ManageEngine
ADAudit Plus

The **Identity** Auditing & Security playbook

From hybrid security assessments to automated threat response, discover how to uncover hidden identities, detect privilege escalation, trace attacker activity, and strengthen security across identity and cloud environments.



Index

Use case 01: Hybrid identity security posture assessment ---- 01

Use case 02: Detection of shadow identities ---- 03

Use case 03: Identity configuration drift ---- 05

Use case 04: AD delegation auditing ---- 07

Use case 05: Detect the "impossible travel" scenarios ---- 09

Use case 06: Privilege escalation ---- 11

Use case 07: High-risk identity changes ---- 13

Use case 08: Lateral movement indicators ---- 15

Use case 09: Joiner-mover-leaver (JML) auditing ---- 17

Use case 10: Compliance audit evidence ---- 19

Use case 11: Detection-to-remediation automation ---- 21

USE CASE 01

Hybrid identity security posture assessment

Continuously scan to find, fix, and prove security gaps across on-premises and cloud environments



Common bottlenecks

Fragmented hybrid visibility	Point-in-time assessments	Hidden misconfigurations	No proof of remediation

The solution

Continuous posture monitoring

- Always-on scans against industry benchmarks

Prioritized risk

- Exposures ranked by severity with remediation guidance

Unified hybrid view

- Correlated visibility across Active Directory (AD), Entra ID, Azure, AWS, and Google Cloud

Measurable progress

- Re-assessments and reports proving risks were reduced

Unified hybrid and multi-cloud view

Complete visibility from AD to the cloud

- ✓ Correlate AD changes with Entra ID modifications and sign-ins
- ✓ Monitor privileged account activity across hybrid environments
- ✓ Detect suspicious behavior spanning on-premises and cloud
- ✓ Get a unified CSPM view of Azure, AWS, and Google Cloud
- ✓ Identify and fix misconfigurations across multi-cloud assets
- ✓ Apply best-practice remediation for cloud compliance

Attack surface analysis

Find and prioritize gaps before attackers do

- ✓ Scan AD continuously against industry benchmarks
- ✓ Replace point-in-time assessments with always-on monitoring
- ✓ Detect 25+ AD attacks, including Kerberoasting, Golden Ticket, and DCSync
- ✓ Uncover pass-the-hash, pass-the-ticket, ransomware, and RID hijacking
- ✓ Rank exposures by severity with remediation guidance
- ✓ Catch anomalies that static checks miss with UBA

Continuous validation

Prove measurable security progress

- ✓ Re-run assessments after every remediation
- ✓ Confirm risks are reduced and no new drift appears
- ✓ Schedule recurring reports that prove risk reduction
- ✓ Feed posture data into SIEM and ITSM platforms

USE CASE 02

Detection of shadow identities

Surface the accounts that no one is watching (known as shadow identities)



Common bottlenecks

Out-of-process account creation	Invisible privilege grants	Revived dormant accounts	Delayed discovery

The solution

Creation-time detection

- Real-time alerts on accounts created outside approved channels

Behavior-backed validation

- Anomaly detection on logons of revived and service accounts

Privilege path tracking

- Every group, permission, and sensitive attribute change recorded

Rapid containment

- Scripted responses backed by forensic audit trails

Uncover shadow identities and privilege paths

Catch every new account and silent escalation

- ✓ Track user, computer, and group creation across AD and Entra ID
- ✓ See who created each account, when, and from where
- ✓ Audit local account creation and Administrators group changes
- ✓ Alert on unapproved creations, off-hours activity, and unexpected OUs
- ✓ Monitor membership changes in built-in and custom privileged groups.
- ✓ Track permission changes on AD objects, OUs, and GPOs
- ✓ Capture before-and-after values for SIDHistory and adminCount

Detect dormant and misused accounts

Flag identities that resurface or behave unusually

- ✓ Spot revived accounts through re-enablement, password resets, and attribute changes
- ✓ Audit service and privileged account logons from unexpected hosts or hours
- ✓ Detect anomalous logons, first-time server access, and activity spikes with UBA

Respond and prove control

Turn detections into action and audit-ready evidence

- ✓ Run automated scripts to disable accounts or log off sessions
- ✓ Retain archived audit trails for forensic investigation
- ✓ Trace when and how an unauthorized identity was introduced
- ✓ Schedule out-of-the-box SOX, PCI DSS, HIPAA, and GDPR reports

USE CASE 03

Identity configuration drift

Catch unauthorized changes before they weaken your identity security. Identity security doesn't stop at AD. In hybrid environments, changes in Entra ID can introduce similar risks or create new paths to privileged access. Extend your monitoring beyond on-premises AD to keep cloud identity configurations under control.



Common bottlenecks

Silent policy changes	Untracked structural edits	Weakened account settings	Cloud blind spots

The solution

Change-level precision

- Old and new values for every policy and GPO setting

Control integrity

- Alerts on settings and audit policies that lower defenses

Foundation monitoring

- Schema, OU, site, and DNS changes tracked end to end

Hybrid consistency

- On-premises and Entra ID changes in a single console

Catch policy and security setting drift

Know exactly what changed in your security policies

- ✓ Audit GPO setting changes with old and new values, who, and when
- ✓ Track GPO creation, deletion, and link changes across domains, sites, and OUs
- ✓ Monitor changes to password, account lockout, and Kerberos policies
- ✓ Track UAC changes like “password never expires” and “password not required”
- ✓ Detect changes that disable Kerberos pre-authentication on accounts
- ✓ Track before-and-after permission and ownership changes on objects, OUs, and GPOs
- ✓ Alert on audit policy changes on DCs and servers that could blind security teams

Monitor the AD foundation

Spot changes to the core of your directory

- ✓ Audit OU creation, deletion, moves, and renames that affect GPOs and delegation
- ✓ Track schema and configuration partition changes
- ✓ Monitor site, subnet, and site link changes
- ✓ Detect DNS zone and record changes that can redirect authentication or disrupt services

Extend drift detection to Entra ID

Same visibility from on-premises to the cloud

- ✓ Audit Entra ID role assignment and policy changes
- ✓ Monitor app and service principal changes, including new credentials
- ✓ Track permission grants that alter who can do what in the cloud
- ✓ Correlate AD and Entra ID changes in a single console

USE CASE 04

AD delegation auditing

Hold every delegated account accountable for its actions



Common bottlenecks

Unchecked help desk actions	Creeping delegated rights	Hidden impersonation paths	Out-of-scope changes

The solution

Per-account accountability

- Every delegated action tied to a performer, object, and time

Impersonation path control

- Unconstrained, constrained, and resource-based delegation changes monitored

Rights change tracking

- Permission, ownership, and operator group changes recorded

Boundary enforcement

- Alerts on after-hours, bulk, and sensitive delegated actions

Audit delegated account activity

Know exactly what each delegated account did

- ✓ Report on password resets, unlocks, and attribute changes by help desk staff
- ✓ See who made each change, on which object, and when
- ✓ Filter activity by user, group, or OU over any time period
- ✓ Email scheduled activity reports to managers for regular review

Track delegated rights and Kerberos delegation changes

Watch who is being handed control

- ✓ Audit permission entries added to or removed from OUs and containers
- ✓ Monitor membership changes to Account, Server, and Backup Operators
- ✓ Detect changes that enable unconstrained delegation on computer accounts
- ✓ Audit changes to constrained delegation targets that let services impersonate users
- ✓ Monitor resource-based constrained delegation changes on computer objects

Detect unusual delegated activity

Spot actions that deviate from expected patterns

- ✓ Alert on delegated activity outside business hours
- ✓ Detect unusually high volumes of changes in a short period
- ✓ Alert on delegated changes to privileged groups and critical accounts

USE CASE 05

Detect the "impossible travel" scenarios

Catch compromised credentials used from places a user can't physically be.



Common bottlenecks

Location-blind logons	Scattered sign-in sources	Overlapping sessions	Unmeasured impact

The solution

Geo-aware auditing

- Location and IP details for every sign-in

Concurrent session detection

- One identity active across many places exposed

Behavioral anomaly spotting

- Unusual hosts, times, and failure patterns flagged

Post-sign-in forensics

- Full activity trail after a suspicious logon

Map every sign-in to a location

Know where each authentication came from

- ✓ Audit Entra ID sign-ins with IP, location, device, and app details
- ✓ Track AD FS authentication attempts with client IP addresses
- ✓ Audit VPN logons via RADIUS (NPS) with source IP addresses

Spot impossible travel and anomalous logons

Catch one identity active in too many places

- ✓ Report on users logged on to multiple computers at once
- ✓ Compare AD logons and Entra ID sign-ins to spot one account in two places
- ✓ Track logon session durations to find overlapping sessions
- ✓ Use UBA to detect logons from hosts a user has never accessed
- ✓ Flag logons at times outside a user's normal pattern
- ✓ Spot failed logon spikes before a sign-in from a new source
- ✓ Alert on sign-ins from unexpected countries or IP ranges

Trace what happened after the sign-in

Follow a suspicious identity to measure the impact

- ✓ Review AD changes and file access after a suspicious sign-in
- ✓ Analyze Entra ID sign-in failure reasons, such as failed MFA
- ✓ Report failed MFA attempts to see which suspicious sign-ins were blocked

USE CASE 06

Privilege escalation

Catch attackers the moment they elevate their rights.



Common bottlenecks

Unnoticed role grants	Hidden SID and ACL paths	Weaponized Group Policy	Host-level blind spots

The solution

Account manipulation control

- Privileged group and Entra ID role grants tracked

Hidden rights exposure

- SIDHistory, AdminSDHolder, and ACL changes surfaced

Policy abuse prevention

- GPO settings, links, and permissions monitored

Endpoint escalation tracking

- Local admin, process, and user rights changes audited

Detect visible and hidden privilege grants

Spot rights granted through groups, roles, and ACLs

- ✓ Audit additions to Domain Admins, Enterprise Admins, and nested groups
- ✓ Track high-privilege Entra ID role assignments like Global Administrator
- ✓ Monitor credentials added to Entra ID apps and service principals
- ✓ Track SIDHistory changes that grant hidden admin-level access
- ✓ Audit AdminSDHolder permission changes that affect all protected accounts
- ✓ Monitor ownership and permission changes on privileged users and groups

Track Group Policy abuse

Catch GPOs being turned into escalation tools

- ✓ Audit GPO changes that add local admins or grant powerful user rights
- ✓ Track GPO links to domain controller OUs or the domain root
- ✓ Monitor GPO permission changes that let non-admins edit policies

Monitor host-level escalation

See how rights are gained on servers and workstations

- ✓ Audit additions to local Administrators groups
- ✓ Track elevated process execution to speed up incident response
- ✓ Monitor changes to sensitive user rights assignments

USE CASE 07

High-risk identity changes

Catch the changes that can turn a trusted identity into an attacker's tool.



Common bottlenecks

Unverified credential resets	Silent attribute tampering	Revived or extended accounts	Exposed high-value identities

The solution

Credential change oversight

- Resets, unlocks, and MFA changes tied to a performer

UPN, contact, and manager edits tracked

- Renames, expiry removals, and restorations flagged

Attribute integrity

- UPN, contact, and manager edits tracked

VIP account shielding

- Scoped alerts and protection changes for critical identities

Watch credential and attribute changes

Catch edits that hand over an account's keys

- ✓ Monitor password resets on privileged and service accounts
- ✓ Investigate unexpected resets by account, performer, and timing
- ✓ Track new Entra ID authentication methods like phones and authenticator apps
- ✓ Report who unlocked accounts to spot unlocks aiding brute-force attacks
- ✓ Track UPN and email changes that enable impersonation or mail interception
- ✓ Audit changes to contact details used for recovery and help desk checks
- ✓ Monitor manager and department changes that affect approvals

Track risky lifecycle changes

Flag changes that quietly extend or revive an identity

- ✓ Audit account renames, including computer accounts renamed to impersonate DCs
- ✓ Track expiration dates removed from temporary and contractor accounts
- ✓ Monitor deleted account restorations that bring old access back

Watch high-value accounts

Keep a closer eye on the identities attackers want most

- ✓ Scope alerts to executive, finance, and IT accounts to flag any change
- ✓ Track Protected Users group removals that strip credential protections
- ✓ Audit changes that lift logon hour and workstation restrictions

USE CASE 08

Lateral movement indicators

Follow attackers as they hop from one system to the next.



Common bottlenecks

Replayed credentials	Unmonitored remote sessions	Disguised remote execution	Untraceable spread

The solution

Credential abuse detection

- Detect credential replay and Kerberos ticket forgery, including pass-the-hash (PtH), pass-the-ticket (PtT), Golden Ticket, and Silver Ticket attacks

Execution trace capture

- Remote services, tasks, and shells exposed

Remote session oversight

- RDP and multi-host logons tracked from source to target

Intrusion path mapping

- Host-by-host movement of every account reconstructed

Detect credential abuse

Catch stolen credentials and forged tickets in use

- ✓ Detect PtH and PtT activity from reused NTLM hashes or Kerberos tickets
- ✓ Identify Golden Ticket and Silver Ticket indicators of forged Kerberos tickets
- ✓ Track abnormal NTLM and Kerberos authentication patterns

Trace remote access and movement

Follow an account from host to host

- ✓ Audit RDP sessions with source, destination, and session duration
- ✓ Report RDP connections from workstations to DCs and critical servers
- ✓ Alert when one account logs on to many hosts in a short window
- ✓ Track service accounts logging on to hosts outside their usual footprint
- ✓ Report an account's logons history across hosts to trace its movement

Expose remote execution

Catch commands and payloads launched on other hosts

- ✓ Track temporary service installations that signal PsExec-style activity
- ✓ Monitor scheduled tasks created remotely to run payloads
- ✓ Audit process creation to spot WMI and PowerShell remoting shells
- ✓ Audit executables and scripts dropped into admin shares and system folders

USE CASE 09

Joiner-mover-leaver (JML) auditing

Keep a complete audit trail of every identity from hire to exit.



Joiner provisioning | Mover transition | Leaver deprovisioning | Post-exit monitoring

Common bottlenecks

Unverified day-one access | Privilege creep | Incomplete offboarding | Reactivated leavers

Usage of shadow identities—eEven after they are long gone—for administrative actions in the ecosystem

The solution

Onboarding verification

- Creation details and initial access validated

Offboarding proof

- Disablement, removals, and post-exit logons recorded

Role change accountability

- Attribute, OU, and group shifts tracked with old and new values

Reversal detection

- Re-enabled, reset, and restored accounts flagged



Audit joiner provisioning

Verify new hires get the right access from day one

- ✔ Record each new account's OU and initial attribute values
- ✔ Review group memberships assigned to new accounts against their role
- ✔ Report first logons to spot accounts used before an employee's start date



Track mover transitions

Catch access that follows people across roles

- ✔ Audit department, title, and manager changes with old and new values
- ✔ Track OU moves when users change teams or locations
- ✔ Review group additions and removals around a role change to spot privilege creep



Verify leaver deprovisioning

Prove access ends when employment does

- ✔ Audit account disabling, deletion, and group removals with who and when
- ✔ Track logon attempts by disabled and expired accounts after exit
- ✔ Spot unusual file access or changes by departing users in their final days
- ✔ Track re-enabling of offboarded accounts and who performed it
- ✔ Audit password resets and group additions on disabled accounts before reuse

USE CASE 10

Compliance audit evidence

Turn everyday audit data into proof that auditors accept



Event collection | Regulation mapping | Long-term retention | Auditor handover

Common bottlenecks

Manual evidence gathering	Unproven access controls	Overwritten event logs	Last-minute audit scrambles

The solution

Always-ready compliance

- Reports grouped by each regulation's requirements

Access control proof

- Privileged, logon, and sensitive file activity documented

Evidence longevity

- Archived data that is able to be restored to any past audit period

Effortless handover

- Scheduled exports and report-only auditor access

Map audit data to regulations

Get evidence organized the way auditors ask for it

- ✓ Access ready-made SOX, HIPAA, PCI DSS, GDPR, FISMA, GLBA, and ISO 27001 reports
- ✓ Group reports by each regulation's specific requirements
- ✓ Build custom compliance reports for internal policies or other standards
- ✓ Cover AD, Entra ID, servers, file servers, and workstations in one view

Document access control

Show that access to sensitive systems and data is controlled

- ✓ Report privileged group and permission changes to show who got elevated access
- ✓ Present logon and failed logon activity on regulated systems
- ✓ Audit file access on cardholder, patient, and other sensitive data

Retain and deliver evidence

Keep proof ready long after events occur

- ✓ Archive audit data for each regulation's required retention period
- ✓ Keep audit data even after native event logs are overwritten
- ✓ Restore archived data to report on past audit periods
- ✓ Schedule compliance reports to reach auditors and compliance teams
- ✓ Export reports in PDF, CSV, HTML, and XLSX
- ✓ Give auditors report-only access without configuration rights

USE CASE 11

Detection-to-remediation automation

Close the loop, from the first suspicious event to a contained threat.



Common bottlenecks

Alert fatigue	Disconnected response tools	Missing investigation context	Slow manual containment

The solution

Precision alerting

- Predefined, threshold, and ML-driven detections

Context-rich triage

- Event details, activity timelines, and risk scores in one place

Connected response

- Alerts routed to email, SMS, ITSM tools, and SIEM tools

Instant containment

- Scripted actions triggered the moment an alert fires

Detect and route alerts

Get the right alert to the right responder

- ✓ Use predefined or custom alert profiles for changes, attacks, and anomalies
- ✓ Set threshold rules that trigger only when activity crosses set limits
- ✓ Catch what static rules miss with ML-based anomaly detection
- ✓ Send email and SMS alerts by severity so critical events go first
- ✓ Raise tickets in ServiceNow, Jira, Zendesk, Freshservice, and Kayako
- ✓ Forward alerts and events to SIEM tools via Syslog, Splunk, and ArcSight

Investigate with full context

Understand an alert's scope before acting

- ✓ Drill down from an alert to who, what, when, and where
- ✓ Review account activity before and after the alert to gauge spread
- ✓ Check risk scores and anomaly history to rule out false positives

Execute remediation automatically

Contain threats in seconds, not hours

- ✓ Run PowerShell or batch scripts the moment an alert fires
- ✓ Deactivate accounts, log off sessions, or shut down machines
- ✓ Pass user, host, and object details into scripts for targeted response
- ✓ Audit remediation actions to confirm each response ran