content.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-FilePlanPropertyAuthority</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Remove-FilePlanPropertyAuthority cmdlet to remove file plan property authorities.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-FilePlanPropertyCategory</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Remove-FilePlanPropertyCategory cmdlet to remove file plan property categories.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-FilePlanPropertyCitation</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Remove-FilePlanPropertyCitation cmdlet to remove file plan property citations.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-FilePlanPropertyDepartment</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p>

Cmdlet	Description
	<p>Use the Remove-FilePlanPropertyDepartment cmdlet to remove file plan property departments.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-FilePlanPropertyReferenceId</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the New-FilePlanPropertyReferenceId cmdlet to remove file plan property reference IDs.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-FilePlanPropertySubCategory</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Remove-FilePlanPropertySubCategory cmdlet to remove file plan property subcategories.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
<p>Remove-HoldCompliancePolicy</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Remove-HoldCompliancePolicy cmdlet to remove preservation policies from the Microsoft Purview compliance portal.</p> <p>Note: The Remove-HoldCompliancePolicy cmdlet is replaced by the Remove-RetentionCompliancePolicy cmdlet. If you have scripts that use Remove-HoldCompliancePolicy, update them to use Remove-RetentionCompliancePolicy.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-HoldComplianceRule</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Remove-HoldComplianceRule cmdlet to remove preservation rules from the Microsoft Purview compliance portal.</p> <p>Note: The Remove-HoldComplianceRule cmdlet is replaced by the Remove-RetentionComplianceRule cmdlet. If you have scripts that use Remove-HoldComplianceRule, update them to use Remove-RetentionComplianceRule.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-ManagedContentSettings</p>	<p>This cmdlet is available only in Exchange Server 2010.</p> <p>Use the Remove-ManagedContentSettings cmdlet to delete managed content settings from a managed folder.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
Remove-ManagedFolder	<p>This cmdlet is available only in Exchange Server 2010.</p> <p>Use the Remove-ManagedFolder cmdlet to remove a managed folder from Active Directory.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Remove-ManagedFolderMailboxPolicy	<p>This cmdlet is available only in Exchange Server 2010.</p> <p>Use the Remove-ManagedFolderMailboxPolicy cmdlet to delete managed folder mailbox policies.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Remove-RetentionCompliancePolicy	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Remove-RetentionCompliancePolicy cmdlet to remove retention policies from the Microsoft Purview compliance portal. This cmdlet also removes the corresponding retention rule.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Remove-RetentionComplianceRule	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Remove-RetentionComplianceRule cmdlet to remove retention rules from the Microsoft Purview compliance portal.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
<p>Remove-RetentionPolicy</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Remove-RetentionPolicy cmdlet to remove a retention policy.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-RetentionPolicyTag</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Remove-RetentionPolicyTag cmdlet to remove a retention tag.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-AdaptiveScope</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Set-AdaptiveScope cmdlet to modify adaptive scopes in your organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-AppRetentionCompliancePolicy</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Set-AppRetentionCompliancePolicy to modify app retention compliance policies.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
Set-AppRetentionComplianceRule	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Set-AppRetentionComplianceRule to modify app retention compliance rules.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Set-ComplianceRetentionEventType	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Set-ComplianceRetentionEventType cmdlet to modify retention event types in the Microsoft Purview compliance portal.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Set-ComplianceTag	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Set-ComplianceTag cmdlet to modify retention labels in the Microsoft Purview compliance portal. Retention labels apply retention settings to content.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Set-FilePlanPropertyAuthority	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Set-FilePlanPropertyAuthority cmdlet to modify file plan property authorities.</p>

Cmdlet	Description
	<p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-FilePlanPropertyCategory</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Set-FilePlanPropertyCategory cmdlet to modify file plan property categories.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-FilePlanPropertyCitation</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Set-FilePlanPropertyCitation cmdlet to modify file plan property citations.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-FilePlanPropertyDepartment</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Set-FilePlanPropertyDepartment cmdlet to modify file plan property departments.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-FilePlanPropertyReferenceId</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Set-FilePlanPropertyReferenceId cmdlet to modify file plan property reference IDs.</p>

Cmdlet	Description
	<p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-FilePlanPropertySubCategory</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Set-FilePlanPropertySubCategory cmdlet to modify file plan property subcategories.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-HoldCompliancePolicy</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Set-HoldCompliancePolicy cmdlet to modify existing preservation policies in the Microsoft Purview compliance portal.</p> <p>Note: The Set-HoldCompliancePolicy cmdlet is replaced by the Set-RetentionCompliancePolicy cmdlet. If you have scripts that use Set-HoldCompliancePolicy, update them to use Set-RetentionCompliancePolicy.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-HoldComplianceRule</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Set-HoldComplianceRule cmdlet to modify existing preservation rules in the Microsoft Purview compliance portal.</p> <p>Note: The Set-HoldComplianceRule cmdlet is replaced by the Set-RetentionComplianceRule cmdlet. If you have scripts that use Set-HoldComplianceRule, update them to use Set-RetentionComplianceRule.</p>

Cmdlet	Description
	<p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-ManagedContentSettings</p>	<p>This cmdlet is available only in Exchange Server 2010.</p> <p>Use the Set-ManagedContentSettings cmdlet to modify existing managed content settings for a managed folder.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-ManagedFolder</p>	<p>This cmdlet is available only in Exchange Server 2010.</p> <p>Use the Set-ManagedFolder cmdlet to modify the settings of managed folders.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-ManagedFolderMailboxPolicy</p>	<p>This cmdlet is available only in Exchange Server 2010.</p> <p>Use the Set-ManagedFolderMailboxPolicy cmdlet to change the settings of a managed folder mailbox policy.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-RecordReviewNotificationTemplateConfig</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Set-RecordReviewNotificationTemplateConfig cmdlet to set up the customized record review notification and reminder that's sent when an item requires review.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-RegulatoryComplianceUI</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p>

Cmdlet	Description
	<p>Use the Set-RegulatoryComplianceUI cmdlet to display the UI option in retention label settings to mark content as a regulatory record.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-RetentionCompliancePolicy</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Set-RetentionCompliancePolicy cmdlet to modify existing retention policies in the Microsoft Purview compliance portal.</p> <p>Note: Running this cmdlet causes a full synchronization across your organization, which is a significant operation. If you need to update multiple policies, wait until the policy distribution is successful before running the cmdlet again for the next policy. For information about the distribution status, see Get-RetentionCompliancePolicy.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-RetentionComplianceRule</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Set-RetentionComplianceRule cmdlet to modify existing retention rules in the Microsoft Purview compliance portal.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-RetentionPolicy</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p>

Cmdlet	Description
	<p>Use the Set-RetentionPolicy cmdlet to change the properties of an existing retention policy.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-RetentionPolicyTag</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Set-RetentionPolicyTag cmdlet to modify the properties of a retention tag.</p> <p>For more information about retention tags, see Retention tags and retention policies in Exchange Server.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Start-ManagedFolderAssistant</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Start-ManagedFolderAssistant cmdlet to immediately start messaging records management (MRM) processing of mailboxes that you specify.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Start-RetentionAutoTagLearning</p>	<p>This cmdlet is available only in Exchange Server 2010.</p> <p>Use the Start-RetentionAutoTagLearning cmdlet to start auto-tagging for a specified mailbox or to cross-validate auto-tagging results for the mailbox.</p> <p>Messaging records management (MRM) must be configured before the Start-RetentionAutoTagLearning cmdlet can be used. For more information, see Understanding Retention Tags and Retention Policies.</p>

Cmdlet	Description
	<p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Stop-ManagedFolderAssistant</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Stop-ManagedFolderAssistant cmdlet to immediately stop messaging records management (MRM) from processing users' mailboxes on the specified servers.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Validate-RetentionRuleQuery</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Validate-RetentionRuleQuery cmdlet to validate the Keyword Query Language (KQL) content search filters for retention rules.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Cmdlet	Description
<p>Add-VivaModuleFeaturePolicy</p>	<p>This cmdlet is available only in the Exchange Online PowerShell module version 3.2.0 or later. For more information, see About the Exchange Online PowerShell module.</p> <p>Use the Add-VivaModuleFeaturePolicy cmdlet to add a new access policy for a specific feature in Viva. The attributes of the policy are defined using the cmdlet parameters. Policies are used to restrict or grant access to the specified feature for specific users, groups, or the entire tenant.</p> <ul style="list-style-type: none"> You can assign up to 10 policies per feature. An additional one policy per feature can be assigned to the entire tenant. Policies assigned to a specific user or group take priority over the policy assigned to the entire tenant when determining whether a feature is enabled. If a user has

Cmdlet	Description
	<p>multiple policies assigned for a feature (directly as a user or member of a group), the most restrictive policy applies.</p> <ul style="list-style-type: none"> Some features only support policies that apply to the entire tenant, not specific users or groups. You can refer to supported policy scopes for a feature using the Get-VivaModuleFeature cmdlet. <p>Some features include the option for user controls (user opt out). Refer to the feature documentation to see if user controls are available for the feature that you intend to set a policy for.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Add-VivaOrgInsightsDelegatedRole</p>	<p>This cmdlet is available only in the Exchange Online PowerShell module version 3.7.1 or later. For more information, see About the Exchange Online PowerShell module.</p> <p>Use the Add-VivaOrgInsightsDelegatedRole cmdlet to add delegate access to the specified account (the delegate) so they can view organizational insights like the leader (the delegator).</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Add-WorkforceInsightsDelegationAccess</p>	<p>This cmdlet is available only in the Exchange Online PowerShell module version 3.9.2-Preview1 or later. For more information, see About the Exchange Online PowerShell module.</p> <p>Use the Add-WorkforceInsightsDelegationAccess cmdlet to add delegate access to the specified account (the delegate) so they can view organizational insights like the leader (the delegator).</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Connect-ExchangeOnline</p>	<p>This cmdlet is available only in the Exchange Online PowerShell module. For more information, see About the</p>

Cmdlet	Description
	<p>Exchange Online PowerShell module.</p> <p>Use the Connect-ExchangeOnline cmdlet in the Exchange Online PowerShell module to use modern authentication to connect to Exchange Online PowerShell or PowerShell for the Built-in security add-on for on-premises mailboxes. This cmdlet works for accounts with or without multi-factor authentication (MFA).</p> <p>To connect to Security & Compliance PowerShell, use the Connect-IPPSSession cmdlet.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Connect-IPPSSession</p>	<p>This cmdlet is available only in the Exchange Online PowerShell module. For more information, see About the Exchange Online PowerShell module.</p> <p>Use the Connect-IPPSSession cmdlet in the Exchange Online PowerShell module to connect to Security & Compliance PowerShell using modern authentication. The cmdlet works for MFA or non-MFA enabled accounts.</p> <p>Note: Version 3.2.0 or later of the module supports REST API mode for virtually all Security & Compliance PowerShell cmdlets (Basic authentication in WinRM on the local computer isn't required for REST API mode). For more information, see Prerequisites for the Exchange Online PowerShell module.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Disconnect-ExchangeOnline</p>	<p>This cmdlet is available only in the Exchange Online PowerShell module. For more information, see About the Exchange Online PowerShell module.</p> <p>Use the Disconnect-ExchangeOnline cmdlet in the Exchange Online PowerShell module to disconnect the connections that you created using the Connect-ExchangeOnline or Connect-IPPSSession cmdlets.</p>

Cmdlet	Description
	<p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-ConnectionInformation</p>	<p>This cmdlet is available only in the Exchange Online PowerShell module version 3.0.0 or later. For more information, see About the Exchange Online PowerShell module.</p> <p>Use the Get-ConnectionInformation cmdlet to get information about all REST-based connections in the current PowerShell instance with Exchange Online.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-DefaultTenantBriefingConfig</p>	<p>This cmdlet is available only in the Exchange Online PowerShell module version 3.2.0 or later. For more information, see About the Exchange Online PowerShell module.</p> <p>Use the Get-DefaultTenantBriefingConfig cmdlet to view the default Briefing email configuration in cloud-based organizations. For details about configuring the Briefing email, see Configure Briefing email.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-DefaultTenantMyAnalyticsFeatureConfig</p>	<p>This cmdlet is available only in the Exchange Online PowerShell module version 3.2.0 or later. For more information, see About the Exchange Online PowerShell module.</p> <p>Use the Get-DefaultTenantMyAnalyticsFeatureConfig cmdlet to view the availability and status of Viva Insights features for the cloud-based organization: digest email, add-in, dashboard, meeting effectiveness survey, and schedule send suggestions.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-EXOCasMailbox</p>	<p>This cmdlet is available only in the Exchange Online PowerShell module. For more information, see About the</p>

Cmdlet	Description
	<p>Exchange Online PowerShell module.</p> <p>Use the Get-EXOCasMailbox cmdlet to view the Client Access settings that are configured on mailboxes.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-EXOMailbox</p>	<p>This cmdlet is available only in the Exchange Online PowerShell module. For more information, see About the Exchange Online PowerShell module.</p> <p>Use the Get-EXOMailbox cmdlet to view mailbox objects and attributes, populate property pages, or supply mailbox information to other tasks.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-EXOMailboxFolderPermission</p>	<p>This cmdlet is available only in the Exchange Online PowerShell module. For more information, see About the Exchange Online PowerShell module.</p> <p>Use the Get-ExOMailboxFolderPermission cmdlet to view folder-level permissions in mailboxes.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-EXOMailboxFolderStatistics</p>	<p>This cmdlet is available only in the Exchange Online PowerShell module. For more information, see About the Exchange Online PowerShell module.</p> <p>Use the Get-EXOMailboxFolderStatistics cmdlet to retrieve information about the folders in a specified mailbox, including the number and size of items in the folder, the folder name and ID, and other information.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
<p>Get-EXOMailboxPermission</p>	<p>This cmdlet is available only in the Exchange Online PowerShell module. For more information, see About the Exchange Online PowerShell module.</p> <p>Use the Get-EXOMailboxPermission cmdlet to retrieve permissions on a mailbox.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-EXOMailboxStatistics</p>	<p>This cmdlet is available only in the Exchange Online PowerShell module. For more information, see About the Exchange Online PowerShell module.</p> <p>Use the Get-EXOMailboxStatistics cmdlet to return information about a mailbox, such as the size of the mailbox, the number of messages it contains, and the last time it was accessed.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-EXOMobileDeviceStatistics</p>	<p>This cmdlet is available only in the Exchange Online PowerShell module. For more information, see About the Exchange Online PowerShell module.</p> <p>Use the Get-EXOMobileDeviceStatistics cmdlet to retrieve the list of mobile devices configured to synchronize with a specified user's mailbox and return a list of statistics about the mobile devices.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-EXORecipient</p>	<p>This cmdlet is available only in the Exchange Online PowerShell module. For more information, see About the Exchange Online PowerShell module.</p> <p>Use the Get-EXORecipient cmdlet to view existing recipient objects in your organization. This cmdlet returns all mail-</p>

Cmdlet	Description
	<p>enabled objects (for example, mailboxes, mail users, mail contacts, and distribution groups).</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-EXORecipientPermission</p>	<p>This cmdlet is available only in the Exchange Online PowerShell module. For more information, see About the Exchange Online PowerShell module.</p> <p>Use the Get-EXORecipientPermission cmdlet to view information about SendAs permissions that are configured for users in a cloud-based organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-MyAnalyticsFeatureConfig</p>	<p>This cmdlet is available only in the Exchange Online PowerShell module. For more information, see About the Exchange Online PowerShell module.</p> <p>Use the Get-MyAnalyticsFeatureConfig cmdlet to view the availability and feature status of MyAnalytics for the specified user.</p> <p>Note: This cmdlet replaces the Get-UserAnalyticsConfig cmdlet.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
Get-UserBriefingConfig	<p>This cmdlet is available only in the Exchange Online PowerShell module. For more information, see About the Exchange Online PowerShell module.</p> <p>Use the Get-UserBriefingConfig cmdlet to get the current state of the Briefing email flag for the specified user. For more details about configuring the Briefing email, see Configure Briefing email.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Get-VivaInsightsSettings	<p>This cmdlet is available only in the Exchange Online PowerShell module. For more information, see About the Exchange Online PowerShell module.</p> <p>Note: This cmdlet is available only in version 2.0.5 or later of the module.</p> <p>Use the Get-VivaInsightsSettings cmdlet to check whether a user has access to features in Microsoft Viva Insights in Microsoft Teams. Only users with provisioned Exchange Online mailboxes can access features within the Viva Insights app in Teams.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Get-VivaModuleFeature	<p>This cmdlet is available only in the Exchange Online PowerShell module version 3.2.0 or later. For more information, see About the Exchange Online PowerShell module.</p> <p>Use the Get-VivaModuleFeature cmdlet to view the features in a Viva module that support feature access controls. This cmdlet provides details about the features, including the feature identifiers and descriptions.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
<p>Get-VivaModuleFeatureEnablement</p>	<p>This cmdlet is available only in the Exchange Online PowerShell module version 3.2.0 or later. For more information, see About the Exchange Online PowerShell module.</p> <p>Use the Get-VivaModuleFeatureEnablement cmdlet to view whether or not a feature in a Viva module is enabled for a specific user or group. Whether or not the feature is enabled is referred to as the feature's "enablement state". The enablement state returned by this cmdlet is based on the access policies set by the admin.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-VivaModuleFeaturePolicy</p>	<p>This cmdlet is available only in the Exchange Online PowerShell module version 3.2.0 or later. For more information, see About the Exchange Online PowerShell module.</p> <p>Use the Get-VivaModuleFeaturePolicy cmdlet to view the access policies for a specified feature in a Viva module in Viva. Policies are used to restrict or grant access to the specified feature for specific users, groups, or the entire tenant. This cmdlet provides details about the policies, including the policy's identifier, name, and creation date. The cmdlet can filter policies based on MemberIds, allowing admins to view policies specific to certain users or groups.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
<p>Get-VivaOrgInsightsDelegatedRole</p>	<p>This cmdlet is available only in the Exchange Online PowerShell module version 3.7.1 or later. For more information, see About the Exchange Online PowerShell module.</p> <p>Use the Get-VivaOrgInsightsDelegatedRole cmdlet to view all delegates of the specified delegator. Delegate accounts can view organizational insights like the specified delegator.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-WorkforceInsightsDelegationAccess</p>	<p>This cmdlet is available only in the Exchange Online PowerShell module version 3.9.2-Preview1 or later. For more information, see About the Exchange Online PowerShell module.</p> <p>Use the Get-WorkforceInsightsDelegationAccess cmdlet to view all delegates of the specified delegator. Delegate accounts can view organizational insights like the specified delegator.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-VivaModuleFeaturePolicy</p>	<p>This cmdlet is available only in the Exchange Online PowerShell module version 3.2.0 or later. For more information, see About the Exchange Online PowerShell module.</p> <p>Use the Remove-VivaModuleFeaturePolicy cmdlet to delete an access policy for a feature in a Viva module in Viva. Once you delete a policy, the policy is permanently deleted. You can't undo the deletion.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-VivaOrgInsightsDelegatedRole</p>	<p>This cmdlet is available only in the Exchange Online PowerShell module version 3.7.1 or later. For more information, see About the Exchange Online PowerShell module.</p>

Cmdlet	Description
	<p>Use the Remove-VivaOrgInsightsDelegatedRole cmdlet to remove delegate access from the specified account (the delegate) so they can't view organizational insights like the leader (the delegator).</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-WorkforceInsightsDelegationAccess</p>	<p>This cmdlet is available only in the Exchange Online PowerShell module version 3.9.2-Preview1 or later. For more information, see About the Exchange Online PowerShell module.</p> <p>Use the Remove-WorkforceInsightsDelegationAccess cmdlet to remove delegate access from the specified account (the delegate) so they can't view organizational insights like the leader (the delegator).</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-DefaultTenantBriefingConfig</p>	<p>This cmdlet is available only in the Exchange Online PowerShell module version 3.2.0 or later. For more information, see About the Exchange Online PowerShell module.</p> <p>Use the Set-DefaultTenantBriefingConfig cmdlet to modify the default Briefing email configuration in cloud-based organizations. For details about configuring the Briefing email, see Configure Briefing email.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-DefaultTenantMyAnalyticsFeatureConfig</p>	<p>This cmdlet is available only in the Exchange Online PowerShell module version 3.2.0 or later. For more information, see About the Exchange Online PowerShell module.</p> <p>Use the Set-DefaultTenantMyAnalyticsFeatureConfig cmdlet to update the availability and status of Viva Insights features for the</p>

Cmdlet	Description
	<p>cloud-based organization: digest email, add-in, dashboard, meeting effectiveness survey, and schedule send suggestions.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-MyAnalyticsFeatureConfig</p>	<p>This cmdlet is available only in the Exchange Online PowerShell module. For more information, see About the Exchange Online PowerShell module.</p> <p>Use the Set-MyAnalyticsFeatureConfig cmdlet to configure the availability and features of MyAnalytics for the specified user.</p> <p>Note: This cmdlet replaces the Set-UserAnalyticsConfig cmdlet.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-UserBriefingConfig</p>	<p>This cmdlet is available only in the Exchange Online PowerShell module. For more information, see About the Exchange Online PowerShell module.</p> <p>Use the Set-UserBriefingConfig cmdlet to enable or disable the Briefing email for a user. For more details about configuring the Briefing email, see Configure Briefing email.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-VivaInsightsSettings</p>	<p>This cmdlet is available only in the Exchange Online PowerShell module. For more information, see About the Exchange Online PowerShell module.</p> <p>Note: This cmdlet is available only in version 2.0.5 or later of the module.</p> <p>Use the Set-VivaInsightsSettings cmdlet to control user access to features in Viva Insights. Only users with provisioned Exchange Online mailboxes can access features within the Viva Insights app in Teams.</p>

Cmdlet	Description
	<p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Update-VivaModuleFeaturePolicy</p>	<p>This cmdlet is available only in the Exchange Online PowerShell module version 3.2.0 or later. For more information, see About the Exchange Online PowerShell module.</p> <p>Use the Update-VivaModuleFeaturePolicy cmdlet to update an access policy for a feature in a Viva module in Viva.</p> <ul style="list-style-type: none"> • You can't update a policy for a particular user or group to include the entire tenant if a policy for the entire tenant already exists for the feature. Only one tenant-wide policy is supported. • Policies assigned to a specific user or group take priority over the policy assigned to the entire tenant when determining whether a feature is enabled. If a user has multiple policies assigned for a feature (directly as a user or member of a group), the most restrictive policy applies. • Some features only support policies that apply to the entire tenant, not specific users or groups. You can refer to supported policy scopes for a feature using the Get-VivaModuleFeature cmdlet. <p>Some features include the option for user controls (user opt out). Refer to the feature documentation to see if user controls are available for the feature that you intend to set a policy for.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
Get-CompromisedUserAggregateReport	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Get-CompromisedUserAggregateReport cmdlet to return general data about compromised users for the last 10 days.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Get-CompromisedUserDetailReport	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Get-CompromisedUserDetailReport cmdlet to return detailed information about compromised users for the last 10 days.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Get-HistoricalSearch	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Get-HistoricalSearch cmdlet to view information about historical searches that have been performed within the last ten days.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Get-LogonStatistics	<p>This cmdlet is functional only in Exchange Server 2010.</p> <p>The Get-LogonStatistics cmdlet is deprecated and is no longer used.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Get-MailDetailDlpPolicyReport	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Get-MailDetailDlpPolicyReport cmdlet to view the details of messages that matched the conditions defined by any</p>

Cmdlet	Description
	<p>data loss prevention (DLP) policies. This cmdlet works on messages that were sent within the last seven days.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-MailDetailEncryptionReport</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Get-MailDetailEncryptionReport cmdlet to view the details of encryption in your cloud-based organization for the last 10 days.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-MailDetailTransportRuleReport</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Get-MailDetailTransportRuleReport cmdlet to view the details of messages that matched the conditions defined by any transport rules for the last 10 days.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-MailFilterListReport</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Get-MailFilterListReport cmdlet to obtain values for various parameters that can be supplied to other reporting cmdlets.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
Get-MailTrafficEncryptionReport	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Get-MailTrafficEncryptionReport cmdlet to view the results of encryption in your cloud-based organization for the last 92 days.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Get-MailTrafficPolicyReport	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Get-MailTrafficPolicyReport cmdlet to view statistics about messages that were affected by data loss prevention (DLP) policies and transport rules for the last 90 days.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Get-MailTrafficSummaryReport	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Get-MailTrafficSummaryReport cmdlet to view summary information about message traffic in your organization for the last 90 days.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Get-MxRecordReport	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Get-MxRecordReport cmdlet to view information about the mail exchanger (MX) records that are configured for a specified domain.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Get-OutboundConnectorReport	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Get-OutboundConnectorReport cmdlet to view the Outbound connectors that are used to deliver mail to specific</p>

Cmdlet	Description
	<p>domains.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-RecipientStatisticsReport</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Get-RecipientStatisticsReport cmdlet to view the recipient statistics report.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-ReportExecutionInstance</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Get-ReportExecutionInstance cmdlet to review the report execution instance in Exchange Online.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-SCInsights</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Get-SCInsights cmdlet to view Microsoft 365 insights information.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-ServiceDeliveryReport</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Get-ServiceDeliveryReport cmdlet to view information about the message delivery path for a specified recipient.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-SupervisoryReviewActivity</p>	<p>This cmdlet is available only in the cloud-based service.</p>

Cmdlet	Description
	<p>Use the Get-SupervisoryReviewActivity cmdlet to view all activities performed by a reviewer for a specific supervision policy. This information might be useful if reviewer activities are required in regulatory compliance audits or in litigation.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-SupervisoryReviewOverallProgressReport</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Get-SupervisoryReviewOverallProgressReport cmdlet to view the total number of supervised communications classified as Pending, Resolved, Compliant, Non-compliant, and Questionable.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-SupervisoryReviewPolicyReport</p>	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Get-SupervisoryReviewPolicyReport cmdlet to view supervisory review policy events in the Microsoft Purview compliance portal.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
Get-SupervisoryReviewReport	<p>This cmdlet is functional only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Get-SupervisoryReviewReport cmdlet to view supervisory review events in the Microsoft Purview compliance portal for the last 90 days.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Get-SupervisoryReviewTopCasesReport	<p>This cmdlet is available only in Security & Compliance PowerShell. For more information, see Security & Compliance PowerShell.</p> <p>Use the Get-SupervisoryReviewTopCasesReport cmdlet to view the current status of the top supervision policies configured in your organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Test-Message	<p>This cmdlet is functional only in the cloud-based service.</p> <p>Use the Test-Message cmdlet to simulate and report on the effects of mail flow rules (transport rules) and unified DLP rules on test email messages. Because this cmdlet introduces email into the DLP evaluation pipeline, actions such as Block, Moderate, etc. can take place on the test message. Related notifications are also sent to any configured recipients.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Cmdlet	Description
Add-ManagementRoleEntry	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p>

Cmdlet	Description
	<p>Use the Add-ManagementRoleEntry cmdlet to add management role entries to an existing management role.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Add-RoleGroupMember</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Add-RoleGroupMember cmdlet to add members to a management role group.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-ManagementRole</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Get-ManagementRole cmdlet to view management roles that have been created in your organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-ManagementRoleAssignment</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Get-ManagementRoleAssignment cmdlet to retrieve management role assignments.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-ManagementRoleEntry</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p>

Cmdlet	Description
	<p>Use the Get-ManagementRoleEntry cmdlet to retrieve management role entries that have been configured on management roles.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-ManagementScope</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Get-ManagementScope cmdlet to return a list of management scopes.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-RoleAssignmentPolicy</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Get-RoleAssignmentPolicy cmdlet to view existing management role assignment policies in your organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-RoleGroup</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Get-RoleGroup cmdlet to retrieve a list of management role groups.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-RoleGroupMember</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p>

Cmdlet	Description
	<p>Use the Get-RoleGroupMember cmdlet to retrieve a list of members of a management role group.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-ManagementRole</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the New-ManagementRole cmdlet to create a management role based on an existing role or create an unscoped management role.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-ManagementRoleAssignment</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the New-ManagementRoleAssignment cmdlet to assign a management role to a management role group, management role assignment policy, user, or universal security group (USG).</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-ManagementScope</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the New-ManagementScope cmdlet to create a regular or exclusive management scope.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-RoleAssignmentPolicy</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p>

Cmdlet	Description
	<p>Use the New-RoleAssignmentPolicy cmdlet to create management role assignment policies in your organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-RoleGroup</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the New-RoleGroup cmdlet to create management role groups.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-ManagementRole</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Remove-ManagementRole cmdlet to remove custom management roles that you don't need anymore.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-ManagementRoleAssignment</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Remove-ManagementRoleAssignment cmdlet to remove management role assignments.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-ManagementRoleEntry</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p>

Cmdlet	Description
	<p>Use the Remove-ManagementRoleEntry cmdlet to remove existing management role entries.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-ManagementScope</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Remove-ManagementScope cmdlet to remove an existing management scope.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-RoleAssignmentPolicy</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Remove-RoleAssignmentPolicy cmdlet to remove existing management role assignment policies from your organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-RoleGroup</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Remove-RoleGroup cmdlet to remove a management role group.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-RoleGroupMember</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p>

Cmdlet	Description
	<p>Use the Remove-RoleGroupMember cmdlet to remove a member of a management role group.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-ManagementRoleAssignment</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Set-ManagementRoleAssignment cmdlet to modify existing management role assignments.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-ManagementRoleEntry</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Set-ManagementRoleEntry cmdlet to change the available parameters on an existing management role entry.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-ManagementScope</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Set-ManagementScope cmdlet to change an existing management scope.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-RoleAssignmentPolicy</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p>

Cmdlet	Description
	<p>Use the Set-RoleAssignmentPolicy cmdlet to modify existing management role assignment policies in your organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-RoleGroup</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Set-RoleGroup cmdlet to modify who can add or remove members to or from management role groups or change the name of the role group.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Update-RoleGroupMember</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Update-RoleGroupMember cmdlet to modify the members of a management role group.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Cmdlet	Description
<p>Add-GlobalMonitoringOverride</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Add-GlobalMonitoringOverride cmdlet to override the thresholds and parameters of the managed availability probes, monitors and responders on all Exchange 2013 or later servers in your organization. The cmdlet enables monitoring changes and threshold tuning to the environment.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Add-ServerMonitoringOverride</p>	<p>This cmdlet is available only in on-premises Exchange.</p>

Cmdlet	Description
	<p>Use the Add-ServerMonitoringOverride cmdlet to override the thresholds and parameters of managed availability probes, monitors, and responders on Exchange servers.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-AvailabilityReportOutage</p>	<p>This cmdlet is available only in Exchange Server 2010.</p> <p>Use the Get-AvailabilityReportOutage cmdlet to return the daily downtime (if any) for each service entity and its overridden value (if set) to the overall reported availability for the day.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-EventLogLevel</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Get-EventLogLevel cmdlet to display a list of Exchange event categories and the corresponding log levels on Exchange servers.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-GlobalMonitoringOverride</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Get-GlobalMonitoringOverride cmdlet to view the overrides of the thresholds and parameters of the managed availability probes, monitors and responders that are configured for all Exchange 2013 or later servers in your organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-HealthReport</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Get-HealthReport cmdlet to return health information for the Exchange server that you specify. You can use the health values to determine the state of the server. The cmdlet also returns an alert value that provides the specific state of your server.</p>

Cmdlet	Description
	<p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-MonitoringItemHelp</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Get-MonitoringItemHelp cmdlet to discover the monitoring items that you can use to return health information about your Exchange servers. Monitoring items are preconfigured to help you with your server health and monitoring.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-MonitoringItemIdentity</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Get-MonitoringItemIdentity cmdlet to discover the monitoring items that you can use to return health information about your Exchange servers.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-ServerComponentState</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Get-ServerComponentState cmdlet to retrieve configuration settings for Microsoft Exchange components and endpoints.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-ServerHealth</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Get-ServerHealth cmdlet to return health information related to the server you specify.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-ServerMonitoringOverride</p>	<p>This cmdlet is available only in on-premises Exchange.</p>

Cmdlet	Description
	<p>Use the Get-ServerMonitoringOverride cmdlet to return all overrides created on the specified server.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-ThrottlingPolicy</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Get-ThrottlingPolicy cmdlet to view the user throttling settings for one or more throttling policies.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-ThrottlingPolicyAssociation</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Get-ThrottlingPolicyAssociation cmdlet to view existing throttling policy associations in your organization. Throttling policies can be associated with mailboxes, user accounts, mail contacts, mail users, and Exchange server computer accounts.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Invoke-MonitoringProbe</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Invoke-MonitoringProbe cmdlet to run a Managed Availability probe on a selected server.</p> <p>This cmdlet can't be used to run every Managed Availability probe. Only some probes (mainly the deep test probes) can be run manually using this cmdlet. Probes that can't be run with this cmdlet return error messages when you use Invoke-MonitoringProbe to run them.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-AvailabilityReportOutage</p>	<p>This cmdlet is available only in Exchange Server 2010.</p> <p>Use the New-AvailabilityReportOutage cmdlet to create an outage to add unrecorded issues to availability reporting.</p>

Cmdlet	Description
	<p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-ThrottlingPolicy</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the New-ThrottlingPolicy cmdlet to create a non-default user throttling policy.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-AvailabilityReportOutage</p>	<p>This cmdlet is available only in Exchange Server 2010.</p> <p>Use the Remove-AvailabilityReportOutage cmdlet to remove existing outages that have been added with the New-AvailabilityReportOutage cmdlet. Other outages must be modified with the Set-AvailabilityReportOutage cmdlet.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-GlobalMonitoringOverride</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Remove-GlobalMonitoringOverride cmdlet to remove a managed availability global override that is configured for a probe, monitor or responder.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-ServerMonitoringOverride</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Remove-ServerMonitoringOverride cmdlet to remove a managed availability local server override that is configured for a probe, monitor or responder.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
Remove-ThrottlingPolicy	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Remove-ThrottlingPolicy cmdlet to remove a non-default Microsoft Exchange throttling policy.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Set-AvailabilityReportOutage	<p>This cmdlet is available only in Exchange Server 2010.</p> <p>Use the Set-AvailabilityReportOutage cmdlet to set the outages that contribute to the overall reported availability for the day.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Set-EventLogLevel	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Set-EventLogLevel cmdlet to set the event log level registry value for the specified category.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Set-ServerComponentState	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Set-ServerComponentState cmdlet to configure and update Microsoft Exchange components and endpoints on servers you specify.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Set-ServerMonitor	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Set-ServerMonitor cmdlet to edit or set a parameter on a single monitor on an Exchange server.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
Set-ThrottlingPolicy	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Set-ThrottlingPolicy cmdlet to modify the settings for a user throttling policy.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Set-ThrottlingPolicyAssociation	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Set-ThrottlingPolicyAssociation cmdlet to associate a throttling policy with a specific object. The object can be a user with a mailbox, a user without a mailbox, a contact, or a computer account.</p> <p>Note: Some parameters in the throttling policy (for example, MessageRateLimit) apply only to objects that have mailbox GUIDs (mailboxes or remote mailboxes) and don't apply to mail users. And, if you want to apply throttling policy to a remote mailbox, first populate the remote mailbox with an ExchangeGUID by using Set-RemoteMailbox -ExchangeGUID.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Test-ServiceHealth	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Test-ServiceHealth cmdlet to test whether all the Microsoft Windows services that Exchange requires on a server have started. The Test-ServiceHealth cmdlet returns an error for any service required by a configured role when the service is set to start automatically and isn't currently running.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Cmdlet	Description
Add-AvailabilityAddressSpace	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p>

Cmdlet	Description
	<p>Use the Add-AvailabilityAddressSpace cmdlet to create availability address space objects that are used to share free/busy data across Exchange organizations.</p> <p>The maximum number off Availability address spaces returned by Active Directory to Exchange is 100. We recommend using 100 or fewer address spaces in order for Availability lookups to work properly.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Add-PublicFolderAdministrativePermission</p>	<p>This cmdlet is available only in Exchange Server 2010.</p> <p>Use the Add-PublicFolderAdministrativePermission cmdlet to add administrative permissions to a public folder or a public folder hierarchy.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Add-PublicFolderClientPermission</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Add-PublicFolderClientPermission cmdlet to add permissions to public folders.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Disable-MailPublicFolder</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Disable-MailPublicFolder cmdlet to mail-disable a public folder.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
<p>Enable-MailPublicFolder</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Enable-MailPublicFolder cmdlet to mail-enable public folders.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-AvailabilityAddressSpace</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Get-AvailabilityAddressSpace cmdlet to view existing availability address space objects that are used to share free/busy data across Exchange organizations.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-AvailabilityConfig</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Get-AvailabilityConfig cmdlet to view information about the sharing of free/busy information between organizations:</p> <ul style="list-style-type: none"> • In on-premises Exchange, the cmdlet returns the accounts that are trusted in the cross-forest sharing of free/busy information. • In Exchange Online, the cmdlet returns the tenant IDs of organizations that free/busy information is being shared with. <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-MailPublicFolder</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to</p>

Cmdlet	Description
	<p>one environment or the other.</p> <p>Use the Get-MailPublicFolder cmdlet to retrieve mail-related information about mail-enabled public folders. If you want information about the basic (not mail-related) settings of mail-enabled public folders, use the Get-PublicFolder cmdlet instead.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-OrganizationRelationship</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Get-OrganizationRelationship cmdlet to retrieve settings for an organization relationship that is created for federated sharing with other federated Exchange organizations or for hybrid deployments with Exchange Online.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-PublicFolder</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Get-PublicFolder cmdlet to retrieve the attributes of a public folder or a set of public folders.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-PublicFolderAdministrativePermission</p>	<p>This cmdlet is available only in Exchange Server 2010.</p> <p>Use the Get-PublicFolderAdministrativePermission cmdlet to get the administrative permissions for a public folder or a public folder hierarchy.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
<p>Get-PublicFolderClientPermission</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Get-PublicFolderClientPermission cmdlet to retrieve the user permissions for a public folder.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-PublicFolderDatabase</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Get-PublicFolderDatabase cmdlet to view public folder database settings for Microsoft Exchange Server 2010 or earlier public folders.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-PublicFolderItemStatistics</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Get-PublicFolderItemStatistics cmdlet to view information about items within a specified public folder. Information returned includes subject, last modification time, creation time, attachments, message size, and the type of item. You can use this raw information to better understand the distribution of items and item characteristics across public folders.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-PublicFolderMailboxDiagnostics</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Get-PublicFolderMailboxDiagnostics cmdlet to view event-level information about a public folder mailbox. This information can be used to troubleshoot public folder issues.</p>

Cmdlet	Description
	<p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-PublicFolderStatistics</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Get-PublicFolderStatistics cmdlet to retrieve statistical information about public folders, such as folder size and last logon time.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-SharingPolicy</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Get-SharingPolicy cmdlet to view existing sharing policies that control how users inside your organization can share free/busy and contact information with users outside your organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-SiteMailbox</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Get-SiteMailbox cmdlet to view information about site mailboxes. This cmdlet is primarily used by Microsoft SharePoint and Exchange to display information to users in the user interface. However, you might find it helpful for discovering information such as the site mailbox's owners, members, and lifecycle status.</p> <p>Site mailboxes were deprecated in Exchange Online and SharePoint Online in 2017. For more information, see Deprecation of Site Mailboxes.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
<p>Get-SiteMailboxDiagnostics</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Get-SiteMailboxDiagnostics cmdlet to view important event-related data for each site mailbox. This information can be used to troubleshoot site mailbox issues.</p> <p>Site mailboxes were deprecated in Exchange Online and SharePoint Online in 2017. For more information, see Deprecation of Site Mailboxes.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-SiteMailboxProvisioningPolicy</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Get-SiteMailboxProvisioningPolicy cmdlet to view site mailbox provisioning policies.</p> <p>Site mailboxes were deprecated in Exchange Online and SharePoint Online in 2017. For more information, see Deprecation of Site Mailboxes.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-AvailabilityConfig</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the New-AvailabilityConfig cmdlet to create the availability configuration that specifies the Microsoft 365 organizations to exchange free/busy information with.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-OrganizationRelationship</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the New-OrganizationRelationship cmdlet to create organization relationships. Organization relationships define the settings that are used with external Exchange organizations to</p>

Cmdlet	Description
	<p>access calendar free/busy information or to move mailboxes between on-premises Exchange servers and Exchange Online as part of hybrid deployments.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-PublicFolder</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the New-PublicFolder cmdlet to create a public folder with the specified name.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-PublicFolderDatabase</p>	<p>This cmdlet is available only in Exchange Server 2010.</p> <p>Use the New-PublicFolderDatabase cmdlet to create a public folder database.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-PublicFolderDatabaseRepairRequest</p>	<p>This cmdlet is available only in Exchange Server 2010.</p> <p>Use the New-PublicFolderDatabaseRepairRequest cmdlet to detect and fix replication issues in the public folder database.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-SharingPolicy</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the New-SharingPolicy cmdlet to create a sharing policy to regulate how users inside your organization can share calendar and contact information with users outside the organization. Users can</p>

Cmdlet	Description
	<p>only share this information after federation is configured in Exchange. After federation is configured, users can send sharing invitations that comply with a sharing policy to external recipients in other Exchange Server 2010 or later organizations that have federation enabled. A sharing policy needs to get assigned to a mailbox to be effective. If a mailbox doesn't have a specific sharing policy assigned, a default policy enforces the level of sharing permitted for this mailbox.</p> <p>Sharing policies provide user-established, people-to-people sharing of both calendar and contact information with different types of external users. Sharing policies allow users to share both their free/busy and contact information (including the Calendar and Contacts folders) with recipients in other external federated Exchange organizations. For recipients that aren't in an external federated organization or are in non-Exchange organizations, sharing policies allow people-to-people sharing of their calendar information with anonymous users through the use of Internet Calendar Publishing.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-SiteMailboxProvisioningPolicy</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the New-SiteMailboxProvisioningPolicy cmdlet to create provisioning policies for site mailboxes.</p> <p>Site mailboxes were deprecated in Exchange Online and SharePoint Online in 2017. For more information, see Deprecation of Site Mailboxes.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-SyncMailPublicFolder</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>The New-SyncMailPublicFolder cmdlet is used by the Import-MailPublicFoldersForMigration.ps1 and Sync-</p>

Cmdlet	Description
	<p>MailPublicFolders.ps1 scripts to create mail-enabled public folder recipient objects in Exchange Online (the scripts synchronize mail-enabled public folder objects from the source on-premises Exchange organization to Exchange Online). Don't use this cmdlet unless you are directed to do so by Microsoft Customer Service and Support or by specific documentation.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-AvailabilityAddressSpace</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Remove-AvailabilityAddressSpace cmdlet to remove existing availability address space objects and the associated credentials that were used to share free/busy data across Exchange organizations.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-AvailabilityConfig</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Remove-AvailabilityConfig cmdlet to remove the availability configuration that specifies the Microsoft 365 organizations to exchange free/busy information with.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-OrganizationRelationship</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Remove-OrganizationRelationship cmdlet to remove the organization relationship with an external Exchange organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
<p>Remove-PublicFolder</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Remove-PublicFolder cmdlet to remove an existing public folder.</p> <p>The Remove-PublicFolder cmdlet removes the public folder data from all servers in your organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-PublicFolderAdministrativePermission</p>	<p>This cmdlet is available only in Exchange Server 2010.</p> <p>Use the Remove-PublicFolderAdministrativePermission cmdlet to remove administrative permissions for a public folder or a public folder hierarchy.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-PublicFolderClientPermission</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Remove-PublicFolderClientPermission cmdlet to remove permissions from public folders.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-PublicFolderDatabase</p>	<p>This cmdlet is available only in Exchange Server 2010.</p> <p>Use the Remove-PublicFolderDatabase cmdlet to delete public folder databases.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
Remove-SharingPolicy	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Remove-SharingPolicy cmdlet to remove a sharing policy. Before you can remove a sharing policy, you must ensure that no mailbox users are provisioned to use that policy.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Remove-SiteMailboxProvisioningPolicy	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Remove-SiteMailboxProvisioningPolicy cmdlet to remove site mailbox provisioning policies.</p> <p>Site mailboxes were deprecated in Exchange Online and SharePoint Online in 2017. For more information, see Deprecation of Site Mailboxes.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Remove-SyncMailPublicFolder	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>The Remove-SyncMailPublicFolder cmdlet is used by the Sync-MailPublicFolders.ps1 script to remove mail-enabled public folder recipient objects from Exchange Online (the script synchronizes mail-enabled public folder objects from the source on-premises Exchange organization to Exchange Online). Don't use this cmdlet unless you are directed to do so by Microsoft Customer Service and Support or by specific documentation.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Resume-PublicFolderReplication	<p>This cmdlet is available only in Exchange Server 2010.</p>

Cmdlet	Description
	<p>Use the Resume-PublicFolderReplication cmdlet to resume public folder content replication when it's been stopped.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-AvailabilityConfig</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Set-AvailabilityConfig cmdlet to set the access level for free/busy information.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-MailPublicFolder</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Set-MailPublicFolder cmdlet to configure the mail-related settings of mail-enabled public folders. If you want to configure basic settings that aren't mail-related, use the Set-PublicFolder cmdlet.</p> <p>NOTE: The settings that you configure on a public folder mailbox might interfere with the existing settings on a public folder within in the mailbox.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-OrganizationRelationship</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Set-OrganizationRelationship cmdlet to modify existing organization relationships. Organization relationships define the settings that are used with external Exchange organizations to access calendar free/busy information or to move mailboxes</p>

Cmdlet	Description
	<p>between on-premises Exchange servers and Exchange Online as part of hybrid deployments.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-PublicFolder</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Set-PublicFolder cmdlet to set the attributes of public folders.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-PublicFolderDatabase</p>	<p>This cmdlet is available only in Exchange Server 2010.</p> <p>Use the Set-PublicFolderDatabase cmdlet to set attributes of public folder databases.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-SharingPolicy</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Set-SharingPolicy cmdlet to modify existing sharing policies that control how users inside your organization can share free/busy and contact information with users outside your organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-SiteMailbox</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Set-SiteMailbox cmdlet to change a site mailbox's settings, such as the Microsoft SharePoint URL. This cmdlet is primarily</p>

Cmdlet	Description
	<p>used by the SharePoint and Microsoft Exchange user interfaces, such as the SharePoint URL. This cmdlet should only be used for diagnostic and troubleshooting purposes.</p> <p>Site mailboxes were deprecated in Exchange Online and SharePoint Online in 2017. For more information, see Deprecation of Site Mailboxes.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-SiteMailboxProvisioningPolicy</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Set-SiteMailboxProvisioningPolicy cmdlet to modify an existing site mailbox provisioning policy.</p> <p>Site mailboxes were deprecated in Exchange Online and SharePoint Online in 2017. For more information, see Deprecation of Site Mailboxes.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Suspend-PublicFolderReplication</p>	<p>This cmdlet is available only in Exchange Server 2010.</p> <p>Use the Suspend-PublicFolderReplication cmdlet to stop public folder replication for the organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Test-OrganizationRelationship</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Test-OrganizationRelationship cmdlet to verify that the organization relationship is properly configured and functioning as expected.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
<p>Test-SiteMailbox</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Test-SiteMailbox cmdlet to test the site mailbox to Microsoft SharePoint connectivity and to test whether users have the correct permissions to use a site mailbox. This cmdlet should be used for troubleshooting and diagnostic purposes.</p> <p>Site mailboxes were deprecated in Exchange Online and SharePoint Online in 2017. For more information, see Deprecation of Site Mailboxes.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Update-PublicFolder</p>	<p>This cmdlet is available only in Exchange Server 2010.</p> <p>Use the Update-PublicFolder cmdlet to start content synchronization of a public folder.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Update-PublicFolderHierarchy</p>	<p>This cmdlet is available only in Exchange Server 2010.</p> <p>Use the Update-PublicFolderHierarchy cmdlet to start content synchronization of the public folder hierarchy.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Update-PublicFolderMailbox</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Update-PublicFolderMailbox cmdlet to update the hierarchy for public folders.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
Update-SiteMailbox	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Update-SiteMailbox cmdlet to trigger a Microsoft SharePoint synchronization. This command synchronizes document content membership and permissions into Microsoft Exchange. You might need to perform this action when troubleshooting document or membership synchronization issues.</p> <p>Site mailboxes were deprecated in Exchange Online and SharePoint Online in 2017. For more information, see Deprecation of Site Mailboxes.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Cmdlet	Description
Disable-UMAutoAttendant	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Disable-UMAutoAttendant cmdlet to disable an existing Unified Messaging (UM) auto attendant that's enabled.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Disable-UMCallAnsweringRule	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Disable-UMCallAnsweringRule cmdlet to disable a call answering rule that is created within a UM-enabled mailbox.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Disable-UMIPGateway	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Disable-UMIPGateway cmdlet to disable a Unified Messaging (UM) IP gateway.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
Disable-UMMailbox	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Disable-UMMailbox cmdlet to disable Unified Messaging (UM) for UM-enabled mailboxes.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Disable-UMServer	<p>This cmdlet is available only in Exchange Server 2010.</p> <p>Use the Disable-UMServer cmdlet to set the status of an Exchange Server 2010 Unified Messaging (UM) server to disabled. This prevents the Unified Messaging server from processing UM calls.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Disable-UMService	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Disable-UMService cmdlet to set the status of an Exchange Server 2010 Unified Messaging server to disabled. This prevents the UM server from processing UM incoming calls.</p> <p>You can run this cmdlet in Exchange 2013 or Exchange 2016, but the target server must be an Exchange 2010 UM server. You can't use this cmdlet to disable the UM service on Exchange 2013 or Exchange 2016 Mailbox servers.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Enable-UMAutoAttendant	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Enable-UMAutoAttendant cmdlet to enable an existing Unified Messaging (UM) auto attendant that's disabled.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
Enable-UMCallAnsweringRule	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Enable-UMCallAnsweringRule cmdlet to enable a call answering rule that is created within a UM-enabled mailbox.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Enable-UMIPGateway	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Enable-UMIPGateway cmdlet to enable a Unified Messaging (UM) IP gateway.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Enable-UMMailbox	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Enable-UMMailbox cmdlet to enable Unified Messaging (UM) for existing mailbox users.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Enable-UMServer	<p>This cmdlet is available only in Exchange Server 2010.</p> <p>Use the Enable-UMServer cmdlet to set the status of a Unified Messaging (UM) server to enabled. This enables the Unified Messaging server to process UM calls.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Enable-UMService	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Enable-UMService cmdlet to set the status of an Exchange Server 2010 Unified Messaging (UM) server to enabled. This setting enables the Unified Messaging server to process UM calls.</p>

Cmdlet	Description
	<p>You can run this cmdlet in Exchange 2013 or Exchange 2016, but the target server must be an Exchange 2010 UM server. You can't use this cmdlet to enable the UM service on Exchange 2013 or Exchange 2016 Mailbox servers.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Export-UMCallDataRecord</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Export-UMCallDataRecord cmdlet to export Unified Messaging (UM) call data records for UM dial plans and UM IP gateways for a date that you've specified.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Export-UMPrompt</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Export-UMPrompt cmdlet to export an audio file being used as a greeting prompt for Unified Messaging (UM) dial plans and auto attendants.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-OnlineMeetingConfiguration</p>	<p>This cmdlet is functional only in the cloud-based service.</p> <p>Use the Get-OnlineMeetingConfiguration cmdlet to view status and usage information about Skype Meetings and Skype for Business Online for mailboxes. Skype Meetings automatically includes Skype for Business Online conference join information in Exchange Online meeting invitations.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-UMActiveCalls</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Get-UMActiveCalls cmdlet to return information about the calls that are active and being processed by the Mailbox server running the Microsoft Exchange Unified Messaging service.</p>

Cmdlet	Description
	<p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-UMAutoAttendant</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Get-UMAutoAttendant cmdlet to retrieve the properties and the values for a Unified Messaging (UM) auto attendant.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-UMCallAnsweringRule</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Get-UMCallAnsweringRule cmdlet to view the properties of a Unified Messaging (UM) call answering rule that is created within a UM-enabled mailbox.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-UMCallDataRecord</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Get-UMCallDataRecord cmdlet to display Unified Messaging (UM) call data records for a specific UM-enabled user's mailbox.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-UMCallRouterSettings</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Get-UMCallRouterSettings cmdlet to view the settings of the Microsoft Exchange Unified Messaging Call Router service. This service exists on Exchange servers that have the Client Access server role installed, and is used by telephony clients to connect to Exchange.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-UMCallSummaryReport</p>	<p>This cmdlet is available only in on-premises Exchange.</p>

Cmdlet	Description
	<p>Use the <code>Get-UMCallSummaryReport</code> cmdlet to return statistics about all calls received or placed by Mailbox servers running the Microsoft Exchange Unified Messaging service in an organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-UMDialPlan</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the <code>Get-UMDialPlan</code> cmdlet to display the properties of a single Unified Messaging (UM) dial plan or to return a list of all UM dial plans associated with Mailbox servers running the Microsoft Exchange Unified Messaging service.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-UMHuntGroup</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the <code>Get-UMHuntGroup</code> cmdlet to display the properties and values for an existing Unified Messaging (UM) hunt group.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-UMIPGateway</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the <code>Get-UMIPGateway</code> cmdlet to return a list of properties and values for a specified Unified Messaging (UM) IP gateway or a list of UM IP gateways.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
Get-UMMailbox	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Get-UMMailbox cmdlet to view existing mailboxes that are Unified Messaging (UM) enabled.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Get-UMMailboxPolicy	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Get-UMMailboxPolicy cmdlet to display the properties and values of a Unified Messaging (UM) mailbox policy.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Get-UMService	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Get-UMService cmdlet to view the settings of the Microsoft Exchange Unified Messaging service on Exchange 2013 or Exchange 2016 Mailbox servers.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Import-UMPrompt	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Import-UMPrompt cmdlet to copy or upload a custom audio file to be used by Unified Messaging (UM) dial plans and auto attendants.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
New-UMAutoAttendant	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the New-UMAutoAttendant cmdlet to create a Unified Messaging (UM) auto attendant.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
New-UMCallAnsweringRule	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the New-UMCallAnsweringRule cmdlet to create a call answering rule.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
New-UMDialPlan	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the New-UMDialPlan cmdlet to create a Unified Messaging (UM) dial plan to establish a link between UM IP gateways, UM hunt groups, and Mailbox servers to enable communication between Unified Messaging components.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
New-UMHuntGroup	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the New-UMHuntGroup cmdlet to create a Unified Messaging (UM) hunt group used to link incoming calls to a specific UM dial plan.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
New-UMIPGateway	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the New-UMIPGateway cmdlet to create a Unified Messaging (UM) IP gateway. A UM IP gateway is used to connect Unified Messaging servers to an IP gateway or a Session Initiation Protocol (SIP)-enabled IP Private Branch eXchange (PBX).</p>

Cmdlet	Description
	<p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-UMMailboxPolicy</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the New-UMMailboxPolicy cmdlet to create a Unified Messaging (UM) mailbox policy.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-UMAutoAttendant</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Remove-UMAutoAttendant cmdlet to delete a Unified Messaging (UM) auto attendant.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-UMCallAnsweringRule</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Remove-UMCallAnsweringRule cmdlet to remove an existing Unified Messaging (UM) call answering rule.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-UMDialPlan</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Remove-UMDialPlan cmdlet to delete an existing Unified Messaging (UM) dial plan.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-UMHuntGroup</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Remove-UMHuntGroup cmdlet to remove and delete an existing Unified Messaging (UM) hunt group.</p>

Cmdlet	Description
	<p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-UMIPGateway</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Remove-UMIPGateway cmdlet to delete a Unified Messaging (UM) IP gateway.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-UMMailboxPolicy</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Remove-UMMailboxPolicy cmdlet to delete a Unified Messaging (UM) mailbox policy.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-UMAutoAttendant</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Set-UMAutoAttendant cmdlet to modify an existing Unified Messaging (UM) auto attendant.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-UMCallAnsweringRule</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Set-UMCallAnsweringRule cmdlet to change properties of an existing UM call answering rule.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-UMCallRouterSettings</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Set-UMCallRouterSettings cmdlet to modify the configuration of the Microsoft Exchange Unified Messaging Call Router service. This service</p>

Cmdlet	Description
	<p>exists on Exchange servers that have the Client Access server role installed, and is used by telephony clients to connect to Exchange.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-UMDialPlan</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Set-UMDialPlan cmdlet to set various properties on a Unified Messaging (UM) dial plan.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-UMIPGateway</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Set-UMIPGateway cmdlet to modify the configuration settings for a single Unified Messaging (UM) IP gateway or to return a list of configuration settings that can be modified on a specified UM IP gateway.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-UMMailbox</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Set-UMMailbox cmdlet to set the Unified Messaging (UM) properties for a user who is currently UM-enabled.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-UMMailboxPIN</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Set-UMMailboxPIN cmdlet to reset the PIN for a Unified Messaging (UM)-enabled mailbox.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-UMMailboxPolicy</p>	<p>This cmdlet is available only in on-premises Exchange.</p>

Cmdlet	Description
	<p>Use the Set-UMMailboxPolicy cmdlet to modify a Unified Messaging (UM) mailbox policy.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-UMService</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Set-UMService cmdlet to modify the properties of the Microsoft Exchange Unified Messaging service on Exchange 2013 or Exchange 2016 Mailbox servers.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Test-UMConnectivity</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Test-UMConnectivity cmdlet to test the operation of Unified Messaging (UM) servers.</p> <p>Note: This cmdlet works best in Exchange 2010. In later versions of Exchange, the functionality of this cmdlet is replaced by Managed Availability. For the best results, use the Invoke-MonitoringProbe cmdlet and specify the relevant active monitor probe instead of using this cmdlet.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
Add-DistributionGroupMember	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Add-DistributionGroupMember cmdlet to add a single recipient to distribution groups and mail-enabled security groups. To replace all members, use the Update-DistributionGroupMember cmdlet.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Add-UnifiedGroupLinks	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Add-UnifiedGroupLinks cmdlet to add members, owners and subscribers to Microsoft 365 Groups in your cloud-based organization. To remove members, owners, and subscribers, use the Remove-UnifiedGroupLinks cmdlet. To modify other properties of Microsoft 365 Groups, use the Set-UnifiedGroup cmdlet.</p> <p>Note</p> <p>You can't use this cmdlet to modify Microsoft 365 Group members, owners, or subscribers if you connect using certificate based authentication (also known as CBA or app-only authentication for unattended scripts) or Azure managed identity. You can use Microsoft Graph instead. For more information, see Group resource type.</p> <p>Using this cmdlet, only group members can be owners of the group. Add users as members before you add them as owners. This limitation doesn't apply in web management portals where you can add non-members as group owners. Guest users can never be group owners.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Disable-DistributionGroup	<p>This cmdlet is available only in on-premises Exchange.</p>

Cmdlet	Description
	<p>Use the Disable-DistributionGroup cmdlet to remove email capabilities from existing mail-enabled security groups and distribution groups.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Disable-MailContact</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Disable-MailContact cmdlet to remove email capabilities from existing mail contacts.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Disable-MailUser</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Disable-MailUser cmdlet to remove email capabilities from existing mail users.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Enable-DistributionGroup</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Enable-DistributionGroup cmdlet to mail-enable existing universal security groups and universal distribution groups that aren't already mail-enabled.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Enable-MailContact</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Enable-MailContact cmdlet to add email capabilities to existing contacts that aren't already mail-enabled.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
<p>Enable-MailUser</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Enable-MailUser cmdlet to mail-enable existing users that aren't already mail-enabled.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-Contact</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Get-Contact cmdlet to view existing contact objects in your organization. This cmdlet returns contacts and mail contacts.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-DistributionGroup</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Get-DistributionGroup cmdlet to view existing distribution groups or mail-enabled security groups. To view the members of a group, use the Get-DistributionGroupMember cmdlet.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-DistributionGroupMember</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Get-DistributionGroupMember cmdlet to view the members of distribution groups and mail-enabled security groups.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
<p>Get-DynamicDistributionGroup</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Get-DynamicDistributionGroup cmdlet to view existing dynamic distribution groups.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-DynamicDistributionGroupMember</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Get-DynamicDistributionGroupMember cmdlet to view the calculated membership list that's stored on dynamic distribution group objects. The results from this cmdlet are updated every 24 hours.</p> <p>Use the Get-DistributionGroupMember cmdlet to view the members of distribution groups and mail-enabled security groups.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-EligibleDistributionGroupForMigration</p>	<p>This cmdlet is functional only in the cloud-based service.</p> <p>Use the Get-EligibleDistributionGroupForMigration cmdlet to identify distribution groups that can be upgraded to Microsoft 365 Groups. You can't upgrade mail-enabled security groups to Microsoft 365 Groups.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-Group</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Get-Group cmdlet to view existing group objects in your organization. In all environments, this cmdlet returns mail-enabled security groups, distribution groups, role groups, and room lists.</p>

Cmdlet	Description
	<p>For details about other supported group types in on-premises Exchange environments, see the RecipientTypeDetails parameter description.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-LinkedUser</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Get-LinkedUser cmdlet to view existing linked user accounts.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-MailContact</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Get-MailContact cmdlet to view existing mail contacts.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-MailUser</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Get-MailUser cmdlet to view mail users and also guest users for Microsoft 365 Groups in cloud environments.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-Recipient</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Get-Recipient cmdlet to view existing recipient objects in your organization. This cmdlet returns all mail-enabled objects</p>

Cmdlet	Description
	<p>(for example, mailboxes, mail users, mail contacts, and distribution groups).</p> <p>Note: In Exchange Online PowerShell, we recommend that you use the Get-EXORecipient cmdlet instead of this cmdlet. For more information, see Connect to Exchange Online PowerShell.</p> <p>In cloud environments, to return Microsoft 365 Groups, you need to use the RecipientTypeDetails parameter with the value GroupMailbox.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-SecurityPrincipal</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Get-SecurityPrincipal cmdlet to return a list of security principals. Security principals are entities, such as users or security groups, which can be assigned permissions and user rights.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-UnifiedGroup</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Get-UnifiedGroup cmdlet to view Microsoft 365 Groups in your cloud-based organization. To view members, owners and subscribers for Microsoft 365 Groups, use the Get-UnifiedGroupLinks cmdlet.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-UnifiedGroupLinks</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Get-UnifiedGroupLinks cmdlet to view membership and ownership information for Microsoft 365 Groups in your cloud-</p>

Cmdlet	Description
	<p>based organization. To view other properties for Microsoft 365 Groups, use the Get-UnifiedGroup cmdlet.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-User</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Get-User cmdlet to view existing user objects in your organization. This cmdlet returns all objects that have user accounts (for example, user mailboxes, mail users, and user accounts).</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-DistributionGroup</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the New-DistributionGroup cmdlet to create distribution groups and mail-enabled security groups.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>New-DynamicDistributionGroup</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the New-DynamicDistributionGroup cmdlet to create dynamic distribution groups. A dynamic distribution group queries mail-enabled objects and builds the group membership based on the results. The group membership is recalculated whenever an email message is sent to the group.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
New-MailContact	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the New-MailContact cmdlet to create mail contacts.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
New-MailUser	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the New-MailUser cmdlet to create mail users. Mail users (also known as mail-enabled users) have email addresses and accounts in the Exchange organization, but they don't have Exchange mailboxes. Email messages sent to mail users are delivered to the specified external email address.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
New-UnifiedGroup	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the New-UnifiedGroup cmdlet to create Microsoft 365 Groups in your cloud-based organization. To add members, owners, and subscribers to Microsoft 365 Groups, use the Add-UnifiedGroupLinks cmdlet.</p> <p>Note: You can't use this cmdlet to create Microsoft 365 Groups if you connect using certificate based authentication (also known as CBA or app-only authentication for unattended scripts) or Azure managed identity. You can use Microsoft Graph instead. For more information, see Create group.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Remove-DistributionGroup	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be</p>

Cmdlet	Description
	<p>exclusive to one environment or the other.</p> <p>Use the Remove-DistributionGroup cmdlet to remove distribution groups and mail-enabled security groups.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-DistributionGroupMember</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Remove-DistributionGroupMember cmdlet to remove a single member from distribution groups or mail-enabled security groups. To replace all members, use the Update-DistributionGroupMember cmdlet.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-DynamicDistributionGroup</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Remove-DynamicDistributionGroup cmdlet to delete dynamic distribution groups.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-MailContact</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Remove-MailContact cmdlet to delete existing mail contacts.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
<p>Remove-MailUser</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Remove-MailUser cmdlet to remove existing mail users.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-UnifiedGroup</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Remove-UnifiedGroup cmdlet to remove Microsoft 365 Groups from your cloud-based organization.</p> <p>Note: You can't use this cmdlet to remove Microsoft 365 Groups if you connect using certificate based authentication (also known as CBA or app-only authentication for unattended scripts) or Azure managed identity. You can use Microsoft Graph instead. For more information, see Delete group.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Remove-UnifiedGroupLinks</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Remove-UnifiedGroupLinks cmdlet to remove members, owners, and subscribers from Microsoft 365 Groups in your cloud-based organization. To add members, owners and subscribers, use the Add-UnifiedGroupLinks cmdlet. To modify other properties of Microsoft 365 Groups, use the Set-UnifiedGroup cmdlet.</p> <p>Note</p> <p>You can't use this cmdlet to modify Microsoft 365 Group members, owners, or subscribers if you connect using certificate based authentication (also known as CBA or app-only authentication for unattended scripts) or Azure managed identity. You can use Microsoft Graph instead. For more information, see Group resource type.</p>

Cmdlet	Description
	<p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-Contact</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Set-Contact cmdlet to modify contact object settings. If the contact is a mail contact, you can use the Set-MailContact cmdlet to modify other Microsoft Exchange settings that aren't available by using the Set-Contact cmdlet.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-DistributionGroup</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Set-DistributionGroup cmdlet to modify the settings of existing distribution groups or mail-enabled security groups. To add or remove group members, use the Add-DistributionGroupMember, Remove-DistributionGroupMember or Update-DistributionGroupMember cmdlets.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-DynamicDistributionGroup</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Set-DynamicDistributionGroup cmdlet to modify existing dynamic distribution groups.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-Group</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be</p>

Cmdlet	Description
	<p>exclusive to one environment or the other.</p> <p>Use the Set-Group cmdlet to modify group object settings. If the group is a mail-enabled security group or a distribution group, you can use the Set-DistributionGroup cmdlet to modify other Microsoft Exchange settings that aren't available by using the Set-Group cmdlet.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-LinkedUser</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Set-LinkedUser cmdlet to modify the properties of an existing linked user account. The Outlook Live Directory Sync (OLSync) service account is a linked user.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-MailContact</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Set-MailContact cmdlet to modify existing mail contacts.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-MailUser</p>	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Set-MailUser cmdlet to modify mail users. Mail users (also known as mail-enabled users) have email addresses and accounts in the Exchange organization, but they don't have Exchange mailboxes.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Cmdlet	Description
Set-UnifiedGroup	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Set-UnifiedGroup cmdlet to modify Microsoft 365 Groups in your cloud-based organization. To modify members, owners, and subscribers of Microsoft 365 Groups, use the Add-UnifiedGroupLinks and Remove-UnifiedGroupLinks cmdlets.</p> <p>Important: You can't use this cmdlet to remove all Microsoft Online Email Routing Address (MOERA) addresses from the Microsoft 365 Group. There must be at least one MOERA address attached to a group. To learn more about MOERA addresses, see How the proxyAddresses attribute is populated in Microsoft Entra ID.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Set-User	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p> <p>Use the Set-User cmdlet to modify user attributes. You can use this cmdlet to modify all objects that have user accounts (for example, user mailboxes, mail users, and user accounts).</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Undo-SoftDeletedUnifiedGroup	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Undo-SoftDeletedUnifiedGroup cmdlet to restore soft-deleted Microsoft 365 Groups in your cloud-based organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Update-DistributionGroupMember	<p>This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings might be exclusive to one environment or the other.</p>

Cmdlet	Description
	<p>Use the Update-DistributionGroupMember cmdlet to replace all members of distribution groups and mail-enabled security groups. To add or remove existing group members, use the Add-DistributionGroupMember and Remove-DistributionGroupMember cmdlets.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Upgrade-DistributionGroup</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Upgrade-DistributionGroup cmdlet to upgrade distribution groups to Microsoft 365 Groups. This cmdlet only works on distribution groups, not mail-enabled security groups.</p> <p>Note: Before you use this cmdlet, verify there are no email address policies that you created with the IncludeUnifiedGroupRecipients parameter; otherwise the command will fail. Remove and recreate the email address policies after you upgrade your distribution groups to Microsoft 365 Groups.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
Cmdlet	Description
<p>Get-ADSiteLink</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Get-ADSiteLink cmdlet to view configuration information about an Active Directory IP site link.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-MailFlowStatusReport</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Get-MailFlowStatusReport cmdlet to return the message counts for a specific date range organized by the final disposition of the message for the last 90 days.</p>

Cmdlet	Description
	<p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-MessageTraceDetailV2</p>	
<p>Get-MessageTraceV2</p>	<p>This cmdlet is available only in the cloud-based service.</p> <p>Use the Get-MessageTraceV2 cmdlet to trace messages as they pass through the cloud-based organization.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-UMMailboxPin</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Get-UMMailboxPin cmdlet to return information from a Unified Messaging (UM)-enabled user's mailbox.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Get-UMServer</p>	<p>This cmdlet is available only in Exchange Server 2010.</p> <p>Use the Get-UMServer cmdlet to view settings that are associated with the Unified Messaging (UM) server role.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-ADSiteLink</p>	<p>This cmdlet is available only in on-premises Exchange.</p> <p>Use the Set-ADSiteLink cmdlet to assign an Exchange-specific cost to an Active Directory IP site link. You can also use this cmdlet to configure the maximum message size that can pass across an Active Directory IP site link.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>
<p>Set-UMServer</p>	<p>This cmdlet is available only in Exchange Server 2010.</p>

Cmdlet	Description
	<p>Use the Set-UMServer cmdlet to modify settings that are associated with the Unified Messaging (UM) server role.</p> <p>For information about the parameter sets in the Syntax section below, see Exchange cmdlet syntax.</p>

Source: <https://docs.microsoft.com/en-us/powershell/module/exchange/?view=exchange-ps#mailboxes>