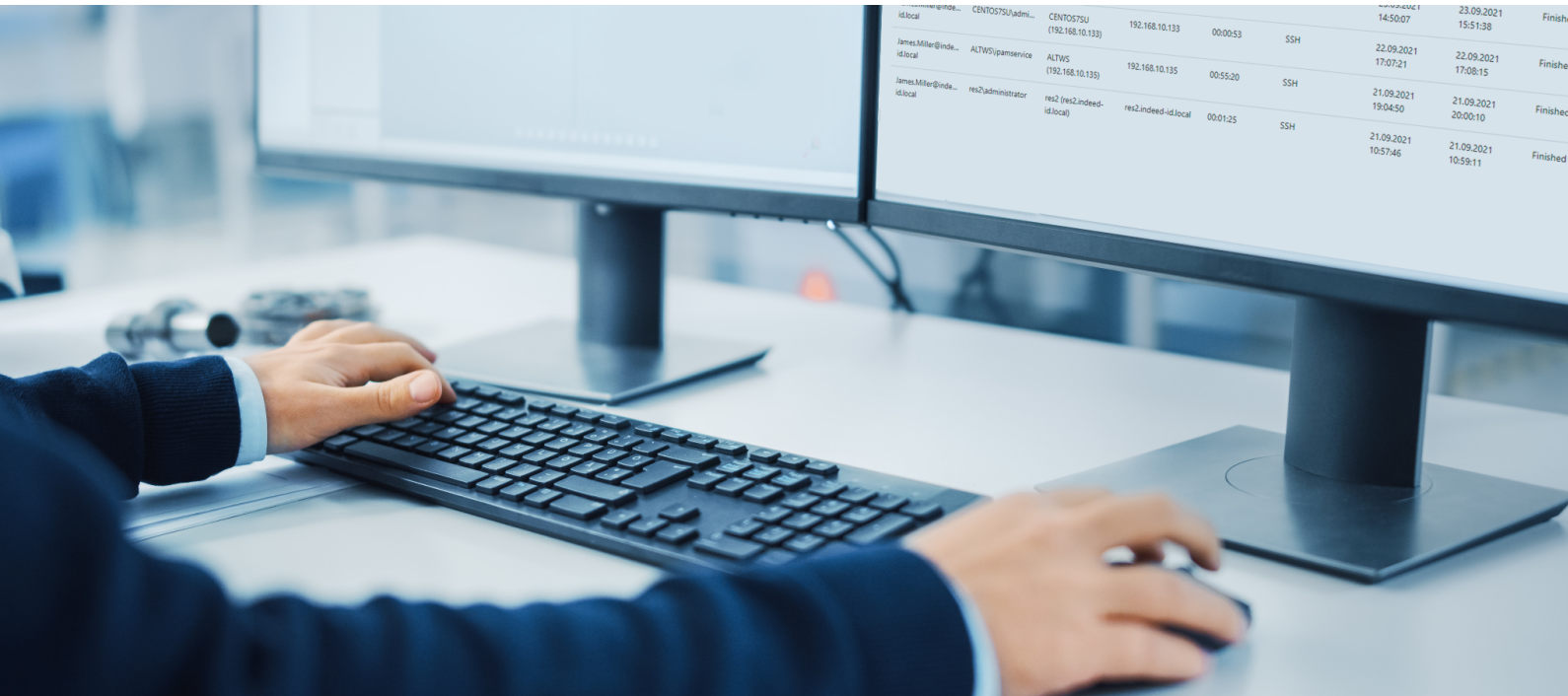
Axidian

WHITE PAPER

Axidian Privilege

Managing Privileged Access to Corporate IT Systems



Contents

Privileged access – a potential security threat

As corporate IT infrastructure continues to grow in size and complexity, privileged access management is becoming a top priority for ensuring cybersecurity. The growing number of information systems and the variety of access scenarios can make this task rather challenging. A malicious user with access to an administrator account can cause your company way more serious damage compared to regular staff with compromised credentials. Administrative accounts can be used to disable the security system, stop the operation of information systems, and gain access to confidential information. Ensuring privileged access security is a sophisticated task; it cannot be achieved by relying exclusively on common approaches to the protection of credentials and requires specialized solutions.

Privileged users

Privileges may be assigned to various categories of in-house and external personnel, which means that all these users can gain access to essential information and critical hardware and software functions.

IT administrators

Each device and application or system software has its own administrator accounts. The fact that administrators should have privileged access rights is self-evident. The list of such personnel may include:

- Active Directory administrators
- Network equipment administrators
- Database administrators
- Server administrators (Windows, Unix/Linux)
- VDI administrators

Business users

Even though business users do not have administrative rights, they may still have wide-ranging privileges in specific information systems. For example, they may be able to transfer money, manage the production process, and gain access to data marked as trade secret.

Contractors and partners

Contractors' employees are normally responsible for maintenance of specialized software and hardware. They may work for a vendor or integrator. These users usually have remote access to corporate infrastructure, which can make the oversight of their operations rather challenging.

Service accounts

Service accounts are needed for process automation. They are utilized to run various services, daemons, scripts, and other software. You can easily forget about such accounts since employees don't use them explicitly every day. And this is why they may be even harder to manage.

Privileged access management

If you want to manage and protect your corporate privileged access effectively, make sure that you do the following:

- Centrally manage user access to controlled resources.
- Prevent uncontrolled use of privileged accounts, i.e. discover them and take them under control. Keep the passwords secret, perform regular checks, and change passwords to random values.
- Reduce the number of privileged accounts required to manage your corporate information systems. Keep an access log containing records of all attempts to use privileged accounts (it must clearly state which employee gained access to which account and when).
- Use multi-factor authentication for access to privileged accounts.
- Apply special mechanisms for investigating incidents and restoring the sequence of events.

Axidian Privilege is a system for management of access to corporate infrastructure under privileged accounts. Below you will learn how Axidian Privilege can help you solve these problems.

Centralized access management

Axidian Privilege keeps the information about all privileged accounts and related permissions for their usage. Permissions are the key tool used for granting privileged access in Axidian Privilege. Permissions are used to define the following access parameters:

- Who – which users or user groups have access.
- Where – which servers, hardware, and applications users can work with.
- Access rights – which account will be used for connection.
- Conditions – access period and schedule, the types of protocols to be used.

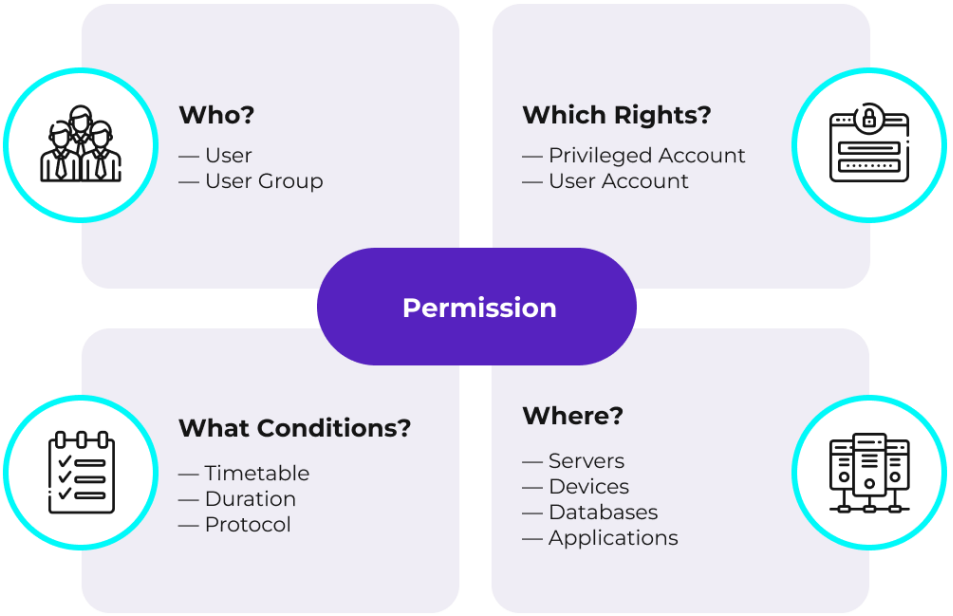


Figure 1. Access permission settings

Permissions are centrally assigned by an administrator in the Axidian Privilege management console. Permissions may be temporarily suspended or revoked if access is no longer required. Axidian Privilege supports integration with Service/Help Desk systems. Thanks to this option, your personnel may continue using the same familiar system to request access approvals, while permissions will be automatically granted and revoked via Axidian Privilege as part of a routine workflow. Axidian Privilege offers two interaction paths for this purpose: a command-line utility and an API.

The system has another access management tool besides permissions – the Axidian Privilege policies. Policies are used to define general access parameters such as:

- Permitted and forbidden commands in SSH sessions
- Whether or not the PAM administrator's approval is required to open privileged sessions
- PC local resources available on a remote resource (disks, clipboard, etc.)
- Whether or not a privileged account password should be reset after the end of a session
- Exclusive mode for privileged accounts (one account can be used to initiate one session only)
- The maximum duration of a privileged session

Controlled use of privileged accounts

Axidian Privilege relies on four mechanisms to exercise control over the use of privileged accounts:

- Privileged account discovery
- Credential storage
- Password and SSH key rotation
- Secure use of credentials

Privileged account discovery

Axidian Privilege incorporates Account Discovery, an engine designed for running regular searches for new accounts across the connected resources and domains. You can customize the search frequency and set different frequency for independent groups of resources. Upon discovery of a new account that is not yet registered in the PAM system, relevant information is added to the credential repository. In addition, the relevant event is recorded in the log, and the administrator may opt to get email notifications about such events, so that he/she can make a prompt decision regarding the use of the new account. Axidian Privilege supports account searches for the following types of resources:

- Windows PC and servers[1]
- *nix systems
- DBMS (MS SQL, MySQL, PostgreSQL, Oracle DB)
- Active Directory

Credential storage

Axidian Privilege is used as a centralized repository for privileged credentials that can only be accessed with a valid permission. Without appropriate permissions, even the PAM administrator will not be able to view passwords and SSH keys.

In addition to storage, Axidian Privilege performs regular checks of passwords and SSH keys to make sure that all credentials in the system are up to date. In the event of a mismatch, the administrator will be notified accordingly.

Password and SSH key rotation

Axidian Privilege changes passwords and SSH keys to random values according to a set schedule in order to maintain their security. You can customize the complexity of generated passwords in line with your company's security policies.

All previous passwords and SSH keys are also stored in the PAM password history, so you can “roll back” a password or a key to any desired point in the past. This function will be essential if you need to restore a target resource using a backup copy, and you need the credentials applicable at the time of creation of the backup copy.

Secure use of privileged credentials

With Axidian Privilege, your company can choose to avoid explicit use of privileged credentials by your personnel. Administrators in charge of servers, network equipment, Active Directory, and application systems no longer need to have administrative credentials – PAM can do this job on their behalf. Your staff member can connect to PAM with their user account; a new session will be started on the target resource under the account with appropriate rights. This way you can prevent uncontrolled use of privileged accounts and make sure that your personnel can no longer keep their credentials in an insecure place (in a file stored on the desktop or network drive, on stickers, etc.) or intentionally disclose passwords to third parties.

[1] The current version supports local user account searches, and future versions will feature searches for service accounts used to run services and scheduled tasks.

Axidian Privilege allows you to enable exclusive mode for your most important privileged accounts. In the exclusive mode, the privileged account can be used to launch one session only. This can help you avoid problems that may arise if simultaneous changes are made in the managed systems.

Single Sign-On

With Axidian Privilege, new sessions are launched with transparent transfer of credentials to the target resource, and this option is available not only for classic remote access protocols such as RDP, SSH, or Telnet. The system includes a specialized SSO agent (Single Sign-On agent) that can automatically fill credentials in web and desktop applications. Thanks to the SSO agent, Axidian Privilege can offer transparent access to network hardware administration web interfaces, fat DBMS clients, and other apps.

Application to Application Password Management[2]

Not only personnel can have accounts with broad access rights. Many automation tools (apps, scripts, etc.) rely on service accounts to perform their functions. Axidian Privilege offers an API for obtaining up-to-date service credentials so that you can eliminate the necessity to save passwords in scripts and configuration files. All operations that have to do with obtaining new passwords will be recorded in the PAM log, and all passwords will be changed to random values after a specified period of time.

Reduced number of privileged accounts

The Account Discovery tool can help you promptly identify the accounts that your administrators and information security staff may have forgotten about (for example, temporary accounts that have not been deleted or disabled in due time). Thanks to this regular “stocktaking”, you can keep your pool of privileged accounts up to date and avoid redundancy. This, in turn, can help you reduce the potential attack surface and enhance cybersecurity in your company.

With PAM, in some cases you may choose not to create personal accounts for administrators altogether and keep the number of privileged accounts at a minimum. Axidian Privilege records all events that have to do with access to managed resources and keeps logs of

- Employees who gained access to a resource
- Resources to which access was granted
- User accounts used to gain access to resources
- Session date and time
- Session duration
- Utilized access protocols

This way, even if anonymized accounts are used for access to resources (administrator, root, etc.), PAM will still have the information about your employees who performed specific operations.

[2] The Application to Application Password Management feature will be added in v.2.7 in III quarter 2022.

Multi-factor authentication

Talking about privileged accounts, it is essential to have strong authentication methods in place in order to ensure that only legitimate users can gain access to corporate resources. Out-of-the-box, Axidian Privilege supports two-factor user authentication that includes a password and an OTP (One-Time Password). Users are expected to use an app installed on their smartphone to generate one-time passwords.

If your company relies on the standard Windows tools for user authentication, including smart cards and digital certificates, you may continue to use this authentication method in Axidian Privilege.

Incident investigation

Privileged sessions can potentially cause disruptions in the standard operation of information systems or result in unwanted behavior. Also with works outsourced to contractors, you cannot always be sure that they have been duly performed to the full extent. In this case, it is essential to be able to identify the exact modifications made in the system, as well as the authors of these changes.

Axidian Privilege can capture user actions in the following formats:

- Video recordings showing the entire screen. You can customize video parameters such as image quality, resolution, and frame rate.
- Screenshots taken at regular intervals. This feature can be useful if you want to save disk space and record non-critical sessions.
- Session text logs. For SSH sessions, all user input/output activity is recorded; for RDP sessions, initiated processes, the titles of active windows, and user input are captured.

PAM administrators have the option to view sessions both in real time and after they end. An administrator who monitors an active session can terminate it in the event of suspicious behavior.

All session materials (videos, screenshots, and text logs) can be downloaded for viewing and analysis in third-party solutions.

Axidian Privilege composition

Figure 2. Axidian Privilege structure

Axidian Privilege includes the following logical and functional modules.

Policies and permissions

Policies and permissions are used to define the following privileged access parameters:

- Persons who are granted access to resources.
- Accounts to which access is granted.
- Resources (servers and hardware) to which access is granted.
- Timeframe (permanent/temporary access, access during business hours, or at any time).
- Type of session records (video recordings and text logs, text only, screenshots, etc.).
- Local resources (disks, smart cards) that will be available to the user during the remote session.
- The user is authorized/not authorized to view the privileged account password.

Centralized policies can help you reduce the cost of system administration and make the access parameters and rights transparent to information security professionals and auditors. For more information about policies and permissions, please see the Centralized access management section.

Credentials

The credentials (usernames, passwords, and SSH keys) required for access to resources are stored in a vault that can only be accessed by the Axidian Privilege server. Strong encryption algorithms are used to encrypt the data for storage and transmission from/to the server. Access to the vault is restricted and reserved exclusively for the PAM server. This is made possible thanks to a special procedure, whereby the database server is hardened.

Users

PAM users are employees who are assigned privileged access rights via the PAM system. Axidian Privilege uses Active Directory as a user directory. User accounts are utilized for gaining access to the user console, access server, SSH Proxy, and management console.

Resources

A resource in Axidian Privilege is an object to which access is granted. In most cases, this means Windows and Linux servers. A specific application can also be a resource, for example, an app designed for managing DBMS or a web-based router configurator.

Sessions

All privileged sessions are recorded and saved in the Axidian Privilege archive. All records in the archive are encrypted and can only be accessed by users with appropriate PAM roles. Sessions can be recorded in the following formats:

- Text logs are kept at all times and include the following data:
  - All input and output in the console for SSH connections
  - All processes launched, windows opened, and keyboard input for RDP connections
- Video recordings are available for both RDP and SSH connections. Video recordings are optional and can be enabled in the policies by the PAM administrator. Video quality can be adjusted; you may set independent settings for different user accounts. For example, you may record domain administrator sessions with maximum quality and operator sessions with compression.
- Screenshots are also available for both RDP and SSH connections. Screenshots are optional and can be enabled in the policies by the PAM administrator. Screenshot frequency and quality can be customized in the policies.

The PAM administrator can monitor active sessions in real time and terminate the session if needed.

Roles

The roles assigned to users determine their rights in the Axidian Privilege management console. Three roles are available by default:

- Administrator – full access to all PAM functions and settings.
- Operator – authority to assign and revoke permissions.
- Inspector – read-only access.

You can change the privileges assigned for each role and adapt them to your company's needs. If you want to set a more nuanced division of authorities, you can create your own roles.

Event log

The event log is stored on a dedicated Axidian Privilege server. Any activity of PAM administrators and users is stored as events. All changes in the system parameters will be logged, as well as user information and used to account for all connections to target resources.

For easy integration with SEIM and timely response to incidents, events may be sent via syslog to a third-party log server.

Access server

The access server implements a centralized privileged access model. First, a user is connected to the access server to complete permissions check and two-factor authentication, and then a new session on the target resource is launched.

The access server is powered by Microsoft RDS (Remote Desktop Services) server with pre-installed Axidian Privilege components. Upon connection to the access server, a specialized Axidian Privilege application is launched as a desktop shell with the following functions:

- User access rights check – permissions to access the desired target resource under the requested account.
- User authentication – before a new session can be launched, a user must provide the second factor to complete 2FA.
- Video recordings and screenshots of the session.

The following client software is used to start new sessions on the target systems and applications on the access server:

- Microsoft RDP client (mstsc) for Windows server connections
- A browser for web application connections
- PuTTY client for SSH and Telnet connections
- Specialized client software for connections to various information systems via proprietary protocols (fat client)

SSH Proxy

SSH Proxy is a main way to connect to Linux/Unix systems via Axidian Privilege. This method has the following advantages:

- You don't need to use Microsoft RDS
- You can use any SSH client
- The SSH client runs locally on the user workstation

SSH Proxy and the access server have similar functions:

- User access rights check
- User authentication

- Session text log (all SSH input/output is recorded)

With SSH Proxy, users can work with the same SSH client as usual to initiate connections from their workstation. The SSH Proxy address should be indicated as the connection server. All users trying to connect to SSH Proxy will be prompted to provide the second authentication factor, and then a new session will be launched on the target resource.

Filter for commands

In SSH sessions, the PAM administrator has the option to make a list of permitted and forbidden commands for specific target resources (the list of resources is set by the scope of a relevant policy). Two modes are available for the command filter:

- Anything that is not forbidden is allowed. In this case, the administrator should specify the list of forbidden commands.
- Anything that is not allowed is forbidden. This is a more rigid filter where the administrator should expressly indicate the allowed commands and disable all other commands.

Regular expressions are used to describe the commands. You can set the following reactions in response to a forbidden command entry:

- Terminate the session.
- Abort the command.

SFTP and SCP[3]

In addition to the SSH protocol, SSH Proxy also supports SFTP and SCP for connections to target resources. The procedure is similar to SSH connection, i.e. a user should indicate SSH Proxy address as the connection server. All users trying to connect to SSH Proxy will be prompted to provide the second authentication factor, and then a new session will be launched on the target resource.

For SFTP and SCP protocols, SSH Proxy creates a session text log that captures all file operations performed by the user.

PAM server

The PAM server is the central module of the Axidian Privilege system responsible for data exchange and smooth operation of other modules. The key needs addressed by the server are as follows:

- Centralized management of all system data (users, resources, credentials, permissions, policies, etc.)
- Encryption of critical data in the PAM database (privileged credentials, etc.)
- Executing scheduled tasks (user account searches, password rotation, etc.)
- Provision of an API for integration with third-party systems

Identity Provider (IDP)

The Identity Provider (IDP) module enables two-factor user authentication for access to all

[3] The SFTP and SCP support will be added in v.2.7 in III quarter 2022.

system components. The first factor is the user's domain password, and the second factor is a one-time password (OTP) generated in the app installed on the user's smartphone.

Upon first login to the management console or user console, users are prompted to register the OTP app. After successful registration, they are granted access to the system.

Besides user login, IDP is also instrumental in the authentication of applications that rely on the PAM server API.

Connectors

Connectors have a number of functions in the privileged account management:

- Routine searches for new privileged accounts on the target resources. This is a protective measure against unscrupulous administrators that may create special accounts to bypass the PAM system.
- Routine checks of passwords and SSH keys to privileged accounts. This feature can help you make sure that all credentials in the PAM vault are up to date and malevolent administrators cannot bypass the PAM system by resetting the password.
- Routine password and SSH key change. Axidian Privilege can generate random complex passwords and SSH keys for managed privileged credentials, thereby protecting them from unauthorized usage.
- Password reset after disclosure to the user. The PAM administrator may allow the users to view passwords to privileged accounts if they need to use such a password explicitly. In this case, Axidian Privilege will reset the password to a new random value after a certain period of time.

Axidian Privilege includes connectors for the following target systems:

- Active Directory connector
- Windows and Windows Server connector
- SSH connector for Linux/Unix connections in various distributions
- DBMS connector (MS SQL, Oracle, PostgreSQL, etc.)

Management console

The management console is a web application that serves as an interface for system customization and audits. Administrators use the console to grant users access to credentials and resources, set up access policies, and view event logs and privileged session records. The console can also be utilized for real-time monitoring of active privileged sessions that can be terminated by the PAM administrator if needed. Users must complete two-factor authentication to gain access to the management console.

User console

The user console is made as a web application. The console features all the permissions granted to the user; he/she can run searches by address or resource name, connection protocol, or account name. After locating the desired resource for connection, the user should download an RDP file that contains the required parameters. This file can be saved

and used again; you do not need to download a new file every time. For SSH resources, you can copy the connection string to clipboard and use it with any SSH client.

Users can also use the console to view the privileged credentials for which they have permissions. Two-factor authentication is required for gaining access to the user console.

Axidian Privilege key features

Access protocols	RDP SSH HTTP(s) Telnet SFTP SCP Any protocol via client publication
Supported types of credentials	Login + password SSH key
Privileged account search and password management	Windows Linux Active Directory DBMS (MS SQL, PostgreSQL, MySQL, Oracle, etc.)
Supported user directories	Active Directory
Two-factor authentication technology	Password + TOTP (password generation algorithm)
Supported session log types	Text log Video recordings Screenshots
Remote access technologies	Microsoft RDS SSH Proxy

About Axidian

Axidian is a global IT security vendor with a corporate center located in Dubai, UAE, and branches in Lithuania and Singapore. We provide authentication, comprehensive access management, privileged access management (PAM), public key infrastructure (PKI) management and identity threat detection and response solutions.

Axidian is where security finds its Axis.

If you have any questions about our products or interested in more detailed information on those, please visit axidian.com.