Identity & Enrollment

Endpoint Administrator

KNOWLEDGE CHEATSHEET

ESTABLISH MANAGEMENT

Identity Join or register → **Enrollment** Establish MDM → **Targeting** Groups and filters → **Access** Evaluate conditions

01 Prepare infrastructure for devices (20– 25%

Device identity and join states

- **Microsoft Entra registered** associates a work identity with a device while preserving its existing sign-in account. It suits personal devices and cloud SSO; registration alone does not enroll a device in Intune.
- **Microsoft Entra joined** Windows devices use an organizational identity for sign-in. **Hybrid joined** devices remain AD DS domain members and also have a cloud device identity. Synchronizing user accounts alone does not complete hybrid device join.
- Use **Access work or school** in Windows Settings for work-account connections and supported join workflows. Microsoft Authenticator or Company Portal can register supported mobile devices; Entra Connect Sync is not a mobile enrollment client.
- **dsregcmd /status** exposes join state, tenant information and the signed-in user's **AzureAdPrt** status. Run it in the relevant user's context when diagnosing primary refresh token and SSO issues.
- Cloud-joined devices can access on-premises resources with suitable synchronized identities, authentication configuration and network connectivity. Joining a device to Entra does not itself create a route to a file server.

Groups, roles and local access

- Entra **Device settings** control which users may join devices and the directory device limit. The **MDM user scope** controls automatic Intune enrollment. These are separate permissions and limits.
- **Dynamic membership** evaluates device attributes. Use **-contains** for a substring and **-in** for membership in a list; do not add wildcard asterisks to a substring value. Device trust types include **AzureAD**, **ServerAD** and **Workplace**.
- An Intune **role** defines permitted actions, **scope groups** define managed users or devices, and **scope tags** limit administrative visibility. Scope tags do not assign policies to endpoints.
- Use **Intune Role Administrator** for role assignments, **Policy and Profile Manager** for configuration management and **Application Manager** for app management. A narrowly defined custom role can reduce permissions further.
- Directory roles and Intune RBAC serve different control planes. **User Administrator** manages users and groups; **Password Administrator** handles permitted password resets; **Conditional Access Administrator** manages access policies.
- Joining users can receive local administrator rights depending on provisioning settings. Use an Autopilot **standard user** account type or controlled provisioning, then manage local groups with **Account protection**. The **Entra Joined Device Local Administrator** role grants broad local administration on Entra-joined devices.

Identity & Enrollment

Endpoint Administrator

KNOWLEDGE CHEATSHEET

ESTABLISH MANAGEMENT

Identity Join or register → **Enrollment** Establish MDM → **Targeting** Groups and filters → **Access** Evaluate conditions

Windows enrollment and ownership

- Automatic MDM enrollment needs eligible Intune and Entra licensing, enrollment permission and an **MDM user scope** containing the user. Assign a selected group when only a department should enroll automatically.
- For existing hybrid devices, use the supported **automatic MDM enrollment Group Policy** or Configuration Manager co-management workflow. Diagnose hybrid join prerequisites, synchronization, domain-controller reachability and cloud endpoint access before retrying enrollment.
- **Co-management** lets Configuration Manager and Intune manage supported Windows devices together. Move individual **workloads** deliberately and use a **pilot collection** to test Intune authority before broad rollout; enrolling the device does not transfer every workload.
- **Enrollment restrictions** govern allowed platforms, supported OS ranges and personal-device enrollment. **Device limit restrictions** constrain user enrollment; priority determines the applicable restriction when several target the same user.
- A **device enrollment manager (DEM)** supports bulk enrollment of up to 1,000 supported devices. DEM has platform and user-affinity limitations; it is not a substitute for Autopilot or automated corporate enrollment.
- **Corporate identifiers** help recognize supported corporate devices. Combine recognized ownership with restrictions that block personal enrollment when building an allowlist. Device categories can drive dynamic grouping from a user's enrollment selection.
- For manual enrollment discovery, create **EnterpriseEnrollment** CNAMEs for the applicable UPN suffixes pointing to **enterpriseenrollment-s.manage.microsoft.com**. **EnterpriseRegistration** points to **enterpriseregistration.windows.net** for device registration discovery.

Android and Apple enrollment

- Connect **Managed Google Play** before deploying Android Enterprise apps. A **personally owned work profile** separates work data on BYOD; **corporate-owned work profile** allows corporate management with a personal area.
- **Fully managed** Android suits corporate single-user devices. **Dedicated** enrollment suits task devices and kiosks, including shared or userless scenarios. Choose the ownership and enrollment mode before building restrictions.
- Android corporate enrollment can use an enrollment token or **QR code** during setup. **Zero-touch** requires eligible reseller-registered hardware and a configuration in Google's zero-touch portal associated with the Intune enrollment profile.

Identity & Enrollment / Deployment & Maintenance

Endpoint Administrator

KNOWLEDGE CHEATSHEET

ESTABLISH MANAGEMENT

Identity Join or register → **Enrollment** Establish MDM → **Targeting** Groups and filters → **Access** Evaluate conditions

- Apple management requires an **Apple MDM push certificate**. **Automated Device Enrollment (ADE)** uses Apple Business Manager or School Manager and an enrollment-program token; supervision enables additional corporate controls.
- **Apple Configurator** prepares supported Apple hardware for enrollment. Company Portal enrollment suits supported user-driven scenarios. Enrollment method, supervision and user affinity determine the available restrictions and update controls.
- Maintain Apple push certificates and enrollment tokens with the appropriate renewal identity. Enrollment **email and push notifications** can communicate successful onboarding; they do not replace the enrollment profile.

Authentication and Conditional Access

- **Windows Hello for Business** uses a device-bound key unlocked with a PIN or biometrics. Configure PIN length and complexity through Hello policy; changing Entra join permissions does not set PIN length.
- **FIDO2 security keys/passkeys** support passwordless authentication without requiring a mobile phone. **Microsoft Authenticator** supports phone-based passwordless sign-in and number matching; SMS and voice are not passwordless methods.
- **Conditional Access** combines user, target resource and condition scopes with grant or session controls. Scope a policy to the required group, cloud app and platform to avoid affecting unrelated access.
- Require **compliant device** status to gate access using Intune evaluation. Use **Require app protection policy** for supported MAM access. App protection alone cannot stop users signing in through every unmanaged client.
- Use **Client apps** conditions to block legacy authentication and **Filter for devices** for supported device properties. An **authentication strength** specifies acceptable MFA methods, including passwordless MFA.
- Protect device enrollment with an appropriately scoped MFA access policy. Test access policies in **report-only** mode, examine sign-in results and retain controlled emergency access before enforcement.

02 Manage and maintain devices (25– 30%

Deployment, upgrade and migration

- An **in-place upgrade** preserves supported apps, settings and files. Match architecture, language, edition path and application compatibility; changing from 32-bit to 64-bit requires a clean installation.
- **Windows 11 readiness** includes a supported processor, TPM 2.0, UEFI/Secure Boot capability, sufficient memory and storage. For Hyper-V, use an appropriately configured **Generation 2** VM with virtual TPM and supported resources.
- **Wipe and load** replaces the operating system. Use **USMT ScanState** to capture supported user state before deployment and **LoadState** to restore it. USMT migrates data and settings, not installed application binaries.

Deployment & Maintenance

Endpoint Administrator

KNOWLEDGE CHEATSHEET

PROVISION AND MAINTAIN

Prepare Readiness and state → **Provision** Image or Autopilot → **Configure** Apps and settings → **Maintain** Updates and recovery

- USMT migration stores can use **/encrypt** at capture and **/decrypt** at restore with the appropriate key. Keep that key available separately from the protected migration store.
- **Subscription activation** steps an eligible activated Windows Pro installation up to Enterprise for a licensed user on a supported join state. It is an edition change, not an OS-version upgrade from Windows 10 to Windows 11.
- **Windows Configuration Designer** creates provisioning packages (**.ppkg**) for settings, apps, certificates and supported bulk join. Protect bulk enrollment tokens and account for their expiration; provisioning can configure an existing installation without reimaging it.

Windows Autopilot and first-run setup

- **Windows Autopilot** customizes OOBE and provisions the installed Windows image. Register device hardware identity through the OEM, partner or a supported hardware-hash CSV import, then assign a deployment profile to a device group.
- **Get-WindowsAutopilotInfo.ps1** collects hardware information for manual registration. Dynamic device groups can recognize Autopilot registration through **[ZTDId]** in device physical IDs; group tags can separate deployment populations.
- **User-driven** deployment prompts an organizational user to sign in. **Self-deploying** mode provisions eligible Entra-joined devices without user authentication and requires supported TPM attestation; it does not provide hybrid join.
- **Pre-provisioning** lets a technician prepare device-targeted apps and settings before the user phase. Configure the join type, user account type, naming options and OOBE experience in the deployment profile.
- The **Enrollment Status Page (ESP)** displays provisioning progress and can block use until selected required apps and configuration complete. Configure timeout, retry and diagnostic collection options there to help investigate failed provisioning.
- Hybrid Autopilot requires the **Intune Connector for Active Directory**, a domain join profile, connectivity and delegated rights to create computer objects in the target OU. Use the connector's configured identity and supported delegation model rather than granting ordinary users broad domain rights.

Images and task sequences

- **MDT Deployment Workbench** organizes operating systems, applications, drivers, packages and task sequences within a deployment share. **Windows ADK** supplies deployment tools; the separate **WinPE add-on** supplies the boot environment.
- A **Standard Client Task Sequence** deploys an OS; **Standard Client Upgrade** uses full operating-system source files for an in-place upgrade. A captured custom WIM alone does not supply all Windows Setup files needed by the upgrade workflow.
- Use **Sysprep /generalize** before capturing a reusable reference image. **DISM** services images; **WinPE** boots deployment and recovery tools. Boot images and installed-OS images have different purposes.

Deployment & Maintenance

Endpoint Administrator

KNOWLEDGE CHEATSHEET

PROVISION AND MAINTAIN

Prepare Readiness and state → **Provision** Image or Autopilot → **Configure** Apps and settings → **Maintain** Updates and recovery

- **Preinstall** handles disk partitioning before the OS is applied. Use GPT/UEFI layouts with the required system and recovery partitions. Install applications and restore supported user state in the appropriate later task-sequence steps.
- **Bootstrap.ini** controls initial connection to the deployment share and early wizard behavior. **CustomSettings.ini** supplies deployment rules such as naming and wizard selections. Updating bootstrap or WinPE components requires regenerated boot images.
- Use **Update Deployment Share** to regenerate Lite Touch boot files. **WDS** can provide network boot and multicast infrastructure in applicable deployments. Driver selection profiles restrict candidates; model-based driver groups can deliberately install a specified driver set.

Configuration, targeting and conflicts

- **Settings catalog** exposes individual configuration settings. **Administrative Templates** expose supported ADMX-backed policy. A **custom OMA-URI** profile addresses a supported Configuration Service Provider setting with the correct path, data type and value.
- **Group Policy analytics** imports GPO reports and identifies MDM-supported settings for migration. Do not assume every GPO setting has an equivalent CSP or behaves identically after migration.
- Assignments target **user or device groups**. Match inclusion and exclusion types; excluding a device group does not reliably cancel a user-targeted assignment. **Assignment filters** refine supported assignments by device properties.
- **Applicability rules** limit supported Windows profiles by OS version or edition. **Scope tags** restrict administrative visibility. Neither replaces the profile's group assignments.
- **Policy sets** bundle supported apps, profiles and compliance policies for common assignments. Platform support and each member's own assignments still matter; not every Intune or Entra object can be added to a set.
- Avoid configuring the same setting differently in baselines, endpoint security and configuration profiles. **MDMWinsOverGP** applies to supported Policy CSP settings; it is not a universal precedence switch for every GPO and MDM setting.

Connectivity, certificates and kiosks

- **Wi-Fi** and **VPN profiles** distribute connection settings to supported platforms. Match connection type, authentication, trusted roots and client requirements; a VPN profile does not by itself grant access to internal resources.
- Deploy a **trusted certificate profile** for root or intermediate CA trust. **SCEP** issues per-device or per-user identity certificates; on-premises SCEP commonly uses **NDES** and the Intune certificate connector.
- **PKCS profiles** use the certificate connector and an issuing CA for supported certificate delivery. **Imported PKCS/PFX** supports distributing an existing user encryption certificate across devices, which is useful for S/MIME decryption.

Deployment & Maintenance

Endpoint Administrator

KNOWLEDGE CHEATSHEET

PROVISION AND MAINTAIN

Prepare Readiness and state → **Provision** Image or Autopilot → **Configure** Apps and settings → **Maintain** Updates and recovery

- **Microsoft Cloud PKI** hosts a root and issuing CA hierarchy without an on-premises connector for that cloud issuance path. Deploy the required trust profiles and a SCEP identity profile; align subject, usage and relying-party trust with the authentication design.
- **S/MIME** signing proves sender identity and message integrity; encryption protects message content using recipient certificates. Mail-app configuration and suitable certificates are both required; do not treat a VPN authentication certificate as a complete S/MIME deployment.
- **Windows kiosk/Assigned Access** constrains a device to the intended app experience. Android dedicated devices support kiosk scenarios; work-profile isolation alone is not a dedicated-device kiosk. Match Windows, Surface Hub and mobile settings to the actual platform.

Updates and servicing controls

- **Quality updates** deliver fixes and security improvements; **feature updates** deliver OS capabilities and versions. Use pilot and production rings to detect problems before broad deployment.
- An **update ring** controls deferrals, deadlines, restarts and user experience. A **feature update policy** targets an OS release. An expedited quality update accelerates an urgent supported update rather than defining the long-term ring schedule.
- **Deferral** delays availability; a **deadline** limits how long installation or restart can be postponed after the applicable trigger. **Grace period** supplies minimum restart time. Active hours are not an indefinite exemption from enforcement.
- **Pause** temporarily stops eligible updates; **Uninstall** requests supported rollback. Feature rollback depends on the configured uninstall window and retained recovery files, not the normal future scheduled installation day.
- **Delivery Optimization** reduces internet downloads through peer caching. **LAN mode** uses local peers; **Group mode** supports an explicitly defined peer group. Configure grouping and foreground/background bandwidth separately from update-ring deadlines.
- For Apple updates, distinguish update installation policy from restrictions that defer visibility or user installation. **Supervision** and enrollment method determine available iOS/iPadOS controls; policies cannot deploy arbitrary unsigned Apple versions.
- Android Enterprise system-update settings can define automatic, postponed or maintenance-window behavior. **Android FOTA** needs a supported OEM integration and connector; otherwise use supported device restrictions. macOS update controls also depend on enrollment and supported OS capabilities.

Deployment & Maintenance / Device Protection

Endpoint Administrator

KNOWLEDGE CHEATSHEET

PROVISION AND MAINTAIN

Prepare Readiness and state → **Provision** Image or Autopilot → **Configure** Apps and settings → **Maintain** Updates and recovery

Windows 365 and Cloud PC provisioning

- **Windows 365 Enterprise** provisions persistent user Cloud PCs through license assignment and provisioning policies. Select join type, network, region and image; use **Cloud PC Administrator** for the relevant provisioning administration.
- **Microsoft-hosted networking** minimizes customer network setup. An **Azure network connection (ANC)** uses a customer virtual network for required private connectivity. Select a network that can actually reach the target resources.
- **Hybrid join** requires AD DS connectivity, working domain DNS and suitable domain-join permissions. A disconnected Azure VNet does not gain on-premises domain reachability simply by being selected in a policy.
- Use a supported, generalized **custom image** with the required architecture, generation and disk format, or a supported gallery image. A Hyper-V VHDX is not automatically a ready-to-upload Azure image artifact.
- Choose a **dedicated** user Cloud PC for persistent access. Shared/Frontline capacity depends on its concurrency model. Apply supported Intune configuration and Windows 365 security baselines to the provisioned devices.

03 Protect devices (15– 20%

Compliance evaluation and enforcement

- **Configuration policies** set device state. **Compliance policies** assess requirements such as minimum OS version, password, encryption and threat risk. **Conditional Access** uses the resulting compliance signal to control resource access.
- Set the tenant option **Mark devices with no compliance policy assigned as** deliberately. To require explicit policy coverage, mark these devices noncompliant; simply creating a policy does not assign it to every device.
- **Actions for noncompliance** include a scheduled noncompliant mark, notifications and supported remote actions. A grace period delays enforcement of the noncompliant state; the compliance validity period governs stale check-in status.
- Use Windows **device health/attestation** settings for supported Secure Boot, code integrity and BitLocker checks. Use the policy's system-security requirements for supported firewall, password and antivirus checks.

Device Protection

Endpoint Administrator

KNOWLEDGE CHEATSHEET

LAYERED ENDPOINT PROTECTION

- **Compliance** — Assess posture
- **Defender** — Detect and respond
- **Encryption** — Protect storage
- **Privilege** — Limit elevation

- **Custom compliance** combines a discovery PowerShell script with a JSON rules file for checks such as BIOS version. Return the expected structured values and monitor per-setting results; a script alone does not define the compliance rule.
- On mobile devices, assess **root/jailbreak**, OS version and password requirements with the platform's own policy. Compliance settings and noncompliance actions differ by platform and enrollment type; do not assume Windows remote actions apply to mobile devices.

Defender integration and threat response

- Connect **Microsoft Defender for Endpoint (MDE)** and Intune through the service connector. Then deploy an **Endpoint detection and response (EDR)** onboarding policy to eligible Windows devices; the connection alone does not onboard every endpoint.
- macOS and Linux require their supported **Defender application/agent** and onboarding configuration. Intune can manage supported macOS deployment; do not send a Windows onboarding package to a different operating system.
- Enable platform signal sharing and configure the compliance policy's **machine risk score** threshold to use Defender risk. Conditional Access can then block noncompliant devices. Machine risk is different from user risk and sign-in risk.
- **Tamper protection** prevents supported unauthorized security-setting changes. Antivirus policies configure scanning and protection; an EDR policy handles onboarding and detection/response configuration, not every antivirus setting.
- Defender **device groups** scope permissions and supported automated investigation/remediation behavior. Rank and matching rules affect grouping; Entra security groups and Azure action groups have different purposes.
- Use **security recommendations**, exposure information, Secure Score and supported **security baseline assessments** to prioritize hardening. Intune security tasks can receive remediation work from Defender integration.

Attack surface and application control

- **Attack surface reduction rules** block risky behaviors such as Office child processes, executable content and selected script activity. **Audit** records impact, **Block** enforces, and supported **Warn** rules allow a user bypass.
- Test ASR policies before broad enforcement. Use a supported **per-rule exclusion** for a justified exception rather than disabling every rule or granting local administrator access.
- **Controlled folder access** protects selected folders from unauthorized changes. Add protected folders and explicitly allowed trusted applications; this controls writing to data, not which applications may execute throughout Windows.

Device Protection

Endpoint Administrator

KNOWLEDGE CHEATSHEET

LAYERED ENDPOINT PROTECTION

- **Compliance** — Assess posture
- **Defender** — Detect and respond
- **Encryption** — Protect storage
- **Privilege** — Limit elevation

- **Exploit protection** mitigates memory exploits with settings such as **DEP** and **ASLR**. Export a tested mitigation XML for deployment when appropriate; system-wide and per-program settings have different scopes.
- **SmartScreen** checks reputation for supported websites and downloaded files. **Network protection** blocks supported access to dangerous destinations. **Defender Firewall** controls network traffic using profile, direction, protocol and endpoint rules.
- **App Control for Business** controls trusted code execution. **Credential Guard** uses virtualization-based isolation to protect secrets. Neither substitutes for disk encryption or app-level data-transfer restrictions.

Encryption, recovery and local passwords

- Use **BitLocker** for Windows volumes and **FileVault** for macOS. Deploy encryption through supported endpoint security policies and escrow recovery material before relying on unattended recovery.
- **BitLocker recovery key rotation** replaces recovery material; reading an escrowed key is a separate operation. Grant the relevant Intune remote-task and device permissions for rotation and the appropriate directory permissions for key retrieval.
- **Windows LAPS** rotates a managed local administrator password and backs it up to the selected directory. Enable Entra backup support, configure an account-protection LAPS policy and select **Microsoft Entra ID** as the backup directory when required.
- LAPS password retrieval, password rotation and local-group membership require different permissions. LAPS does not automatically make the administrator who reads a password a member of the local Administrators group.
- Use **Local user group membership** policy to manage Administrators or Remote Desktop Users. Distinguish adding/removing selected members from **replace** behavior, which can remove other required memberships.

Endpoint Privilege Management

- **Endpoint Privilege Management (EPM)** lets standard users elevate approved work on supported Windows endpoints without permanent local administrator membership. Enable EPM through an elevation settings policy and the required entitlement.
- An **elevation settings policy** controls default handling, validation and reporting. An **elevation rules policy** identifies specific files and their approved elevation behavior.
- Use reliable file identity such as a **hash** or constrained publisher certificate and file attributes. A broad filename-only rule can elevate unintended content; scope rules to the smallest required population.

Device Protection / Applications & Data

Endpoint Administrator

KNOWLEDGE CHEATSHEET

APPLICATION MANAGEMENT

- **Packaging** — Prepare installers
- **Assignment** — Deliver apps
- **Protection** — Guard work data
- **Configuration** — Set app behavior

- **Automatic**, **user-confirmed** and **support-approved** elevation serve different approval models. Configure authentication or business justification where supported; a default deny response governs requests without an applicable allowing rule.
- Control **child process behavior** independently so an approved executable cannot freely elevate unrelated descendants. Review elevation reports and overlapping policy assignments before expanding access.

04 Manage and secure applications (15– 20%

App types, packaging and assignments

- Use the **Microsoft Win32 Content Prep Tool** to package an installer and its supporting files into **.intunewin**. Define silent install/uninstall commands, requirements, detection rules, return codes and restart behavior.
- **Requirements** determine eligibility; **detection rules** determine whether the app is installed. A successful installer exit code without correct detection can still lead to an unsuccessful deployment result.
- Configure a Win32 **dependency** on the dependent app so its prerequisite installs first. **Supersedence** relates replacement or upgrade behavior; detection alone does not establish installation order.
- **Required** installs automatically on eligible assigned targets. **Available** publishes a supported self-service app to Company Portal. **Uninstall** removes it where supported. User targeting follows users to eligible devices; device targeting follows the device.
- Mobile package types include **.ipa** for iOS/iPadOS and **.apk** for Android. Prefer the appropriate Managed Google Play distribution path for Android Enterprise, including private corporate apps; Apple custom apps require the appropriate signing and distribution model.
- Store/catalog apps and **web links** differ from uploaded LOB or Win32 packages. The **Enterprise App Catalog** supplies supported Windows apps through Enterprise App Management. Verify licensing, installation context and targeting rather than treating every app type identically.

Microsoft 365 Apps and Office policy

- Deploy **Microsoft 365 Apps** using the dedicated Intune app type or **Office Deployment Tool (ODT)**. Choose architecture, products, languages, update channel and applicable installation options.
- The **Office Customization Tool** creates configuration XML. ODT **setup.exe /download configuration.xml** retrieves files; **setup.exe /configure configuration.xml** applies installation settings. Downloading alone does not install Office.
- Choose **Monthly Enterprise Channel** for a predictable monthly enterprise release cadence. App-suite selections and assignments define who receives Project or Visio; product selection does not grant their licenses.

Applications & Data

Endpoint Administrator

KNOWLEDGE CHEATSHEET

APPLICATION MANAGEMENT

- **Packaging** — Prepare installers
- **Assignment** — Deliver apps
- **Protection** — Guard work data
- **Configuration** — Set app behavior

- Use **Cloud Policy** for supported Office user-policy settings such as macros, feedback and privacy behavior. Distinguish Office application policy from Intune device configuration and from the suite's installation XML.
- Set default **document formats**, WebView2 behavior and other supported options in the management plane that owns them. An app update channel, Office privacy control and OS update ring are independent settings.

App protection and corporate data

- **App protection policies (APP/MAM)** protect corporate identities and data inside supported apps, including on personal mobile devices without MDM enrollment. The app must integrate the Intune SDK or supported wrapping mechanism.
- Use **Data protection** settings for cut/copy/paste, save locations, printing, backups, encryption and supported screen-capture restrictions. These controls do not automatically govern every unprotected application on the device.
- Use **Access requirements** for the app PIN, passcode complexity and recheck behavior. The app PIN is distinct from the device-unlock passcode and Windows Hello PIN.
- Use **Conditional launch** for minimum OS/app versions, compromised devices and offline access limits. Distinguish blocking access from **selective wipe**; corporate data is removed when the supported app can process the policy action.
- Create separate policies for distinct platform or protection requirements, such as a department with a shorter offline wipe threshold. Avoid contradictory overlapping policies and validate effective app protection on a test user.
- Pair APP with **Conditional Access requiring app protection** to restrict eligible resource access to protected clients. For Windows MAM, assess the supported **Microsoft Edge** work-browsing scenario rather than assuming every desktop Office app is protected.

App configuration and Tunnel for MAM

- **App configuration policies** supply supported application settings such as Outlook account options, Chrome bookmarks or app-defined notifications. **Managed devices** configuration uses MDM; **managed apps** configuration uses the supported app-management channel.
- App configuration can enable supported Outlook **S/MIME** settings; app protection governs corporate data transfer. Neither app configuration nor app protection creates a missing signing or decryption certificate.
- **Microsoft Tunnel** provides access to internal resources through a gateway running on supported Linux container infrastructure. **Tunnel for MAM** extends access to supported unenrolled Android and iOS/iPadOS apps.
- Deploy the **Tunnel gateway** before adding MAM support, then apply the required app configuration and app protection policies. A generic device VPN profile does not configure an unenrolled MAM app's tunnel behavior.

Applications & Data / Operations & Reporting

Endpoint Administrator

KNOWLEDGE CHEATSHEET

OBSERVE AND IMPROVE

Collect Endpoint telemetry → **Analyze** Reports and queries → **Act** Support and remediate → **Validate** Results and trends

- For Android MAM web access, plan for **Microsoft Defender**, **Edge** and **Company Portal** prerequisites. On iOS/iPadOS, supported apps integrate the **Tunnel for MAM SDK**; the same Android client-app requirements do not apply.
- Use trusted roots for internal TLS endpoints and the supported per-app tunnel configuration. App management, authentication and network reachability must all succeed before the user can open an internal application.

05 Optimize endpoint operations by using automation, monitoring, and reporting (10– 15%

Remote actions and device lifecycle

- **Sync** requests a policy check-in. **Collect diagnostics** gathers supported troubleshooting logs. Device actions depend on the platform, ownership, enrollment and network reachability; an offline device cannot execute a new command immediately.
- **Retire** removes supported organizational data and management while preserving personal content. **Wipe** resets a supported device toward factory state. Windows wipe options can change whether enrollment or associated user data is retained.
- **Autopilot Reset** prepares an eligible device for another user while retaining Entra join and Intune management. **Fresh Start** refreshes Windows and removes supported preinstalled apps; it has different retention options and prerequisites.
- **Delete** removes a management record and has platform-dependent retirement effects. **Device cleanup rules** hide stale Intune records; they are not a substitute for issuing a required security wipe or retiring corporate data.
- **Remote lock**, **Locate device** and custom notifications have different platform and ownership support. Check the device action report for results; bulk actions also have action-specific selection limits.

Remote support and management

- **Enable-PSRemoting** configures PowerShell remoting, WinRM service/listeners and applicable firewall access. **Invoke-Command** runs commands remotely; creating a client session does not enable the target computer's listener.
- For public-network Windows clients, **-SkipNetworkProfileCheck** supports the applicable setup while retaining local-subnet firewall scope. Avoid expanding the rule to any remote address when only local-subnet access is required.
- Grant access to the required remoting **session endpoint** and use constrained permissions or **Just Enough Administration** for privileged tasks. Membership in Remote Management Users does not make every administrative command permissible.

Operations & Reporting

Endpoint Administrator

KNOWLEDGE CHEATSHEET

OBSERVE AND IMPROVE

Collect Endpoint telemetry → **Analyze** Reports and queries → **Act** Support and remediate → **Validate** Results and trends

- **Remote Desktop** needs host support, access permission, network/firewall reachability and logon rights. **Deny log on through Remote Desktop Services** overrides a corresponding allow right. **NLA** authenticates before the full session is created.
- Configure drive and clipboard redirection in the RDP client and applicable host policies. Configure **RD Gateway** in the connection's gateway settings. **Windows Admin Center** uses browser access to its gateway and WinRM to managed targets; certificate trust and target remoting are separate requirements.
- **Remote Help** requires tenant enablement, appropriate helper/sharer licensing, supported clients and scoped RBAC. Viewing, full control and elevation are separate permissions. Conditional Access can restrict the helper's sign-in to approved devices.

Analytics, queries and automation

- **Endpoint analytics** uses endpoint performance and user-experience telemetry to assess startup, restart behavior and application reliability. Enable the applicable data collection policy and permissions; an Azure log workspace alone does not onboard endpoints to these reports.
- Use **baselines** to compare performance over time and by device model. Required devices, reporting latency and entitlement affect what appears; compare a representative population before attributing a regression to an update.
- **Device query** retrieves current state from supported corporate-owned, Intune-managed Windows devices that are Entra joined or hybrid joined. It requires the appropriate advanced analytics entitlement and prerequisites, plus a responding endpoint.
- Select the query entity for the evidence required: **WindowsQfe** for installed hotfix entries, **OsVersion** for OS information and **FileInfo** for supported filesystem checks. An absent hotfix row alone may not establish that a superseding cumulative update is missing.
- **Remediations** pair a detection script with a remediation script. Configure run context, architecture, signature behavior and schedule; run the fix when detection signals the defined issue and monitor results.
- Use **Microsoft Graph PowerShell** for repeatable administration with least-privilege consent. For licensing, set the user's usage location, identify the tenant SKU and assign it with **Set-MgUserLicense**; a display name is not a SKU identifier.

Operations & Reporting

Endpoint Administrator

KNOWLEDGE CHEATSHEET

OBSERVE AND IMPROVE

Collect Endpoint telemetry → **Analyze** Reports and queries → **Act** Support and remediate → **Validate** Results and trends

Reports, logs and security insights

- Intune **device and per-setting reports** explain configuration and compliance state. **App protection reports** describe protected app users, including supported unenrolled scenarios. **Device actions** reports track operations such as wipe.
- Entra **sign-in logs** show which resource a user requested and the evaluated Conditional Access result. A noncompliant-device inventory does not by itself show that the device attempted to access OneDrive or SharePoint.
- Use **Intune Data Warehouse** with **Power BI/OData** for historical enrollment, compliance and app/OS trends. Use native reports or supported live queries when current operational state is required.
- **Diagnostic settings** route supported Intune logs to **Log Analytics**, Storage or Event Hubs. Audit logs record administrative changes; operational logs help investigate events such as enrollment problems. **KQL**, workbooks and alerts analyze the exported data.
- For supported Windows client event collection, use **Azure Monitor Agent** and a **data collection rule (DCR)** selecting event logs or performance counters. The client installation path uses a **monitored object** association; distinguish it from Azure VM agent associations.
- **Defender for Cloud Apps** uses Cloud Discovery to identify application use and risk. **Custom app tags** track review status; sanctioned/unsanctioned decisions and supported warn/block controls serve different governance purposes.
- **Attack simulation training** evaluates user responses to simulated threats and assigns follow-up learning. It complements endpoint hardening; app inventory, training completion and device compliance are different evidence sets.