Organization & Resources

Microsoft 365 Messaging

KNOWLEDGE CHEATSHEET

RECIPIENT AND CLIENT MANAGEMENT

- **Recipients** — Mailbox types
- **Directory** — GAL and ABP
- **Access** — Delegates and clients
- **Resources** — Booking and folders

01 Manage organizational settings and resources

Recipient types and mailbox lifecycle

- A **user mailbox** stores mail for a licensed user. A **mail user** has a sign-in account and an external delivery address; a **mail contact** represents an external recipient without a sign-in account.
- A **shared mailbox** keeps a team's common email and calendar. Grant delegates access and block direct sign-in to its associated account. Converting a mailbox preserves its contents; deleting its account can delete the mailbox.
- For a departing employee, **convert to shared**, grant the required delegates, and check licensing requirements before reclaiming the license. Extra capacity, archive and preservation features can require licensing.
- **Soft-deleted** mailboxes are recoverable within the applicable recovery window. An **inactive mailbox** preserves a deleted user's content under a qualifying retention policy or hold; it serves compliance rather than ordinary delegated access.

SMTP addresses and bulk changes

- An **accepted and verified domain** plus a recipient's **proxy address** enables delivery to an additional address. Keep the old proxy address when changing the primary address to preserve incoming mail.
- **Primary SMTP address** controls the default sending identity. An alias adds a receiving address; changing the tenant's default domain does not rewrite existing recipients' addresses.
- On-premises **email address policies** combine a recipient filter, address templates and priority. **%g** means given name, **%s** surname, and a numeric prefix limits characters, such as **%1s%g** for surname initial plus given name.
- **EmailAddressPolicyEnabled** controls whether an on-premises recipient follows address policies. For cloud-only user mailboxes, manage addresses directly; for synchronized recipients, change authoritative on-premises attributes and synchronize.
- Use **Import-Csv** with recipient cmdlets for repeatable bulk operations. For multivalued properties, use **@{Add=...;Remove=...}** where supported to preserve unrelated entries.

Organization & Resources

Microsoft 365 Messaging

KNOWLEDGE CHEATSHEET

RECIPIENT AND CLIENT MANAGEMENT

- **Recipients** — Mailbox types
- **Directory** — GAL and ABP
- **Access** — Delegates and clients
- **Resources** — Booking and folders

Address lists, GALs and segmentation

- A **global address list (GAL)** is the organization's broad recipient directory. An **address list** selects recipients by attributes using an **OPATH RecipientFilter**, such as title, department, city or custom attributes.
- Combine filters deliberately: **-and** requires both conditions, **-or** accepts alternatives, and parentheses control grouping. Include **RecipientTypeDetails** when only a specific mailbox type should qualify.
- An **address book policy (ABP)** bundles one GAL, one offline address book, a room list and address lists. Assign the ABP to mailboxes with **Set-Mailbox -AddressBookPolicy** to give each population its intended directory view.
- **ABP routing** makes recipients in different GALs appear external to each other in supported mail scenarios. Address book segmentation controls discovery and presentation; use dedicated controls for communication restrictions.
- **HiddenFromAddressListsEnabled** hides a recipient from address lists without preventing delivery to a known address. Add an address list to an ABP without replacing its existing lists unintentionally.

Offline and hierarchical address books

- An **offline address book (OAB)** supplies cached directory data to Outlook. If Outlook on the web sees a new recipient before cached Outlook does, investigate OAB generation, download and client refresh.
- An OAB can contain selected address lists while the **online GAL** remains broader. Select the OAB through the appropriate mailbox or address book policy configuration.
- A **hierarchical address book (HAB)** presents an organizational tree. Set the root with **Set-OrganizationConfig -HierarchicalAddressBookRoot** and mark hierarchy distribution groups with **IsHierarchicalGroup**; group membership builds the hierarchy.

Groups and mailbox delegation

- A **distribution group** distributes mail; a **mail-enabled security group** also supports permission assignments. A **Microsoft 365 group** adds a shared conversation space and collaboration services.
- A **dynamic distribution group** uses recipient attributes to determine its audience. Maintain the underlying attributes and allow for membership refresh; it does not use a manually maintained member list.
- Group **delivery restrictions**, required sender authentication, allowed senders and moderation control who can send. Check these settings when an internal group returns **5.7.1 Delivery not authorized**.

Organization & Resources

Microsoft 365 Messaging

KNOWLEDGE CHEATSHEET

RECIPIENT AND CLIENT MANAGEMENT

- **Recipients** — Mailbox types
- **Directory** — GAL and ABP
- **Access** — Delegates and clients
- **Resources** — Booking and folders

- **Full Access** allows opening and managing mailbox content. **Send As** makes mail appear from the mailbox; **Send on Behalf** visibly identifies the delegate. Sending permissions are separate from Full Access.
- Use **Add-MailboxPermission** for Full Access, **Add-RecipientPermission** for Send As in Exchange Online, and **Set-Mailbox -GrantSendOnBehalfTo** for Send on Behalf. Use folder permissions for calendar or other folder-specific access.
- A group's **display name**, primary address and aliases are separate properties. Renaming a team does not automatically create a new SMTP alias. Distribution-group upgrades require eligibility checks; not every group type supports conversion.

Resource mailboxes and booking

- **Room mailboxes** represent meeting spaces; **equipment mailboxes** represent bookable devices such as projectors or smartboards. Their calendar receives booking requests without requiring an ordinary user sign-in.
- **Get-CalendarProcessing** inspects booking behavior; **Set-CalendarProcessing** configures it. **AutomateProcessing AutoAccept** activates automatic resource processing subject to booking policy.
- **BookInPolicy** identifies users allowed automatic booking. **RequestInPolicy** permits approval requests; **ResourceDelegates** identifies approvers. Configure the corresponding **AllBookInPolicy** and **AllRequestInPolicy** switches deliberately.
- Set **MaximumDurationInMinutes**, booking horizon, conflict and recurring-meeting limits to match policy. **AddAdditionalResponse** and **AdditionalResponse** add custom text to booking responses.

Public folders and permissions

- Create a **public folder mailbox**, then the **public folder**, then assign client permissions. The first public folder mailbox holds the writable hierarchy; additional mailboxes hold hierarchy copies and folder content.
- **Mail-enable** a public folder to receive SMTP posts. **Disable-MailPublicFolder** removes mail reception while preserving the folder and normal Outlook access. A mail-enabled folder can participate in a distribution group.
- **Default** permissions apply to authenticated users without a specific entry; **Anonymous** applies to unauthenticated senders. External posting can require Anonymous **CreateItems** without permission to read folder contents.

Organization & Resources

Microsoft 365 Messaging

KNOWLEDGE CHEATSHEET

RECIPIENT AND CLIENT MANAGEMENT

- **Recipients** — Mailbox types
- **Directory** — GAL and ABP
- **Access** — Delegates and clients
- **Resources** — Booking and folders

- **Author** reads and creates items and edits or deletes owned items. **Publishing Author** adds subfolder creation. **Editor** can edit and delete all items; **Publishing Editor** adds subfolder creation. **Owner** also manages folder permissions.
- **Get-PublicFolder** retrieves folder attributes; **Get-MailPublicFolder** retrieves mail settings. **Get-PublicFolderStatistics** reports folder usage; **Get-PublicFolderItemStatistics** reports individual item details, including dates and attachment information.

Outlook on the web policies

- **OwaMailboxPolicy** controls Outlook on the web features, including attachment handling, calendar sharing, mobile-device options and deleted-item recovery. Create a separate policy and assign it to the affected mailboxes for departmental requirements.
- **Direct file access**, file-type allow/block lists and cloud attachment settings govern different attachment behaviors. When adding a blocked extension, preserve existing entries and remove conflicting allow entries as needed.
- **Conditional Access** can apply session restrictions to unmanaged devices; the OWA policy determines supported restricted behavior such as **ReadOnly**. Validate the policy assignment, device state and browser support together.

Mobile devices and access

- **Exchange ActiveSync access rules** allow, block or quarantine device classes. **Mobile device mailbox policies** set supported password, security and synchronization requirements. **Set-CASMailbox -ActiveSyncEnabled** enables or disables the protocol per mailbox.
- **Get-MobileDevice** returns device identity and access state, including the applied access rule. **Get-MobileDeviceStatistics** adds synchronization and usage information; device/operator reports depend on information supplied by the client.
- Enable **ActiveSync debug logging** with **Set-CASMailbox** and retrieve available mailbox logs through **Get-MobileDeviceStatistics**. Check last successful sync and policy compliance before changing organization-wide access.
- **Remote wipe** behavior depends on the client: native ActiveSync can support a full device wipe, while Outlook mobile removes Outlook data. Distinguish a whole-device wipe, an account-only wipe and an Intune selective wipe.
- **Conditional Access** and **Intune app protection** govern supported apps, identities and device conditions. Requiring Outlook alone needs an app-aware design and appropriate licensing; a device password policy does not by itself restrict clients to Outlook.

Organization & Resources / Mail Transport

Microsoft 365 Messaging

KNOWLEDGE CHEATSHEET

RECIPIENT AND CLIENT MANAGEMENT

- **Recipients** — Mailbox types
- **Directory** — GAL and ABP
- **Access** — Delegates and clients
- **Resources** — Booking and folders

Client connectivity and authentication

- **Autodiscover** locates mailbox settings. Check the user's address and identity, public DNS, internal DNS and the on-premises **service connection point (SCP)**. A stale SCP can affect domain-joined Outlook after migration.
- **Modern Authentication** uses OAuth tokens and supports Conditional Access and MFA. **Basic authentication** sends reusable credentials; use authentication controls appropriate to the environment to block legacy sign-in.
- If web access works but desktop Outlook fails, check the license's client-access entitlement, Outlook profile, add-ins, authentication and network path. TLS inspection can introduce certificate trust or protocol failures.
- Use the **Remote Connectivity Analyzer** for protocol and external connectivity tests. Local Outlook diagnostics, safe mode and profile repair address client crashes; a message trace addresses server-side delivery rather than application startup.

02 Plan and manage mail transport

DNS and domain purpose

- **MX** selects the inbound mail destination. Point it at the hygiene service that must receive mail first. **Autodiscover CNAME** supports client configuration; it serves a different purpose from MX.
- An **authoritative accepted domain** expects every recipient to be known locally. An **internal relay domain** supports recipients split across systems and needs a route to the other system. Synchronize valid recipients to support recipient validation.
- A **remote domain** controls outbound behavior for a destination, including out-of-office replies, automatic replies, forwarding, delivery reports and message formatting. A domain-specific setting takes precedence over the default remote domain.
- **TNEFEnabled $false** on a remote domain prevents Transport Neutral Encapsulation Format for that destination and helps avoid **winmail.dat**. Remote domains do not select the primary sending address or establish transport routes.

Mail Transport

Microsoft 365 Messaging

KNOWLEDGE CHEATSHEET

MESSAGE DELIVERY PATH

DNS Destination → **Connectors** Route and trust → **Rules** Policy actions → **Trace** Delivery outcome

Connectors and conditional routing

- Exchange Online **inbound connectors** define trusted or restricted incoming paths; **outbound connectors** route messages to partners, on-premises systems or smart hosts. Direction is relative to Microsoft 365.
- Match a connector using the intended sender domains, source public IP addresses or certificate identity. Requiring **TLS** and validating the expected certificate or IP restricts who can use the path.
- An outbound connector can apply to specified recipient domains or be selected by a **mail flow rule**. For content-, sender- or department-specific routing, create the connector and the rule that directs matching messages to it.
- With a third-party gateway, set inbound restrictions to prevent direct bypass, route outbound mail through the gateway, and use **Enhanced Filtering for Connectors** to recover the original source for filtering. **EFSkipIPs** identifies intermediary IPs to skip.

Application and device SMTP

- **SMTP AUTH client submission** authenticates to a mailbox and requires supported authentication and TLS. It is distinct from a connector that identifies a sending server by certificate or public IP.
- **Direct send** delivers to recipients in the tenant through its MX endpoint. It does not provide general relay to external recipients.
- **Microsoft 365 SMTP relay** uses an inbound connector and the tenant MX endpoint on port **25**. Identify the device or relay using an approved certificate or static public IP; shared NAT identity can authorize more devices than intended.
- After retiring an on-premises relay, update printers and applications, firewall rules and sender-domain authorization. Test both internal and external delivery using the chosen method.

Mail flow rules and message limits

- A **mail flow rule** combines conditions, exceptions and actions. Use it for disclaimers, attachment restrictions, moderation, custom rejection text, encryption or connector selection. Rule priority and **stop processing** affect later rules.
- **Enforce** performs rule actions. **Test without Policy Tips** supports evaluation without delivery-changing enforcement; inspect trace and reporting results before enabling moderation or rejection.
- Attachment conditions can inspect extensions, filenames, size or supported content. Blocking one extension differs from blocking every attachment. Account for unsupported, encrypted or uninspectable attachments in the rule design.

Mail Transport

Microsoft 365 Messaging

KNOWLEDGE CHEATSHEET

MESSAGE DELIVERY PATH

DNS Destination → **Connectors** Route and trust → **Rules** Policy actions → **Trace** Delivery outcome

- A **disclaimer** needs a fallback action when the service cannot modify a message: wrap, reject or ignore. An exception matching existing disclaimer text can prevent repeated insertion.
- Message delivery is constrained by the applicable **organization, connector, mailbox and client limits**. Increasing a mailbox's send/receive size does not override a lower client limit or recipient restriction; encoding increases wire size.

TLS, certificates and message encryption

- **TLS** encrypts a transport connection between mail systems. To require it for both directions with a partner, configure the appropriate inbound and outbound paths. Opportunistic TLS alone does not guarantee mandatory encryption.
- Hybrid SMTP requires a **publicly trusted certificate**, a private key, valid dates and names matching the configured identity. Request or renew, import the issued certificate, then enable it for the required services.
- After certificate replacement, verify **SMTP binding** and connector **TlsCertificateName** values. Rerun the Hybrid Configuration wizard or update the relevant Send and Receive connector certificate identities when required.
- **S/MIME** uses users' certificates for digital signing and encryption. **Microsoft Purview Message Encryption** and rights protection protect message content beyond a transport hop; mail flow rules or sensitivity labels can apply protection automatically.

Trace, headers and delivery troubleshooting

- **Message trace** follows messages accepted by Exchange Online, including recipient outcomes, transport-rule events and failures. A message still in the sender's Outbox has not entered the service and will not appear in trace.
- Filter by **sender, recipient, time and delivery status**. Summary, enhanced summary and extended reports expose different detail; export the report suited to the required fields and time range.
- **4xx SMTP replies** indicate temporary failures that normally queue for retry; **5xx** replies indicate permanent rejection. Read the NDR's enhanced status, diagnostic text, failing server and recipient before changing configuration.
- **5.1.10 RecipientNotFound** points toward recipient address or directory resolution. **5.7.1** commonly indicates authorization or policy rejection. **5.1.8 bad outbound sender** can indicate a restricted sender; investigate compromise before unblocking.
- Inspect **Received headers** for hop delays and **Authentication-Results** for authentication verdicts. On-premises **message tracking logs** record transport events, **protocol logs** record SMTP dialogue, and **queues** show pending delivery.
- Use **Inbound SMTP** connectivity tests for DNS/MX reachability and SMTP acceptance. Review trace and quarantine for a missing individual message; use mail-flow reports and alert policies for delayed-message thresholds and operational notifications.

Hybrid & Migration

Microsoft 365 Messaging

KNOWLEDGE CHEATSHEET

HYBRID MIGRATION SEQUENCE

Prepare Identity and endpoints → **Configure** Hybrid coexistence → **Synchronize** Mailbox data → **Complete** Switch and validate

03 Manage hybrid configuration and migration

Hybrid foundations and topology

- The **Hybrid Configuration wizard (HCW)** establishes coexistence settings such as secure mail flow and cross-premises availability. **Directory synchronization** supplies a common recipient view; HCW does not replace identity synchronization.
- **Full hybrid** suits sustained coexistence; **minimal hybrid** targets migration with fewer coexistence features. **Classic** publishes required endpoints; **Modern Hybrid** uses the Hybrid Agent for supported web-service traffic.
- The **Hybrid Agent** supports mailbox moves and free/busy requests through outbound connectivity. **SMTP does not traverse the agent** and still needs its own route, certificate and port **25** connectivity.
- **Hybrid Modern Authentication** and on-premises integrations needing published client endpoints require the appropriate **Classic hybrid** design. Modern Hybrid topology and Modern Authentication describe different capabilities.
- Plan namespace resolution, trusted certificates and HTTPS **443** reachability for web services. For an **Edge Transport** path, establish the Edge Subscription and select the intended transport servers in hybrid configuration.

Sharing, synchronization and remote recipients

- An **organization relationship** exposes free/busy information to another organization. Choose **AvailabilityOnly** to hide subject and location, or **LimitedDetails** to share them; scope sharing to a supported mail-enabled security group when required.
- Sharing is **directional**: each organization controls what it exposes. For bidirectional availability, configure both sides. A **sharing policy** instead governs user-initiated calendar sharing with external recipients.
- In hybrid deployments, maintain an on-premises **remote mailbox** object for a cloud mailbox. **New-RemoteMailbox** creates the account and remote recipient; **Enable-RemoteMailbox** enables an existing account. Use the shared switch for a shared remote mailbox where appropriate.
- **RemoteRoutingAddress** points to the tenant's routing domain; the **primary SMTP address** is the user's normal address. Missing or unsynchronized recipient objects can cause GAL omissions and cross-premises delivery failures.
- **Organization Configuration Transfer** copies supported Exchange configuration during HCW. Review what transfers and validate the target; it is distinct from directory synchronization and continuous configuration replication.

Hybrid & Migration

Microsoft 365 Messaging

KNOWLEDGE CHEATSHEET

HYBRID MIGRATION SEQUENCE

Prepare Identity and endpoints → **Configure** Hybrid coexistence → **Synchronize** Mailbox data → **Complete** Switch and validate

Hybrid Modern Authentication

- **HMA** uses the cloud identity service to authenticate supported clients accessing on-premises mailboxes. Confirm supported Exchange builds, identity synchronization, OAuth trust and published service URLs.
- Validate **OAuth** on the relevant Autodiscover, EWS, MAPI and OAB virtual directories, and register the required on-premises HTTPS namespaces with the appropriate cloud service principal.
- The **authorization server**, organization OAuth settings and client configuration must align. Check sign-in logs and client authentication status; enabling MFA alone does not repair an incomplete OAuth configuration.
- For Hybrid Agent proxy access, configure the agent's supported **outbound proxy** settings and the Exchange server's own proxy settings separately. Successful agent installation does not prove every hybrid traffic path works.

Mailbox moves and migration operations

- A **migration endpoint** stores connection settings and credentials. **MRSProxy** on the EWS virtual directory supports remote mailbox moves. Update endpoint credentials after a privileged-account password change.
- A **migration batch** groups users, commonly from a CSV. Separate initial data synchronization from **completion**, when the mailbox switches over; pre-stage data to reduce user disruption.
- **StartAfter** schedules a batch's start; **CompleteAfter** schedules eligible completion. Manual completion permits a coordinated cutover after synchronization and readiness checks.
- **Get-MigrationBatch**, migration-user statistics, **Get-MoveRequest** and move statistics expose progress and errors. Resume a suspended request only after fixing its cause and confirming its completion settings.
- Plan **delegate relationships** during moves. Cross-premises Full Access, Send As and Send on Behalf have different prerequisites and limitations; migrate tightly coupled mailboxes together when possible.

IMAP, cutover, PST and cross-tenant migration

- **IMAP migration** transfers mail folders and messages, not calendars, contacts or tasks. Provision and license target mailboxes, create the IMAP endpoint and CSV, synchronize the batch, then change mail routing at cutover.
- **Cutover migration** moves an Exchange organization's mailboxes together. The source migration account needs sufficient mailbox access, such as scoped **Full Access** or database **Receive As**; target permissions differ from source access.
- For **PST network upload**, obtain the upload location and SAS token, upload with **AzCopy**, create a CSV mapping files to target mailboxes or archives, validate the import job, then start and monitor the import.

Hybrid & Migration / Security & Compliance

Microsoft 365 Messaging

KNOWLEDGE CHEATSHEET

HYBRID MIGRATION SEQUENCE

Prepare Identity and endpoints → **Configure** Hybrid coexistence → **Synchronize** Mailbox data → **Complete** Switch and validate

- **Mailbox Import Export** is a specific Exchange management role. Grant the additional permissions needed to create import jobs instead of assuming ordinary mailbox delegation provides import administration.
- **Cross-tenant mailbox migration** needs tenant-to-tenant authorization, an application/service principal configuration, organization relationships, a target endpoint and correctly prepared target mail users. Match mailbox identifiers and addresses and assess licensing before creating the batch.

Public folders and cloud archives in hybrid

- Public-folder batch migration requires source inventory, checks, a folder-to-mailbox mapping and target preparation. Synchronize, lock the source for finalization, complete the batch and validate access before removing source data.
- For **hybrid public-folder access**, configure the remote folder location and synchronize mail-enabled folder representations in the correct direction. Cloud-to-on-premises access uses the public-folder mailbox import and cloud-to-on-premises synchronization scripts.
- A **Microsoft 365 group** can replace suitable public-folder collaboration, but its flat model does not preserve every hierarchy or folder type. Inventory functionality and content before choosing migration or export/import.
- A **cloud archive** can accompany an on-premises primary mailbox in a supported hybrid design. Enable it through the authoritative on-premises recipient configuration; enabling a local archive is a different operation.

04 Secure and govern messaging

RBAC roles, entries and scopes

- Exchange **RBAC** separates **role** capabilities, **role assignments**, **management scopes** and **role groups**. A **role entry** exposes a cmdlet and its permitted parameters; a scope limits the recipients or configuration it can modify.
- **Recipient Management** administers recipients; **View-Only Organization Management** supports read-only Exchange configuration access. Use dedicated management roles when a built-in role group grants more than the task requires.
- Build a **custom child role** to remove unnecessary cmdlets or parameters with **Remove-ManagementRoleEntry** or role-entry settings. Removing one assignment does not remove the same effective permission granted through another group.
- Use **Get-ManagementRoleEntry** to inspect cmdlets, **Get-ManagementRoleAssignment** to find who receives a role, and **Get-RoleGroupMember** to inspect membership. Match cmdlet permissions to the effective role and scope.
- Delegate departmental administration with an appropriate **recipient write scope**, such as a filter, OU or supported administrative-unit scope. Membership in an administrative unit alone grants no management permission.

Security & Compliance

Microsoft 365 Messaging

KNOWLEDGE CHEATSHEET

MESSAGING PROTECTION LAYERS

- **RBAC** — Authorized actions
- **Protection** — Threat filtering
- **Retention** — Preserve and expire
- **Audit** — Investigate changes

Self-service and administrative access

- A **role assignment policy** controls users' self-service mailbox tasks. Assign a custom policy to affected mailboxes when restricting personal details, distribution-group creation or mailbox options.
- Roles such as **MyContactInformation**, **MyDistributionGroups** and **MyBaseOptions** govern different self-service features. Changing a tenant-wide default can affect more users than intended.
- Microsoft 365 **directory roles**, Exchange role groups and Purview roles authorize different services. A mailbox license, Full Access delegation or a sign-in location does not itself grant administrative role permissions.
- Connect using the **ExchangeOnlineManagement** module and **Connect-ExchangeOnline** with supported authentication. Protect administrative sign-in with Conditional Access and least-privilege roles; do not use broad roles merely to enable PowerShell.

Authentication and protection layers

- **SPF** publishes authorized sending infrastructure in a DNS TXT record and checks the envelope sender domain. Include every legitimate outbound source; receiving mail successfully does not prove outbound authentication is configured.
- **DKIM** signs selected headers and message content using a domain key. Publish the provider-specified **selector1** and **selector2 CNAME** targets for custom-domain signing and rotation; use the exact values supplied for the tenant.
- **DMARC** checks alignment of the visible From domain with a passing SPF or DKIM identity and publishes a handling/reporting policy. A DKIM pass alone does not guarantee DMARC alignment or safe content.
- **DNSSEC** authenticates DNS data. **DANE for SMTP** uses DNSSEC-protected **TLSA** records to bind TLS expectations to mail servers, addressing a different threat from sender-domain authentication.
- **EOP** provides connection, anti-spam and anti-malware filtering. **Defender for Office 365** adds capabilities such as Safe Links and Safe Attachments according to licensing. Protection applies only to traffic that actually traverses the service.

Anti-spam, anti-malware and impersonation

- **Connection filtering** evaluates source IP reputation and IP allow/block entries. An allow entry for a shared service IP can affect unrelated senders; investigate false positives before creating broad bypasses.
- **Inbound anti-spam** policies control verdict actions and bulk handling. **Outbound anti-spam** policies control outbound abuse, restricted senders and automatic forwarding. Other remote-domain and rule restrictions can still block forwarding.
- **SCL** expresses spam confidence; **BCL** expresses bulk-mail complaint likelihood. Read **SFV**, **IPV** and authentication headers alongside the policy outcome instead of treating one score as proof of intent.

Security & Compliance

Microsoft 365 Messaging

KNOWLEDGE CHEATSHEET

MESSAGING PROTECTION LAYERS

- **RBAC** — Authorized actions
- **Protection** — Threat filtering
- **Retention** — Preserve and expire
- **Audit** — Investigate changes

- **Anti-malware** policies scan malicious content and can block selected common attachment types. **Safe Attachments** adds detonation analysis; an attachment extension policy is separate from a malicious-content verdict.
- **Anti-phishing** policies address spoofing and supported user/domain impersonation. Distinguish the recipients protected by the policy from the people or domains whose identities are protected against impersonation.
- Use narrow **trusted sender** exceptions for verified legitimate applications or personal addresses when appropriate. A recipient exclusion removes that recipient from policy protection; it does not authorize a sender globally.

Safe Links, Safe Attachments and policy priority

- **Safe Links** evaluates URLs, including checks when links are clicked. Configure click-through and tracking behavior for the protected recipients; URL click reports identify who followed a suspicious link.
- **Safe Attachments Dynamic Delivery** delivers the message body with attachment placeholders while scanning continues, then releases safe attachments. Malicious content is quarantined; Dynamic Delivery depends on supported Exchange Online mailbox behavior.
- A policy's **recipient conditions** determine whom it protects. Sender-based exceptions or special transport processing are different controls; avoid confusing an external sender domain with a recipient-domain condition.
- **Strict** and **Standard preset security policies** can take precedence over custom policies. Raising a custom policy's priority does not override a higher-precedence preset that already covers the recipient.

Quarantine, submissions and security operations

- **Quarantine** isolates messages according to protection verdicts. The **quarantine policy** determines user permissions and notification availability; global quarantine settings control shared notification presentation and cadence.
- Trace identifies delivery outcomes; quarantine tools let authorized users inspect, release or request release. Available actions and retention depend on the verdict and policy; quarantine retention is separate from mailbox retention.
- **Zero-hour auto purge (ZAP)** acts on supported messages after delivery when threat verdicts change. Investigate it when a previously visible message disappears or moves to quarantine.
- Configure **user-reported message settings**, submission destinations and alert notifications for suspicious-mail workflows. Use **advanced delivery** settings for designated SecOps mailboxes or approved simulations, with narrowly scoped exceptions.
- **Configuration analyzer** compares protection settings with Standard or Strict baselines and tracks supported changes. **Attack simulation training** tests user response: Credential Harvest imitates a sign-in lure; other techniques use malicious links or attachments.

Security & Compliance

Microsoft 365 Messaging

KNOWLEDGE CHEATSHEET

MESSAGING PROTECTION LAYERS

- **RBAC** — Authorized actions
- **Protection** — Threat filtering
- **Retention** — Preserve and expire
- **Audit** — Investigate changes

MRM tags and archive processing

- Exchange **Messaging Records Management (MRM)** uses retention tags linked to a mailbox retention policy. The **Managed Folder Assistant** processes eligible items asynchronously; archive actions require an enabled archive mailbox.
- A **default policy tag (DPT)** applies to untagged items. A **retention policy tag (RPT)** applies to a particular default folder. **Personal tags** let users tag supported folders or items and override inherited MRM behavior.
- Use **separate archive and deletion tags** for separate actions: for example, one archive DPT after two years and one deletion DPT after seven years. A policy can contain one RPT per default-folder type, so different folders can share one policy.
- **Move to archive** is supported by DPTs and personal tags. **Delete and allow recovery** moves content into recoverable storage; **Permanently delete** does not defeat a preservation hold.
- **Retention-disabled personal tags** can provide Never Delete or Never Move behavior for MRM. Removing a tag from a policy does not automatically strip that tag from already tagged items.
- **RetentionHoldEnabled** temporarily suspends MRM aging actions, useful for an absence. It does not provide legal preservation. **ElcProcessingDisabled** controls Managed Folder Assistant processing more broadly.

Preservation, archives and inactive mailboxes

- **Purview retention policies** can retain, delete, or retain then delete across supported workloads. **Retention labels** apply item-level settings and are published to selected users or locations; **sensitivity labels** classify and protect information.
- A **static scope** selects locations explicitly. An **adaptive scope** selects eligible users or resources by attributes, such as job title, so scope membership can change automatically.
- **Litigation Hold** preserves mailbox content, including deleted and modified items in recoverable storage. A duration is based on item age rather than a countdown from when the administrator enabled the hold.
- Enable an **archive mailbox** to provide separate mailbox storage. **Auto-expanding archiving** supplies additional archive capacity for eligible mailboxes; primary mailbox quotas and archive capacity are distinct limits.
- **Recovering an inactive mailbox** makes it active as a primary mailbox for a returning user. **Restoring** copies its contents into another active mailbox while retaining the inactive source for compliance.

Security & Compliance

Microsoft 365 Messaging

KNOWLEDGE CHEATSHEET

MESSAGING PROTECTION LAYERS

- **RBAC** — Authorized actions
- **Protection** — Threat filtering
- **Retention** — Preserve and expire
- **Audit** — Investigate changes

DLP, eDiscovery, auditing and journaling

- **Data loss prevention (DLP)** detects sensitive information, labels or other conditions and applies actions such as blocking, notification, approval or permitted override. A **policy tip** informs the user; it is separate from the enforcement action.
- An **eDiscovery case** organizes searches, case membership and holds. Use a query-based hold to preserve matching content, with both query and locations scoped deliberately. Searching content alone does not preserve it.
- **eDiscovery Managers** manage cases they create or can access as members. **eDiscovery Administrators** have broader access across cases. **Search And Purge** is a distinct permission from search and case management.
- **Administrator audit logs** record supported configuration-changing operations; **mailbox audit logs** record supported owner, delegate and administrator mailbox activities. Use the relevant actor, operation and time filters to investigate access or policy changes.
- **Audit retention policies** govern audit records independently of email retention tags. Required licensing and policy scope apply to the users generating events; retaining a mailbox does not automatically extend audit-log retention.
- **Journaling** sends reports containing copies of matching communications to a separate archive destination. Use the system through which the messages pass; Exchange Online mailboxes cannot serve as Exchange Online journal-report destinations.