

Eric Parietti Ingénieur Avant Vente One Identity
Eric.Parietti@OneIdentity.com



Safeguard for Authentication Services and Sudo management

AD bridging authentication and Sudo management
Linux, Unix, Mac

The Challenge : Identity – Privilege - Operations

Identity

- Multiple identity silos
- Local accounts and passwords
- Inconsistent password policies
- Complex provisioning/deprovisioning
- Difficult access governance
- Unix/Linux/macOS disconnected from the enterprise identity model

Privilege

- Excessive root/sudo privileges
- Distributed sudo policies
- Inconsistent privilege rules
- Shared privileged access
- Limited accountability
- Difficult auditing and compliance reporting

Operations

- Manual configuration of individual systems
- Configuration drift
- Repetitive administration
- Limited centralized visibility
- Difficult deployment at scale

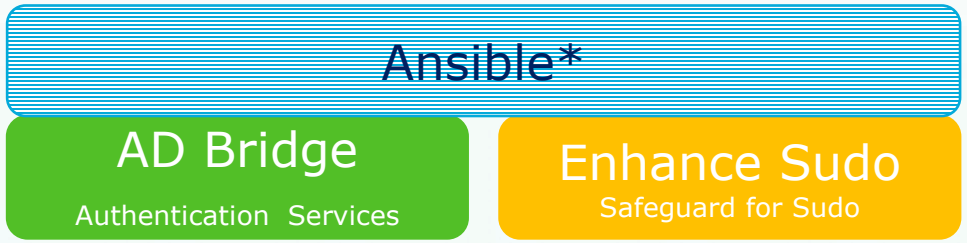
Safeguard Authentication Service and Sudo management

One Identity approach: Centralize Identity + Control Privilege + Automate at Scale

- Consolidates identities
- Extends the security of Active Directory to Unix-based systems and applications
- Audit trail for individual accountability
- Enables least-privileged access for “root” or application accounts
- Centralized and single source access control reporting

Safeguard for Authentication Services (SAS) & sudo

- Safeguard for Authentication Services and sudo management



*Ansible is not bundled with the OI Products and is not an OI product

One Identity SAS Ansible Catalog (Ansible Galaxy) and Playbooks

The main benefit of the official One Identity Ansible Authentication Services collection is instead of connecting to every Linux/macOS system and manually executing the SAS installation, configuration and domain-join commands, **Ansible can orchestrate those operations across your target systems**.

Orchestrate Ansible automation.

If needed Ansible AWX or RedHat Ansible Automation



Active Directory Bridge

AD Bridging Authentication Services

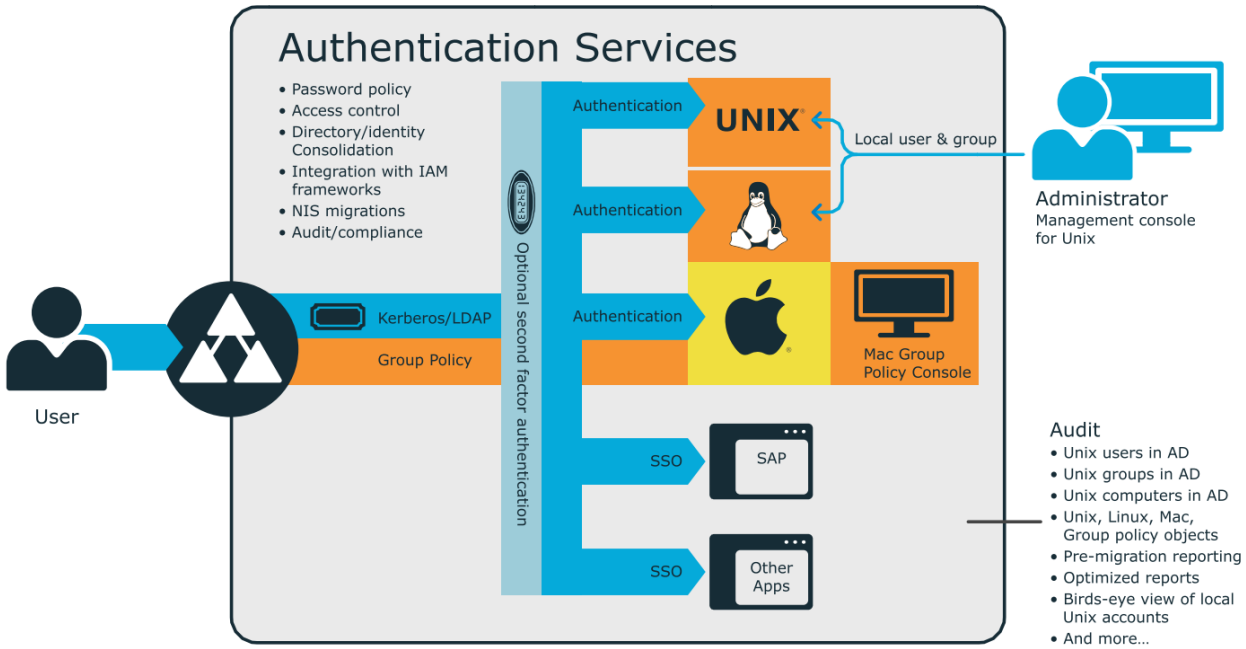
Manage Unix, Linux, Mac users and access from AD

- Authenticate Unix, Mac users with AD Kerberos
- Consolidate identities & directories into one AD
- Grant Access to Unix, Linux, Mac Systems by AD Group Membership
- Enhance password security
  - Extend AD password policies
  - Eliminate redundant, inconsistent, and non-secure passwords
  - Extend AD-based self-service password reset capabilities
  - Unix access is locked with AD account

Here’s how it works …

Architecture

- Using LDAP / Kerberos
- No Changes to AD Schema
- GPO extension
- Integrates natively through local facilities (NSS / PAM* / LAM)
- Clients are AD “Site-Aware”

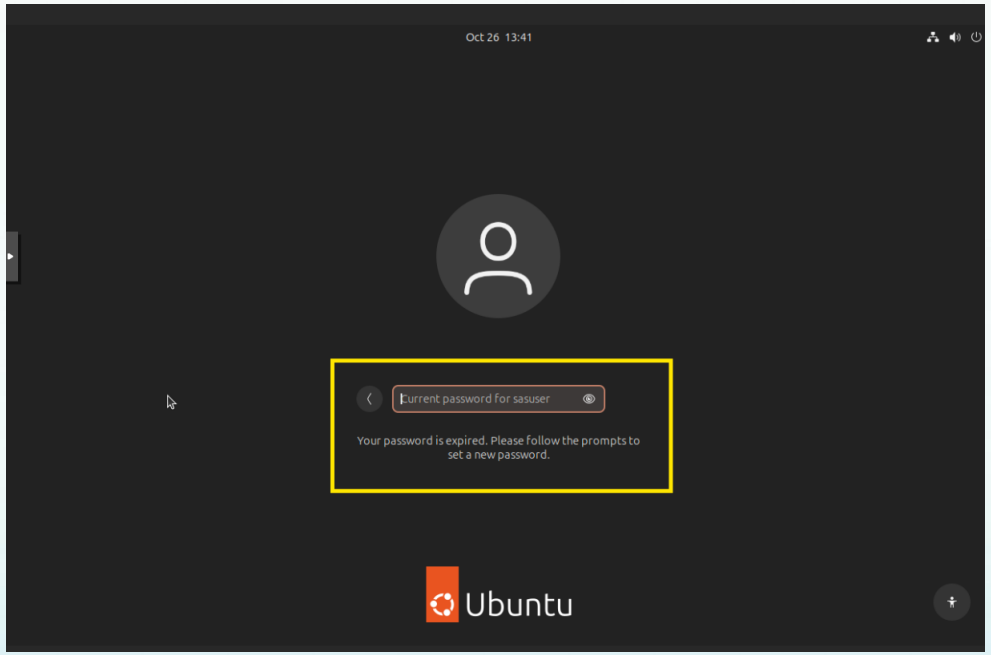


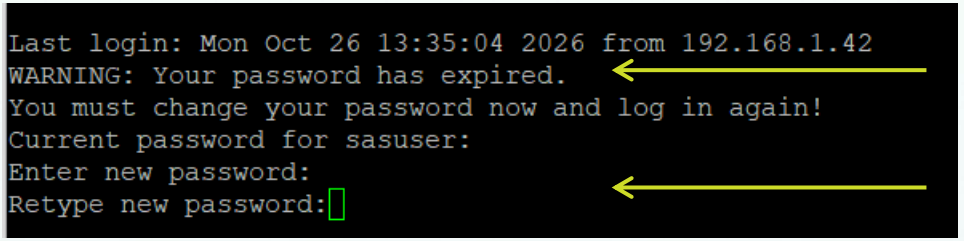
Authentication Services natively implements Kerberos, LDAP and single sign-on for UNIX, Linux and Mac OS X systems in the same way they are implemented in Windows.

* PAM Pluggable Authentication Module

Password policy

- Extend AD password policy to Unix, Linux and Mac
- Immediately improve password security
- Extend AD-based self-service password rests to Unix, Linux and Mac
- Eliminate redundant, inconsistent, and non-secure passwords
- Enhance login with multifactor authentication (One Identity Defender)

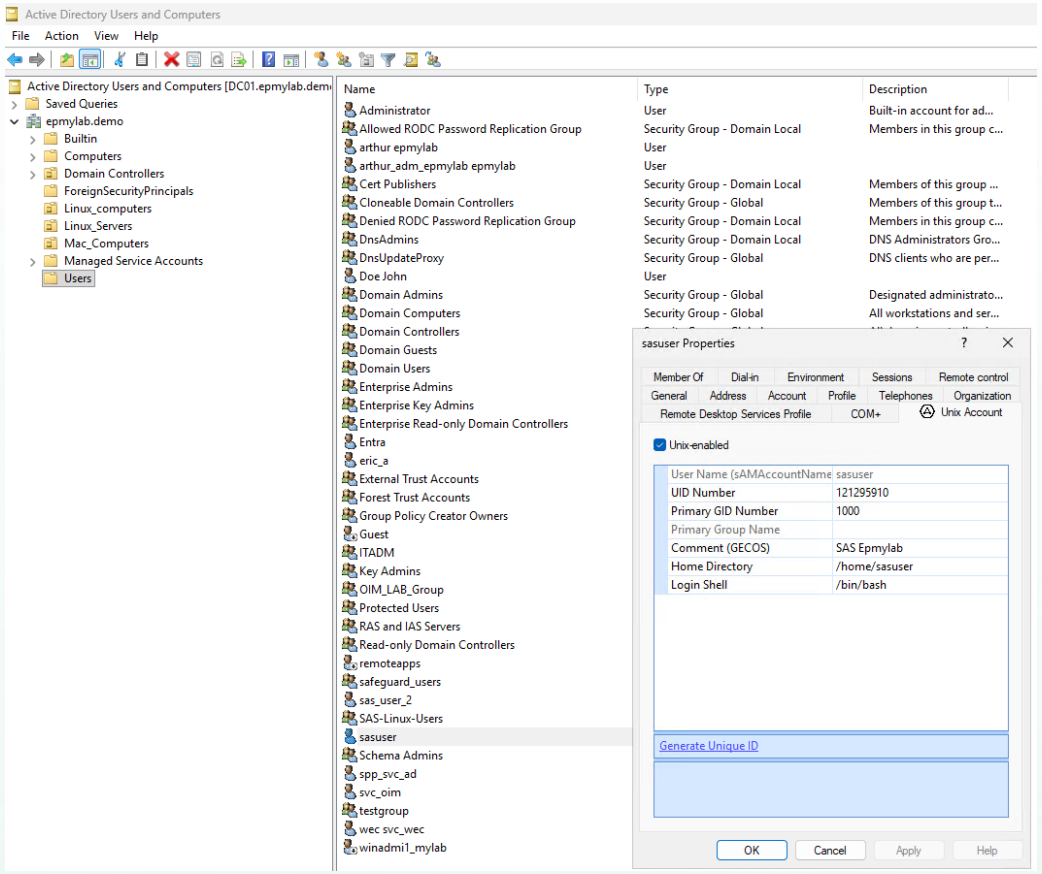


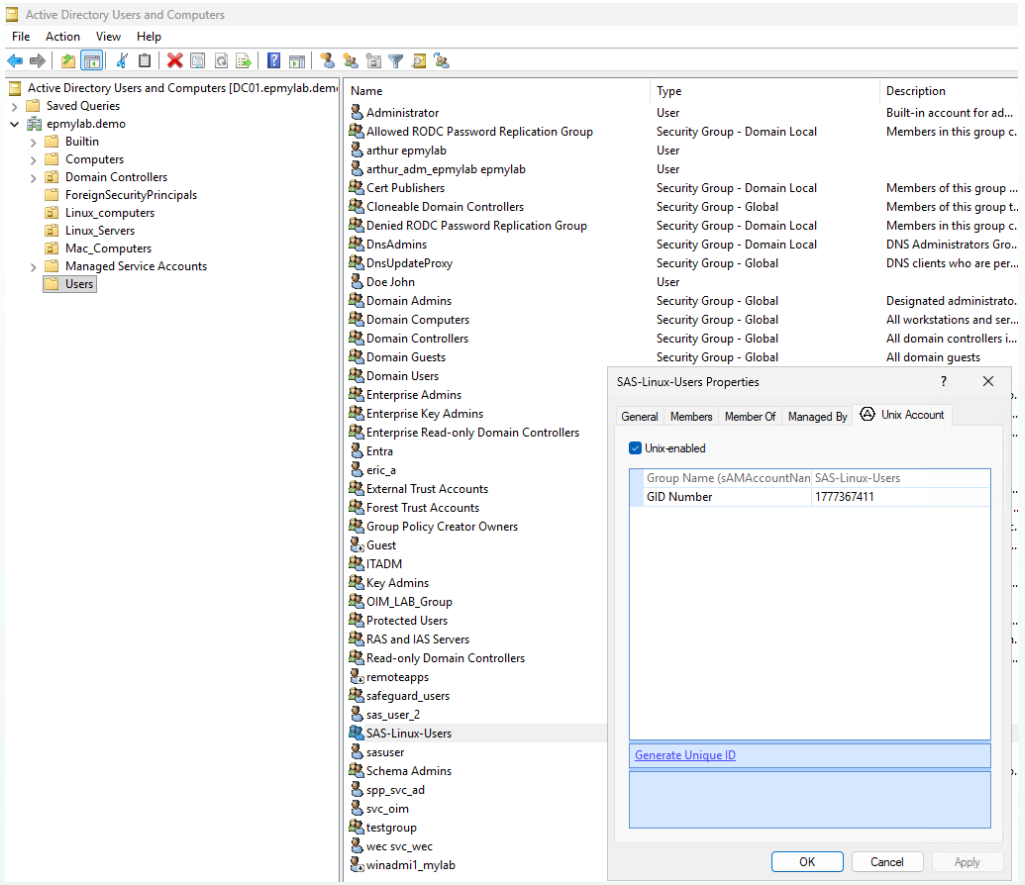


Access Control

- Leverage AD groups for Unix/Linux/Mac access
- Achieve full audit alerting and change tracking for non-Windows systems in AD
- Centralize authentication and authorization
- Achieve granular access control
- Expand access control through additional PAM (Privileged Access Management) offerings

Manage Accounts and Groups from ADUC

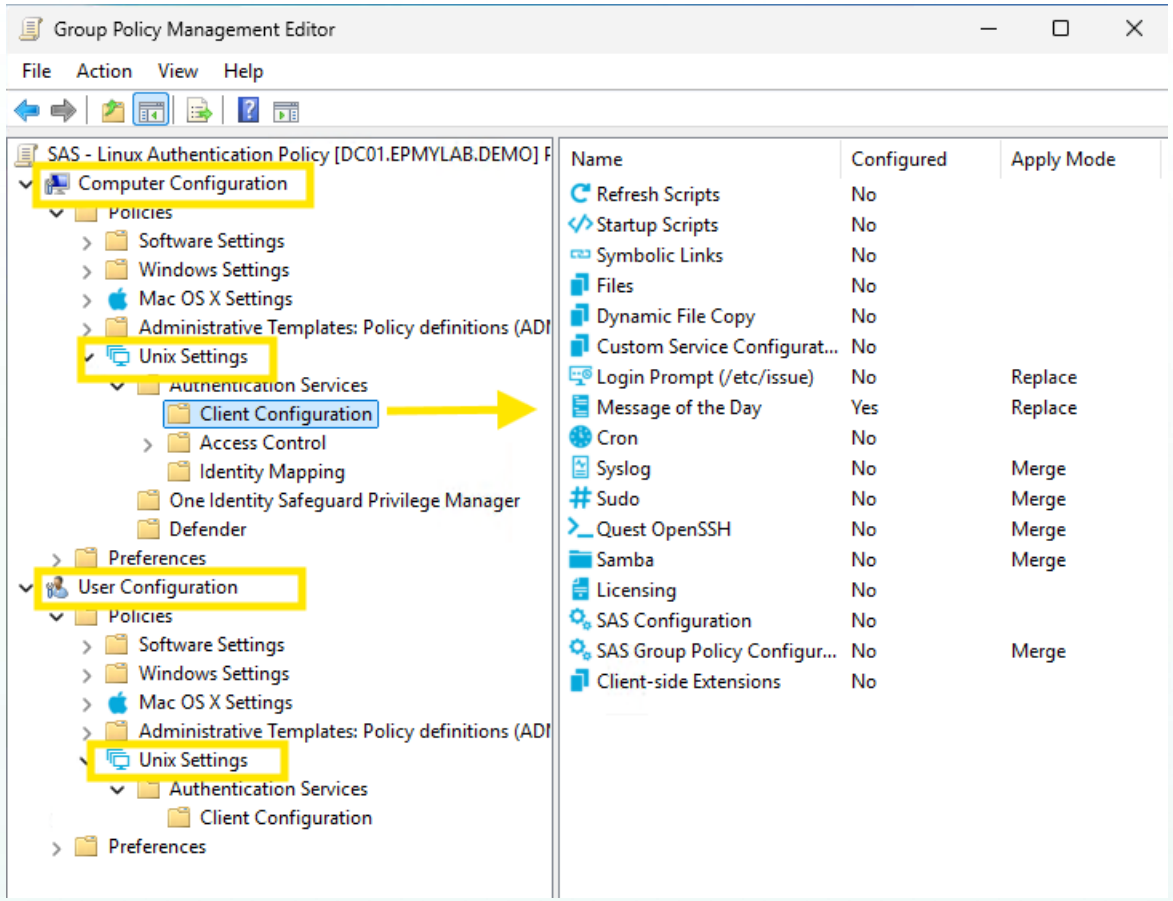


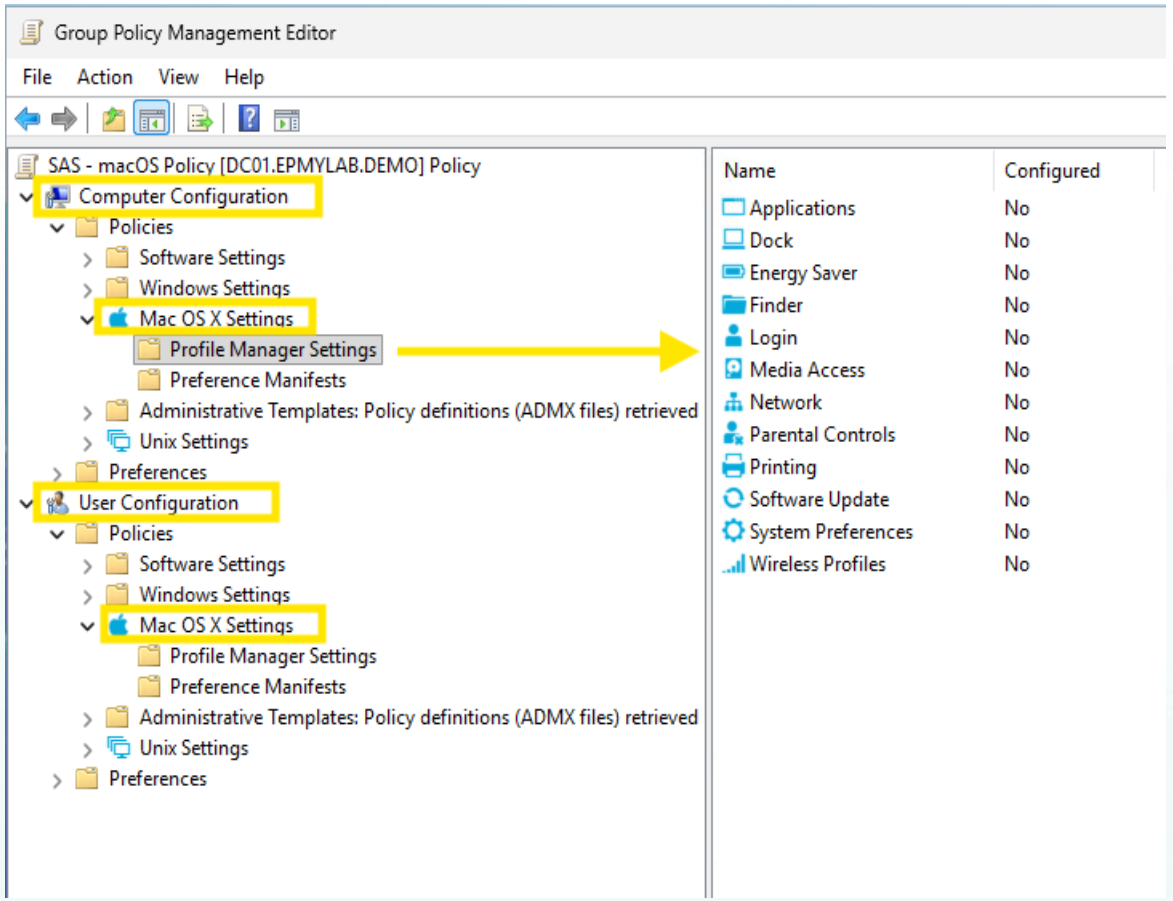


Enterprise group policy

- Flexibly extend group policy to Unix, Linux and Mac
- Manage all Mac settings and preferences with a purpose-built interface and support for preference manifest files
- Track changes to non-Windows group policy objects
- Control additional IAM functionality through group policy – privileged management and multifactor authentication

Group Policy Editor for UNIX/Linux and MAC OS





Étendre Active Directory jusqu'aux Macs

SAS Safeguard Authentication Services transforme les Mac en citoyens de l'Active Directory :

- Authentification AD, Kerberos
- Contrôle d'accès
- Politiques centralisées
- Certificats et paramètres de sécurité macOS

SAS étend l'authentification, l'autorisation et l'administration Active Directory à UNIX, Linux et macOS

Versions de Mac OS Supportés, sur la version 7.2 de Safeguard Authentication Services
Mac OS 15.x, 26.x, 27.x
ICI

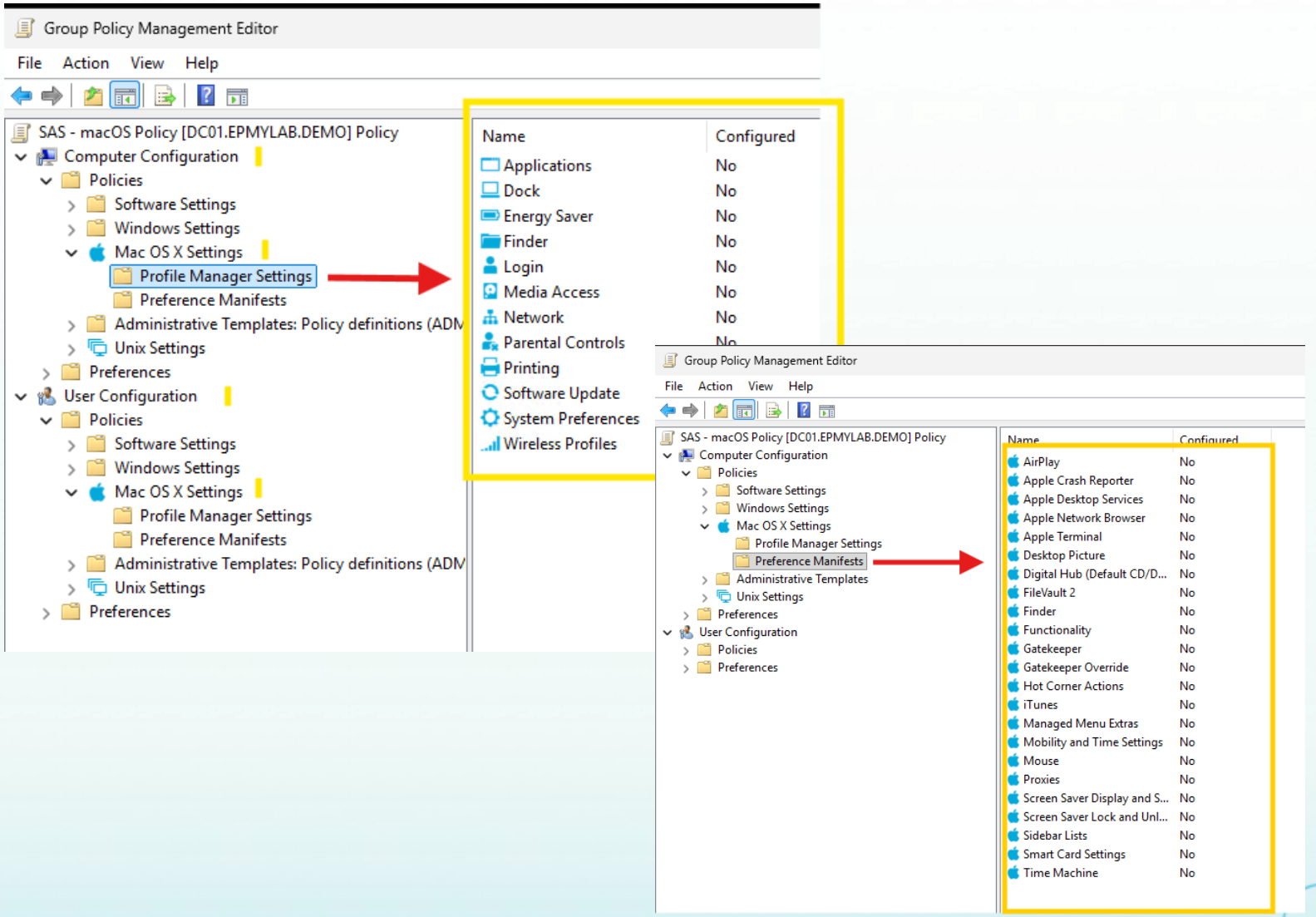
Special Macs

SAS MacOS couvre notamment :

- Authentification avec les comptes Active Directory
- Group Policy pour MacOS
- Configuration de profils
- Montage automatique des home folders via Group Policy
- Paramètres d’applications, Dock, Finder et login
- Certificats et auto-enrollment
- Réglages réseau, imprimantes, Time Machine et autres paramètres spécifiques MacOS

Les deux familles de politiques macOS exposées par le snap-in SAS dans GPMC

- Gestionnaire de profils
- Manifestes de préférences



Exemple

- Certificat machine AD CS pour autoriser le VPN

Certificat machine AD CS pour autoriser le VPN

Automatiser l'identité machine des Mac depuis la PKI Microsoft

- Le Mac est joint au domaine Active Directory grâce à SAS.
- Un certificat machine est demandé auprès de l'infrastructure **Microsoft AD**

Certificate Services / AD CS.

- L'auto-enrollment est piloté par les politiques de groupe.
- Le certificat est installé sur le Mac et peut servir d'identité machine.
- Le concentrateur VPN peut alors autoriser uniquement les terminaux disposant d'un certificat valide délivré par la PKI de l'organisation.



Valeur métier

- Suppression des demandes manuelles de certificats
- Identité machine liée au cycle de vie de l'objet ordinateur AD
- Accès VPN limité aux appareils effectivement enrôlés
- Modèle cohérent avec la PKI Microsoft déjà utilisée pour Windows
- Centralisation de la stratégie dans AD plutôt que configuration individuelle des Mac

SAS automatise le déploiement du certificat machine depuis AD CS. Ce certificat peut ensuite être utilisé par la solution VPN comme preuve que le Mac est un terminal enrôlé et approuvé.



Safeguard for Sudo

Centralized Privilege Elevation and Recording

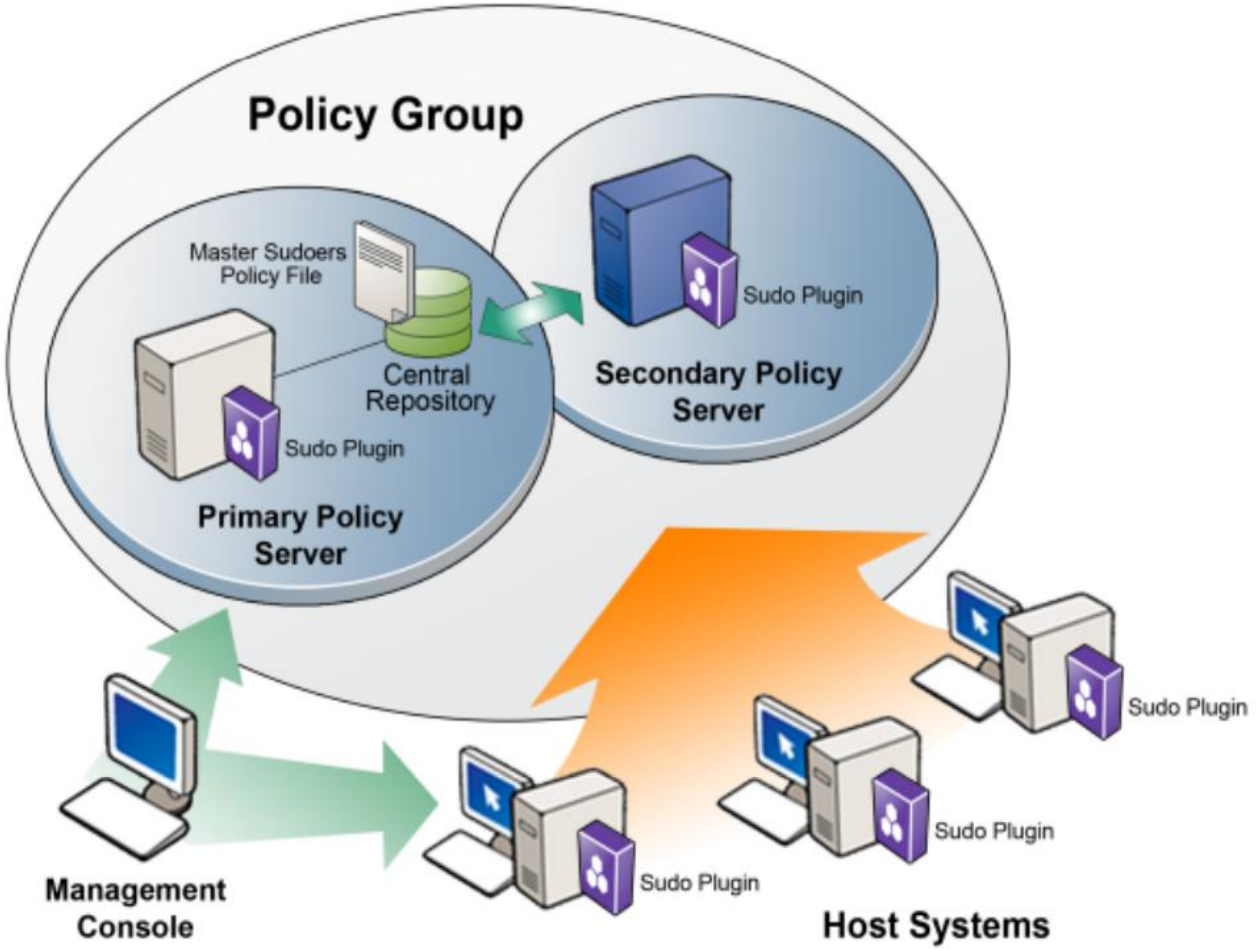
ONE IDENTITY by Quest

Safeguard for Sudo

- Centralized management of sudo across any number of Unix/Linux servers
- Centralized reporting on sudo policy, activities, and history
- Event and keystroke logging
- Offline policy evaluation and log synchronization
- Policy revision management with change tracking and reporting and policy roll-back

Architecture

- Central Sudo Policy
- Centralized Management
- Event Logging
- Keystroke Logging
- Offline Policy Evaluation and Log Synchronization
- Separation of Duty Enforcement



Sudo 1.9 – Safeguard for Sudo 7.2



Session (I/O log) recording

Safeguard SPS

sudo_pair

User → sudo → policy → **approval plugin** → accept/deny

Approval

Audit

python™

Plugins

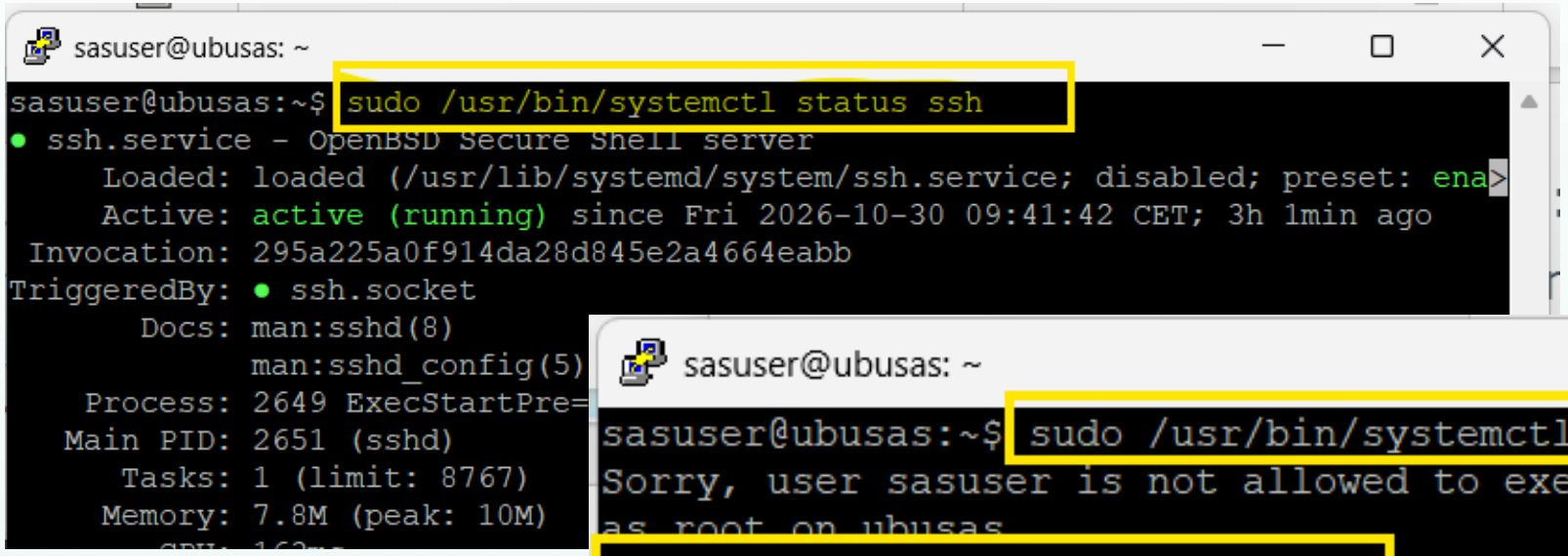
Complements the native audit capabilities

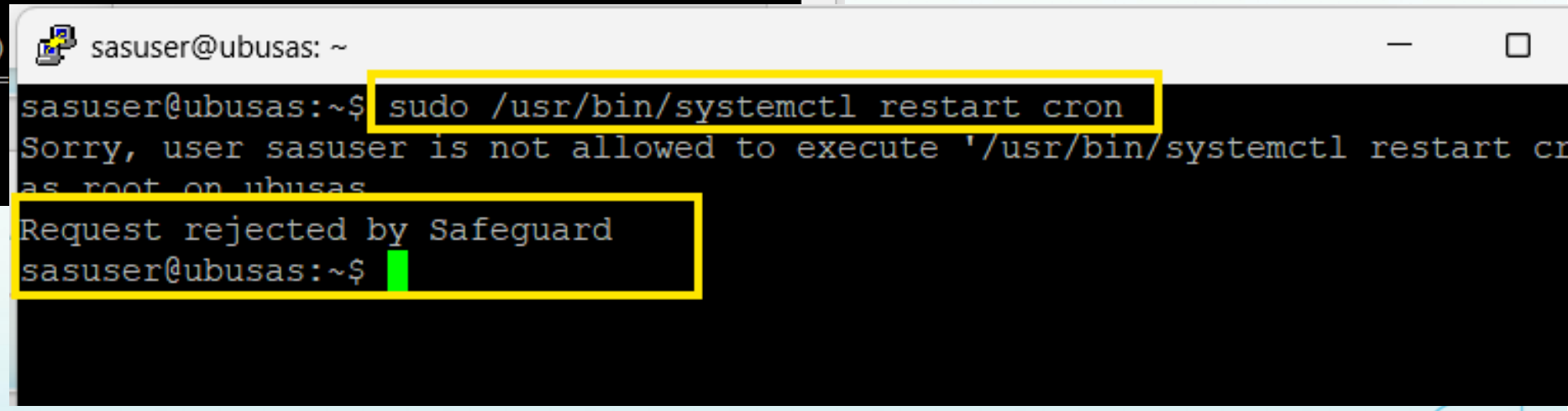
Safeguard for Sudo - Features

- Easy-to-use installation
  - Preflight and sudo plug-in installation
- Policy Management – Edit, Version control of sudoers file, including rollback and change tracking
- Sudo policy evaluation engine
- Secure off-line policy caching
- Sudo Reporting
  - Ability to run reports on hosts/users to get detailed information on sudo permissions (who can run what via Sudo)
  - Event Activity
  - Commands run
  - Policy changes
- Separation of Duty

• Sudoers file centralized and deployed Sudo elevation : approve and deny

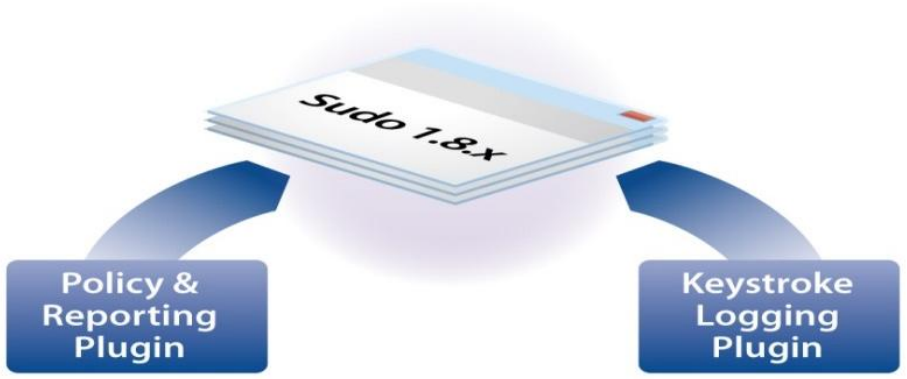
```
1  # LAB SG for Sudo Policy - Restrict privileges for the user sasuser
2  sasuser ALL=(root) /usr/bin/systemctl status ssh, /usr/bin/systemctl restart ssh,
   /usr/bin/tail /var/log/auth.log
```





Merci
N’hésitez pas à venir discuter avec nous

Sudo 1.8



- Central Policy plug-in
- Keystroke Logging plug-in