63-51 / Emerging Technologies

May 2025

Dylan Sanderson, Maxime Bossi, Nadja Lötscher, Johann von Roten

Introduction

PAM solutions

Goal

To protect privileged accounts from misuse and compromise by ensuring strict control, complete visibility, and traceability of access to critical systems within an organization.

- Reduce the attack surface from internal and external cyber threats
- Ensure compliance with standards (ISO 27001, GDPR, PCI DSS, etc.)
- Minimize the impact of breaches by restricting access

Target

All privileged accounts that could cause significant harm if misused or compromised:

- System and network administrators
- Root accounts (Linux/Unix)
- Critical service accounts
- DevOps accounts (CI/CD pipelines, APIs, cloud infrastructure)
- Temporary privileged users (e.g., consultants)

Scope

Covers the full lifecycle of privileged access, including:

- Credential management: storing, encrypting, and rotating passwords
- Session recording and monitoring
- Just-in-Time (JIT) access for specific tasks
- Role-Based Access Control (RBAC)
- MFA and Zero Trust integration
- Compatibility with DevOps tools, SaaS, cloud, and hybrid infrastructure

Why Pam Matters?

A Short History of PAM

PAM solutions emerged in the 2000s

Organizations faced increasing threats linked to privileged accounts

Traditional tools like Active Directory lacked fine-grained controls

Dedicated PAM platforms to secure admin access

Hybrid and cloud environments

Privilege Escalation & Critical Account Risks

Attackers often target:

- **Local Administrator Accounts** (reused passwords across devices)
- **Domain Admin Accounts** (full Active Directory control)
- **Service Accounts** (undocumented, non-expiring, unmonitored)

Common techniques:

- Credential dumping (e.g., Mimikatz)
- Lateral movement
- Golden Ticket attacks (Kerberos ticket forging)
- Shadow Admins (hidden high-privilege accounts)

Major Recent Breaches

Tesla Data Leak (2023 & 2025)

Two former employees leaked over 100 GB of PII, including Social Security numbers, bank details, and in-car recordings.

In 2025, a website called *DogeQuest* displayed personal Tesla user data on a live map.

These incidents highlight the danger of poorly controlled internal access.

Major Recent Breaches

Dropbox Sign Breach (2024)

A threat actor accessed the production backend of Dropbox Sign through an automated system configuration tool.

Stolen data included:

- Customer emails, usernames, and phone numbers
- Hashed passwords, API keys, OAuth tokens
- Multi-factor authentication data

The breach emphasizes the need for strong access controls and real-time monitoring of backend systems.

How PAM Mitigates These Risks

Removes standing privileges using Just-in-Time access

Centralized credential vault eliminates local password storage

Full session recording for accountability (SSH/RDP)

Automated password rotation to prevent reuse

Approval workflows and MFA to control high-risk access

Audit & Monitoring

The chosen solution

Small Market Analysis: Leaders and Alternatives

Gartner Magic Quadrant (Aug 2024) – shown in background

Leaders: CyberArk, BeyondTrust, Delinea

Challengers: ARCON, **ManageEngine (PAM360)**

Visionaries: WALLIX, One Identity

Niche Players: Broadcom (Symantec), Netwrix

ManageEngine PAM360 is positioned as a Challenger, showing growing maturity in execution with a strong vision for integrated, cloud-compatible PAM solutions.

Figure 1: Magic Quadrant for Privileged Access Management

Gartner

Why We Didn’t Choose CyberArk or BeyondTrust

Solution	Strengths	Limitations for Our PoC
CyberArk	Industry leader, comprehensive, robust	Too complex and costly for a student PoC or small-scale testing
BeyondTrust	Great balance of usability and control	Professional license required, more complex to deploy
JumpServer	Open-source, multi-protocol, lightweight	Less polished UI, limited scalability, fewer enterprise features

Why PAM360 Was the Best Fit

- Full license provided by our partner Kidan
- Native integration with Azure AD, RDP, SSH, Linux
- Ready-to-use compliance templates (ISO 27001, GDPR, PCI DSS)

PAM360 → complete and realistic platform

Strategic Partnership with Kidan

Thanks to Kidan.co, official ManageEngine partner in Switzerland:

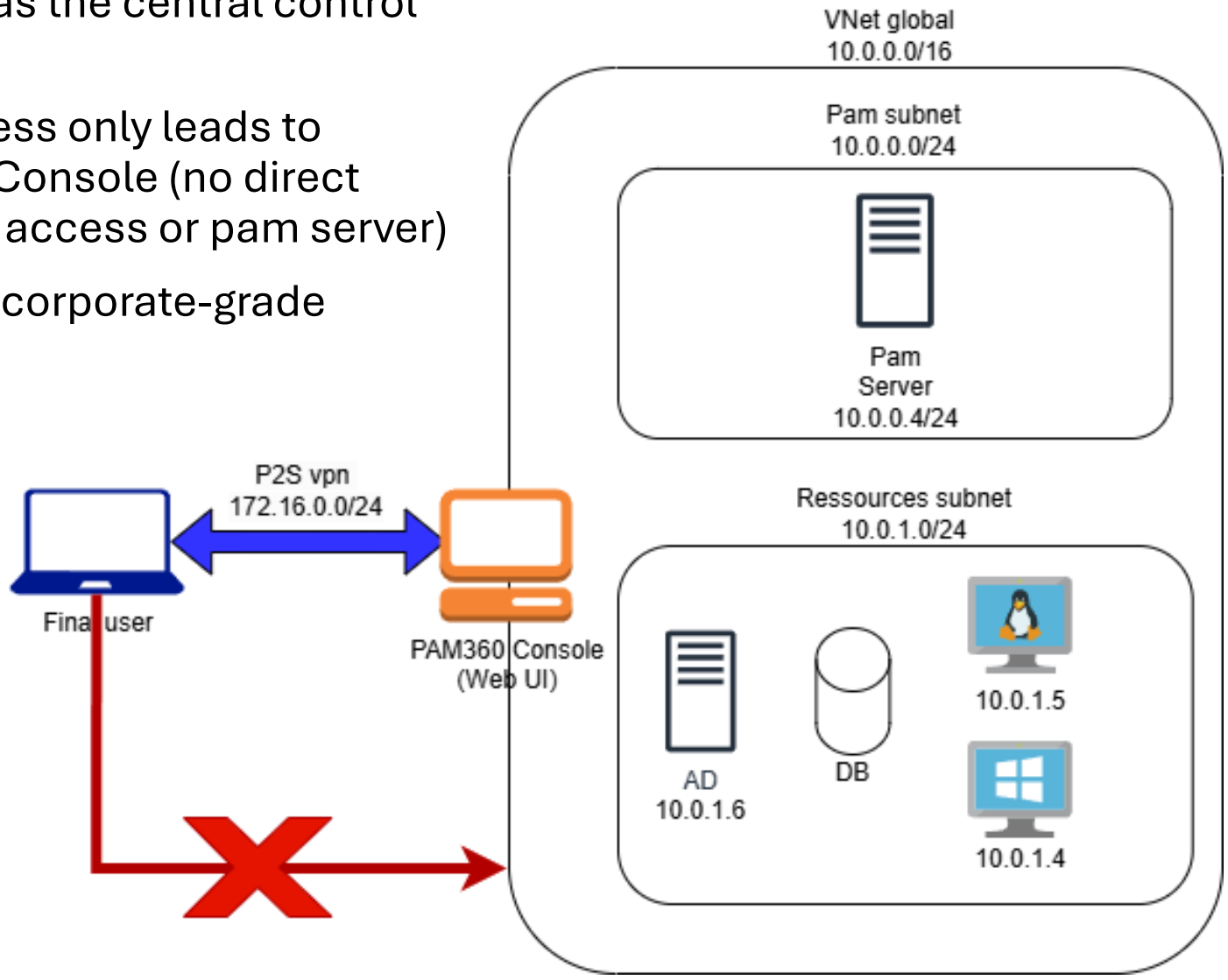
- We received a full-featured PAM360 license
- Gained professional-level documentation and support
- Opportunity for future collaboration (internship, projects, company training)
- This transformed our project into a market-relevant experience, aligned with real business needs.

PAM 360‘s SWOT

Architecture

Overview of Our Lab Architecture

- Hosted on Azure
- 2 subnets: Management and Resources
- PAM360 as the central control point
- VPN access only leads to PAM360 Console (no direct resource access or pam server)
- Realistic corporate-grade topology



Core module implementation

Core PAM Modules Implemented in Our PoC

Privileged Account & Credential Vaulting
→ Centralized and encrypted password storage, auto-rotation

Privileged Session Management
→ Monitored RDP/SSH sessions, with full playback and live oversight

Access Workflow Control
→ Role-based access approval, request → approval → checkout → audit

Audit & Compliance
→ Detailed audit logs, reports aligned with ISO 27001 / GDPR

VPN – Secure Access

Assignment: Dynamic / Static

Enable active-active mode * : Enabled / Disabled

Configure BGP ASN * : Enabled / Disabled

Once your VPN gateway is deployed correctly

VpnPam
Virtual network gatewa

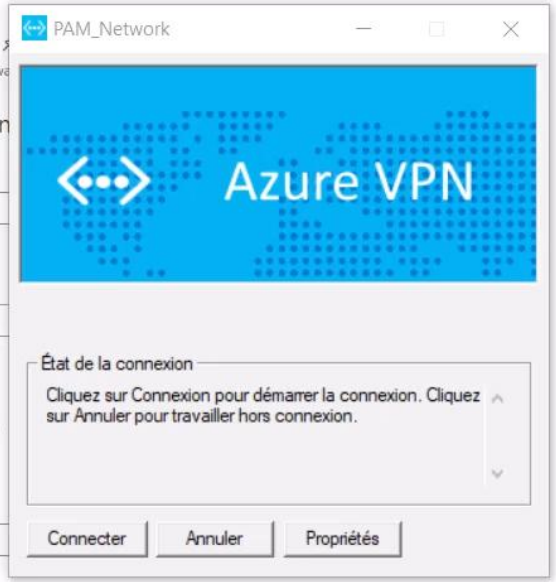
Click on it an go un

Address pool *
172.16.1.0/24

Tunnel type
IKEv2 and SSTP (SSL)

IPsec / IKE policy
Default Custom

Authentication type
Azure certificate



Root certificates

Name	Public certificate data
VpnPam	MIIC7TCCAdWgAwIBAgIQaB63o4iJKIRC2NHVcTStOT...

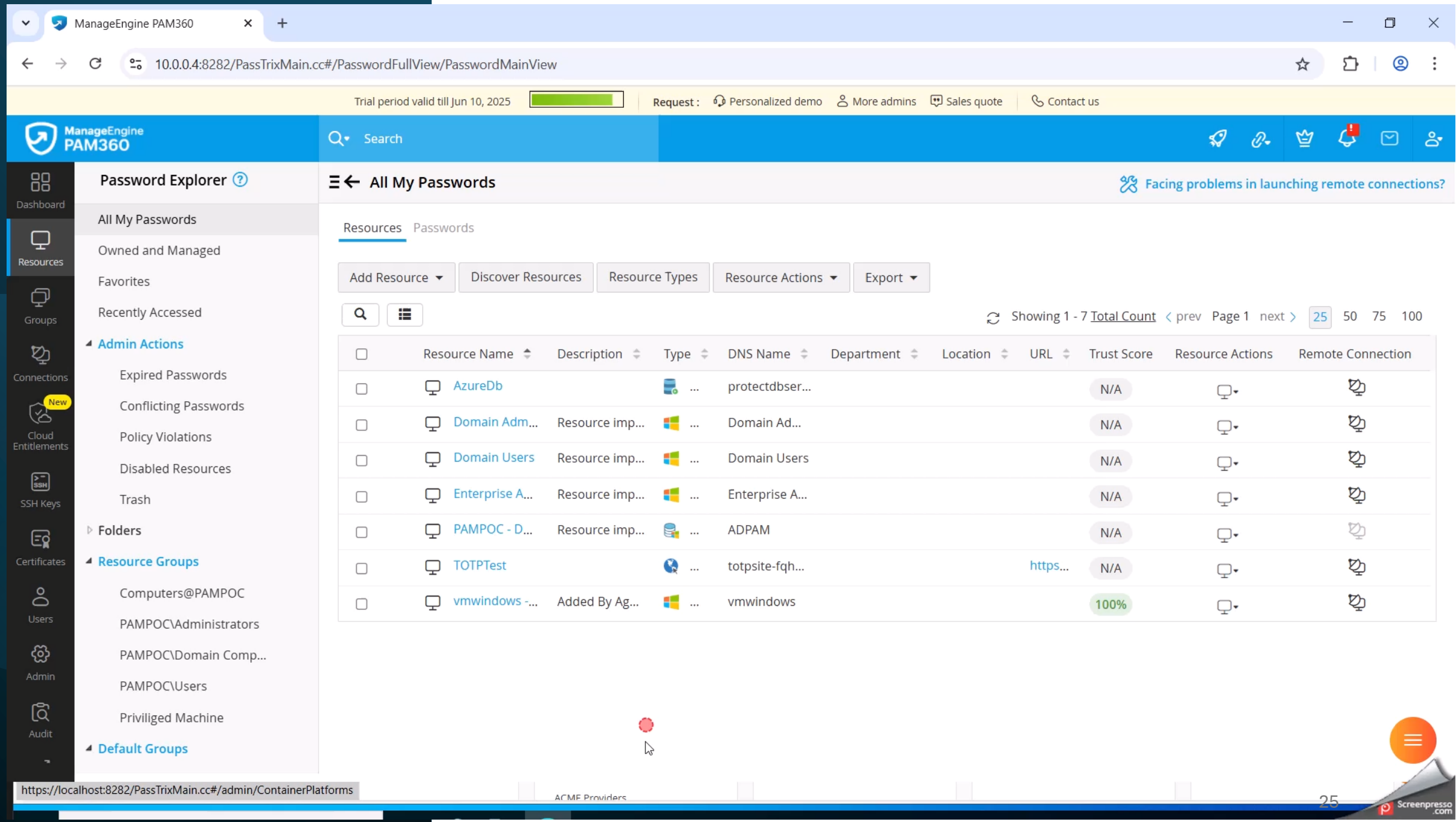
Address pool is for the ip that will be dynamiccally associated to your computer when initiating a vpn connection

Tunnel type → choose IKEv2 and SSTP so that you can use it on windows and MAC devices

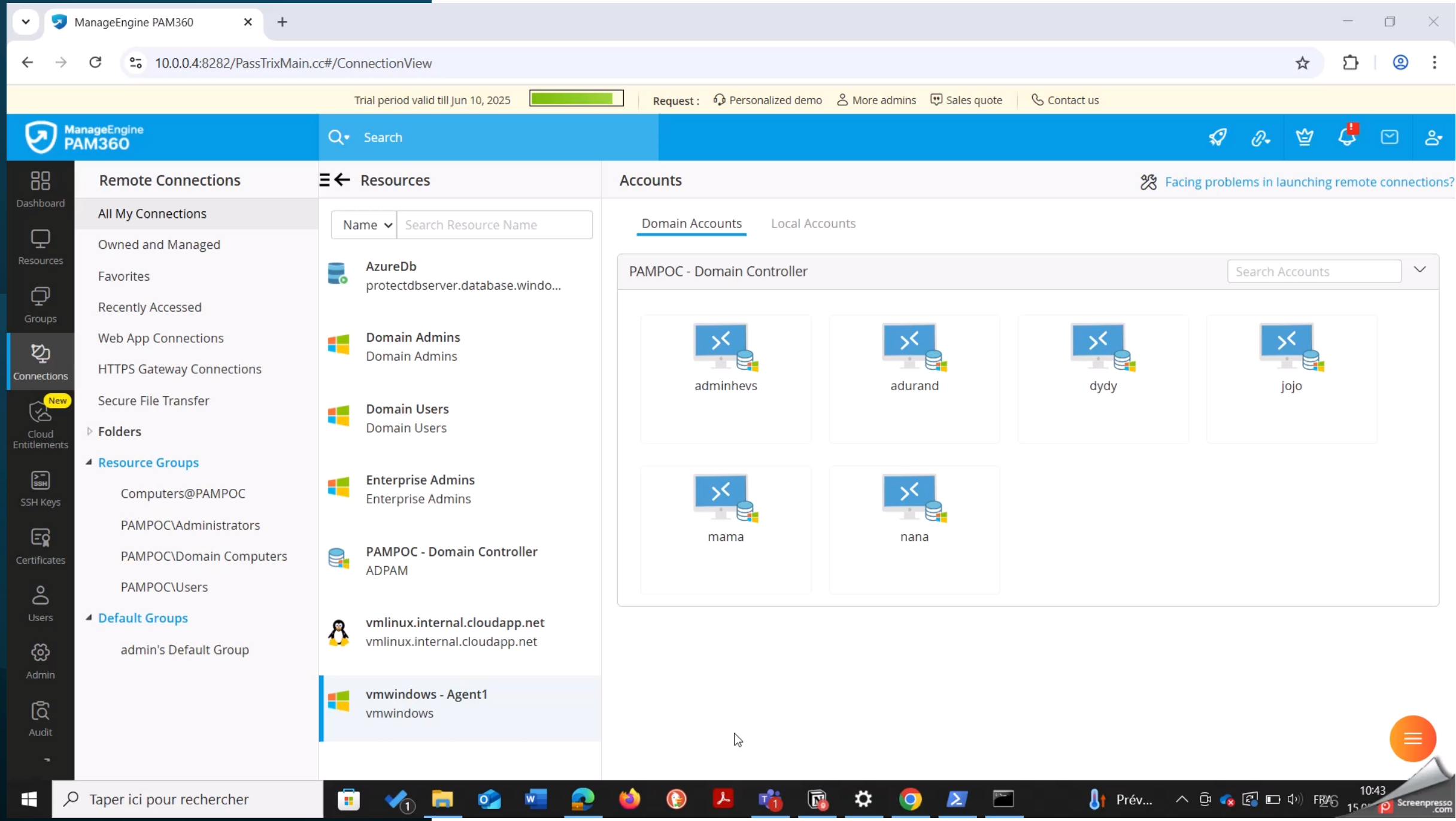
Short reminder

Taper ici pour rechercher
Taux...
FRA
10:31
Screenpresso.com

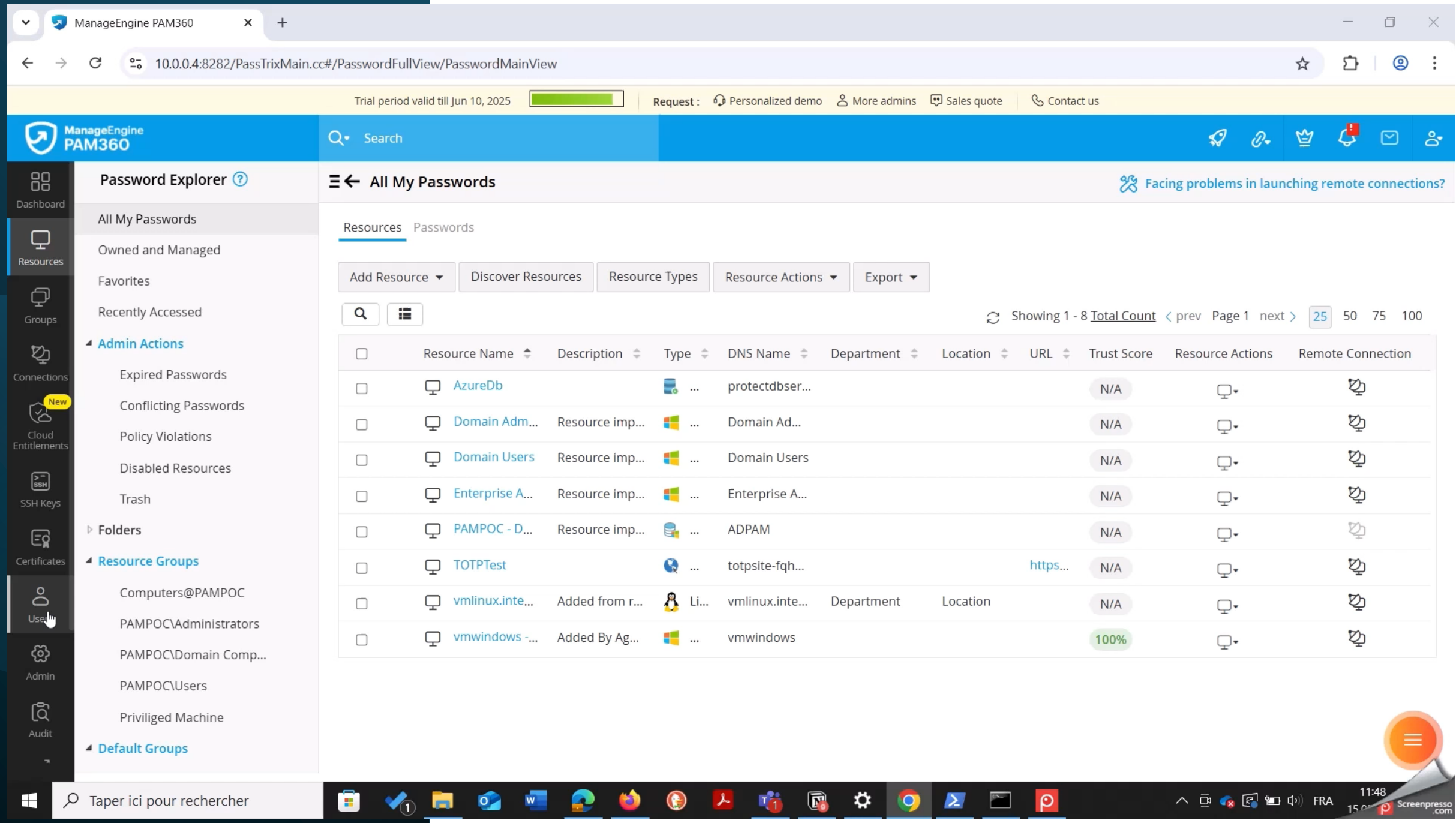
Discover Resources



File Share & Session Recording



Access Policy



Remote App Access

ManageEngine PAM360

10.0.0.4:8282/PassTrixMain.cc#/AuditQuickView/RecordedSession

Trial period valid till Jun 10, 2025 | Request : Personalized demo | More admins | Sales quote | Contact us

ManageEngine PAM360

Search

Dashboard
Resources
Groups
Connections
Cloud Entitlements (New)
SSH Keys
Certificates
Users
Admin
Audit

Audit

- Resource Audit
- Active Privileged Sessions
- Recorded Server Connections
- Recorded Website Connections
- Keys Audit
- Certificate Audit
- Cloud Entitlements
- SDK Application Audit
- User Audit
- User Sessions
- Task Audit
- Privileged Task Automation

Recorded Server Connections

Facing problems in recorded sessions playback?

Configure Session Recording | Audit Actions

Create | -- All --

Showing 1 - 25 of 134 | 1 2 3 4 5 | 25 50 75 100

Resource Name	User Account	Operated By	IP Address	Status	Time Stamp	Reason	Play	Activity Logs	Chat Log	Delete
PAMPOC - Domain Con...	adminhevs	admin	172.16.1.130	Succ...	May 15, 2025 08:43 AM	Retrieved b...			-	
PAMPOC - Domain Con...	adminhevs	admin	172.16.1.130	Succ...	May 15, 2025 08:42 AM	Retrieved b...			-	
PAMPOC - Domain Con...	adminhevs	admin	172.16.1.130	Succ...	May 15, 2025 08:41 AM	Retrieved b...			-	
PAMPOC - Domain Con...	dydy	admin	172.16.1.130	Succ...	May 15, 2025 08:40 AM	Retrieved b...			-	
PAMPOC - Domain Con...	dydy	admin	172.16.1.130	Succ...	May 15, 2025 08:38 AM	Retrieved b...			-	
PAMPOC - Domain Con...	dydy	admin	172.16.1.130	Succ...	May 15, 2025 08:38 AM	Retrieved b...			-	
vmwindows - Agent1	dylsan	admin	172.16.1.130	Succ...	May 15, 2025 08:36 AM	Retrieved b...			-	
vmwindows - Agent1	dylsan	admin	172.16.1.130	Succ...	May 15, 2025 08:33 AM	Retrieved b...			-	
PAMPOC - Domain Con...	adminhevs	admin	172.16.1.130	Succ...	May 15, 2025 08:09 AM	Retrieved b...			-	
vmwindows - Agent1	dylsan	admin	172.16.1.130	Succ...	May 15, 2025 08:09 AM	Retrieved b...			-	
vmwindows - Agent1	dylsan	admin	172.16.1.130	Succ...	May 15, 2025 07:33 AM	Retrieved b...			-	
vmwindows - Agent1	dylsan	admin	172.16.1.130	Succ...	May 15, 2025 07:25 AM	Retrieved b...			-	

Taper ici pour rechercher

10:46

Screenpresso.com

Remote App Access

ManageEngine PAM360

10.0.0.4:8282/PassTrixMain.cc#/admin/adminMain

Trial period valid till Jun 10, 2025 | Request : Personalized demo | More admins | Sales quote | Contact us

ManageEngine PAM360

Search

Search term

- Dashboard
- Resources
- Groups
- Connections
- Cloud Entitlements (New)
- SSH Keys
- Certificates
- Users
- Admin
- Audit

Authentication

- Active Directory
- Microsoft Entra ID
- LDAP
- SAML Single Sign-On
- RADIUS
- Smart Card / PKI / Certificate
- Two-Factor Authentication
- Super Administrators

Resource Config

- Discover Resources
- Password Policies
- Resource Additional Fields
- Account Additional Fields
- Resource Types
- JDBC Properties

Zero Trust

- Configuration
- Trust Score
- Access Policy
- Conflict Resolver

Customization

- Roles
- Password Reset Listener
- Auto Logon Helper
- Rebrand
- Email Templates
- Message Templates
- Password Reset Plugin
- SSH Command Sets

Settings

- Log Level
- Export / Offline Access
- Mail Server Settings
- Proxy Server

Connections

- RemoteApp
- Gateway Server Settings
- Session Configuration
- Landing Servers

Privilege Elevation

- Allowed Apps/Scripts
- Manage Commands
- Application Control

SSH/SSL Config

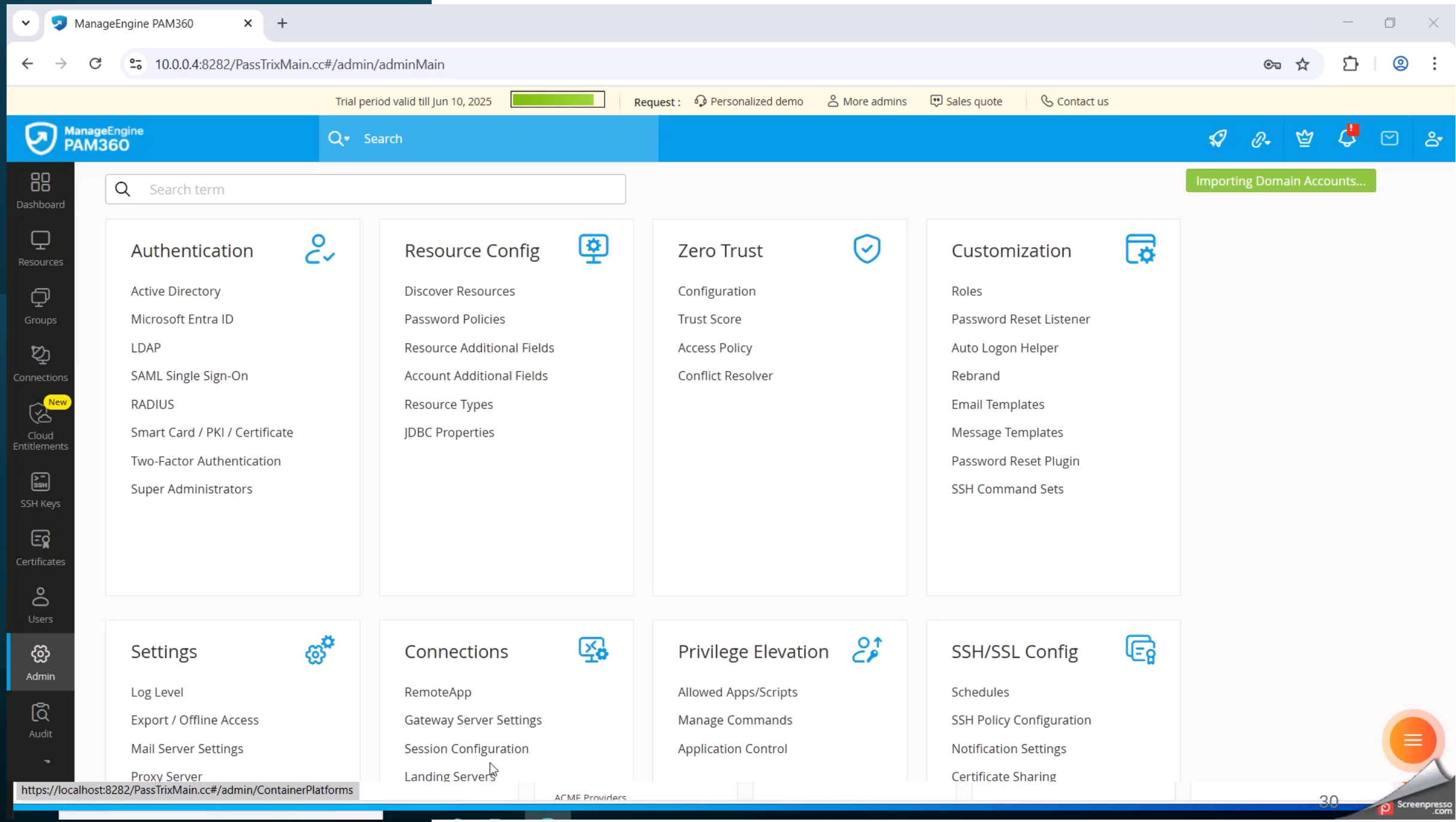
- Schedules
- SSH Policy Configuration
- Notification Settings
- Certificate Sharing

Taper ici pour rechercher

FRA 10:56

Screenpresso.com

Secure Command SSH

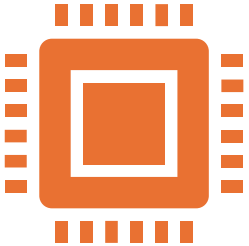


Challenges, learnings and conclusion

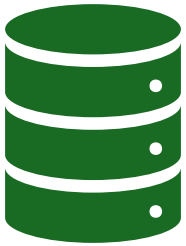
What We Learned from the Project

- The **complexity of secure privileged access**: understanding vaulting, session isolation, JiT, and least privilege logic.
- How to configure a **VPN gateway and restrict direct access** through NSG rules.
- Full deployment of a **realistic PAM solution** (PAM360) including:
  - MFA
  - Session recording
  - SSH/RDP access brokerage
  - Password rotation
  - Certificate integration
- Understand Zero Trust Framework and how to implement it

What challenge have we met?



VPN + certificate setup was the most technical part (cert generation, .pfx/.cer, P2S configuration)



Understanding and enforcing **Zero Trust logic** across multiple subnets

Remote connections in general (RDP, SSH, …) due to a lack of logs

What's Next? – Maturity Model and Next Steps

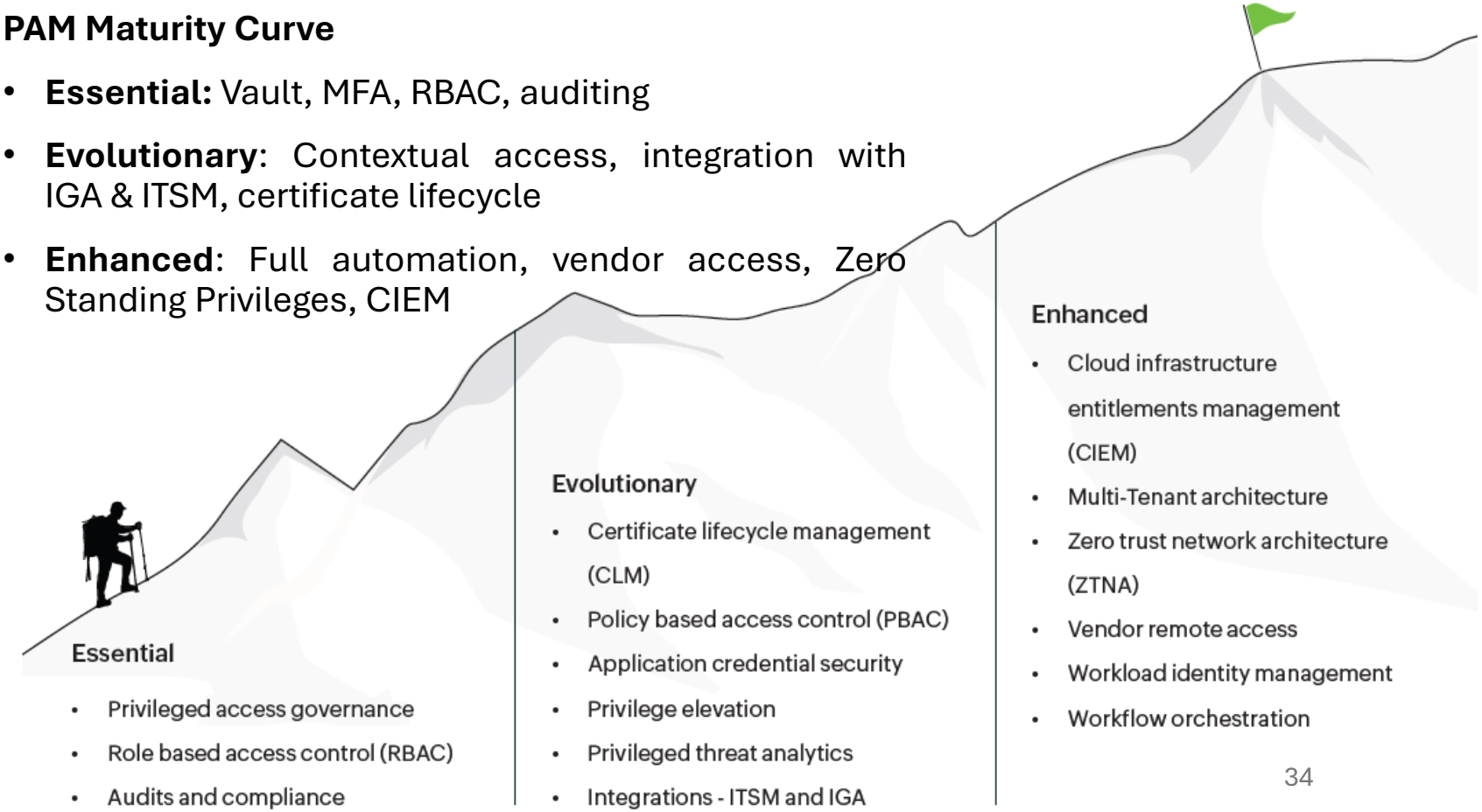
Recommendations

- Move toward **JIT (Just-in-Time)** and **PBAC** (Policy-Based Access Control)
- Enhance automation: Credential lifecycle, session termination
- Integrate **DevOps, CI/CD tools**, or third-party app credentials
- Strengthen monitoring with **SIEM integration (Azure Sentinel)**

ManageEngine

PAM Maturity Curve

- **Essential:** Vault, MFA, RBAC, auditing
- **Evolutionary**: Contextual access, integration with IGA & ITSM, certificate lifecycle
- **Enhanced**: Full automation, vendor access, Zero Standing Privileges, CIEM



Conclusion: What PAM360 Taught Us

Privileged access is one of the most critical risks in modern infrastructure. Through this project, we deployed and tested PAM360 in a realistic Azure environment, applying key cybersecurity principles like:

- Least privilege
- Just-in-Time access
- Zero Trust enforcement

Key takeaway:

- PAM360 proved to be a professional-grade solution that is also well-suited for education and experimentation.
- This PoC helped us understand real-world privileged access risks and defenses.

Questions ?