Managed Services Policies Pushed Out

Office 365 Best Practices

Exchange Online Operations:

Additional Spam Policy

This script will create a new spam policy in Exchange Online.

Script will connect to Azure AD, then save all domains. It will then check to see whether a policy of the same name already exists and if it does it will not try and create a new script.

If there is no existing policy the following policies will be set:

Bulk Spam Action: Move the message to the user's Quarantine. Is required by zero-hour auto purge (ZAP) for spam. ZAP is an automatic purge/deletion of data (emails in this case) that are no longer needed or are older than a specific duration of time.

Bulk Threshold: specifies the Bulk Complaint Level (BCL) threshold setting. Valid values are from 1 - 9, where 1 marks most bulk email as spam, and 9 allows the most bulk email to be delivered. This determines what level of bulk spam is allowed into the inbox, and what is held in quarantine. We set it to 4 by default.

H**igh Confidence Spam Action:** Specifies the action to take on messages that are classified as high confidence spam. Our setting routes high confidence spam to quarantine.

I**n Line Safety Tips Enabled**: Specifies whether to enable or disable safety tips that are shown to recipients in messages. We have enabled these tips.

Mark as Spam Bulk Mail: Classifies the message as spam when the message is identified as a bulk email message. This policy is enabled.

Enable Language Blocklist: Enables or disables blocking email messages that are written in specific languages, regardless of the message contents. This specifies the languages to block when messages are blocked based on their language. See below the language blocklist:

'af','sq','ar','hy','az','bn','eu','be','bs','br','bg','ca','zh-cn','zh-

tw','hr','cs','da','nl','eo','et','fo','tl','fi','fr','fy','gl','ka','de','el','kl','gu','ha','he','hi','hu','is','id','ga','zu','it','ja','kn','kk','sw','ko','ku','ky','la','lv','lt','lb','mk','ms','ml','mt','mi','mr','mn','nb','nn','ps','fa','pl','pt','pa','ro','rm','ru','se','sr','sk','sl','wen','es','sv','ta','te','th','tr','uk','ur','uz','vi','cy','yi'

Enable Region Blocklist: Enables or disables blocking email messages that are sent from specific countries or regions, regardless of the message contents. Specifies the region to block when messages are blocked based on their source region. See below the region blocklist:

'AF','AL','DZ','AO','AI','AM','AZ','BD','BY','BZ','BJ','BT','BO','BQ','BW','BV','BF','BI','CV','CM','CF','TD','KM','CG','CD','CI','CW','DJ','DM','DO','EC','EG','SV','GQ','ER','ET','GA','GM','GE','GH','GP','GT','GN','GW','GY','HT','HM','HN','IR','IQ','XJ','SJ','JO','KZ','KG','LA','LV','LB','LS','LR','LY','MO','MK','MW','MV','ML','MR','MU','YT','MF','MN','ME','MS','MZ','MM','NA','NE','NG','NU','KP','MP','OM','PK','PW','PS','PA','PY','PE','RE','RU','RW','XS','BL','KN','LC','PM','VC','ST','SN','RS','SC','SL','XE','SX','SI','SO','SH','SD','SR','SZ','SY','TJ','TZ','TK','TN','TM','TC','TV','UG','UA','UY','UZ','VE','WF','YE','ZM','ZW'

Increase Score with Image Links: Increases the spam score of messages that contain image links to remote websites. This increases the level of spam confidence, and the likeliness to be quarantined. We have this setting turned off.

Increase Score with Numeric Ips: Increases the spam score of messages that contain links to IP addresses. This increases the level of spam confidence, and the likeliness to be quarantined. We have this setting turned off.

Increase Score with Redirect to other port: Increases the spam score of messages that contain links that redirect to other TCP ports. This increases the level of spam confidence, and the likeliness to be quarantined. We have this setting turned off.

Increase score with .biz or .info URLs = off: Increases the spam score of messages that contain links to .biz or .info domains. This increases the level of spam confidence, and the likeliness to be quarantined. We have this setting turned off.

Mark as spam empty messages: Classifies the message as spam when the message is empty. We have this setting turned off.

Mark as spam java script in html: Classifies the message as spam when the message contains JavaScript or VBScript. We have this setting turned off.

Mark as spam frames in html: Classifies the message as spam when the message contains HTML frame or iframe tags. These tags can divide a browser into multiple

sections, which can all display different content or embed external content. We have this setting turned off.

Mark as spam object tags in html: Classifies the message as spam when the message contains HTML object tags. We have this setting turned off.

M**ark as spam embed tags in html**: Classifies the message as spam when the message contains HTML embed tags. We have this setting turned off.

M**ark as spam form tags in html**: Classifies the message as spam when the message contains HTML form tags. We have this setting turned off.

M**ark as spam web bugs in html**: Classifies the message as spam when the message contains web bugs. We have this setting turned off.

M**ark as spam sensitive wordlist**: Classifies the message as spam when the message contains words from the sensitive words list. We have this setting turned off.

Markas spam SPF record hard fail: Classifies the message as spam when Sender Policy Framework (SPF) record checking encounters a hard fail. We have this setting turned off.

Mark as spam from address auth fail: Classifies the message as spam when Sender ID filtering encounters a hard fail. We have this setting turned off.

M**ark as spam NDR back scatter =off**: Classifies the message as spam when the message is a non-delivery report (NDR) to a forged sender. We have this setting turned off.

Phish spam action: Specifies the action to take on messages that are classified as phishing (messages that use fraudulent links or spoofed domains to get personal information. We have it set to route to quarantine, and is required by zero-hour auto purge (ZAP) for spam.

Spam action: Specifies the action to take on messages that are classified as spam (not high confidence spam, bulk email, or phishing). We have it set to route to quarantine and is required by zero-hour auto purge (ZAP) for spam.

Enable end user spam notifications: End-users periodically receive notifications when a message that was supposed to be delivered to them was quarantined as spam. We have this setting turned on.

Enable spam notification frequency: The End User Spam Notification Frequency parameter specifies the repeat interval in days that end-user spam quarantine notifications are sent. A valid value is an integer between 1 and 15. We set it to 3 by default.

Quarantine Retention Period: The Quarantine Retention Period parameter specifies the number of days that spam messages remain in quarantine when an email is sent to quarantine due to a spam filter. We have this setting set to 30 days.

Zap enabled: Specifies whether to enable zero-hour auto purge (ZAP) for spam. ZAP detects unread spam messages that have already been delivered to the user's Inbox. Unread spam messages that are detected in the user's Inbox are automatically moved to the Junk Email folder. We have this setting enabled.

Additional Malware Policy

This script will create a new malware policy in Exchange Online. A new script is created to allow easier debugging and management.

Script will connect to Azure AD and check to see whether a policy of the same name already exists and if it does it will not try and create a new script.

If there is no existing policy the following parameters will be set:

File type action: Specifies the action to take when malware is detected in a message. If malware is detected in an email, the email is rejected and an NDR message is sent to the sender.

Enable file filter: Enables or disables common attachment blocking. This is the filter that will reject emails based on the file extensions of attachments. We have this setting turned on.

Enable External Sender Admin Notifications: Enables or disables sending notification messages to an administrator when malware is detected in messages from external senders. We have this setting turned off

Internal Sender Admin Address: Specifies the email address of the administrator who will receive notifications messages when messages from internal senders contain malware.

External Sender Admin Address: Specifies the email address of the administrator who will receive notifications messages when messages from external senders contain malware.

ZAP enabled: Whether to enable zero-hour auto purge (ZAP) for malware. ZAP detects malware in unread messages that have already been delivered to the user's Inbox. Unread messages in the user's Inbox that contain malware are moved to the Junk Email folder. We have this setting turned on.

Connection Filtering Policy

Reports on all the connection policies and their settings in a tenant.

Mailbox Alerts Policy

This policy will enable alerts for mailboxes in Exchange online.

Each mailbox will have its auditing enabled.

Extend Mailbox Audit Log Time Limit

Sets the maximum age of audit log entries mailboxes. Log entries older than the specified value are removed. The specified value we set is 90 days.

Extend deleted items retention

Sets all mailbox deleted items retention period to 30 days

Enable Mailbox Archive

Set mailbox archiving for all tenant mailboxes that it isn't enabled for.

Sets mailbox archiving for all tenant mailboxes that currently don’t have their email archiving enabled. This minimises the amount of information that is synced down locally to a device, and how much storage it takes up in the drive.

Set Remote Domain Options

This script sets the remote domain option for Exchange Online for the tenant.

Sets the follow parameters:

Allowed OOF Type: Specifies the type of automatic replies or out-of-office (also known as OOF) notifications than can be sent to recipients in the remote domain. We have this set to external, so only automatic replies that are designated as external are sent to recipients in the remote domain.

Auto Forward Enabled: Specifies whether to allow messages that are auto forwarded

by client email programs in your organization. We have this set to false, which means auto-forwarded messages aren't delivered to recipients in the remote domain.

Auto Reply Enabled: Specifies whether to allow messages that are automatic replies from client email programs in your organization (for example, automatic reply messages that are generated by rules in Outlook. We have this enabled, so automatic replies are delivered to recipients in the remote domain.

Delivery Report: Specifies whether to allow delivery reports from client software in your organization to recipients in the remote domain. We have this option enabled.

Meeting Forward Notification Enabled: Specifies whether to enable meeting forward notifications for recipients in the remote domain. We have this enabled, meaning meeting requests forwarded to recipients in the remote domain generate a meeting forward notification to the meeting organizer.

TNEF: Specifies whether Transport Neutral Encapsulation Format (TNEF) message encoding is used on messages sent to the remote domain. We have this setting turned off, meaning TNEF encoding isn't specified for the remote domain. This is the default value.

Trusted Mail Inbound: Specifies whether messages from senders in the remote domain are treated as trusted messages. We have this setting turned off, meaning inbound messages from senders in the remote domain won't bypass content filtering and recipient filtering. This is the default value.

Trusted Mail Outbound: Specifies whether messages sent to recipients in the remote domain are treated as trusted messages. We have this setting turned off, meaning outbound messages to recipients in the remote domain won't bypass content filtering and recipient filtering. This is the default value.

Disable Mailbox Forwards

This script disables all individual Exchange Online mailbox forwarding. This will disable any mailbox that has forwarding configured.

This script sets the following options for all mailboxes:

Forwarding Address: Specifies a forwarding address in your organization for messages that are sent to this mailbox. You can use any value that uniquely identifies the internal

recipient. We have this policy not configured by default but can configure for email forwarding as required. This means no forwarding recipient is configured.

Forwarding SMTP Address: Specifies a forwarding SMTP address for messages that are sent to this mailbox. Typically, this is used to specify external email addresses that aren't validated. We have this setting not configured by default, which means no forwarding email address is configured

This script simply removes any existing mailbox forwarding, it does not prevent forwarding from being reconfigured on the mailbox after this script is run. If you wish to block email forwarding for all mailboxes permanently then do that at the tenant level.

Disable IMAP and POP for Mailboxes

This script disables all individual Exchange Online mailbox POP and IMAP Access. This will disable any mailbox that has these protocols enabled configured.

Disable Exchange Web Services for Mailboxes

Exchange Web Services (EWS) is a cross-platform API that enables applications to access mailbox items such as email messages, meetings, and contacts from Exchange Online, Exchange Online as part of Office 365, or on-premises versions of Exchange starting with Exchange Server 2007.

The disabling of EWS Prevents these connections from being possible.

Set Exchange Online Tenant Best Practices

This script sets the Exchange Online tenant to best practices settings. This will change the way that email functions within the tenant.

This script will firstly check to see whether the expanding archive option has been set for all mailboxes. If it hasn't, then all mailboxes will be enabled for auto expanding archive.

The script will then set the following options:

Activity based authentication time out: enables timed logoff feature

Activity Based Authentication Timeout Interval: Specifies the time span for logoff. We have set it to 30 minutes by default.

Activity Based Authentication Timeout with Single Sign on: Specifies whether to keep single sign-on enabled. We have kept it enabled.

Apps for Office: Specifies whether to enable apps for Outlook features. We have this policy enabled. If the policy is turned off, no new apps can be activated for any user in the organization.

Audit Disabled: This feature specifies whether to enable or disable mailbox auditing for the organization. Auditing is disabled when this feature is on. We enable auditing of mailboxes, so we have this feature turned off.

Bookings Enabled: Specifies whether to enable Microsoft Bookings in an Exchange Online organization. We have this setting enabled.

Bookings Payments Enabled: Specifies whether to enable online payment node inside Bookings. We have this setting enabled.

Bookings Social Sharing Restricted: This feature allows control as to whether, or not, users can see social sharing options inside Bookings. We have this setting disabled.

Connectors Actionable Messages: Specifies whether to enable or disable actionable buttons in messages (connector cards) from connected apps on Outlook on the web. We have this setting enabled.

Connectors Enabled: Specifies whether to enable or disable all connected apps in organization. The workloads that are affected by this parameter are Outlook, SharePoint, Teams, and Yammer.

Connectors enabled for Outlook: Specifies whether to enable or disable connected apps in Outlook on the web. We have this enabled.

Connectors enabled for SharePoint: Specifies whether to enable or disable connected apps on Sharepoint. We have this setting enabled.

Connectors enabled for teams: Specifies whether to enable or disable connected apps on Teams. We have this setting enabled.

Connectors enabled for Yammer: Specifies whether to enable or disable connected apps on Yammer. We have this setting enabled.

Default group access type: Specifies the default access type for Office 365 groups. We have group access set to private, meaning only allowed members can access them.

Distribution group name blocked words list: Specifies words that can't be included in the names of distribution groups. We have this setting not configured by default, so every word is allowed.

EWS allow entourage: Specifies whether to enable or disable Entourage 2008 to access Exchange Web Services (EWS) for the entire organization.

Exchange notification: Enables or disables Exchange notifications sent to administrators regarding their organizations. We have this setting enabled.

Exchange Notification Recipients: Specifies the recipients for Exchange notifications sent to administrators regarding their organizations. If this feature is turned off, no notification messages are sent. We have this feature set to send notification messages.

Focused inbox on: Enables or disables Focused Inbox for the organization. We have this feature disabled, but it can be enabled on the end user's side.

Link preview enabled: Specifies whether link preview of URLs in email messages is allowed for the organization. We have this setting turned on.

Mail tips all tips enabled: Specifies whether MailTips are enabled. We have mail tips enabled.

Mail tips external recipients' tips enabled: Specifies whether MailTips for external recipients are enabled. We have this setting turned off.

Mail tips group metrics enabled: Specifies whether MailTips that rely on group metrics data are enabled. We have this setting enabled.

Mail Tips Mailbox Sourced Tips Enabled: Specifies whether MailTips that rely on mailbox data (out-of-office or full mailbox) are enabled. We have this setting enabled.

OAuth2 Client Profile Enabled: Enables or disables modern authentication in the Exchange organization. We have this setting enabled.

Outlook Pay Enabled = $false: Enables or disables Payments in Outlook in the Office 365 organization. We have this setting disabled.

Public Computers Detection Enabled: Specifies whether Outlook on the web will detect when a user signs from a public or private computer or network, and then

enforces the attachment handling settings from public networks. We have this setting enabled.

Read Tracking Enabled: Specifies whether the tracking for read status for messages in an organization is enabled. We have this setting disabled.

SMTP Actionable Messages Enabled: Specifies whether to enable or disable action buttons in email messages in Outlook on the web. We have this setting enabled.

Unblock Unsafe Sender Prompt Enabled: Specifies whether to enable or disable the prompt to unblock unsafe senders in Outlook on the web. We have this setting enabled, meaning unsafe senders can be unblocked.

Web Push Notifications Disabled: Specifies whether to enable or disable Web Push Notifications in Outlook on the Web. This feature provides web push notifications which appear on a user's desktop while the user is not using Outlook on the Web. This brings awareness of incoming messages while they are working elsewhere on their computer. We have this setting disabled.

Web Suggested Replies Disabled: Specifies whether to enable or disable suggested Replies in Outlook on the web. We have this setting disabled.

Enable Litigation Hold for Mailboxes

Enable litigation hold for all mailboxes

This feature preserves all relevant information/documents in a mailbox when litigation is underway or anticipated, preventing the destruction of forementioned information. This feature cycles through all mailboxes and enable litigation hold.

Enable Modern Authentication for Exchange Online

This feature sets the Exchange Online tenant to best practices settings. This will change the way that email functions within the tenant.

It will first check to see whether the expanding archive option has been set for all mailboxes. If it hasn't then all mailboxes will be enabled for auto expanding archive.

The following options will then be set:

Activity based authentication timeout enabled: Specifies whether the timed logoff feature is enabled. We have this feature enabled.

Activity Based Authentication Timeout Interval: Specifies the time span for logoff. We

have this time span set to 30 minutes by default.

Activity Based Authentication Timeout with Single Sign on Enabled: Specifies whether to keep single sign-on enabled. We have this setting enabled.

Apps for Office Enabled: Specifies whether to enable apps for Outlook features. If this setting is turned off, no new apps can be activated for any user in the organization. We have this setting enabled.

Audit Disabled: Specifies whether to disable or enable mailbox auditing for the organization. We have this setting turned off.

Bookings Enabled: Specifies whether to enable Microsoft Bookings in an Exchange Online organization. We have this setting enabled.

Bookings Payments Enabled: Specifies whether to enable online payment node inside Bookings. We have this setting enabled.

Bookings Social Sharing Restricted: This feature allows control as to whether, or not, users can see social sharing options inside Bookings. We have this setting turned off.

Connectors Actionable Messages Enabled: Specifies whether to enable or disable actionable buttons in messages (connector cards) from connected apps on Outlook on the web. We have this setting enabled.

Connectors Enabled: Specifies whether to enable or disable all connected apps in organization. The workloads that are affected by this feature are Outlook, SharePoint, Teams, and Yammer. We have this setting enabled.

Connectors enabled for Outlook: Specifies whether to enable or disable connected apps in Outlook on the web. We have this setting enabled.

Connectors enabled for SharePoint: Specifies whether to enable or disable connected apps on Sharepoint. We have this setting enabled.

Connectors enabled for teams: Specifies whether to enable or disable connected apps on Teams. We have this setting enabled.

Connectors enabled for Yammer: Specifies whether to enable or disable connected apps on Yammer. We have this setting enabled.

Default group access type: Specifies the default access type for Office 365 groups. We have this set to private for default access.

Distribution group name blocked words list: Specifies words that can't be included in the names of distribution groups. We have this feature not configured by default, so nothing is blocked by default.

EWS allow entourage: Specifies whether to enable or disable Entourage 2008 to access Exchange Web Services (EWS) for the entire organization. We have this setting turned off.

Exchange notification enabled: Enables or disables Exchange notifications sent to administrators regarding their organizations. We have this setting enabled.

Exchange Notification Recipients: Specifies the recipients for Exchange notifications sent to administrators regarding their organizations. If the Exchange Notification Enabled feature is turned off, no notification messages are sent. Exchange notifications are sent to all administrators. We have set this feature to notify administrators.

Focused inbox on: Enables or disables Focused Inbox for the organization. We have this feature turned off by default but can be enabled by the user.

Link preview enabled: Specifies whether link preview of URLs in email messages is allowed for the organization. We have this setting enabled.

Mail tips all tips enabled: Specifies whether MailTips are enabled. We have this setting enabled.

Mail tips external recipients tips enabled: Specifies whether MailTips for external recipients are enabled. We have this setting turned off.

Mail tips group metrics enabled: Specifies whether MailTips that rely on group metrics data are enabled. We have this setting enabled.

Mail Tips Mailbox Sourced Tips Enabled: Specifies whether MailTips that rely on mailbox data (out-of-office or full mailbox) are enabled. We have this setting enabled.

OAuth2 Client Profile Enabled: Enables or disables modern authentication in the Exchange organization. We have this setting enabled.

Outlook Pay Enabled: Enables or disables Payments in Outlook in the Office 365

organization. We have this setting turned off.

Public Computers Detection Enabled: Specifies whether Outlook on the web will detect when a user signs from a public or private computer or network, and then enforces the attachment handling settings from public networks. We have this setting enabled. We have this setting enabled.

Read Tracking Enabled: Specifies whether the tracking for read status for messages in an organization is enabled. We have this setting turned off.

SMTP Actionable Messages Enabled: Specifies whether to enable or disable action buttons in email messages in Outlook on the web. We have this setting enabled. We have this setting enabled.

Unblock Unsafe Sender Prompt Enabled: Specifies whether to enable or disable the prompt to unblock unsafe senders in Outlook on the web. We have this setting enabled. This means that unsafe senders can be unblocked.

Web Push Notifications Disabled: Specifies whether to enable or disable Web Push Notifications in Outlook on the Web. This feature provides web push notifications which appear on a user's desktop while the user is not using Outlook on the Web. This brings awareness of incoming messages while they are working elsewhere on their computer. We have this setting turned off.

Web Suggested Replies Disabled: Specifies whether to enable or disable Suggested Replies in Outlook on the web. We have this setting turned off.

Disable Basic Authentication

Basic authentication is also known as *proxy authentication* because the email client transmits the username and password to Exchange Online, and Exchange Online forwards or *proxies* the credentials to an authoritative identity provider (IdP) on behalf of the email client or app. The IdP depends your organization's authentication model:

- **Cloud authentication**: The IdP is Microsoft Entra ID.
- **Federated authentication**: The IdP is an on-premises solution like Active Directory Federation Services (AD FS).

Cloud Authentication:

1. The email client sends the username and password to Exchange Online.

Note: When Basic authentication is blocked, it's blocked at this step.

2. Exchange Online sends the username and password to Microsoft Entra ID.
3. Microsoft Entra ID returns a user ticket to Exchange Online, and the user is authenticated.

Federated Authentication:

1. The email client sends the username and password to Exchange Online.

Note: When Basic authentication is blocked, it's blocked at this step.

2. Exchange Online sends the username and password to the on-premises IdP.
3. Exchange Online receives a Security Assertion Markup Language (SAML) token from the on-premises IdP.
4. Exchange Online sends the SAML token to Microsoft Entra ID.
5. Microsoft Entra ID returns a user ticket to Exchange Online, and the user is authenticated.

How Basic authentication is blocked in Exchange Online:

You block Basic authentication in Exchange Online by creating and assigning authentication policies to individual users. The policies define the client protocols where Basic authentication is blocked, and assigning the policy to one or more users blocks their Basic authentication requests for the specified protocols.

When it's blocked, Basic authentication in Exchange Online is blocked at the first pre-authentication step (Step 1 in the previous diagrams) before the request reaches Microsoft Entra ID or the on-premises IdP. The benefit of this approach is brute force or password spray attacks won't reach the IdP (which might trigger account lock-outs due to incorrect login attempts).

Because authentication policies operate at the user level, Exchange Online can only block Basic authentication requests for users that exist in the cloud organization. For federated authentication, if a user doesn't exist in Exchange Online, the username and password are forwarded to the on-premises IdP.

In an Exchange hybrid deployment, authentication for your on-premises mailboxes will be handled by your on-premises Exchange servers, and authentication policies won't apply. For mailboxes moved to Exchange Online, the Autodiscover service will redirect them to Exchange Online, and then some of the previous scenarios will apply.

Authentication Policy Procedures in Exchange Online

We manage all aspects of authentication policies in Exchange Online. Typically, when blocking Basic authentication for a user, it is recommended that you block Basic authentications for all protocols.

For email clients and apps that don't support modern authentication, you need to allow Basic authentication for the protocols and services that they require. These protocols and services are described in the following table:

Office 365 Centralized Deployment:

Add Standard Outlook Add ins for Users

This feature will deploy the Report Message, Message Header Analyzer and FindTime Outlook Add in centrally to all uses OWA and Outlook on the desktop.

However, the Office 365 Central Deployment module currently does not support MFA and will need to use the web interface to provision these add ins.

Security and Compliance:

Create Standard Activity Alerts

This feature creates several standard Office 365 Activity alerts in the Security and compliance centre.

This feature creates the following alerts:

- SharePoint anti-virus engine detects malware in a file.

- User created an anonymous link to a resource. User updated an anonymous link to a resource. An anonymous user accessed a resource by using an anonymous link.

- User shared a resource in SharePoint Online or OneDrive for Business with a user who isn't in your organization's directory. A SharePoint or global administrator changed a SharePoint sharing policy.

- Change in the unmanaged devices policy. Change in the location-based access policy (also called a trusted network boundary)

- Creation of a new site collection OneDrive for Business site provisioned. A site was deleted. Site collection administrator or owner adds a person as a site collection administrator for a site.

- Site administrator enables Office on Demand, which lets users access the latest version of Office desktop applications.

- An administrator assigned/removed the Full Access mailbox permission to a user (known as a delegate) to another person's mailbox.

- User password changes.

- Added/Removed a user to an admin role in Office 365.

- Change company information or password policy.

- Change of a custom domain in a tenant.

- Looking for search and export of data.

Create Standard Protection Alerts

This feature adds several standard protection alerts to the tenant.

The feature will check to see whether an alert of the same name already exists. If it doesn't then the following alerts are created:

-**User submitted email**: User reported a problem with mail filtering. This can include false positives, missed spam, or missed phishing email messages.

-**Detected malware in files**: Office 365 detected malware in either a SharePoint or OneDrive file.

-**DLP Policy match**: A data loss prevention policy match is detected.

-**Created site collection**: Global administrator creates a new site collection in your SharePoint Online organization.

-**Set host site**: Global administrator changes the designated site to host personal or OneDrive for Business sites.

-**Granted mailbox permission**: User granted permission for same or another user to access a target mailbox.

-**Created anonymous link**: User created an anonymous link to a resource. Anyone with this link can access the resource without having to be authenticated.

-**Created sharing invitation**: User shared a resource in SharePoint Online or OneDrive for Business with a user who isn't in your organization's directory.

-**Added site collection admin**: Site collection administrator or owner adds a person as a site collection administrator for a site. Site collection administrators have full control permissions for the site collection and all subsites.

-**Changed sharing policy**: An administrator changed a SharePoint sharing policy by using the Office 365 Admin centre, SharePoint admin centre, or SharePoint Online Management Shell. Any change to the settings in the sharing policy in your organization will be logged. The policy that was changed is identified in the Modified Property field property when you export the search results.

-**Failed user login attempt**: A user failed to login to the tenant. This is typically because of an incorrect password.

-**Added exempt user agent**: Global administrator adds a user agent to the list of exempt user agents in the SharePoint admin centre.

Add Standard DLP Policies

This feature adds several standard Data Loss Prevention policies to the tenant.

The feature will check to see whether a policy of the same name already exists. If it doesn't then the following policies are created across all data locations (Exchange, OneDrive for Business, SharePoint and Teams):

-**Australian Privacy Act**: Helps detect the presence of information commonly considered to be subject to the privacy act in Australia, like driver's license and passport number.

-**Australian Financial Data**: Helps detect the presence of information commonly considered to be financial data in Australia, including credit cards, and SWIFT codes.

-**Australian Personally Identifiable Information (PII) Data**: Helps detect the presence of information commonly considered to be subject to the privacy act in Australia, like driver's license and passport number.

-**Australian Health Records Act (HRIP Act)**: Helps detect the presence of information commonly considered to be subject to the Health Records and Information Privacy (HRIP) act in Australia, like medical account number and tax file number.

The following common settings are then configured for each policy:

Block access: Specifies an action for the DLP rule that blocks access to the source item when the conditions of the rule are met. If this setting is enabled, it blocks further access to the source item that matched the rule. The owner, author, and site owner can still access the item. We have this setting enabled.

Access scope: Specifies a condition for the DLP rule that's based on the access scope of the content. The rule is applied to content that matches the specified access scope. We have the access scope set to not inside the organisation. The rule is applied to content that's accessible outside the organization.

Block access scope: Specifies the scope of the block access action. If this setting is set to all, the setting will block access to everyone except the owner and the last modifier.

Disabled: Specifies whether the DLP rule is disabled. If The rule is enabled.

-**GenerateAlert = SiteAdmin**: Specifies an action for the DLP rule that notifies the specified users when the conditions of the rule are met. You can specify multiple values separated by commas. The email message that's generated by this action contains a link to detailed information in the Security & Compliance Center (the details aren't in the email message itself).

-**GenerateIncidentReport = SiteAdmin**: Specifies an action for the DLP rule that sends an incident report to the specified users when the conditions of the rule are met. You can specify multiple values separated by commas.

-**IncidentReportContent = All**: Specifies the content to include in the report when you use the GenerateIncidentReport parameter. You can specify multiple values separated by commas. You can only use the value All by itself. If you use the value Default, the report includes the following content: DocumentAuthor, MatchedItem, RulesMatched,

Service, Title.

-**NotifyAllowOverride = FalsePositive,WithJustification**: Specifies the notification override options when the conditions of the rule are met. FalsePositive: Allows overrides in the case of false positives. WithoutJustification: Allows overrides without justification. WithJustification: Allows overrides with justification. You can specify multiple values separated by commas. The values WithoutJustification and WithJustification are mutually exclusive.

-**NotifyUser = Owner,SiteAdmin,LastModifier**: Secifies an action for the DLP rule that notifies the specified users when the conditions of the rule are met. Options include -LastModifier, Owner, SiteAdmin, email address. You can specify multiple values separated by commas.

These values are then configured using the new-dlpcompliancerule command.

Skype for Business Operations:

Enable Modern Authentication for Skype for Business

In Skype for Business Server, server-to-server authentication (for example, the authentication that enables Skype for Business Server and Exchange to share information) is carried out using the OAuth security protocol. OAuth is always on in Skype for Business Server; there is no need (or even any way) to enable or disable the protocol. However, if Skype for Business Server needs to communicate with other server products you might need to modify your OAuth configuration settings; for example, you might need to specify the autodiscover URL for the Office 365 version of Exchange, and you might need to specify your Realm name. These settings can only be managed by using the CsOAuthConfiguration cmdlets; options for managing OAuth settings are not available in the Skype for Business Server Control Panel.

Note that, for the on-premises version of Skype for Business Server, you can have only a single, global collection of OAuth settings: you cannot not create additional collections of OAuth settings nor can you delete the global collection. Each Skype for Business Online tenant is also limited to a single collection of OAuth configuration settings.

Skype for Business Server Control Panel: The functions carried out by the Set-CsOAuthConfiguration cmdlet are not available in the Skype for Business Server Control Panel.

The following parameters are not applicable to Skype for Business Online: AdditionalAudienceUrls, AlternateAudienceUrl, ClientAuthorizationOAuthServerIdentity, ExchangeAutodiscoverAllowedDomains,

ExchangeAutodiscoverUrl, Force, Identity, Instance, PipelineVariable, Realm, ServiceName, and Tenant

Inputs:

The Set-CsOAuthConfiguration cmdlet accepts pipelined instances of the Microsoft.Rtc.Management.WritableConfig.Settings.SSAuth.OAuthSettings object.

Outputs:

None. Instead, the Set-CsOAuthConfiguration cmdlet modifies existing instances of the Microsoft.Rtc.Management.WritableConfig.Settings.SSAuth.OAuthSettings object.

Enable Stream Transcription

The CsTeamsMeetingPolicy cmdlets enable administrators to control the type of meetings that users can create or the features that they can access while in a meeting. It also helps determine how meetings deal with anonymous or external users.

The Set-CsTeamsMeetingPolicy cmdlet allows administrators to update existing meeting policies that can be assigned to particular users to control Teams features related to meetings.

Inputs:

System.Management.Automation.PSObject

Outputs:

System.Object

Sharepoint Online:

Set Sharepoint Online Best Practices

This script Set the best practice parameters for SharePoint Online

The script sets the following parameters running the set-spotenant command:

- **ApplyAppEnforcedRestrictionsToAdHocRecipients = $false**: When the feature is enabled, all guest users are subject to conditional access policy. By default guest users who are accessing SharePoint Online files with pass code are exempt from the conditional access policy.

- **BccExternalSharingInvitations = $false**: When the feature is enabled, all external sharing invitations that are sent will blind copy the e-mail messages listed in the BccExternalSharingsInvitationList.

- **BccExternalSharingInvitationsList = $notifyusers**: Specifies a list of e-mail addresses to be BCC'd when the BCC for External Sharing feature is enabled. Multiple addresses can be specified by creating a comma separated list with no spaces.

- **CommentsOnSitePagesDisabled' = $null**: - Disables commenting on modern SharePoint pages.

- **ConditionalAccessPolicy = AllowFullAccess**: See - https://docs.microsoft.com/en-us/sharepoint/control-access-from-unmanaged-devices

- **CustomizedExternalSharingServiceUrl = $null**: Specifies a URL that will be appended to the error message that is surfaced when a user is blocked from sharing externally by policy. This URL can be used to direct users to internal portals to request help or to inform them about your organization's policies. An example value is "https://www.contoso.com/sharingpolicies".

- **DefaultSharingLinkType = $null**: Lets administrators choose what type of link appears is selected in the “Get a link” sharing dialog box in OneDrive for Business and SharePoint Online.

- **DisallowInfectedFileDownload = $true**: Prevents the Download button from being displayed on the Virus Found warning page. Accepts a value of true (enabled) to hide the Download button or false (disabled) to display the Download button.

- **DisplayStartASiteOption = $true**: Determines whether tenant users see the Start a Site menu option.

- **EnableGuestSignInAcceleration = $true**: Accelerates guest-enabled site collections as well as member-only site collections when the SignInAccelerationDomain parameter is set.

- **ExternalServicesEnabled = $true**: Enables external services for a tenant. External services are defined as services that are not in the Office 365

datacenters.

- **FileAnonymousLinkType = $null**

- **FolderAnonymousLinkType'= $null**

- **IPAddressAllowList = $null**: Configures multiple IP addresses or IP address ranges (IPv4 or IPv6).

- **IPAddressEnforcement = $false**: Allows access from network locations that are defined by an administrator.

- **LegacyAuthProtocolsEnabled = $false**: Setting this parameter to $False prevents Office clients using non-modern authentication protocols from accessing SharePoint Online resources.

- **NoAccessRedirectUrl = $null**: Specifies the URL of the redirected site for those site collections which have the locked state

- **NotificationsInOneDriveForBusinessEnabled = $true**:

- **NotificationsInSharePointEnabled = $true**:

- **NotifyOwnersWhenInvitationsAccepted = $true**: When this parameter is set to $true and when an external user accepts an invitation to a resource in a user's OneDrive for Business, the OneDrive for Business owner is notified by e-mail.

- **NotifyOwnersWhenItemsReshared = $true**: When this parameter is set to $true and another user re-shares a document from a user's OneDrive for Business, the OneDrive for Business owner is notified by e-mail.

- **ODBAccessRequests = $null**: Lets administrators set policy on access requests and requests to share in OneDrive for Business.

- **ODBMembersCanShare = $null**: Lets administrators set policy on re-sharing behavior in OneDrive for Business.

- **OfficeClientADALDisabled = $false**: When set to true this will disable the ability to use Modern Authentication that leverages ADAL across the tenant.

- **OneDriveForGuestsEnabled = $false**: Lets OneDrive for Business creation for administrator managed guest users. Administrator managed Guest users use credentials in the resource tenant to access the resources.

- **OneDriveStorageQuota = $odfbquota**: Sets a default OneDrive for Business storage quota for the tenant. It will be used for new OneDrive for Business sites created. In this case it will be set at 5TB.

- **OrphanedPersonalSitesRetentionPeriod = 3650**: Specifies the number of days after a user's Active Directory account is deleted that their OneDrive for Business content will be deleted.

- **OwnerAnonymousNotification = $true**:

- **PermissiveBrowserFileHandlingOverride = $false**: Enables the Permissive browser file handling. By default, the browser file handling is set to Strict. The Strict setting adds headers that force the browser to download certain types of files. The forced download improves security by disallowing the automatic execution of Web content. When the setting is set to Permissive, no headers are added and certain types of files can be executed in the browser instead of download.

- **PreventExternalUsersFromResharing = $true**:

- **ProvisionSharedWithEveryoneFolder = $false**: Creates a Shared with Everyone folder in every user's new OneDrive for Business document library.

- **RequireAcceptingAccountMatchInvitedAccount = $true**: Ensures that an external user can only accept an external sharing invitation with an account matching the invited email address.

- **RequireAnonymousLinksExpireInDays = $linkexpirydays**: Specifies all anonymous links that have been created (or will be created) will expire after the set number of days.

- **SharingAllowedDomainList = $null**: Specifies a list of email domains that is allowed for sharing with the external collaborators. Use the space character as the delimiter for entering multiple values. For example, “contoso.com fabrikam.com”.

- **SharingBlockedDomainList = $null**: Specifies a list of email domains that is blocked or prohibited for sharing with the external collaborators. Use space character as the delimiter for entering multiple values. For example, “contoso.com fabrikam.com”.

- **SharingCapability = "ExternalUserAndGuestSharing"**: Determines what level of sharing is available for the site.

- **SharingDomainRestrictionMode = $null**: Specifies the external sharing mode for domains.

- **ShowPeoplePickerSuggestionsForGuestUsers = $true**: To enable the option to search for existing guest users at Tenant Level, set this parameter to $true.

- **SigninAccelerationDomain = Primary tenant domain**: Specifies the home realm discovery value to be sent to Azure Active Directory (AAD) during the user sign-in process

- **SocialBarOnSitePagesDisabled = $false**: The Social Bar will appear on all modern SharePoint pages with the exception of the home page of a site. It will give users the ability to like a page, see the number of views, likes, and comments on a page, and see the people who have liked a page.

- **SpecialCharactersStateInFileFolderNames = "allowed"**: Permits the use of special characters in file and folder names in SharePoint Online and OneDrive for Business document libraries.

- **SyncAadB2BManagementPolicy = $true**: See - https://docs.microsoft.com/en-us/sharepoint/sharepoint-azureb2b-integration-preview

- **UsePersistentCookiesForExplorerView = $false**: Lets SharePoint issue a special cookie that will allow this feature to work even when "Keep Me Signed In" is not selected.

- **UserVoiceForFeedbackEnabled = $false**: When set to $true, the "Feedback" link will be shown at the bottom of all modern SharePoint Online pages. The "Feedback" link will allow the end user to fill out a feedback form inside SharePoint Online which will then create an entry in the public SharePoint UserVoice topic. When set to $false, feedback link will not be shown anymore.

Set Sharepoint and OneDrive Idle Timeout

Use idle session timeout to configure a policy on how long users are inactive in your organization before they're signed out of Sharepoint and OneDrive. This helps protect sensitive company data and adds another layer of security for end users who work on non-company or shared devices.

When a user reaches the idle timeout session you've set, they'll get a notification that they're about to be signed out. They have to select to stay signed in or they'll be automatically signed out of Sharepoint and OneDrive.

Microsoft Online:

Block User Mailbox Add ins

Sets company-level configuration settings.

The **Set-MsolCompanySettings** cmdlet is used to set company-level configuration settings. Use Get-MsolCompanyInformation to read the current values of these settings.

Intune Best Practices

Create Endpoint Security ASR Attack Surface Reduction policy

Set Endpoint Security - ASR - Attack Surface Reduction policy. Once the polices are pushed out, the JSON data is sent to the Graph endpoint to create a new Intune policy.

These polices consist of:

Block execution of potentially obfuscated scripts:

This rule detects suspicious properties within an obfuscated script and blocks them. Script obfuscation is a common technique that both malware authors and legitimate applications use to hide intellectual property or decrease script loading times

Block executable files running unless they meet prevalence age trusted list criterion: This rule blocks executable files, such as .exe, .dll, or .scr, from launching. Thus, launching untrusted or unknown executable files can be risky, as it might not be initially clear if the files are malicious.

Block all office applications from creating child processes:

This rule blocks Office apps from creating child processes. Office apps include Word, Excel, PowerPoint, OneNote, and Access.

Creating malicious child processes is a common malware strategy. However, some legitimate line-of-business applications might also generate child processes for benign purposes, such as spawning a command prompt or using PowerShell to configure registry settings.

Block office communication app from creating child processes:

This rule prevents Outlook from creating child processes, while still allowing legitimate Outlook functions. This rule protects against social engineering attacks and prevents exploiting code from abusing vulnerabilities in Outlook. It also protects against Outlook rules and forms exploits that attackers can use when a user's credentials are compromised.

Block adobe reader from creating child processes:

This rule prevents attacks by blocking Adobe Reader from creating processes.

Malware can download and launch payloads and break out of Adobe Reader through social engineering or exploits. By blocking child processes from being generated by Adobe Reader, malware attempting to use Adobe Reader as an attack vector are prevented from spreading.

Block credential stealing from windows local security authority subsystem:

This rule helps prevent credential stealing by locking down Local Security Authority Subsystem Service (LSASS).

LSASS authenticates users who sign in on a Windows computer. Microsoft Defender Credential Guard in Windows normally prevents attempts to extract credentials from LSASS. Some organizations can't enable Credential Guard on all their computers because of compatibility issues with custom smartcard drivers or other programs that load into the Local Security Authority (LSA)

Block JavaScript or VB script from launching downloaded executable content:

This rule prevents scripts from launching potentially malicious downloaded content. Malware written in JavaScript or VBScript often acts as a downloader to fetch and launch other malware from the Internet.

Block untrusted unsigned processes that run from USB:

With this rule, admins can prevent unsigned or untrusted executable files from running from USB removable drives, including SD cards. Blocked file types include executable files (such as .exe, .dll, or .scr)

Block persistence through WMI event subscription:

This rule prevents malware from abusing WMI to attain persistence on a device.

Fileless threats employ various tactics to stay hidden, to avoid being seen in the file system, and to gain periodic execution control. Some threats can abuse the WMI repository and event model to stay hidden.

Block use of copied or impersonated system tools:

This rule blocks the use of executable files that are identified as copies of Windows system tools. These files are either duplicates or impostors of the original system tools.

Some malicious programs may try to copy or impersonate Windows system tools to avoid detection or gain privileges. Allowing such executable files can lead to potential attacks. This rule prevents propagation and execution of such duplicates and impostors of the system tools on Windows machines.

Block process creations from PSExec and WMI commands:

This rule blocks processes created through PsExec and WMI from running. Both PsExec and WMI can remotely execute code. There's a risk of malware abusing functionality of PsExec and WMI for command-and-control purposes, or to spread an infection throughout an organization's network.

Block office applications from creating executable content:

This rule prevents Office apps, including Word, Excel, and PowerPoint, from creating potentially malicious executable content, by blocking malicious code from being written to disk.

Malware that abuses Office as a vector might attempt to break out of Office and save malicious components to disk. These malicious components would survive a computer reboot and persist on the system. Therefore, this rule defends against a common persistence technique. This rule also blocks execution of untrusted files that may have been saved by Office macros that are allowed to run in Office files.

Block office applications from injecting code into other processes:

This rule blocks code injection attempts from Office apps into other processes.

Attackers might attempt to use Office apps to migrate malicious code into other processes through code injection, so the code can masquerade as a clean process.

There are no known legitimate business purposes for using code injection.

This rule applies to Word, Excel, OneNote, and PowerPoint.

Block executable content from email client and webmail:

This rule blocks email opened within the Microsoft Outlook application, or Outlook.com and other popular webmail providers from propagating the following file types:

- Executable files (such as .exe, .dll, or .scr)
- Script files (such as a PowerShell .ps1, Visual Basic .vbs, or JavaScript .js file)

Create Endpoint Security ASR App and Browser Isolation policy

Set Endpoint Security - ASR - Windows 10 App and Browser Isolation policy

This policy creates an application guard for Microsoft Edge and applications in windows environments:

- **Enabled for Edge** - Application Guard opens unapproved sites in a Hyper-V virtualized browsing container.
- **Enabled for isolated Windows environments** - Application Guard is turned on for any applications enabled for App Guard within Windows.
- **Enabled for Edge AND isolated Windows environments** - Application Guard is configured for both scenarios.

Application Guard acts as a Virtual Machine, isolating Microsoft Edge browsing and applications running within the guard, protecting form external plug ins.

When set to *Enabled for Edge* or *Enabled for Edge AND isolated Windows environments*, the following settings are available, which apply to Edge:

- **Clipboard behaviours**

  Choose what copy and paste actions are allowed from the local PC and an Application Guard virtual browser:

  - **Not configured** (*default*)

    - **Block copy and paste between PC and browser**
    - **Allow copy and paste from browser to PC only**
    - **Allow copy and paste from PC to browser only**
    - **Allow copy and paste between PC and browser**
- **Block external content from non-enterprise approved sites**
    - **Not configured** (*default*)
    - **Yes** - Block content from unapproved websites from loading.
- **Collect logs for events that occur within an Application Guard browsing session**
    - **Not configured** (*default*)
    - **Yes** - Collect logs for events that occur within an Application Guard virtual browsing session.
    - **Allow user-generated browser data to be saved**
      Not configured (*default*)
    - **Yes** - Allow user data that is created during an Application Guard virtual browsing session to be saved. Examples of user data include passwords, favourites, and cookies.
- **Enable hardware graphics acceleration**
    - **Not configured** (*default*)
    - **Yes** - Within the Application Guard virtual browsing session, use a virtual graphics processing unit to load graphics-intensive websites faster.
- **Allow users to download files onto the host**
    - **Not configured** (*default*)
    - **Yes** - Allow users to download files from the virtualized browser onto the host operating system.
- **Application Guard allow camera and microphone access**
    - **Not configured** (*default*) - Applications inside Microsoft Defender Application Guard can't access the camera and microphone on the user's device.

        - **Yes** - Applications inside Microsoft Defender Application Guard can access the camera and microphone on the user's device.
        - **No** - Applications inside Microsoft Defender Application Guard can't access the camera and microphone on the user's device. This is the same behaviour as *Not configured*.
- **Application guard allow print to local printers**
    - **Not configured** (*default*)
    - **Yes** - Allow printing to local printers.
- **Application guard allow print to network printers**
    - **Not configured** (*default*)
    - **Yes** - Allow printing print to network printers.
- **Application guard allow print to PDF**
    - **Not configured** (*default*)
    - **Yes**- Allow printing print to PDF.
- **Application guard allow print to XPS**
    - **Not configured** (*default*)
    - **Yes** - Allow printing print to XPS.

Create Intune Enterprise Application Catalogue policy for Chrome on Windows

Create an Intune Windows Google Chrome for Business Application policy

Create Intune Application Settings Catalogue policy for Edge Search

Create Intune Enterprise Application Catalogue policy for Firefox

Create Endpoint Security Local Administrator Password Solution LAPS policy

Create Intune Enterprise Application Catalogue policy for Visual Studio Code

Create Intune Windows Compliance policy

Create Intune iOS Compliance policy

Create Android Enterprise Compliance policy

Create iOS Company Portal Application policy

Create Windows Company Portal Application policy

Create Windows Brave Browser Application policy

Create Windows ClickChamp Application policy

Create Windows Loop Application policy

Create Windows Microsoft to Do Application policy

Create Windows Microsoft Whiteboard Application policy

Create Windows PowerShell Application policy

Create Windows Terminal Application policy

Create Windows Endpoint Security Baseline policy

Create Defender for Endpoint Security Baseline policy

Create Edge Security Baseline policy

Create Microsoft 365 Apps Security Baseline policy

Create Endpoint Anti-virus policy

Create Endpoint BitLocker policy

Create Endpoint Windows Firewall policy

Create Endpoint EDR policy

Create Endpoint Account Protection policy

Create Endpoint Device Control policy

Create iOS Microsoft Teams Application policy

Create iOS OneDrive for Business Application policy

Create iOS Outlook Application policy

Create iOS To do Application policy

Create iOS Microsoft Authenticator Application policy

Create iOS Microsoft Word Application policy

Create iOS Microsoft Excel Application policy

Create iOS Microsoft 365 Office Application policy

Create iOS Microsoft OneNote Application policy

Create Android Microsoft Authenticator Application policy

Create iOS Microsoft Defender Application policy

Create iOS Adobe Acrobat Reader for PDF Application policy

Create iOS Microsoft PowerPoint Application policy

Create iOS Microsoft Edge Application policy

Create iOS SharePoint Application policy

Create iOS Microsoft Copilot Application policy

Create iOS TeamViewer QuickSupport Application policy

Create Windows 1Password Application policy

Create Windows Acrobat Express Application policy

Create Windows Bitwarden Application policy

Create Windows Lastpass Application policy

Create Windows Mozilla Firefox Application policy

Create Windows Keepass Classic Intune Enterprise Application Catalogue policy

Create Windows Microsoft Visual C++ 2008 Redistributable (x64) Intune Enterprise Application Catalog policy

Create Windows Microsoft Visual C++ 2015-2022 Redistributable (x64) Intune Enterprise Application Catalog policy

Create Windows Snagit 2024 Intune Enterprise Application Catalog policy

Windows Zoom Client for Meetings Intune Enterprise Application Catalog policy