Product Documentation

PAM
Security Hardening Guide

Contents

Security Hardening Guide

Introduction

This section outlines some of the best practices for securing your PAM instance, whether it be installed on a single server or in a multi-clustered environment.

Technical Support

If questions remain or issues arise while using PAM, please contact the Support team: https://support.imprivata.com/.

Implementation

It is critical to build a secure process around your PAM implementation.

This needs to include a layered approach to security (defense in depth) starting at the operating system, software updates, access to physical systems, protocols, system settings, backups, and personnel procedures.

General

- **Keep Host Operating System up-to-date.** Operating System (OS) vendors, whether commercial or open source, regularly released security patches that resolve vulnerabilities and improve system security. We recommend keeping your server up-to-date.
- **Backup At Least Daily.** Consider your Disaster Recovery plan.
- **Review System Log for Errors.** It is important to periodically check the OS System Logs for any recurring errors especially after system updates.

Database

- **Limit access to your PAM database.** When you create your PAM database or scheme, you must limit access to as few users as possible. PPAM encrypts sensitive data in the database using its Master password which is stored outside of this database (in the PAM User Directory). However, the database contains hierarchical structure and the permissions scheme that could be modified by a malicious user. Consider enabling monitoring of the PAM database scheme for unauthorized access.
- **Limit access to your database backups.** Database backups are critical for disaster recovery, but they also carry a risk if someone gains access. The PAM database is encrypted but you must still limit access to ensure that you are following “defense in depth.” Make sure to limit access to database backups to as few individuals as possible.
- **Don't store the database on a server that contains less sensitive databases.** Putting the database on a server with other less secure database instances can open up vulnerabilities. For example, an attacker might potentially use SQL injection on another application to access your privatePAM database.
- **Review Database vendor recommendations for SQL security.** Follow your database vendor’s recommendations for general security best practices.

Application Server

- **Use SSL / HTTPS**. Secure Sockets Layer (SSL) is required to ensure that all communication between the web browser and PAM is encrypted and secure (and not cleartext travelling across your network). It is suggested that you install a third-party certificate trusted by a major Internet authority, domain certificate, or self-signed certificate on your Web server.
- **Force SSL / HTTPS**. Even after you install an SSL certificate, users might still be able to access PAM through HTTP. To prevent access through HTTP, disable non-SSL traffic to the PAM server by disabling the open HTTP port 8080 in the server.xml file.
- **Limit access to your PAM directory**. It is important to limit access to your PAM home directory. This contains the PAM database and user directory connection information. These values are encrypted but remember "defense in depth." Try to grant access to as few users as possible.
- **Limit access to shared Content and Export directory**. It is important to limit access to your Content and Export directories. These directories contain session recordings, important certificates for integration with 3rd party systems as well as periodic system exports. Content and Export directories are shared between system nodes in the case of multi-node deployments.
- **Limit log on rights to the Application Server**. Administrators accessing the Application Server directly might attempt to monitor memory in use on the server. They also have better chances to access PAM home directory. PAM does several things to protect application memory but the best safeguard is to limit access to the Application Server to as few users as possible.
- **Secure traffic with Active Directory or other external user directories.** It is a good practice to setup integration with Active Directory through its SSL communication channel using the LDAPS protocol.
- **Limit access to PAM user directory.** The PAM user directory stores the master key and local PAM users with their passwords. In case of High-Availability deployments, the PAM User Directory is installed on each PAM node in replication mode. PAM user directory services can be accessed using the LDAPS protocol over port 10636. Make sure that this port is blocked by a firewall to access by anyone but the PAM server.
- **Limit access to PAM session manager.** The PAM Session Manager routes the session traffic and by default it listens on port 4822. The traffic handled by the Session Manager module is encrypted by SSL certificates. Make sure that the port is blocked by firewall by anyone but PAM server. Make sure that the traffic to all system Session Managers is secured with SSL certificate (watch for green session manager entry in the Administration / Settings / Proximity Groups configuration).
- **Protect your Master key**. The Master key for PAM is stored in the PAM user directory service. The Master key is obfuscated and encrypted, but "defense in depth" would require limiting access to the directory. Make sure you back up the original master key and store it in a very safe and secure location.

Application Settings

- **Secure the Local Admin Account.** When you create the first user in PAM, it is a privileged admin account that you can use when your domain is down. We recommend protecting this account with a very strong password. This password should be stored in a physical safe with limited access (there is no need to use this account except in emergencies where other accounts are not working, if AD is down or for some other reason).

- **Review Activity Reports.** It is a good practice to regularly review the activity and permissions reports. This can help find anomalies in system access.
- **Use Event Subscriptions or SIEM to notify of any security anomalies.** Event subscriptions can be used to send email alerts on various events in the system, and syslog can send PAM events to a SIEM tool for correlation. This might be used to notify administrators if there are failed login attempts or if certain Secrets are viewed, and so on.

Maintenance

Web Browser

AutoComplete

Browser AutoComplete allows web browsers to save the account credentials for the PAM login screen.

These credentials are often kept by the web browser in an insecure manner on the user's workstation.

Allowing AutoComplete also interferes with the security policy of your PAM deployment by not requiring the user to re-enter their login credentials on your desired timeout schedule.

Force Password Masking

Password Masking prevents over the shoulder viewing of your passwords by a casual observer (passwords show as *******).

The number of asterisks does not relate to the length of the password for added security.

Use the copy password to clipboard option instead of displaying the passwords on the screen to increase security.

Permissions and Authentication

Login Password Requirements

Passwords that are used by local users to log in to PAM can be strengthened by requiring a minimum length and the use of various character sets. Configure the password formula for local users to match policies of your organization.

Two-Factor Authentication

Users must authenticate to PAM at least once by using either local PAM credentials or their Active Directory credentials.

However, when a password gets compromised, you can protect yourself by enabling two factor authentication (MFA) in PAM.

When you use multiple factors of authentication, each factor must be a different type of information – that is, either a piece of information a user **knows**, **possesses**, or **is** (for example, when a fingerprint is used as a biometric identifier).

It is a good practice to protect logins to PAM using two-factor authentication.

Roles

PAM uses role-based access control, which allows administrative and user capabilities to be partitioned by these roles.

This can allow for granular control over which areas of the application a user has access to – for example, allowing someone the rights to view reports in PAM, but no other administrative permissions otherwise.

Separation of Duties

PAM administration workflows allow for the delegation of administrative function to different users.

The workflows can also create a dual-control environment where important administrative functions could only be performed with peer approval of other administrators.