ManageEngine

Meeting compliance and managing risks with identity-based GRC

www.manageengine.com/ad-manager ↗

What is GRC?

Governance, risk, and compliance (GRC) is a strategic framework that enables organizations to achieve business objectives while maintaining security, managing risks, and adhering to regulatory requirements

ManageEngine

The core functions of GRC

Governance:
Establishes policies, guidelines, and strategic direction for security and compliance

Risk management:
Identifies potential threats and implements proactive measures to mitigate risks

Compliance:
Ensures adherence to industry regulations and legal mandates

ManageEngine

GRC in ACTION

Implementation methods:
GRC is enforced through regular audits, policies, risk assessments, and reporting mechanisms

Why it matters:
Aligns IT with business goals while tightening security and meeting compliance

ManageEngine

KEY CHALLENGES when implementing GRC

Managing complex user access: Balancing security with efficiency while preventing excessive privileges

Meeting regulatory compliance requirements: Maintaining continuous audit trails and monitoring security controls

Role-based and least privilege access control: Ensuring role-based access management without loopholes

Identity life cycle management: Automating user provisioning, deprovisioning, and role modifications

Audit readiness and reporting: Simplifying compliance audits with structured and real-time reports

ManageEngine

THE GROWING THREAT LANDSCAPE:

WHY **GRC** IS **CRUCIAL**

Insider threats: Unauthorized access, privilege misuse, and data leaks

Regulatory penalties: Heavy fines for non-compliance with data security laws

Cybersecurity breaches: Increasing attacks targeting IAM vulnerabilities

Data governance risks: Unstructured and excessive access to sensitive information

Introducing

ManageEngine

ADManager Plus

Introducing **ADManager Plus**

A **powerful identity governance** and administration tool that helps you achieve GRC objectives

- Simplifies user provisioning, access control, and compliance
- Automates repetitive Active Directory (AD) tasks, like onboarding, offboarding, and group management
- Generates audit-ready reports for regulatory requirements
- Integrates seamlessly with AD, Microsoft 365, Google Workspace, and other enterprise applications

ManageEngine
ADManager Plus

Governance capabilities

Automated user provisioning and deprovisioning: Streamlines identity life cycle management, ensures appropriate access controls, and mitigates insider threats

Access certification campaigns: Enables automation of user access reviews across your organization; streamlines the process of approving or revoking access permissions, allowing you to perform periodic reviews and prevent privilege escalation

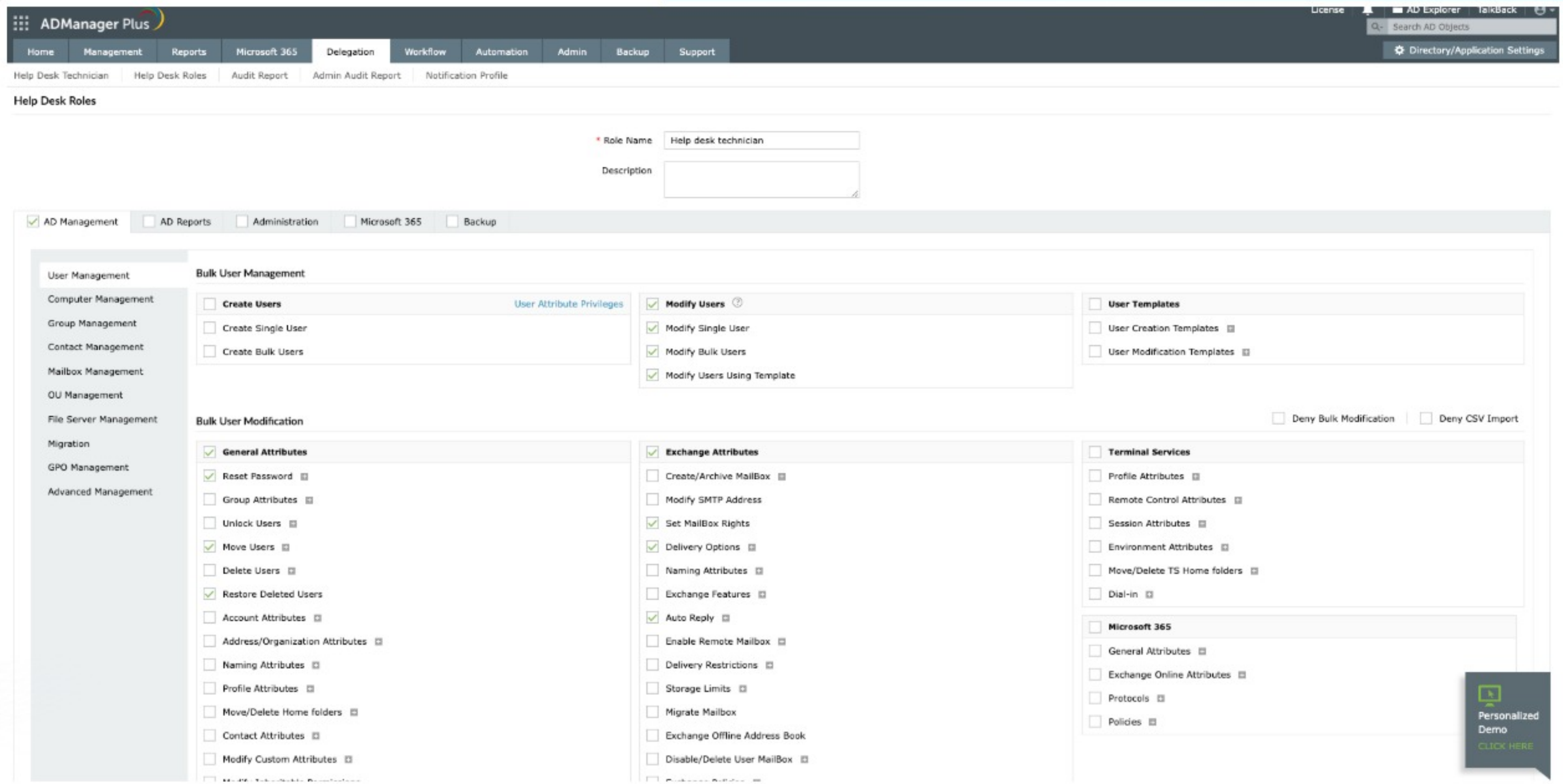
Permission-based delegation: Assigns granular permissions for administrative tasks based on job roles

Approval-based workflows: Multi-level approval processes for access requests and changes

Delegated administration: Secure delegation of IAM tasks without full administrator privileges

Streamline administration with permission-based delegation

- ADManager Plus enables granular delegation by allowing you to assign AD permissions for administrative tasks based on job functions
- Predefined roles limit overprivileged access for administrative functions



Help Desk Roles

* Role Name: Help desk technician

Description:

☑ AD Management | □ AD Reports | □ Administration | □ Microsoft 365 | □ Backup

User Management
Computer Management
Group Management
Contact Management
Mailbox Management
OU Management
File Server Management
Migration
GPO Management
Advanced Management

Bulk User Management

□ **Create Users** — User Attribute Privileges
□ Create Single User
□ Create Bulk Users

☑ **Modify Users**
☑ Modify Single User
☑ Modify Bulk Users
☑ Modify Users Using Template

□ **User Templates**
□ User Creation Templates
□ User Modification Templates

Bulk User Modification

□ Deny Bulk Modification | □ Deny CSV Import

☑ **General Attributes**
☑ Reset Password
□ Group Attributes
□ Unlock Users
☑ Move Users
□ Delete Users
☑ Restore Deleted Users
□ Account Attributes
□ Address/Organization Attributes
□ Naming Attributes
□ Profile Attributes
□ Move/Delete Home folders
□ Contact Attributes
□ Modify Custom Attributes
□ Modify Inheritable Permissions

☑ **Exchange Attributes**
□ Create/Archive MailBox
□ Modify SMTP Address
☑ Set MailBox Rights
☑ Delivery Options
□ Naming Attributes
□ Exchange Features
☑ Auto Reply
□ Enable Remote Mailbox
□ Delivery Restrictions
□ Storage Limits
□ Migrate Mailbox
□ Exchange Offline Address Book
□ Disable/Delete User MailBox
□ Exchange Policies

□ **Terminal Services**
□ Profile Attributes
□ Remote Control Attributes
□ Session Attributes
□ Environment Attributes
□ Move/Delete TS Home folders
□ Dial-in

□ **Microsoft 365**
□ General Attributes
□ Exchange Online Attributes
□ Protocols
□ Policies

USE CASES

Streamline administration with permission-based delegation

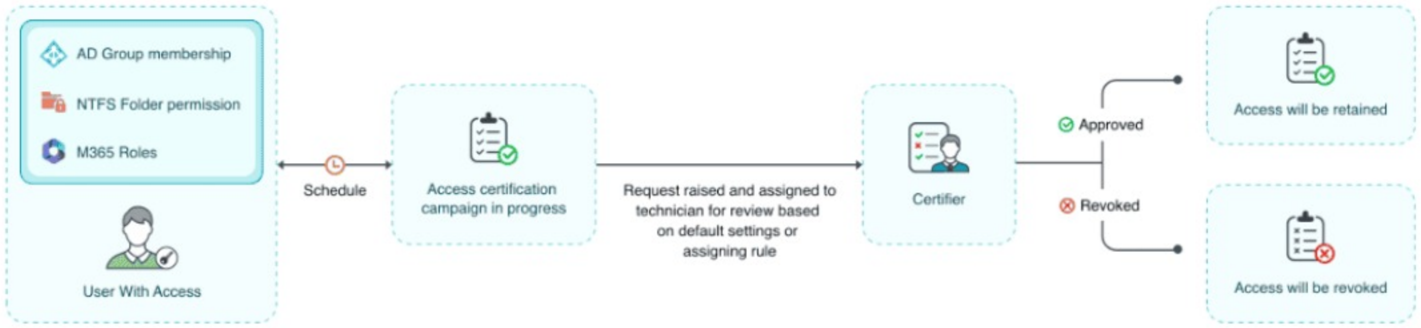
Help desk teams: Can reset passwords and unlock accounts but cannot create or delete users

HR teams: Can manage employee onboarding and offboarding without full AD administrative access

Branch admins: Can handle local user management without global AD administrative privileges

Automate access reviews to maintain continuous compliance

- Facilitates periodic access reviews to ensure users retain only necessary permissions
- Automated workflows allow managers to easily approve or revoke access, streamlining the process



USE CASES

Automate access reviews to maintain continuous compliance

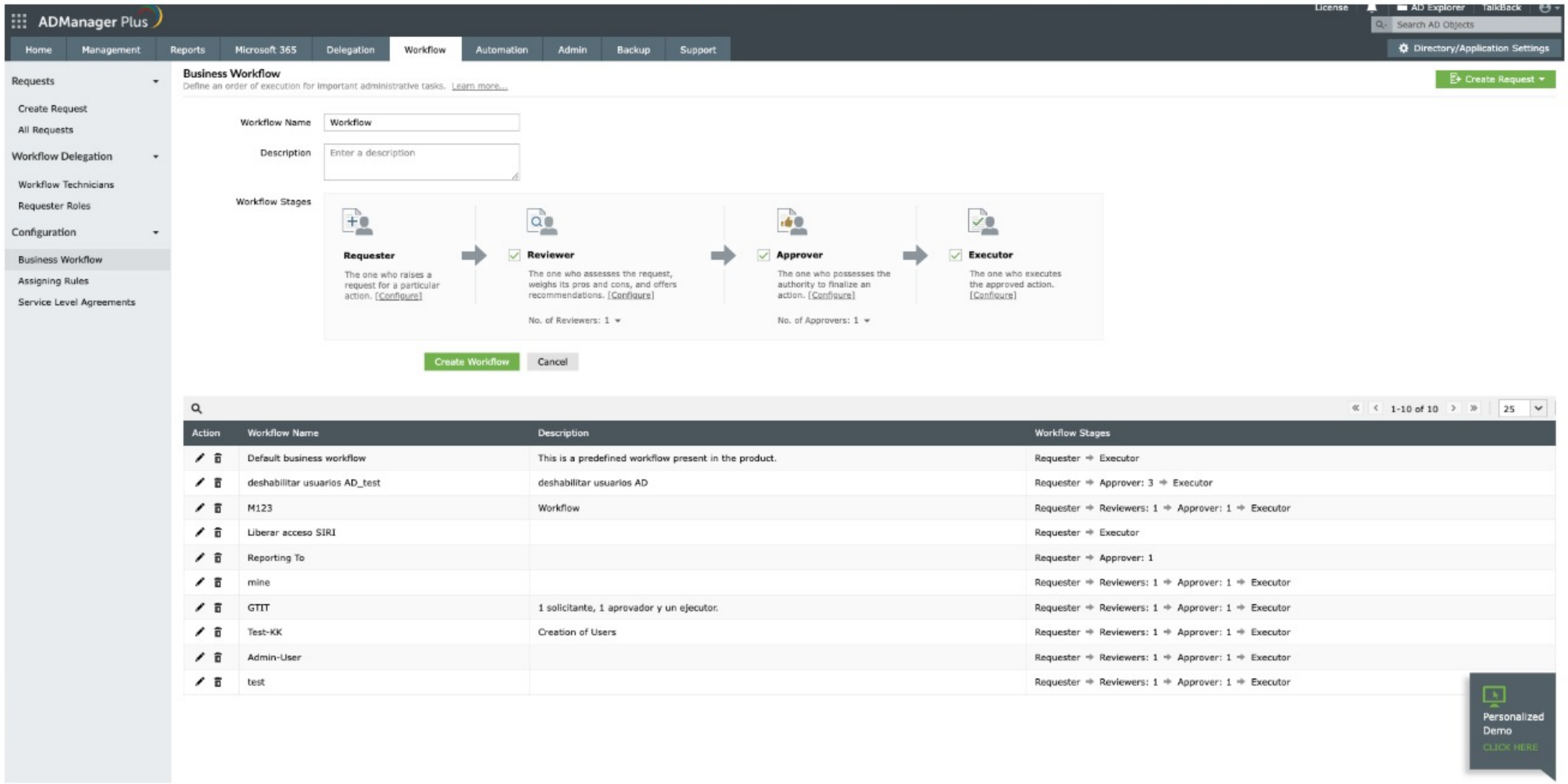
Quarterly SOX reviews: Department heads confirm financial system access for their teams

JML process: HR certifies that all terminations are promptly deprovisioned

Privileged access: IT leadership revalidates administrative rights every 90 days

Multi-level approvals for secure access control

- Configure approval workflows in ADManager Plus for AD changes (e.g., user creation or group modifications)
- Ensures compliance by requiring manager or IT team approval before granting access or making significant changes



Business Workflow

Define an order of execution for important administrative tasks. Learn more...

Workflow Name: Workflow

Description: Enter a description

Workflow Stages:

- **Requester** – The one who raises a request for a particular action. [Configure]
- ☑ **Reviewer** – The one who assesses the request, weighs its pros and cons, and offers recommendations. [Configure] No. of Reviewers: 1
- ☑ **Approver** – The one who possesses the authority to finalize an action. [Configure] No. of Approvers: 1
- ☑ **Executor** – The one who executes the approved action. [Configure]

1-10 of 10 | 25

Action	Workflow Name	Description	Workflow Stages
✎ 🗑	Default business workflow	This is a predefined workflow present in the product.	Requester → Executor
✎ 🗑	deshabilitar usuarios AD_test	deshabilitar usuarios AD	Requester → Approver: 3 → Executor
✎ 🗑	M123	Workflow	Requester → Reviewers: 1 → Approver: 1 → Executor
✎ 🗑	Liberar acceso SIRI		Requester → Executor
✎ 🗑	Reporting To		Requester → Approver: 1
✎ 🗑	mine		Requester → Reviewers: 1 → Approver: 1 → Executor
✎ 🗑	GTIT	1 solicitante, 1 aprovador y un ejecutor.	Requester → Reviewers: 1 → Approver: 1 → Executor
✎ 🗑	Test-KK	Creation of Users	Requester → Reviewers: 1 → Approver: 1 → Executor
✎ 🗑	Admin-User		Requester → Reviewers: 1 → Approver: 1 → Executor
✎ 🗑	test		Requester → Reviewers: 1 → Approver: 1 → Executor

USE CASES

Multi-level approvals for secure access control

Temporary access: Contractors should request access to finance groups (approved by the IT team and project lead)

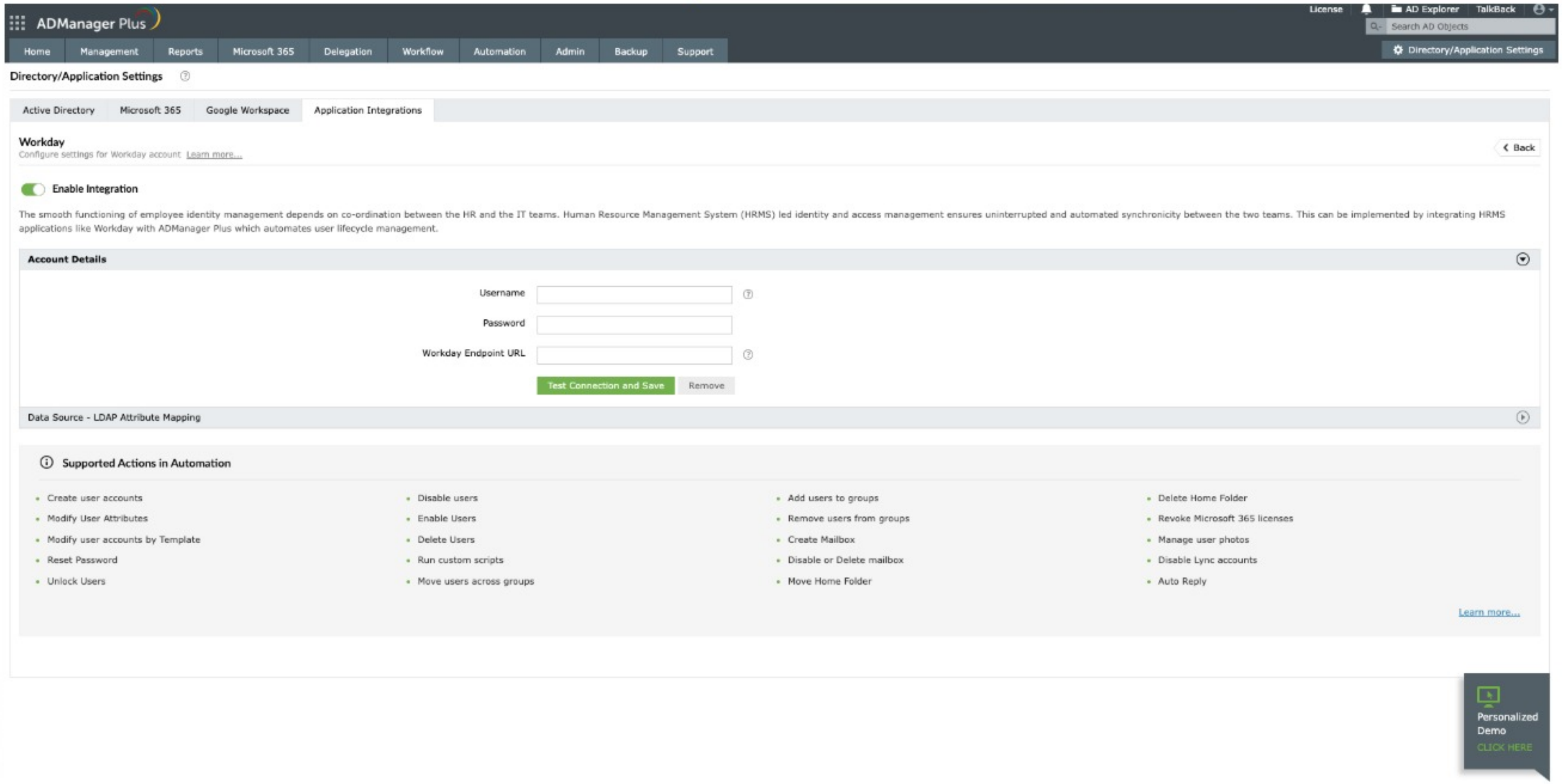
High-privilege requests: Granting Domain Admin rights requires a senior-level executive's approval

Group membership changes: Adding users to the Executives group triggers HR approval

End-to-end AD life cycle automation

- ADManager Plus automates user onboarding and offboarding via HR integrations (e.g., Workday or Zoho People)

- Instant deprovisioning reduces insider threats from orphaned accounts by promptly revoking access



Directory/Application Settings

Workday

Configure settings for Workday account Learn more...

Enable Integration

The smooth functioning of employee identity management depends on co-ordination between the HR and the IT teams. Human Resource Management System (HRMS) led identity and access management ensures uninterrupted and automated synchronicity between the two teams. This can be implemented by integrating HRMS applications like Workday with ADManager Plus which automates user lifecycle management.

Account Details

Username

Password

Workday Endpoint URL

Data Source - LDAP Attribute Mapping

Supported Actions in Automation

- Create user accounts
- Modify User Attributes
- Modify user accounts by Template
- Reset Password
- Unlock Users
- Disable users
- Enable Users
- Delete Users
- Run custom scripts
- Move users across groups
- Add users to groups
- Remove users from groups
- Create Mailbox
- Disable or Delete mailbox
- Move Home Folder
- Delete Home Folder
- Revoke Microsoft 365 licenses
- Manage user photos
- Disable Lync accounts
- Auto Reply

Learn more...

USE CASES

End-to-end AD life cycle automation

Onboarding: New hires automatically have an AD account and email address created and are added to department groups, all on day one

Offboarding: Disables accounts, revokes licenses, and removes group access upon termination or an employee leaving the company

Role changes: Automatically moves users between OUs or groups when department or job role changes occur

ManageEngine
ADManager Plus

Risk management

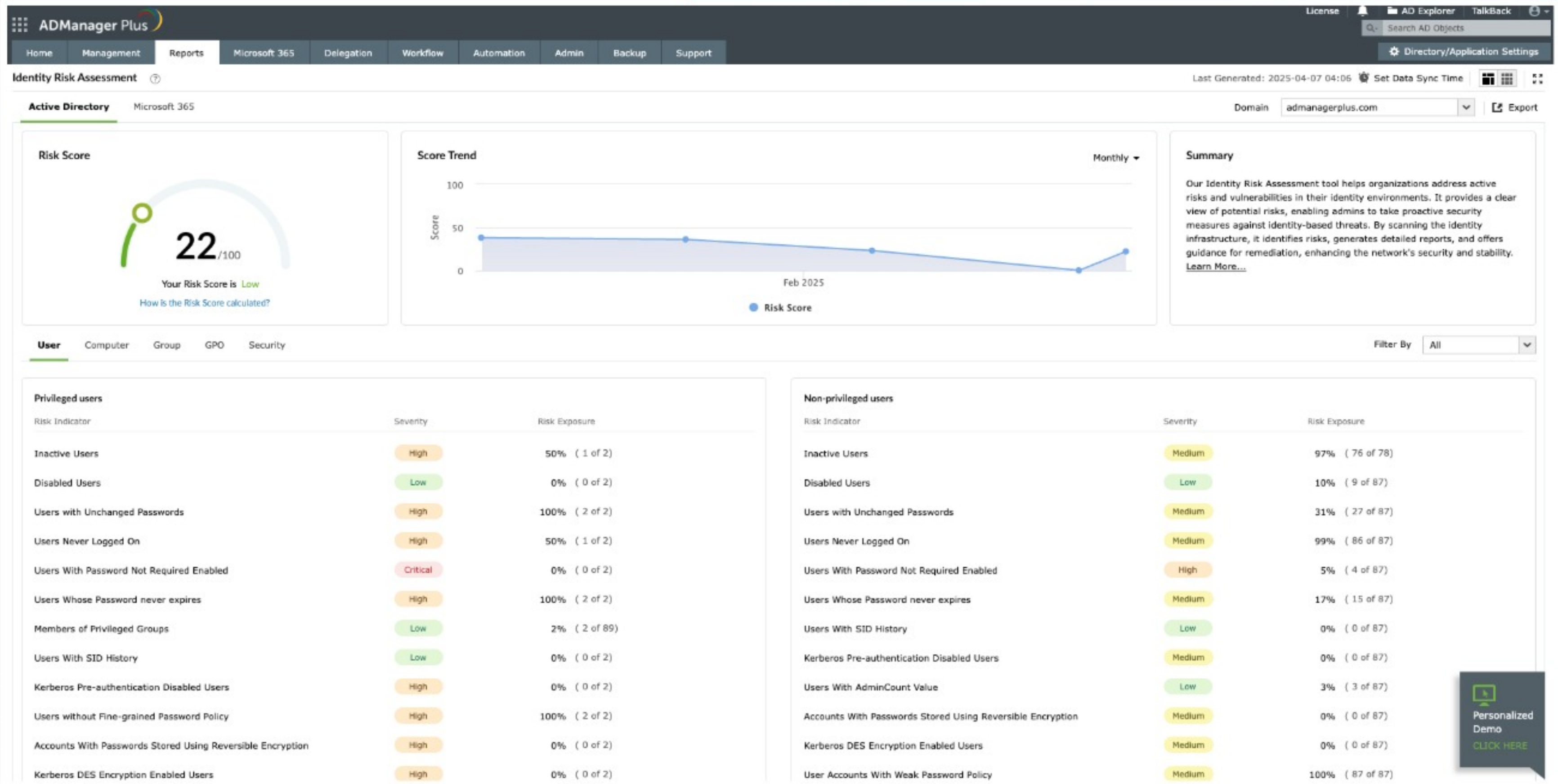
Identity risk assessment: Detects risks in AD and Microsoft 365 and views the overall risk score for your organization

On-the-fly actions and remediation measures: Take immediate actions to mitigate potential risk factors and view the recommended remediation measures for each identified risk

Risk exposure management: Visualize potential attack paths and access permissions that a malicious actor could exploit to compromise privileged entities, then view the necessary remediation measures to prevent such attacks

Proactive risk detection in AD and Microsoft 365

- Scans AD and Microsoft 365 for vulnerabilities (e.g., stale accounts, excessive permissions, or weak passwords)
- Assigns an overall risk score to prioritize remediation and quantify organizational exposure to potential threats



Last Generated: 2025-04-07 04:06

Domain: admanagerplus.com

Your Risk Score is Low

How is the Risk Score calculated?

Summary

Our Identity Risk Assessment tool helps organizations address active risks and vulnerabilities in their identity environments. It provides a clear view of potential risks, enabling admins to take proactive security measures against identity-based threats. By scanning the identity infrastructure, it identifies risks, generates detailed reports, and offers guidance for remediation, enhancing the network's security and stability. Learn More...

Filter By: All

Privileged users

Risk Indicator	Severity	Risk Exposure
Inactive Users	High	50% (1 of 2)
Disabled Users	Low	0% (0 of 2)
Users with Unchanged Passwords	High	100% (2 of 2)
Users Never Logged On	High	50% (1 of 2)
Users With Password Not Required Enabled	Critical	0% (0 of 2)
Users Whose Password never expires	High	100% (2 of 2)
Members of Privileged Groups	Low	2% (2 of 89)
Users With SID History	Low	0% (0 of 2)
Kerberos Pre-authentication Disabled Users	High	0% (0 of 2)
Users without Fine-grained Password Policy	High	100% (2 of 2)
Accounts With Passwords Stored Using Reversible Encryption	High	0% (0 of 2)
Kerberos DES Encryption Enabled Users	High	0% (0 of 2)

Non-privileged users

Risk Indicator	Severity	Risk Exposure
Inactive Users	Medium	97% (76 of 78)
Disabled Users	Low	10% (9 of 87)
Users with Unchanged Passwords	Medium	31% (27 of 87)
Users Never Logged On	Medium	99% (86 of 87)
Users With Password Not Required Enabled	High	5% (4 of 87)
Users Whose Password never expires	Medium	17% (15 of 87)
Users With SID History	Low	0% (0 of 87)
Kerberos Pre-authentication Disabled Users	Medium	0% (0 of 87)
Users With AdminCount Value	Low	3% (3 of 87)
Accounts With Passwords Stored Using Reversible Encryption	Medium	0% (0 of 87)
Kerberos DES Encryption Enabled Users	Medium	0% (0 of 87)
User Accounts With Weak Password Policy	Medium	100% (87 of 87)

USE CASES

Proactive risk detection in AD and Microsoft 365

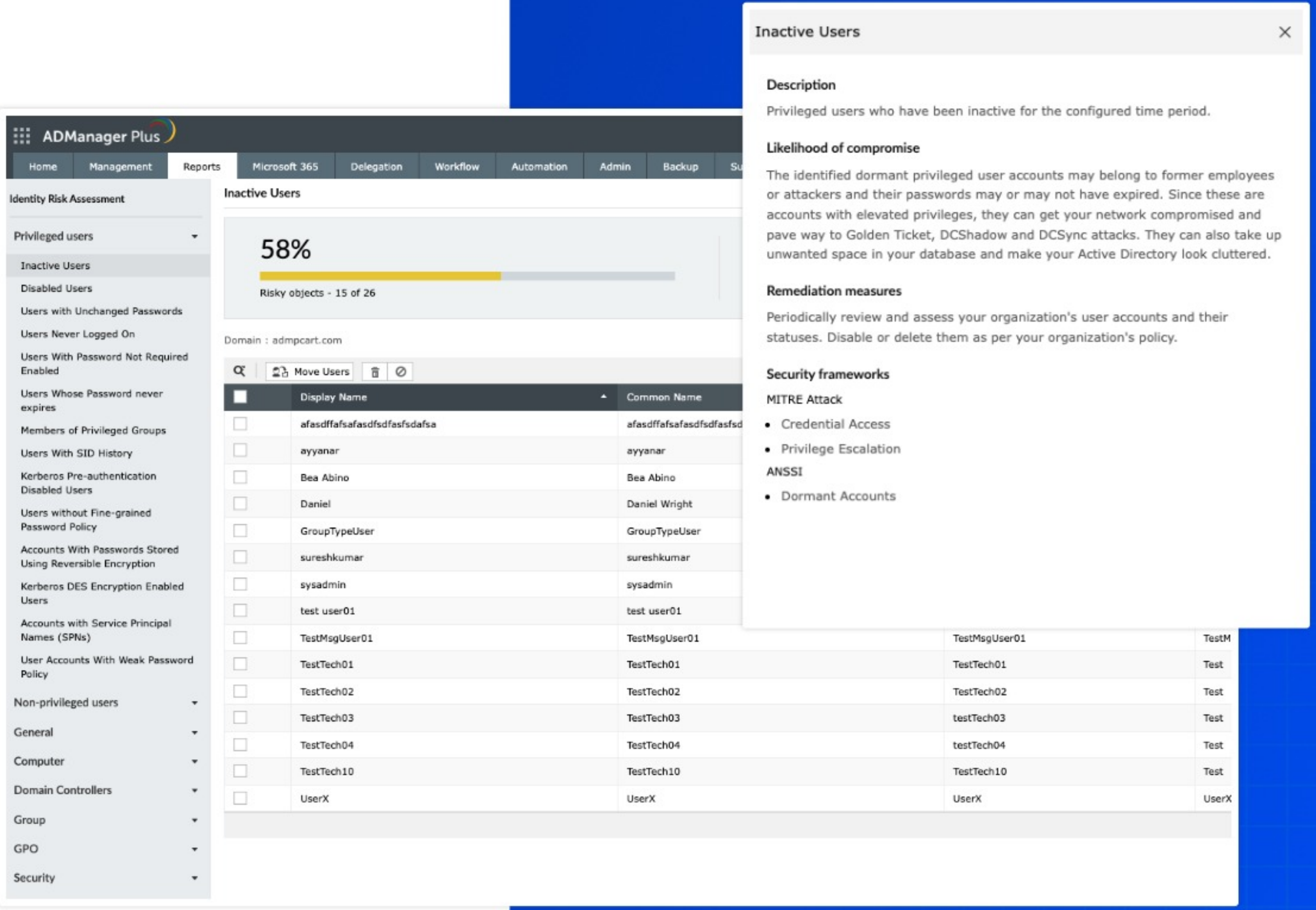
Stale accounts: Detect inactive users with active access, flagging potential insider threat risks

Compliance audits: Identify non-compliant accounts (e.g., users with never-expiring passwords) that could lead to audit failure

Mergers and acquisitions: Assess inherited AD risks during the integration of new systems and users

On-the-fly risk mitigation

- Immediate mitigation: Resolve risks directly from the dashboard (e.g., disable stale accounts or move groups)
- Guided remediation: View step-by-step recommendations for each risk (e.g., Periodically review and assess your organization's user accounts and their statuses. Disable or delete them as per your organization's policy.)


ADManager Plus
Home
Management
Reports
Microsoft 365
Delegation
Workflow
Automation
Admin
Backup
Su
Identity Risk Assessment
Privileged users
Inactive Users
Disabled Users
Users with Unchanged Passwords
Users Never Logged On
Users With Password Not Required Enabled
Users Whose Password never expires
Members of Privileged Groups
Users With SID History
Kerberos Pre-authentication Disabled Users
Users without Fine-grained Password Policy
Accounts With Passwords Stored Using Reversible Encryption
Kerberos DES Encryption Enabled Users
Accounts with Service Principal Names (SPNs)
User Accounts With Weak Password Policy
Non-privileged users
General
Computer
Domain Controllers
Group
GPO
Security
Move Users

Inactive Users

58%

Risky objects - 15 of 26

Domain : admpcart.com

□	Display Name	Common Name		
□	afasdffafsafasdfsdfasfsdafsa	afasdffafsafasdfsdfasfsd		
□	ayyanar	ayyanar		
□	Bea Abino	Bea Abino		
□	Daniel	Daniel Wright		
□	GroupTypeUser	GroupTypeUser		
□	sureshkumar	sureshkumar		
□	sysadmin	sysadmin		
□	test user01	test user01		
□	TestMsgUser01	TestMsgUser01	TestMsgUser01	TestM
□	TestTech01	TestTech01	TestTech01	Test
□	TestTech02	TestTech02	TestTech02	Test
□	TestTech03	TestTech03	testTech03	Test
□	TestTech04	TestTech04	testTech04	Test
□	TestTech10	TestTech10	TestTech10	Test
□	UserX	UserX	UserX	UserX

Inactive Users ×

Description

Privileged users who have been inactive for the configured time period.

Likelihood of compromise

The identified dormant privileged user accounts may belong to former employees or attackers and their passwords may or may not have expired. Since these are accounts with elevated privileges, they can get your network compromised and pave way to Golden Ticket, DCShadow and DCSync attacks. They can also take up unwanted space in your database and make your Active Directory look cluttered.

Remediation measures

Periodically review and assess your organization's user accounts and their statuses. Disable or delete them as per your organization's policy.

Security frameworks

MITRE Attack

- Credential Access
- Privilege Escalation

ANSSI

- Dormant Accounts

USE CASES

On-the-fly risk mitigation

Help desk: Quickly disable compromised accounts during a breach with one-click actions

Auditors: Document corrective actions for compliance reports with the remediation measures capability

ManageEngine
ADManager Plus

Compliance and audit

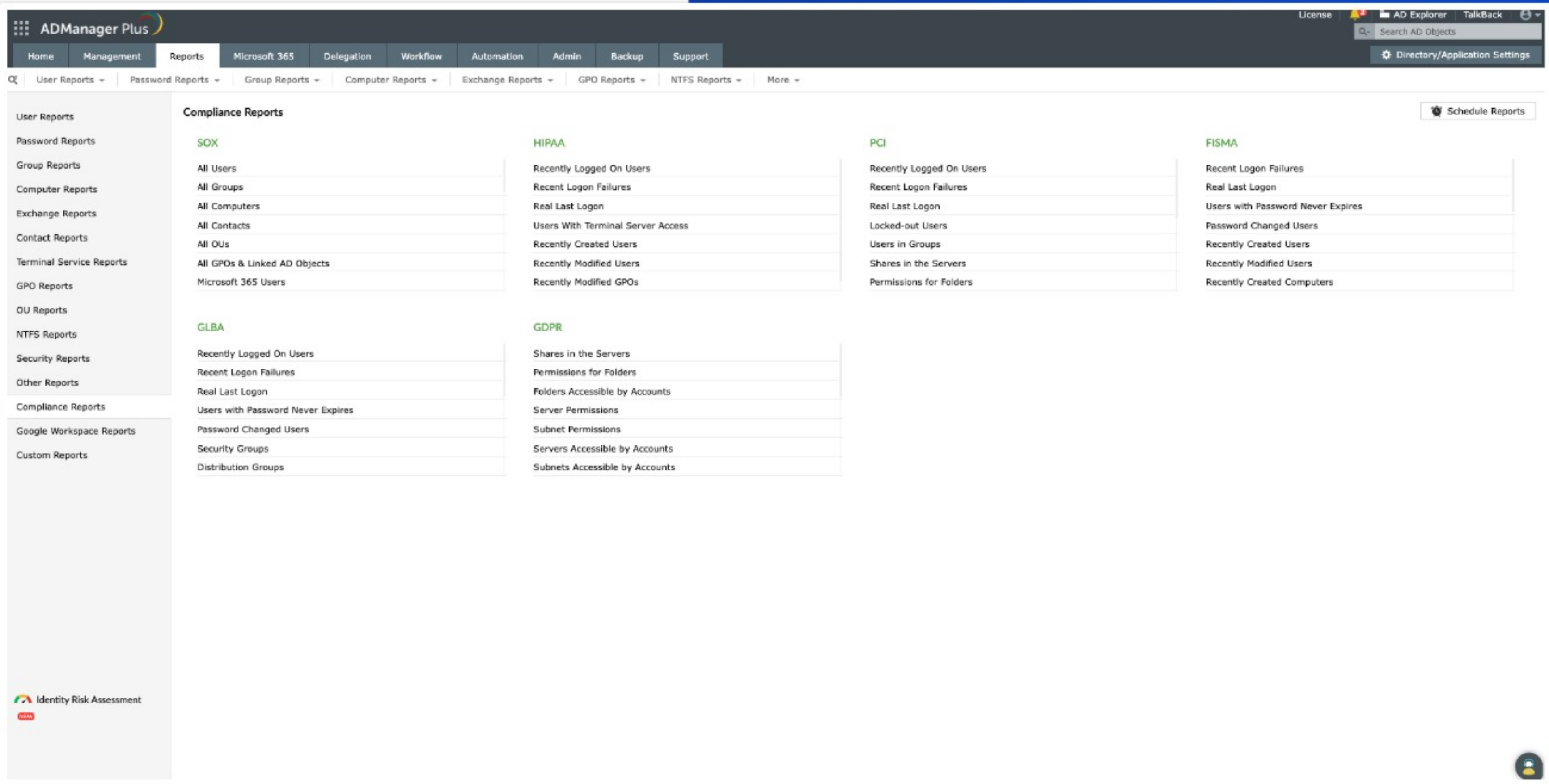
Prebuilt compliance reports: Generate reports for the GDPR, SOX, HIPAA, the PCI DSS, and other regulatory frameworks

Audit tracking: Logs all user and administrative activities for accountability and security

Automated access certifications: Conducts periodic access reviews to maintain continuous compliance

One-click compliance reports for the GDPR, HIPAA, SOX, and more

- ❖ Ready-to-use reports for major regulations (e.g., the GDPR, SOX, HIPAA, and the PCI DSS)
- ❖ Maps AD and Microsoft 365 data to compliance requirements (e.g., user access logs and permission changes)



Compliance Reports

SOX

- All Users
- All Groups
- All Computers
- All Contacts
- All OUs
- All GPOs & Linked AD Objects
- Microsoft 365 Users

HIPAA

- Recently Logged On Users
- Recent Logon Failures
- Real Last Logon
- Users With Terminal Server Access
- Recently Created Users
- Recently Modified Users
- Recently Modified GPOs

PCI

- Recently Logged On Users
- Recent Logon Failures
- Real Last Logon
- Locked-out Users
- Users in Groups
- Shares in the Servers
- Permissions for Folders

FISMA

- Recent Logon Failures
- Real Last Logon
- Users with Password Never Expires
- Password Changed Users
- Recently Created Users
- Recently Modified Users
- Recently Created Computers

GLBA

- Recently Logged On Users
- Recent Logon Failures
- Real Last Logon
- Users with Password Never Expires
- Password Changed Users
- Security Groups
- Distribution Groups

GDPR

- Shares in the Servers
- Permissions for Folders
- Folders Accessible by Accounts
- Server Permissions
- Subnet Permissions
- Servers Accessible by Accounts
- Subnets Accessible by Accounts

USE CASES

One-click compliance reports for the GDPR, HIPAA, SOX, and more

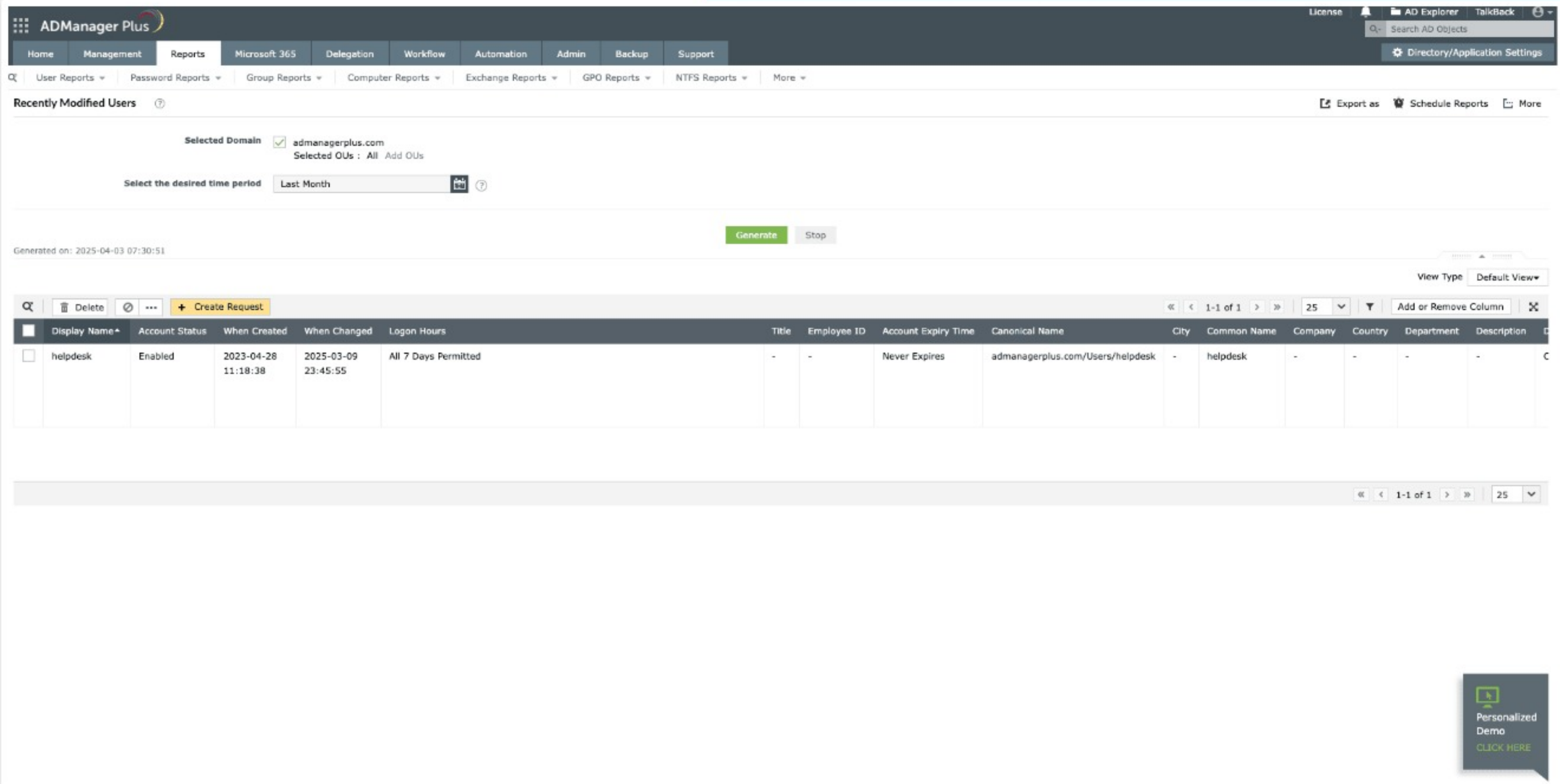
SOX audit: Easily prove that only authorized users have access to financial systems

HIPAA compliance: Quickly identify all users with access to the Patient Records group

GDPR cleanup: Find and remove inactive users who may still hold personally identifiable information

Tamper-proof audit logs for complete accountability

- Logs all AD and Microsoft 365 activities (e.g., password resets, group membership changes and account deletions)
- Receive tamper-proof records that are crucial for forensic investigations and demonstrating compliance



Recently Modified Users

Selected Domain ☑ admanagerplus.com
Selected OUs : All Add OUs

Select the desired time period: Last Month

Generated on: 2025-04-03 07:30:51

Display Name	Account Status	When Created	When Changed	Logon Hours	Title	Employee ID	Account Expiry Time	Canonical Name	City	Common Name	Company	Country	Department	Description
helpdesk	Enabled	2023-04-28 11:18:38	2025-03-09 23:45:55	All 7 Days Permitted	-	-	Never Expires	admanagerplus.com/Users/helpdesk	-	helpdesk	-	-	-	-

ManageEngine
ADManager Plus

USE CASES

Tamper-proof audit logs for complete accountability

Insider threat investigation: Trace who granted administrative rights to a terminated employee

Compliance proof: Demonstrate that no unauthorized changes occurred during an audit period

Troubleshooting: Identify accidental permission changes that may be breaking applications

GRC IN ACTION:

Real-world use cases and benefits

Financial sector: Ensures SOX compliance with automated audits and effective delegated administration

Healthcare: Meets HIPAA regulations by tracking user access and maintaining detailed audit logs

Education: Automates student and staff onboarding and offboarding with appropriate access assignments

Enterprises: Implements least-privilege access through secure delegation to reduce security risks and unauthorized access

ManageEngine
ADManager Plus

Next steps:

Turn GRC vision into action

Try ADManager Plus: Free, 30-day trial available

Book a consultation: Schedule a personalized demo to address your IAM and compliance challenges with experts

Stay compliant and secure: Implement best practices for GRC

ManageEngine
ADManager Plus

Secure your organization with GRC and ADManager Plus

Take control of your identity governance today with robust GRC strategies

www.manageengine.com/ad-manager