ManageEngine

Your 2026 guide to

Complying with BACEN Resolution CMN 4,893/2021

Table of contents

Introduction

BACEN Resolution CMN 4,893/2021 is one of the most significant cybersecurity mandates governing Brazil's financial ecosystem, fundamentally reshaping how regulated institutions manage cyber risk, data protection, and operational resilience. Issued by the National Monetary Council (CMN) in February 2021 and effective from July 1, 2021, the resolution establishes mandatory cybersecurity governance requirements for financial institutions supervised by the Central Bank of Brazil (BACEN), with a strong focus on policy formalization, incident preparedness, and third-party risk management.

Introduced in response to rapid digital transformation, growing cloud adoption, expanding third-party dependencies, and increasingly sophisticated cyberthreats, the resolution replaces earlier frameworks (Resolutions 4,658/2018 and 4,752/2019) with a more comprehensive and enforceable standard. It mandates the implementation of formal cybersecurity policies; appointment of accountable security leadership; defined incident response and recovery plans; annual governance reporting; and strict controls over data processing, storage, and cloud service providers. These requirements are designed to safeguard the confidentiality, integrity, and availability of information systems while preserving the overall stability of Brazil's financial system.

For financial institutions, compliance with BACEN Resolution CMN 4,893/2021 goes far beyond meeting regulatory obligations. It strengthens governance and accountability; improves visibility into identity and access risks; reduces the likelihood and impact of cyber incidents; and minimizes financial, operational, and reputational exposure. Most importantly, it shifts organizations from reactive crisis response to proactive cyber risk management. By aligning with the principles of BACEN Resolution CMN 4,893/2021, institutions demonstrate security maturity, build long-term resilience, and meet the level of trust and stability expected of modern financial entities operating in a highly regulated digital economy.

Compliance levels and requirements

BACEN Resolution CMN 4,893/2021 is divided into five chapters, each covering a key component of the cybersecurity governance framework mandated for financial institutions operating in Brazil. Together, these chapters define the strategic, operational, and oversight mechanisms required to ensure cyber resilience, protect sensitive information, and maintain the integrity of financial operations.

CHAPTER I

Object and scope of application

This first chapter defines the purpose, applicability, and general principles of the resolution. It states that every financial institution and other non-financial entities that fall under the Central Bank's supervision must:

- Establish and maintain a comprehensive cybersecurity policy proportionate to its size, risk profile, business model, and data sensitivity.
- Implement standards and procedures to ensure the confidentiality, integrity, and availability of data and systems.
- Apply these controls not only internally but also to outsourced environments, including data processing, data storage, and cloud computing services.

The chapter also clarifies exceptions—notably, that payment institutions are governed by their own regulatory framework and not by this resolution. It also introduces the principle of proportionality, emphasizing that cybersecurity measures must be consistent with the scale and operational complexity of the institution rather than uniform across all entities.

CHAPTER II

Cybersecurity policy

The second chapter forms the core of the regulation, setting forth how institutions must establish, disclose, and operationalize their cybersecurity policies. It is subdivided into three key sections.

SECTION I: Implementation of the cybersecurity policy

This section defines the minimum content and operational requirements of a cybersecurity policy. Institutions must adopt a formal document approved by senior management or the board that explicitly details objectives, responsibilities, and controls.

Key components include:

- **Cybersecurity objectives:** Define prevention, detection, and mitigation strategies for vulnerabilities, incidents, and intrusions.
- **Comprehensive controls:** Cover encryption, authentication, network segmentation, access management, intrusion prevention and detection, malware defense, and information-leakage prevention.
- **Traceability and accountability:** Maintain mechanisms to trace sensitive data and access histories for auditability.
- **Incident management:** Ensure continuous monitoring, classification, and analysis of events with cause identification and impact evaluation.
- **Business continuity planning:** Integrate cybersecurity scenarios into continuity and disaster-recovery plans.
- **Cybersecurity culture:** Promote awareness among employees, clients, and outsourced entities through periodic training.
- **Information sharing:** Establish channels for collaboration with other institutions and the Central Bank on threats and best practices.

The goal of this section is to ensure an environment where cybersecurity is embedded into enterprise risk management rather than treated as a siloed technical function.

SECTION II: Disclosure of the cybersecurity policy

This section mandates that institutions disseminate their cybersecurity policies internally and externally, ensuring all relevant parties are informed and aligned.
Core obligations set forward:

- The complete policy must be available to all employees, executives, and third-party service providers.
- A public summary must be published, describing the main objectives and principles without disclosing sensitive or confidential information.
- The content and format of disclosures must be clear, accessible, and appropriate to the audience's level of understanding.

The goal is to ensure awareness and promote uniform adoption of security standards across the entire ecosystem, including vendors and clients.

SECTION III: Plan of action and response to cybersecurity incidents

This section requires institutions to create an operational plan that ensures immediate response to and recovery from cybersecurity incidents.

The plan must:

- Define organizational structures, responsibilities, and escalation paths for incident prevention, detection, and resolution.
- Include procedures and technologies to record and analyze incidents, assess impacts, and implement corrective measures.
- Assign a specific director who will be solely responsible for cybersecurity, ensuring direct accountability to senior management and regulators.
  Provide annual reporting, detailing:
  - Effectiveness of the policy and control mechanisms.
  - Incidents recorded and lessons learned.
  - Results of business continuity and disaster recovery tests.
- The annual cybersecurity report must be submitted to the board or equivalent governing body by March 31 of the following year. Both the policy and the response plan must undergo an annual review and re-approval, ensuring continuous improvement and adaptation to evolving threats.

CHAPTER III

Contracting of data processing, data storage, and cloud computing services

This chapter governs how institutions outsource technology operations, both domestically and internationally. It emphasizes that while services can be outsourced, responsibility cannot be.

Major obligations:

- **Risk management integration:** Outsourced services must be incorporated into the institution's risk management and internal control frameworks.

- **Due diligence before contracting:** The provider's technical, legal, and operational capacity to safeguard confidentiality, integrity, and data recovery must be evaluated.

  Governance evaluation: Providers must be evaluated for:
  - Security and access control mechanisms.
  - Data segregation between clients.
  - Certifications and audit transparency.
  - Availability of independent audit reports and compliance attestations.

- **Contractual requirements:** Contracts must clearly specify responsibilities, including service-level agreements (SLAs), data access terms, and incident reporting obligations.

For foreign providers, additional controls apply:

- Ensure data location clarity, guaranteeing that the Central Bank can access the information even if the data is stored abroad.
- Confirm the existence of supervisory cooperation agreements between the Central Bank and the foreign jurisdiction's regulator.
- Require explicit contractual clauses for:
  - Data confidentiality and localization.
  - Termination and data return procedures.
  - Audit and inspection rights
  - Compliance with Brazilian law and regulator access.

This chapter establishes a legal and operational bridge between cybersecurity governance and third-party risk management, ensuring that outsourcing does not weaken regulatory oversight.

CHAPTER IV

General provisions

The fourth chapter reinforces the integration of cybersecurity and outsourcing controls into broader business continuity and governance frameworks.

Key requirements:

- Develop a crisis management framework with criteria defining crisis situations related to cyber incidents or service disruptions.
- Implement continuous monitoring mechanisms, including performance indicators, control metrics, and periodic internal audits.
- Ensure that the continuity of critical operations is maintained during and after security events.
- Require incident reporting to the Central Bank whenever an event has systemic impact or originates from a third-party provider.

The underlying principle is that institutions must be capable of maintaining essential services even amid severe disruptions or cyberattacks.

CHAPTER V

Final provisions

The final chapter provides procedural, administrative, and enforcement details.
It mandates that:

- Institutions must maintain all cybersecurity documentation, including policies, plans, board resolutions, reports, and outsourcing contracts, for a minimum of five years.
- The Central Bank retains authority to:
  - Specify additional technical requirements.
  - Impose corrective actions or deadlines.
  - Restrict or prohibit contracts that pose security risks.
  - Apply administrative sanctions for non-compliance.
- The resolution established July 1, 2021 is the effective date for full compliance.
- It revokes any previous norms that conflict with its provisions, consolidating all cybersecurity obligations for the above mentioned supervised entities under one regulatory standard.

How ManageEngine can help

Below are some of the main requirements from BACEN Resolution CMN 4,893/2021 and how ManageEngine can help achieve them.

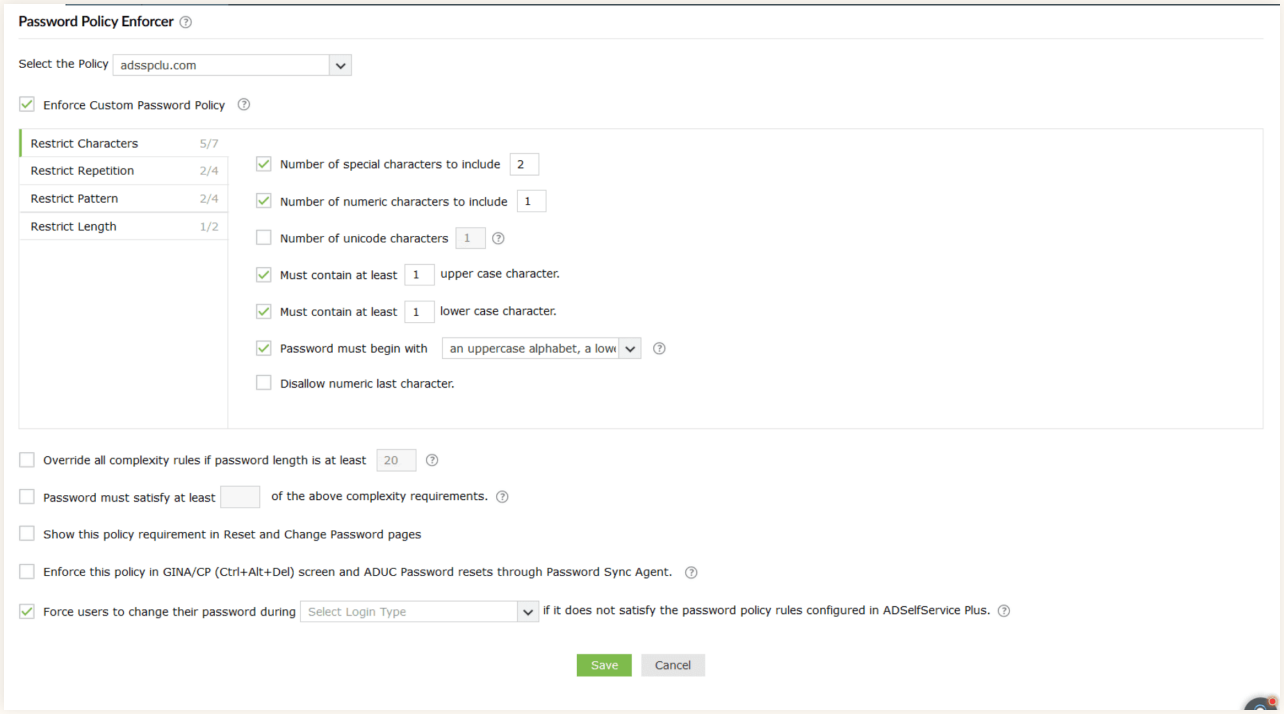
Chapter II, Section I – Art. 3 (II)

"Procedures and controls adopted to reduce the institution's vulnerability to incidents and to address other cyber security objectives."

AD360: Password Policy Enforcer

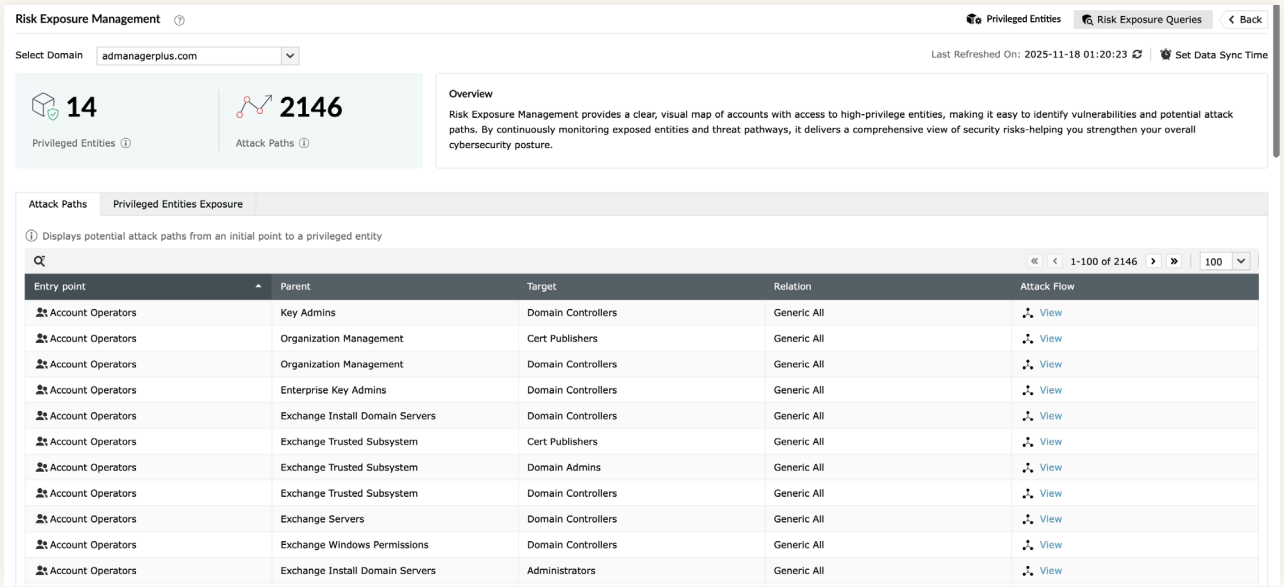
The Password Policy Enforcer strengthens one of the most critical control points in a financial institution: user credentials. It extends native Active Directory (AD) password policies with advanced controls such as banning weak and dictionary-based passwords, keyboard sequences, and predictable patterns, and it lets you enforce different password rules for different OUs and groups across AD, Microsoft 365, and Google Workspace.

By forcing users to choose strong, compliant passwords during creation and reset, the feature directly reduces vulnerability to credential stuffing, brute-force attacks, and account takeover while helping the institution meet cybersecurity objectives and regulatory expectations around password strength and identity protection.



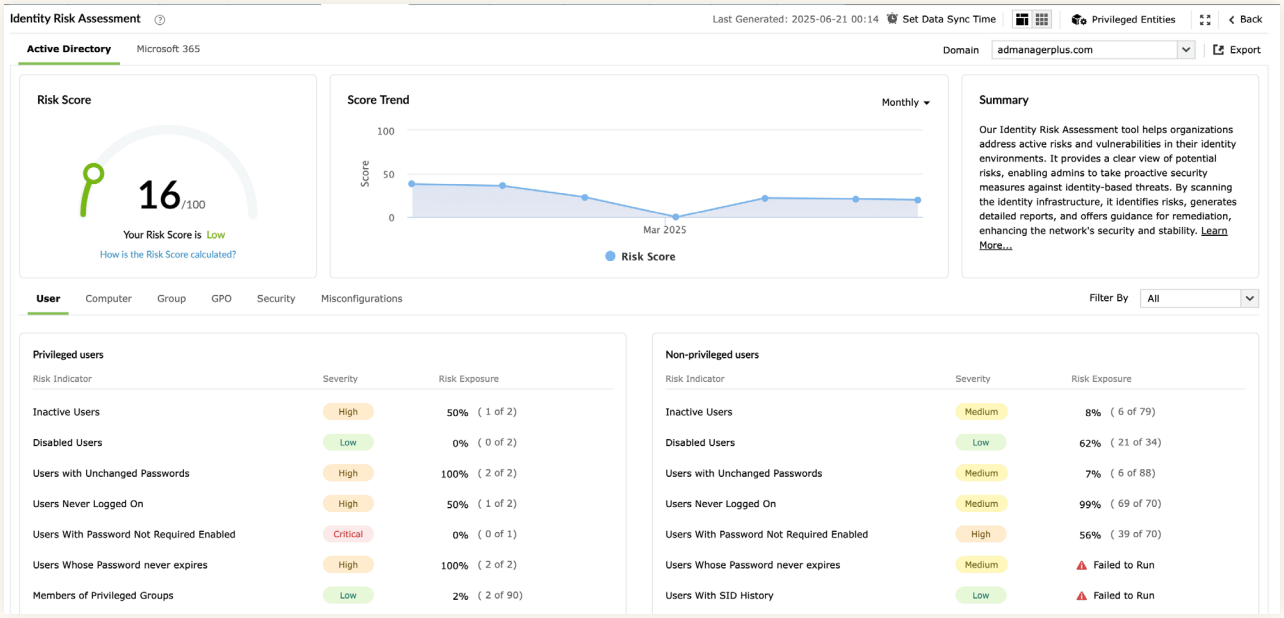
AD360: Risk exposure management

Risk exposure management in AD360 continuously analyzes AD to spot risky permissions and privileged entities, then maps how these could be chained into real-world attack paths toward high-privilege groups such as domain admins. Instead of static lists of group members, it gives security teams a visual representation of potential escalation routes and highlights high-risk objects so they can remediate misconfigurations, tighten privileges, and break attack paths in advance. This is a direct example of a proactive procedure and control that reduces vulnerability to incidents like lateral movement and privilege escalation, and it supports broader cybersecurity objectives such as least privilege and continuous risk reduction in identity infrastructure.



AD360: Identity risk assessment

Identity risk assessment in AD360 provides a structured way to identify, quantify, and track identity-related risks across both AD and Microsoft 365, following NIST SP 800-30 style guidance to compute likelihood and impact-based risk scores. The report highlights risky configurations, vulnerable accounts, and misaligned privileges, and determines an overall risk posture, so security teams can prioritize remediation where it will most reduce exposure. By embedding this kind of formal risk assessment into routine operations, the institution can demonstrate that it has defined procedures for discovering identity risks early, reducing the chance that these weaknesses are exploited and aligning with cybersecurity objectives around continuous risk management and governance.

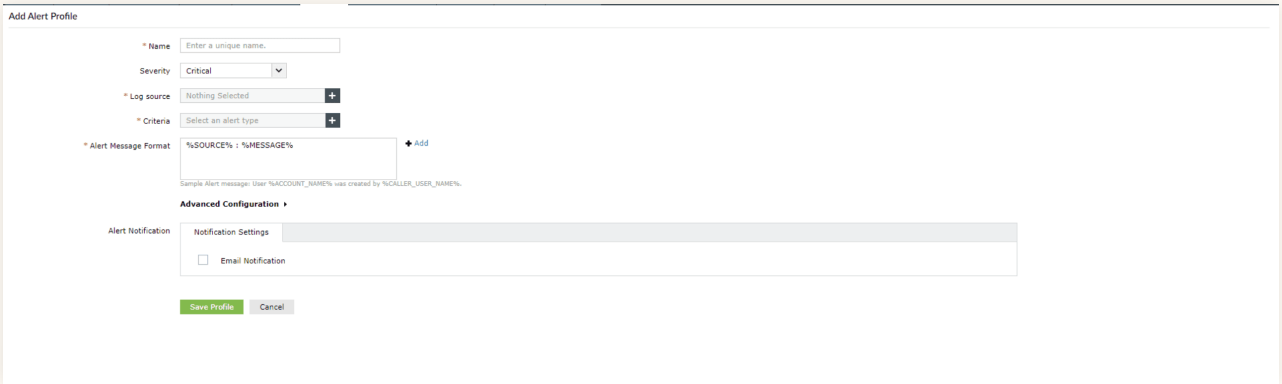


Log360: Real-time AD change auditing

Log360 acts as real-time AD change auditing and monitoring software that tracks and reports on changes to users, groups, OUs, GPOs, file servers, and permissions, issuing alerts on unwarranted or high-risk modifications. With hundreds of event-specific reports and live email alerts, it allows security and operations teams to quickly detect privilege escalation attempts, anomalous account changes, and insider activity that could precede or constitute an incident. This capability turns AD from an opaque control plane into a monitored and auditable environment, reducing the window of undetected malicious activity and supporting the clause by providing concrete procedures and controls for early detection, investigation, and response around identity-centric incidents.

Log360: Predefined alert profiles and out-of-the-box detections

The Log360 platform ships with hundreds of predefined alert criteria and over 1,000 out-of-the-box reports covering Windows, Unix, applications, network devices, and other infrastructure, along with real-time violation alerts and compliance-focused templates. These predefined alerts allow institutions to monitor for brute-force attempts, suspicious logons, privilege abuse, policy violations, and other threat patterns without having to design every rule from scratch, while reports support ongoing review and compliance. As a result, Log360 embeds a library of tested detection logic and monitoring procedures that immediately reduce the institution's vulnerability to common attack techniques and support cybersecurity objectives around continuous monitoring, incident detection, and compliance-driven oversight.



Chapter II, Section I – Art. 3 (III)

"The specific controls, including those directed at information traceability, aiming to ensure the security of sensitive information."

AD360: Mailbox and attachment search with alerts

AD360 enables deep search across multiple mailboxes and attachments with support for condition- and pattern-based filtering, scheduled scans, and alerting for compliance or suspicious activity. This makes it possible to trace exactly when sensitive emails or attachments are created, modified, or transported, providing a full audit trail of information flows. By automating these searches and alerts, AD360 strengthens oversight over sensitive communications and helps the institution maintain traceability and control over confidential data. As a result, it directly supports confidentiality and accountability controls required under data-security regulations.

Log360: Permission Analysis

Log360's permission analysis scans file servers to identify over-permissioned users, unnecessary permissions, broken inheritance, and over-exposed folders. It highlights where sensitive data may be accessible to more users than needed and helps security teams tighten access rights. This control ensures that only the right people have access to sensitive information, improving data governance and reducing risk of data leakage or unauthorized access—a key requirement for security and traceability of sensitive information.

Log360: File integrity monitoring (FIM)

Log360 offers real-time FIM: It tracks all modifications, creations, deletions or permission changes to critical files and folders, and generates alerts when unauthorized changes occur. This ensures that any tampering or unexpected changes are immediately visible, preserving the integrity of sensitive data and making all file activities traceable. As such, it provides a strong control to prevent inappropriate modifications, support forensic investigations, and maintain data integrity compliance.compliance-driven oversight.

Log360: Real-time file server auditing/file access auditing

The product continuously monitors and logs every file and folder access event (read, write, delete, rename, permission change, etc.) on servers or shared drives, capturing who accessed what, when, and from where. This produces detailed audit trails ideal for forensic analysis, ensuring full traceability of sensitive information usage and modifications. It supports compliance requirements by making file-level access and changes transparent and reviewable over time—essential for maintaining strict control over sensitive data.

Log360: User access auditing/data access and exfiltration monitoring

Log360 aggregates logs from multiple sources—servers, databases, file systems, applications—and applies real-time correlation, alerting, and behavior analytics to detect unauthorized access, data exfiltration attempts, anomalous activity, or privilege abuse. By maintaining comprehensive, timestamped records of who accessed which resource, when, and what they did, along with anomaly detection, Log360 supports strong traceability over information flows. This makes it an effective control for preventing unauthorized data exposure, enforcing least-privilege principles, and ensuring sensitive information is strictly monitored.

Chapter II, Section I – Art. 3 (IV)

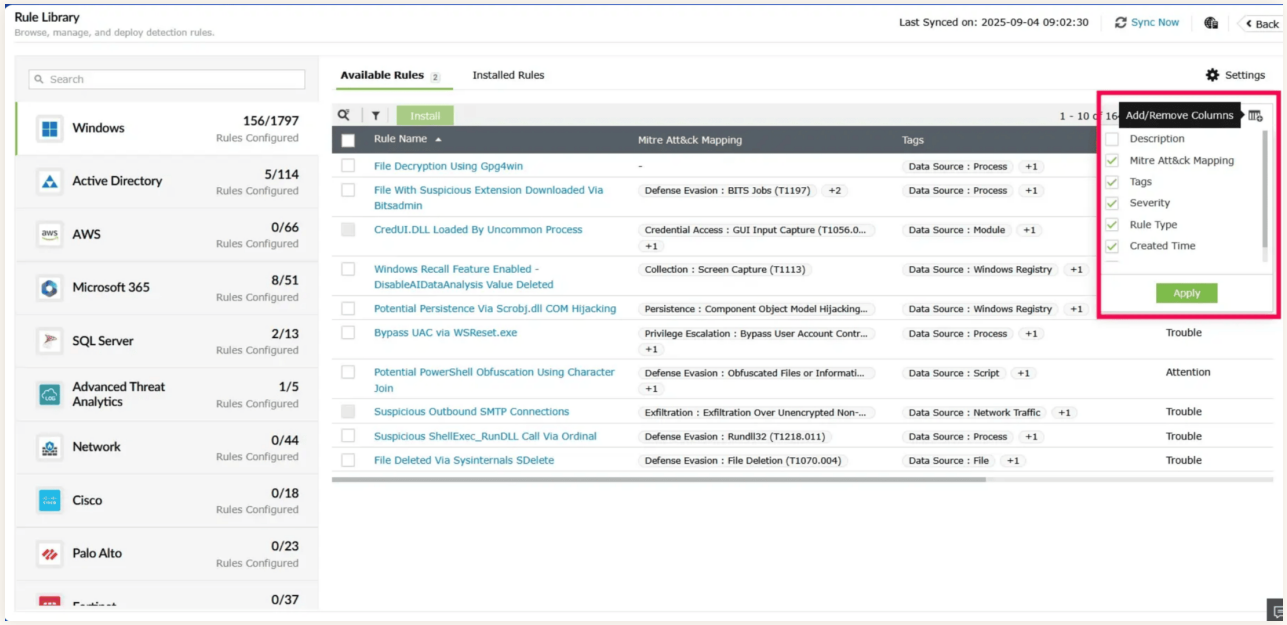
"The record of incidents relevant to the institution's activities, as well as the analysis of their cause and impact, and the control of their effects."

Log360: Centralized incident repository

Log360 acts as a unified SIEM backbone that consolidates logs and events from across AD, cloud services, servers, databases, applications, and network devices, effectively serving as a centralized incident repository. This centralized storage ensures that all relevant security events are captured, stored, and correlated over time, giving the institution a complete record of incidents. That archival trail supports thorough post-incident analysis, root-cause investigations, and compliance reporting. Moreover, having a single pane of visibility avoids silos and ensures no incident goes unlogged, which is essential for accountability and impact assessment.

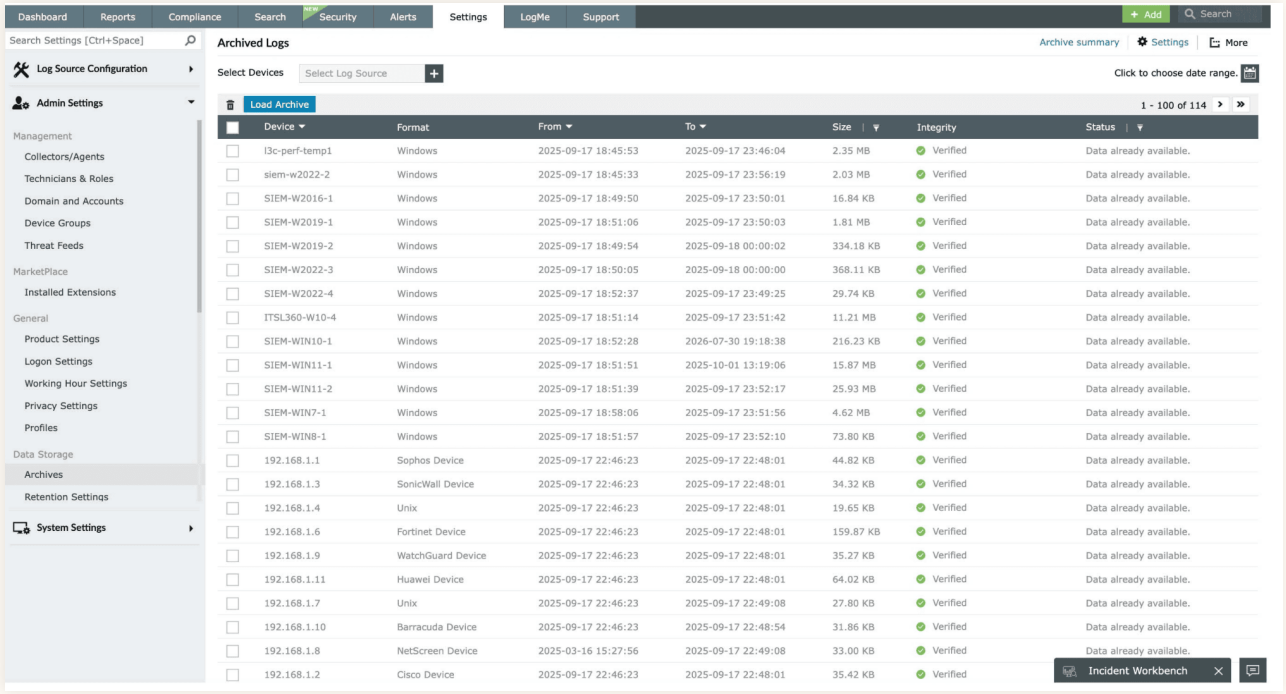
Log360: Correlation engine for detecting attack chains

Log360's real-time correlation engine links related events from multiple systems, such as AD changes, network activity, authentication patterns, and application logs, to detect coordinated or multi-stage attack behaviors that would otherwise appear as isolated alerts. Instead of investigating after the fact, the engine proactively identifies suspicious chains of actions that resemble lateral movement, privilege escalation, brute-force sequences, or data-access anomalies. By surfacing these correlated attack patterns early, Log360 strengthens incident detection and helps teams contain threats before they escalate. This proactive detection capability contributes directly to maintaining an accurate record of relevant incidents and supports faster control of their effects.



Log360: Event-forensics and incident timeline reconstruction

Log360, a core component of Log360, collects and archives logs from hundreds of sources—servers, network devices, applications, databases, etc.—and provides powerful search, parsing, and log-forensics capabilities. In the aftermath of a security event, it lets analysts reconstruct detailed incident timelines, who did what, when, and on which system, which is vital for understanding the chain of actions leading to the breach. By enabling forensic reconstruction, it supports accurate cause-and-impact analysis, helps quantify damage, and aids compliance and reporting obligations following an incident.

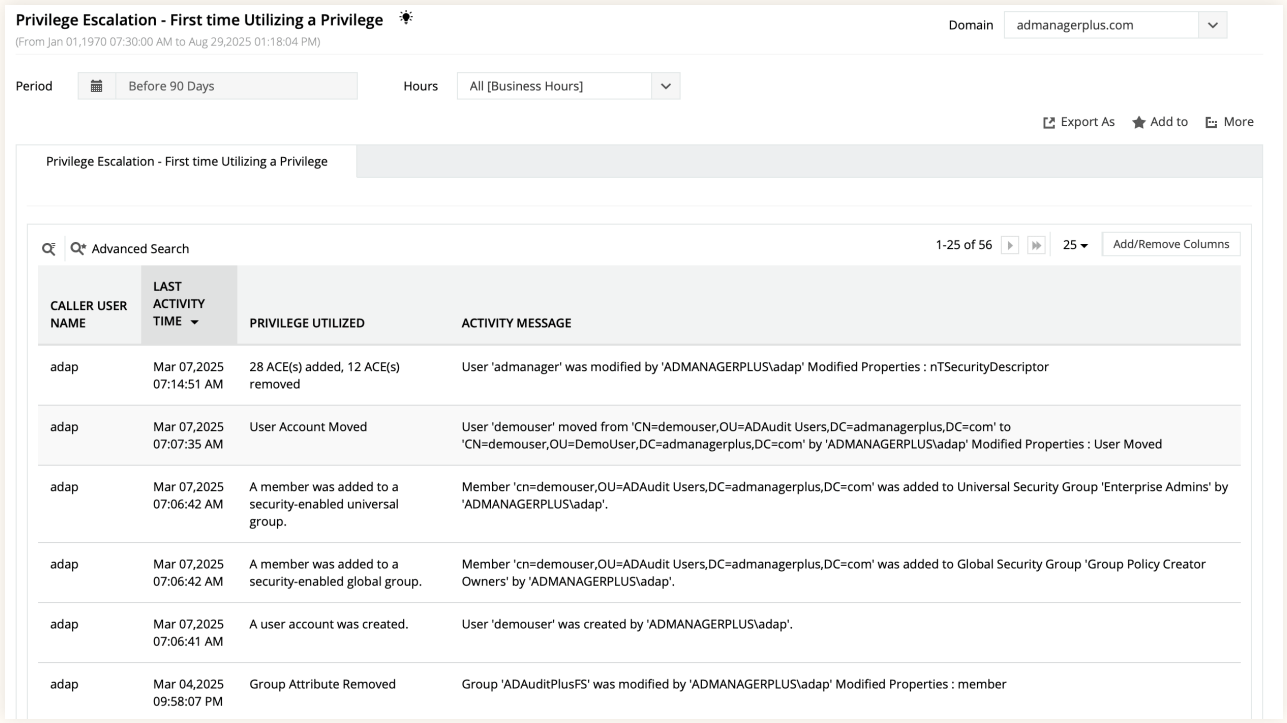


Log360: File auditing for ransomware impact and recovery scope assessment

Log360 monitors and logs all file server activities—read, write, delete, rename, permission changes, and more—providing a detailed audit trail of file-level operations. In case of a ransomware or data-tampering incident, these logs allow security and operations teams to assess exactly which files and folders were encrypted, modified, or deleted; by which user; and when. This visibility supports impact analysis and helps define recovery scope (what data needs to be restored, what must be quarantined, and what permissions need reviewing). As a result, Log360 gives you both a record of what happened and a roadmap for post-incident remediation, aligning directly with the clause's requirement for record, analysis, and control of incident effects.

Log360: Admin group tracking to catch unauthorized privilege escalation during incidents

The AD auditing component embedded in Log360 tracks changes to AD objects, group memberships, privileges, GPOs, and other critical configurations in real time. If an attacker tries to elevate privileges (e.g., by adding users to admin groups) during an incident, Log360 captures those changes instantly, with details on who made the change and when. This enables rapid detection of privilege misuse or escalation, a common tactic in complex attacks, and supports incident containment. The audit logs also serve as proof for post-incident root-cause analysis, aiding both technical remediation and regulatory/compliance reporting about the incident's nature and scope.

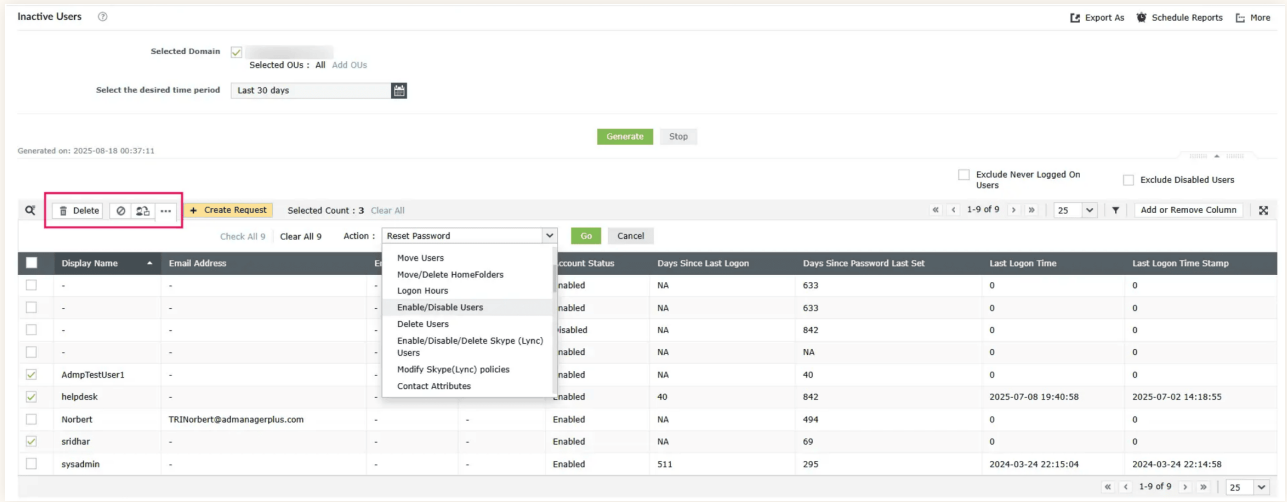


Chapter II, Section I – Art. 3 (Paragraph 1)

"When defining the cybersecurity objectives mentioned in item I, the institution must consider its capacity to prevent, detect, and reduce the vulnerability to cyber incidents."

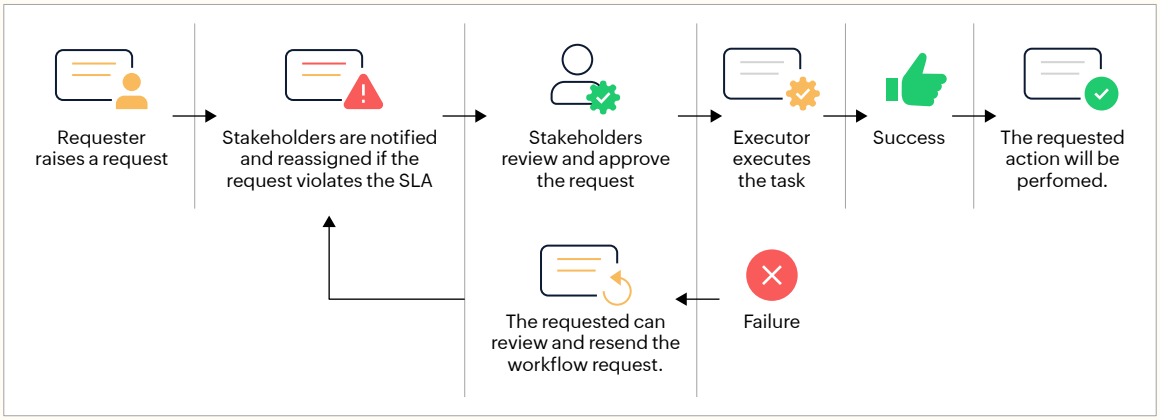
AD360: Automated account life cycle management

AD360 automates provisioning, deprovisioning, and cleanup of accounts across AD and Microsoft 365, eliminating dormant or orphaned accounts that attackers commonly target. Automated life cycle workflows ensure accounts are disabled or removed the moment an employee leaves or changes roles. By removing these hidden entry points, the institution enhances its prevention and detection capability and reduces systemic vulnerability in its identity infrastructure.



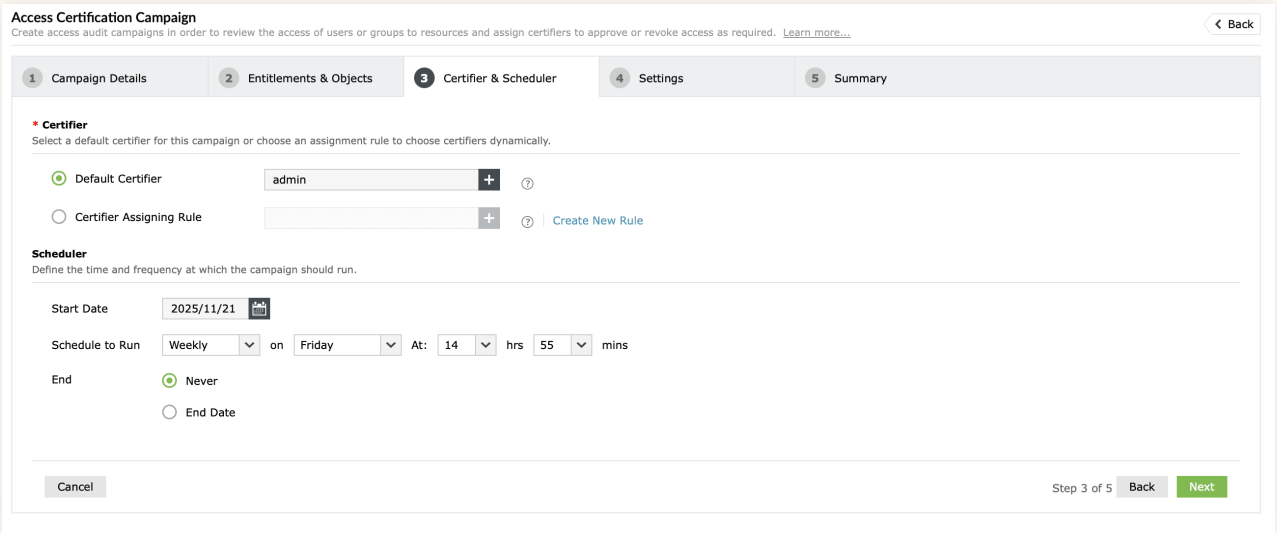
AD360: Multi-layer authorization workflows

Multi-layer authorization workflows require multiple levels of approval before executing sensitive administrative operations, such as privilege changes, group modifications, or provisioning actions. This prevents unauthorized or risky changes from slipping through and ensures oversight and accountability across the change process. By adding structured checkpoints, the institution lowers the likelihood of accidental or malicious configurations that could weaken its defenses, directly supporting prevention and vulnerability reduction.



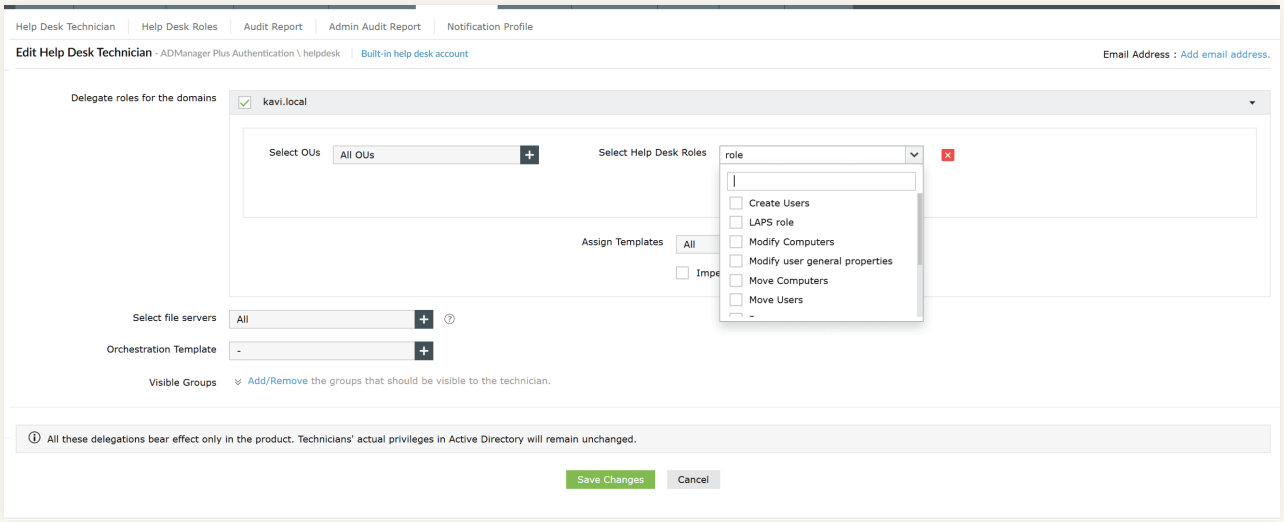
AD360: Access certification and periodic attestation

Access certification campaigns in AD360 automate the periodic review of user permissions, group memberships, and privileged access. By prompting managers or security owners to validate or revoke access rights regularly, the institution ensures excessive or stale access is systematically removed. This reduces privilege creep, minimizes the attack surface, and aligns cybersecurity objectives with proactive prevention and continuous vulnerability reduction.



AD360: Delegation management for admin rights

Delegation management provides fine-grained control over administrative permissions, allowing tasks to be delegated without granting full administrative privileges. This reduces the privilege-escalation attack surface, limits lateral movement opportunities, and ensures only appropriate individuals can perform sensitive operations. By tightening administrative boundaries, the institution strengthens both its preventative controls and its ability to reduce vulnerability to privilege-based cyber incidents.

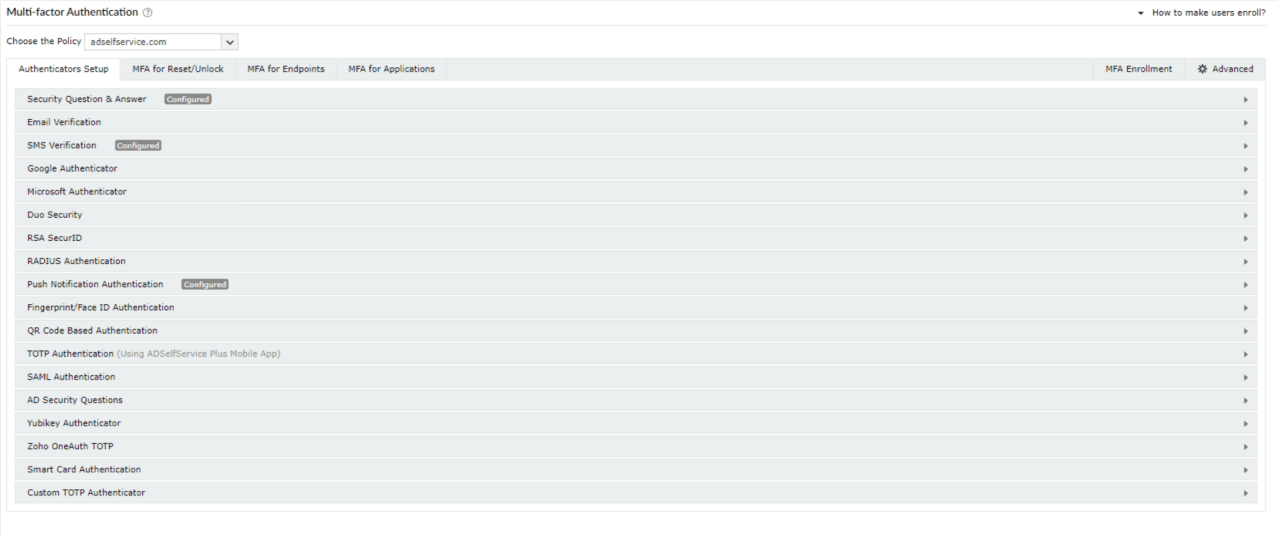


Chapter II, Section I – Art. 3 (Paragraph 2)

"The procedures and controls mentioned in item II must comprise, at least, authentication, cryptography, prevention and detection of intrusions, prevention of information leaking, performance of periodic tests and scanning to detect vulnerabilities, protection against malicious software, implementation of traceability mechanisms, control of access and segmentation of the computer network, and maintenance of data and information backups."

AD360: MFA enforcement for system, VPN, and application logins

AD360 strengthens authentication controls by enforcing multi-factor authentication (MFA) across system logins, VPN access, and critical business applications. MFA ensures that even if a password is phished, leaked, or compromised, unauthorized access attempts are blocked through an additional verification layer. This helps prevent intrusions stemming from credential abuse—one of the most common initial vectors in cyberattacks—and supports strong authentication and access control requirements under the clause. By securing login pathways across on-premises and cloud systems, the institution establishes foundational preventive control against identity-driven threats.



AD360: Complete AD backup for disaster recovery

AD360 creates comprehensive AD backups that preserve all directory data required for full environmental restoration. By maintaining secure, up-to-date copies of users, groups, OUs, DNS settings, GPOs, and configurations, the institution ensures resilience in the face of malicious attacks, misconfigurations, or corruption. This directly supports the clause's requirement for robust data and information backup maintenance.

AD360: Full and incremental backups for optimized recovery points

The platform supports a hybrid model of full and incremental backups, reducing storage overhead while maintaining detailed recovery points across time. Incremental backups capture only changes, allowing more frequent backup intervals without operational burden. This enables the institution to meet backup retention and recovery objectives while maintaining an efficient, continuous protection process.

AD360: Retention policies for backup optimization

Configurable retention policies automatically remove outdated or unnecessary backup versions to optimize storage consumption and maintain compliance with data retention requirements. These policies ensure that the institution maintains only relevant, secure, and compliant backup sets while continuously preserving the most recent, restorable versions. This aligns with the clause's mandate for structured backup maintenance and life cycle controls.

AD360: Granular restoration for fast, targeted recovery

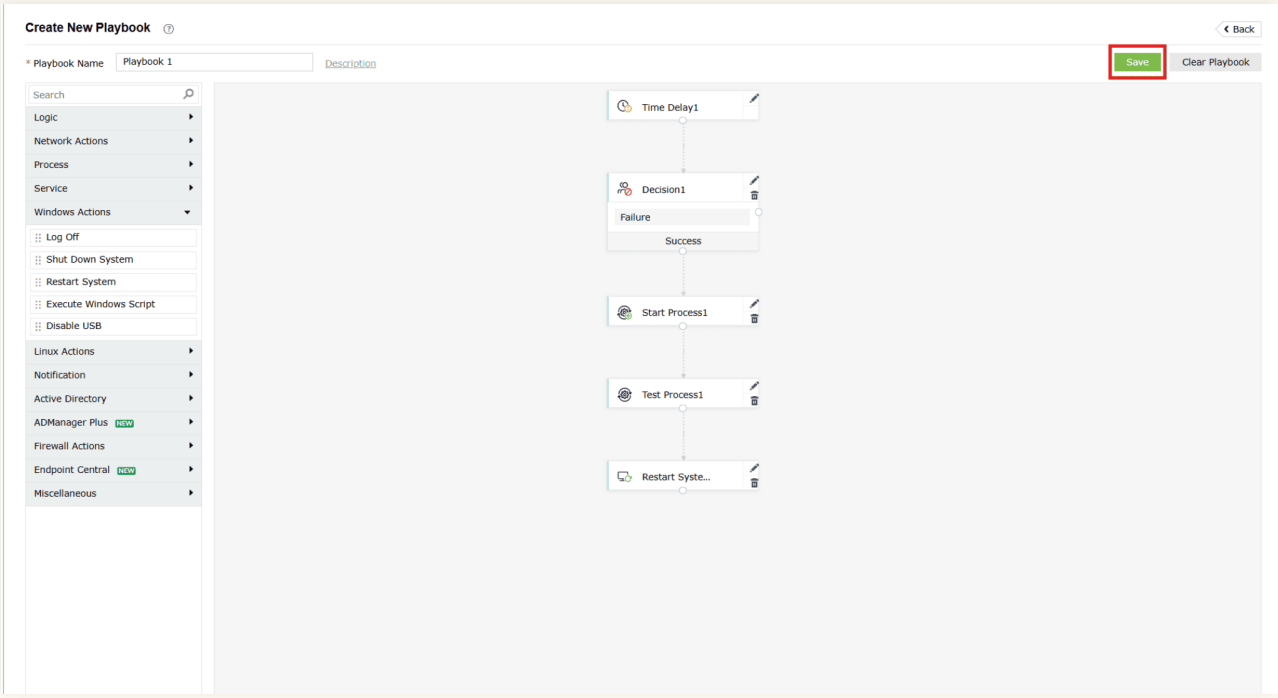
Granular restoration capabilities allow administrators to recover individual objects—such as users, groups, OUs, GPOs, or even specific attribute values—without performing a full AD rollback. This minimizes downtime and prevents over-correction during recovery, ensuring that only the intended portion of the directory is restored. Such precision supports rapid incident response, limits operational impact, and fulfills requirements for controlled, efficient restoration mechanisms within backup and recovery procedures.

Chapter II, Section III – Art. 6

"The institutions mentioned in art. 1 must establish a plan of action and response to incidents, aiming at the implementation of the cyber security policy."

Log360: Playbook automation for immediate response actions

Log360's playbook automation provides a structured, repeatable mechanism for responding to detected threats by triggering predefined actions the moment an alert is raised. These actions can include disabling user accounts, isolating compromised hosts, blocking IPs, enriching logs, or escalating incidents to security teams. By embedding automated response procedures into the platform, institutions ensure that critical steps in their action-and-response plan are executed consistently and without delay. This forms a core component of an actionable incident response plan, strengthening the operational side of the institution's cybersecurity policy.



Log360: Forensic reports with before/after object comparisons

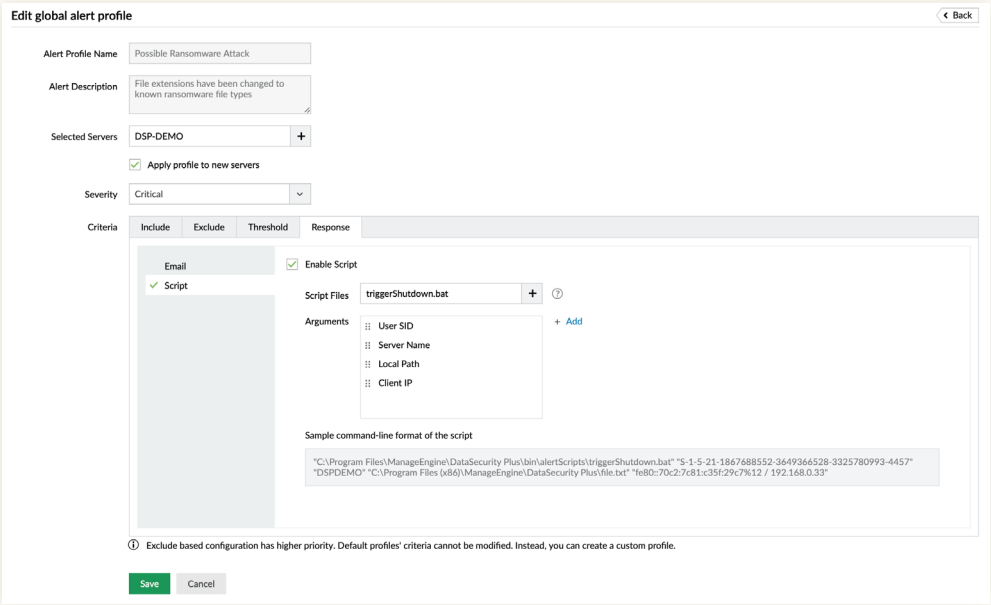
Log360 generates detailed forensic reports that show precise before-and-after snapshots of object changes, such as user attributes, group memberships, and permissions. This enables teams to reconstruct what changed, who made the change, and how the environment was affected—essential for scoping the impact of an incident. Such clarity supports structured investigation workflows within the institution's response plan and ensures each incident can be analyzed accurately in line with cybersecurity policy requirements. It also helps teams validate whether corrective actions restored systems to a secure baseline.

Log360: Alert profiles for systematic detection and incident categorization

Log360's alert profiles define standardized detection logic for brute-force attempts, privilege misuse, suspicious logons, lateral movement, malware behaviors, and other threat patterns. These profiles categorize incidents consistently, ensuring that each event is automatically mapped to its relevant incident type. This systematic classification supports the institution's incident response plan by ensuring alerts are triaged correctly, routed to the appropriate handlers, and escalated according to predefined procedures. As a result, detection becomes predictable, structured, and aligned with the broader cybersecurity policy.

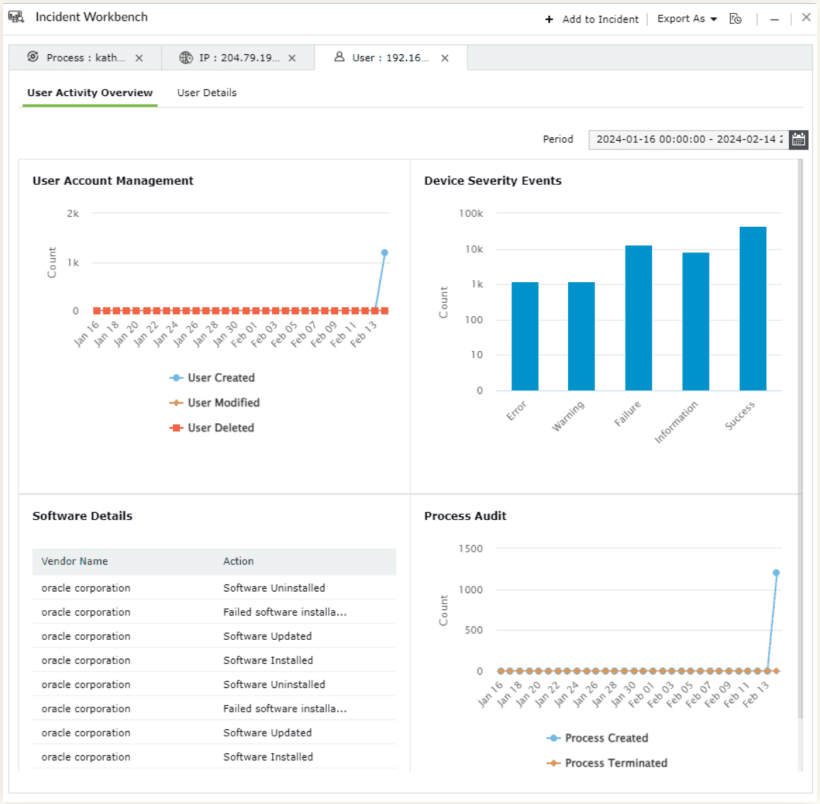
Log360: Ransomware isolation and automated containment

Log360 provides real-time ransomware detection and automated isolation of affected users or systems, preventing the spread of encryption activity across file servers. This rapid containment mechanism ensures that immediate protective actions—such as blocking access, quarantining processes, or halting further writes—are executed as soon as malicious behavior is detected. By operationalizing containment steps within the product, the institution builds tangible, enforceable response actions directly into its incident plan. These controls help ensure that ransomware events are mitigated swiftly and systematically in accordance with cybersecurity policy requirements.



Log360: Incident Workbench for centralized analysis and response coordination

Log360's Incident Workbench consolidates all contextual data relevant to an alert—logs, correlated events, user activity, threat indicators, asset details—into a single investigative view. This unified workspace helps responders analyze incidents quickly, understand the root cause and scope, and take guided remediation actions. The structured workflow supports the execution of the institution's incident response plan by ensuring all analysis, evidence collection, and actions are performed methodically and are documented. It reinforces the operational implementation of cybersecurity policies by ensuring incidents are handled consistently and with full context.



Chapter III – Art. 11

"The institutions mentioned in art. 11 must ensure that their policies, strategies, and structures for risk management established in regulation in force, specifically regarding to the criteria for decision on the outsourcing of services, include the contracting of relevant data processing, data storage, and cloud computing services, in the country or abroad."

Log360: Multi-platform monitoring of data handling in outsourced services

Log360 provides unified visibility into data processing activities across multiple cloud service platforms, allowing institutions to track how sensitive information is accessed, transmitted, and modified within outsourced environments. This monitoring capability helps validate that third-party providers handle institutional data in accordance with security, processing, and governance requirements defined in internal risk-management frameworks. By continuously observing data flows in contracted services—whether domestic or international—the institution strengthens its ability to evaluate outsourcing risk and ensure cloud vendors meet regulatory expectations.

Log360: Out-of-the-box reports for cloud provider compliance verification

The solution includes prebuilt compliance and security reports that help institutions assess whether cloud service providers adhere to required controls, such as access policies, configuration standards, and data-handling procedures. These reports simplify ongoing oversight and provide evidence-based validation of a vendor's compliance posture. This supports risk-based decision-making in outsourcing arrangements and ensures the institution can demonstrate proactive evaluation of cloud services, as mandated by the clause.

D360: Monitoring of Microsoft 365 data processing activities

AD360 offers detailed monitoring of user activity, data access, file changes, mailbox operations, and administrative actions within Microsoft 365. By tracking these events, the institution gains visibility into how its data is processed, stored, and secured across Microsoft's cloud infrastructure. This oversight is critical for evaluating the suitability of cloud providers and ensuring that outsourced data-handling activities align with internal security policies and regulatory requirements for third-party service assessments.

AD360: Cloud backup storage for data-recovery strategies

AD360 supports cloud-based backup storage options, enabling institutions to maintain secure, geographically distributed backup sets outside the primary environment. This ensures resiliency and recoverability, even when mission-critical directory data is stored or processed in outsourced cloud environments. By incorporating cloud backup capabilities, institutions strengthen their risk-management strategies for outsourced storage, satisfying regulatory expectations for continuity and safeguards in third-party services.

AD360: Multi-tenant support for managing multiple cloud providers

The platform's multi-tenant backup and recovery model allows institutions to manage and protect AD data across multiple cloud providers simultaneously. This capability supports diversified outsourcing strategies, enabling institutions to evaluate, compare, and operate across different domestic and international cloud vendors. By maintaining centralized control and visibility over outsourced environments, institutions improve governance, reduce risk concentration, and ensure that cloud service contracting aligns with the decision criteria required under the clause.

Conclusion

BACEN Resolution CMN 4,893/2021 sets a clear and uncompromising standard for how financial institutions must govern cybersecurity, manage identity-related risks, and ensure operational resilience across every layer of their digital infrastructure. Complying with this regulation is not just a legal obligation—it is fundamental to safeguarding customer trust, reducing exposure to breaches, strengthening incident readiness, and maintaining uninterrupted financial operations in an increasingly complex threat landscape. With ManageEngine's IAM and SIEM portfolio, institutions gain the visibility, control, and automation required to meet these expectations with confidence. From identity governance and privileged oversight to real-time threat detection, forensic auditing, and resilient recovery, ManageEngine equips financial organizations with an integrated security framework that aligns directly with BACEN's requirements and elevates their overall cybersecurity maturity.

Our Products

Log360 | ADManager Plus | ADAudit Plus | ADSelfService Plus

Exchange Reporter Plus | RecoveryManager Plus

About AD360

ManageEngine AD360 is a unified identity platform that seamlessly connects people, technology and experiences while giving enterprises full visibility and control over their identity infrastructure. It offers automated life cycle management; secure SSO; adaptive MFA; and risk-based governance, auditing, compliance and identity analytics—all from a single, intuitive console. With extensive out-of-the-box integrations and support for custom connectors, AD360 easily integrates into existing IT ecosystems to enhance security and streamline identity operations. Trusted by leading enterprises across healthcare, finance, education, and government, AD360 simplifies identity management, fortifies security and ensures compliance with evolving regulatory standards.

For more information, please visit www.manageengine.com/active-directory-360/.

$ Get Quote Download

Our Products

AD360 | ADAudit Plus | EventLog Analyzer | DataSecurity Plus

Exchange Reporter Plus | M365 Manager Plus

About Log360

Log360 is a unified SIEM solution with integrated DLP and CASB capabilities that detects, prioritizes, investigates and responds to security threats. Vigil IQ, the solution's TDIR module, combines threat intelligence, an analytical Incident Workbench, ML-based anomaly detection and rule-based attack detection techniques to detect sophisticated attacks, and it offers an incident management console for effectively remediating detected threats. Log360 provides holistic security visibility across on-premises, cloud and hybrid networks with its intuitive and advanced security analytics and monitoring capabilities.

For more information about Log360, visit manageengine.com/log-management/ and follow the LinkedIn page for regular updates.

$ Get Quote Download