Privileged Access Management

Controlling Administrative Access in OT Environments

OT Security Learning Series

Document 880 | January 2026

Contributors: Matthias Niedermaier

Created with AI assistance

LEARNING RESOURCE

Contents

1 Introduction

Information

Privileged Access Management (PAM) controls and monitors access by users with elevated permissions to critical systems. In OT environments, privileged accounts include not only administrative credentials but also vendor remote access, engineering workstation logins, and service accounts that can modify industrial control system configurations.

Privileged accounts represent the keys to the kingdom in any environment, but in OT they carry additional weight. A compromised privileged account can modify PLC logic, disable safety systems, or disrupt physical processes. Unlike IT environments where privileged access primarily affects data, OT privileged access can affect safety and operations.

2 Privileged Access in OT

2.1 Types of Privileged Accounts

Account Type	Description and Risk
System Administrator	Full access to servers, workstations, network devices
OT Engineer	Can modify PLC/DCS logic, HMI configurations
Vendor/Integrator	Remote access for maintenance, often with broad permissions
Service Accounts	Automated processes with elevated privileges
Emergency/Break-Glass	High-privilege accounts for disaster recovery
Shared Accounts	Generic logins used by multiple operators

Table 1: Types of privileged accounts in OT environments

2.2 OT-Specific Challenges

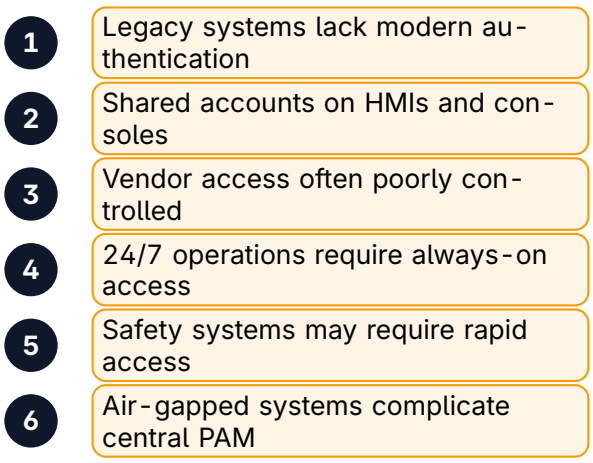

Figure 1: OT-specific PAM challenges

Warning

Many OT systems were designed before cybersecurity was a concern. PLCs may have no authentication, HMIs may use shared local accounts, and vendor access may rely on static VPN credentials. PAM strategies must account for these limitations.

3 PAM Architecture for OT

3.1 Core Components

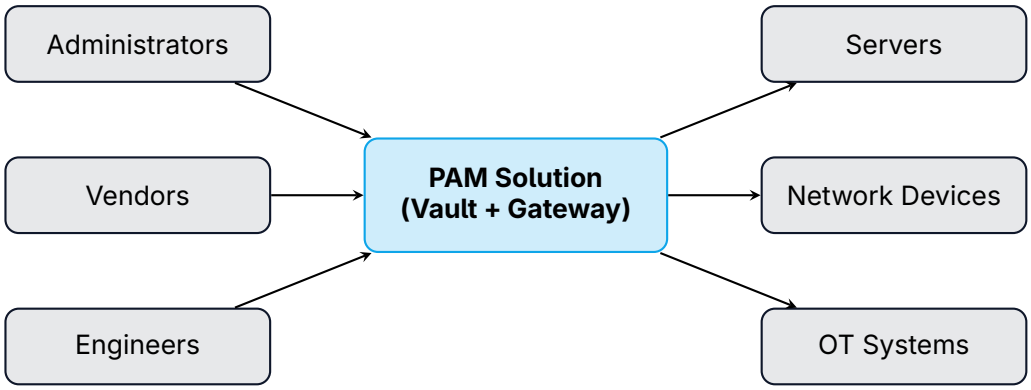

Figure 2: PAM architecture overview

- **Credential Vault** – Securely stores and rotates privileged credentials
- **Session Gateway** – Proxies and records privileged sessions
- **Access Request Workflow** – Manages approval for privileged access
- **Just-in-Time Access** – Grants temporary elevated permissions
- **Session Recording** – Captures keystrokes, screens, commands

3.2 Jump Server Architecture

Jump servers (or bastion hosts) provide controlled access points into OT networks:

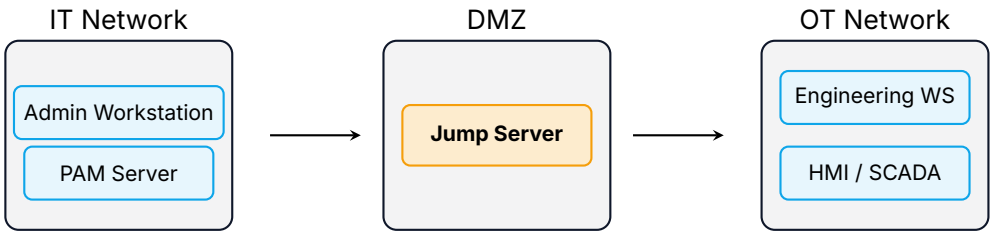

Figure 3: Jump server placement in OT architecture

Tip

Jump servers should be hardened systems with minimal software, full session logging, and multi-factor authentication. All administrative access to OT systems should traverse the jump server—direct connections must be blocked.

4 Vendor Access Management

4.1 The Vendor Access Problem

OT environments often depend heavily on vendor support:

- Equipment vendors for PLC/DCS troubleshooting
- System integrators for configuration changes
- Software vendors for updates and patches
- Managed service providers for ongoing support

Critical

Vendor remote access is one of the most common attack vectors in OT incidents. Attackers compromise vendor credentials or infrastructure, then use trusted connections to reach multiple customer sites. The 2021 Kaseya attack demonstrated this at scale.

4.2 Vendor Access Controls

Control	Implementation
No Persistent Access	Disable vendor connections when not in use
Explicit Approval	Require customer approval before each session
Time-Limited Sessions	Auto-terminate access after defined period
Least Privilege	Limit access to specific systems needed
Multi-Factor Auth	Require MFA for all vendor connections
Session Recording	Record all vendor activity for audit
Real-Time Monitoring	Alert on unusual vendor behavior

Table 2: Essential vendor access controls

4.3 Vendor Access Workflow

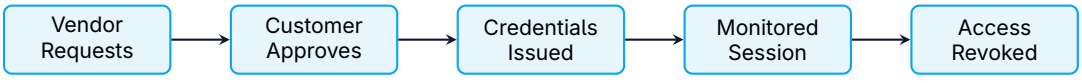

Figure 4: Controlled vendor access workflow

5 Credential Management

5.1 Password Vaulting

Centralized password vaults eliminate password sharing and enable rotation:

- Store all privileged credentials in encrypted vault
- Users check out credentials through PAM system
- Automatic rotation after each use or on schedule
- Eliminate local copies of privileged passwords
- Audit trail for all credential access

5.2 Rotation Challenges in OT

Challenge	Mitigation
Hardcoded credentials	Document, plan remediation in maintenance windows
Service account dependencies	Map dependencies before rotation
Offline/air-gapped systems	Manual rotation procedures with verification
Legacy systems without APIs	Agent-based or manual rotation with scripts
24/7 operations	Schedule rotation during planned maintenance

Table 3: OT password rotation challenges and mitigations

5.3 Service Account Management

Service accounts require special attention:

- **Inventory** – Document all service accounts and their purposes
- **Ownership** – Assign responsible owner for each account
- **Least Privilege** – Limit permissions to minimum required
- **Monitoring** – Alert on interactive logins to service accounts
- **Rotation** – Rotate credentials on defined schedule

6 Session Management

6.1 Session Recording

Recording privileged sessions provides forensic capability and deters misuse:

- **Video Recording** – Capture screen activity for GUI sessions
- **Keystroke Logging** – Record all commands entered
- **Command Filtering** – Block or alert on dangerous commands

- **Metadata Capture** – Log session duration, systems accessed

Key Point

Session recordings are invaluable for incident investigation. When a configuration change causes a process upset, recorded sessions show exactly what was modified and by whom.

6.2 Real-Time Monitoring

Beyond recording, active monitoring can prevent damage:

- Alert on sensitive command execution
- Terminate sessions on policy violations
- Notify supervisors of high-risk activities
- Integrate with SIEM for correlation

7 Emergency Access

7.1 Break-Glass Procedures

Emergency situations may require bypassing normal PAM controls:

Element	Description
Emergency Accounts	Pre-created high-privilege accounts in sealed storage
Access Criteria	Defined conditions that justify emergency access
Notification	Automatic alerts when emergency access is used
Time Limits	Auto-disable after defined emergency period
Post-Incident Review	Mandatory review of all emergency access use

Table 4: Break-glass procedure elements

Warning

Emergency access procedures must balance security with operational reality. Overly restrictive procedures that delay response to safety events are unacceptable. Test emergency procedures regularly to ensure they work when needed.

8 Implementation Approach

8.1 Phased Deployment

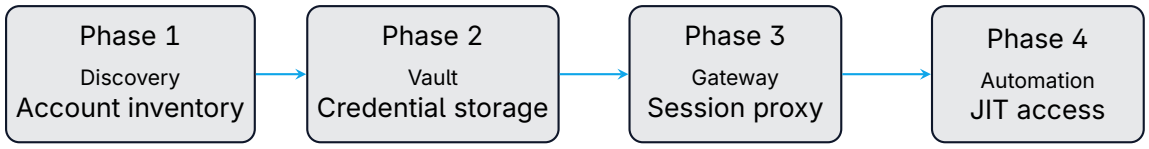

Figure 5: Phased PAM implementation approach

8.2 Priority Systems

Focus initial PAM deployment on highest-risk access:

1. Vendor and third-party remote access
2. Domain administrator and root accounts
3. Engineering workstations with OT access
4. Service accounts for critical applications
5. Local administrator accounts on OT systems

9 Summary

Key Takeaways

- **OT Privileged Access:** Includes not just admin accounts but vendor access, engineering workstations, and service accounts that can modify industrial systems
- **Vendor Risk:** Third-party remote access is a primary attack vector; implement approval workflows, time limits, and session recording
- **Jump Servers:** Force all administrative access through monitored bastion hosts in the DMZ
- **Credential Vaulting:** Centralize privileged credentials with automatic rotation; eliminate shared passwords
- **Session Recording:** Record all privileged sessions for audit and forensic capability
- **Emergency Access:** Maintain break-glass procedures that balance security with operational needs

10 Further Reading

Standards

- **IEC 62443-2-1** – Security program requirements for IACS asset owners
  https://webstore.iec.ch/publication/7030

- **NIST SP 800-53** – Security and Privacy Controls (Access Control family)
  https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

Resources

- **CISA Remote Access Guidance** – Securing remote access to OT
  https://www.cisa.gov/topics/industrial-control-systems
- **NIST SP 800-82** – Guide to ICS Security
  https://csrc.nist.gov/pubs/sp/800/82/r3/final

Books

- Bejtlich – *The Practice of Network Security Monitoring* (No Starch Press)
- Knapp & Langill – *Industrial Network Security* (Syngress)

Part of the OT Security Learning Series