Securden

Unified PAM

Security and Server Hardening Guide

Index

Hardening Securden at the Application Level

What is Security Hardening?

Security hardening is a process by which a server or a machine is rendered invulnerable to threats. Its achieved by reducing the threat surface significantly against all attack vectors. As a cyberdefense strategy, it is recommended to eliminate vulnerabilities at the application level, machine level and at the network level.

- At the application level, it is important to remove all unnecessary applications and files installed on the server.
- At the machine level, unnecessary permissions and unused user accounts should be removed. The firmware of the server and the applications installed should be free of known vulnerabilities and up-to-date.
- At the network level, the firewall settings and rules should be strictly monitored and controlled. Unused ports should be blocked, remote access points should be secured, unnecessary protocols and services should be disabled or removed. All network traffic should be encrypted.

This document explains the steps recommended to harden the security posture of the organization at the application level, device level, and at the network level.

Hardening Securden at the Application Level

Securden provides you with tools for secure access management right out of the box. We also recommend certain security best practices for you to follow and make your instance completely robust in nature. Some of the recommendations listed below should be verified from time to time.

Secure the local admin account

When you create the first user in PAM, it is a privileged local 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 notifications or SIEM to notify of any security anomalies. Event notifications 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 credentials are viewed, and so on.

Limit the number of super-administrators

You can choose to completely eliminate the super administrator role from your organization. (Since the super administrator is used for break glass scenarios, if you choose to not have any super administrators, you will not be able to take a complete backup of all passwords for offline use.) You should decide whether you want to have the super administrator role in Securden.

If you want to keep the role, you can also limit the number of super administrators allowed. The recommended approach is to create one or two super administrators and then completely turn off further creation.

Navigate to **Admin >> Customization >> Configurations** to enable or disable creation of super admins.

Limited administrative access

Reducing the number of privileged accounts and/or the extent of their privileges reduces the overall attack surface. This is true both for the enterprise as a whole and for each solution implemented, including Securden PAM. The core principle of this control is that there should only be a few Securden administrators, and they should only possess limited privileges unless elevated through a strong approval process.

If you want to keep the role, you can also limit the number of super administrators allowed. The recommended approach is to create one or two super administrators and then completely turn off further creation.

- Eliminate unnecessary Securden PAM administrative accounts.
- Reduce privileges of Securden PAM administrative accounts.
- Restrict administrators to only access accounts either owned by them or shared with them. (enabled by default)
- Require privilege elevation (with dual control or ticketing system integration) for system configuration changes or to access credentials that the Securden PAM administrator does not have a valid reason to access otherwise.
- Use the audit trails section to closely monitor Securden administration
- Require multi-factor authentication for all avenues of administrative access.

Protect sensitive accounts and encryption keys

Like many applications, the Securden PAM has sensitive accounts and encryption keys. These sensitive accounts come in two forms: administrators and super administrators.

- Ensure that access to the administrator and super administrator credentials requires more than one individual.
- Consider storing the super administrator password in a physical safe.
- Store the encryption key in a secure location.

Have a robust disaster recovery plan

Having a disaster recovery plan that specifically takes into account your organization's Securden PAM deployment, and periodically validating it will ensure that you can quickly recover your data and restore operations, in the unlikely event of a disaster.

A good disaster recovery plan begins with an assessment of the various risks, the likelihood of occurrence, and their impact. The disaster recovery plan needs to provide information about the physical infrastructure, key contacts, processes to access out-of-band credentials, and procedures to recover from likely and/or high-impact problems. Furthermore, it is important to ensure that Unified PAM is included and accounted for as a vital step in recovery as part of your general disaster recovery process, throughout the enterprise.

Login password requirements

Passwords that are used by local users to log in to Unified PAM can be strengthened by enforcing best practices such as requiring a minimum length and the use of various character sets. Configure the password complexity rules for local users to match the policies of your organization.

Multi-factor authentication

Users must authenticate to PAM at least once by using either local PAM credentials or their Active Directory credentials. However, as a contingency method for situations where the password gets compromised, you can protect yourself by enabling two-factor authentication (MFA) in PAM.

Role based access

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.

For example, granting someone the right to view reports in PAM, but no other administrative permissions otherwise.

Separation of duties

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

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

Steps to Harden the Securden Primary Server

Securden server component needs to be hosted on a dedicated, hardened machine. By default, the Securden installation directory contains all of the components required for Securden to function.

Create strong password for the Securden server

Create a long and complex password so that the server in which Securden is installed is secure. Eliminate password reuse and use a unique, strong password for the Operating System.

Have an exclusive service account

Use a unique service account for Securden in your domain controller. This service account should be used to run Securden and import users and accounts from Active Directory, Google Workspace, and other LDAP-compliant directories.

To start using the dedicated service account, run “services.msc” in the server where Securden is installed and navigate to the properties of the Securden PAM service. Replace the existing local system account with the newly created service account.

Disable remote access

Disable remote access to the PAM server for all normal domain users in your company using domain group policies. Only one or two domain administrators should have write permissions to the Securden PAM drive or folders, and all other administrators should only have read permissions.

Set up firewall rules

Set up inbound and outbound firewalls to protect against incoming and outgoing traffic. This parameter can also be used to specify which server ports must be opened for various operations including password management and remote connections to target IT assets.

Other recommendations for hardening the Securden primary server

Securden and its associated services are sensitive assets. The core principle of these recommendations is to treat Securden infrastructure with the highest level of security.

- Do not install other applications on the Securden Server, as it is detrimental to hardening the component server.
- Limit the user accounts that can access Securden servers (Primary and secondary application server). Ensure that any domain accounts used to access Securden servers are unable to access domain controllers and other member servers and workstations.
- Use network-based firewalls and IPsec to restrict, encrypt and authenticate inbound administrative traffic.

- Enforce application whitelisting and limit access to authorized applications.
- Apply Microsoft security updates regularly.

Steps to Harden Securden Application Servers

Limit access to your PAM installation folder

It is important to limit access to your PAM installation folder. This contains the PAM database, user and accounts related information, audit reports, session recordings, etc. These values are encrypted but for employing a security model that aligns with the “defense in depth” strategy, grant access to as few users as possible.

Securden has various provisions for protecting the database. However, it is advisable to grant access to the Securden server and the database server to a few users at the maximum. The database server is accessed only through the primary server, but in the case of distributed deployments, the database server is shared between the primary server and the secondary application server.

Restrict 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 the PAM installation folder. Unified PAM has several measures 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 the Active Directory

It is a good practice to set up integration with Active Directory through a SSL communication channel using the LDAPS protocol.

Secure sessions routed through the Securden Session Manager

The Securden Session Manager (SSM) routes the session traffic and by default, it uses RDP port 3389. For added security, it is recommended to enable SSH tunneling for the remote connections launched from Securden.

Steps to Harden the Network

Network hardening is recommended to protect against vulnerabilities involved in establishing connection and communication from the primary server to the secondary server, the session manager to the primary server, and the server to the endpoints. You can use secure communication protocols and restrict access to network devices to eliminate network-based vulnerabilities.

Use secure protocols for communication

The use of insecure protocols can easily render other controls invalid. To reduce the risk of eavesdropping and other network-based attacks, use the following encrypted and authenticated protocols for secure communication.

- HTTPS for REST APIs

- LDAPS for the Digital Vault LDAP integration
- RDP/TLS for connections to the SSM
- SSH (instead of Telnet) for Password Management
- TLS for RDP, SMTP, and Syslog

We recommend that you only utilize TLS V 1.2t as a best practice. The steps to do so are outlined below. Navigate to **<Securden Installation Folder>/conf** and open the server to enable TLS 1.2 in Securden. Open the properties file in a text editor of your choice and change the value to True, as shown below.

SERVER_TLS_V1.2_ONLY = False to SERVER_TLS_V1.2_ONLY = True, and ensure to save the changes before closing the text editor.

Validate proper server roles

Server roles can be set using the Server Manager. Ensure that the unnecessary roles are not installed on the server

Restrict network protocols

Install only the required protocols and remove unnecessary ones.

For example, only TCP/IP is necessary, and ensure that no additional protocols such as IPX or NetBEUI are allowed.

Restrict access to the UI by blacklisting and whitelisting IP addresses

Users, APIs, native mobile applications, and browser extensions will attempt to communicate with the Securden Unified PAM server once it has been installed in your environment.

You can impose IP address-based limitations on this kind of communication using Securden. We strongly advise you to limit the number of client systems that can connect to the Securden Interface.

To set up IP address-based restrictions, go to **Admin >> Security >> IP Address Restrictions**. The IP restrictions can be configured at different levels and in different ways - for example, using defined IP ranges, specific IP addresses, or CIDR notation. Specific IP ranges and addresses can be added to the **Restrict Access** list if you prefer to restrict access rather than just allow it. If you want to impose additional restrictions you can block access to any of the above features. To block extensions, APIs, and mobile apps, navigate to **Admin >> Block Access**.

Restrict Securden web server to a bound IP address

Securden's web server will automatically bind to all of the accessible IP addresses on the server where the application is installed. As a result, Securden PAM will be accessible via any IP address using the configured port (5959). To restrict this, we advise you to configure the web server up to bind to a single IP address and only accept incoming communications from that IP address. To configure the bound IP address, follow the steps below.

1. Stop '**Securden PAM Service**' from services.msc if running.
2. Open the "server.properties" file present in the \conf folder.
3. Change the value of "**ENABLE_SERVER_SPECIFIC_HOSTNAME_ONLY_ACCESS**" from **False** to **True**. Specify the IP address/FQDN or the server name against "**SERVER_ACCESS_HOSTNAMES =**" (If you are specifying multiple hostnames, ensure that it is specified in the comma-separated form)

General Hardening Tasks

This section outlines the manual hardening procedures that are part of system maintenance and are required for all deployment types. You should carry them out on a regular basis, such as when you make changes to the environment (such as adding servers or upgrading hardware), and as part of routine maintenance.

Update your operating system

Microsoft releases periodic updates (security updates and service packs) to address security issues that have been discovered in their software. Make sure your operating system is updated to the latest version. Keep the 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.

Install an anti-virus solution

Servers without anti-virus protection are exposed to two risks:

- Server infected with viruses that might damage the server and the entire network.
- Trojan horses are planted to allow remote control of the server and to all the information on it.
- Install an anti-virus solution and update it as needed.

Rename default accounts

It is recommended to change the names of both the administrator and the guest account to names that don't provide information about their permissions.

It is also recommended to create a new locked and unprivileged administrator user name as bait.

Regular backups

Backup at least once a day and store the backup copies in a secure location. The corresponding encryption key with which the backups are encrypted should also be stored in a secure location. Ensure the location in which the key is stored is different from the location in which the backup file is located.