Deployment & Least Privilege

CyberArk Endpoint Privilege Manager

KNOWLEDGE CHEATSHEET

LEAST PRIVILEGE ROLLOUT

Discover Administrative work → **Define** Approved policies → **Pilot** Validate workflows → **Enforce** Remove standing rights

01 Deployment and least privilege

Discover, pilot and enforce

- **Least privilege** removes standing administrative access while preserving approved business tasks through controlled elevation. Application control and credential protection add separate layers of defense.
- Start with **Privilege Management**: discover administrative activity, identify business requirements, build and test policies, then remove unnecessary administrator membership in controlled groups.
- **Discovery** reveals applications and operations needing administrative rights. Review representative users, workflows and child processes before restricting unhandled activity.
- Use a **pilot** and helpdesk request process; monitor exceptions and policy coverage before expanding enforcement. Add application control and threat protection deliberately after testing their impact.

Sets, targets and computer groups

- A **set** groups endpoints under a common policy and configuration boundary. Separate servers and desktops when they require different default policies or operational treatment.
- **Policy targets** select applicable computers and users or groups. A policy must match both its application definition and its target scope to affect a launch.
- **Computer groups** organize endpoints within a set. Define membership deliberately, then use groups for policy or configuration targeting; review membership after device changes.
- For **CSV group synchronization**, enable the relevant set feature, validate computer and group identifiers, import the mapping and check resulting membership.
- **Non-persistent VDI** benefits from a dedicated set and image-aware deployment. Short-lived computer identities need different inventory cleanup and targeting practices from persistent machines.

Licensing and agent capabilities

- Distinguish **workstation** and **server** licensing by the endpoint workload and applicable entitlement. A multiuser server requires the appropriate server entitlement.
- **Full Protection** and **Credential Rotation** sets serve different purposes. Match the set, installation package and licensed capabilities before enrolling endpoints.
- **Immediate Enforcement** agents support a specialized enforcement deployment. Enable the set download option before expecting the corresponding package in the Download Center.
- Check the **agent capability matrix** for the operating system and deployment type. Windows, macOS, Linux, VDI and Immediate Enforcement do not imply identical features.

Deployment & Least Privilege / Policies & Elevation

CyberArk Endpoint Privilege Manager

KNOWLEDGE CHEATSHEET

LEAST PRIVILEGE ROLLOUT

- **Discover** — Administrative work
- → **Define** — Approved policies
- → **Pilot** — Validate workflows
- → **Enforce** — Remove standing rights

Installation and platform preparation

- Use the **Download Center** for the correct agent kit and supporting utilities, including OPAG. Keep the package, set association and installation credentials together during deployment.
- Deploy **Windows** agents interactively or through supported software distribution. Validate OS support, required UAC settings, connectivity and security-tool exclusions in the pilot.
- For **macOS**, download the appropriate kit, install using the supported package workflow, approve required system extensions and Full Disk Access, then confirm registration and policy receipt.
- Preserve the macOS **EPM service account** created for agent operation. For local credential management, verify required macOS Secure Token support as well as agent permissions.
- For **Linux**, use the platform-specific package, service configuration and log controls. Confirm service health and connectivity rather than applying Windows executable names or installation switches.

02 Policies and controlled elevation

Default, application and user policies

- **Default policies** establish broad behavior for a set. Key areas include Privilege Management, Privilege Threat Protection and Local Privileged Accounts Management.
- **Application policies** identify software and assign execution or privilege behavior. **Application groups** collect applications governed by a shared action.
- **Advanced policies** provide detailed application matching, targets, access permissions, timing, auditing and conditional enforcement. Name policies by purpose, action and target audience.
- **User policies** govern supported user capabilities such as JIT access, removable-drive access, filesystem and registry access, and Windows service permissions.
- **Policy precedence** depends on the policy category, action and applicable priority rules. Inspect the effective policies when definitions overlap; creation order alone is not a safe decision rule.

Policies & Elevation

CyberArk Endpoint Privilege Manager

KNOWLEDGE CHEATSHEET

POLICY DECISION

Identify Application → **Target** User and endpoint → **Decide** Action and conditions → **Audit** Effective behavior

Application actions and privilege boundaries

- **Allow** permits execution. **Elevate** grants administrative privileges under policy control. **Elevate if Necessary** supplies elevation when the application needs it.
- **Block** prevents a matched application from running. An allowed application does not automatically receive administrative rights, and elevated execution does not exempt it from every security control.
- **Unhandled applications** have no applicable explicit handling rule. Default policy settings determine their detection, elevation or application-control treatment.
- Predefined groups include **Elevate**, **Allow**, **Block** and **Developer Applications**. Review the group action and membership before adding broad application definitions.

Trusted sources and application identity

- **Trusted sources** express approved software provenance, such as publishers, installers or controlled distribution locations. Use narrow criteria and protect the source from unauthorized writes.
- **Publisher**, product, installation package and installing identity can help define trust in supported Windows workflows. A digital signature establishes origin and integrity, not universal safety.
- For **macOS trust**, distinguish publisher-signature trust from installation-package trust. Do not assume every Windows trust source or targeting mechanism is available on macOS.
- **Trusted applications** can use Elevate if Necessary rather than always running elevated. Trust rules still require deliberate scope and the appropriate policy action.
- For **unsigned executables**, gather stable application properties and create a narrowly scoped definition. A filename or writable folder alone is weak evidence of identity.

Child processes, conditions and access tokens

- **Child-process handling** controls whether a parent policy also covers spawned programs. A working main window can still fail when a menu launches a helper needing separate privileges.
- Enable child-process inclusion or elevation only for the required process chain. Test helpers and command interpreters; unrestricted inheritance can enlarge the privileged execution path.
- **Conditional enforcement** can use a script result to decide whether a policy applies. Validate the script, execution context, timeout and behavior when the condition cannot be evaluated.

Policies & Elevation

CyberArk Endpoint Privilege Manager

KNOWLEDGE CHEATSHEET

POLICY DECISION

Identify Application → **Target** User and endpoint → **Decide** Action and conditions → **Audit** Effective behavior

- A **custom user access token** limits the privileges and permissions supplied by an Elevate policy. It is a least-privilege execution control, separate from an agent maintenance token.
- **Developer Applications** reduces expensive source tracking for tools generating many files. Treat this as a performance-sensitive classification and grant any required elevation through appropriate policy.

Temporary access and offline authorization

- **Just-In-Time access and elevation** grants temporary privileges to a defined user and target. Set the duration, record the reason and collect audit information.
- Review **Terminate administrative processes when the policy expires**. Expiring permission to start privileged work and terminating already-running administrative processes are distinct controls.
- **Offline Policy Authorization Generator (OPAG)** supports authorized elevation when an endpoint cannot retrieve a new policy online. Scope the authorization to the intended request and validity period.
- In an **offline authorization** workflow, the user provides the request information, helpdesk validates it and generates the authorization, and the user applies it on the endpoint. Audit the exception.

End-user dialogs and policy maintenance

- **End-User UI** settings control the dialog shown for an elevation or block action. Use clear text identifying the action and the next approved support step.
- A **blocked application request** can collect user justification and contact email. Configure request action buttons and approval notification rather than relying on the main message alone.
- **Audit Video** has separate recording, retention, storage and user-notification settings. Check the configured recording triggers and lifecycle when expected evidence is missing.
- **Policy Recommendations** and **CORA AI** assist policy decisions using observed activity. Review recommendations against least privilege and business requirements before applying them.
- Use **policy import/export** for controlled reuse and backup. Recheck application definitions, target identities, groups and effective actions in the destination set.

Threat Protection

CyberArk Endpoint Privilege Manager

KNOWLEDGE CHEATSHEET

PROTECTION LAYERS

- **Privilege** — Reduce exposure
- **Threat** — Protect credentials
- **Ransomware** — Protect files
- **Rotation** — Change secrets

03 Threat and credential protection

Credential theft and threat deception

- **Privilege Threat Protection** detects or blocks access patterns associated with credential theft and lateral movement, including attempts against sensitive operating-system resources.
- Target protection modules to the **supported OS and application**. A module protecting a particular application needs appropriate targets; agent availability alone does not establish module support.
- **Credential lures** plant deceptive credential artifacts and produce detection events when attackers interact with them. Use a distinctive lure identity that does not collide with a real account.
- **Detect** collects evidence without the corresponding preventive enforcement. Use detection events and threat dashboards to investigate actor, process, target resource and affected endpoints.
- For a legitimate application triggering **LSASS protection**, prefer a narrow module-specific exclusion. A global threat-protection exclusion or Files to Be Ignored Always removes a wider layer of inspection.

Protected files and authorized applications

- **Ransomware Protection** monitors unauthorized access to protected data. Its application authorization and file scope are separate from the decision to allow an application to launch.
- Review **Authorized Applications (Ransomware Protection)** before enforcing restrictions. Include only software that legitimately needs access to the protected resources.
- Configure **protected files, folders and extensions** in the ransomware policy scope. Adding an application to the authorized group does not add a protected file type.
- **Detect** helps establish a baseline; **Restrict** enforces ransomware protection. Check the ransomware mode directly rather than relying on a separate unhandled-application block setting.
- A **ransomware authorization** is a scoped exception for protected-data access. It is distinct from an Allow application policy and from a global agent inspection exclusion.

Threat Protection / Agent Operations

CyberArk Endpoint Privilege Manager

KNOWLEDGE CHEATSHEET

PROTECTION LAYERS

- **Privilege** — Reduce exposure
- **Threat** — Protect credentials
- **Ransomware** — Protect files
- **Rotation** — Change secrets

Threat intelligence and risk interpretation

- **Threat intelligence** adds external reputation or analysis to application investigation. Distinguish a hash lookup from uploading an actual file for sandbox analysis.
- **NSRL** identifies known software through reference hashes. **Not found** means the file is absent from the reference data; it establishes neither maliciousness nor safety.
- **VirusTotal**, **WildFire** and application risk analysis services provide different evidence. Check what data is submitted, the integration configuration and licensing before enabling a service.
- Treat **reputation results** as investigation inputs. Combine them with signature, provenance, behavior and business need before creating a trust or elevation policy.

Local administrator removal and rotation

- **Remove Local Administrators** manages membership of local administrative groups. Preserve approved recovery access and review retained accounts; built-in Administrator is treated specially.
- **Credential rotation** changes passwords of managed local privileged accounts. Membership removal and password rotation address different risks and require separate configuration.
- For **loosely connected devices**, the EPM agent and service relay credential-management operations between the endpoint and the CyberArk PAM environment. Verify account onboarding and connectivity.
- **PVWA** supplies a PAM web interface; credential-management services and the endpoint agent perform other parts of the workflow. Do not confuse console access with the component changing the local password.
- For macOS rotation failures, check **Secure Token**, service-account health, endpoint password requirements and connectivity. Full Disk Access approval and password-rotation prerequisites are distinct checks.

04 Agent operations and troubleshooting

Connectivity, cached policy and event timing

- The agent communicates with **EPM SaaS over HTTPS on TCP 443**. Validate DNS, proxy configuration, TLS trust and outbound access to the correct service endpoints.
- A disconnected agent continues using its **last received policies**. A console change cannot affect an offline endpoint until it receives the update or a supported offline authorization.
- Test the **service URL from the affected endpoint** and inspect agent diagnostics. Successful ping does not prove that HTTPS, proxy authentication or certificate validation works.

Agent Operations

CyberArk Endpoint Privilege Manager

KNOWLEDGE CHEATSHEET

TROUBLESHOOTING SEQUENCE

Connect HTTPS and TLS → **Inspect** Effective policies → **Diagnose** Logs and scope → **Restore** Tested protection

- **Event Queue Flush Period** controls event upload timing. **Policy Update Rate** governs policy refresh; heartbeat settings concern connectivity status. Diagnose the relevant channel separately.
- Inspect **Active Policies**, agent logs and the support-information bundle to confirm what the endpoint actually received. A console policy definition alone does not prove effective enforcement.

Self-defense and maintenance authorization

- **Agent self-defense** protects the EPM installation and configuration against tampering. Administrative OS rights alone may be insufficient for protected maintenance operations.
- Use an authorized **EPM secure token** for supported maintenance, such as disabling protection or uninstalling a protected agent. Limit scope and lifetime to the intended computers and task.
- For a disconnected endpoint, a **server-side configuration change** cannot arrive immediately. Use the supported offline maintenance authorization rather than a token generated for an unrelated computer.
- Plan **agent upgrades** through the management console or supported software distribution with the required installation credentials. Validate the upgrade method against self-defense requirements.
- Keep three concepts separate: **EPM secure token** authorizes maintenance; **custom user access token** shapes an elevated process; **macOS Secure Token** is an operating-system account capability.

Mutual exclusions and targeted diagnosis

- **Mutual exclusions** mean configuring EPM to exclude the required third-party security components and configuring those products to exclude EPM, using supported exclusion guidance.
- **Files to Be Ignored Always** is a broad inspection exclusion. Use exact supported paths and applications; avoid turning a performance workaround into an unrestricted trust boundary.
- **Driver-level exclusion changes** can require an endpoint reboot. A service restart does not necessarily reload kernel-level protection configuration.
- Use a **custom agent configuration** to isolate one endpoint when troubleshooting. Time-limit policy suspension, record the test and restore protection after collecting evidence.
- For failed elevation, inspect **UAC configuration**, policy targets, application matching, child processes and agent logs. **DLL hijacking protection** is separate from agent self-defense.

Administration & Evidence

CyberArk Endpoint Privilege Manager

KNOWLEDGE CHEATSHEET

OPERATIONAL EVIDENCE

- **Catalog** — Applications
- **Inventory** — Endpoints
- **Events** — Activity
- **Admin audits** — Console changes

05 Administration, inventory and evidence

Console access and SAML

- **Account Administrators** manage account-wide configuration; **Set Administrators** operate within assigned sets. Grant the narrowest console role needed for the task.
- **SAML** federates console authentication to an identity provider. Validate the trusted signing certificate, signature, audience, recipient and user mapping; authentication and EPM role assignment are separate.
- **Automatic user provisioning** maps identity-provider attributes to the EPM user and authorized access. Validate the required binding attribute and permissions before broad deployment.
- To enforce **SSO**, use the account login restriction setting after testing SAML. Preserve the intended Account Administrator recovery route and verify a fresh sign-in.

Application Catalog and endpoint inventory

- **Application Catalog** provides a consolidated view of detected applications, including software covered by policies and software still unhandled. Review properties and analysis results before authoring rules.
- **Application Coverage by Policies** measures how much detected activity is handled. Coverage supports rollout decisions but does not itself establish that every handling rule is least privilege.
- **Application scans** discover installed software on selected endpoints. Check File Types to Scan for Application Catalog when executable types are missing; an offline endpoint cannot execute a new scan immediately.
- **Endpoint inventory** includes device identity and installed-program information. Check agent connectivity, scan progress and collected-data settings before treating an absent entry as absent software.

Administration & Evidence

CyberArk Endpoint Privilege Manager

KNOWLEDGE CHEATSHEET

OPERATIONAL EVIDENCE

- **Catalog** — Applications
- **Inventory** — Endpoints
- **Events** — Activity
- **Admin audits** — Console changes

Reports, audits, data and automation

- Use **Events** for endpoint activity, **Policies** for policy-related evidence, **Endpoints** for computer state and **Admin Audits** for console administration such as token generation.
- **Aggregated events** group similar activity for review. Inspect their count, time range, application and affected endpoints before interpreting one row as one occurrence.
- A **Threat Detection Dashboard** summarizes detection activity; detailed threat events support investigation. Correlate timestamps using the report time-zone convention.
- **Retention** differs among events, administrator activity, endpoint cleanup and audit video. Configure collection and export around evidence needs; expired local video is not restored by a longer future retention setting.
- **SaaS data protection** includes encrypted transport, protected storage and customer-data isolation. Distinguish endpoint telemetry from administrator sign-in and audit data, and scope access accordingly.
- The **EPM REST API / Web Services SDK** automates supported operations on EPM objects and event data. Authenticate with an appropriately scoped identity and preserve set boundaries in requests.