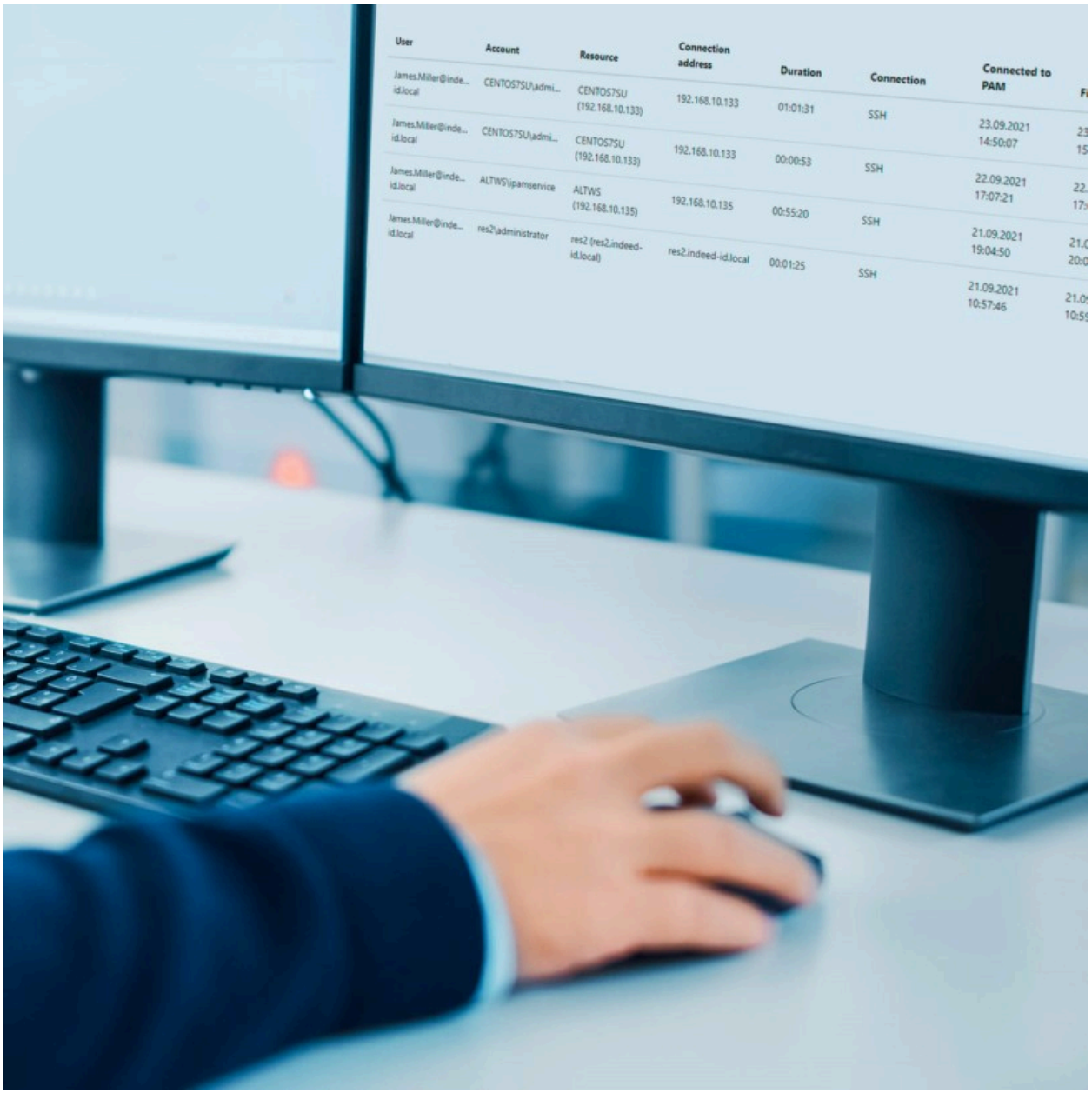


Axidian Privilege

Technical Documentation

Version: 3.5

Date: 2026-09-29

Contents

Overview 5

Components 6

Licensing 15

System Requirements 22

- Server components 23
- DBMS 41
- User workspace 42

Deployment Architecture 43

Installation steps 53

Preparation for Installation 55

- User Directory Accounts 56
- Certificates 60
- Databases 64
- Media Storage 68
  - SMB Storage 69
  - NFS Storage 70
  - S3 Storage 78
- Servers 80
- IIS Web Server 83
- Accounts for Installing PAM via Web Wizard 84

Installation 85

- Basic on Windows 86
- Basic on Linux 103
- Fault Tolerant on Windows 120
- Fault Tolerant on Linux 137

Setup 154

- Additional Components 155
  - PamSU 156
  - Privilege Agent 159
  - Desktop Console 160
- Syslog Server 161
- RDP File Signature Configuring 165
- Enabling Restart of Proxy Service Containers 169
- Appendix A. Configuration files 173

PAM Configuration Change 176

Security Recommendations 180

- Backup Accounts 181

Security of Passwords and Secret Keys 182
Process Filtering and File Security 187
Session Logs Encryption 193
Access Server Security Policy 194
Access Server Security Settings 307
Changing the Encryption Key of the PAM Database 310
Authentication 318
X.509 Certificate 319
OpenID Connect Protocol 322
RADIUS Configuring 327
Kerberos Authentication 330
TOTP Second Factor via Email Setup 351
Service Operations 352
Administration 356
Management console 359
Users 361
User Groups 375
Resources 381
Setting Up a Service Connection for Resources 403
Checking Key Fingerprints of SSH Server 408
Services 413
Resource Groups 419
Accounts 425
Account Operations 430
Bulk Operations for Accounts 440
Domains 441
Adding a Domain 443
Configuring Service Connection for Domains 444
Domain Operations 445
Bulk Operations for Domains 448
Structure 449
Permissions 452
Action Requests 459
Active Sessions 462
All Sessions 463
Events 465
Reports history 466
Notifications 470
Configuration 471
Specifying the Length of a Video Segment when Recording an RDP Session 492
Connector Creation Tool Usage 493

Roles 503
Applications 505
First Launch 510
Policy Setup 513
Configuring User Connections via SSH keys 541
Dumping Passwords 543
Usage of PostgreSQL and MSSQL Proxy 546
Usage of Web Proxy 550
Dashboard 553
User Manual 559
User Console 560
Connection to the Resource 565
RDP, SSH, Web and SQL Connection 566
SCP/SFTP Connection to the Resource 582
Command Line 583
WinSCP 586
FileZilla 589
Authentication in SSH Proxy via SSH key 590
Additional Utilities 594
Usage of PamSu 595
Usage of Desktop Console 596
Automation 597
Integration with Ansible 598
Ansible Lookup Plugin 599
Connecting via SSH Proxy 611
AAPM Reference 629
Python SDK 630
AAPM API 643
Console Tool 652
ConsoleApp 656
Troubleshooting 685
Certificate issues 686
Technical Support 693
Logs 696
Collecting Logs of Server Components 697
Collecting Logs of Client Components 712
References 715
Events 716
Claims 734
Mapping user directory and PAM attributes 742
What's new 746

Overview

Axidian Privilege is a software solution for managing privileged user access to a company's IT systems.

A single point of access for privileged users to target resources.

Components

Management Server

The Management Server is the main component of Axidian Privilege, which manages the operation of all components and performs the following tasks:

- Centralized management of all data in PAM.
- Encryption of critical data in the database, such as privileged user passwords.
- Monitoring of all actions and their recording in the audit log.
- Scheduled tasks, such as discovering new accounts on a resource or SSH key rotation.

Axidian Privilege Core

The central component of the Management Server that controls all Axidian Privilege objects.
The component performs the following tasks:

- Management of accounts, resources, and domains.
- Granting of permissions and revocation of access rights
- Launching and monitoring sessions.
- Policy enforcement.
- PAM audit and event logging.
- Background operations, such as domain synchronization or resource access verification.

Component composition and execution environment

Infrastructure	Windows	Linux
Execution environment	Windows Server 2016–2022	Docker
Web server	Internet Information Services (IIS)	Nginx
Web application	core	core

Axidian Privilege IdP

IdP (Identity Provider) — the authentication center for Axidian Privilege users and components. The component performs the following tasks:

- User authentication when accessing PAM, including two-factor authentication.
- Authentication of Axidian Privilege components.
- Application authentication using the API.

Component composition and execution environment

Infrastructure	Windows	Linux
Execution environment	Windows Server 2016–2022	Docker
Web server	Internet Information Services (IIS)	Nginx
Web application	idp	idp

Axidian Privilege Management Console

A web application for managing Axidian Privilege. In the administration console, you can configure access to resources, grant permissions for opening sessions, export logs, or view statistics. For more information about working in the console, see the Administrator's Guide.

Component composition and execution environment

Infrastructure	Windows	Linux
Execution environment	Windows Server 2016–2022	Docker
Web server	Internet Information Services (IIS)	Nginx
Web application	mc	mc

Axidian Privilege User Console

A web application for accessing protected objects in Axidian Privilege. Through the user console, you can connect to a resource and open a session in accordance with the permission granted. For more information about working in the console, see the User Guide.

Component composition and execution environment

Infrastructure	Windows	Linux
Execution environment	Windows Server 2016–2022	Docker
Web server	Internet Information Services (IIS)	Nginx
Web application	uc	uc

Axidian Log Server

A Management Server component responsible for collecting, processing, and storing events.

Component composition and execution environment

Infrastructure	Windows	Linux
Execution environment	Windows Server 2016–2022	Docker
Web server	Internet Information Services (IIS)	Nginx
Web application	ls	ls

Access Server

The Access Server is a link between the user and the target resource to which access needs to be granted. Resources can be servers, databases, websites, or applications.

When a user opens a session, for example by executing a copied SSH command in a terminal to connect to a resource, authentication in PAM occurs. The Access Server then verifies the user's permissions and, if authorized, provides access to the target resource.

Axidian Privilege Gateway

A set of applications and clients that provide access to Windows resources using RDP/SSH/Telnet protocols in RemoteApp mode. The component records video of the session and saves its artifacts: text logs, screenshots, and transferred files.

The component is automatically deployed to the RDS Access Server during PAM installation. The server requires deployment of the Remote Desktop Services role.

Component composition and execution environment

Execution environment: Windows Server 2016–2022

Composition:

- ProxyApp.exe application
- File system driver Pam.FsFilter
- Service for Pam.FsFilter interaction Pam.Service
- Modified SSH client Putty.exe
- Extension for mstsc.exe
- Set of FFmpeg utilities and libraries
- Process launch control module Pam.Proxy.ProcessCreateHook

Axidian Privilege RDP Proxy

A proxy server that provides access to Linux resources using the RDP protocol without exposing privileged account credentials. The component records video of the session and saves its artifacts: text logs, screenshots, and transferred files.

The component is automatically deployed to the RDP Access Server during PAM installation and requires no additional configuration.

Component composition and execution environment

Execution environment: Linux

Composition: Docker container pam-rdp-proxy

Axidian Privilege SSH Proxy

A proxy server that provides access to resources using SSH, SCP, and SFTP protocols. The component saves text session logs and transferred files.

The component is automatically deployed to the SSH Access Server during PAM installation and supports various SSH clients.

Component composition and execution environment

Execution environment: Linux

Composition: Docker container pam-ssh-proxy

Axidian Privilege PostgreSQL Proxy

A proxy server that controls access to PostgreSQL databases. The component simplifies connection to PostgreSQL, provides users access without exposing privileged account credentials, and maintains text logging of SQL sessions. The component supports various database management clients.

PostgreSQL Proxy is automatically deployed to the PostgreSQL Access Server during PAM installation.
For information on how to configure the component and open SQL sessions, see Usage of PostgreSQL and MSSQL Proxy.

Component composition and execution environment

Execution environment: Linux

Composition: Docker container pam-sql-proxy

Axidian Privilege MSSQL Proxy

A proxy server that controls access to Microsoft SQL Server (MSSQL) databases. The component simplifies connection to MSSQL, provides users access without exposing privileged account credentials, and maintains text logging of SQL sessions. The component supports various database management clients.

MSSQL Proxy is automatically deployed to the MSSQL Access Server during PAM installation.
For information on how to configure the component and open SQL sessions, see Usage of PostgreSQL and MSSQL Proxy.

Component composition and execution environment

Execution environment: Linux

Composition: Docker container pam-tsql-proxy

Axidian Privilege Web Proxy

A proxy server that provides secure access to web applications and websites through a browser without the need to use Microsoft RDS. Web sessions are launched directly from the user console. The component supports video logging of sessions.

Web Proxy is automatically deployed to the Web Access Server during PAM installation.
For information on how to configure the component and open web sessions, see Usage of Web Proxy.

Component composition and execution environment

Execution environment: Linux

Composition: Docker container pam-web-proxy

Axidian ESSO Agent and Axidian Admin Pack

A set of components for automatic form filling in authentication forms for web resources and applications. The components are installed on the RDS Access Server and automatically populate user credentials during a session opened in RemoteApp mode.

Component composition and execution environment

Execution environment: Windows Server 2016–2022

Composition:

- Set of applications, services, and tools for interacting with authentication forms and Axidian Privilege components
- Extensions for browsers Internet Explorer, Google Chrome, Microsoft EDGE

Clients

Axidian Privilege Web Terminal

The Web Terminal is a client that allows you to launch RDP and SSH sessions directly from your browser via the RDP Proxy and SSH Proxy components. Proxy servers provide control and recording of sessions opened through the Web Terminal.

Component composition and execution environment

Execution environment: Linux

Composition: Docker container pam-web-terminal

Additional Components

Axidian Privilege Agent

A component for text logging of RDP sessions. The log contains records of active window changes, application and process launches, as well as keyboard input data.

For more information about installation and configuration, see the Privilege Agent section.

Component composition and execution environment

Execution environment:

- Windows Server 2012R2–2022
- Windows XP SP3 x64
- Windows 7 x64 and higher

Composition:

- Service Pam.Proxy.WindowsAgentService
- Application Pam.Proxy.WindowsAgent

Axidian PamSU

A component that allows PAM users to execute commands with administrator privileges. When connecting to a resource, the PAM account password is requested instead of the local user password under which the session is opened.
Instead of `sudo`, the `pamsu` command is used.

For more information about installation and configuration, see PamSU section.

Component composition and Linux distributions supporting PamSU

Composition: Installation package in .deb or .rpm format

Linux distributions:

- CentOS 7 and higher
- Oracle Linux 7.9 and higher
- Rocky Linux 8.8 and higher
- Debian 10 and higher
- Ubuntu 18 LTS and higher
- Red Hat Enterprise Linux (RHEL) 6 and higher

Axidian Privilege Desktop Console

A client application that allows you to connect through Axidian Privilege to target resources using SSH and RDP protocols. The component is installed on the user's workstation.

For more information about installation and configuration, see Desktop Console section.

Component composition

Multi-protocol remote connection manager mRemoteNG.exe

Licensing

Axidian Privilege supports the following licensing models:

- Per privileged user — the license grants the right to use Axidian Privilege for a specified number of users and an unlimited number of resources.
- Per resource — the license grants the right to connect to a specified number of resources: servers, hosts, etc. The number of users connecting via PAM is not limited.
- Per privileged session — the license grants the right to open a specified number of simultaneous sessions in Axidian Privilege. All active sessions are counted. The number of PAM users and resources is not limited.

> ⚠ **PAY ATTENTION**
> You can select only one licensing model per Axidian Privilege installation.

Regardless of the licensing model, you can also purchase licenses for additional functional modules. Such licenses do not affect users' ability to establish a session via PAM or the administrator's ability to grant permissions. Licenses for functional modules limit the use of additional features. These licenses include:

- AAPM
- ad hoc resources
- SQL Proxy

Licensing per privileged users

When selecting this licensing model, you will need to determine the number of users in your Axidian Privilege installation. The number of sessions (simultaneous connections) is not limited. User licenses can be redistributed between users (revoke licenses from some users and allocate them to others).

Issuance

To issue a user license, add at least one active permission to a user. After this, the license will automatically be considered taken by this user. If all user licenses are taken, you cannot add a permission to a new user.

Revocation

A user license is released when a user has no active permissions left, i.e., as a result of the following actions on a permission:

- Revocation
- Suspension
- Expiration

Validity Period

Types of licenses according to the validity period:

- Not time-limited
- Valid until a specific calendar date
  - Trial period
  - Subscription

Once the license expires, the following operations will no longer be available:

- Adding a resource
- Adding a user (even if some licenses have not been taken)
- Opening a session (connecting to a resource)

> ⚠ **CAUTION**
> If you do not have unlimited licenses, connections will no longer be available when the licenses expire.

Licensing per resources

When selecting this licensing model, you will need to determine the number of resources in your Axidian Privilege installation. The number of sessions (simultaneous connections) is not limited. Resource licenses can be freed and then taken by other resources.

Issuance

To issue a resource license, create or restore a resource in Axidian Privilege. After this, the license will automatically be considered taken by this resource. If all resource licenses are taken, you cannot

create a new resource.

Revocation

A resource license is released when the resource is deleted.

Validity Period

Types of licenses according to the validity period:

- Not time-limited
- Valid until a specific calendar date
  - Trial period
  - Subscription

Once the license expires, the following operations will no longer be available:

- Adding a resource
- Adding a user (even if some licenses have not been taken)
- Opening a session (connecting to a resource)

> ⚠ **CAUTION**
> If you do not have unlimited licenses, connections will no longer be available when the licenses expire.

Licensing per privileged sessions

When selecting this licensing model, you will need to determine the number of sessions (simultaneous connections that can be opened via Axidian Privilege). The number of users and resources is not limited.

Issuance and Release

A session license is considered taken at the moment the session is opened and is released at the moment the session ends (the reason for termination is not important).

Validity Period

Types of licenses according to the validity period:

- Not time-limited
- Valid until a specific calendar date
  - Trial period
  - Subscription

Once the license expires, you will no longer be able to open sessions.

The following operations will remain available:

- Editing permissions
- Editing existing resources
- Editing accounts

> ⚠ **CAUTION**
> If you do not have unlimited licenses, connections will no longer be available when the licenses expire.

AAPM License

The AAPM (Application to Application Password Management) license allows third-party applications to retrieve account secrets from Axidian Privilege.

When purchasing licenses of this type, you need to specify the number of accounts that can be accessed using AAPM.

There is no limit on the number of applications, application users, or permissions.

> ⓘ **INFO**
> The AAPM license is independent of the selected licensing model.
>
> The AAPM license can be purchased or removed at any time.

Issuance and Release

An AAPM license is considered taken when the first permission for an application is added to an account.

The AAPM license is released when all permissions are revoked from that account.

> ⚠ **PAY ATTENTION**
> Suspension of a permission does not release the AAPM license.

Validity Period

Types of licenses according to the validity period:

- Not time-limited
- Valid until a specific calendar date
  - Trial period
  - Subscription

Once the license expires, the following operations will no longer be available:

- Adding new permissions to applications
- Using scenarios in which third-party applications retrieve account secrets from Axidian Privilege

Ad hoc Resources License

This license allows you to connect to ad hoc resources. The license does not limit the number of permissions or simultaneous connections to ad hoc resources.

> ⓘ **INFO**
> The ad hoc resources license is independent of the selected licensing model.
>
> The ad hoc resources license can be purchased or removed at any time.

Validity Period

Types of licenses according to the validity period:

- Not time-limited

- Valid until a specific calendar date
    - Trial period
    - Subscription

Once the license expires, previously created permissions will be set to the *Inactive* state, and the following operations will no longer be available:

- Adding or renewing permissions to connect to ad hoc resources
- Opening sessions to ad hoc resource

SQL Proxy License

This license allows you to connect to resources of the PostgreSQL and MSSQL types. This license defines the number of active permissions for resources of the PostgreSQL and MSSQL types.

> ⓘ **INFO**
> The SQL Proxy license is independent of the selected licensing model.
>
> The SQL Proxy license can be purchased or removed at any time.

Issuance

To take the SQL Proxy license, grant a user at least one active permission to a resource of the PostgreSQL or MSSQL type. If all SQL Proxy licenses are taken, you cannot add a permission to a resource of the PostgreSQL or MSSQL type to a new user.

Revocation

The SQL Proxy license is released as a result of the following actions on a permission to a resource of the PostgreSQL or MSSQL type:

- Revocation
- Suspension
- Expiration

Validity Period

Types of licenses according to the validity period:

- Not time-limited
- Valid until a specific calendar date
    - Trial period
    - Subscription

Once the license expires, the following operations will no longer be available:

- Adding or renewing permissions to connect to resources of the PostgreSQL and MSSQL types
- Adding users to a user group that has an active permission to a resource of the PostgreSQL or MSSQL type
- Adding resources to a resource group that has an active permission to a resource of the PostgreSQL or MSSQL type
- Selecting the PostgreSQL or MSSQL type when editing a user connection of a resource that has an active permission
- Opening a session to a resource of the PostgreSQL or MSSQL type

System Requirements

Server components

System requirements for the Axidian Privilege server components

DBMS

Hardware requirements for DBMS

User workspace

System requirements for the user workspace

Server components

Recommended software and Hardware requirements are provided for each component. To calculate an individual PAM configuration, contact technical support.

Management Server

> **NOTE**
> The system requirements were determined during tests in a test environment with a typical load profile.

Windows

Hardware requirements			
Parameters	**50 sessions**	**100 sessions**	**200 sessions**
CPU	8 cores	16 cores	32 cores
RAM	8 GB	16 GB	32 GB
HDD/SSD	120 GB	120 GB	120 GB
Network adapter	1 Gbps	1 Gbps	1 Gbps
Operating system	Windows Server 2016–2022		
Domain	Microsoft Active Directory		
Web Server	Internet Information Services 8.5–10.0		

Modules for the IIS Web server	• Basic Authentication • Windows Authentication • Static Content • HTTP Redirection • ASP.NET Core Runtime • ISAPI Extensions • .NET Extensibility • ISAPI Filters • IIS Management Console
Additional Microsoft components	• Microsoft .NET Core 8 • URL Rewrite

Network Connectivity

Incoming

Protocol	Port	Description
TCP	443	User console, API, IdP connection

Outgoing

Protocol	Port	Description
TCP	389, 636	Directory Service Reading
TCP	389, 636	Service operations in Directory Service
TCP	5985, 5986, 139, 445	Service operations in Windows
TCP	22	Service operations in Linux, IOS XE, Inspur BMC
TCP	1433	Service operations or data recording in Microsoft SQL Server database

Protocol	Port	Description
TCP	5432	Service operations or data recording in PostgreSQL database
TCP	1521	Service operations in OracleDB database
TCP	3306	Service operations in MySQL database
TCP	445	Recording screenshots to media storage
TCP	5443	Reading a session stream from a Windows access server
TCP	8443	Reading a session stream from a Linux access server

Linux

Hardware requirements

Parameters	50 sessions	100 sessions	200 sessions
CPU	2 cores	2 cores	2 cores
RAM	4 GB	4 GB	4 GB
HDD/SSD	120 GB	120 GB	120 GB
Network adapter	1 Gbps	1 Gbps	1 Gbps
Operating system	• Debian 11 and higher • Ubuntu 22.04 and higher		
Container engine	• Docker 18.09 and higher • Docker Compose 1.29.2 and higher **Note:** Docker must be installed from the Linux distribution's repository.		

Additional components	• iptables 1.4 and higher • python 3.8 and higher • openssh-server (the version depends on the Linux distribution)
Disk partitioning	• Root file system (`/`) — partition with application and operating system files. It is recommended to allocate 10–20 GB depending on the installed software. • `/home` — partition for storing user data. Also used for storing temporary files and docker images during PAM installation. At least 10 GB of free space must be allocated. • `/var` — partition for storing temporary files, logs, databases, caches. It is recommended to allocate 20 GB or more. • `/tmp` — partition with temporary files. The partition size should be sufficient for temporary operations, such as unpacking files or storing caches. It is recommended to allocate 10 GB or more. • `/boot` — partition containing the bootloader and kernel. It is recommended to allocate 1 GB taking into account future expansions and updates. • `swap` — partition used as virtual memory. It is recommended to allocate a size equal to the RAM size. • `/var/lib/docker` — partition for Docker root directory, containing docker images, volumes and temporary files. As the number of user sessions increases, the partition size needs to be increased. It is recommended to allocate 100 GB or more. • `/etc/axidian` — partition for PAM data: configurations, certificates, keys, logs. Temporary data awaiting transfer to remote media storage is saved to the partition. It is recommended to allocate 40 GB or more.

Disk partitioning example

120 GB

Example of partitioning for a server with a disk volume of 120 GB and 16 GB of RAM.

Partition	Disk volume, GB	% of total disk
Root file system (`/`)	10	8,33
`/home`	10	8,33
`/var`	20	16,68
`/tmp`	10	8,33
`/boot`	1	0,83
`swap`	16	13,33
`/var/lib/docker`	38	31,67
`/etc/axidian`	15	12,50

Note: The `/var/lib/docker` and `/etc/axidian` partitions are smaller than the recommended sizes. This layout is suitable only if you use remote media storage and have a typical load profile. As the number of sessions grows, expand the disk and these partitions.

240 GB

Example of partitioning for a server with a disk volume of 240 GB and 32 GB of RAM.

Partition	Disk volume, GB	% of total disk

Root file system (`/`)	20	8,33
`/home`	10	4,17
`/var`	20	8,33
`/tmp`	10	4,17
`/boot`	1	0,42
`swap`	32	13,33
`/var/lib/docker`	100	41,67
`/etc/axidian`	47	19,58

Network Connectivity

Incoming

Protocol	Port	Description
TCP	443	User console, API, IdP connections

Outgoing

Protocol	Port	Description
TCP	389, 636	Directory Service Reading
TCP	389, 636	Service operations in Directory Service
TCP	5985, 5986, 139, 445	Service operations in Windows

Protocol	Port	Description
TCP	22	Service operations in Linux, IOS XE, Inspur BMC
TCP	1433	Service operations or data recording in Microsoft SQL Server
TCP	5432	Service operations or data recording in PostgreSQL
TCP	1521	Service operations in OracleDB
TCP	3306	Service operations in MySQL
TCP	445	Recording screenshots to media storage
TCP	5443	Reading a session stream from a Windows access server
TCP	8443	Reading a session stream from a Linux access server

RDS Access Server

> **NOTE**
> The system requirements were determined during tests in a test environment with a typical load profile.

Hardware requirements			
Parameters	**10 RDP or SSH sessions**	**50 RDP or SSH sessions**	**100 RDP or SSH sessions**

CPU	8 cores	16 cores	32 cores
RAM	12 GB	32 GB	64 GB
HDD/SSD	160 GB + 5 GB per Axidian Privilege User	320 GB + 5 GB per Axidian Privilege User	520 GB + 5 GB per Axidian Privilege User
Network adapter	1 Gbps	1 Gbps	1 Gbps
Operating system	Windows Server 2016–2022		
Domain	Microsoft Active Directory		
Roles	• Remote Desktop Services Broker (RDCB) • Remote Desktop Services Host (RDSH) • Remote Desktop Web Access (RDWA)		
Additional Microsoft components	• Microsoft .NET Desktop Runtime x64 v8 • Microsoft C++ 2015–2019 Redistributable		
Browser	• Google Chrome • Microsoft EDGE		
Other requirements	• Support for Simultaneous MultiThreading (AMD) or Hyper-Threading (Intel) • Monitor width resolution of at least 1280 pixels		

Network Connectivity

Incoming

Protocol	Port	Description
TCP	3389	Connection to the Access server

Protocol	Port	Description
TCP	5443	Reading a session stream

Outgoing

Protocol	Port	Description
TCP	443	Interaction with the Management server **Note**: In a fault-tolerant setup, interaction with the Management server is performed through a load balancer
TCP	3389	Connection to a resource via RDP protocol
TCP	22	Connection to a resource via SSH protocol
TCP	23	Connection to a resource via Telnet protocol
TCP	445	Recording videos of sessions in media storage

RDP Access Server

> **INFO**
> The system requirements were determined during tests in a test environment with a typical load profile.

Hardware requirements			
Parameters	**10 RDP sessions**	**50 RDP sessions**	**100 RDP sessions**

CPU	2 cores	8 cores	8 cores
RAM	4 GB	12 GB	12 GB
HDD/SSD	120 GB	120 GB	120 GB
Network adapter	1 Gbps	1 Gbps	1 Gbps
Operating system	• Debian 11 and higher • Ubuntu 22.04 and higher		
Container engine	• Docker 18.09 and higher • Docker Compose 1.29.2 and higher **Note:** Docker must be installed from the Linux distribution's repository.		
Additional components	• iptables 1.4 and higher • python 3.8 and higher • openssh-server (the version depends on the Linux distribution)		
Other requirements	Monitor width resolution of at least 1280 pixels		

Network Connectivity

Incoming

Protocol	Port	Description
TCP	3390	Connection to the Access server
TCP	8443	Reading a session stream

Outgoing

Protocol	Port	Description
TCP	443	Interaction with the Management server **Note**: In a fault-tolerant setup, interaction with the Management server is performed through a load balancer
TCP	3389	Connection to a resource via RDP protocol
TCP	445	Recording videos of sessions in media storage

SSH Access Server

> **NOTE**
> The system requirements were determined during tests in a test environment with a typical load profile.

Hardware requirements

Parameters	50 SSH sessions	100 SSH sessions	200 SSH sessions
CPU	2 cores	2 cores	4 cores
RAM	2 GB	4 GB	4 GB
HDD/SSD	120 GB	120 GB	120 GB
Network adapter	1 Gbps	1 Gbps	1 Gbps
Operating system	• Debian 11 and higher • Ubuntu 22.04 and higher		

Container engine	• Docker 18.09 and higher • Docker Compose 1.29.2 and higher **Note:** Docker must be installed from the Linux distribution's repository.
Additional components	• iptables 1.4 and higher • python 3.8 and higher • openssh-server (the version depends on the Linux distribution)

Network Connectivity

Incoming

Protocol	Port	Description
TCP	2222	Connection to the Access server

Outgoing

Protocol	Port	Description
TCP	443	Interaction with the Management server **Note**: In a fault-tolerant setup, interaction with the Management server is performed through a load balancer
TCP	22	Connection to a resource via SSH/SCP/SFTP protocol
TCP	445	Saving transferred files

PostgreSQL Access Server

> **NOTE**
> The system requirements were determined during tests in a test environment with a typical load profile.

Hardware requirements			
Parameters	**50 SQL sessions**	**100 SQL sessions**	**200 SQL sessions**
CPU	2 cores	2 cores	2 cores
RAM	4 GB	4 GB	4 GB
HDD/SSD	120 GB	120 GB	120 GB
Network adapter	1 Gbps	1 Gbps	1 Gbps
Operating system	• Debian 11 and higher • Ubuntu 22.04 and higher		
Container engine	• Docker 18.09 and higher • Docker Compose 1.29.2 and higher **Note:** Docker must be installed from the Linux distribution's repository.		
Additional components	• iptables 1.4 and higher • python 3.8 and higher • openssh-server (the version depends on the Linux distribution)		

Network Connectivity

Incoming

Protocol	Port	Description
TCP	5432	Connection to the Access server

Outgoing

Protocol	Port	Description
TCP	443	Interaction with the Management server **Note**: In a fault-tolerant setup, interaction with the Management server is performed through a load balancer
TCP	5432	Writing data to the PostgreSQL DBMS

MSSQL Access Server

Operating system	• Debian 11 and higher • Ubuntu 22.04 and higher
Container engine	• Docker 18.09 and higher • Docker Compose 1.29.2 and higher **Note:** Docker must be installed from the Linux distribution's repository.
Additional components	• iptables 1.4 and higher • python 3.8 and higher • openssh-server (the version depends on the Linux distribution)

Network Connectivity

Incoming

Protocol	Port	Description
TCP	1433	Connection to the Access server

Outgoing

Protocol	Port	Description
TCP	443	Interaction with the Management server **Note**: In a fault-tolerant setup, interaction with the Management server is performed through a load balancer
TCP	1433	Writing data to the MSSQL DBMS

Web Terminal Server

> **NOTE**
> The system requirements were determined during tests in a test environment with load distribution:
>
> - 40% on SSH session
> - 60% on RDP session

Hardware requirements

Parameters	25 sessions	50 sessions	75 sessions	100 sessions

CPU	single-core	2 cores	3 cores	4 cores
RAM	2 GB	4 GB	6 GB	8 GB
HDD/SSD	120 GB	120 GB	120 GB	120 GB
Network adapter	1 Gbps	1 Gbps	1 Gbps	1 Gbps
Operating system	• Debian 11 and higher • Ubuntu 22.04 and higher			
Container engine	• Docker 18.09 and higher • Docker Compose 1.29.2 and higher **Note:** Docker must be installed from the Linux distribution's repository.			
Additional components	• iptables 1.4 and higher • python 3.8 and higher • openssh-server (the version depends on the Linux distribution)			

Network Connectivity

Incoming

Protocol	Port	Description
HTTPS	443	Connection to the Web Terminal
TCP	58090	Server health monitoring

Outgoing

Protocol	Port	Description
TCP	2222	• Connection to a resource via SSH Proxy protocol • Interaction with the SSH Proxy through a load balancer

Protocol	Port	Description
TCP	3389	Connection to a resource via RDP Proxy protocol
TCP	3390	Interaction with the RDP Proxy through a load balancer

Web Access Server

> **NOTE**
> The system requirements were determined during tests in a test environment with a typical load profile and based on the recommended scaling for the Video Resolution. Configure this setting before opening a web session.

Hardware requirements			
Parameters	**10 Web sessions**	**50 Web sessions**	**100 Web sessions**
CPU	2 cores	8 cores	16 cores
RAM	6 GB	18 GB	32 GB
HDD/SSD	120 GB	120 GB	120 GB
Network adapter	1 Gbps	1 Gbps	1 Gbps
Operating system	• Debian 11 and higher • Ubuntu 22.04 and higher		
Container engine	• Docker 18.09 and higher • Docker Compose 1.29.2 and higher **Note:** Docker must be installed from the Linux distribution's repository.		

Additional components	• iptables 1.4 and higher • python 3.8 and higher • openssh-server (the version depends on the Linux distribution)

Network Connectivity

Incoming

Protocol	Port	Description
TCP	5443	Connection to the Access server
TCP	58080	Server health monitoring

Outgoing

Protocol	Port	Description
TCP	443	Connection to a web resource via the HTTPS protocol
TCP	80	Connection to a web resource via the HTTP protocol

CIS Benchmark Security Settings

PAM servers must have CIS Benchmark security settings applied.

DBMS

Review the system requirements for the Axidian Privilege DBMS.

Hardware requirements			
Parameters	**50 sessions**	**100 sessions**	**200 sessions**
CPU	2 cores	2 cores	2 cores
RAM	2 GB	4 GB	4 GB
HDD/SSD	1 TB	1 TB	1 TB
Network adapter	1 Gbps	1 Gbps	1 Gbps
Supported DBMS	• Microsoft SQL Server 2016–2022 with support for Full-Text and Semantic Extractions for Search • PostgreSQL 12–18		

User workspace

Review the system requirements for the user workspace.

Browsers

Axidian Privilege consoles are supported in the following browsers:

- Google Chrome
- Microsoft Edge

Desktop Console

Hardware requirements	• At least 2 GB RAM • At least 500 MB of free disk space
Operating system	• Windows 7 and higher • Windows Server 2008 and higher
Additional Microsoft components	Microsoft .NET Framework 4.6.2 and higher

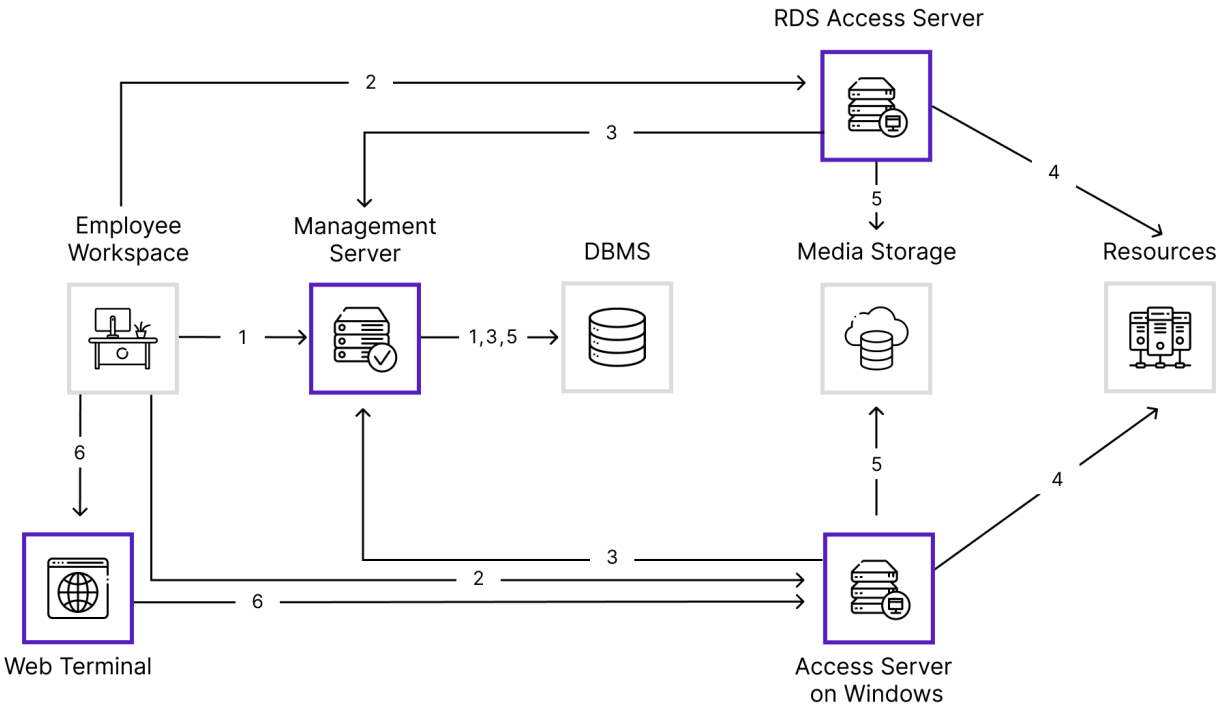
Deployment Architecture

This section describes the possible deployment options for Axidian Privilege components. The choice of deployment scheme depends on testing and production scenarios: the set of components and servers, as well as their roles, may vary.

Basic scheme

Axidian Privilege components are installed on three separate servers. In this deployment scheme, the Axidian Privilege business logic is isolated from the access components. Recommended for production deployments.

User scenario



ABOUT THE SCHEME

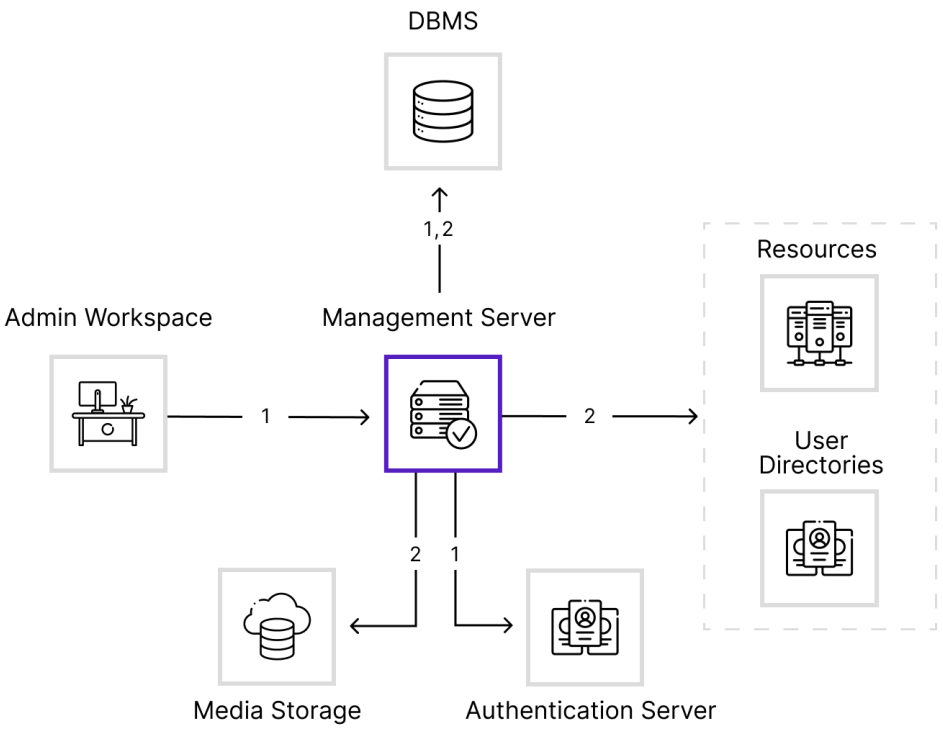
The Management Server can run on Windows or Linux.

1. The user connects to the Management Server via the Desktop Console application or the user console in a browser. The Management Server authenticates the user by querying the IdP database or external authentication services to verify the user's credentials and provide a list of available resources from the Core database.
2. After authentication, the user can connect to a resource through a proxy server:

- RDS Access Server — for sessions using the RDP protocol or in RemoteApp mode.
- Linux Access Server — for sessions using the RDP, SSH, SCP, SFTP, or HTTP (browser-based web session) protocols, as well as for connections to PostgreSQL and MSSQL databases via a console or client application.

3. The Access Server queries the Management Server to re-authenticate the user, verify permissions, and retrieve privileged account credentials from the database.
4. After verification, the Access Server opens a session to the target resource on behalf of the privileged account.
5. During the session, the Access Server records the user's activity and saves the session video, transferred files, and screenshots to media storage, and the text log to the Core database. Session logging depends on the connection type.
6. An SSH or RDP session can be launched in a browser via the Web Terminal, which is hosted on the Linux Access Server. The Access Server identifies the user through the Management Server and monitors the session on the resource.

Administrator scenario



1. **Connecting to the management console**
   The administrator connects to the console on the Management Server via a browser. The

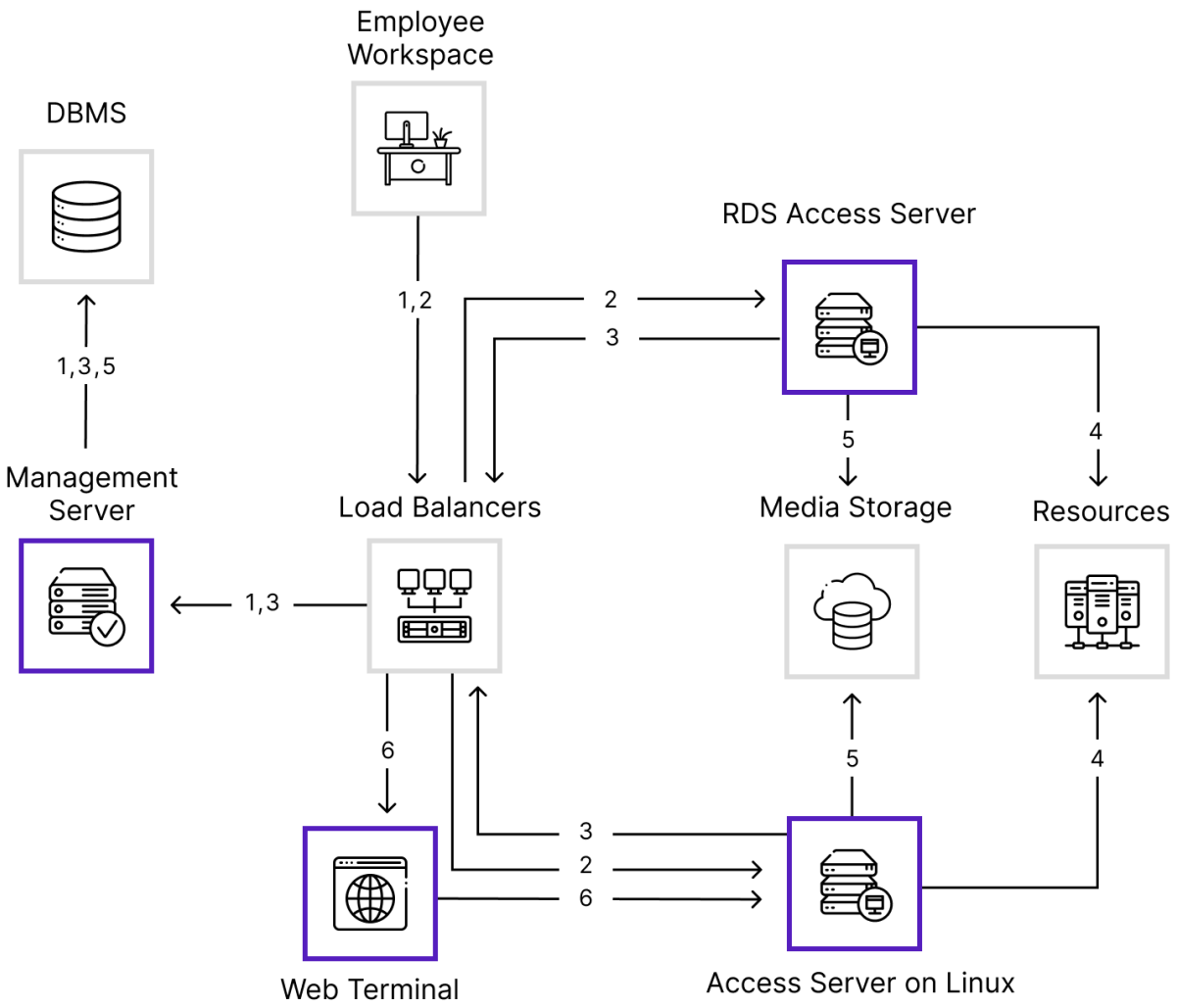
Management Server verifies the account through the authentication server and queries the IdP database to identify the user and determine their privileges.

2. **Administering Axidian Privilege**
   After authentication, the administrator manages PAM objects, i.e. resources, users, and access permissions, and performs audits and service operations.

Fault-tolerant scheme

In this deployment scenario, the servers hosting Axidian Privilege components are duplicated to ensure fault tolerance. Recommended for production deployments.

User scenario



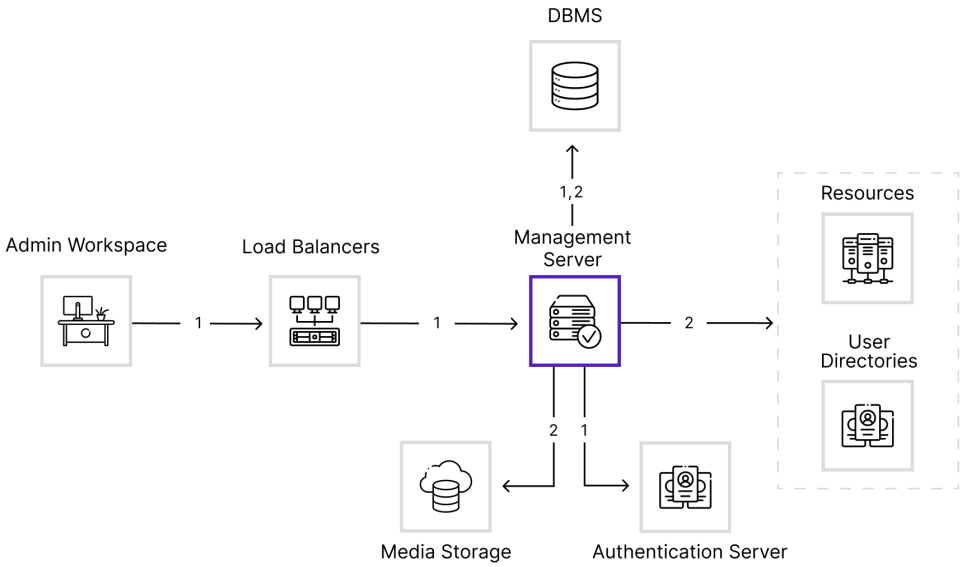
ⓘ ABOUT THE SCHEME

Interaction between the user and PAM components occurs through a load balancer.

The Management Server can run on Windows or Linux.

1. The user connects to the Management Server via the Desktop Console application or the user console in a browser. The Management Server authenticates the user by querying the IdP database or external authentication services to verify the user's credentials and provide a list of available resources from the Core database.
2. After authentication, the user can connect to a resource through a proxy server:
   - RDS Access Server — for sessions using the RDP protocol or in RemoteApp mode.
   - Linux Access Server — for sessions using the RDP, SSH, SCP, SFTP, or HTTP (browser-based web session) protocols, as well as for connections to PostgreSQL and MSSQL databases via a console or client application.
3. The Access Server queries the Management Server to re-authenticate the user, verify permissions, and retrieve privileged account credentials from the database.
4. After verification, the Access Server opens a session to the target resource on behalf of the privileged account.
5. During the session, the Access Server records the user's activity and saves the session video, transferred files, and screenshots to media storage, and the text log to the Core database. Session logging depends on the connection type.
6. An SSH or RDP session can be launched in a browser via the Web Terminal, which is hosted on the Linux Access Server. The Access Server identifies the user through the Management Server and monitors the session on the resource.

Administrator scenario

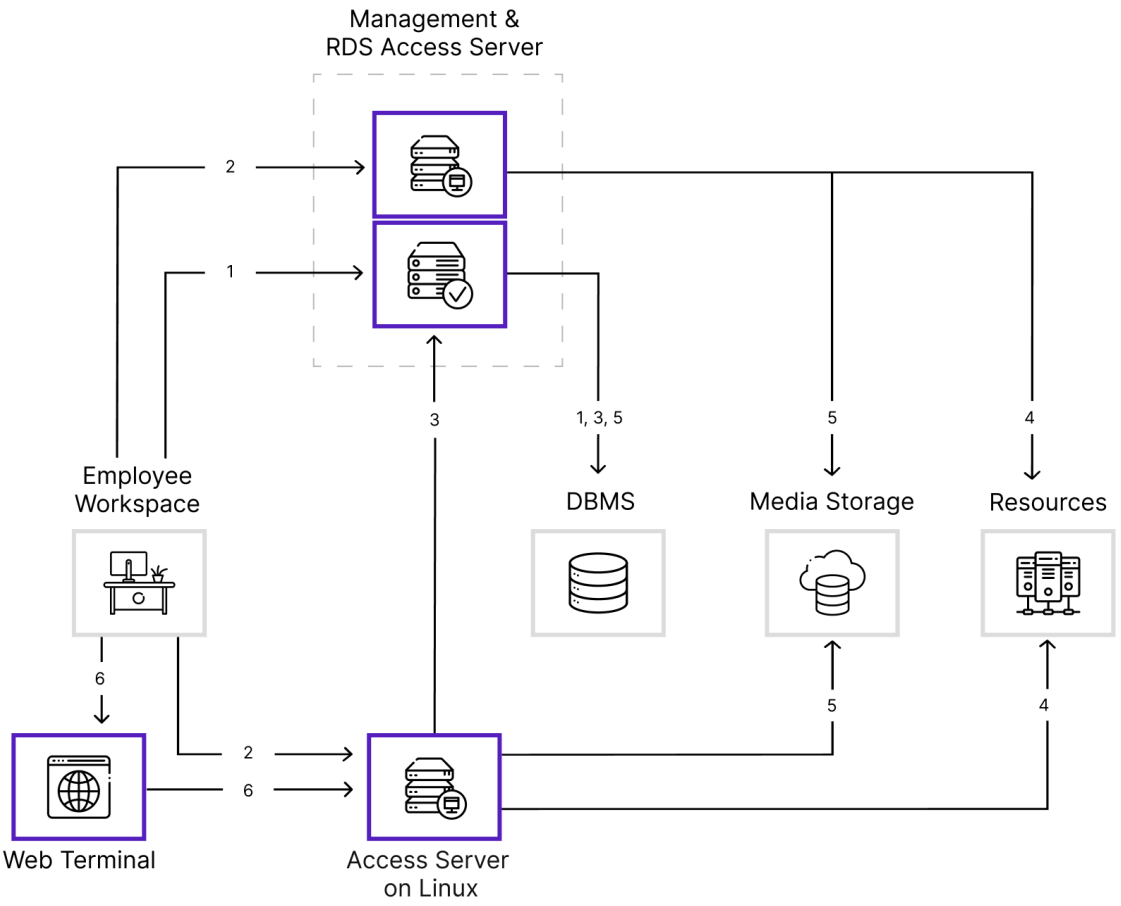


1. **Connecting to the management console**
   The administrator connects to the console on the Management Server via a browser. All actions go through the load balancer. The Management Server verifies the account through the authentication server and queries the IdP database to identify the user and determine their privileges.
2. **Administering Axidian Privilege**
   After authentication, the administrator manages PAM objects, i.e. resources, users, and access permissions, and performs audits and service operations.

Windows deployment

Axidian Privilege components are installed on two separate servers. Recommended for evaluation and testing.

User scenario



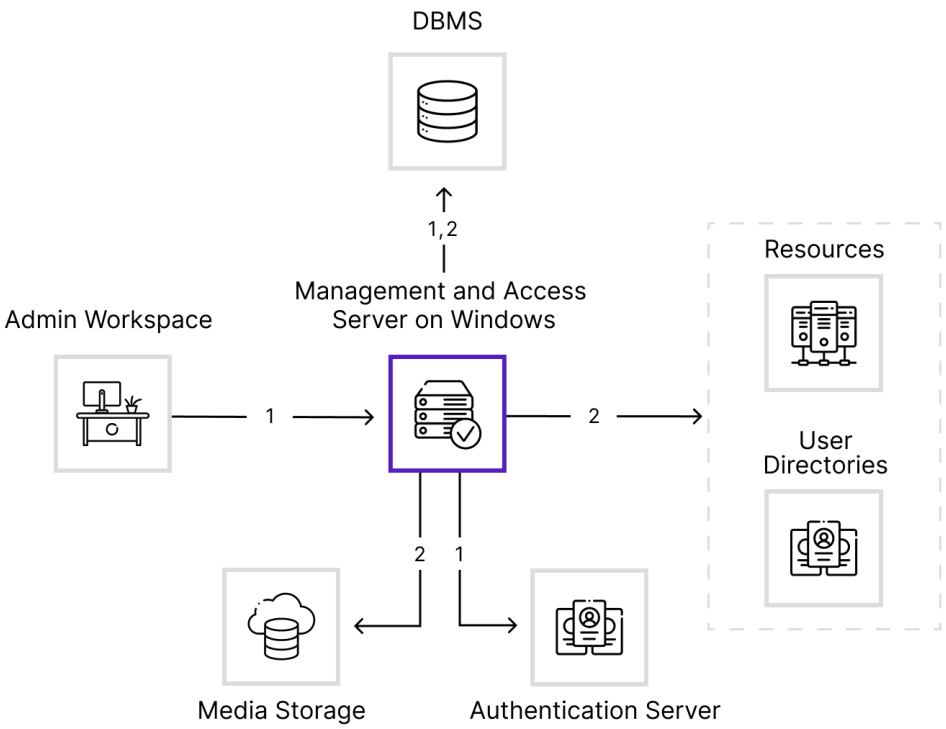
ABOUT THE SCHEME

The Management Server and the RDS Access Server run on Windows and are hosted on the same server.

1. The user connects to the Management Server via the Desktop Console application or the user console in a browser. The Management Server authenticates the user by querying the IdP database or external authentication services to verify the user's credentials and provide a list of available resources from the Core database.
2. After authentication, the user can connect to a resource through a proxy server:
   - RDS Access Server — for sessions using the RDP protocol or in RemoteApp mode.
   - Linux Access Server — for sessions using the RDP, SSH, SCP, SFTP, or HTTP (browser-based web session) protocols, as well as for connections to PostgreSQL and MSSQL databases via a console or client application.
3. The Access Server queries the Management Server to re-authenticate the user, verify permissions, and retrieve privileged account credentials from the database.
4. After verification, the Access Server opens a session to the target resource on behalf of the privileged account.

5. During the session, the Access Server records the user's activity and saves the session video, transferred files, and screenshots to media storage, and the text log to the Core database. Session logging depends on the connection type.
6. An SSH or RDP session can be launched in a browser via the Web Terminal, which is hosted on the Linux Access Server. The Access Server identifies the user through the Management Server and monitors the session on the resource.

Administrator scenario

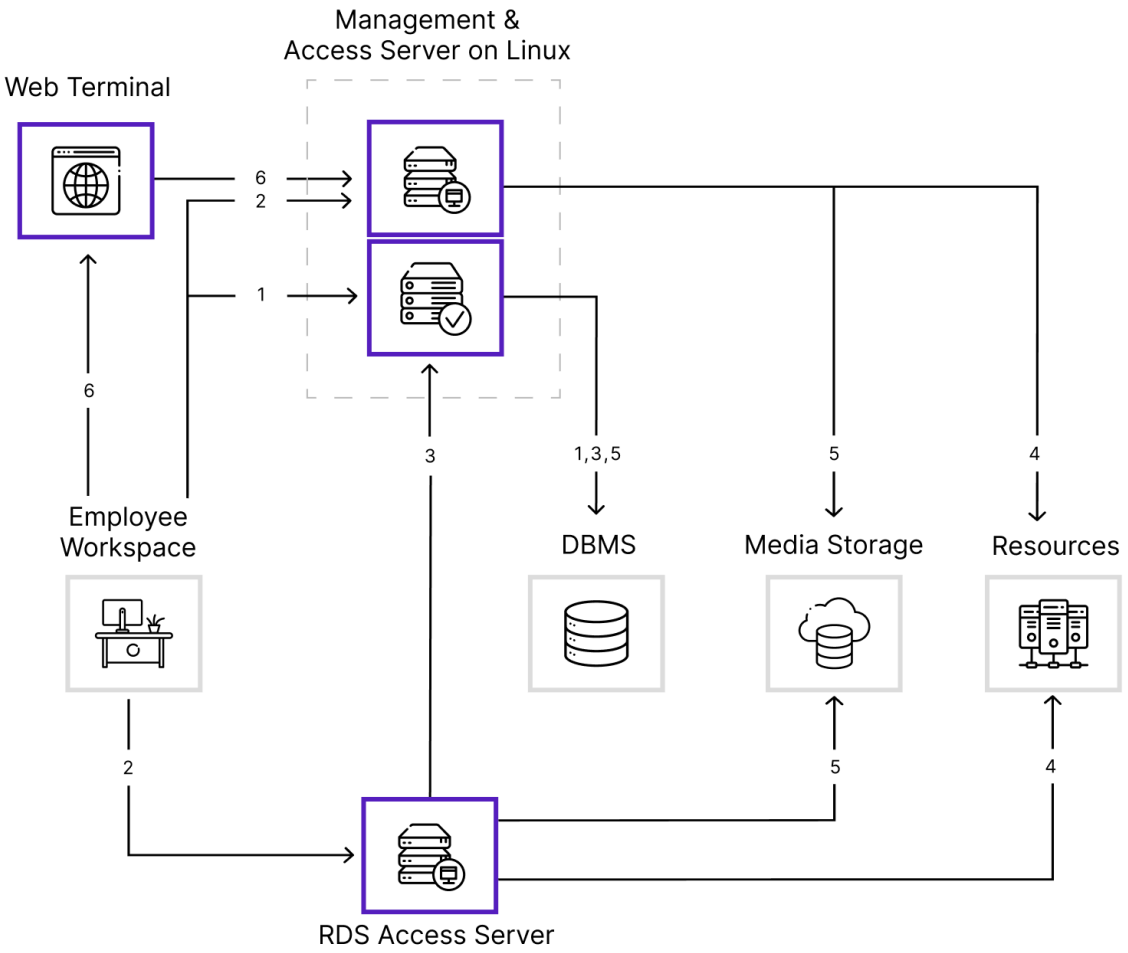


1. **Connecting to the management console**
   The administrator connects to the console on the Management Server via a browser. The Management Server verifies the account through the authentication server and queries the IdP database to identify the user and determine their privileges.
2. **Administering Axidian Privilege**
   After authentication, the administrator manages PAM objects, i.e. resources, users, and access permissions, and performs audits and service operations.

Linux deployment

Axidian Privilege components are installed on two separate servers. Recommended for evaluation and testing.

User scenario



ABOUT THE SCHEME

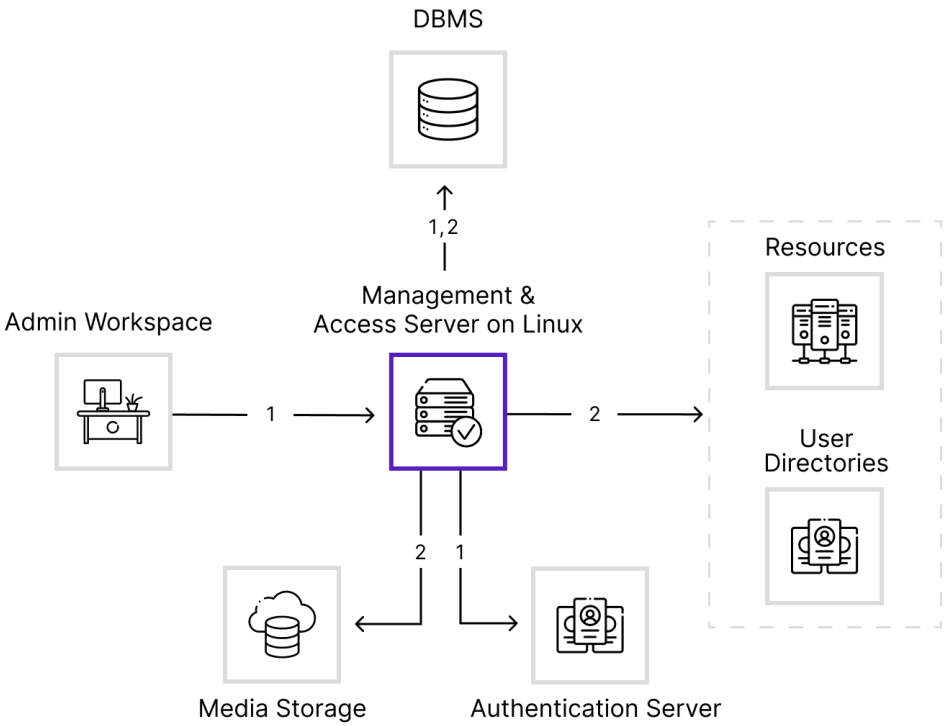
The Management Server and the SSH, RDP, Web, PostgreSQL, and MSSQL Access Servers run on Linux and are hosted on the same server.

1. The user connects to the Management Server via the Desktop Console application or the user console in a browser. The Management Server authenticates the user by querying the IdP database or external authentication services to verify the user's credentials and provide a list of available resources from the Core database.
2. After authentication, the user can connect to a resource through a proxy server:
   - RDS Access Server — for sessions using the RDP protocol or in RemoteApp mode.

- Linux Access Server — for sessions using the RDP, SSH, SCP, SFTP, or HTTP (browser-based web session) protocols, as well as for connections to PostgreSQL and MSSQL databases via a console or client application.

3. The Access Server queries the Management Server to re-authenticate the user, verify permissions, and retrieve privileged account credentials from the database.
4. After verification, the Access Server opens a session to the target resource on behalf of the privileged account.
5. During the session, the Access Server records the user's activity and saves the session video, transferred files, and screenshots to media storage, and the text log to the Core database. Session logging depends on the connection type.
6. An SSH or RDP session can be launched in a browser via the Web Terminal, which is hosted on the Linux Access Server. The Access Server identifies the user through the Management Server and monitors the session on the resource.

Administrator scenario



1. **Connecting to the management console**
   The administrator connects to the console on the Management Server via a browser. The Management Server verifies the account through the authentication server and queries the IdP database to identify the user and determine their privileges.

2. **Administering Axidian Privilege**

   After authentication, the administrator manages PAM objects, i.e. resources, users, and access permissions, and performs audits and service operations.

Installation steps

Preparing the Infrastructure

1. Providing server and client resources in accordance with their system and hardware requirements.
2. Installation and configuration of Remote Desktop Services role.
3. Installation of additional Microsoft components required for correct operation of Axidian Privilege server components.
4. Configuration of networking between server and client components according to the requirements.
5. Configuration of Axidian Privilege data storage:
    1. Installation of Microsoft SQL Server, PostgreSQL or providing access to an existing Microsoft SQL Server and PostgreSQL instance.
    2. Creation of databases.
    3. Configuration of service account or providing access to an existing account.
    4. Create and configure a media storage for storing videos, screenshots, and files.
6. Definition of LDAP paths to containers and organization units to place Axidian Privilege end users to.
7. Creation and configuration of service account for use with user directory or providing access to an existing account.
8. Creation and configuration of service account to use for service operations or providing access to an existing account.

Installation and Configuration of Axidian Privilege Server Components

Windows

1. Management Server on Windows OS
2. RDS Access Server

Linux

1. Management Server on Linux OS
2. RDP Access Server
3. SSH Access Server
4. PostgreSQL Access Server
5. MSSQL Access Server
6. Web Access Server
7. Web Terminal Server

Installation and Configuration of Axidian Privilege Client Components

1. Installation of the PamSu component.
2. Installation of Axidian Privilege Agent client component.
3. Installation of Axidian Privilege Desktop Console utility.

Test Run of Axidian Privilege

1. Checking for server and client components.
2. Troubleshooting.
3. Checking of system functions and customer scenarios:
    1. Configuration of service operations for Windows resources.
    2. Configuration of service operations for Linux resources.
    3. Configuration of user connections.
    4. Configuration service operations in active directory.

Final Step

1. Demonstrate the functionality.
2. Train users to work with PAM.
3. Put the PAM into operation.

Preparation for Installation

User Directory Accounts

Create accounts to work with user directory and for service operations

Certificates

Create management server certificates

Databases

Create databases and a service account for Axidian Privilege data storage

Media Storage

3 items

Servers

Add RDS role (for Windows) or install required components (for Linux)

IIS Web Server

Add a registry entry and configure IIS (for Windows)

Accounts for Installing PAM via Web Wizard

Review the list of accounts required to run the wizard

User Directory Accounts

Axidian Privilege interacts with end users through a service account that reads directory users and their attributes.

Account to Use with User Directory

Active Directory

1. Run the **Active Directory Users and Computers** snap-in.
2. Open the context menu of the organizational unit or container.
3. Select **Create** → **User** item from the menu.
4. Specify the user name, e.g, **IPAMADReadOps**.
5. Fill in the required fields and complete the account creation.

FreeIPA

1. Run the FreeIPA snap-in as a user with administrator privileges.
2. Create a user, for example, **IPAMADReadOps**.
3. Open the **IPA Server** tab.
4. From the **Role-Based Access Control** drop-down menu, select **Permissions**.
5. Create a permission with the following values:
   - **Permission name**: `pam_attr_read`
   - **Granted Rights**: `read`, `search`
   - **Effective attributes**: `entryDn`, `entryUUID`, `ipaUniqueID`, `ipaNTSecurityIdentifier`, `memberOf`, `uid`, `givenName`, `krbPrincipalName`, `cn`, `sn`, `photo` (or `jpegPhoto`), `member`, `nsOsVersion`, `fqdn`, `initials`, `krbPasswordExpiration`
6. From the **Role-Based Access Control** drop-down menu, select **Privileges**.
7. Create a new privilege (e.g. `pam_privilege_read`) and add the created `pam_attr_read` permission to it.
8. From the **Role-Based Access Control** drop-down menu, select **Roles**.
9. Create a new role (for example, `IPAMADReadOps_role`) and add the created `pam_privilege_read` privilege to it.
10. Assign the created role to the **IPAMADReadOps** user in one of the following ways:

- assign a role to a user
- assign the role to a user group and add the user to that group

OpenLDAP

1. Create a user, for example, **IPAMADReadOps**.
2. Grant the user read permissions to the following attributes:
   - `entryUUID`
   - `entryDn`
   - `uid`
   - `cn`
   - `osVersion`
   - `groupOfUniqueNames`
   - `uniqueMember`

Account for Service Operations in Active Directory

Active Directory

1. Run the **Active Directory Users and Computers** snap-in.
2. Open the context menu of the organizational unit or container.
3. Select **Create** → **User** item from the menu.
4. Specify the user name, e.g, **IPAMADServiceOps**.
5. Fill in the required fields and complete the account creation.
6. Open the context menu of organizational unit, container or domain root.
7. Select **Properties**.
8. Open **Security** tab.
9. Click **Add**.
10. Select an account **IPAMADServiceOps** and click **Ok**.
11. Click **Advanced**.
12. Select an account **IPAMADServiceOps** and click **Edit**.
13. Specify the value of the field **Applies to** to the **Descendant User objects**.

14. In the **Permissions** section check the **Reset password** checkbox.
15. Save.

FreeIPA

1. Run the FreeIPA snap-in as a user with administrator privileges.
2. Create a user, for example, **IPAMADServiceOps**.
3. Open **IPA Server** tab.
4. From the **Role-Based Access Control** drop-down menu, select **Permissions**.
5. Create a permission with the following values:
   - **Permission name**: `pam_attr_read`
   - **Granted Rights**: `read`, `search`
   - **Effective attributes**: `entryDn`, `entryUUID`, `ipaUniqueID`, `ipaNTSecurityIdentifier`, `memberOf`, `uid`, `givenName`, `krbPrincipalName`, `cn`, `sn`, `photo` (or `jpegPhoto`), `member`, `nsOsVersion`, `fqdn`, `initials`, `krbPasswordExpiration`
6. Create another permission with the following values:
   - **Permission name**: `pam_attr_write`
   - **Granted Rights**: `write`
   - **Effective attributes**: `userPassword`, `krbPasswordExpiration`
7. From the **Role-Based Access Control** drop-down menu, select **Privileges**.
8. Create a new privilege (e.g. `pam_privilege_change_pswd`) and add the two permissions `pam_attr_read` and `pam_attr_write` you just created to it.
9. From the **Role-Based Access Control** drop-down menu, select **Roles**.
10. Create a new role (for example, `IPAMADServiceOps_role`) and add the created `pam_privilege_change_pswd` privilege to it.
11. Assign the created role to the **IPAMADServiceOps** user in one of the following ways:
    - assign a role to a user
    - assign the role to a user group and add the user to that group

OpenLDAP

1. Create a user, for example, **IPAMADServiceOps**.
2. Grant the user read permissions to the following attributes:
   - `entryUUID`
   - `entryDn`

- `uid`
- `cn`
- `osVersion`
- `groupOfUniqueNames`
- `uniqueMember`

3. Grant the user write permissions for the `userPassword` attribute.

Certificates

Prepare certificates before installing Axidian Privilege. All certificates should have the same password.

> ⚠ **CAUTION**
> All certificates except the CA certificate must be in .pfx format.
>
> The CA certificate must be in .crt format.

Certificate requirements

- Certificates must be valid.
- Minimum RSA key length: 2048.
- Settings configured:
  - *Server Authentication* is specified for the *Enhanced Key Usage (EKU)* extension.
  - The setting allows you to use the certificate for server authentication.
  - *Digital Signature* and *Key Encryption* are specified for the *Key Usage* extension. The setting defines cryptographic operations: it allows the key to create digital signatures and allows you to encrypt symmetric session keys.
- The certificate contains Common Name (CN) and Subject Alternative Names (SAN).
  The fields contain the domain names of the host in the FQDN format.

CN and SAN completion scheme

When generating a certificate, the CN and SAN fields are filled in depending on the role and membership of the host in a fault-tolerant cluster (Keepalived), as well as the presence of a load balancer.

Availability of a load balancer	The load balancer host in the Keepalived cluster	The host combines an access server	Configuration of the certificate
No	-	-	Subject field: `CN` — hostname SAN field: `DNS` — hostname
Yes	Yes	-	Subject field: `CN` — hostname SAN field: `DNS` — hostname `DNS` — PAM FQDN
Yes	No	Yes	Subject field: `CN` — hostname SAN field: `DNS` — hostname `DNS` — PAM FQDN
Yes	No	No	Subject field: `CN` — hostname SAN field: `DNS` — hostname

List of certificates

Installation without balancing

The following certificates are required:

- Certificate of the certification authority without a private key in PEM (Base64) format with the .crt extension.
- PAM FQDN certificate with private key in .pfx format.
- Certificates for all access servers with a private key in .pfx format. Except when the access server is installed on the same host as the management server.

Fault-tolerant installation with HAProxy

The following certificates are required:

- Certificate of the certification authority without a private key in PEM (Base64) format with the .crt extension.
- PAM FQDN certificate with private key in .pfx format.
- Certificates for all management servers with a private key in .pfx format.
- Certificates for all access servers with alternative names of all balancers and PAM FQDN with a private key in .pfx format. Except when the access server is installed on the same host as the management server.

> ⚠ **CAUTION**
> If you plan to place the balancer and the management server on the same host, you will need a certificate with an alternative PAM FQDN name.
>
> When using vIP, each balancer certificate requires a PAM FQDN alternative name.
>
> If there are Windows access servers, their certificates must contain the PAM FQDN or be the same as for the PAM FQDN, otherwise the certificate check in the wizard will result in an error.

Fault-tolerant installation with a third-party balancer

The following certificates are required:

- Certificate of the certification authority without a private key in PEM (Base64) format with the .crt extension.
- Certificates for all management servers with a private key in .pfx format.
- Certificates for all access servers with alternative names of all balancers and PAM FQDN with a private key in .pfx format. Except when the access server is installed on the same

host as the management server.

- Certificates for all balancers with a private key in .pfx format.

> ⚠ **CAUTION**
>
> If you plan to place the balancer and management server on the same host, you will need a certificate with an alternative PAM FQDN name.
>
> When using vIP, each balancer certificate requires a PAM FQDN alternative name.

> ⓘ **INFO**
>
> It is possible to use a wildcard certificate. In this case, the certificate must be issued for the entire domain or have the addresses of all PAM hosts in alternative names.

For LDAPS to work correctly, place the CA certificate in `AxidianPAM_3.5\axidian-pam\state\ca-certificates` before running the wizard.

Databases

To store data, Axidian Privilege uses the following databases:

- **Core** — the Core component database. Used to store privileged account data, resources, permissions, and other service data.
- **CoreJobs** — the Core component database. Used to store and run background jobs, such as resource and account synchronization, password changes, session management, and artifact rotation.
- **Idp** — the IdP component database. Used to store authenticators of Axidian Privilege users and administrators.
- **IdpJobs** — the IdP component database. Used to run background authentication service jobs.
- **ILS** — the Log Server component database. Used to store Axidian Privilege events.

Create databases

MSSQL

1. Open **Microsoft SQL Server Management Studio** (SSMS) and connect to your Microsoft SQL Server instance.
2. In **Object Explorer**, right-click **Databases**, and then select **New Database**.
3. Create the following databases: **Core**, **CoreJobs**, **Idp**, **IdpJobs**, and **ILS**.

PostgreSQL

pgAdmin

1. Open **pgAdmin** and connect to your PostgreSQL instance.
2. Right-click **Databases**, and then select **Create** → **Database**.
3. Create the following databases: **Core**, **CoreJobs**, **Idp**, **IdpJobs**, and **ILS**.

psql command-line client

1. Open a terminal as root.
2. Connect to your PostgreSQL instance as the `postgres` superuser:

```
psql -U postgres -h <host> -p <port>
```

- `host` — the IP address or DNS name of the server
- `port` — the port number (default: `5432`)

After you connect, the command prompt changes to `postgres=#`.

3. Create the following databases: **Core**, **CoreJobs**, **Idp**, **IdpJobs**, and **ILS**.
   To preserve the case of the database names, enclose each name in double quotation marks.

```
CREATE DATABASE "Core";
CREATE DATABASE "CoreJobs";
CREATE DATABASE "Idp";
CREATE DATABASE "IdpJobs";
CREATE DATABASE "ILS";
```

4. Verify that the databases were created:

```
\l
```

Create a service account

MSSQL

1. Open **Microsoft SQL Server Management Studio** (SSMS) and connect to your Microsoft SQL Server instance.
2. In **Object Explorer**, expand **Security**.
3. Right-click **Logins**, and then select **New Login**.
4. In **Login name**, enter a name for the account, for example, **IPAMSQLServiceOps**.
5. Select **SQL Server authentication**, and then fill in the required fields.
6. Go to the **User Mapping** page.
7. Select the **Core**, **CoreJobs**, **Idp**, **IdpJobs**, and **ILS** databases.
8. For the selected databases, select the **db_owner**, **db_datareader**, and **db_datawriter** roles.
9. Select **OK**.

> **INFO**
>
> The **db_owner** role is required only for the first connection to the database.
>
> To use Axidian Privilege, install a certificate for your Microsoft SQL Server instance.

PostgreSQL

pgAdmin

1. Open **pgAdmin** and connect to your PostgreSQL instance.
2. Right-click **Login/Group Roles**.
3. Select **Create** → **Login/Group Role**.
4. In **Name**, enter a name for the account, for example, **IPAMSQLServiceOps**.
5. On the **Definition** tab, in **Password**, enter a password for the account.
6. On the **Privileges** tab, turn on **Can login?** and **Superuser?**.
7. Select **Save**.

psql command-line client

1. Open a terminal as root.
2. Connect to your PostgreSQL instance as the `postgres` superuser:

   ```
   psql -U postgres -h <host> -p <port>
   ```

   - `host` — the IP address or DNS name of the server
   - `port` — the port number (default: `5432`)

   After you connect, the command prompt changes to `postgres=#`.
3. Create a role with a name and password:

   ```
   CREATE ROLE "<username>" WITH LOGIN PASSWORD '<password>' SUPERUSER;
   ```

   - `username` — the account name, for example, `IPAMSQLServiceOps`.
     To preserve the case of the name, enclose it in double quotation marks.
   - `LOGIN` — allows the role to connect to the database server.

- `PASSWORD` — sets the role password. Replace `password` with a password, for example, `DB_Prod_Password789!`.
- `SUPERUSER` — grants superuser privileges to the role.

> **INFO**
> Superuser privileges are required only for the first connection to the database.

4. Verify that the role was created and that the `Attributes` column contains `Superuser`:

```
\du "<username>"
```

Media Storage

SMB Storage

Create and configure SMB media storage

NFS Storage

Create and configure NFS media storage

S3 Storage

Create and configure S3 media storage

SMB Storage

Axidian Privilege supports file data storage operation based on the SMB (Server Message Block) network access protocol. SMB data storage is a standard network data storage for Windows OS.

To create and configure data storage:

1. Log in to the server, which will act as a file storage.
2. Create a directory, for example *IPAMStorage*.
3. Open the context menu and select **Give access to** and **Specific people**.
4. Enter the username, for example *IPAMStorageOps* .
5. Click **Add**.
6. Select *IPAMStorageOps* from the added list.
7. Change **Permission level** to **Read/Write**.
8. Click **Share**.

System requirements

> **INFO**
> System requirements for data storage are calculated based on an example PAM installation with 700 simultaneous sessions with video logging.

Recommended system requirements:

- CPU Cores: 6 cores.
- CPU Frequency: 2.8 GHz base clock or higher.
- CPU Technology: Hyper-Threading (or equivalent SMT) support is required.
- RAM: 16 GB.
- Network: 1 Gbps network interface and channel bandwidth.
- Storage: RAID 0 (striping) array or a hybrid solution with SSD cache (e.g., using a RAID controller with cachecade/SSD caching).

NFS Storage

Axidian Privilege supports file storage based on the NFS Network Access Protocol (Network File System).

Preparing storage on Linux OS

RPM

1. Install the required packages:

```
sudo dnf install nfs-utils
```

2. Start NFS server services:

```
sudo systemctl start nfs-server.service
sudo systemctl enable nfs-server.service
sudo systemctl status nfs-server.service
```

3. Create file systems for export or sharing on NFS server and set the owner and group:

```
sudo mkdir -p /mnt/data_storage/
sudo chown -R 23041:23041 /mnt/data_storage/
```

4. Export filesystems to the NFS server configuration file, `/etc/exports`, to define local physical filesystems accessible to NFS clients:

Path template

```
/mnt/data_storage/ <Client IP/Network/Mask/*>
(rw,sync,all_squash,anonuid=23041,anongid=23041)
```

Path example

```
/mnt/data_storage/ 192.168.131.0/24(rw,sync,all_squash,anonuid=23041,anongid=23041)
```

5. Once you have made your changes, run the command to make them take effect:

```
sudo exportfs -arv
```

6. Bypassing built-in security utilities:

   In RPM-based distros (e.g. CentOS, RHEL, Fedora), the SELinux security utility may block NFS access if it is not configured properly.

   - To disable SELinux temporarily for testing:

     ```
     sudo setenforce 0
     ```

   - To configure SELinux to work with NFS:

     ```
     sudo setsebool -P nfs_export_all_rw 1
     sudo setsebool -P nfs_export_all_ro 1
     ```

   Also make sure that your firewall is not blocking ports required for NFS to work. Open required ports:

   ```
   sudo firewall-cmd --permanent --add-service=nfs
   sudo firewall-cmd --permanent --add-service=rpc-bind
   sudo firewall-cmd --permanent --add-service=mountd
   sudo firewall-cmd --reload
   ```

DEB

1. Install the required packages:

   ```
   sudo apt update
   sudo apt install nfs-kernel-server
   ```

2. Start NFS server services:

   ```
   sudo systemctl start nfs-kernel-server.service
   sudo systemctl enable nfs-kernel-server.service
   sudo systemctl status nfs-kernel-server.service
   ```

3. Create file systems for export or sharing on NFS server and set the owner and group:

```
sudo mkdir -p /mnt/data_storage/
sudo chown -R 23041:23041 /mnt/data_storage/
```

4. Export filesystems to the NFS server configuration file, `/etc/exports`, to define local physical filesystems accessible to NFS clients:

Path template

```
/mnt/data_storage/ <Client IP/Network/Mask/*>
(rw,sync,all_squash,anonuid=23041,anongid=23041)
```

Path example

```
/mnt/data_storage/ 192.168.131.0/24(rw,sync,all_squash,anonuid=23041,anongid=23041)
```

5. Once you have made your changes, run the command to make them take effect:

```
sudo exportfs -arv
```

6. Bypassing built-in security utilities:

   On DEB based distros (e.g. Ubuntu, Debian) you may also need to configure your firewall to allow NFS access.

   - To check the firewall status and, if necessary, open ports for NFS:

```
sudo ufw status
sudo ufw allow from <Client IP> to any port nfs
sudo ufw allow 2049/tcp
sudo ufw allow 111/tcp
sudo ufw allow 111/udp
```

   - If you are using AppArmor, make sure that the profiles for NFS are configured properly. In some cases, you may need to adjust or temporarily disable them.

```
sudo aa-status
```

     If AppArmor interferes with NFS, you can temporarily disable it for testing:

```
sudo systemctl stop apparmor
sudo systemctl disable apparmor
```

Configuring PAM to work with NFS

The storage is configured after installing Axidian Privilege.

Linux

1. Create a folder for mounting media storage on the server. You can also use a ready-made folder, for example, `/etc/axidian/axidian-pam/media-data`.

   ```
   sudo mkdir -p /mnt/pamstorage/
   ```

2. Install NFS mount client:

   - RPM:

     ```
     sudo yum install nfs-utils
     ```

   - DEB:

     ```
     sudo apt install nfs-common
     ```

3. Mount the storage:

   Command template

   ```
   sudo mount -t nfs <fqdn_or_ip_nfs_server>:/path/to/media_storage /path/to/mount/folder
   ```

   Command example

   ```
   sudo mount -t nfs 192.168.131.200:/mnt/data_storage/ /mnt/pamstorage/
   ```

4. Add storage mount to autostart:

To automatically mount NFS on system startup, add an entry to the `/etc/fstab` file:

Command template

```
<fqdn_or_ip_nfs_server>:/path/to/media_storage /path/to/mount/folder nfs defaults 0 0
```

File example:

Command example

```
192.168.131.200:/mnt/data_storage/ /mnt/pamstorage/ nfs defaults 0 0
```

To verify the mount, run the command:

```
sudo mount
```

5. Edit the volumes section in the docker-compose files for Core and Gateway-Service:
   - Core: Path to the file on the management server: `/etc/axidian/axidian-pam/docker-compose.management-server.yml`
   - Gateway-Service: Path to the file on the access server: `/etc/axidian/axidian-pam/docker-compose.access-server.yml`

   You need to add the path to the mounted storage to the `volumes` section:

   ```
   - /path/to/mount/folder:/mnt/storage:rw,z
   ```

   Example for Core:

```yaml
core:
  image: nexus.axidian-id.hq:5050/pam/axidian-pam-core:${TAG}
  container_name: pam-core
  extends:
    file: docker-compose.common-services.yml
    service: base
  pids_limit: 5000
  depends_on:
    - ca-certificates
    - pgsql
  environment:
    - COMPlus_EnableDiagnostics=0
  user: root
  read_only: false
  security_opt:
    - apparmor=pam-management
  volumes:
    - ./core/events:/var/lib/axidian/axidian-pam/events:rw,Z
    - ./core/appsettings.json:/app/appsettings.json:ro,z
    - ./keys/shared/protector:/etc/axidian/axidian-pam/keys/shared/protector:ro,z
    - ./keys/core:/etc/axidian/axidian-pam/keys/core:ro,Z
    - ./logs/core:/app/logs:rw,Z
    - /mnt/pamstorage:/mnt/storage:rw,z  # NFS mount example
    - pam-core-temp-data:/var/lib/axidian/axidian-pam:rw
    - pam-ca-cert-store:${CERT_STORE}:ro
  tmpfs:
    - /tmp
  networks:
    - pam-core-network
    - pam-ls-network
```

6. Edit the Storage section of the Core and Gateway-Service configuration files:

   - Core: Path to the configuration file on the management server: `/etc/axidian/axidian-pam/core/appsettings.json`
   - Gateway-Service: Path to the configuration file on the access server: `/etc/axidian/axidian-pam/gateway-service/appsettings.json`

   In both files you need to specify the path to the mounted storage:

```json
"Storage": {
  "Type": "FileSystem",
  "Settings": {
    "Root": "/mnt/storage"
  }
}
```

7. Restart containers using the following command:

```
sudo bash /etc/axidian/axidian-pam/scripts/run-pam.sh
```

Windows

1. Install NFS mount client:

    1. Click **Start** → **Server Manager** in the lower left corner.
    2. Click **Add Roles and Features**.
    3. On the **Features** page, enable the **Client for NFS** checkbox and click **Next**.
    4. Confirm the settings by clicking **Install**.

2. Mount the storage and add it to autostart:

    Use PowerShell without elevated privileges.

    Command template

    ```
    New-PSDrive -PSProvider FileSystem -Name <drive_letter> -Root \\
    <fqdn_or_ip_nfs_server>\path\to\media_storage -Persist
    ```

    Command example

    ```
    New-PSDrive -PSProvider FileSystem -Name Z -Root \\192.168.131.200\mnt\data_storage\ -
    Persist
    ```

3. Edit the `Storage` section of the Core and Gateway-Service configuration files:

    - Core: Path to the configuration file on the management server: `C:\inetpub\wwwroot\core\appsettings.json`
    - Gateway-Service: Path to the configuration file on the access server: `C:\Program Files\Axidian\Axidian Privilege\Gateway\Pam.Gateway.Service\appsettings.json`

    Change the `Storage` section to:

    Section template

```
"Storage": {
  "Type": "FileSystem",
  "Settings": {
    "Root": "\\\\<fqdn_or_ip_nfs_server>\\path\\to\\media_storage"
  }
},
```

Section example

```
"Storage": {
  "Type": "FileSystem",
  "Settings": {
    "Root": "\\\\192.168.131.200\\mnt\\data_storage\\"
  }
},
```

4. Restart IIS and Gateway-Service:

   - Restart IIS on the management server:

     Open **IIS Manager** and run the **Restart** command on the server.

   - Restart Gateway-Service:

     Open **Task Manager**, find the PAM.Gateway.Service and restart it.

S3 Storage

Object data storages based on the S3 (Simple Storage Service) protocol allow storing files of any type. For grouping and storing files, special containers are used — buckets. Axidian Privilege supports S3 data storage MinIO.

To create and configure a data storage:

1. Log in to the server that will act as the file data storage.
2. Go to the **Buckets** section on the left panel.
3. Click **Create bucket**.
4. Fill in the **Bucket Name** field.
5. Click **Create bucket**.
6. Make sure that the created data storage appears in the **Buckets** section.
7. Go to the **Access Keys** section in the left panel.
8. Click **Create Access Key**.
9. Fill in the **Access Key** and **Secret Key** fields.

> ⓘ **INFO**
> Keys are required by Axidian Privilege Gateway Service to access the data storage. Specify the Access Key and Secret Key in the wizard when setting up the data storage.

10. Open the command prompt as administrator and check the data storage availability:

```
rclone lsjson \
--s3-endpoint <hostname> \
--s3-provider Other \
--s3-access-key-id <access-key-id> \
--s3-secret-access-key <secret-access-key> \
--s3-acl public-read-write \
:s3:<bucket_name>
```

- `hostname` — IP address or DNS name of the server with data storage.
  Example: `"http://127.0.0.1:9000"`

- `access-key-id` — Access key.
- `secret-access-key` — Secret key.
- `bucket_name` — data storage name.

If the media storage is available and contains no files, the command will return an empty list: `[]`.

Servers

Windows

For installing Axidian Privilege components, servers on Windows OS must:

- access one DNS server
- be in the same domain and network
- have the WinRM service running
- have a hostname that matches the DNS name of the server, in lowercase and FQDN format
  Example: pam.my-company.local

For hardware and software requirements, as well as networking for servers, see the System Requirements section.

Starting the WinRM Service

To install Axidian Privilege components on management and access servers, start the WinRM service:

1. Run PowerShell as administrator.
2. Execute the command:

```
Enable-PSRemoting -Force
```

The command sets standard WinRM settings, changes the service startup type to automatic, and allows incoming network connections through Windows Firewall to ports 5985 and 5986.

Configuring the RDS Access Server

PAM users can open Web/Desktop sessions through the RDS access server. The connection is implemented using Microsoft Remote Desktop Services. When a user connects to the RDS access server, the Axidian Privilege application launches. The application checks user permissions, authenticates them, and logs the session. Applications are launched in RemoteApp mode.

To prepare the server for operation, enable the WinRM service, deploy the RDS role, and configure the firewall.

Before deploying a server with the RDS role, make sure that:

- no group policies related to remote access are applied to it
- it does not have any of the RDS role components (RDCB, RDG, RDL, RDSH, RDVH, RDWA)

Deploying the Remote Desktop Services role

1. Open **Server Manager** and in the **Manage** menu select **Add Roles and Features**.
2. Select the **Remote Desktop Services Installation** type and click **Next**.
3. Select the **Standard deployment** type and click **Next**.
4. Select the **Session-based desktop deployment** type and click **Next**.
5. Skip the **Role Services** step and click **Next**.
6. Select the current server name on the **RD Connection Broker**, **RD Web Access**, **RD Session Host** and click **Next**.
7. Select the **Restart the destination server automatically if required** option and click **Deploy**.
8. After reboot, open **Server Manager** and wait for the process to complete.

Configuring a firewall rule

1. Go to the **Local server** tab and click on the **Windows Defender Firewall** parameter value.
2. Go to the **Firewall & network protection** window and click **Advanced settings**.
3. Go to the **Windows Defender Firewall with Advanced Security** window and open the **Inbound Rules** tab.
4. Click **New Rule** and configure the settings:
    1. Select the **Port** rule type and click **Next**.
    2. Specify the port in the **Specific local ports** field:
        - 5985 — for connections via HTTP
        - 5986 — for connections via HTTPS
    3. Select the **Allow the connection** option and click **Next**.
    4. Select all profiles and click **Next**.
    5. Enter the rule name in the **Name** field and click **Finish**.

Linux

To install Axidian Privilege components, servers on Linux OS must:

- access one DNS server
- be in the same domain and network
- have a hostname that matches the DNS name of the server, in lowercase and FQDN format
  Example: pam.my-company.local

For hardware and software requirements, as well as networking for servers, see the System requirements section.

IIS Web Server

When deploying Management server on Windows Server and IIS, do the following steps:

1. Add the following registry entries:

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\HTTP\Parameters]
"MaxFieldLength"=dword:8000 (hex)
"MaxRequestBytes"=dword:8000 (hex)
```

2. Start IIS on the management server.
3. Navigate to `Default Web Site\core`.
4. In the **Manage** section, open **Configuration Editor**.
5. Expand the dropdown list **Section** and select `system.webServer\serverRuntime`.
6. Set the **uploadReadAheadSize** parameter value to **1048576**.
7. In the **Actions** section, click **Apply**.
8. Restart the server

Accounts for Installing PAM via Web Wizard

Before proceeding to the Installation section, make sure you have prepared all the accounts described below and their passwords. Axidian Privilege cannot be installed without these accounts.

- Host accounts (individual or shared domain account).

  Read more

  These accounts will be used to install PAM components on hosts.

  For Windows hosts, it must be possible to connect via WinRM and the account must have local administrator privileges. For Linux, it must be possible to connect via SSH, and the account must have root privileges.

  The credentials for these accounts will be saved in the wizard backup for use in future wizard operations, such as changing the configuration or updating Axidian Privilege.

- Balancer accounts, if a fault-tolerant installation is planned.
- DBMS account (e.g. **IPAMSQLServiceOps**).
- An account for accessing the media storage if the storage type is SMB.
- An account to read the user directory (e.g. **IPAMADReadOps**).
- Role Administrator account. It is the user who will be granted rights to manage PAM roles. This user will be able to grant access rights to the PAM management console to other users.
- An account for authentication on the SMTP server if you plan to select Email as the second factor.

Installation

Basic on Windows

Install Axidian Privilege in accordance with the basic deployment scheme without load balancing with the management server on Windows

Basic on Linux

Install Axidian Privilege in accordance with the basic deployment scheme without load balancing with the management server on Linux

Fault Tolerant on Windows

Install Axidian Privilege in accordance with the fault tolerant deployment scheme with load balancing with the management server on Windows

Fault Tolerant on Linux

Install Axidian Privilege in accordance with the fault tolerant deployment scheme with load balancing with the management server on Linux

Basic on Windows

Axidian Privilege components are installed on three servers. This type of installation allows you to separate the managing components from the components that provide access. Suitable for implementation and operation in production. Deployment scheme without balancing.

Before starting the installation, please prepare the environment.

Wizard Launch

Web Wizard is a web application that allows you to install, upgrade, or change the configuration of Axidian Privilege. The Web Wizard is supplied as part of the PAM distribution. To use the Wizard, you will need to run it in a Docker container using a special script.

1. Download and unpack the Web Wizard distribution on your Linux machine.
2. Place the CA certificate in `..PAM_3.5\axidian-pam\state\ca-certificates`. This is required for LDAPS to function properly. Skipping this step will result in an error for the wizard.
3. Launch the Web Wizard by the command:

   ```
   sudo bash run-wizard.sh
   ```

4. Wait for the script to complete.
5. Once the script is completed, go to the URL you see in the console.
6. In the **Authentication Code** field, enter the value you see in the console after executing the script.
   Code example: `vVHyTVRyKX5pxUKM6e1ZgCWEnOdXFdOy`.

   > **INFO**
   > By default, the code will be requested again after 2 hours, which means that all the work needs to be completed during this time.

7. Click **Enter** and proceed to work with the wizard.

Scenario

1. Select the **New PAM installation** scenario, and then select **Next**.

2. Select an installation option:

   - **Clean installation** — installation in which you complete all wizard steps.
     Select this option if you're installing Axidian Privilege for the first time.

   - **Installation from backup** — installation based on a saved PAM configuration.
     Select this option if you have a PAM configuration backup, for example, to resume an interrupted installation.

     On the next step, upload the configuration backup file and enter its password. To verify the backup version and continue, select **Verify backup**.

     After verification, all wizard settings are filled in according to the uploaded configuration. The settings can be edited.

     > ⚠ **CAUTION**
     > The backup version can't be higher than the wizard version.
     > Example: wizard version 3.4 won't work with a backup of version 3.5. Backups of versions 3.4 or 3.0 are suitable for it.

3. Select **Next** to go to the next wizard step.

<details>
<summary>More about scenarios</summary>

The following scenarios are available in the Web Wizard:

- **New PAM Installation** is an Axidian Privilege installation (clean or from a backup).
- **PAM Upgrade** is an upgrading of all Axidian Privilege components to the new version (for example, from 2.10 to 3.0). During the upgrade PAM will be unavailable. All current sessions will be terminated.
- **PAM Configuration Change** is making changes to the current PAM installation. For example, changing the set of hosts. The PAM version will remain the same. During the configuration change PAM will be unavailable. All current sessions will be terminated.
</details>

Hosts Scheme

A host is a physical or virtual server on which the PAM components will be located.

1. In the **Hosts Scheme** step, enter the fully qualified domain name of the management server in the **PAM FQDN** field.
   Example: pam.my-company.local.

2. Add the management server and the required access servers. You cannot add multiple hosts with the same address. The RDS access server is used for RemoteApp connections.

   > ⚠ **CAUTION**
   > Deploy PAM in a fault tolerance if you plan to install a Web Terminal server and host Web, RDP, SSH, MSSQL, or PostgreSQL access servers on two or more hosts.

   Management Server

   1. Click **Add Host**.
   2. For the **Host Operating System** setting, select **Windows**.
   3. Enable the **Management Server** checkbox.
   4. Enter the IP address or DNS in the **Host Address** field. Please note that you cannot add multiple hosts with the same address.
   5. Enter the port in the **Port** field.
   6. Select the account type for the host: a **shared domain account** or a **separate account for this host**.
   7. Enter **Login** in UPN or SAM format and **Password** for the specified account.
   8. Click **Add**.

RDS Access Server

> ⚠ **CAUTION**
> When adding an RDS access server, note that you must add a directory in the User Directories step. You cannot continue with internal users only.

1. Click **Add Host**.
2. For the **Host Operating System** setting, select **Windows**.
3. Enable the **RDS Access Server** checkbox.
4. Enter the IP address or DNS in the **Host Address** field. Please note that you cannot add multiple hosts with the same address.
5. Enter the port in the **Port** field.
6. Select the account type for the host: a **shared domain account** or a **separate account for this host**.
7. Enter **Login** in UPN or SAM format and **Password** for the specified account.
8. Click **Add**.

SSH Access Server

1. Click **Add Host**.
2. For the **Host Operating System** setting, select **Linux**.
3. Enable the **SSH Access Server** checkbox.
4. Enter the IP address or DNS in the **Host Address** field. Please note that you cannot add multiple hosts with the same address.
5. Enter the port in the **Port** field.
6. Select the method for authenticating your account on the host: **by password** or **by SSH key**.
   - If **by password** selected, enter **Login** and **Password**.
   - If **by SSH key** selected, enter **Login**, **sudo password**, **SSH key** and **Passphrase**.
7. Click **Add**.

PostgreSQL Access Server

1. Click **Add Host**.
2. For the **Host Operating System** setting, select **Linux**.
3. Enable the **PostgreSQL Access Server** checkbox.
4. Enter the IP address or DNS in the **Host Address** field. Please note that you cannot add multiple hosts with the same address.
5. Enter the port in the **Port** field.
6. Select the method for authenticating your account on the host: **by password** or **by SSH key**.
   - If **by password** selected, enter **Login** and **Password**.
   - If **by SSH key** selected, enter **Login**, **sudo password**, **SSH key** and **Passphrase**.
7. Click **Add**.

MSSQL Access Server

1. Click **Add Host**.
2. For the **Host Operating System** setting, select **Linux**.
3. Enable the **MSSQL Access Server** checkbox.
4. Enter the IP address or DNS in the **Host Address** field. Please note that you cannot add multiple hosts with the same address.
5. Enter the port in the **Port** field.
6. Select the method for authenticating your account on the host: **by password** or **by SSH key**.
   - If **by password** selected, enter **Login** and **Password**.
   - If **by SSH key** selected, enter **Login**, **sudo password**, **SSH key** and **Passphrase**.
7. Click **Add**.

Web Access Server

1. Click **Add Host**.
2. For the **Host Operating System** setting, select **Linux**.
3. Enable the **Web Access Server** checkbox.
4. Enter the IP address or DNS in the **Host Address** field. Please note that you cannot add multiple hosts with the same address.
5. Enter the port in the **Port** field.
6. Select the method for authenticating your account on the host: **by password** or **by SSH key**.
   - If **by password** selected, enter **Login** and **Password**.
   - If **by SSH key** selected, enter **Login**, **sudo password**, **SSH key** and **Passphrase**.
7. Click **Add**.

Web Terminal Server

1. Click **Add Host**.
2. For the **Host Operating System** setting, select **Linux**.
3. Enable the **Web Terminal Server** checkbox.
4. Enter the IP address or DNS in the **Host Address** field. Please note that you cannot add multiple hosts with the same address.
5. Enter the port in the **Port** field.
6. Select the method for authenticating your account on the host: **by password** or **by SSH key**.
   - If **by password** selected, enter **Login** and **Password**.
   - If **by SSH key** selected, enter **Login**, **sudo password**, **SSH key** and **Passphrase**.
7. Click **Add**.

INFO

Management Server and RDS Access Server can be located on the same host.
The Web Terminal Server and RDP, Web, SSH, MSSQL, and PostgreSQL access servers can be located on the same host.

3. Review the host table and make sure that the data entered is correct. If you need to edit the host data, click on the line with the desired host, make changes and click **Save**. If you need to delete a host, click next to that host.

4. For the **Balancer** setting, select **Do not use**.

5. Click **Next** to proceed to the next step of the wizard.

Ports

> **INFO**
> Ports of PAM components must be unique.

1. Specify ports for PAM components according to your network architecture or leave the default values.

Component	Default port
SSH Proxy	2222
RDP Proxy	3390
PostgreSQL Proxy	5432
MSSQL Proxy	1433
Web Proxy	5443
MC/UC HTTP	80
MC/UC HTTPS	443
Gateway Service Web Terminal	8443

2. Click **Next** to proceed to the next step of the wizard.

Certificates

In this step you need to upload previously prepared certificates.

1. Upload the CA certificate without the private key in PEM (Base64) format with the .crt extension.
2. Upload certificates for hosts with the .pfx extension or a wildcard certificate and specify the password.
3. Click **Next** to proceed to the next step of the wizard.

Databases

1. Select **Server Type** Microsoft SQL.
2. Enter **Server Address** and **MSSQL Instance Name**.
3. Enable the **Secure connection to DBMS** checkbox.
4. Enter username and password for the database account.
5. For the **Encryption keys** setting, select **Generate new**.
6. Enter the names of the databases you created in the Preparation for Installation step:
    - DB for privileged accounts
    - DB for authenticators of PAM users
    - DB for PAM events
    - DB for Scheduled Jobs of the Core component
    - DB for Scheduled Jobs of the Idp component
7. Click **Next** to proceed to the next step of the wizard.

Selecting PostgreSQL

1. Select **Server Type** PostgreSQL.
2. Enter **Server Address**.
3. Enable the **Secure connection to DBMS** checkbox.
4. Enter username and password for the database account.
5. For the **Encryption keys** setting, select **Generate new**.
6. Enter the names of the databases you created in the Preparation for Installation step:
   - DB for privileged accounts
   - DB for authenticators of PAM users
   - DB for PAM events
   - DB for Scheduled Jobs of the Core component
   - DB for Scheduled Jobs of the Idp component
7. Click **Next** to proceed to the next step of the wizard.

Data Storage

1. Select **Storage Type** File System.
2. If necessary, edit the **Storage root directory** field.
3. Click **Next** to proceed to the next step of the wizard.

> **INFO**
> After PAM installation is complete, configure file storage (NFS).

Other storage types

If you select SMB, fill in the following fields:

- Network path
- Domain
- Username
- Password

If you select S3, fill in the following fields:

- Network address of the S3 server
- Path to the storage root directory on the S3 server
- Access key id
- Secret access key
- Region (optional)
- Location restriction (optional)

User Directories

Add one or more user directories, or click **Next** to use PAM with internal users only.

> ⚠ **CAUTION**
> If you added an RDS access server on the **Hosts Scheme** step, be sure to add a user directory. You cannot continue with internal users only.

Selecting FreeIPA or OpenLDAP

1. Click **Add User Directory**.
2. In the **Directory Service** field, select **FreeIPA** or **OpenLDAP**.
3. In the **Catalog ID** field, enter the catalog ID in PAM.
   The value can consist of Latin letters and numbers, with a maximum length of 32 characters. If you plan to use multiple directories, then their IDs should be different.
4. Fill in the **Domain DNS name** field.
5. (Optional) In the **Domain Controllers** field, specify the address of the domain controller in the FQDN format.
   You can specify multiple addresses separated by commas.
   If you do not specify an address, PAM will connect using the DNS name of the domain.
6. In the **DN of the user container** field, specify the container where the system users are located.
7. Enter the user's name in DN format and their password.
   Example: `uid=pamadmin,cn=users,cn=accounts,dc=my,dc=company`.
8. (Optional) Enable the option **Use LDAPS**.
9. If you selected FreeIPA, specify **User and Group Identifier Format**: SID or GUID.
10. (Optional) Change the mapping of user attributes of users and/or attributes of user groups.
11. Click **Add**.
12. Click **Next** to proceed to the next step of the wizard.

Selecting Active Directory

1. Click **Add User Directory**.
2. In the **Directory Service** field, select **Active Directory**.
3. In the **Catalog ID** field, enter the catalog ID in PAM.
   The value can consist of Latin letters and numbers, with a maximum length of 32 characters. If you plan to use multiple directories, then their IDs should be different.
4. Fill in the **Domain DNS name** field.
5. (Optional) In the **Domain Controllers** field, specify the address of the domain controller in the FQDN format.
   You can specify multiple addresses separated by commas.
   If you do not specify an address, PAM will connect using the DNS name of the domain.
6. In the **DN of the user container** field, specify the container where the system users are located.
7. Enter the user's name in UPN format and their password.
   Example: `pamadmin@my.company`.
8. (Optional) Enable the option **Use LDAPS**.
9. (Optional) Change the mapping of user attributes of users and/or attributes of user groups.
10. Click **Add**.
11. Click **Next** to proceed to the next step of the wizard.

Role Administrators

> **INFO**
> You can only specify one role administrator in the wizard.

You can select a user from the directory or an internal user to become the role administrator. The selected user will be granted the rights to manage the PAM roles. This user will be able to grant access rights to the PAM management console to other users.

User from the directory

1. Select an account from the directory.

2. Click **Next** to proceed to the next step of the wizard.

Internal user

1. Set login.

   > ⚠ **CAUTION**
   > The login cannot be changed after PAM is installed.

2. Set or generate a password. The password is only required for the first login. After logging in, the system will automatically request its change.

3. Enter an email.

4. Click **Next** to proceed to the next step of the wizard.

User Authentication

On this step you need to set up an authentication mechanism and configure two-factor authentication.

Authentication mechanism

1. Select the authentication mechanism: LDAP, RADIUS or Kerberos.

   > ⓘ **INFO**
   > Kerberos authentication supports a single Active Directory domain.
   >
   > Signing in with a username and password is available only for internal PAM users.

2. If you selected RADIUS, add a RADIUS server and enter the required information.

RADIUS authentication

> ⚠ **CAUTION**
> RADIUS authentication is unavailable for internal users. The settings specified here apply only to users from the directory.

If you select RADIUS as the authentication mechanism, you will need to specify the RADIUS server details.

1. Click **Add RADIUS Server**.
2. Select an authentication scheme. Possible values: PAP, CHAP, MSCHAPV2. It is not recommended to select the PAP scheme, as it is insecure since the password is transmitted in clear text.
3. Enter **Server Address**, **Port** and **Secret**.
4. Leave the **Check Message-Authenticator attribute** option enabled. This attribute is used to ensure the integrity of packets and protect them from forgery. Disabling the option is only permissible if the software you are using does not support working with this attribute.
5. Select **Name Format for Authentication**. Select the **Name without domain** value for authentication in FreeRadius. Select **Name in SAM format** or **Name in UPN format** for NPS RADIUS authentication.

You can specify multiple RADIUS servers to provide system fault tolerance. In this case, PAM sends the request to the RADIUS servers sequentially, in the order servers are specified in the configuration file. In other words, if it was unable to connect to the first RADIUS server, then PAM will try to connect to next one.

2FA configuration

> ⚠ **CAUTION**
> When selecting the RADIUS authentication mechanism, users from the directory are authenticated via RADIUS, and the following settings apply only to internal users.

1. Tick the **Enable two-factor authentication for all users by default** checkbox.
2. For the **Second factor type** switch, select the value: TOTP or Email.
3. Tick the components for which you want to enable second factor caching:

- Management Console
- User Console
- Desktop Console
- SSH Proxy
- RDP Proxy
- RDS Proxy

4. Optionally, edit the **Cache Time** field value.
5. Click **Next** to proceed to the next step of the wizard.

TOTP Second Factor via Email

If you select Email as the second factor, fill in the following fields:

- SMTP server
- Sender email address, it is the address from which the letter will be sent
- Port
- Username, it is the login for authorization on the server
- Password

Access Server

1. If necessary, edit the **Agent Maximum Response Time** and **Agent Healthcheck Interval** fields.
2. Click **Next** to proceed to the next step of the wizard.

Logging

1. If necessary, edit the **Logging Level**, the maximum number of management server log files, and the maximum number of access server log files.
2. Click **Next** to proceed to the next step of the wizard.

Syslog Events

The Syslog server is used for integration with a SIEM system and serves as a unified data storage for PAM event records and/or text session logs. Data is updated in real time: during an active remote connection, not after its completion.

1. Fill in the data for connecting the Syslog server.
   You can skip this step and, if necessary, add a Syslog server after installing PAM.

   Syslog server

   When adding a Syslog server, you will need to fill in the following fields:

   - Server address
   - Network protocol: TCP or UDP
   - Port
   - Event format: CEF or LEEF
   - Syslog version: RFC3164 or RFC5424

2. Click **Next** to proceed to the next step of the wizard.

Backup

A backup file of the wizard is an encrypted file that is used to restore the wizard state. You will need this file the next time you upgrade PAM to a new version or change the configuration of the current version of PAM.

> ⚠ **CAUTION**
> Save the backup file of the wizard and remember its password.
>
> Without this file and the password to it, you will not be able to change the configuration of your PAM installation in the future or update PAM to a new version via the wizard.

1. Set a password for the backup file.
2. Click **Download backup**.
3. Click **Next** to proceed to the next step of the wizard.

Installation

1. For the **Installation method** setting, select **From the wizard**.
2. Click **Install PAM**.
3. Track the process of installation using the progress bar. Wait until the installation is completed.

> **INFO**
>
> The installation log files are located at the following path: ..PAM_3.5/axidian-pam/logs/.
>
> If an installation error occurs, review these files and, if necessary, contact technical support for assistance in correcting the error.

4. Open the management console in a new tab to configure Axidian Privilege. Log in to the console using the credentials you specified in the Role Administrators step. For detailed information on initial setup, see the First Launch page.
5. Click **Stop the wizard** or run the following command in the terminal:

```
sudo bash stop-wizard.sh
```

Basic on Linux

Axidian Privilege components are installed on three servers. This type of installation allows you to separate the managing components from the components that provide access. Suitable for implementation and operation in production. Deployment scheme without balancing.

Before starting the installation, please prepare the environment.

Wizard Launch

Web Wizard is a web application that allows you to install, upgrade, or change the configuration of Axidian Privilege. The Web Wizard is supplied as part of the PAM distribution. To use the Wizard, you will need to run it in a Docker container using a special script.

1. Download and unpack the Web Wizard distribution on your Linux machine.
2. Place the CA certificate in `..PAM_3.5\axidian-pam\state\ca-certificates`. This is required for LDAPS to function properly. Skipping this step will result in an error for the wizard.
3. Launch the Web Wizard by the command:

   ```
   sudo bash run-wizard.sh
   ```

4. Wait for the script to complete.
5. Once the script is completed, go to the URL you see in the console.
6. In the **Authentication Code** field, enter the value you see in the console after executing the script.
   Code example: `vVHyTVRyKX5pxUKM6e1ZgCWEnOdXFdOy`.

   > **INFO**
   > By default, the code will be requested again after 2 hours, which means that all the work needs to be completed during this time.

7. Click **Enter** and proceed to work with the wizard.

Scenario

1. Select the **New PAM installation** scenario, and then select **Next**.

2. Select an installation option:

   - **Clean installation** — installation in which you complete all wizard steps.
     Select this option if you're installing Axidian Privilege for the first time.

   - **Installation from backup** — installation based on a saved PAM configuration.
     Select this option if you have a PAM configuration backup, for example, to resume an interrupted installation.

     On the next step, upload the configuration backup file and enter its password. To verify the backup version and continue, select **Verify backup**.

     After verification, all wizard settings are filled in according to the uploaded configuration. The settings can be edited.

     > ⚠ **CAUTION**
     > The backup version can't be higher than the wizard version.
     > Example: wizard version 3.4 won't work with a backup of version 3.5. Backups of versions 3.4 or 3.0 are suitable for it.

3. Select **Next** to go to the next wizard step.

<details>
<summary>More about scenarios</summary>

The following scenarios are available in the Web Wizard:

- **New PAM Installation** is an Axidian Privilege installation (clean or from a backup).
- **PAM Upgrade** is an upgrading of all Axidian Privilege components to the new version (for example, from 2.10 to 3.0). During the upgrade PAM will be unavailable. All current sessions will be terminated.
- **PAM Configuration Change** is making changes to the current PAM installation. For example, changing the set of hosts. The PAM version will remain the same. During the configuration change PAM will be unavailable. All current sessions will be terminated.
</details>

Hosts Scheme

A host is a physical or virtual server on which the PAM components will be located.

1. In the **Hosts Scheme** step, enter the fully qualified domain name of the management server in the **PAM FQDN** field.
   Example: pam.my-company.local.

2. Add the management server and the required access servers. You cannot add multiple hosts with the same address. The RDS access server is used for RemoteApp connections.

   > ⚠ **CAUTION**
   > Deploy PAM in a fault tolerance if you plan to install a Web Terminal server and host Web, RDP, SSH, MSSQL, or PostgreSQL access servers on two or more hosts.

   Management Server

   1. Click **Add Host**.
   2. For the **Host Operating System** setting, select **Linux**.
   3. Enable the **Management Server** checkbox.
   4. Enter the IP address or DNS in the **Host Address** field. Please note that you cannot add multiple hosts with the same address.
   5. Enter the port in the **Port** field.
   6. Select the method for authenticating your account on the host: **by password** or **by SSH key**.
      - If **by password** selected, enter **Login** and **Password**.
      - If **by SSH key** selected, enter **Login**, **sudo password**, **SSH key** and **Passphrase**.
   7. Click **Add**.

RDP Access Server

1. Click **Add Host**.
2. For the **Host Operating System** setting, select **Linux**.
3. Enable the **RDP Access Server** checkbox.
4. Enter the IP address or DNS in the **Host Address** field. Please note that you cannot add multiple hosts with the same address.
5. Enter the port in the **Port** field.
6. Select the method for authenticating your account on the host: **by password** or **by SSH key**.
   - If **by password** selected, enter **Login** and **Password**.
   - If **by SSH key** selected, enter **Login**, **sudo password**, **SSH key** and **Passphrase**.
7. Click **Add**.

SSH Access Server

1. Click **Add Host**.
2. For the **Host Operating System** setting, select **Linux**.
3. Enable the **SSH Access Server** checkbox.
4. Enter the IP address or DNS in the **Host Address** field. Please note that you cannot add multiple hosts with the same address.
5. Enter the port in the **Port** field.
6. Select the method for authenticating your account on the host: **by password** or **by SSH key**.
   - If **by password** selected, enter **Login** and **Password**.
   - If **by SSH key** selected, enter **Login**, **sudo password**, **SSH key** and **Passphrase**.
7. Click **Add**.

PostgreSQL Access Server

1. Click **Add Host**.
2. For the **Host Operating System** setting, select **Linux**.
3. Enable the **PostgreSQL Access Server** checkbox.
4. Enter the IP address or DNS in the **Host Address** field. Please note that you cannot add multiple hosts with the same address.
5. Enter the port in the **Port** field.
6. Select the method for authenticating your account on the host: **by password** or **by SSH key**.
   - If **by password** selected, enter **Login** and **Password**.
   - If **by SSH key** selected, enter **Login**, **sudo password**, **SSH key** and **Passphrase**.
7. Click **Add**.

MSSQL Access Server

1. Click **Add Host**.
2. For the **Host Operating System** setting, select **Linux**.
3. Enable the **MSSQL Access Server** checkbox.
4. Enter the IP address or DNS in the **Host Address** field. Please note that you cannot add multiple hosts with the same address.
5. Enter the port in the **Port** field.
6. Select the method for authenticating your account on the host: **by password** or **by SSH key**.
   - If **by password** selected, enter **Login** and **Password**.
   - If **by SSH key** selected, enter **Login**, **sudo password**, **SSH key** and **Passphrase**.
7. Click **Add**.

Web Access Server

1. Click **Add Host**.
2. For the **Host Operating System** setting, select **Linux**.
3. Enable the **Web Access Server** checkbox.
4. Enter the IP address or DNS in the **Host Address** field. Please note that you cannot add multiple hosts with the same address.
5. Enter the port in the **Port** field.
6. Select the method for authenticating your account on the host: **by password** or **by SSH key**.
   - If **by password** selected, enter **Login** and **Password**.
   - If **by SSH key** selected, enter **Login**, **sudo password**, **SSH key** and **Passphrase**.
7. Click **Add**.

Web Terminal Server

1. Click **Add Host**.
2. For the **Host Operating System** setting, select **Linux**.
3. Enable the **Web Terminal Server** checkbox.
4. Enter the IP address or DNS in the **Host Address** field. Please note that you cannot add multiple hosts with the same address.
5. Enter the port in the **Port** field.
6. Select the method for authenticating your account on the host: **by password** or **by SSH key**.
   - If **by password** selected, enter **Login** and **Password**.
   - If **by SSH key** selected, enter **Login**, **sudo password**, **SSH key** and **Passphrase**.
7. Click **Add**.

INFO

Management Server, Web Terminal and RDP, Web, SSH, MSSQL and PostgreSQL Access Servers can be located on the same host.

3. Review the host table and make sure that the data entered is correct. If you need to edit the host data, click on the line with the desired host, make changes and click **Save**. If you need to delete a host, click next to that host.

4. For the **Balancer** setting, select **Do not use**.

5. Click **Next** to proceed to the next step of the wizard.

Ports

> **INFO**
> Ports of PAM components must be unique.

1. Specify ports for PAM components according to your network architecture or leave the default values.

Component	Default port
SSH Proxy	2222
RDP Proxy	3390
PostgreSQL Proxy	5432
MSSQL Proxy	1433
Web Proxy	5443
MC/UC HTTP	80
MC/UC HTTPS	443
Gateway Service Web Terminal	8443

2. Click **Next** to proceed to the next step of the wizard.

Certificates

In this step you need to upload previously prepared certificates.

1. Upload the CA certificate without the private key in PEM (Base64) format with the .crt extension.
2. Upload certificates for hosts with the .pfx extension or a wildcard certificate and specify the password.
3. Click **Next** to proceed to the next step of the wizard.

Databases

1. Select **Server Type** PostgreSQL.
2. Enter **Server Address**.
3. Enable the **Secure connection to DBMS** checkbox.
4. Enter username and password for the database account.
5. For the **Encryption keys** setting, select **Generate new**.
6. Enter the names of the databases you created in the Preparation for Installation step:
    - DB for privileged accounts
    - DB for authenticators of PAM users
    - DB for PAM events
    - DB for Scheduled Jobs of the Core component
    - DB for Scheduled Jobs of the Idp component
7. Click **Next** to proceed to the next step of the wizard.

Selecting Microsoft SQL

1. Select **Server Type** Microsoft SQL.
2. Enter **Server Address** and **MSSQL Instance Name**.
3. Enable the **Secure connection to DBMS** checkbox.
4. Enter username and password for the database account.
5. For the **Encryption keys** setting, select **Generate new**.
6. Enter the names of the databases you created in the Preparation for Installation step:
   - DB for privileged accounts
   - DB for authenticators of PAM users
   - DB for PAM events
   - DB for Scheduled Jobs of the Core component
   - DB for Scheduled Jobs of the Idp component
7. Click **Next** to proceed to the next step of the wizard.

Data Storage

1. Select **Storage Type** File System.
2. Click **Next** to proceed to the next step of the wizard.

> **INFO**
> After PAM installation is complete, configure file storage (NFS).

Other storage types

If you select SMB, fill in the following fields:

- Network path
- Domain
- Username
- Password

If you select S3, fill in the following fields:

- Network address of the S3 server
- Path to the storage root directory on the S3 server
- Access key id
- Secret access key
- Region (optional)
- Location restriction (optional)

User Directories

Add one or more user directories, or click **Next** to use PAM with internal users only.

Selecting FreeIPA or OpenLDAP

1. Click **Add User Directory**.
2. In the **Directory Service** field, select **FreeIPA** or **OpenLDAP**.
3. In the **Catalog ID** field, enter the catalog ID in PAM.
   The value can consist of Latin letters and numbers, with a maximum length of 32 characters. If you plan to use multiple directories, then their IDs should be different.
4. Fill in the **Domain DNS name** field.
5. (Optional) In the **Domain Controllers** field, specify the address of the domain controller in the FQDN format.
   You can specify multiple addresses separated by commas.
   If you do not specify an address, PAM will connect using the DNS name of the domain.
6. In the **DN of the user container** field, specify the container where the system users are located.
7. Enter the user's name in DN format and their password.
   Example: `uid=pamadmin,cn=users,cn=accounts,dc=my,dc=company`.
8. (Optional) Enable the option **Use LDAPS**.
9. If you selected FreeIPA, specify **User and Group Identifier Format**: SID or GUID.
10. (Optional) Change the mapping of user attributes of users and/or attributes of user groups.
11. Click **Add**.
12. Click **Next** to proceed to the next step of the wizard.

Selecting Active Directory

1. Click **Add User Directory**.
2. In the **Directory Service** field, select **Active Directory**.
3. In the **Catalog ID** field, enter the catalog ID in PAM.
   The value can consist of Latin letters and numbers, with a maximum length of 32 characters. If you plan to use multiple directories, then their IDs should be different.
4. Fill in the **Domain DNS name** field.
5. (Optional) In the **Domain Controllers** field, specify the address of the domain controller in the FQDN format.
   You can specify multiple addresses separated by commas.
   If you do not specify an address, PAM will connect using the DNS name of the domain.
6. In the **DN of the user container** field, specify the container where the system users are located.
7. Enter the user's name in UPN format and their password.
   Example: `pamadmin@my.company`.
8. (Optional) Enable the option **Use LDAPS**.
9. (Optional) Change the mapping of user attributes of users and/or attributes of user groups.
10. Click **Add**.
11. Click **Next** to proceed to the next step of the wizard.

INFO

You can add multiple user directories.

Role Administrators

INFO

You can only specify one role administrator in the wizard.

You can select a user from the directory or an internal user to become the role administrator. The selected user will be granted the rights to manage the PAM roles. This user will be able to grant access rights to the PAM management console to other users.

User from the directory

1. Select an account from the directory.
2. Click **Next** to proceed to the next step of the wizard.

Internal user

1. Set login.

   > ⚠ **CAUTION**
   > The login cannot be changed after PAM is installed.

2. Set or generate a password. The password is only required for the first login. After logging in, the system will automatically request its change.
3. Enter an email.
4. Click **Next** to proceed to the next step of the wizard.

User Authentication

On this step you need to set up an authentication mechanism and configure two-factor authentication.

Authentication mechanism

1. Select the authentication mechanism: LDAP, RADIUS or Kerberos.
   - If you select RADIUS, add a RADIUS server and enter the required information.

RADIUS authentication

> ⚠ **CAUTION**
> RADIUS authentication is unavailable for internal users. The settings specified here apply only to users from the directory.

If you select RADIUS as the authentication mechanism, you will need to specify the RADIUS server details.

a. Click **Add RADIUS Server**.
b. Select an authentication scheme. Possible values: PAP, CHAP, MSCHAPV2. It is not recommended to select the PAP scheme, as it is insecure since the password is transmitted in clear text.
c. Enter **Server Address**, **Port** and **Secret**.
d. Leave the **Check Message-Authenticator attribute** option enabled. This attribute is used to ensure the integrity of packets and protect them from forgery. Disabling the option is only permissible if the software you are using does not support working with this attribute.
e. Select **Name Format for Authentication**. Select the **Name without domain** value for authentication in FreeRadius. Select **Name in SAM format** or **Name in UPN format** for NPS RADIUS authentication.

You can specify multiple RADIUS servers to provide system fault tolerance. In this case, PAM sends the request to the RADIUS servers sequentially, in the order servers are specified in the configuration file. In other words, if it was unable to connect to the first RADIUS server, then PAM will try to connect to next one.

- If you select Kerberos, upload the `keytab` file. The file must be generated with AES-256 encryption. For more information about configuring authentication, see Kerberos Authentication.

2FA configuration

> ⚠ **CAUTION**
> When selecting the RADIUS authentication mechanism, users from the directory are authenticated via RADIUS, and the following settings apply only to internal users.

1. Tick the **Enable two-factor authentication for all users by default** checkbox.
2. For the **Second factor type** switch, select the value: TOTP or Email.
3. Tick the components for which you want to enable second factor caching:
    - Management Console
    - User Console
    - Desktop Console
    - SSH Proxy
    - RDP Proxy
    - RDS Proxy
4. Optionally, edit the **Cache Time** field value.
5. Click **Next** to proceed to the next step of the wizard.

TOTP Second Factor via Email

If you select Email as the second factor, fill in the following fields:

- SMTP server
- Sender email address, it is the address from which the letter will be sent
- Port
- Username, it is the login for authorization on the server
- Password

Access Server

1. If necessary, edit the **Agent Maximum Response Time** and **Agent Healthcheck Interval** fields.
2. Click **Next** to proceed to the next step of the wizard.

Logging

1. If necessary, edit the **Logging Level**, the maximum number of management server log files, and the maximum number of access server log files.
2. Click **Next** to proceed to the next step of the wizard.

Syslog Events

The Syslog server is used for integration with a SIEM system and serves as a unified data storage for PAM event records and/or text session logs. Data is updated in real time: during an active remote connection, not after its completion.

1. Fill in the data for connecting the Syslog server.
   You can skip this step and, if necessary, add a Syslog server after installing PAM.

   Syslog server

   When adding a Syslog server, you will need to fill in the following fields:

   - Server address
   - Network protocol: TCP or UDP
   - Port
   - Event format: CEF or LEEF
   - Syslog version: RFC3164 or RFC5424

2. Click **Next** to proceed to the next step of the wizard.

Backup

A backup file of the wizard is an encrypted file that is used to restore the wizard state. You will need this file the next time you upgrade PAM to a new version or change the configuration of the current version of PAM.

> ⚠ **CAUTION**
> Save the backup file of the wizard and remember its password.
>
> Without this file and the password to it, you will not be able to change the configuration of your PAM installation in the future or update PAM to a new version via the wizard.

1. Set a password for the backup file.
2. Click **Download backup**.
3. Click **Next** to proceed to the next step of the wizard.

Installation

1. For the **Installation method** setting, select **From the wizard**.
2. Click **Install PAM**.
3. Track the process of installation using the progress bar. Wait until the installation is completed.

> **INFO**
>
> The installation log files are located at the following path: ..PAM_3.5/axidian-pam/logs/.
>
> If an installation error occurs, review these files and, if necessary, contact technical support for assistance in correcting the error.

4. Open the management console in a new tab to configure Axidian Privilege. Log in to the console using the credentials you specified in the Role Administrators step. For detailed information on initial setup, see the First Launch page.
5. Click **Stop the wizard** or run the following command in the terminal:

```
sudo bash stop-wizard.sh
```

Fault Tolerant on Windows

Axidian Privilege components are installed on three servers. This type of installation allows you to separate the managing components from the components that provide access. An additional server is used for fault tolerance. Suitable for implementation and operation in production. Deployment scheme with balancing.

Before starting the installation, please prepare the environment.

Wizard Launch

Web Wizard is a web application that allows you to install, upgrade, or change the configuration of Axidian Privilege. The Web Wizard is supplied as part of the PAM distribution. To use the Wizard, you will need to run it in a Docker container using a special script.

1. Download and unpack the Web Wizard distribution on your Linux machine.
2. Place the CA certificate in `..PAM_3.5\axidian-pam\state\ca-certificates`. This is required for LDAPS to function properly. Skipping this step will result in an error for the wizard.
3. Launch the Web Wizard by the command:

   ```
   sudo bash run-wizard.sh
   ```

4. Wait for the script to complete.
5. Once the script is completed, go to the URL you see in the console.
6. In the **Authentication Code** field, enter the value you see in the console after executing the script.
   Code example: `vVHyTVRyKX5pxUKM6e1ZgCWEnOdXFdOy`.

   > **INFO**
   > By default, the code will be requested again after 2 hours, which means that all the work needs to be completed during this time.

7. Click **Enter** and proceed to work with the wizard.

Scenario

1. Select the **New PAM installation** scenario, and then select **Next**.

2. Select an installation option:

   - **Clean installation** — installation in which you complete all wizard steps.
     Select this option if you're installing Axidian Privilege for the first time.

   - **Installation from backup** — installation based on a saved PAM configuration.
     Select this option if you have a PAM configuration backup, for example, to resume an interrupted installation.

     On the next step, upload the configuration backup file and enter its password. To verify the backup version and continue, select **Verify backup**.

     After verification, all wizard settings are filled in according to the uploaded configuration. The settings can be edited.

     > ⚠ **CAUTION**
     > The backup version can't be higher than the wizard version.
     > Example: wizard version 3.4 won't work with a backup of version 3.5. Backups of versions 3.4 or 3.0 are suitable for it.

3. Select **Next** to go to the next wizard step.

<details>
<summary>More about scenarios</summary>

The following scenarios are available in the Web Wizard:

- **New PAM Installation** is an Axidian Privilege installation (clean or from a backup).
- **PAM Upgrade** is an upgrading of all Axidian Privilege components to the new version (for example, from 2.10 to 3.0). During the upgrade PAM will be unavailable. All current sessions will be terminated.
- **PAM Configuration Change** is making changes to the current PAM installation. For example, changing the set of hosts. The PAM version will remain the same. During the configuration change PAM will be unavailable. All current sessions will be terminated.
</details>

Hosts Scheme

A host is a physical or virtual server on which the PAM components will be located.

1. In the **Hosts Scheme** step, enter the fully qualified domain name of the management server in the **PAM FQDN** field.
   Example: pam.my-company.local.

2. Add the management server and the required access servers. You cannot add multiple hosts with the same address. The RDS access server is used for RemoteApp connections.

   Management Server

   1. Click **Add Host**.
   2. For the **Host Operating System** setting, select **Windows**.
   3. Enable the **Management Server** checkbox.
   4. Enter the IP address or DNS in the **Host Address** field. Please note that you cannot add multiple hosts with the same address.
   5. Enter the port in the **Port** field.
   6. Select the account type for the host: a **shared domain account** or a **separate account for this host**.
   7. Enter **Login** in UPN or SAM format and **Password** for the specified account.
   8. Click **Add**.

RDS Access Server

1. Click **Add Host**.
2. For the **Host Operating System** setting, select **Windows**.
3. Enable the **RDS Access Server** checkbox.
4. Enter the IP address or DNS in the **Host Address** field. Please note that you cannot add multiple hosts with the same address.
5. Enter the port in the **Port** field.
6. Select the account type for the host: a **shared domain account** or a **separate account for this host**.
7. Enter **Login** in UPN or SAM format and **Password** for the specified account.
8. Click **Add**.

SSH Access Server

1. Click **Add Host**.
2. For the **Host Operating System** setting, select **Linux**.
3. Enable the **SSH Access Server** checkbox.
4. Enter the IP address or DNS in the **Host Address** field. Please note that you cannot add multiple hosts with the same address.
5. Enter the port in the **Port** field.
6. Select the method for authenticating your account on the host: **by password** or **by SSH key**.
   - If **by password** selected, enter **Login** and **Password**.
   - If **by SSH key** selected, enter **Login**, **sudo password**, **SSH key** and **Passphrase**.
7. Click **Add**.

PostgreSQL Access Server

1. Click **Add Host**.
2. For the **Host Operating System** setting, select **Linux**.
3. Enable the **PostgreSQL Access Server** checkbox.
4. Enter the IP address or DNS in the **Host Address** field. Please note that you cannot add multiple hosts with the same address.
5. Enter the port in the **Port** field.
6. Select the method for authenticating your account on the host: **by password** or **by SSH key**.
   - If **by password** selected, enter **Login** and **Password**.
   - If **by SSH key** selected, enter **Login**, **sudo password**, **SSH key** and **Passphrase**.
7. Click **Add**.

MSSQL Access Server

1. Click **Add Host**.
2. For the **Host Operating System** setting, select **Linux**.
3. Enable the **MSSQL Access Server** checkbox.
4. Enter the IP address or DNS in the **Host Address** field. Please note that you cannot add multiple hosts with the same address.
5. Enter the port in the **Port** field.
6. Select the method for authenticating your account on the host: **by password** or **by SSH key**.
   - If **by password** selected, enter **Login** and **Password**.
   - If **by SSH key** selected, enter **Login**, **sudo password**, **SSH key** and **Passphrase**.
7. Click **Add**.

Web Access Server

1. Click **Add Host**.
2. For the **Host Operating System** setting, select **Linux**.
3. Enable the **Web Access Server** checkbox.
4. Enter the IP address or DNS in the **Host Address** field. Please note that you cannot add multiple hosts with the same address.
5. Enter the port in the **Port** field.
6. Select the method for authenticating your account on the host: **by password** or **by SSH key**.
   - If **by password** selected, enter **Login** and **Password**.
   - If **by SSH key** selected, enter **Login**, **sudo password**, **SSH key** and **Passphrase**.
7. Click **Add**.

Web Terminal Server

1. Click **Add Host**.
2. For the **Host Operating System** setting, select **Linux**.
3. Enable the **Web Terminal Server** checkbox.
4. Enter the IP address or DNS in the **Host Address** field. Please note that you cannot add multiple hosts with the same address.
5. Enter the port in the **Port** field.
6. Select the method for authenticating your account on the host: **by password** or **by SSH key**.
   - If **by password** selected, enter **Login** and **Password**.
   - If **by SSH key** selected, enter **Login**, **sudo password**, **SSH key** and **Passphrase**.
7. Click **Add**.

INFO

Management Server and RDS Access Server can be located on the same host.
The Web Terminal Server and RDP, Web, SSH, MSSQL, and PostgreSQL access servers can be located on the same host.

3. Review the host table and make sure that the data entered is correct. If you need to edit the host data, click on the line with the desired host, make changes and click **Save**. If you need to delete a host, click next to that host.

4. For the **Balancer** setting, select **HAProxy**. This is a balancer that is shipped with PAM and is installed and configured as part of the PAM installation process. You can specify a maximum of 2 HAProxy balancers.

> **INFO**
> If you use a third-party load balancer, please note that you will need to configure it yourself. Make sure PAM is available at the address specified in the PAM FQDN field.

5. Add a balancer. Please note that you cannot add multiple balancers with the same address.

Balancer

1. Click **Add balancer**.
2. Enter the IP address or DNS in the **Balancer Address** field.
3. Enter the port in the **Port** field.
4. Select the method for authenticating your account on the host: **by password** or **by SSH key**.
   - If **by password** selected, enter **Login** and **Password**.
   - If **by SSH key** selected, enter **Login**, **sudo password**, **SSH key** and **Passphrase**.
5. Click **Add**.

6. Click **Next** to proceed to the next step of the wizard.

Ports

> **INFO**
> Ports of PAM components must be unique. Ports of HAProxy must be unique.

1. Specify ports for PAM components according to your network architecture or leave the default values.

Component	Default port
SSH Proxy	2222
RDP Proxy	3390
PostgreSQL Proxy	5432
MSSQL Proxy	1433
Web Proxy	5443
MC/UC HTTP	80
MC/UC HTTPS	443
Gateway Service Web Terminal	8443

2. Specify ports for HAProxy according to your network architecture or leave the default values.

HAProxy	Default port
HAProxy SSH	2222
HAProxy RDP	3390
HAProxy PostgreSQL	5432
HAProxy HTTP	80
HAProxy HTTPS	443

3. Click **Next** to proceed to the next step of the wizard.

Certificates

In this step you need to upload previously prepared certificates.

1. Upload the CA certificate without the private key in PEM (Base64) format with the .crt extension.

2. Upload certificates for hosts with the .pfx extension or a wildcard certificate and specify the password.
3. Click **Next** to proceed to the next step of the wizard.

Databases

1. Select **Server Type** Microsoft SQL.
2. Enter **Server Address** and **MSSQL Instance Name**.
3. Enable the **Secure connection to DBMS** checkbox.
4. Enter username and password for the database account.
5. For the **Encryption keys** setting, select **Generate new**.
6. Enter the names of the databases you created in the Preparation for Installation step:
   - DB for privileged accounts
   - DB for authenticators of PAM users
   - DB for PAM events
   - DB for Scheduled Jobs of the Core component
   - DB for Scheduled Jobs of the Idp component
7. Click **Next** to proceed to the next step of the wizard.

Selecting PostgreSQL

1. Select **Server Type** PostgreSQL.
2. Enter **Server Address**.
3. Enable the **Secure connection to DBMS** checkbox.
4. Enter username and password for the database account.
5. For the **Encryption keys** setting, select **Generate new**.
6. Enter the names of the databases you created in the Preparation for Installation step:
   - DB for privileged accounts
   - DB for authenticators of PAM users
   - DB for PAM events
   - DB for Scheduled Jobs of the Core component
   - DB for Scheduled Jobs of the Idp component
7. Click **Next** to proceed to the next step of the wizard.

Data Storage

1. Select **Storage Type** File System.
2. If necessary, edit the **Storage root directory** field.
3. Click **Next** to proceed to the next step of the wizard.

> ⓘ **INFO**
> After PAM installation is complete, configure file storage (NFS).

Other storage types

If you select SMB, fill in the following fields:

- Network path
- Domain
- Username
- Password

If you select S3, fill in the following fields:

- Network address of the S3 server
- Path to the storage root directory on the S3 server
- Access key id
- Secret access key
- Region (optional)
- Location restriction (optional)

User Directories

Add one or more user directories, or click **Next** to use PAM with internal users only.

> ⚠ **CAUTION**
> If you added an RDS access server on the **Hosts Scheme** step, be sure to add a user directory. You cannot continue with internal users only.

Selecting FreeIPA or OpenLDAP

1. Click **Add User Directory**.
2. In the **Directory Service** field, select **FreeIPA** or **OpenLDAP**.
3. In the **Catalog ID** field, enter the catalog ID in PAM.
   The value can consist of Latin letters and numbers, with a maximum length of 32 characters. If you plan to use multiple directories, then their IDs should be different.
4. Fill in the **Domain DNS name** field.
5. (Optional) In the **Domain Controllers** field, specify the address of the domain controller in the FQDN format.
   You can specify multiple addresses separated by commas.
   If you do not specify an address, PAM will connect using the DNS name of the domain.
6. In the **DN of the user container** field, specify the container where the system users are located.
7. Enter the user's name in DN format and their password.
   Example: `uid=pamadmin,cn=users,cn=accounts,dc=my,dc=company`.
8. (Optional) Enable the option **Use LDAPS**.
9. If you selected FreeIPA, specify **User and Group Identifier Format**: SID or GUID.
10. (Optional) Change the mapping of user attributes of users and/or attributes of user groups.
11. Click **Add**.
12. Click **Next** to proceed to the next step of the wizard.

Selecting Active Directory

1. Click **Add User Directory**.
2. In the **Directory Service** field, select **Active Directory**.
3. In the **Catalog ID** field, enter the catalog ID in PAM.
   The value can consist of Latin letters and numbers, with a maximum length of 32 characters. If you plan to use multiple directories, then their IDs should be different.
4. Fill in the **Domain DNS name** field.
5. (Optional) In the **Domain Controllers** field, specify the address of the domain controller in the FQDN format.
   You can specify multiple addresses separated by commas.
   If you do not specify an address, PAM will connect using the DNS name of the domain.
6. In the **DN of the user container** field, specify the container where the system users are located.
7. Enter the user's name in UPN format and their password.
   Example: `pamadmin@my.company`.
8. (Optional) Enable the option **Use LDAPS**.
9. (Optional) Change the mapping of user attributes of users and/or attributes of user groups.
10. Click **Add**.
11. Click **Next** to proceed to the next step of the wizard.

Role Administrators

> **INFO**
> You can only specify one role administrator in the wizard.

You can select a user from the directory or an internal user to become the role administrator. The selected user will be granted the rights to manage the PAM roles. This user will be able to grant access rights to the PAM management console to other users.

User from the directory

1. Select an account from the directory.

2. Click **Next** to proceed to the next step of the wizard.

Internal user

1. Set login.

   > ⚠ **CAUTION**
   > The login cannot be changed after PAM is installed.

2. Set or generate a password. The password is only required for the first login. After logging in, the system will automatically request its change.

3. Enter an email.

4. Click **Next** to proceed to the next step of the wizard.

User Authentication

On this step you need to set up an authentication mechanism and configure two-factor authentication.

Authentication mechanism

1. Select the authentication mechanism: LDAP, RADIUS or Kerberos.

   > ⓘ **INFO**
   > Kerberos authentication supports a single Active Directory domain.
   >
   > Signing in with a username and password is available only for internal PAM users.

2. If you selected RADIUS, add a RADIUS server and enter the required information.

RADIUS authentication

> ⚠ **CAUTION**
> RADIUS authentication is unavailable for internal users. The settings specified here apply only to users from the directory.

If you select RADIUS as the authentication mechanism, you will need to specify the RADIUS server details.

1. Click **Add RADIUS Server**.
2. Select an authentication scheme. Possible values: PAP, CHAP, MSCHAPV2. It is not recommended to select the PAP scheme, as it is insecure since the password is transmitted in clear text.
3. Enter **Server Address**, **Port** and **Secret**.
4. Leave the **Check Message-Authenticator attribute** option enabled. This attribute is used to ensure the integrity of packets and protect them from forgery. Disabling the option is only permissible if the software you are using does not support working with this attribute.
5. Select **Name Format for Authentication**. Select the **Name without domain** value for authentication in FreeRadius. Select **Name in SAM format** or **Name in UPN format** for NPS RADIUS authentication.

You can specify multiple RADIUS servers to provide system fault tolerance. In this case, PAM sends the request to the RADIUS servers sequentially, in the order servers are specified in the configuration file. In other words, if it was unable to connect to the first RADIUS server, then PAM will try to connect to next one.

2FA configuration

> ⚠ **CAUTION**
> When selecting the RADIUS authentication mechanism, users from the directory are authenticated via RADIUS, and the following settings apply only to internal users.

1. Tick the **Enable two-factor authentication for all users by default** checkbox.
2. For the **Second factor type** switch, select the value: TOTP or Email.
3. Tick the components for which you want to enable second factor caching:

- Management Console
- User Console
- Desktop Console
- SSH Proxy
- RDP Proxy
- RDS Proxy

4. Optionally, edit the **Cache Time** field value.
5. Click **Next** to proceed to the next step of the wizard.

TOTP Second Factor via Email

If you select Email as the second factor, fill in the following fields:

- SMTP server
- Sender email address, it is the address from which the letter will be sent
- Port
- Username, it is the login for authorization on the server
- Password

Access Server

1. If necessary, edit the **Agent Maximum Response Time** and **Agent Healthcheck Interval** fields.
2. Click **Next** to proceed to the next step of the wizard.

Logging

1. If necessary, edit the **Logging Level**, the maximum number of management server log files, and the maximum number of access server log files.
2. Click **Next** to proceed to the next step of the wizard.

Syslog Events

The Syslog server is used for integration with a SIEM system and serves as a unified data storage for PAM event records and/or text session logs. Data is updated in real time: during an active remote connection, not after its completion.

1. Fill in the data for connecting the Syslog server.
   You can skip this step and, if necessary, add a Syslog server after installing PAM.

   Syslog server

   When adding a Syslog server, you will need to fill in the following fields:

   - Server address
   - Network protocol: TCP or UDP
   - Port
   - Event format: CEF or LEEF
   - Syslog version: RFC3164 or RFC5424

2. Click **Next** to proceed to the next step of the wizard.

Backup

A backup file of the wizard is an encrypted file that is used to restore the wizard state. You will need this file the next time you upgrade PAM to a new version or change the configuration of the current version of PAM.

> ⚠ **CAUTION**
> Save the backup file of the wizard and remember its password.
>
> Without this file and the password to it, you will not be able to change the configuration of your PAM installation in the future or update PAM to a new version via the wizard.

1. Set a password for the backup file.
2. Click **Download backup**.
3. Click **Next** to proceed to the next step of the wizard.

Installation

1. For the **Installation method** setting, select **From the wizard**.
2. Click **Install PAM**.
3. Track the process of installation using the progress bar. Wait until the installation is completed.

> **INFO**
>
> The installation log files are located at the following path: ..PAM_3.5/axidian-pam/logs/.
>
> If an installation error occurs, review these files and, if necessary, contact technical support for assistance in correcting the error.

4. Open the management console in a new tab to configure Axidian Privilege. Log in to the console using the credentials you specified in the Role Administrators step. For detailed information on initial setup, see the First Launch page.
5. Click **Stop the wizard** or run the following command in the terminal:

```
sudo bash stop-wizard.sh
```

Fault Tolerant on Linux

Axidian Privilege components are installed on three servers. This type of installation allows you to separate the managing components from the components that provide access. An additional server is used for fault tolerance. Suitable for implementation and operation in production. Deployment scheme with balancing.

Before starting the installation, please prepare the environment.

Wizard Launch

Web Wizard is a web application that allows you to install, upgrade, or change the configuration of Axidian Privilege. The Web Wizard is supplied as part of the PAM distribution. To use the Wizard, you will need to run it in a Docker container using a special script.

1. Download and unpack the Web Wizard distribution on your Linux machine.
2. Place the CA certificate in `..PAM_3.5\axidian-pam\state\ca-certificates`. This is required for LDAPS to function properly. Skipping this step will result in an error for the wizard.
3. Launch the Web Wizard by the command:

   ```
   sudo bash run-wizard.sh
   ```

4. Wait for the script to complete.
5. Once the script is completed, go to the URL you see in the console.
6. In the **Authentication Code** field, enter the value you see in the console after executing the script.
   Code example: `vVHyTVRyKX5pxUKM6e1ZgCWEnOdXFdOy`.

   > **INFO**
   > By default, the code will be requested again after 2 hours, which means that all the work needs to be completed during this time.

7. Click **Enter** and proceed to work with the wizard.

Scenario

1. Select the **New PAM installation** scenario, and then select **Next**.

2. Select an installation option:

   - **Clean installation** — installation in which you complete all wizard steps.
     Select this option if you're installing Axidian Privilege for the first time.

   - **Installation from backup** — installation based on a saved PAM configuration.
     Select this option if you have a PAM configuration backup, for example, to resume an interrupted installation.

     On the next step, upload the configuration backup file and enter its password. To verify the backup version and continue, select **Verify backup**.

     After verification, all wizard settings are filled in according to the uploaded configuration. The settings can be edited.

     > ⚠ **CAUTION**
     > The backup version can't be higher than the wizard version.
     > Example: wizard version 3.4 won't work with a backup of version 3.5. Backups of versions 3.4 or 3.0 are suitable for it.

3. Select **Next** to go to the next wizard step.

More about scenarios

The following scenarios are available in the Web Wizard:

- **New PAM Installation** is an Axidian Privilege installation (clean or from a backup).
- **PAM Upgrade** is an upgrading of all Axidian Privilege components to the new version (for example, from 2.10 to 3.0). During the upgrade PAM will be unavailable. All current sessions will be terminated.
- **PAM Configuration Change** is making changes to the current PAM installation. For example, changing the set of hosts. The PAM version will remain the same. During the configuration change PAM will be unavailable. All current sessions will be terminated.

Hosts Scheme

A host is a physical or virtual server on which the PAM components will be located.

1. In the **Hosts Scheme** step, enter the fully qualified domain name of the management server in the **PAM FQDN** field.
   Example: pam.my-company.local.

2. Add the management server and the required access servers. You cannot add multiple hosts with the same address. The RDS access server is used for RemoteApp connections.

   Management Server

   1. Click **Add Host**.
   2. For the **Host Operating System** setting, select **Linux**.
   3. Enable the **Management Server** checkbox.
   4. Enter the IP address or DNS in the **Host Address** field. Please note that you cannot add multiple hosts with the same address.
   5. Enter the port in the **Port** field.
   6. Select the method for authenticating your account on the host: **by password** or **by SSH key**.
      - If **by password** selected, enter **Login** and **Password**.
      - If **by SSH key** selected, enter **Login**, **sudo password**, **SSH key** and **Passphrase**.
   7. Click **Add**.

RDP Access Server

1. Click **Add Host**.
2. For the **Host Operating System** setting, select **Linux**.
3. Enable the **RDP Access Server** checkbox.
4. Enter the IP address or DNS in the **Host Address** field. Please note that you cannot add multiple hosts with the same address.
5. Enter the port in the **Port** field.
6. Select the method for authenticating your account on the host: **by password** or **by SSH key**.
   - If **by password** selected, enter **Login** and **Password**.
   - If **by SSH key** selected, enter **Login**, **sudo password**, **SSH key** and **Passphrase**.
7. Click **Add**.

SSH Access Server

1. Click **Add Host**.
2. For the **Host Operating System** setting, select **Linux**.
3. Enable the **SSH Access Server** checkbox.
4. Enter the IP address or DNS in the **Host Address** field. Please note that you cannot add multiple hosts with the same address.
5. Enter the port in the **Port** field.
6. Select the method for authenticating your account on the host: **by password** or **by SSH key**.
   - If **by password** selected, enter **Login** and **Password**.
   - If **by SSH key** selected, enter **Login**, **sudo password**, **SSH key** and **Passphrase**.
7. Click **Add**.

PostgreSQL Access Server

1. Click **Add Host**.
2. For the **Host Operating System** setting, select **Linux**.
3. Enable the **PostgreSQL Access Server** checkbox.
4. Enter the IP address or DNS in the **Host Address** field. Please note that you cannot add multiple hosts with the same address.
5. Enter the port in the **Port** field.
6. Select the method for authenticating your account on the host: **by password** or **by SSH key**.
   - If **by password** selected, enter **Login** and **Password**.
   - If **by SSH key** selected, enter **Login**, **sudo password**, **SSH key** and **Passphrase**.
7. Click **Add**.

MSSQL Access Server

1. Click **Add Host**.
2. For the **Host Operating System** setting, select **Linux**.
3. Enable the **MSSQL Access Server** checkbox.
4. Enter the IP address or DNS in the **Host Address** field. Please note that you cannot add multiple hosts with the same address.
5. Enter the port in the **Port** field.
6. Select the method for authenticating your account on the host: **by password** or **by SSH key**.
   - If **by password** selected, enter **Login** and **Password**.
   - If **by SSH key** selected, enter **Login**, **sudo password**, **SSH key** and **Passphrase**.
7. Click **Add**.

Web Access Server

1. Click **Add Host**.
2. For the **Host Operating System** setting, select **Linux**.
3. Enable the **Web Access Server** checkbox.
4. Enter the IP address or DNS in the **Host Address** field. Please note that you cannot add multiple hosts with the same address.
5. Enter the port in the **Port** field.
6. Select the method for authenticating your account on the host: **by password** or **by SSH key**.
   - If **by password** selected, enter **Login** and **Password**.
   - If **by SSH key** selected, enter **Login**, **sudo password**, **SSH key** and **Passphrase**.
7. Click **Add**.

Web Terminal Server

1. Click **Add Host**.
2. For the **Host Operating System** setting, select **Linux**.
3. Enable the **Web Terminal Server** checkbox.
4. Enter the IP address or DNS in the **Host Address** field. Please note that you cannot add multiple hosts with the same address.
5. Enter the port in the **Port** field.
6. Select the method for authenticating your account on the host: **by password** or **by SSH key**.
   - If **by password** selected, enter **Login** and **Password**.
   - If **by SSH key** selected, enter **Login**, **sudo password**, **SSH key** and **Passphrase**.
7. Click **Add**.

INFO

Management Server, Web Terminal and RDP, Web, SSH, MSSQL and PostgreSQL Access Servers can be located on the same host.

3. Review the host table and make sure that the data entered is correct. If you need to edit the host data, click on the line with the desired host, make changes and click **Save**. If you need to delete a host, click next to that host.

4. For the **Balancer** setting, select **HAProxy**. This is a balancer that is shipped with PAM and is installed and configured as part of the PAM installation process. You can specify a maximum of 2 HAProxy balancers.

> ⓘ **INFO**
> If you use a third-party load balancer, please note that you will need to configure it yourself. Make sure PAM is available at the address specified in the PAM FQDN field.

5. Add a balancer. Please note that you cannot add multiple balancers with the same address.

> ▼ **Balancer**
>
> 1. Click **Add balancer**.
> 2. Enter the IP address or DNS in the **Balancer Address** field.
> 3. Enter the port in the **Port** field.
> 4. Select the method for authenticating your account on the host: **by password** or **by SSH key**.
>   - If **by password** selected, enter **Login** and **Password**.
>   - If **by SSH key** selected, enter **Login**, **sudo password**, **SSH key** and **Passphrase**.
> 5. Click **Add**.

6. Click **Next** to proceed to the next step of the wizard.

Ports

> ⓘ **INFO**
> Ports of PAM components must be unique. Ports of HAProxy must be unique.

1. Specify ports for PAM components according to your network architecture or leave the default values.

Component	Default port
SSH Proxy	2222
RDP Proxy	3390
PostgreSQL Proxy	5432
MSSQL Proxy	1433
Web Proxy	5443
MC/UC HTTP	80
MC/UC HTTPS	443
Gateway Service Web Terminal	8443

2. Specify ports for HAProxy according to your network architecture or leave the default values.

HAProxy	Default port
HAProxy SSH	2222
HAProxy RDP	3390
HAProxy PostgreSQL	5432
HAProxy HTTP	80
HAProxy HTTPS	443

3. Click **Next** to proceed to the next step of the wizard.

Certificates

In this step you need to upload previously prepared certificates.

1. Upload the CA certificate without the private key in PEM (Base64) format with the .crt extension.

2. Upload certificates for hosts with the .pfx extension or a wildcard certificate and specify the password.
3. Click **Next** to proceed to the next step of the wizard.

Databases

1. Select **Server Type** PostgreSQL.
2. Enter **Server Address**.
3. Enable the **Secure connection to DBMS** checkbox.
4. Enter username and password for the database account.
5. For the **Encryption keys** setting, select **Generate new**.
6. Enter the names of the databases you created in the Preparation for Installation step:
   - DB for privileged accounts
   - DB for authenticators of PAM users
   - DB for PAM events
   - DB for Scheduled Jobs of the Core component
   - DB for Scheduled Jobs of the Idp component
7. Click **Next** to proceed to the next step of the wizard.

Selecting Microsoft SQL

1. Select **Server Type** Microsoft SQL.
2. Enter **Server Address** and **MSSQL Instance Name**.
3. Enable the **Secure connection to DBMS** checkbox.
4. Enter username and password for the database account.
5. For the **Encryption keys** setting, select **Generate new**.
6. Enter the names of the databases you created in the Preparation for Installation step:
   - DB for privileged accounts
   - DB for authenticators of PAM users
   - DB for PAM events
   - DB for Scheduled Jobs of the Core component
   - DB for Scheduled Jobs of the Idp component
7. Click **Next** to proceed to the next step of the wizard.

Data Storage

1. Select **Storage Type** File System.
2. Click **Next** to proceed to the next step of the wizard.

> **INFO**
> After PAM installation is complete, configure file storage (NFS).

Other storage types

If you select SMB, fill in the following fields:

- Network path
- Domain
- Username
- Password

If you select S3, fill in the following fields:

- Network address of the S3 server
- Path to the storage root directory on the S3 server
- Access key id
- Secret access key
- Region (optional)
- Location restriction (optional)

User Directories

Add one or more user directories, or click **Next** to use PAM with internal users only.

Selecting FreeIPA or OpenLDAP

1. Click **Add User Directory**.
2. In the **Directory Service** field, select **FreeIPA** or **OpenLDAP**.
3. In the **Catalog ID** field, enter the catalog ID in PAM.
   The value can consist of Latin letters and numbers, with a maximum length of 32 characters. If you plan to use multiple directories, then their IDs should be different.
4. Fill in the **Domain DNS name** field.
5. (Optional) In the **Domain Controllers** field, specify the address of the domain controller in the FQDN format.
   You can specify multiple addresses separated by commas.
   If you do not specify an address, PAM will connect using the DNS name of the domain.
6. In the **DN of the user container** field, specify the container where the system users are located.
7. Enter the user's name in DN format and their password.
   Example: `uid=pamadmin,cn=users,cn=accounts,dc=my,dc=company`.
8. (Optional) Enable the option **Use LDAPS**.
9. If you selected FreeIPA, specify **User and Group Identifier Format**: SID or GUID.
10. (Optional) Change the mapping of user attributes of users and/or attributes of user groups.
11. Click **Add**.
12. Click **Next** to proceed to the next step of the wizard.

Selecting Active Directory

1. Click **Add User Directory**.
2. In the **Directory Service** field, select **Active Directory**.
3. In the **Catalog ID** field, enter the catalog ID in PAM.
   The value can consist of Latin letters and numbers, with a maximum length of 32 characters. If you plan to use multiple directories, then their IDs should be different.
4. Fill in the **Domain DNS name** field.
5. (Optional) In the **Domain Controllers** field, specify the address of the domain controller in the FQDN format.
   You can specify multiple addresses separated by commas.
   If you do not specify an address, PAM will connect using the DNS name of the domain.
6. In the **DN of the user container** field, specify the container where the system users are located.
7. Enter the user's name in UPN format and their password.
   Example: `pamadmin@my.company`.
8. (Optional) Enable the option **Use LDAPS**.
9. (Optional) Change the mapping of user attributes of users and/or attributes of user groups.
10. Click **Add**.
11. Click **Next** to proceed to the next step of the wizard.

Role Administrators

> **INFO**
> You can only specify one role administrator in the wizard.

You can select a user from the directory or an internal user to become the role administrator. The selected user will be granted the rights to manage the PAM roles. This user will be able to grant access rights to the PAM management console to other users.

User from the directory

1. Select an account from the directory.

2. Click **Next** to proceed to the next step of the wizard.

Internal user

1. Set login.

   > ⚠ **CAUTION**
   > The login cannot be changed after PAM is installed.

2. Set or generate a password. The password is only required for the first login. After logging in, the system will automatically request its change.
3. Enter an email.
4. Click **Next** to proceed to the next step of the wizard.

User Authentication

On this step you need to set up an authentication mechanism and configure two-factor authentication.

Authentication mechanism

1. Select the authentication mechanism: LDAP, RADIUS or Kerberos.
   - If you select RADIUS, add a RADIUS server and enter the required information.

RADIUS authentication

> ⚠ **CAUTION**
> RADIUS authentication is unavailable for internal users. The settings specified here apply only to users from the directory.

If you select RADIUS as the authentication mechanism, you will need to specify the RADIUS server details.

a. Click **Add RADIUS Server**.
b. Select an authentication scheme. Possible values: PAP, CHAP, MSCHAPV2. It is not recommended to select the PAP scheme, as it is insecure since the password is transmitted in clear text.
c. Enter **Server Address**, **Port** and **Secret**.
d. Leave the **Check Message-Authenticator attribute** option enabled. This attribute is used to ensure the integrity of packets and protect them from forgery. Disabling the option is only permissible if the software you are using does not support working with this attribute.
e. Select **Name Format for Authentication**. Select the **Name without domain** value for authentication in FreeRadius. Select **Name in SAM format** or **Name in UPN format** for NPS RADIUS authentication.

You can specify multiple RADIUS servers to provide system fault tolerance. In this case, PAM sends the request to the RADIUS servers sequentially, in the order servers are specified in the configuration file. In other words, if it was unable to connect to the first RADIUS server, then PAM will try to connect to next one.

- If you select Kerberos, upload the `keytab` file. The file must be generated with AES-256 encryption. For more information about configuring authentication, see Kerberos Authentication.

2FA configuration

> ⚠ **CAUTION**
> When selecting the RADIUS authentication mechanism, users from the directory are authenticated via RADIUS, and the following settings apply only to internal users.

1. Tick the **Enable two-factor authentication for all users by default** checkbox.
2. For the **Second factor type** switch, select the value: TOTP or Email.
3. Tick the components for which you want to enable second factor caching:
    - Management Console
    - User Console
    - Desktop Console
    - SSH Proxy
    - RDP Proxy
    - RDS Proxy
4. Optionally, edit the **Cache Time** field value.
5. Click **Next** to proceed to the next step of the wizard.

TOTP Second Factor via Email

If you select Email as the second factor, fill in the following fields:

- SMTP server
- Sender email address, it is the address from which the letter will be sent
- Port
- Username, it is the login for authorization on the server
- Password

Access Server

1. If necessary, edit the **Agent Maximum Response Time** and **Agent Healthcheck Interval** fields.
2. Click **Next** to proceed to the next step of the wizard.

Logging

1. If necessary, edit the **Logging Level**, the maximum number of management server log files, and the maximum number of access server log files.
2. Click **Next** to proceed to the next step of the wizard.

Syslog Events

The Syslog server is used for integration with a SIEM system and serves as a unified data storage for PAM event records and/or text session logs. Data is updated in real time: during an active remote connection, not after its completion.

1. Fill in the data for connecting the Syslog server.
   You can skip this step and, if necessary, add a Syslog server after installing PAM.

   Syslog server

   When adding a Syslog server, you will need to fill in the following fields:

   - Server address
   - Network protocol: TCP or UDP
   - Port
   - Event format: CEF or LEEF
   - Syslog version: RFC3164 or RFC5424

2. Click **Next** to proceed to the next step of the wizard.

Backup

A backup file of the wizard is an encrypted file that is used to restore the wizard state. You will need this file the next time you upgrade PAM to a new version or change the configuration of the current version of PAM.

> ⚠ **CAUTION**
> Save the backup file of the wizard and remember its password.
>
> Without this file and the password to it, you will not be able to change the configuration of your PAM installation in the future or update PAM to a new version via the wizard.

1. Set a password for the backup file.
2. Click **Download backup**.
3. Click **Next** to proceed to the next step of the wizard.

Installation

1. For the **Installation method** setting, select **From the wizard**.
2. Click **Install PAM**.
3. Track the process of installation using the progress bar. Wait until the installation is completed.

> **INFO**
>
> The installation log files are located at the following path: ..PAM_3.5/axidian-pam/logs/.
>
> If an installation error occurs, review these files and, if necessary, contact technical support for assistance in correcting the error.

4. Open the management console in a new tab to configure Axidian Privilege. Log in to the console using the credentials you specified in the Role Administrators step. For detailed information on initial setup, see the First Launch page.
5. Click **Stop the wizard** or run the following command in the terminal:

```
sudo bash stop-wizard.sh
```

Setup

Additional Components

3 items

Syslog Server

Syslog server is used to store PAM events and text session logs.

RDP File Signature Configuring

Edit the appsettings.json configuration file

Enabling Restart of Proxy Service Containers

Enable container restart for RDP Proxy and SSH Proxy access servers (optional)

Appendix A. Configuration files

Learn about the location of configuration files

Additional Components

PamSU

Component enables PAM users to run commands with administrative privileges

Privilege Agent

Component for text logging of RDP sessions

Desktop Console

Application for connecting to resources via SSH and RDP

PamSU

The PamSu component enables Axidian Privilege users to run commands with root privileges using the password of their own Active Directory user account.

Installation is performed manually on Linux resources, where you need to run commands with root privileges.

Installation

Depending on the Linux distribution, select the required installation package format:

- The .deb format is intended for Debian-based distributions: these include Debian and Ubuntu.
- The .rpm format is intended for RHEL-based distributions: these include CentOS, Oracle Linux, Rocky Linux and RHEL.

DEB

To install PamSu:

1. Go to the folder with the distribution `AxidianPAM_3.5\axidian-pam-tools\pamsu\`.
2. Install the PamSu utility of the latest OSSL version:

```
sudo dpkg -i "axidian-privilege.pamsu-ossl(3.1.8)-v3.5.0-master.373564.x64.deb"
```

If errors occurred during installation or PamSu does not work:

1. Remove the utility:

```
sudo dpkg -P pamsu
```

2. Install:
   - an earlier OSSL version, for example:

```
sudo dpkg -i "axidian-privilege.pamsu-ossl(1.1.1s)-v3.5.0-master.373564.x64.deb"
```

   - NO-SSL version, if additional cryptographic modules for OpenSSL are already installed:

```
sudo dpkg -i "axidian-privilege.pamsu-no-ossl(3.1.8)-v3.5.0-master.373564.x64.deb"
```

RPM

To install PamSu:

1. Go to the folder with the distribution `AxidianPAM_3.5\axidian-pam-tools\pamsu\`.
2. Install the PamSu utility of the latest OSSL version:

```
sudo dpkg -i "axidian-privilege.pamsu-ossl(3.1.8)-v3.5.0-master.373564.x64.rpm"
```

If errors occurred during installation or PamSu does not work:

1. Remove the utility:

```
sudo dpkg -P pamsu
```

2. Install:
   - an earlier OSSL version, for example:

```
sudo dpkg -i "axidian-privilege.pamsu-ossl(1.1.1s)-v3.5.0-master.373564.x64.rpm"
```

   - NO-SSL version, if additional cryptographic modules for OpenSSL are already installed:

```
sudo dpkg -i "axidian-privilege.pamsu-no-ossl(3.1.8)-v3.5.0-master.373564.x64.rpm"
```

If you were unable to install PamSu, contact technical support.

Configuration

On the resource, you need to configure trust for the certificates of the Core and IdP components.

To verify correct operation with certificates, execute the command:

```
curl https://pam.company.local/idp/
```

Open the `/etc/pamsu.conf` file in any editor with root privileges and specify the following parameters:

- **idp_url** — idp URL address
- **core_url** — core URL address
- **log_path** — path to the folder with log files
- **log_level** — logging level, can be INFO, WARN, ERROR, FATAL

Example

```
Set idp_url https://pam.company.local/idp
Set core_url https://pam.company.local/core
Set log_path /var/log
Set log_level INFO
```

On some Linux systems, the SSH server does not allow the **LC_ *** environment variables by default. For the application to work correctly, add the following line to the `/etc/ssh/sshd_config` file:

```
AcceptEnv LC_PAM_USER LC_PAM_SESSION_ID
```

or just

```
AcceptEnv LC_*
```

> ⓘ **INFO**
> To allow the execution of the pamsu command, you must enable the **Allow run pamsu** option in the **SSH** section in the policy.

Privilege Agent

The Privilege Agent component is used for text logging of RDP sessions. The session log contains records of active window changes, application and process launches, as well as keyboard input data.

Prerequisites

For the component to work, enable the Save session text logs option in the policy applied to the resource.

The session is aborted automatically if Privilege Agent is not installed on the resource, but a policy that requires saving logs is applied to the resource.

Installation

To install Privilege Agent and the service:

1. Go to the `[AxidianPAM distribution]\axidian-pam-tools\agent` folder.
2. Copy the installation packages for Axidian.Privilege.Agent and Axidian.Privilege.AgentService to the resource.

   > **INFO**
   > The service reduces high CPU load when several RDP sessions are open on the resource at the same time. During a session, the service starts automatically.

3. Install the agent and the service on the resource.
4. Reboot the resource.

Desktop Console

Configuring for Domain Computers

1. Copy the contents of the `axidian-pam-tools\desktop-console\PolicyDefinitions` folder on the domain controller to the `C:\Windows\sysvol\domain\policies\PolicyDefinitions` folder.
2. On the domain controller, start the **Group Policy Management Console** snap-in.
3. Select the required GPO, go to the section `Computer Configuration\Policies\Administrative Templates\Axidian Privilege\General\`.
4. Set **Enable** and fill in **Axidian Privilege connection settings**. Specify the following URLs: https://<your_FQDN>/core and https://<your_FQDN>/idp.
5. Update group policies on user's computer.

Configuring for Computers to which Domain Policies are not Applied

1. Copy the contents of the `axidian-pam-tools\desktop-console\PolicyDefinitions` folder to the `C:\Windows\PolicyDefinitions`.
2. Start local group policy editor **gpedit.msc**.
3. Go to the section `Computer Configuration\Policies\Administrative Templates\Axidian Privilege\General\`.
4. Set **Enable** and fill in **Axidian Privilege connection settings**. Specify the following URLs: https://<your_FQDN>/core and https://<your_FQDN>/idp.

Syslog Server

Send Events to Syslog

The Syslog server is used for integration with a SIEM system and serves as a unified data storage for PAM event records and/or text session logs. Data is updated in real time: during an active remote connection, not after its completion.

To send Event log records to a Syslog server, configure the configuration files according to the instructions below.
Sending text session logs to a Syslog server is configured in the Configuration section.

Windows

1. Go to the `C:\inetpub\wwwroot\ls\targetConfigs` folder, create a copy of the `sampleSyslog.config` file and rename it to `Pam.Syslog.config`, then edit the `<Settings> … </Settings>` according to the information below:

   - **HostName** — Syslog server name
   - **Port** — Syslog port number
   - **Protocol** — Syslog connection type: TCPoverTLS, TCP, UDP
   - **Format** — logging format: Plain, CEF, LEEF
   - **SyslogVersion** — select syslog protocol: RFC3164, RFC5424

   C:\inetpub\wwwroot\ls\targetConfigs

   ```
   <Settings HostName="localhost" Port="5081" Protocol="TCP" Format="CEF"
   SyslogVersion="RFC3164" />
   ```

2. In the `C:\inetpub\wwwroot\ls\clientApps.config` file edit `pam` section for work with the `Pam.Syslog.config` file. Add a new `TargetId` for the `WriteTarget`:

   C:\inetpub\wwwroot\ls\clientApps.config

```
<Application Id="pam" SchemaId="Pam.Schema">
  <ReadTargetId>Pam.TargetDb</ReadTargetId>
  <WriteTargets>
    <TargetId>Pam.TargetDb</TargetId>
    <TargetId>Pam.Syslog</TargetId>
  </WriteTargets>
  <AccessControl>
    <!--<CertificateAccessControl CertificateThumbprint="001122...AA11" Rights="Read" />-->
  </AccessControl>
</Application>
```

3. In the same file, in the `Targets` section add a new element, it should be the same as the configuration file name without extension:

C:\inetpub\wwwroot\ls\clientApps.config

```
<Targets>
  ...
  <Target Id="Pam.TargetDb" Type="mssql"/>
  <Target Id="Pam.Syslog" Type="syslog"/>
</Targets>
```

In `Target Id="Pam.TargetDb"` specify `Type` depending on the database you are using: `mssql` or `pgsql`.

Linux

1. Go to the `/etc/axidian/axidian-pam/ls/targets` folder, edit the `<Settings> … </Settings>` section of the `Pam.Syslog.config` file according to the information below:

   - **HostName** — Syslog server name
   - **Port** — Syslog port number
   - **Protocol** — Syslog connection type: TCPoverTLS, TCP, UDP
   - **Format** — logging format: Plain, CEF, LEEF
   - **SyslogVersion** — select syslog protocol: RFC3164, RFC5424

/etc/axidian/axidian-pam/ls/targets

```
<Settings HostName="localhost" Port="5081" Protocol="TCP" Format="CEF"
SyslogVersion="RFC3164" />
```

2. In the `/etc/axidian/axidian-pam/ls/clientApps.config` file edit `pam` section for work with the `Pam.Syslog.config` file. Add a new `TargetId` for the `WriteTarget`:

/etc/axidian/axidian-pam/ls/clientApps.config

```
<Application Id="pam" SchemaId="Pam.Schema">
  <ReadTargetId>Pam.DbTarget</ReadTargetId>
  <WriteTargets>
    <TargetId>Pam.DbTarget</TargetId>
    <TargetId>Pam.Syslog</TargetId>
  </WriteTargets>
  <AccessControl>
    <!--<CertificateAccessControl CertificateThumbprint="001122...AA11"
Rights="Read"/>-->
  </AccessControl>
</Application>
```

3. In the same file, in the `Targets` section add a new element, it should be the same as the configuration file name without extension:

/etc/axidian/axidian-pam/ls/clientApps.config

```
<Targets>
  ...
  <Target Id="Pam.DbTarget" Type="mssql"/>
  <Target Id="Pam.Syslog" Type="syslog"/>
</Targets>
```

In `Target Id="Pam.DbTarget"` specify `Type` depending on the database you are using: `mssql` or `pgsql`.

Send Text Logs to Syslog

To configure sending session text logs to the Syslog server, do the following:

1. In the administrator console, go to Configuration → System Settings.

2. Fill in the Syslog server parameters.

Option	Description
Syslog server	IP address or DNS name of Syslog server
Port	Syslog server port
Protocol	Network protocol for connection to Syslog server: TCP, UDP
Format	Event format used by syslog server: CEF, LEEF
Syslog version	IETF standard of Syslog protocol: RFC3164, RFC5424

3. Once the data is filled in, click **Check connection to the Syslog server**.
   Make sure that the test message has arrived at the Syslog server.

RDP File Signature Configuring

Configuring RDP file signing is performed on the management server with the Core component installed.

To enable signing, a PFX certificate issued by a certificate authority is required.

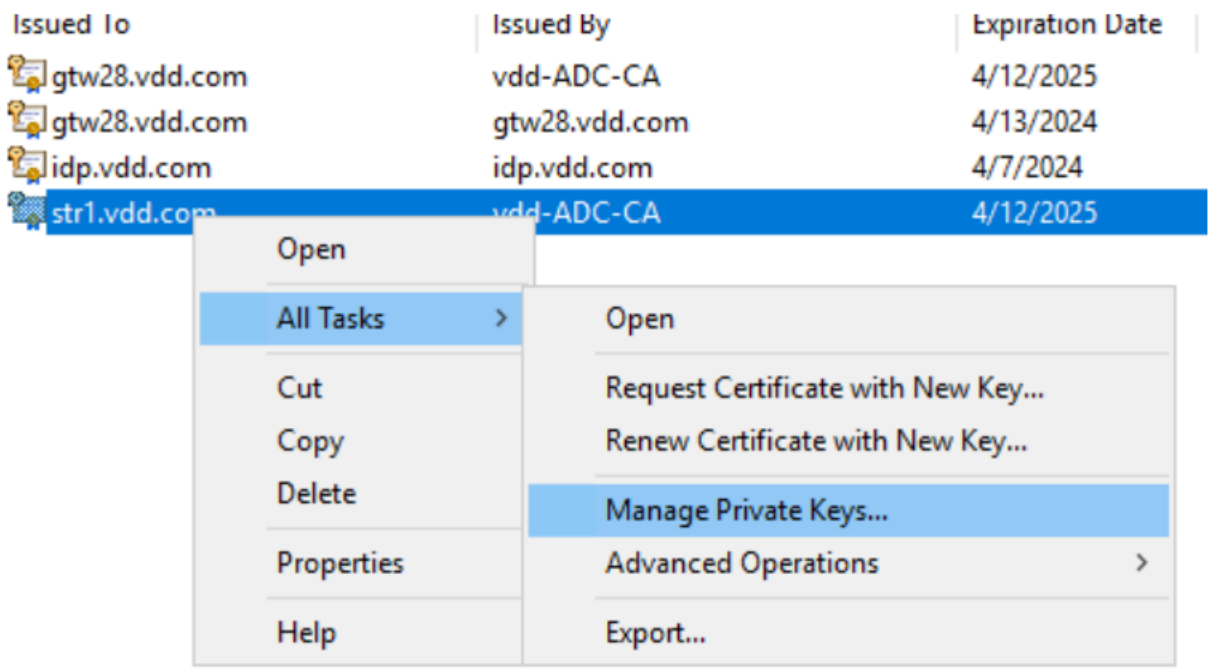
Windows

Configuring a certificate with thumbprint

1. Run PowerShell as administrator.
2. Open the Certificates snap-in using the command:

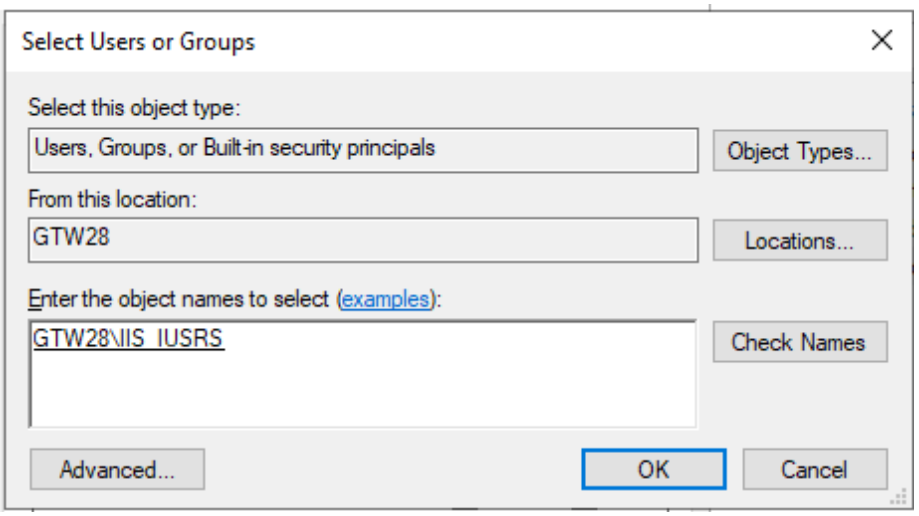
```
certlm.msc
```

3. Add the certificate to the computer's personal data storage.
4. Right-click on the certificate and select **All Tasks** → **Manage Private Keys**.



5. Click **Add**.
6. In the window that opens, click **Locations**, select the local computer, and click **OK**.

7. In the text field, enter the name `IIS_IUSRS`, click **OK**, and then **Apply**.



8. Double-click on the certificate and go to the **Details** tab.

9. In the list, find the **Thumbprint** field and click on it.

10. Copy the certificate thumbprint value without spaces.

Editing the configuration file

1. Open the `appsettings.json` configuration file of the Core component in an editor, which is located at the path:

C:\inetpub\wwwroot\core\appsettings.json

```
{
   "Rdp": {
       "UseRemoteApp": false,
       "SignRdpFile": true,
       "Certificate": "16c214ba7dec702a7ce5e4ac727502b0c0d448e2",
       "Password": ""
   }
}
```

2. Edit the `RDP` section:

   - For the `SignRdpFile` , set the value to `true` (enable RDP file signing).
   - For the `Certificate` specify the certificate thumbprint.

3. Save the changes.

Restarting the Core component

After editing the configuration file, you need to restart the Axidian Privilege Core component.

1. Run PowerShell as administrator.
2. Restart the Core application pool:

```
C:\Windows\System32\inetsrv\appcmd.exe recycle apppool Axidian.Privilege.Core
```

Linux

Configuring a certificate with key import

1. Copy the certificate to the folder `/etc/axidian/axidian-privilege/keys/core/`.
2. Open the configuration file `appsettings.json` of the Core component in an editor, which is located at:

/etc/axidian/axidian-privilege/core/appsettings.json

```
{
   "Rdp": {
     "UseRemoteApp": false,
     "SignRdpFile": true,
     "Certificate": "/etc/axidian/axidian-privilege/keys/core/rdp-sign.pfx",
     "Password": "1234"
   }
}
```

3. Edit the `RDP` section:
   - For the `SignRdpFile` key set the value to `true` (enable RDP file signing).
   - For the `Certificate` key, specify the path to the certificate.
   - For the `Password` key, specify the password that was set when exporting the certificate.
4. Save the changes.
5. Navigate to the folder `/etc/axidian/axidian-privilege/scripts/` with elevated privileges:

```
sudo -i
```

```
cd /etc/axidian/axidian-privilege/scripts/
```

6. Reset permissions on files with the script:

```
bash set-permissions.sh
```

Restarting the Core component

After editing the configuration file, you need to restart the Axidian Privilege Core component.

1. Go to the folder `/etc/axidian/axidian-privilege/scripts/` with elevated privileges:

```
sudo -i
```

```
cd /etc/axidian/axidian-privilege/scripts/
```

2. Restart the Core component with the script:

```
bash run-pam.sh
```

Enabling Restart of Proxy Service Containers

The RDP Proxy, SSH Proxy and SQL Proxy Docker containers require periodic restarting (rotation) to eliminate the effects of memory, thread and handle leaks. In Axidian PAM, this is implemented by a special script that runs automatically according to a schedule. PAM does not stop working during a restart (user sessions are not interrupted).

By default, restart is disabled. To enable it, you need to do the following steps:

1. Change the parameter value in the configuration file.
2. Reinstall the Access Server components.
3. Restart the Access Server.

Enabling Restart in the Configuration File

1. Open the `./scripts/ansible/vars.yml` file.
2. In the `proxy\_recycling` section, change the value of the `enabled` parameter from `false` to `true`.
3. Go to the next step: reinstalling the Access Server components.

> ⚠ **CAUTION**
> When using SELinux in Enforcing mode on the access server, you will need to manually add a context for the script, you will see a message about this:
>
> ```
> TASK [Warn about SELinux mode] ************************
>
> msg:
>
> 'Warning: SELinux is in enforcing mode. Add script context manually:'
> semanage fcontext -a -t bin_t /etc/axidian/axidian-privilege/scripts/recycle-proxy.sh &&
> restorecon -Fv /etc/axidian/axidian-privilege/scripts/recycle-proxy.sh
> ```
>
> So run the following command:
>
> ```
> semanage fcontext -a -t bin_t /etc/axidian/axidian-privilege/scripts/recycle-proxy.sh &&
> restorecon -Fv /etc/axidian/axidian-privilege/scripts/recycle-proxy.sh
> ```

Additional Settings

In the `./scripts/ansible/vars.yml` file, in the `proxy\_recycling` section there are several more parameters. Specify their values (optional) or use the default values.

- `replicas` — the number of Master replicas (active replicas that accept connections). Default is 1.
- `proxies` — types of proxies for which the restart will be performed. It is an array of values. Default is [rdp,ssh].
- `rotation\_hours` — replica rotation time in hours. Default is 168.
- `session\_hours` — maximum session duration in hours for a replica in the DRAIN state (when the server does not accept new connections, but processes existing ones). Default is 24.

Reinstalling the Access Server Components

> ⚠ **CAUTION**
> During the reinstalling the Access Server components PAM will be unavailable. All current sessions will be terminated.

1. If CIS Benchmark Docker security settings are applied, then run the installation script with the command:

   ```
   sudo bash run-deploy.sh
   ```

   If CIS Benchmark Docker security settings are not applied, then run the installation script with the command:

   ```
   sudo bash run-deploy.sh --bench-skip
   ```

2. At the **Enter target IP** step press ENTER.

3. When prompted, enter your local sudo user name (for example, root) and password.

4. Wait until the installation is complete

   > ⓘ **INFO**
   > If the script aborted with an error, send the log file to technical support.

5. Go to the next step: restarting the Access Server.

Restarting the Access Server

> ⚠ **CAUTION**
> Run all the commands from the /etc/axidian/axidian-privilege folder.

To restart the Axidian Privilege Access Server components, use the following commands:

```
sudo docker compose -f docker-compose.access-server.yml down
sudo docker compose -f docker-compose.access-server.yml up -d
```

or

```
sudo docker-compose -f docker-compose.access-server.yml down
sudo docker-compose -f docker-compose.access-server.yml up -d
```

Example of Restarting the RDP Proxy Component

```
sudo docker compose -f docker-compose.access-server.yml up -d rdp-proxy --force-recreate
```

or

```
sudo docker-compose -f docker-compose.access-server.yml up -d rdp-proxy --force-recreate
```

Example of Restarting the SSH Proxy Component

```
sudo docker compose -f docker-compose.access-server.yml up -d ssh-proxy --force-recreate
```

or

```
sudo docker-compose -f docker-compose.access-server.yml up -d ssh-proxy --force-recreate
```

Example of Restarting the SQL Proxy Component

```
sudo docker compose -f docker-compose.access-server.yml up -d sql-proxy --force-recreate
```

or

```
sudo docker-compose -f docker-compose.access-server.yml up -d sql-proxy --force-recreate
```

Appendix A. Configuration files

The section contains information about the location of configuration files.

After editing the configuration file, restart the component.

Windows

To restart the component:

1. Run PowerShell as administrator.
2. Launch IIS Manager:

```
start inetmgr
```

3. Click on the desired server in the left panel.
4. Click **Restart** in the right panel.

Component	Path to file
IdP	`C:\inetpub\wwwroot\idp\appsettings.json`
Core	`C:\inetpub\wwwroot\core\appsettings.json`
Management Console (mc)	`C:\inetpub\wwwroot\mc\assets\config\config.prod.json`
User Console (uc)	`C:\inetpub\wwwroot\uc\assets\config\config.prod.json`
ProxyApp	`C:\Program Files\Axidian\Axidian Privilege\Gateway\ProxyApp\appsettings.json`
Gateway Service	`C:\Program Files\Axidian\Axidian Privilege\Gateway\Pam.Gateway.Service\appsettings.json`

Component	Path to file

Log Server (ls)	`C:\inetpub\wwwroot\ls\appsettings.json`
	
	`C:\inetpub\wwwroot\ls\clientApps.config`

Linux

To restart the component:

1. Go to the folder `/etc/axidian/axidian-privilege/scripts`.

```
cd /etc/axidian/axidian-privilege/scripts/
```

2. Execute the command:

```
bash restart-pam.sh <component name>
```

Component	Path to file	Component name
IdP	`/etc/axidian/axidian-privilege/idp/appsettings.json`	`idp`
Core	`/etc/axidian/axidian-privilege/core/appsettings.json`	`core`
Management Console (mc)	`/etc/axidian/axidian-privilege/mc/config.prod.json`	`mc`
User Console (uc)	`/etc/axidian/axidian-privilege/uc/config.prod.json`	`uc`
SSH Proxy	`/etc/axidian/axidian-privilege/ssh-proxy/appsettings.json`	`ssh-proxy`
RDP Proxy	`/etc/axidian/axidian-privilege/rdp-proxy/appsettings.json`	`rdp-proxy`
PostgreSQL Proxy	`/etc/axidian/axidian-privilege/sql-proxy/appsettings.json`	`sql-proxy`

Component	Path to file	Component name
MSSQL Proxy	`/etc/axidian/axidian-privilege/tsql-proxy/appsettings.json`	`tsql-proxy`
Web Proxy	`/etc/axidian/axidian-privilege/web-proxy/appsettings.json`	`web-proxy`
Gateway Service	`/etc/axidian/axidian-privilege/gateway-service/appsettings.json`	`gateway-service`

Log Server (ls)	`/etc/axidian/axidian-privilege/ls/clientApps.config`
	`/etc/axidian/axidian-privilege/ls/targets/Pam.DbTarget.config`
	`/etc/axidian/axidian-privilege/ls/appsettings.json`
		`ls`

File .env	`/etc/axidian/axidian-privilege/.env`	—
Web Terminal	`/etc/axidian/axidian-privilege/web-terminal-proxy/appsettings.json` `/etc/axidian/axidian-privilege/web-terminal-tunnel/appsettings.yml`	`web-terminal-proxy`

PAM Configuration Change

Changing the configuration of the current PAM installation is performed using the Web Wizard. To change the configuration, you will need the backup file that was generated the last time you used the Web Wizard.

> ⚠ **CAUTION**
> During the configuration change PAM will be unavailable. All current sessions will be terminated.

Wizard Launch

Web Wizard is a web application that allows you to install, upgrade, or change the configuration of Axidian Privilege. The Web Wizard is supplied as part of the PAM distribution. To use the Wizard, you will need to run it in a Docker container using a special script.

1. Download and unpack the Web Wizard distribution on your Linux machine.
2. Place the CA certificate in `..PAM_3.4\axidian-pam\state\ca-certificates`. This is required for LDAPS to function properly. Skipping this step will result in an error for the wizard.
3. Launch the Web Wizard by the command:

   ```
   sudo bash run-wizard.sh
   ```

4. Wait for the script to complete.
5. Once the script is completed, go to the URL you see in the console.
6. In the **Authentication Code** field, enter the value you see in the console after executing the script.
   Code example: `vVHyTVRyKX5pxUKM6e1ZgCWEnOdXFdOy`.

   > ⓘ **INFO**
   > By default, the code will be requested again after 2 hours, which means that all the work needs to be completed during this time.

7. Click **Enter** and proceed to work with the wizard.

Scenario

1. Select **PAM Configuration Change**.
2. Click **Next**.

More about scenarios

The Web Wizard is used to perform one of three scenarios:

- **New PAM Installation** is an Axidian Privilege installation.
- **PAM Upgrade** is an upgrading of all Axidian Privilege components to the new version. For example, from 2.10 to 3.0. During the upgrade PAM will be unavailable. All current sessions will be terminated.
- **PAM Configuration Change** is making changes to the current PAM installation. For example, changing the set of hosts. The PAM version will remain the same. During the configuration change PAM will be unavailable. All current sessions will be terminated.

Uploading a Backup File

1. Upload the backup file and enter the password.
2. Click **Verify Backup**.
3. Once the verification is successfully completed, click **Next**.

Changing the Pre-filled Values of the Wizard

Because of the backup file you uploaded in the previous step, the wizard is pre-filled with the values of settings of your current Axidian Privilege installation. Change the desired parameters and/or set of hosts and proceed to the next step of the PAM configuration change.

Please note the limitations:

- Removing PAM from hosts that have been excluded from the host list is not implemented in the wizard. Removing PAM from hosts is done manually, without using the wizard.

- When adding a user directory, a certificate from the certification authority may be required.

  Read more

  Check which certification authority issued the LDAPS certificate for this user directory.

  Windows

  If there is no certificate of such CA in the storage of trusted CA on the PAM management servers, then add this CA certificate to the list of trusted root CA and restart the management server components in IIS.

  Linux

  If the certificate for this CA is not located in `/etc/axidian/axidian-pam/ca-certificates/` on the PAM management servers:

  i. Add the certificate of this CA to `/etc/axidian/axidian-pam/ca-certificates/`.

  ii. Navigate to the PAM folder:

  ```
  cd /etc/axidian/axidian-pam/
  ```

  iii. Set the rights to the certificate:

  ```
  sudo bash scripts/set-permissions.sh
  ```

  iv. Restart the management server components:

  ```
  sudo bash scripts/restart-pam.sh
  ```

- Passwords restored from a backup file cannot be viewed, but they can be changed.

Downloading a Backup File

In this step, you will need to download a new backup file, which you will need the next time you upgrade PAM to a new version or change the configuration of the current version of PAM.

1. Set a password for the backup file.
2. Click **Download backup**.

3. Click **Next** to proceed to the next step of the wizard.

Configuration Changing

> ⚠ **CAUTION**
> During the configuration change PAM will be unavailable. All current sessions will be terminated.

1. For the **Configuration change method** setting, select **From the wizard**.
2. Click **Apply Changes**.
3. Track the process of applying changes using the progress bar. Wait until the changes are applied.

   > ⓘ **INFO**
   > The log files are located at the following path: `..PAM_3.5/axidian-pam/logs/`.
   >
   > If an installation error occurs, review these files and, if necessary, contact technical support for assistance in correcting the error.

4. Once the changes are complete, click **Stop the wizard** or run the following command in the terminal:

   ```
   sudo bash stop-wizard.sh
   ```

Security Recommendations

Backup Accounts

Create a backup account for each resource

Security of Passwords and Secret Keys

Encrypt configuration files after finishing the installation

Process Filtering and File Security

Add processes allowed to run to the processprotection.settings.json configuration file (optional)

Session Logs Encryption

Read about encryption of session materials

Access Server Security Policy

Import a set of recommended policies to the Access Server

Access Server Security Settings

Apply the necessary security settings on the Access Server

Changing the Encryption Key of the PAM Database

Change your encryption key if it is compromised

Backup Accounts

Solutions of Privileged Access Management class are a combination of hardware, software and organizational tools that protect privileged accounts from unauthorised use.

One of the Axidian Privilege protection mechanisms is isolation of account passwords in the Axidian Privilege Core storage, encryption of those, as well as change of passwords to random or user-specified values on schedule or upon request.

The Axidian Privilege Core storage is a critical element. If it is damaged, then all the resources become inaccessible, since account passwords are unknown either to administrators or users.

It is highly recommended to assign a backup account for every resource. This account must possess local administrator privileges (Windows) or have privileges to execute SUDO command (Unix\Linux). This would allow to restore resource accessibility in case the data storage of Axidian Privilege Core fails. Therefore, you should assign an employee who is responsible for storing the backup accounts and passwords.

Security of Passwords and Secret Keys

By default, configuration files are automatically encrypted during component installation for additional system protection. Encryption of configuration critical files is performed using the AES-256 encryption key generated by the Data Protection API. The key is stored on the Axidian Privilege server and additionally encrypted by the Windows Data Protection API.

Component configuration files are encrypted:

- Core
- IdP
- Log Server
- ProxyApp
- RDP Proxy
- SSH Proxy
- PostgreSQL Proxy
- MSSQL Proxy
- Web Proxy
- Web Terminal
- Gateway Service

Windows Utility

Unencryption

1. Go to the `..PAM_3.5\axidian-pam-tools\configuration-protector\` folder, where the PAM distribution is located.

2. Run PowerShell as administrator.

3. Run one of the commands to perform unencryption.

    - Unencryption of all configuration files located in standard directories:

    ```
    .\Pam.Tools.Configuration.Protector.exe unprotect
    ```

> **INFO**
> The standard directory for configuration files is: C:\inetpub\wwwroot\<component_name>\appsettings.json.

- Unencryption of configuration files of individual components:

```
.\Pam.Tools.Configuration.Protector.exe unprotect --component enter_component_name
```

Example:

```
.\Pam.Tools.Configuration.Protector.exe unprotect --component core
```

- Unencryption of a configuration file located outside the standard directory:

```
.\Pam.Tools.Configuration.Protector.exe unprotect --component enter_component_name --file "file_path"
```

Example:

```
.\Pam.Tools.Configuration.Protector.exe unprotect --component Core --file "C:\inetpub\wwwroot\core\appsettings.json"
```

> **INFO**
> It is possible to specify the path without quotes if the path does not contain spaces.

Encryption

1. Go to the `..PAM_3.5\axidian-pam-tools\configuration-protector\` folder, where the PAM distribution is located.
2. Run PowerShell as administrator.
3. Run one of the commands to perform encryption.

- Encryption of all configuration files located in standard directories:

```
.\Pam.Tools.Configuration.Protector.exe protect
```

> **INFO**
> The standard directory for configuration files is: C:\inetpub\wwwroot\<component_name>\appsettings.json.

- Encryption of configuration files of individual components:

```
.\Pam.Tools.Configuration.Protector.exe protect --component enter_component_name
```

Example:

```
.\Pam.Tools.Configuration.Protector.exe protect --component core
```

- Encryption of a configuration file located outside the standard directory:

```
.\Pam.Tools.Configuration.Protector.exe protect --component enter_component_name --file "file_path"
```

Example:

```
.\Pam.Tools.Configuration.Protector.exe protect --component Core --file "C:\inetpub\wwwroot\core\appsettings.json"
```

> **INFO**
> It is possible to specify the path without quotes if the path does not contain spaces.

Linux Script

Unencryption

1. Go to the directory with the protector script:

```
cd /etc/axidian/axidian-privilege/tools
```

2. Run one of the commands to perform unencryption.

- Unencryption of all configuration files located in standard directories:

```
bash protector.sh unprotect
```

- Unencryption of configuration files of individual components:

```
bash protector.sh unprotect –component enter_component_name
```

Example:

```
bash protector.sh unprotect –component core
```

Encryption

1. Go to the directory with the protector script:

```
cd /etc/axidian/axidian-privilege/tools
```

2. Run one of the commands to perform encryption.

- Encryption of all configuration files located in standard directories:

```
bash protector.sh protect
```

- Encryption of configuration files of individual components:

```
bash protector.sh protect –component enter_component_name
```

Example:

```
bash protector.sh protect –component core
```

Encryption Mechanism Details

Encryption is performed using the AES-256 algorithm by a keyset which is generated using the Data Protection API. Keys are stored on the Axidian Privilege Server and encrypted using the Windows Data Protection API.

Location of keys:

- Windows Server — `%ProgramData%\Axidian\Keys`
- Linux OS — `/etc/axidian/axidian-pam/keys`

Directory usage rights are granted only to Axidian Privilege applications.

Process Filtering and File Security

Some functions have been implemented for the Access Server to protect against the launch of unwanted processes, as well as to restrict access to files that are vulnerable and necessary for normal operation.

Preventing Users from Starting Unwanted Processes

Each time the process starts, a series of checks are performed. The process is allowed to start if at least one of the checks is passed:

- If the user is `LOCAL_SYSTEM`, `LOCAL_SERVICE` or `NETWORK_SERVICE`.
- If the user is an administrator on the RDS server.
- If the parent process is one of the known system processes (svchost.exe, winlogon.exe, userinit.exe, rdpinit.exe).
- Process start is allowed in the `processprotection.settings.json` configuration file.

If none of the checks are passed, then the launch of the process is denied.

The behavior is configured in the following file:
`C:\Program Files\Axidian\Axidian Privilege\Gateway\ProcessCreateHook\processprotection.settings.json`.

Example of the processprotection.settings.json file

```
{
  "BlackListRules": [
    {
      "Comment": "Common, iexplore from shortcut",
      "ParentProcessPaths": [
        "C:\\Windows\\System32\\svchost.exe"
      ],
      "ApplicationPaths": [
        "C:\\Program Files\\Internet Explorer\\IEXPLORE.EXE",
        "C:\\Program Files (x86)\\Internet Explorer\\IEXPLORE.EXE"
      ]
    }
  ],

  "WhiteListRules": [
    {
      "Comment": "Common, record video",
      "ParentProcessPaths": [
        "C:\\Program Files\\Axidian\\Axidian Privilege\\Gateway\\ProxyApp\\Pam.Proxy.App.exe"
      ],
      "ApplicationPaths": [
        "C:\\Program Files\\Axidian\\Axidian Privilege\\Gateway\\ProxyApp\\ffmpeg.exe",
        "C:\\Program Files\\Axidian\\Axidian Privilege\\Gateway\\ProxyApp\\ffprobe.exe"
      ]
    },
    {
      "Comment": "Common, UserInit process",
      "ParentProcessPaths": [
        "C:\\Windows\\System32\\userinit.exe"
      ],
      "ApplicationPaths": [
        "C:\\Windows\\system32\\rdpinit.exe",
        "C:\\Program Files\\Axidian\\Axidian Privilege\\Gateway\\ProxyApp\\Pam.Proxy.App.exe"
      ]
    },
    {
      "Comment": "Common, RdpInit process",
      "ParentProcessPaths": [
        "C:\\Windows\\system32\\rdpinit.exe"
      ],
      "ApplicationPaths": [
        "C:\\Windows\\system32\\rdpshell.exe",
        "C:\\Program Files\\Axidian\\Axidian Privilege\\Gateway\\ProxyApp\\Pam.Proxy.App.exe"
      ]
    },
    {
      "Comment": "Common, start WebView for authentication on IDP",
      "ParentProcessPaths": [
        "C:\\Program Files\\Axidian\\Axidian Privilege\\Gateway\\ProxyApp\\Pam.Proxy.App.exe",
        "C:\\Program Files\\Axidian\\Axidian Privilege\\Gateway\\ProxyApp\\Microsoft.WebView2.FixedVersionRuntime\\msedgewebview2.exe"
```

```
      ],
      "ApplicationPaths": [
        "C:\\Program Files\\Axidian\\Axidian Privilege\\Gateway\\ProxyApp\\Microsoft.WebView2.FixedVersionRuntime\\msedgewebview2.exe"
      ]
    },
    {
      "Comment": "RDP",
      "ParentProcessPaths": [
        "C:\\Program Files\\Axidian\\Axidian Privilege\\Gateway\\ProxyApp\\Pam.Proxy.App.exe"
      ],
      "ApplicationPaths": [
        "C:\\Windows\\system32\\mstsc.exe",
        "C:\\Windows\\SysWOW64\\mstsc.exe"
      ]
    },
    {
      "Comment": "SSH",
      "ParentProcessPaths": [
        "C:\\Program Files\\Axidian\\Axidian Privilege\\Gateway\\ProxyApp\\Pam.Proxy.App.exe"
      ],
      "ApplicationPaths": [
        "C:\\Program Files\\Axidian\\Axidian Privilege\\Gateway\\SshClient\\Pam.Putty.exe"
      ]
    }
  ]
}
```

- `BlackListRules` — rules for prohibited processes.
- `WhiteListRules` — rules for permitted processes.

Rules parameters:

- `Comment` — comment for the rule.
- `ApplicationPaths` — paths to executable files that are allowed to launch.
- `ParentProcessPaths` — paths to executable files whose processes can launch applications from `ApplicationPaths`.

Protecting Vulnerable Files

It is a mechanism for differentiating access rights to files at the process level.

Users of the Local Administrators group have access to any file from any process. Other users can open any file from any process, except for vulnerable files. For vulnerable files, the process is checked: if the process is in the list of allowed, then access is allowed, otherwise it is denied.

The behavior is configured in the following file:

`C:\Program Files\Axidian\Axidian Privilege\Gateway\Service\filesprotection.settings.json`.

By default, vulnerable Axidian Privilege files are added to the configuration file, no additional configuration is required.

Example of the filesprotection.settings.json file

```
{
  "VulnerableFiles": [
    {
      "Path": "C:\\Program Files\\Axidian\\Axidian Privilege\\Gateway\\ProxyApp\\appsettings.json",
      "AllowedProcesses": [
        "C:\\Program Files\\Axidian\\Axidian Privilege\\Gateway\\ProxyApp\\Pam.Proxy.App.exe"
      ]
    },
    {
      "Path": "C:\\ProgramData\\Axidian\\Axidian Privilege\\SessionTemp\\RDP",
      "AllowedProcesses": [
        "C:\\Program Files\\Axidian\\Axidian Privilege\\Gateway\\ProxyApp\\Pam.Proxy.App.exe",
        "C:\\Windows\\System32\\mstsc.exe",
        "C:\\Windows\\SysWOW64\\mstsc.exe"
      ]
    },
    {
      "Path": "C:\\ProgramData\\Axidian\\Axidian Privilege\\SessionTemp\\SSH",
      "AllowedProcesses": [
        "C:\\Program Files\\Axidian\\Axidian Privilege\\Gateway\\ProxyApp\\Pam.Proxy.App.exe",
        "C:\\Program Files\\Axidian\\Axidian Privilege\\Gateway\\SshClient\\Pam.Putty.exe"
      ]
    },
    {
      "Path": "C:\\ProgramData\\Axidian\\Axidian Privilege\\SessionTemp\\Video",
      "AllowedProcesses": [
        "C:\\Program Files\\Axidian\\Axidian Privilege\\Gateway\\ProxyApp\\Pam.Proxy.App.exe",
        "C:\\Program Files\\Axidian\\Axidian Privilege\\Gateway\\ProxyApp\\ffmpeg.exe",
        "C:\\Program Files\\Axidian\\Axidian Privilege\\Gateway\\ProxyApp\\ffprobe.exe"
      ]
    },
    {
      "Path": "C:\\ProgramData\\Axidian\\Axidian Privilege\\PrivilegeStorage",
      "AllowedProcesses": [
        "C:\\Program Files\\Axidian\\Axidian Privilege\\Gateway\\ProxyApp\\Pam.Proxy.App.exe",
        "C:\\Program Files\\Axidian\\Axidian Privilege\\Gateway\\ProxyApp\\ffmpeg.exe",
        "C:\\Program Files\\Axidian\\Axidian Privilege\\Gateway\\ProxyApp\\ffprobe.exe",
        "C:\\Program Files\\Axidian\\Axidian Privilege\\Gateway\\SshClient\\Pam.Putty.exe"
      ]
    }
  ]
}
```

Parameters:

- `VulnerableFiles` — list of vulnerable files.
- `Path` — the path to the vulnerable file. You can specify both a specific file and a directory.

- `AllowedProcesses` — list of processes that are allowed to access the vulnerable file. Specify the required executable modules.

> ⚠ **CAUTION**
>
> After changing the configuration file, a restart of the Pam.Service service is required. You can do this in the Task manager, or with powershell command:

```
Restart-Service PAM.Service -Force
```

Session Logs Encryption

Providing access to protected privileged accounts is not the only task of Axidian Privilege. Logging tools are used to ensure the security of the account and the work process. During the session actions are recorded using video and screenshots. The footage is critical in terms of information security, as it is used to investigate incidents and is often confidential.

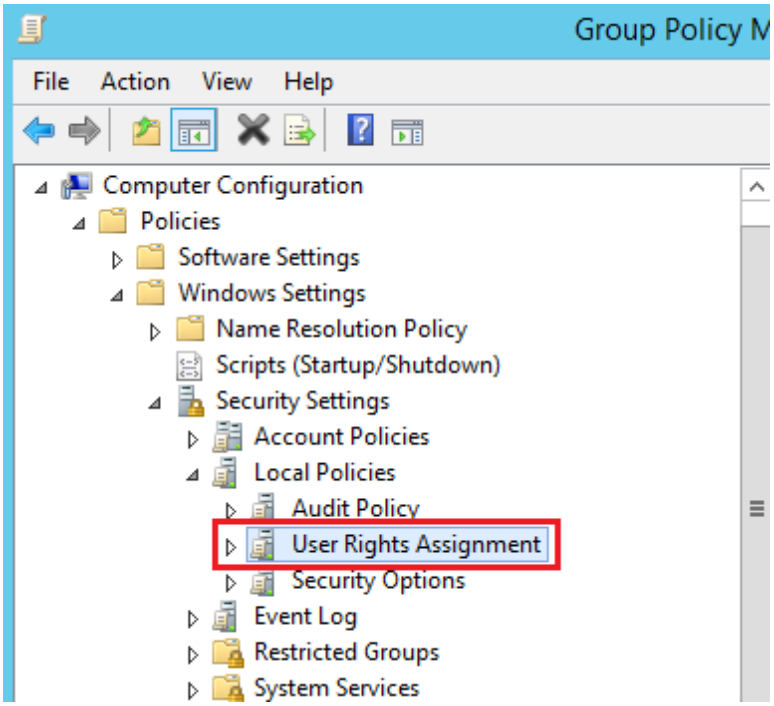
To ensure the security of footage, Axidian Privilege implements an encryption mechanism that allows you to safely store and use it within the solution. Encryption is performed using the AES256 algorithm, the key itself is unique for each Axidian Privilege session.

Access Server Security Policy

A set of standard Active Directory domain group policies recommended for use on a server performing the Axidian Privilege Gateway role to ensure security.

User Rights Assignment Section

Computer Configuration → Policies → Windows Settings → Security Settings → Local Policies → User Rights Assignment



Description of policies

Policy	Description	Values
Access Credential Manager as a trusted caller	This setting is used by Credential Manager during backup and recovery. This privilege should not be granted to accounts as it is only granted by Winlogon. Users' stored credentials can be compromised if this privilege is granted to others.	Undefined

Policy	Description	Values
Act as part of the operating system	This user right allows a process to impersonate any user without authentication. The process can thus access the same local resources as the user. Processes that require this privilege must use a LocalSystem account that already contains this privilege, rather than a separate user account with this privilege. If your organization only uses servers running the Windows Server 2003 family of operating systems, there is no need to assign this privilege to users. However, if your organization has servers running Windows 2000 or Windows NT 4.0, you may need to assign this privilege to users to make them possible to use applications that exchange passwords in plain text format. Attention! Assigning this right to a user may pose a security risk. Assign such rights only to trusted users.	Undefined

Policy	Description	Values
Adjust memory quotas for a process	This privilege determines who can change the maximum amount of memory used by a process. This user right is defined in the default domain controller's Group Policy Object (GPO) and in the local workstation and server security policy. Note. This privilege is useful when configuring a system, but its use can be harmful in such cases like attacks of type service denial.	NT AUTHORITY\NETWORK SERVICE, NT AUTHORITY\LOCAL SERVICE, BUILTIN\Administrators
Allow log on locally	This setting determines who can log on to the computer.	BUILTIN\Administrators
Allow log on through Remote Desktop Services	This security setting determines which users or groups have permission to log on as a Remote Desktop Services client.	BUILTIN\Administrators

Policy	Description	Values
Back up files and directories	This user right determines which users can override permissions on files, directories, the registry, and other persistent objects for the purpose of system backup. Specifically, this user right is similar to granting the following permissions to a user or group on all folders and files on the system: - Browse Folders/Execute Files - Folder Contents/Read Data - Reading attributes - Reading extended attributes - Reading Permissions Attention! Assigning this right to a user may pose a security risk. Since it is impossible to know exactly what the user is doing with the data - creating an archive, stealing or copying for distribution - assign this right only to trusted users.	BUILTIN\Administrators
Bypass traverse checking	This user right controls which users can browse directory trees, even if those users do not have directory permissions. This privilege does not allow users to view the contents of the directory, only browsing.	BUILTIN\Administrators, NT AUTHORITY\Authenticated Users, NT AUTHORITY\LOCAL SERVICE, NT AUTHORITY\NETWORK SERVICE

Policy	Description	Values
Change the system time	This user right determines which users and groups can change the time and date of the computer's internal clock. Users with this right can influence the view of event logs. If the system time has been changed, the tracked event entries will reflect the new time rather than the actual time the events occurred.	BUILTIN\Administrators, NT AUTHORITY\LOCAL SERVICE
Change the time zone	This user right determines which users and groups can change the time zone that the computer uses to display local time, which is the sum of the computer's system time and the time zone offset. The system time itself is absolute and does not change when you change the time zone.	BUILTIN\Administrators, NT AUTHORITY\LOCAL SERVICE

Policy	Description	Values
Create a token object	This security setting determines which accounts can be used by processes to create tokens, which can then be used to gain access to any local resources if the process uses an internal interface (API) to create the access token. This right is used by the operating system for internal purposes. Unless necessary, do not grant this right to any user, group, or process other than the Local System user. Attention! Assigning this right to a user may pose a security risk. Do not assign this right to a user, group, or process that you do not want to be allowed to control the system.	Undefined
Create global objects	This security setting determines whether users can create global objects that are available to all sessions. Users can still create objects for their sessions without this right. The creation of global objects can affect processes running in other users' sessions, leading to application errors and data corruption. Attention! Assigning this right to a user may pose a security risk. Assign it only to trusted users.	BUILTIN\Administrators, NT AUTHORITY\SERVICE

Policy	Description	Values
Create permanent shared objects	This user right controls which accounts can be used by processes to create a directory object using the Object Manager. This user right is used internally by the operating system and is useful for kernel-mode components that extend an object's namespace. Because this right is already assigned to components running in kernel mode, it does not need to be specifically assigned.	Undefined
Create symbolic links	This privilege defines the ability for a user to create symbolic links from the computer they are logged on to. Attention! Assign it only to trusted users. Symbolic links can expose vulnerabilities in applications that are not designed to handle them.	BUILTIN\Administrators

Policy	Description	Values
Debug programs	This user right controls which users can attach a debugger to any process or kernel.This right does not need to be assigned to developers who are debugging their own applications. Developers will need it to debug new system components. This user right provides full access to important operating system components. Attention! Assigning this right to a user may pose a security risk. Assign it only to trusted users.	BUILTIN\Administrators
Deny access to this computer from the network	This security setting determines which users are denied access to the computer from the network. This setting replaces the **Allow access to this computer from the network** policy setting if both policies apply to the user account.	BUILTIN\Guests
Deny log on as a batch job	This security setting determines which accounts are denied login as a batch job. This setting replaces the Allow logon as a batch job option if both options apply to the user account.	BUILTIN\Guests

Policy	Description	Values
Deny log on as a service	This security setting determines which service accounts are denied to execute registration of a process as a service. This policy setting replaces the "Allow logon as a service" setting if both options apply to the user account. Note. This security setting does not apply to the *System*, *Local Service*, or *Network Service* accounts.	BUILTIN\Guests
Deny log on locally	This security setting determines which users are denied to log on. This policy setting replaces the Allow local logon setting if both policies apply to the account. Attention! If this security setting is applied to the Everyone group, no one will be able to log on locally.	BUILTIN\Guests
Deny log on through Terminal Services	This security setting determines which users and groups are prohibited from logging on as a Remote Desktop Services client.	BUILTIN\Guests

Policy	Description	Values
Enable computer and user accounts to be trusted for delegation	This security setting determines which users can set the Delegation Allowed setting for a user or computer object. A user or object after getting this privilege will have write access to control flags of the user account or computer object. A server process running on a computer (or in a user context) that has delegation enabled can access the resources of another computer using the client's delegated credentials until the "Account cannot be delegated" control flag is set on the client account. This user right is defined in the default domain controller's Group Policy Object (GPO) and in the local workstation and server security policy. Attention! Improper use of this user right or the Delegation Allowed setting can leave the network vulnerable to sophisticated Trojan horse malware attacks that impersonate incoming clients and use their credentials to gain access to network resources.	BUILTIN\Administrators

Policy	Description	Values
Force shutdown from a remote system	This security setting determines which users are allowed to shut down the computer remotely. Improper use of this user right may result in a denial of service. This user right is defined in the default domain controller's Group Policy Object (GPO) and in the local workstation and server security policy.	BUILTIN\Administrators
Generate security audits	This security setting determines which accounts can be used by the process to write entries to the security log. The security log is used to track unauthorized access to the system. Improper use of this user right can cause multiple audit events to be generated that can hide evidence of an attack or cause a denial of service if the "Audit: Shut down system immediately if security audit logging cannot be logged" security setting is enabled. For more information, see "Audit: Shut down system immediately if security audit logging cannot be logged".	NT AUTHORITY\LOCAL SERVICE, NT AUTHORITY\NETWORK SERVICE

Policy	Description	Values
Impersonate a client after authentication	Granting a user this privilege allows programs running as that user to impersonate the client. Requiring this privilege for such impersonation prevents an unauthorized user from persuading a client to connect (for example, through a remote procedure call (RPC) or named pipes) to a service it has created and then impersonating the client, thereby elevating the client to administrative or system level privileges. Attention! Assigning this right to a user may pose a security risk. Assign such rights only to trusted users. Note. By default, the built-in Service group is added to the access tokens of services started by Service Control Manager. The built-in Service group is also added to the access tokens of COM servers that are launched by the COM framework and configured to run under a specific account. Therefore, these services receive this user right when they start. Additionally, a user can impersonate an access token if any of the following conditions are met: An impersonated access token is assigned to this user.In this login session, the user created an access token by explicitly providing login credentials.The requested level is lower	BUILTIN\Administrators, NT AUTHORITY\SERVICE

Policy	Description	Values
	than "Impersonate", for example: "Anonymous" or "Identify". Therefore, users generally do not need this user right. More information can be found by searching for SeImpersonatePrivilege in the Microsoft Platform SDK. Attention! Enabling this setting may cause programs that have this privilege to lose their Impersonate privilege and block their execution.	
Increase scheduling priority	This security setting determines which accounts can use a process that has the Write Property right on another process to elevate the execution priority assigned to the other process. A user with this privilege can change the execution priority of a process through the Task Manager user interface.	BUILTIN\Administrators

Policy	Description	Values
Load and unload device drivers	This user right determines which users can dynamically load and unload device drivers or other kernel-mode code. This user right does not apply to Plug and Play device drivers. It is not recommended to assign this privilege to other users. Attention! Assigning this right to a user may pose a security risk. Do not assign this right to a user, group, or process that you do not want to be allowed to control the system.	BUILTIN\Administrators
Lock pages in memory	This security setting determines which accounts can use processes to save data to physical memory to prevent that data from being flushed to virtual memory on disk. Using this privilege can significantly impact system performance by reducing the amount of available random access memory (RAM).	Undefined
Log on as a batch job	This security setting allows the user to log on using a tool that uses a batch job queue, and is provided only for compatibility with previous versions of Windows. For example, if a user submits a job using the Job Scheduler, the Job Scheduler logs the user into the system as a batch logon user rather than as an interactive user.	BUILTIN\Administrators

Policy	Description	Values
Manage auditing and security log	This security setting determines which users can specify object access audit settings for individual resources, such as files, Active Directory objects, and registry keys. This security setting does not allow the user to enable auditing of access to files and objects in general. To enable such auditing, you need to configure the access parameter to the "Audit" object in the path "Computer Configuration\Windows Settings\Security Settings\Local Policies\Audit Policies". Audit events can be viewed in the Event Viewer security log. A user with this privilege can also view and clear the security log.	BUILTIN\Administrators
Modify an object label	This privilege determines which user accounts are allowed to change the integrity labels of objects, such as files, registry keys, or processes that are owned by other users. Processes running under a user account without this privilege can demote the label level of an object that the user owns.	Undefined

Policy	Description	Values
Modify firmware environment values	This security setting determines who can change the hardware environment settings. Hardware environment variables are settings stored in the non-volatile memory of non-x86 computers. The parameter depends on the processor. On x86 computers, the only hardware environment value that can be changed by assigning this user right is the Last Known Good Configuration setting, which should only be changed by the system. On Itanium-based computers, boot data is stored in nonvolatile memory. This user right must be assigned to users to run the bootcfg.exe program and change the Default Operating System option in the Boot and Recovery component of the System Properties dialog box. On all computers, this user right is required to install and update Windows. Note. This security setting does not affect users who can change the system and user environment variables that appear on the Advanced tab of the System Properties dialog box. For information about how to change these variables, see Add or change the value of environment variables.	BUILTIN\Administrators

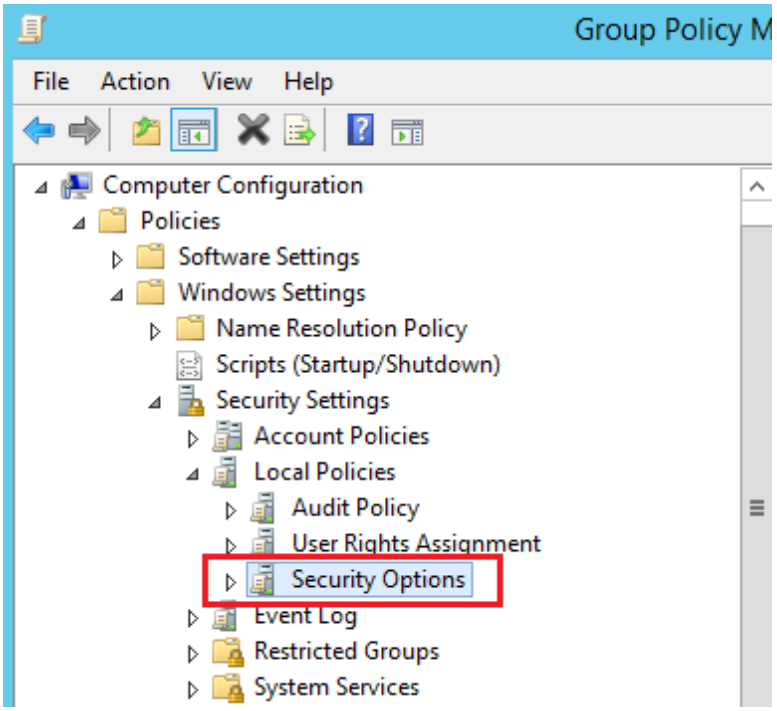
Policy	Description	Values
Perform volume maintenance tasks	This security setting determines the users and groups that can perform volume maintenance tasks, such as remote defragmentation. Be careful when assigning this user right. Users with this right can browse disks and add files to memory occupied by other data. After opening additional files, the user can read and change the requested data.	BUILTIN\Administrators
Profile single process	This security setting determines the users who can use performance monitoring tools to monitor the performance of non-system processes.	BUILTIN\Administrators
Profile system performance	This security setting determines the users who can use performance monitoring tools to monitor the performance of system processes.	BUILTIN\Administrators
Replace a process level token	This security setting determines the user accounts that can call the API procedure CreateProcessAsUser() to allow one service to start another. The Task Scheduler is an example of a process that uses this user right. For information about the Task Scheduler, see the Task Scheduler overview.	NT AUTHORITY\LOCAL SERVICE, NT AUTHORITY\NETWORK SERVICE

Policy	Description	Values
Restore files and directories	This security setting defines users who can bypass permissions on files, directories, the registry, and other persistent objects when restoring backup copies of files and directories, and users who can make any valid security principal the owner of an object. Specifically, this user right is similar to granting the following permissions to a user or group on all folders and files on the system: - Browse Folders/Execute Files -Write Attention! Assigning this right to a user may pose a security risk. Assign it only to trusted users, because this setting allows the user to overwrite registry settings, hide data, and take ownership of system objects.	BUILTIN\Administrators
Shut down the system	This security setting determines which users can shut down the operating system by using the Shut Down command after logging on locally. Improper use of this user right may result in a denial of service.	BUILTIN\Administrators

Policy	Description	Values
Take ownership of files or other objects	This security setting determines the users who can take ownership of any securable system object, including: Active Directory objects, files and folders, printers, registry keys, processes, and threads. Attention! Assigning this right to a user may pose a security risk. Assign it only to trusted users, because objects are fully controlled by their owners.	BUILTIN\Administrators

Security Options Section

Computer Configuration → Policies → Windows Settings → Security Settings → Local Policies → Security Options



Accounts

Description of policies

Policy	Description	Values
Accounts: Administrator account status	This security setting determines whether the local administrator account is enabled or disabled. Notes. If the current administrator's password does not meet the password requirements, you will not be able to re-enable the administrator account if it was previously disabled. In this case, the administrator account password must be reset by another member of the administrators group. For information, see Reset Your Password overview. Disabling the administrator account may hinder maintenance in some circumstances. When restarting in Safe Mode, a disabled administrator account can only be enabled if the computer is not joined to a domain and there are no other active local administrator accounts. If the computer is joined to a domain, the disabled administrator account cannot be enabled.	Enabled
Accounts: Guest account status	This security setting determines whether the guest account is enabled or disabled. Note. If the guest account is disabled and the Network Access: Sharing and security model for local accounts security setting is set to Guests only, network logon attempts made by, for example, Microsoft Network Server (SMB service) will fail.	Disabled

Policy	Description	Values
Accounts: Limit local account use of blank passwords to console logon only	This security setting determines whether local accounts that are not password-protected can be used to sign in from locations other than the computer's physical console. If enabled, local accounts that are not password protected can only log in using the computer keyboard. Attention! Computers located in physically unsecured locations should always enforce strong password settings for all local user accounts. Otherwise, any user with physical access to the computer can log in using a user account that does not have a password. This is especially important for laptop computers. If this security setting is applied to the Everyone group, no one will be able to log on through Remote Desktop Services. Notes. This setting has no effect if domain accounts are used to log in. Applications that use remote interactive logon can bypass this setting.	Enabled

Audit

Description of policies

Policy	Description	Values
Audit: Audit the use of Backup and Restore privilege	This security setting determines whether the use of all user privileges, including backup and restore, will be audited when the "Audit privilege use" policy is enabled. When the "Audit privilege use" policy is enabled, enabling this setting generates an audit event for each file that is backed up or restored. If this security setting is disabled, backup and restore privilege usage is not audited even if the "Audit privilege usage" option is enabled. Note. In versions of Windows earlier than Vista, changes made by configuring this security setting will not take effect until you restart Windows. Enabling this setting can cause a very large number of events (sometimes several hundred per second) during archiving.	Enabled

Devices

Description of policies

Policy	Description	Values
Devices: Allowed to format and eject removable media	This security setting determines who is allowed to format and eject NTFS removable media.	Administrators
Devices: Prevent users from installing printer drivers	For a local computer to use a shared printer, the shared printer driver must be installed on this local computer. This security setting determines who is allowed to install the printer driver when adding a shared printer. If this setting is enabled, only administrators can install the printer driver when adding a shared printer. If this option is disabled, anyone can install the printer driver when adding a shared printer. Notes. This setting does not affect the ability to add a local printer. This setting does not affect administrators.	Enabled
Devices: Restrict CD-ROM access to locally logged-on user only	This security setting determines whether the CD drive is accessible to both local and remote users. When enabled, access to CDs is limited to users who are logged on interactively. If this option is enabled and no one is logged on interactively, the CD drive will be accessible over the network.	Enabled

Policy	Description	Values
Devices: Restrict floppy access to locally logged-on user only	This security setting determines whether a removable floppy drive can be accessed by both local and remote users. When this setting is enabled, access to removable floppy drives is limited to users who are logged on interactively. If this option is enabled and no one is logged on interactively, the floppy drive will be accessible over the network.	Enabled

Interactive Logon

Description of policies

Policy	Description	Values
Interactive logon: Do not display last user name	This security setting determines whether the Windows logon screen displays the name of the last user logged on to this computer.If this policy is enabled, the username will not be displayed.	Enabled
Interactive logon: Do not require CTRL+ALT+DEL	This security setting determines whether CTRL+ALT+DEL is required before logging on. If this policy is enabled, you do not need to press CTRL+ALT+DEL before logging on. Not requiring users to press CTRL+ALT+DEL before logging in leaves users vulnerable to password sniffing attacks. Mandatory CTRL+ALT+DEL key presses before logging in ensure that data is transmitted over a trusted channel when users enter passwords. If this policy is disabled, pressing CTRL+ALT+DEL is required for any user before logging on to Windows.	Disabled

Policy	Description	Values
Interactive logon: Number of previous logons to cache (in case domain controller is not available)	The login information for each unique user is cached locally to ensure that logon is possible if the domain controller is not accessible during subsequent logon attempts. Cached login information is stored from the previous session. If the domain controller cannot be accessed and the user's logon information is not cached, the following message appears: "There are currently no login servers available to service your login request". For this policy setting, a 0 value disables login caching. Any value above 50 only caches 50 login attempts. Windows supports a maximum of 50 cache entries, with the number of entries consumed per user depending on the credentials. For example, Windows can cache up to 50 unique user accounts with passwords, but no more than 25 user accounts with a smart card, because both password and smart card information are stored. When a user with cached login information logs on again, that user's cached information is replaced with new data.	0 logons
Interactive logon: Require Domain Controller authentication to unlock workstation	To unlock a locked computer, you must provide login information. For domain accounts, this security setting determines whether a domain controller must be contacted to unlock the computer. If this setting is disabled, the user can unlock the computer using cached credentials. If this setting is enabled, the domain account used to unlock the computer must be verified as authentic by the domain controller.	Enabled

Microsoft Network Client

Description of policies

Policy	Description	Values
Microsoft network client: Send unencrypted password to third-party SMB servers	When this security setting is enabled, the Server Message Block (SMB) redirector is allowed to send cleartext passwords to non-Microsoft SMB servers that do not support password encryption during authentication. Sending unencrypted passwords poses a security risk.	Disabled

Network Access

Description of policies

Policy	Description	Values
Network access: Allow anonymous SID/Name translation	This policy setting determines whether an anonymous user can query another user's security identifier (SID) attributes. If this policy is enabled, then an anonymous user can request the SID of any other user.For example, an anonymous user who knows the administrator's SID can connect to a computer that has this policy enabled and obtain the administrator's name. This setting affects both the SID to name conversion and the reverse conversion (name to SID). If this policy setting is disabled, an anonymous user cannot request another user's SID.	Disabled

Policy	Description	Values
Network access: Do not allow anonymous enumeration of SAM accounts	This security setting determines what additional permissions are given to anonymous connections to this computer. Windows allows anonymous users to perform certain actions, such as listing domain account names and network shares. This is useful, for example, when an administrator needs to grant access to users in a trusted domain that does not support mutual trust. This security setting allows you to place additional restrictions on anonymous connections. Enabled: Do not allow enumeration of SAM accounts. This setting replaces the **Everyone** setting with the **Authenticated** in security permissions for resources. Disabled: No additional restrictions. Default permissions are used.	Enabled
Network access: Do not allow anonymous enumeration of SAM accounts and shares	This security setting determines whether anonymous users are allowed to enumerate SAM accounts and shares. Windows allows anonymous users to perform some actions (for example, enumeration domain account names and shared folders). This is useful if an administrator wants to grant access to users in a trusted domain that does not support mutual trust. Enable this setting to prevent anonymous users from enumerating SAM accounts and shares.	Enabled

Policy	Description	Values
Network access: Do not allow storage of passwords and credentials for network authentication	This security setting determines whether Credential Manager stores passwords and credentials during domain authentication (for later use). If this setting is enabled, Credential Manager does not save passwords and credentials on this computer. If this policy setting is disabled or not set, Credential Manager will store passwords and credentials on this computer (for future use during domain authentication). Note. Changes to the configuration of this security setting will take effect only after you restart Windows.	Enabled

Policy	Description	Values
Network access: Let Everyone permissions apply to anonymous users	This security setting determines what additional permissions are given to anonymous connections to your computer. Windows allows anonymous users to perform some actions (for example, enumeration domain account names and shared folders). This is useful if an administrator wants to grant access to users in a trusted domain that does not support mutual trust. By default, the Public SID is removed from the token generated for anonymous connections. Therefore, permissions in the Public group do not affect anonymous users. When this setting is set anonymous users have access only to resources that they are explicitly allowed to access. When enabled, the Public SID is added to the token generated for anonymous connections. In this case, anonymous users have access to any resource allowed in the Public group.	Disabled
Network access: Named Pipes that can be accessed anonymously	This security setting determines which communication sessions (channels) will have attributes and permissions that allow anonymous access.	Undefined
Network access: Remotely accessible registry paths	This security setting determines which registry paths can be accessed over the network, regardless of the users or user groups specified in the access control list (ACL) of the winreg registry key.	Undefined
Network access: Remotely accessible registry paths and sub-paths	This security setting determines which registry paths and subpaths can be accessed over the network, regardless of the users or user groups specified in the access control list (ACL) of the winreg.	Undefined

Policy	Description	Values
Network access: Restrict anonymous access to Named Pipes and Shares	When enabled, this security setting restricts anonymous access to shares and named pipes based on the following settings: - Network access: Allow anonymous access to named pipes - Network access: Allow anonymous access to shared resources	Enabled
Network access: Shares that can be accessed anonymously	This security setting determines which shares anonymous users can access.	Undefined

Policy	Description	Values
Network access: Sharing and security model for local accounts	This security setting determines how local accounts are authenticated when logging on to the network. If this setting is set to Normal, when you log on to the network with local account credentials, authentication is performed using those credentials. Setting the Normal value allows more flexible control of access to resources. It can be used to provide different types of access to different users to the same resource.When this setting is set to Guest, network logins using local account credentials are automatically mapped to the guest account. When setting the Guest value there is no difference between users. All users are authenticated with a guest account and given the same level of access to that resource — Read Only or Modify. By default on domain computers: Normal. By default on standalone computers: Guest. Attention! If the guest model is used, any user who has access to the computer over the network (including anonymous Internet users) can access shared resources. To protect your computer from unauthorized access, you must use Windows Firewall or another similar program. Additionally, when setting the Normal, local accounts must be password protected so that they cannot be used to access system shares. Note. This setting does not affect interactive logon operations that are performed remotely by using services such as Telnet or Remote Desktop Services.	Classic - local users authenticate as themselves

Network Security

Description of policies

Policy	Description	Values
Network security: Do not store LAN Manager hash value on next password change	This security setting determines whether the LAN Manager (LM) hash value for the new password should be stored the next time the password is changed. The LM hash is relatively weak and vulnerable to attack compared to the more secure Windows NT hash. Since the LM hash is stored in the security database on the local machine, if the security database is attacked, the passwords can be decrypted.	Enabled

Policy	Description	Values
Network security: Force logoff when logon hours expire	This security setting determines whether users are logged out when they connect to the local computer outside of the logon time that is configured for their account. This setting affects the Server Message Block (SMB) component. When this policy is enabled, client sessions with the SMB server are forced to terminate after the client logon timeout expires. If this policy is disabled, the client's session is retained after the client's login timeout expires. Note. This security setting is applied in the same way as an account policy. Domain accounts can only have one account policy. The account policy must be defined in the default domain policy; it is enforced by controllers in that domain. A domain controller always gets its account policy from the Default Domain Policy Group Policy Object (GPO), even if there is another account policy that applies to the organizational unit that contains that domain controller. By default, workstations and servers that are members of a domain receive the same account policy for their local accounts. However, the local account policies of these computers may differ from the domain account policies if an account policy is defined for the organizational unit that contains these computers. Kerberos settings do not apply to such computers.	Enabled

Policy	Description	Values
Network security: LAN Manager authentication level	This security setting determines which challenge-response authentication protocols are used for network logon. The value of this setting affects the level of authentication protocol that clients use, the level of negotiated session security, and the level of authentication accepted by servers as follows. Send LM and NTLM responses: Clients use LM and NTLM authentication and never use NTLMv2 session security; Domain controllers accept LM, NTLM, and NTLMv2 authentication. Send LM and NTLM - Use NTLMv2 session security when negotiating: Clients use LM and NTLM authentication, and NTLMv2 session security if the server supports it; Domain controllers accept LM, NTLM, and NTLMv2 authentication. Send NTLM response only: Clients use only NTLM authentication, and use NTLMv2 session security if the server supports it; Domain controllers accept LM, NTLM, and NTLMv2 authentication. Send NTLMv2 response only: Clients use only NTLMv2 authentication, and use NTLMv2 session security if the server supports it; Domain controllers accept LM, NTLM, and NTLMv2 authentication. Send only NTLMv2 response and refuse LM: Clients use only NTLMv2 authentication, and use NTLMv2 session security if the server supports it; Domain controllers reject LM (accepting only NTLM and NTLMv2 authentication). Send only NTLMv2 response and refuse LM and NTLM: Clients use only NTLMv2 authentication, and use NTLMv2 session security if the server supports	Send NTLMv2 response only. Refuse LM & NTLM

Policy	Description	Values
	it; Domain controllers reject LM and NTLM (accepting only NTLMv2 authentication).	
Network security: Minimum session security for NTLM SSP based (including secure RPC) clients	This security setting allows the client to require negotiation of 128-bit encryption and/or NTLMv2 session security. These values depend on the LAN Manager Authentication Level security setting. The following options are available: Require NTLMv2 session security. If the NTLMv2 protocol is not negotiated, the connection will not be established. Require 128-bit encryption. If 128-bit encryption is not negotiated, the connection will not be established.	Require NTLMv2 session security: Enabled Require 128-bit encryption: Enabled
Network security: Minimum session security for NTLM SSP based (including secure RPC) servers	This security setting allows the server to require negotiation of 128-bit encryption and/or NTLMv2 session security. These values depend on the LAN Manager Authentication Level security setting. The following options are available: Require NTLMv2 session security. If message integrity is not consistent, the connection will not be established. Require 128-bit encryption. If 128-bit encryption is not negotiated, the connection will not be established.	Require NTLMv2 session security: Enabled Require 128-bit encryption: Enabled

Shutdown

Description of policies

Policy	Description	Values
Shutdown: Allow system to be shut down without having to log on	This security setting determines whether you can shut down your computer without logging on to Windows. If this policy is enabled, the Shutdown option can be selected on the Windows logon screen. If this policy is disabled, the Shut Down command does not appear on the Windows logon screen. In this case, to shut down the system, the user must be successfully logged in and must have the Shut Down privilege.	Disabled
Shutdown: Clear virtual memory pagefile	This security setting determines whether the virtual memory page file is cleaned up when the system shuts down. Virtual memory support uses the system page file to swap memory pages to disk when they are not in use. While the system is running, the paging file is opened by the operating system in exclusive mode and is well protected. However, if the system is configured to allow other operating systems to boot, you must ensure that the system's page file is cleared when the system is shut down. This ensures that sensitive process memory information that may have ended up in the page file is not available to users who gain direct unauthorized access to the page file. If this policy is enabled, the system page file is cleared when the system shuts down properly. When enabled, this security setting also resets the hibernation file (hiberfil.sys) when hibernation is disabled.	Enabled

System Settings

Description of policies

Policy	Description	Values
System settings: Optional subsystems	This security setting determines which additional subsystems can be launched to support applications. This parameter allows you to specify all the subsystems that are required by your environment to support applications.	Undefined
System settings: Use Certificate Rules on Windows Executables for Software Restriction Policies	This security setting controls whether digital certificate processing occurs when a user or process attempts to run a program with an EXE file name extension. It allows you to enable or disable certificate rules (a software restriction policy rule). With these policies, you can create a certificate rule that allows or denies launch of programs signed with Authenticode, depending on digital certificate. To apply certificate rules, you must enable this security setting. When certificate rules are enabled, software restriction policies check the certificate revocation list (CRL) to ensure that the program's certificate and signature are valid. This may cause performance degradation when running signed programs. You can disable this feature. In the Trusted Publisher Properties window, clear the Publisher and Timestamp check boxes. For more information, see Trusted Publisher Settings.	Enabled

User Account Control

Description of policies

Policy	Description	Values
User Account Control: Admin Approval Mode for the Built-in Administrator account	This policy setting determines the administrator approval behavior characteristics of the built-in administrator account. Possible values: Enabled. The built-in Administrator account uses Administrator approval mode. By default, any operation that requires elevation of privilege prompts the user to confirm the operation. Disabled (default). The built-in Administrator account runs all applications with full Administrator rights.	Enabled
User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop	This policy setting controls whether UIAccess applications (UIA programs) can automatically disable the secure desktop for promotion requests used by a standard user. Enabled. UIA programs, including Windows Remote Assistance, automatically disable the secure desktop for elevation requests. If the "User Account Control: Switch to secure desktop when prompted for elevation" policy setting is not disabled, the prompt appears on the user's interactive desktop rather than on the secure desktop. Disabled (default). Secure Desktop can only be disabled by the Interactive Desktop user or by disabling the "User Account Control: Switch to Secure Desktop when prompted for elevation" policy setting.	Disabled

Policy	Description	Values
User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode	This policy setting controls the behavior of the privilege elevation prompt for administrators. Possible values: Promotion without request. Allows privileged accounts to perform an operation that requires elevation of privileges without requiring consent or entering credentials. Note. This option should only be used in highly restrictive environments. Prompt for credentials on the secure desktop. For any operation that requires elevation of privilege, the secure desktop prompts you to enter your privileged user name and password. If privileged credentials are entered, the operation continues with the user's maximum available privileges. Prompt for consent on a secure desktop. For any operation that requires elevation of privileges, the secure desktop prompts you to choose either Allow or Deny. If the user selects Allow, the operation continues with the user's maximum available privileges. For any operation that requires elevation of privileges, you are prompted to enter the user name and password for the administrator account. If valid credentials are entered, the operation continues with appropriate privileges. Prompt for consent. For any operation that requires elevation of privileges, the user is prompted to select either Allow or Deny. If the user selects Allow, the operation continues with the user's maximum available privileges.	Prompt for consent for non-Windows binaries

Policy	Description	Values
	Prompt for consent for third party (non-Windows) binaries (default). When an operation for a non-Microsoft application requires elevation of privileges, you are prompted to choose Allow or Deny on the secure desktop. If the user selects Allow, the operation continues with the user's maximum available privileges.	
User Account Control: Behavior of the elevation prompt for standard users	This policy setting determines the behavior of the privilege escalation prompt for standard users. Possible values: Prompt for credentials (default). When an operation requires elevation of privileges, you are prompted to enter the user name and password of a user account with administrator privileges. If the user enters valid credentials, the operation continues with appropriate privileges. Automatically reject requests to escalate privileges. When an operation requires elevation of privileges, an access denied error message is displayed. Organizations whose desktop computers are used by standard users can select this policy setting to reduce the number of support calls. Prompt for credentials on the secure desktop. When an operation requires elevation of privileges, the secure desktop prompts you to enter the other user's name and password. If the user enters valid credentials, the operation continues with appropriate privileges.	Prompt for credentials on the secure desktop

Policy	Description	Values
User Account Control: Only elevate UIAccess applications that are installed in secure locations	User Account Control: Elevate privileges only for UIAccess applications installed in a secure location. This policy setting determines whether applications that request execution at the UIAccess integrity level must reside in a secure folder on the file system. Only the following folders are considered safe: - …\Program Files\, including subfolders - …\Windows\system32\ - …\Program Files (x86)\, including subfolders for 64-bit versions of Windows Note. Windows enforces mandatory PKI signature verification on any interactive application that requests execution at the UIAccess integrity level, regardless of the state of this security setting. Possible values: Enabled (default). The application will only run with the UIAccess integrity level if it is located in a secure folder on the file system. Disabled. The application will run with the UIAccess integrity level even if it is not in a secure file system folder.	Enabled

Policy	Description	Values
User Account Control: Run all administrators in Admin Approval Mode	This policy setting determines the characteristics of all User Account Control policies for the computer. If you change this policy setting, you must restart the computer. Possible values: Enabled (default). Administrator approval mode is enabled. To allow the built-in Administrator account and all other users who are members of the Administrators group to operate in Administrator Approved mode, this policy must be enabled, and all associated account control policies must also be set accordingly. Disabled. Administrator approval mode and all associated User Account Control policy settings will be disabled. Note. If this policy setting is disabled, Security Center will notify you that the overall security of the operating system has been reduced.	Enabled

Policy	Description	Values
User Account Control: Switch to the secure desktop when prompting for elevation	This policy setting determines whether elevation prompts are displayed on the user's interactive desktop or on the secure desktop. Possible values: Enabled (default). All elevation requests are displayed on the secure desktop, regardless of the prompt behavior policy settings for administrators and standard users. Disabled. All requests for elevation of rights are displayed on the user's interactive desktop. The invitation behavior policy settings for administrators and standard users are used.	Enabled
User Account Control: Virtualize file and registry write failures to per-user locations	This policy setting controls the redirection of failures of writing the applications to specific locations in the registry and file system. This policy setting helps to reduce the risk of applications that run as an administrator and write the data to the %ProgramFiles%, %Windir%; %Windir%\system32 folder or in the HKLM\Software... folder at run time. Possible values: Enabled (default). Application write failures are redirected at runtime to user-defined locations in the file system and registry. Disabled. Applications that write data to secure locations fail with an error.	Enabled

Other

Description of policies

Policy	Description	Values
Accounts: Block Microsoft accounts	This policy setting prevents users from adding new Microsoft accounts on this computer. If you select the "Users can't add Microsoft accounts" option, users won't be able to create new Microsoft accounts on this computer, convert local accounts to Microsoft accounts, or connect domain accounts to Microsoft accounts. This option is preferred if you want to limit the number of Microsoft accounts you can use in your organization. If you select the "Users can't add or use Microsoft accounts to sign in" option, existing Microsoft account users won't be able to sign in to Windows. Selecting this option may make logging in and management of the system unavailable to an existing administrator on the computer. If this policy is disabled or not configured (recommended), users will be able to use Microsoft accounts in Windows.	Users can't add Microsoft accounts

Policy	Description	Values
Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings	Windows Vista and later versions of Windows allow you to more precisely control your audit policy by using audit policy subcategories. Setting an audit policy at the category level will override the new subcategory audit policy feature. To allow audit policy to be managed by subcategories without having to change Group Policy, Windows Vista and later versions provide a new registry value (SCENoApplyLegacyAuditPolicy) that prevents category-level audit policy from being applied from Group Policy and the Local Security Policy administration tool. If the category level audit policy set here is inconsistent with the events generated, then the cause may be because this registry key is set.	Enabled

Policy	Description	Values
Domain member: Disable machine account password changes	Determines whether the password for a domain member's computer account needs to be changed periodically. When you enable this setting, a domain member does not attempt to change the computer account password. If this setting is disabled, the domain member attempts to change the computer account password according to the Domain Member: Maximum computer account password age setting, which defaults to every 30 days. Default: Disabled. Notes. You should not enable this security setting. Account passwords are used to establish secure communication channels between domain members and domain controllers, and between domain controllers themselves within a domain. Once communication is established, the secure channel is used to transmit sensitive data needed to perform authentication and authorization. This option should not be used to support dual boot scenarios that use the same computer account. To dual boot two installations in the same domain, give the installations different computer names.	Disabled
Domain member: Maximum machine account password age	This security setting determines how often a domain member will attempt to change the computer account password.	30 days

Policy	Description	Values
Domain member: Require strong (Windows 2000 or later) session key	This security setting determines whether secure channel encrypted data requires a 128-bit key. When you join a computer to a domain, a computer account is created. Then, when the system starts, the computer account password is used to create a secure channel with the domain controller. This secure channel is used to perform operations such as NTLM pass-through authentication, LSA name or SID lookup, etc. Depending on the version of Windows used on the domain controller with which the connection is made, as well as on the parameter values: Domain Member: Digital signature or encryption of secure channel data is always required. Domain Member: Encrypt secure channel data whenever possible. All or some of the data transmitted over the secure channel will be encrypted. This policy setting determines whether encrypted secure channel data requires a 128-bit key. If this setting is enabled, a secure connection will only be established if 128-bit encryption is possible. If this setting is disabled, the key strength is negotiated with the domain controller.	Enabled

Policy	Description	Values
Interactive logon: Display user information when the session is locked	This setting determines whether additional information such as email address or domain/username is displayed with the username on the login screen. For customers running Windows 10 versions 1511 and 1507 (RTM), this setting works the same as in previous versions of Windows. Because of the addition of a new privacy setting in Windows 10 version 1607, this setting applies differently to these clients. Changes in Windows 10 version 1607 Starting with version 1607, Windows 10 has new functionality that lets you hide user information such as your email address by default, and change default settings to show this information. You can configure this functionality using the new privacy setting under Settings → Accounts → Sign-in Options. By default, the privacy setting is turned off and additional user information is hidden. This Group Policy setting defines this same functionality. Possible values: Display user name, domain and user names: If logged in locally, the user's full name is displayed. If the user signs in with a Microsoft account, the user's email address is displayed. If you are logged into a domain, the domain/username is displayed. Username Only: Displays the full name of the user who locked the session. Don't display user information: No names are displayed, but all versions of Windows older than Windows 10 will display users' full names on the change user screen. Starting with version 1607 of Windows 10, this	User display name only

Policy	Description	Values
	feature is no longer supported. If this value is selected, the full name of the user who has blocked the session will be displayed on the screen. This change makes this setting consistent with the new privacy setting. To prevent any user information from being displayed on the screen, enable the Interactive Logon Group Policy setting: Do not display information about the last logged on user. Empty: Default value. Means "Undefined", but the user's full name will be displayed on the screen in the same way as if "Username Only" was selected. Hotfix for Windows 10 version 1607 If you are using Windows 10 version 1607, user information will not be displayed on the login screen even if you select "Display user name, domain and user names" because the privacy setting is disabled. If you enable this option, the data will appear on the screen. You cannot change privacy settings in groups. Instead, you can apply KB4013429 to clients running Windows 10 version 1607 so that the system behaves similarly to previous versions of Windows. Interaction with the "Prevent user from displaying account information on login screen" command. In all versions of Windows 10, only the username is displayed by default. When set to "Prevent user from displaying account information on login screen", only the user's display name will be displayed on the login screen, regardless of Group Policy settings. Users will not be able to display their information.	

Policy	Description	Values
	If you do not set the "Prevent user from displaying account information on login screen" setting, you can set the "Interactive logon: Display user information if session is locked" setting to "Display user name, domain and user names" so that the screen displays additional user information such as domain\username when logging in. In this case, KB4013429 must be applied to client computers running Windows 10 version 1607. Users will not be able to hide additional information. Recommendations. Whether you can enforce this policy depends on your security requirements for the login credentials displaying. If you work with computers that store sensitive information and have monitors in unsecured locations, or if your computers with sensitive information are accessed remotely, displaying the full names of logged-in users or domain account names may be against your overall security policy. Based on your security policy, it may be appropriate to set the value to "Interactive logon: Do not display last user's credentials."	

Policy	Description	Values
Interactive logon: Machine account lockout threshold	This security setting determines the number of failed logon attempts before the computer restarts. Computers that have Bitlocker enabled to protect OS volumes will be locked. To remove the lock, you must specify the recovery key in the console. Make sure the appropriate access recovery policies are enabled. The number of unsuccessful access attempts can be specified as a number from 1 to 999. If you set this value to 0, the computer will never lock. Values between 1 and 3 will be interpreted as 4. Failed password attempts on workstations or member servers that are locked using CTRL+ALT+DEL or password-protected screen savers are considered failed login attempts.	5 invalid logon attempts
Microsoft network server: Amount of idle time required before suspending session	This security setting determines how long an SMB session can elapse before it is suspended due to inactivity. Administrators can use this setting to control when the computer suspends an inactive SMB session. If client activity resumes, the session is automatically re-established. For this parameter, a value of "0" means the session will be disconnected as soon as possible. The maximum value is 99999, which is 208 days; in effect, this value disables this option. Default: parameter not defined; this means that the system treats the parameter as having a value of "15" for servers and an undefined value for workstations.	15 minutes

Policy	Description	Values
Microsoft network server: Attempt S4U2Self to obtain claim information	This security setting is intended to support clients with systems released before Windows 8 that attempt to access a file share that requires a user request. It determines whether the local file server will attempt to use the Kerberos Service-For-User-To-Self (S4U2Self) feature to obtain network client principal requests from the client account domain. This setting only needs to be enabled if the file server uses user claims to control access to files and if it will support client principals whose accounts are in a domain with client computers and domain controllers running an operating system that was released before Windows 8. This setting should be set to Automatic (the default) so that the file server can automatically determine whether a user is required to enroll. This setting should only be explicitly set to Enabled if you have local file access policies that include user access claims. When this security setting is enabled, the Windows File Server will analyze the subject access token of the authenticated network client and determine whether the claim information is present. If there are no claims, the file server will use the Kerberos S4U2Self function to contact the Windows Server 2012 domain controller in the client account's domain and obtain a claim-aware access token for the client subject.A claim-aware token may be required to access files and folders that have a claim-based access control policy applied to them. If this setting is disabled, Windows File Server will not attempt to obtain a claims-based access token for the client principal.	Disabled

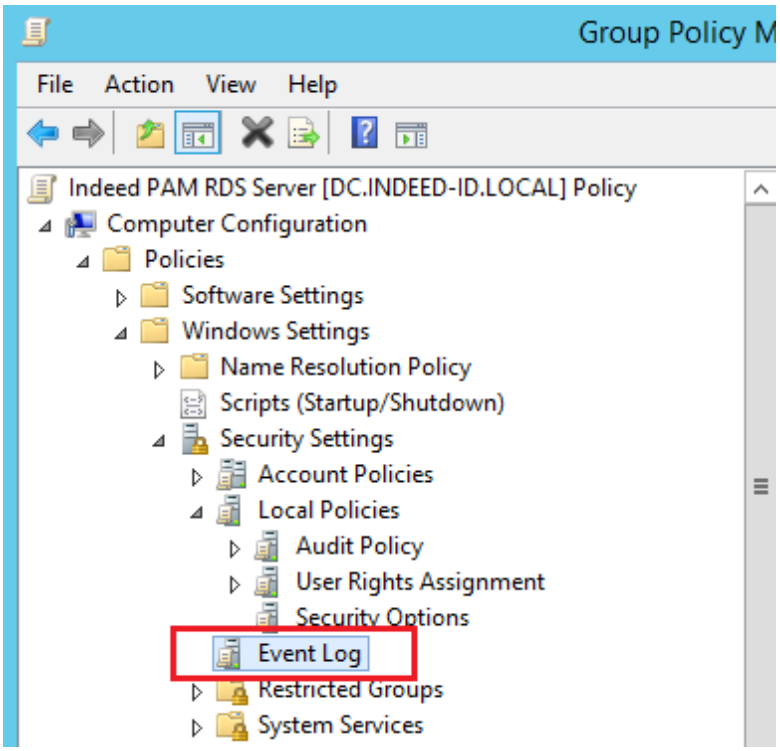
Policy	Description	Values
Microsoft network server: Disconnect clients when logon hours expire	This security setting determines whether users connected to the local computer are logged off after the allowed logon time that is configured for their account has expired. This setting affects the SMB protocol component. When enabled, client sessions with the SMB service are forced to terminate after the client's allowed logon time has expired. If this setting is disabled, the client's session is saved after the client's allowed login time has expired.	Enabled

Policy	Description	Values
Microsoft network server: Server SPN target name validation level	This policy setting controls the level of verification that the folder or printer shares computer (server) performs on the service principal name provided by the client computer when it establishes a session using the SMB protocol. The SMB protocol provides the basis for file and printer sharing and other network operations, such as remote Windows administration. The SMB protocol supports verification of the SMB server's SPN in the blob provided by the SMB client to prevent a class of attacks against SMB servers called hijack attacks. This setting affects SMB1 and SMB2. This security setting determines the level of verification that the SMB server performs on the service principal name provided by the SMB client when the client establishes a session with the SMB server. Parameters: Disabled - The SMB client SPN is not required (not checked) by the SMB server. Accept if provided by client - The SMB server accepts and validates the SPN provided by the SMB client and resolves the session if it matches the SMB server's list of SPNs. If the name does NOT match, the session for the SMB client is rejected. Require from client - The SMB client MUST send a service principal name when setting up the session, and the name supplied MUST match the SMB server to which the connection request was sent. If the SPN is not specified by the client or it does not match, the session is rejected.	Off

Policy	Description	Values
Recovery console: Allow automatic administrative logon	This security setting determines whether you must provide a password for the Administrator account to gain access to the system. When this setting is enabled, the Recovery Console does not require a password, allowing you to log in automatically.	Disabled
Recovery console: Allow floppy copy and access to all drives and all folders	When you enable this security setting, the Recovery Console SET command is available and allows you to set the following Recovery Console environment variables. AllowWildCards: allows wildcards to be used for some commands (such as the DEL command). AllowAllPaths: allows access to any files and folders on the computer. AllowRemovableMedia: allows you to copy files to removable media, such as floppy disks. NoCopyPrompt: cancels the warning when overwriting existing files.	Disabled

Event Log

Computer Configuration → Policies → Windows Settings → Security Settings → Event Log


Group Policy M
File
Action
View
Help
Indeed PAM RDS Server [DC.INDEED-ID.LOCAL] Policy
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Event Log
Restricted Groups
System Services

Description of policies

Policy	Description	Values
Maximum application log size	This security setting determines the maximum size of the application event log (max. 4 GB). In practice, a lower limit is used (approximately 300 MB). Notes. Log file sizes must be multiples of 64 KB. If you enter a value that is not a multiple of 64 KB, Event Viewer will set the log file size to a multiple of 64 KB. This setting is not included in the local computer policy object.The file size and how log events are rewritten should be specified based on the business and security requirements determined when developing the enterprise security plan. You can implement these event log settings at the site, domain, or organizational unit level to take advantage of Group Policy settings.	100032 KB
Maximum security log size	This security setting determines the maximum size of the security event log (maximum 4 GB). In practice, a lower limit is used (approximately 300 MB).	100032 KB
Maximum system log size	This security setting determines the maximum size of the system event log (max. 4 GB). In practice, a lower limit is used (approximately 300 MB).	100032 KB
Prevent local guests group from accessing application log	This security setting determines whether guests are denied access to the application event log. Notes. This setting is not included in the local computer policy object.	Enabled

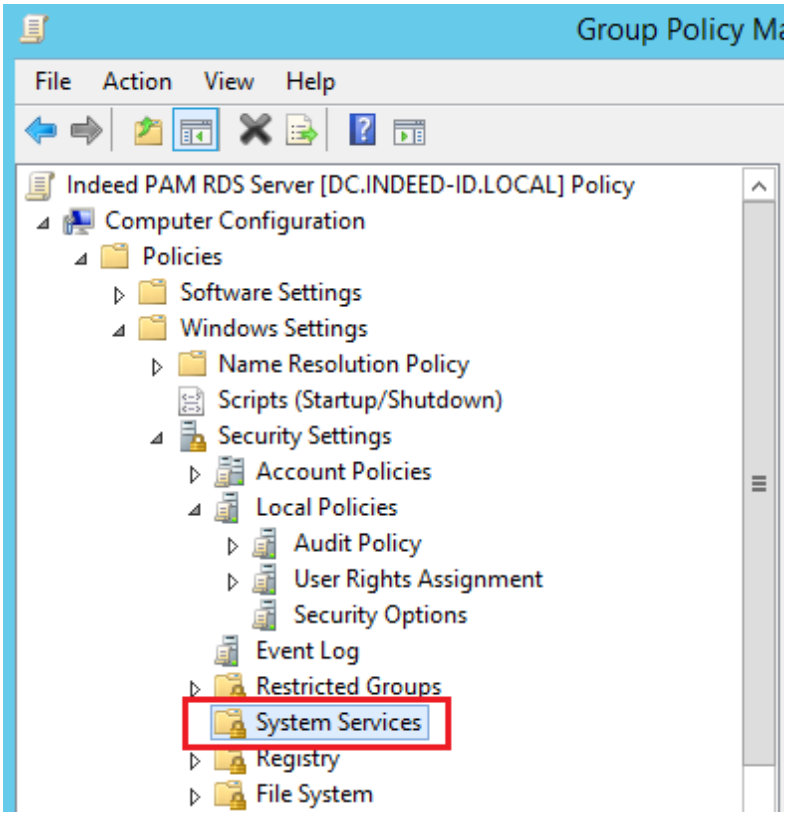
Policy	Description	Values
Prevent local guests group from accessing security log	This security setting determines whether guests are denied access to the security event log. Notes. This setting is not included in the local computer policy object.	Enabled
Prevent local guests group from accessing system log	This security setting determines whether guests are denied access to the system event log. Notes. This setting is not included in the local computer policy object.	Enabled

Policy	Description	Values
Retention method for application log	This security setting determines how the application log is rewritten. If you are not archiving the application log, in the Properties dialog box for this policy, select the Define this policy setting check box, and then select Overwrite events when necessary. If you want to archive the log at specified intervals, select the Define this policy setting check box in the Policy's Properties dialog box, then select Overwrite old events by day and specify the number of days you want using the Keep events logged option. applications". Make sure that the maximum application log size is large enough so that it is not reached within this period of time. If you want all events to be logged, select the Define this policy setting check box in the Policy's Properties dialog box, and then select Do not overwrite events (clear log manually). If you select this option, you must manually clear the log. In this case, after the maximum log size is reached, new events are rejected. Note. This setting is not included in the local computer policy object.	As needed
Retention method for security log	This security setting determines how the security log is overwritten. Notes. This setting is not included in the local computer policy object. To access the security log, the user must have the Manage Audit and Security Log privilege.	As needed

Policy	Description	Values
Retention method for system log	This security setting determines how the system log is overwritten. Note. This setting is not included in the local computer policy object.	As needed

System Services

Computer Configuration → Policies → Windows Settings → Security Settings → System Services



Description of policies

Service Name (Service Startup Mode)	Permissions	Audit
Routing and Remote Access (Startup Mode: Disabled)	Undefined	Undefined
Special Administration Console Helper (Startup Mode: Disabled)	Undefined	Undefined
SNMP Trap (Startup Mode: Disabled)	Undefined	Undefined
Telephony (Startup Mode: Disabled)	Undefined	Undefined
Windows Error Reporting Service (Startup Mode: Disabled)	Undefined	Undefined
WinHTTP Web Proxy Auto-Discovery Service (Startup Mode: Disabled)	Undefined	Undefined

File System

Computer Configuration → Policies → Windows Settings → Security Settings → File System

%SystemRoot%\System32\config

Description of policies

Configure this file or folder then: Propagate inheritable permissions to all subfolders and files

Permissions

Type	Value	Access	Applies To
Allow	ALL APPLICATION PACKAGES	Read and Execute	This folder, subfolders and files
Allow	CREATOR OWNER	Full Control	Subfolders and files only
Allow	NT AUTHORITY\SYSTEM	Full Control	This folder, subfolders and files
Allow	BUILTIN\Administrators	Full Control	This folder, subfolders and files

Inheritance disabled

Auditing

Type	Principal	Access	Applies
Fail	Everyone	Traverse Folder/Execute File, List folder / Read data, Read attributes, Read extended attributes	This folder, subfolders and files
All	Everyone	Create files / Write data, Create folders / Append data, Write attributes, Write extended attributes, Delete subfolders and files, Delete, Change permissions, Take ownership	This folder, subfolders and files

Inheritance enabled

%SystemRoot%\System32\config\RegBack

Description of policies

Configure this file or folder then: Propagate inheritable permissions to all subfolders and files

Permissions

Type	Principal	Access	Applies To
Allow	ALL APPLICATION PACKAGES	Read and Execute	This folder, subfolders and files
Allow	CREATOR OWNER	Full Control	Subfolders and files only
Allow	NT AUTHORITY\SYSTEM	Full Control	Subfolders and files only
Allow	BUILTIN\Administrators	Full Control	Subfolders and files only

Inheritance disabled

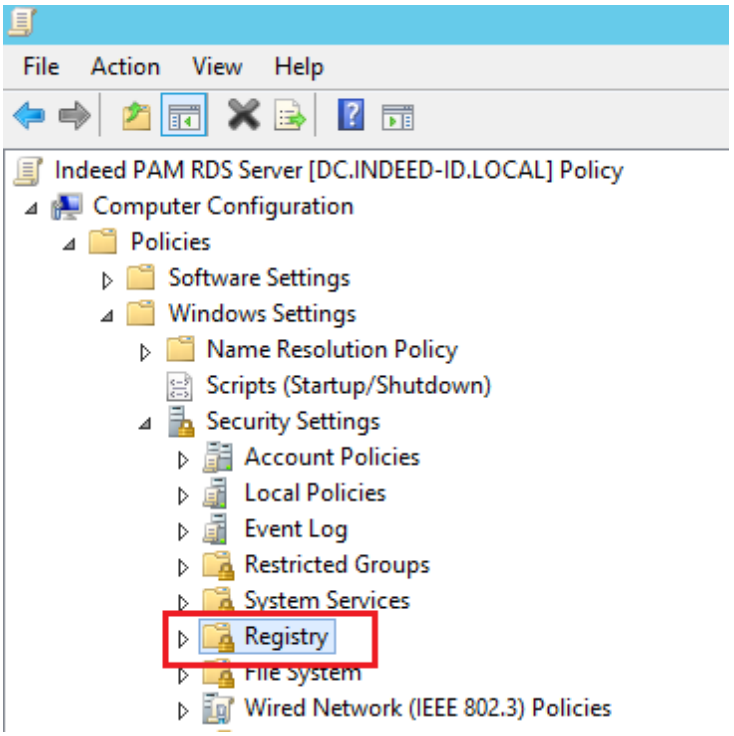
Auditing

Type	Principal	Access	Applies To
Fail	Everyone	Traverse Folder/Execute File, List folder / Read data, Read attributes, Read extended attributes	This folder, subfolders and files
All	Everyone	Create files / Write data, Create folders / Append data, Write attributes, Write extended attributes, Delete subfolders and files, Delete, Change permissions, Take ownership	This folder, subfolders and files

Inheritance enabled

Registry

Computer Configuration → Policies → Windows Settings → Security Settings → Registry



MACHINE\SOFTWARE

Description of policies

Configure this key then: Propagate inheritable permissions to all subkeys

Permissions

Type	Principal	Access	Applies To
Allow	BUILTIN\Administrators	Full Control	This key and subkeys
Allow	CREATOR OWNER	Full Control	Subkeys only
Allow	NT AUTHORITY\SYSTEM	Full Control	This key and subkeys
Allow	BUILTIN\Users	Read	This key and subkeys
Allow	ALL APPLICATION PACKAGES	Read	This key and subkeys

Inheritance disabled

Auditing

Type	Principal	Access	Applies To
All	Everyone	Create Subkey, Create Link, Delete, Read permissions, Change permissions	This key and subkeys
Success	Everyone	Set Value	This key and subkeys

Inheritance enabled

MACHINE\SYSTEM

Description of policies

Configure this key then: Propagate inheritable permissions to all subkeys

Permissions

Type	Principal	Access	Applies To
Allow	BUILTIN\Administrators	Full Control	This key and subkeys
Allow	CREATOR OWNER	Full Control	Subkeys only
Allow	NT AUTHORITY\SYSTEM	Full Control	This key and subkeys
Allow	BUILTIN\Users	Read	This key and subkeys
Allow	ALL APPLICATION PACKAGES	Read	This key and subkeys

Inheritance disabled

Auditing

Type	Principal	Access	Applies To
All	Everyone	Create Subkey, Create Link, Delete, Read permissions, Change permissions	This key and subkeys
Success	Everyone	Set Value	This key and subkeys

Inheritance enabled

MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg

Description of policies

Configure this key then: Propagate inheritable permissions to all subkeys

Permissions

Type	Principal	Access	Applies To
Allow	BUILTIN\Administrators	Full Control	This key and subkeys
Allow	CREATOR OWNER	Full Control	Subkeys only
Allow	NT AUTHORITY\SYSTEM	Full Control	This key and subkeys
Allow	BUILTIN\Users	Read	This key and subkeys
Allow	ALL APPLICATION PACKAGES	Read	This key and subkeys

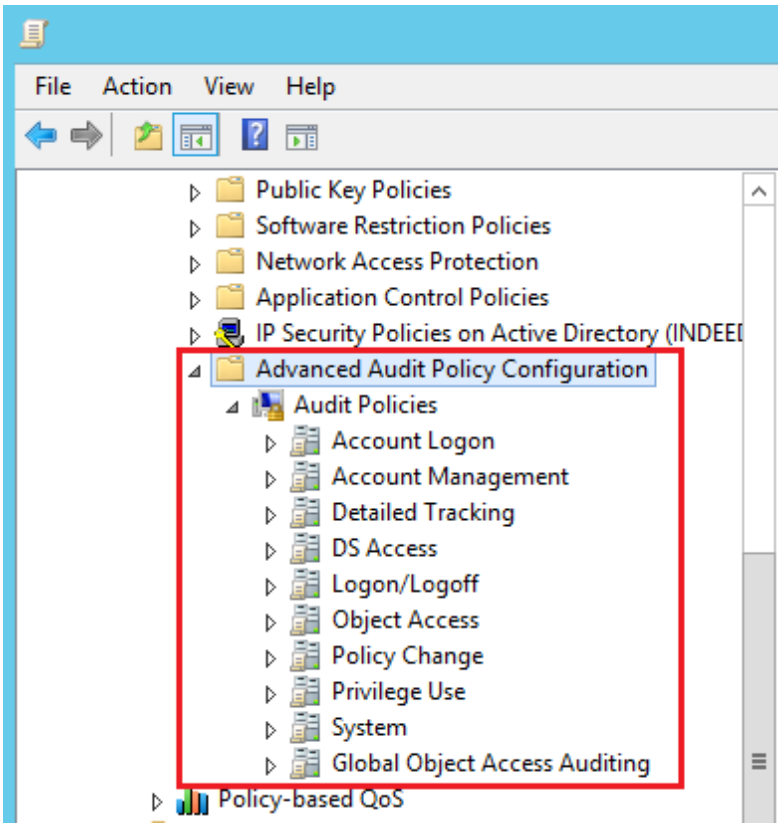
Inheritance disabled

Auditing

No auditing specified

Advanced Audit Configuration

Computer Configuration → Policies → Windows Settings → Security Settings → Advanced Audit Configuration



Account Logon

Description of policies

Policy	Description	Values
Audit Credential Validation	This policy setting allows you to audit events that occur when validating the login credentials of a user account. Events in this subcategory only occur on computers that are trusted by those credentials. For domain credentials, the domain controller has the appropriate authority. For local accounts, the local computer has the appropriate permissions.	Success, Failure
Audit Other Account Logon Events	Other account login events. This policy setting allows you to audit events that occur when responses to user account logon requests that are not related to credential verification and that are not Kerberos tickets are received.	Success, Failure

Account Management

Description of policies

Policy	Description	Values
Audit Application Group Management	This policy setting allows you to audit events that occur when you make the following changes to application groups: Create, edit, or delete an application group. Add or remove a member to an application group.	Success, Failure
Audit Computer Account Management	This policy setting allows you to audit events that occur when computer accounts are modified, such as when they are created, modified, or deleted.	Success, Failure
Audit Distribution Group Management	This policy setting allows you to audit events that occur when you make the following changes to distribution groups: Create, edit, or delete a distribution group. Add a member to or remove a member from a distribution group. Change the distribution group type. Note. Events in this subcategory are logged only on domain controllers.	Success, Failure

Policy	Description	Values
Audit Other Account Management Events	This policy setting allows you to audit events that occur when other user account changes are made that are not listed in this category: Accessing the password hash for a user account. This operation is typically performed when migrating passwords using the Active Directory management tool. Call the Password Policy Check API. This function can be called in attacks where a malicious application checks a policy to reduce the number of attempts during a dictionary attack. Changes the default domain group policy to the following group policy paths: Computer Configuration\Windows Settings\Security Options\Account Policies\Password Policies Computer Configuration\Windows Settings\Security Options\Account Settings\Account Lockout Policy Note. A security audit event is logged when the policy setting is applied. No events are logged while parameters are changed.	Success, Failure
Audit Security Group Management	This policy setting allows you to audit events that occur when the following security group changes are made: Create, edit, or delete a security group. Add a member to or remove a member from a security group. Changing the group type.	Success, Failure

Policy	Description	Values
Audit User Account Management	This policy setting allows you to audit changes made to user accounts. The following events are monitored: Create, edit, delete, rename, disable, enable, block and unblock accounts. Set or change the user account password. Adds a security identifier (SID) to the user account SID log. Set a password for Directory Services Restore mode. Change permissions for administrator accounts. Archive or restore Credential Manager credentials.	Success, Failure

Logon/Logoff

Description of policies

Policy	Description	Values
Audit Account Lockout	This policy setting allows you to audit events generated when a logon attempt to a locked account fails. When this policy setting is configured, an audit event is generated when an account cannot log on to a computer because the account is locked. Successful and unsuccessful audit events are recorded in corresponding records. Login events are important for understanding user activity and detecting possible attacks.	Success, Failure
Audit Logoff	This policy setting allows you to audit events that occur when a logon session is closed. These events occur on the computer that was accessed. When you log off interactively, a security audit event occurs on the computer that you are logged on to using the user account. When this policy setting is configured, an audit event occurs when the logon session is closed. Successful and unsuccessful attempts to close sessions are recorded in corresponding records. If this policy setting is not configured, no audit events are raised when the logon session is closed.	Success, Failure

Policy	Description	Values
Audit Logon	This policy setting allows you to audit events that occur when you attempt to log on using a user account. Events in this subcategory are related to the creation of logon sessions and occur on the computer being accessed. When you log on interactively, a security audit event occurs on the computer that you are logged on to using the account. When you log on to a network, for example when accessing a shared folder on the network, a security audit event occurs on the computer that hosts the resource. The following events are monitored: Successful login attempts. Failed login attempts. Attempts to login using explicitly specified credentials. This event occurs when a process attempts to log on to an account by explicitly specifying the appropriate credentials. This event typically occurs in batch logon configurations, such as scheduled tasks or RUNAS commands. Denying logins as a result of security identifier (SID) filtering.	Success, Failure
Audit Network Policy Server	This policy setting allows you to audit events that occur when user access requests are made using the RADIUS (IAS) and Network Access Protection (NAP) protocols. Requests for grant, denial, revocation, quarantine, blocking and unblocking are tracked. When this policy setting is configured, an audit event is raised for every IAS or NAP user access request. Successful and unsuccessful user access requests are recorded in corresponding records.	Success, Failure

Policy	Description	Values
Audit Other Logon/Logoff Events	This policy setting allows you to audit other logon and logout events that are not covered by the Logon/Logout policy setting, for example: Ending Terminal Services sessions. Creating new Terminal Services sessions. Locking and unlocking a workstation. Calling up the screensaver. Disabling the screensaver. Detection of a Kerberos replay attack in which a Kerberos request is sent twice with the same data. This condition may be due to improper network settings. Granting access to a wireless network to a user or computer account. Granting access to a wired 802.1x network to a user or computer account.	Success, Failure

Policy	Description	Values
Audit Special Logon	This policy setting allows you to audit events that occur when you perform special logon operations such as the following: Using a special login, that is, a login with rights similar to an administrator's, which can be used to elevate a process. Special group member login. When using special groups, audit events are triggered when a member of a specific group logs into the network. You can configure a list of group security identifiers (SIDs) in the registry. An event is logged when one of the specified SIDs is added to the token and that subcategory is enabled.	Success, Failure

Object Access

Description of policies

Policy	Description	Values
Audit Application Generated	This policy setting enables auditing of applications that raise events using the Windows audit APIs. This subcategory is used to log audit events that are associated with the operation of applications that use the Windows audit APIs. The following events in this subcategory are monitored: Creating the application client context. Deleting the application client context. Initializing the application client context. Other application operations using Windows auditing APIs.	Success, Failure

Policy	Description	Values
Audit Certification Services	This policy setting provides auditing of Active Directory Certificate Services (AD CS) operations. AD CS operations include the following: Starting, shutting down, backing up, and restoring AD CS services. Changing the certificate revocation list (CRL). Requesting for new certificates. Issuing a certificate. Revocation of a certificate. Changing certificate manager settings for AD CS. Changing AD CS services configuration. Changing the Certificate Services template. Importing a certificate. Publishing a CA certificate to Active Directory Domain Services. Changing security permissions for AD CS services. Archiving the key. Importing a key. Removing the key. Starting the OCSP response service. Stopping the OCSP response service.	Success, Failure

Policy	Description	Values
Audit Detailed File Share	This policy setting allows you to audit attempts to access files and folders in public folders. The option allows you to log events for any attempt to access a file or folder, while the Shared Folders option logs only one event for any connection established between the client and the shared folder. Audit events for this setting include detailed information about permissions or other criteria for granting or denying access. When this setting is configured, an audit event is raised when attempting to access a file or folder in a shared folder. The administrator can enable auditing for success, failure, or both. Note. Public folders do not have system access control lists (SACLs). When this policy setting is enabled, access to all shared files and folders on the system is audited.	Failure
Audit File Share	This policy setting allows you to audit attempts to access public folders. When this setting is configured, an audit event is raised when an attempt is made to access a shared folder. When this parameter is set, the administrator can specify that auditing of successes, failures, or both be performed. Note. Public folders do not have system access control lists (SACLs). When this policy setting is enabled, access to all public folders on the system is audited.	Success, Failure

Policy	Description	Values
Audit File System	This policy setting audits attempts to access file system objects by users. Security audit events occur only for objects that have system access control lists (SACLs) defined, and only if the type of access being requested is write, read, or modify and the requesting account matches the parameters set in the SACL. Note. To set a SACL for a file system object, use the Security tab of the object's Properties dialog box.	Success, Failure
Audit Kernel Object	This policy setting provides auditing of attempts to access the kernel using mutexes and semaphores. Security audit events only occur on kernel objects with a corresponding system access control list (SACL). Note. Auditing: The default SACLs for kernel objects are controlled by the Global System Objects access audit setting.	Success, Failure
Audit Registry	This policy setting audits attempts to access registry objects. Security audit events occur only for objects that have system access control lists (SACLs) defined, and only if the type of access being requested is read, write, or modify and the requesting account matches the parameters set in the SACL. Note. To set a SACL for a registry object, use the Permissions dialog box.	Success, Failure
Audit Removable Storage	This policy setting allows you to audit user attempts to access file system objects on a removable storage device. The security audit event is generated only for all objects and all requested access types.	Success

Policy	Description	Values
Audit SAM	This policy setting audits events that occur when you attempt to access Security Accounts Manager (SAM) objects. SAM objects include the following: SAM_ALIAS – local group. SAM_GROUP – a group that is not local. SAM_USER – user account. SAM_DOMAIN – domain. SAM_SERVER – computer account. Note. You can only change the system access control list (SACL) for the SAM_SERVER object.	Success, Failure

Policy Change

Description of policies

Policy	Description	Values
Audit Audit Policy Change	This policy setting allows you to audit changes to security audit policy settings, such as the following: Set permissions and audit settings for an audit policy object. Changes in system audit policy. Logging security event sources. Unregistration of security event sources. Changes to audit settings for individual users. Changes in the CrashOnAuditFail parameter value. Changes to the system access control list for a file system or registry object. Changes to the list of special groups. Note. System access control list (SACL) change auditing occurs when the SACL on an object changes and the policy change category is enabled. Auditing of user access control list (DACL) changes and ownership changes occurs when object access auditing is enabled and the object's SACL is configured to audit DACL or ownership changes.	Success, Failure

Policy	Description	Values
Audit Authentication Policy Change	This policy setting allows you to audit events that occur when you make changes to security groups, such as the following: Create trusts for a forest or domain. Change trust relationships for a forest or domain. Remove trusts for a forest or domain. Changes to the Kerberos policy in the following path: Computer Configuration\Windows Settings\Security Options\Account Policies\Kerberos Policy. Grant a user or group the following privileges: Access to a computer from the network. Local input. Logging in using Terminal Services. Logging in using a batch job. Login to the service. There is a namespace conflict (for example, if the name of the new trust is the same as the name of an existing namespace). Note. A security audit event is logged when the policy setting is applied. No events are logged while parameters are changed.	Success, Failure

Policy	Description	Values
Audit Authorization Policy Change	This policy setting allows you to audit events that occur when authorization policy changes are made, such as the following: Assigning privileges to users, such as SeCreateTokenPrivilege, that are not audited in the "Change Authentication Policy" subcategory. Removing user privileges, such as SeCreateTokenPrivilege, that are not audited under the "Change Authentication Policy" subcategory. Encrypting File System (EFS) policy changes. Changes to object resource attributes. Changes to the centralized access policy (CAP) applied to an object.	Success, Failure
Audit Filtering Platform Policy Change	This policy setting allows you to audit events that occur when Windows Filtering Platform (WFP) changes are made, such as the following: IPsec service status. Changes to IPsec policy settings. Changes to Windows Firewall policy settings. Changes to suppliers and WFP module.	Success, Failure

Policy	Description	Values
Audit MPSSVC Rule-Level Policy Change	This policy setting allows you to audit events that occur when policy rules used by the Microsoft Protection Service (MPSSVC) are changed. This service is used by Windows Firewall. The following events are monitored: Messages from active policies when the Windows Firewall service starts. Changes to Windows Firewall rules. Changes to the Windows Firewall exceptions list. Changes to Windows Firewall settings. Rules are skipped or not enforced by the Windows Firewall service. Changes to Windows Firewall Group Policy settings.	Success, Failure

Privilege Use

Description of policies

Policy	Description	Values
Audit Non Sensitive Privilege Use	This policy setting provides auditing of events that occur when privileges that do not affect sensitive data (user privileges) are used. Using the following privileges does not affect sensitive data: Access the Credential Manager as a trusted caller. Access to a computer from the network. Adding workstations to a domain. Setting memory quotas for a process. Local login. Login through Terminal Services. Bypass cross-validation. Changing the system time. Creating a swap file. Creating global objects. Creating permanent shared objects. Creating symbolic links. Access to the computer from the network is denied. Login as a batch job is denied. Login as a service is denied. Local login is denied. Login through Terminal Services is denied. Force remote shutdown. Increasing the working set of a process. Increasing execution priority. Locking pages in memory. Login in as a batch job. Login as a service. Changing the object's label. Performing volume maintenance tasks. Profiling a single process. System performance profiling. Disconnecting the computer from the docking station. Shutting down the system. Directory service data synchronization.	Success, Failure

Policy	Description	Values
Audit Sensitive Privilege Use	This policy setting audits events that occur when rights are used that affect sensitive data (user rights) as follows: Call a privileged service. Call one of the following privileges: Action on behalf of an operating system component. Archiving files and directories. Creating a token object. Debugging programs. Enable computer and user accounts that are allowed to delegate. Creating a security audit. Impersonate the client after authentication. Loading and unloading device drivers. Audit and security log management. Changing the value of hardware environment parameters. Process-level token replacement. Recovering files and directories. Changing the owner of a file or other object.	Failure

System

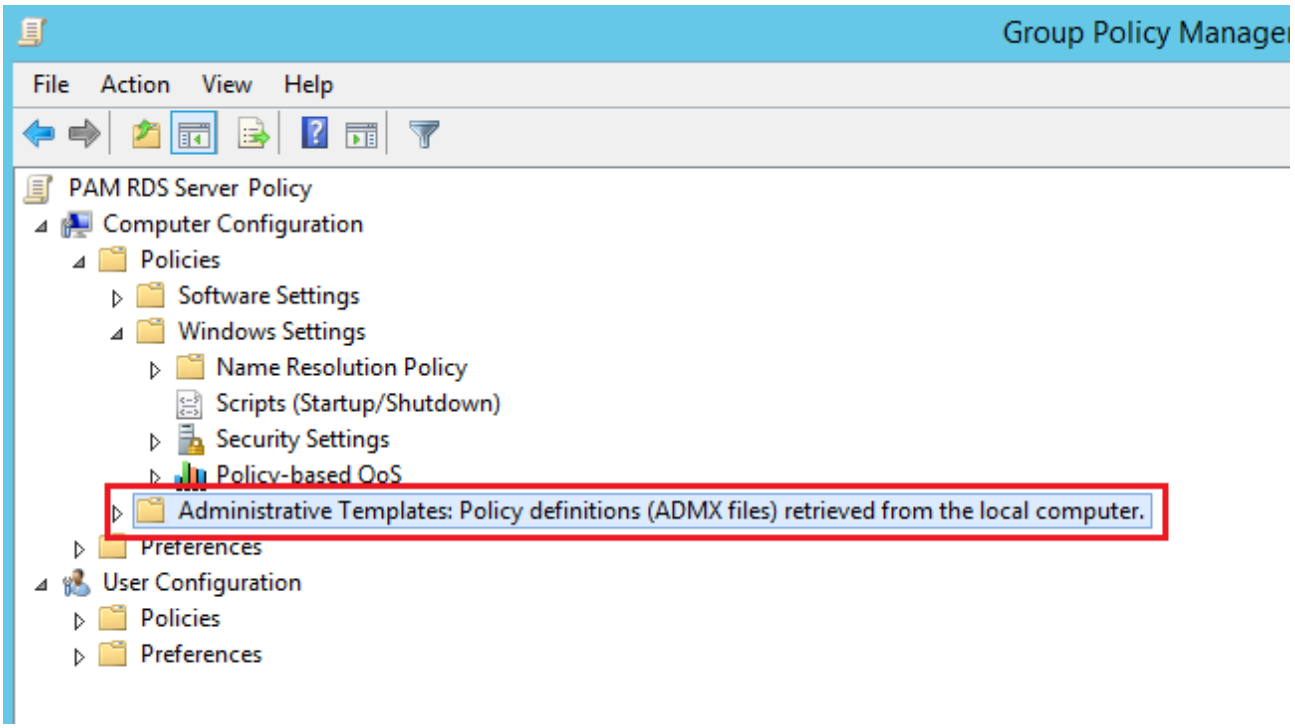
Description of policies

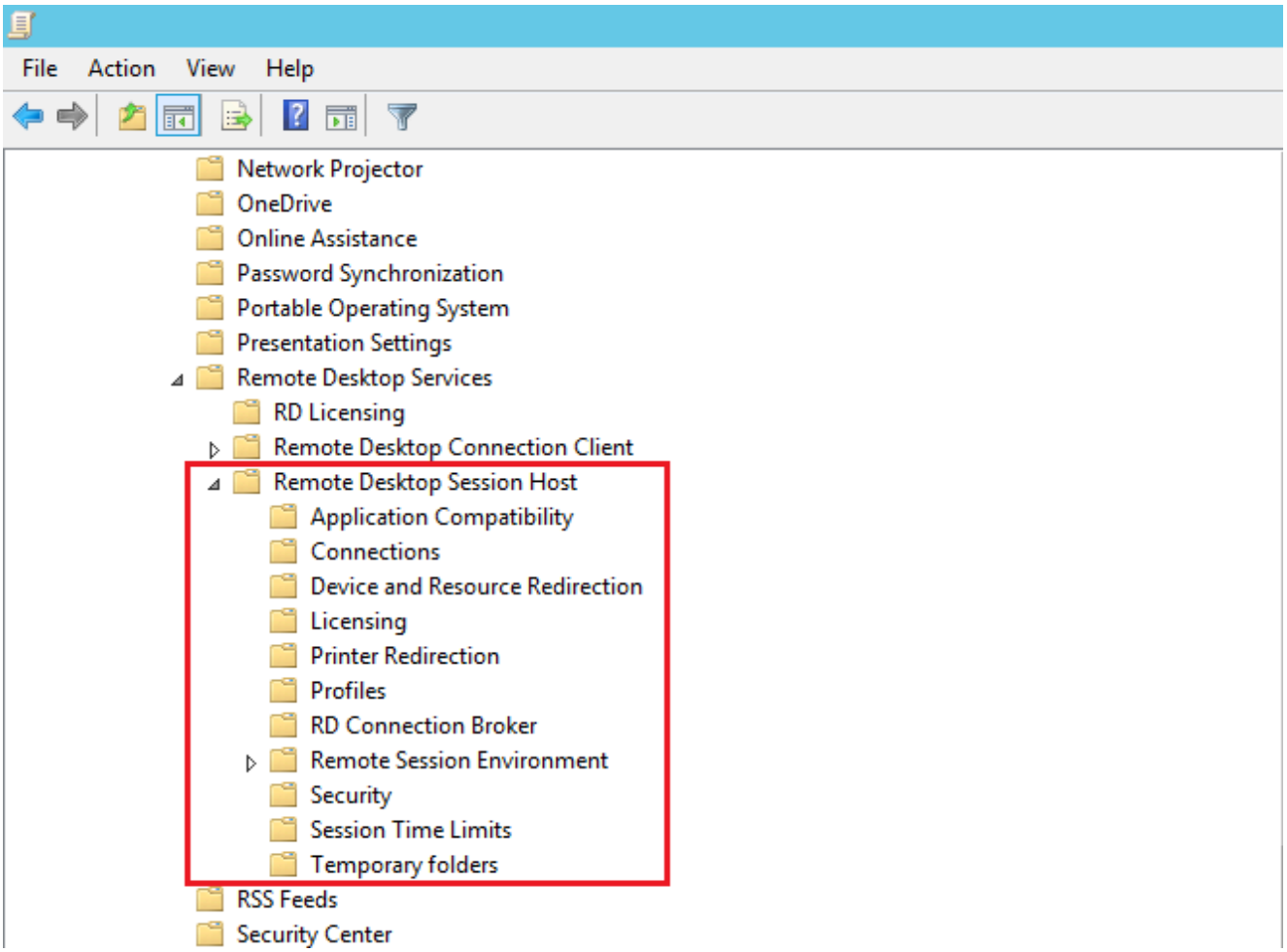
Policy	Description	Values
Audit Other System Events	This policy setting allows you to audit the following events: Starting and stopping the Windows Firewall service and driver. Security policy processing by the Windows Firewall service. Operations with encryption key files and migration operations.	Success, Failure
Audit Security State Change	This policy setting allows you to audit events that occur when you make changes to the computer's security state, such as the following: Starting and shutting down the computer. Changing the system time. System recovery for the CrashOnAuditFail event, which is logged after a system restart if the event log is full and the CrashOnAuditFail registry entry is configured.	Success, Failure
Audit Security System Extension	This policy setting allows you to audit events related to the security extension, such as the following: Download a security extension, such as an authentication, notification, or security package, and register it with the Local Security Administrator (LSA). It is used to authenticate login attempts, login requests, and any changes to accounts or passwords. Examples of security extensions are Kerberos and NTLM. Install and register the service in Service Control Manager. The audit log records information about the name, binaries, type, startup type, and account of the service.	Success, Failure

Policy	Description	Values
Audit System Integrity	This policy setting allows you to audit events related to security subsystem integrity violations, such as the following: Events that cannot be recorded in the event log due to errors in the auditing system. Processes that use an invalid local procedure call (LPC) port to impersonate a client by responding to, reading, or writing to the client's address space. Detection of a remote procedure call (RPC) that compromises the integrity of the system. Detection of an invalid executable hash value by a code integrity checker. Encryption operations that violate the integrity of the system.	Success, Failure

Administrative Templates Section

Computer Configuration → Policies → Administrative Templates





Connections

Windows Components → Remote Desktop Services → Remote Desktop Session Host → Connections

Description of policies

Policy	Description	Values
Automatic reconnection	Determines whether Remote Desktop Connection clients are allowed to automatically reconnect to sessions on the Remote Desktop Session Host server when a network connection is temporarily unavailable. By default, you are allowed a maximum of 20 reconnection attempts at 5-second intervals. When set to Enabled, all clients running a Remote Desktop connection attempt to reconnect automatically when a network connection is unavailable. If the setting is set to Disabled, automatic client reconnections are disabled. If the state is set to Not Configured, automatic reconnection is not defined at the Group Policy level. However, users can set up automatic reconnection by selecting the Reconnect when disconnected checkbox on the Interaction tab of the Remote Desktop Connection dialog box.	Disabled

Policy	Description	Values
Configure keep-alive connection interval	This policy setting allows you to enter a keepalive interval to ensure that the session state on the RD Session Host server matches that of the client. After a RD Session Host server client loses connectivity to an RD Session Host server, the session on that server can remain active rather than going into a disconnected state, even if the client is physically disconnected from the RD Session Host server. If the client logs on to the same RD Session Host server again, a new session may be established (if the RD Session Host server is configured to allow multiple sessions) and the original session may still be active. If this policy setting is enabled, a keepalive interval must be entered. The keepalive interval determines how often (in minutes) the server checks the session state. Valid values range from 1 to 999 999. If this policy setting is disabled or not configured, the keepalive interval is not set and the server does not check session state.	Enabled Keep-Alive interval: 1

Policy	Description	Values
Set rules for remote control of Remote Desktop Services user sessions	When you enable this policy setting, administrators can interact with a user's Remote Desktop Services session based on the option they select. Select your desired level of control and permissions from the list of options: Remote control not allowed: Prevents the administrator from using remote control or viewing remote user sessions. Full control with user permission: Allows the administrator to interact with the session, subject to the user's consent. Full control without user permission: Allows the administrator to interact with the session even without the user's consent. Monitor session with user permission: Allows an administrator to view a remote user's session with the user's consent. Monitor session without user permission: Allows an administrator to view a remote user's session without the user's consent. If you disable this policy setting, administrators can interact with a user's Remote Desktop Services session if the user consents.	Enabled Options: Full Control without user's permission

Device and Resource Redirection

Windows Components → Remote Desktop Services → Remote Desktop Session Host → Device and Resource Redirection

Description of policies

Policy	Description	Values
Do not allow COM port redirection	Determines whether data redirection from the remote computer to client COM ports should be disabled in Remote Desktop Services sessions. You can use this policy setting to prevent users from redirecting data to peripheral devices connected to COM ports or mapping local COM ports when connecting to a Remote Desktop Services session. By default, Remote Desktop Services allows data redirection to COM ports. If you enable this policy setting, users cannot forward server data to the COM ports of local computers. If you disable this policy setting, COM port redirection is always allowed by Remote Desktop Services. If you do not configure this policy setting, COM port redirection is not defined at the Group Policy level.	Enabled

Policy	Description	Values
Do not allow LPT port redirection	This policy setting determines whether data forwarding to client LPT ports in Remote Desktop Services sessions should be disabled. This policy setting can be used to prevent users from mapping local LPT ports and redirecting data from a remote computer to local peripheral devices connected to LPT ports. By default, Remote Desktop Services allows LPT port forwarding. If you enable this policy setting, users during a Remote Desktop Services session cannot forward server data to local LPT ports. If you disable this policy setting, redirection to LPT ports is always allowed. If you do not configure this policy setting, LPT port redirection is not defined at the Group Policy level.	Enabled

Policy	Description	Values
Do not allow supported Plug and Play device redirection	This policy setting allows you to control whether supported Plug and Play devices, such as Windows Portable Devices, are redirected to a remote computer during a Remote Desktop Services session. By default, Remote Desktop Services allows redirection of supported Plug and Play devices.Users can use the Advanced setting on the Local Resources tab of the Remote Desktop Connection dialog box to select supported plug-and-play devices to redirect to the remote computer. If you enable this policy setting, users cannot redirect supported Plug and Play devices to a remote computer. If you disable or do not configure this policy setting, users can redirect supported Plug and Play devices to the remote computer. Note. You can use policy settings in the Computer Configuration\Administrative Templates\System\Device Installation\Device Installation Restrictions folder to prevent redirection of certain types of supported Plug and Play devices.	Enabled

Remote Session Environment

Windows Components → Remote Desktop Services → Remote Desktop Session Host → Remote Session Environment

Description of policies

Policy	Description	Values
Remove "Disconnect" option from Shut Down dialog	This policy setting allows you to remove the "Disconnect Session" item from the Shut Down Windows dialog box in Remote Desktop Services sessions. By using this policy setting, you can prevent users from using this familiar method of disconnecting a client computer from the Remote Desktop Session Host server. When this policy setting is enabled, the Disconnect Session option does not appear in the drop-down list in the Shut Down Windows dialog box. If this policy setting is disabled or not configured, the Disconnect Session item is not removed from the list in the Shut down Windows dialog box. Note. This policy setting only affects the Shut Down Windows dialog box. It does not prevent users from using other methods to disconnect from a Remote Desktop Services session. This policy setting also does not prevent sessions from being disconnected on the server. You can set the period of time that a disconnected session will remain active on the server by configuring the setting: Computer Configuration\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Session Time Limits\Set Time Limit.	Enabled

Policy	Description	Values
Remove Windows Security item from Start menu	Determines whether the Windows Security item should be removed from the Options menu on Remote Desktop Services clients. You can use this policy setting to prevent insufficiently experienced users from being inadvertently disconnected from Remote Desktop Services. When set to Enabled, Windows Security does not appear in the Start menu. As a result, in order to open the Windows Security dialog box on the client computer, the user must use a special keyboard shortcut (CTRL+ALT+END). If the setting is set to Disabled or Not Configured, Windows Security remains in the Start menu.	Enabled

Security

Windows Components → Remote Desktop Services → Remote Desktop Session Host → Security

Description of policies

Policy	Description	Values
Require secure RPC communication	Indicates whether the Remote Desktop Session Host server requires secure RPC connections from all clients or allows insecure connections. This setting can be used to improve the security of client RPC connections by allowing only authenticated and encrypted requests. When the status is Enabled, Remote Desktop Services accepts requests only from RPC clients that support secure requests and does not allow insecure connections from untrusted clients. When the status is Disabled, Remote Desktop Services always requests that all RPC traffic be sent securely. If the status is Not Configured, insecure connections are allowed. Note. The RPC interface is used to administer and configure Remote Desktop Services.	Enabled

Policy	Description	Values
Set client connection encryption level	This policy setting determines whether a special level of encryption is required for secure communications between client computers and RD Session Host servers during remote RDP connections. If you enable this policy setting, all communications between clients and RD Session Host servers during remote connections must use the encryption method that is specified in this setting. The default encryption level is set to High. The following encryption methods are supported: High. A value of "High" means that data exchanged between the client and server is encrypted using strong 128-bit encryption. Use this level in environments that contain only 128-bit clients (for example, clients using the Remote Desktop Connection service). Clients that do not support this level of encryption cannot connect to Remote Desktop Session Host servers. Client compatible. A value of "Client Compatible" means that data exchanged between the client and server is encrypted using the strongest key supported by the client. Use this level of encryption in environments with clients that do not support 128-bit encryption. Low. When set to Low, only data sent from the client to the server is encrypted using 56-bit encryption. If the setting is disabled or not configured, Group Policy does not control the level of encryption used for remote connections to Remote Desktop Session Host servers. Important!	Enabled Encryption Level: High Level

Policy	Description	Values
	FIPS compliance can be configured through System Encryption Tools. Use FIPS-compliant algorithms for encryption, hashing, and digital signature settings in Group Policy (Computer Configuration\Windows Settings\Security Options\Local Policies\Security Options). The FIPS Compliant setting encrypts and decrypts data sent from the client to the server and back using FIPS 140-1 (Federal Information Processing Standard) encryption algorithms using Microsoft encryption modules. Use this level of encryption for communications between clients and RD Session Host servers that require the highest level of encryption.	

Session Time Limits

Windows Components → Remote Desktop Services → Remote Desktop Session Host → Session Time Limits

Description of policies

Policy	Description	Values
End session when time limits are reached	This policy setting determines whether a Remote Desktop Services session is timed out instead of disconnected. You can use this setting to force a Remote Desktop Services session to end (which forces the user to log off and the session information is deleted from the server) when the active or inactive session limit is reached. By default, Remote Desktop Services disconnects sessions after their specified session time has expired. Time limits are enforced by the server administrator locally or through Group Policy. See the policy settings "Set a time limit for active Remote Desktop Services sessions" and "Set a time limit for active but idle Remote Desktop Services sessions." If you enable this policy setting, Remote Desktop Services terminates all timed-out sessions. If you disable this policy setting, Remote Desktop Services always disconnects sessions that time out, even if your server administrator has specified different behavior for this policy setting. If you do not configure this policy setting, Remote Desktop Services disconnects sessions that time out, unless otherwise specified in local settings. Note. This policy setting applies only to administrator-defined timeout restrictions. This policy setting does not apply to timeout events that are determined by network connection conditions. This option is available in the Computer Configuration and User Configuration folders. If	Enabled

Policy	Description	Values
	both settings are configured, the setting in the Computer Configuration folder takes priority.	
Set time limit for disconnected sessions	This policy setting allows you to configure a time limit for disconnected Remote Desktop Services sessions. This policy setting allows you to define the maximum period of time that a disconnected session remains active on the server. By default, Remote Desktop Services allows users to disconnect from a Remote Desktop Services session without ending or logging out of the session. When a session is in a disconnected state, running programs continue to run even though the user is not connected. By default, such disconnected sessions remain open on the server indefinitely. If you enable this policy setting, disconnected sessions are deleted from the server after the specified time. To ensure the default behavior that disconnected sessions are serviced without time limit, select Never. For a console session, time limits do not apply to disconnected sessions. If you disable or do not configure this policy setting, it is not defined at the Group Policy level. By default, disconnected Remote Desktop Services sessions remain opened without time limits. Note. This setting is located in the Computer Configuration and User Configuration folders. If policy settings are specified in both folders, the setting in the Computer Configuration folder takes precedence.	Enabled End a disconnected session: 1 minute

Temporary Folders

Windows Components → Remote Desktop Services → Remote Desktop Session Host → Temporary folders

Description of policies

Policy	Description	Values
Do not delete temp folders upon exit	This policy setting determines whether Remote Desktop Services temporary folders are saved after sessions end. This policy setting allows temporary user session folders to remain on the remote computer even after the session ends. By default, Remote Desktop Services deletes users' temporary folders when the user logs off. If you enable this policy setting, temporary user session folders are not deleted when sessions end. If you disable this policy setting, temporary folders are deleted when the session ends, even if the server administrator has specified otherwise. If you do not configure this policy setting, Remote Desktop Services deletes temporary folders from the remote computer when you log off, unless otherwise specified by the server administrator. Note. This setting is only relevant if the server uses temporary session folders. If the "Do not use temporary folders for session" policy setting is enabled, this setting has no effect.	Disabled

Policy	Description	Values
Do not use temporary folders per session	This policy setting prevents Remote Desktop Services from creating temporary session folders. This policy setting allows you to prevent the remote computer from creating separate temporary folders for each session. By default, Remote Desktop Services creates a separate temporary folder for each active user session on the remote computer. Such temporary folders are created on the remote computer in the Temp folder of the user profile folder and are named after the session code. If you enable this policy setting, temporary session folders are not created. Instead, the user's temporary files for all sessions on the remote computer are stored in the Temp shared folder of the user's profile folder on the remote computer. If you disable this policy setting, separate temporary folders are always created for each session, even if a different mode is specified by the server administrator. If you do not configure this policy setting, separate temporary folders are created for each session unless a different mode is specified by the server administrator.	Disabled

Policies Import Procedure

1. On the domain controller, create a new GPO, for example "Axidian Privilege RDS Server".
2. Configure GPO security filters to apply only to the Axidian Privilege Gateway server object.
3. Download the archive with a set of policies and unpack it into a temporary folder.
4. Right-click on the created GPO and select "Import settings..." from the context menu.
5. Specify the path to the folder with the unpacked archive.
6. In the "Transfer Links" window, select the "copy them exactly from source" checkbox.
7. After successful import, open the GPO and edit the "Allow log on through Remote Desktop Services" policy by adding a security group for users who need remote access.

8. Link the GPO to the organizational unit that owns the Axidian Privilege Gateway server.
9. Apply the policies by running the gpupdate /force command on the Axidian Privilege Gateway server.

Access Server Security Settings

> ⚠ **CAUTION**
> Be sure to follow the instructions listed on this page. This is required for the Axidian PAM to function properly.

Applying Settings Using the Utility

To apply the necessary access server security settings, follow these steps:

1. Go to the `..PAM_3.5\axidian-pam-tools\configuration-protector\` distribution folder.
2. Run the terminal (Windows PowerShell) as Administrator.
3. Run the command:

   ```
   .\Pam.Tools.Configuration.Protector.exe apply-gateway-security
   ```

4. Set the **Prohibit access to Control Panel and PC settings** option to **Enabled**.
   Path: User configuration → Administrative Templates → Control Panel → Prohibit access to Control Panel and PC settings
5. Restart the access server machine.
6. Make sure that the required access server security settings have been applied.
7. Check your resources, make sure the **Require Use of Specific Security Layer for Remote (RDP) Connections** option of the group policy is set to one of the following values:

   - **Not Configured**
   - **Enabled: Negotiate**
   - **Enabled: SSL**

   Path: Computer Configuration → Administrative Templates → Windows Components → Remote Desktop Services → Remote Desktop Session Hosts → Security → Require Use of Specific Security Layer for Remote (RDP) Connections

> ⚠ **CAUTION**
>
> Value **Enabled: RDP** is not supported by Axidian PAM.

Verifying that the Access Server Security Settings have been Successfully Applied

To ensure that the required access server security settings have been applied, follow these steps:

1. Go to the `..PAM_3.5\axidian-pam-tools\configuration-protector\` distribution folder.
2. Run the terminal (Windows PowerShell) as Administrator.
3. Run the command:

```
.\Pam.Tools.Configuration.Protector.exe validate-gateway-security
```

Applying Settings Manually

If using the Pam.Tools.Configuration.Protector utility is impossible for some reason, then apply the necessary security settings manually, as described below.

1. **Copying the library file to the ProxyApp directory**

   Go to the `C:\Program Files\dotnet\shared\Microsoft.NETCore.App\3.1.24` directory, copy the `Microsoft.DiaSymReader.Native.amd64.dll` file into the `C:\Program Files\Axidian\Axidian Privilege\Gateway\ProxyApp` directory. The version in the path may vary depending on the version of Dotnet Runtime installed on the server. Use the largest available version starting from 3.1.

2. **Disabling a user CA trusted root certificate storage**

   There are two ways to do so:

   1. Via Group Policy.
   2. Via a setting in the registry on the RDS Gateway server, if group policy is not applied.

   Way 1 — via Group Policy

   Change the setting in group policy that applies to the RDS Gateway server:

   Path: Computer Configuration → Windows Settings → Security Settings → Public Key Policies → Certificate Path Validation Settings.

In **Stores** tab:

1. Enable **Define these policy settings** option.
2. Disable **Allow user trusted root CAs to be used to validate certificates** option.

Way 2 — Via a setting in the registry

In `HKLM\SOFTWARE\Policies\Microsoft\SystemCertificates\Root\ProtectedRoot`, create a **Flags** key with **DWORD** type and set the value to **1**. The user CA trusted root certificate storage is disabled if the first bit of the value in **Flags** is **1**.

3. **Disabling Windows push notification system services**

   Disable the following services:

   - **Windows Push Notifications (WpnService)**
   - **Windows Push Notifications User (WpnUserService)**

4. **Disabling the Control Panel for users in the Group Policy**

   Set the **Prohibit access to Control Panel and PC settings** option to **Enabled**.

   Path: User configuration → Administrative Templates → Control Panel → Prohibit access to Control Panel and PC settings.

5. **Checking the Selected Security Layer for Remote RDP Connections in the Group Policy of Your Resources**

   Check your resources, make sure the **Require Use of Specific Security Layer for Remote (RDP) Connections** option of the group policy is set to one of the following values:

   - **Not Configured**
   - **Enabled: Negotiate**
   - **Enabled: SSL**

   Path: Computer Configuration → Administrative Templates → Windows Components → Remote Desktop Services → Remote Desktop Session Hosts → Security → Require Use of Specific Security Layer for Remote (RDP) Connections.

> ⚠ **CAUTION**
> Value **Enabled: RDP** is not supported by Axidian PAM.

Changing the Encryption Key of the PAM Database

Key compromise is a situation when a key becomes known and can be used by third parties. If the encryption keys of PAM databases have been compromised, change the keys by updating the PAM configuration. For key rotation, the KeyRotator utility is used.

Paths to component configuration files are provided in the table.

Component	Windows	Linux
KeyRotator	`AxidianPAM_3.5\axidian-pam-tools\key-rotator\appsettings.json`	`/etc/axidian/axidian-privilege/tools/key-rotator/appsettings.json`
Core	`C:\inetpub\wwwroot\core\appsettings.json`	`/etc/axidian/axidian-privilege/core/appsettings.json`
IdP	`C:\inetpub\wwwroot\idp\appsettings.json`	`/etc/axidian/axidian-privilege/idp/appsettings.json`

Setting up KeyRotator configuration

1. Decrypt the PAM configuration files depending on the installation scheme.
2. Open the KeyRotator configuration file.
3. In the `Database` section, specify the DBMS server type for the `Provider` parameter: `PgSql` or `MsSql`.
   Do not close the file.

KeyRotator configuration file

```
"Database": {
  "Provider": "MsSql", // Specify DBMS
  "PamCore": "PAM_CORE_DB_CONNECTION_STRING",
  "PamIdp": "PAM_IDP_DB_CONNECTION_STRING"
}
```

4. Open the Core configuration file.

5. In the `ConnectionStrings` section, copy the value of the `PamCore` parameter.
   Specify this value in the KeyRotator configuration file in the `Database` section for the `PamCore` parameter.

Core configuration file

```
  "$schema": "appsettings.schema.json",
  "ConnectionStrings": {
    "PamCore": "a4a1b2e2910371e15b353", // Copy this value
    "JobsQueue": "ecda23a59b856554561ce"
  }
```

KeyRotator configuration file

```
"Database": {
  "Provider": "MsSql",
  "PamCore": "a4a1b2e2910371e15b353", // Paste the value from the Core component file
  "PamIdp": "PAM_IDP_DB_CONNECTION_STRING"
 }
```

6. Open the Idp configuration file.

7. In the `ConnectionStrings` section, copy the value of the `DefaultConnection` parameter.
   Specify this value in the KeyRotator configuration file in the `Database` section for the `PamIdp` parameter.

Idp configuration file

```
"ConnectionStrings": {
    "DefaultConnection": "77f6951e7881ed232cd2d", // Copy this value
    "JobsQueue": "0786670f99283fcceee86"
  }
```

KeyRotator configuration file

```
"Database": {
   "Provider": "MsSql",
   "PamCore": "ENCRYPTED_CfDJ8DpxpXA-mxxMpMmnxTrA",
   "PamIdp": "77f6951e7881ed232cd2d" // Paste the value from the IdP component file
 }
```

8. Save the changes in the KeyRotator configuration file.

Encryption key change

Change the encryption keys of the Core or Idp component databases. If changes are needed for both components, change the keys sequentially, as the KeyRotator configuration file stores only one set of keys.

Core Component Database

1. Generate a new encryption key.

Windows

To generate a key using the KeyGen script:

1. Run PowerShell as administrator.
2. Navigate to the PAM installation package at the path `AxidianPAM_3.5\axidian-pam-tools\key-gen`.
3. Execute the command:

```
powershell -ExecutionPolicy Bypass -File dbkeygen.ps1
```

4. Save or copy the key.

Linux

To generate a key using the OpenSSL utility, execute the command:

```
openssl rand -hex 32
```

- `rand` — command for generating random data.
- `-hex` — output the key in hexadecimal format.
- `32` — key size in bytes.

The key will appear in the console, for example, `e16155e21c73e86c4792c`. Save or copy it.

2. Open the Core configuration file. In the `Encryption` section, for the `Key` parameter, copy the old key and save it, then specify the new encryption key.

Core configuration file

```
"Encryption": {
  "Primary": {
    "Algorithm": "AES",
    "HashAlgorithm": "SHA512",
    "Key": "1c697af0512e1a20ce099", // Copy the old key, then paste the new key
    "MediaFiles": {
      "Algorithm": "AES"
    }
  }
}
```

3. Open the KeyRotator configuration file.

4. In the `Encryption` section, for the `Key` parameter, specify the new encryption key.
In the `Secondary` section, for the `Key` parameter, specify the value of the old key from the Core configuration file.

KeyRotator configuration file

```
"Encryption": {
// new encryption settings
  "Primary": {
    "Algorithm": "AES",
    "HashAlgorithm": "SHA512",
    "Key": "e16155e21c73e86c4792c" // Insert the new key
  },
// old encryption settings
  "Secondary": {
    "Algorithm": "AES",
    "HashAlgorithm": "SHA512",
    "Key": "1c697af0512e1a20ce099" //  Insert the old key from the Core component file
    }
  }
```

5. Save the changes in the KeyRotator and Core configuration files.

6. Perform key rotation using the KeyRotator utility.

Windows

1. Navigate to the PAM installation package at `AxidianPAM_3.5\axidian-pam-tools\key-rotator`.
2. Run the Pam.Tools.KeyRotator.exe utility.

Linux

Execute the command in the terminal:

```
sudo bash /etc/axidian/axidian-privilege/tools/key-rotator.sh rotate --component Core
```

7. Encrypt the configuration file and restart the management server.

Idp component database

1. Generate a new encryption key.

Windows

To generate a key using the KeyGen script:

1. Run PowerShell as administrator.
2. Navigate to the PAM installation package at the path `AxidianPAM_3.5\axidian-pam-tools\key-gen`.
3. Execute the command:

```
powershell -ExecutionPolicy Bypass -File dbkeygen.ps1
```

Linux

To generate a key using the OpenSSL utility, execute the command:

```
openssl rand -hex 32
```

- `rand` — command for generating random data.
- `-hex` — output the key in hexadecimal format.
- `32` — key size in bytes.

The key will appear in the console, for example, `594d73ab13ead58463da6`. Save or copy it.

2. Open the Idp configuration file. In the `Encryption` section, for the `Key` parameter, copy the old key and save it, then specify the new encryption key.

Idp configuration file

```
"Encryption": {
  "Primary": {
    "Algorithm": "AES",
    "HashAlgorithm": "SHA512",
    "Key": "ceaaa7f6ac059e0140051", // Copy the old key, then paste the new key
    }
  }
```

3. Open the KeyRotator configuration file.

4. In the `Encryption` section, for the `Key` parameter, specify the new encryption key.
   In the `Secondary` section, for the `Key` parameter, specify the value of the old key from the IdP configuration file.

   KeyRotator configuration file

```
"Encryption": {
// new encryption settings
  "Primary": {
    "Algorithm": "AES",
    "HashAlgorithm": "SHA512",
    "Key": "594d73ab13ead58463da6" // Insert the new key
  },
// old encryption settings
  "Secondary": {
    "Algorithm": "AES",
    "HashAlgorithm": "SHA512",
    "Key": "ceaaa7f6ac059e0140051" // Insert the old key from the Core component file
    }
  }
```

5. Save the changes in the KeyRotator and IdP configuration files.

6. Perform key rotation using the KeyRotator utility.

   Windows

   1. Navigate to the PAM installation package at `AxidianPAM_3.5\axidian-pam-tools\key-rotator`.
   2. Run the Pam.Tools.KeyRotator.exe utility.

   Linux

   Execute the command in the terminal:

```
sudo bash /etc/axidian/axidian-privilege/tools/key-rotator.sh rotate --component Core
```

7. Encrypt the configuration file and restart the management server.

Encryption and restart of the management server

After modifying the KeyRotator, Core, or IdP configuration files, perform file encryption and restart the PAM management server containers.

Windows

1. Perform encryption of PAM configuration files.
2. Run PowerShell as administrator.
3. Launch IIS Manager:

```
start inetmgr
```

4. Click on the desired server in the left panel.
5. In the right panel, click **Restart**.

Linux

1. Perform encryption of PAM configuration files.
2. Navigate to the PAM scripts folder and restart the component:

```
sudo bash /etc/axidian/axidian-privilege/scripts/run-pam.sh
```

Authentication

X.509 Certificate

Set up authentication with an X.509 certificate

OpenID Connect Protocol

Configure authentication via an external Identity Provider

RADIUS Configuring

Edit the appsettings.json configuration file

Kerberos Authentication

Authenticate Active Directory users with the Kerberos protocol

TOTP Second Factor via Email Setup

Edit the appsettings.json configuration file (optional)

X.509 Certificate

An X.509 certificate is a digital document for verifying users, servers, devices, or websites. The certificate uses a Public Key Infrastructure (PKI) and contains owner information, a public key, and a digital signature from the CA validating the certificate's authenticity.

During authentication, Axidian Privilege verifies the certificate and compares the `Distinguished Name` (`DN`) value extracted from the `Subject` field in the certificate with the `Subject` value of the user in PAM. If the values match, the user logs into the Axidian Privilege console.

To set up X.509 certificate authentication:

1. Prepare X.509 certificates according to the requirements and place them in the host certificate store.
2. Select the certificate authentication mode.
3. Add the certificate `Subject` value for users in Axidian Privilege.
   Each user must have a unique `Subject`.
4. Open the user or administrator console and authenticate using the X.509 certificate.

> ⓘ **INFO**
> Proxy components do not support certificate authentication.
> To access resources, enable the Session opening without re-authentication and/or SSH key authentication options.

Certificate requirements

- A valid certificate in .cer, .crt, .pem, or .der format.
- The certificate is signed by a root certificate or an issuing CA certificate.
- The `Subject` field specifies the DN in RFC 4514 format.
  Example: `CN=John Smith,OU=Development,O=Company,C=US`.

Set up authentication

To enable X.509 certificate authentication:

1. In the admin console, go to **Configuration → User Authentication**.

2. For the **Certificate authentication** parameter, select the mode:
    - **Enabled (optional)** — users can log in using a certificate or a username and password.
    - **Mandatory for users with specified certificate Subject** — users with a specified certificate `Subject` can log in only using a certificate. Other users log in via login and password.
    - **Mandatory for all users** — console login is only possible using a certificate.

    > ⚠ **CAUTION**
    > When selecting the **Mandatory for all users** mode, ensure that users have the `Subject` field filled in correctly, otherwise they will not be able to log into the console.

3. Click **Save**.

Add a certificate Subject

> ⓘ **INFO**
> To add a `Subject` value for a user, the administrator must have the *Manage X.509 certificate Subject for users* claim.

Specify the `Subject` value for all users with X.509 certificate authentication enabled. If `Subject` is not set or entered incorrectly, the user will not be able to log into the console.

To add a certificate `Subject`:

1. In the admin console, go to the **Users** section.
2. Open the user profile and go to the **Authenticators** tab.
3. Next to the **Subject** field, click ✎ and select one of the options:
    - **Paste manually** — enter the certificate `Subject` value.

Example

Single line, comma-separated

```
CN=John Smith,OU=Development Department,O=Company
```

Multiline

```
CN=John Smith
OU=Development Department
O=Company
```

- **Upload certificate** — select and upload a certificate in .cer, .crt, .pem, or .der format.
  If the certificate is correct, the recognized `Subject` value will be displayed.

4. Click **Save**.

Sign in to PAM

> **INFO**
> If the certificate is incorrect or expired, restart the browser and choose a different certificate.

1. Open the user or administrator console.
2. In the window that appears, select the correct X.509 certificate and click **OK**.

OpenID Connect Protocol

OpenID Connect (OIDC) is an authentication protocol based on OAuth 2.0. The protocol allows applications to verify user identity and obtain user information from an Identity Provider.

Axidian Privilege supports the following OIDC authentication modes:

- Compatibility mode — sign-in by email address and identifier

  If a user has no identifier (`sub`) set, authentication compares the PAM user's email address with the `email` in the Identity Provider. If the addresses match, the user signs in to the console, and the received identifier is saved and used for subsequent authentication.

- Strict mode — sign-in by identifier only

  Only users with a defined identifier (`sub`) can sign in to the Axidian Privilege console; matching by email address is disabled. The identifier is not saved automatically and is set by the administrator in the PAM console. Use strict mode to reduce the risk of unwanted linking of privileged accounts.

> ⓘ **INFO**
> Proxy components do not support OpenID Connect authentication.
> To access resources, enable the Session opening without re-authentication and/or SSH Key Authentication options.

Set up authentication

To set up authentication via an external Identity Provider:

1. In the administrator console, go to the **Configuration** → **User Authentication** → **Authentication via OIDC Identity Provider** section.

2. Fill in the required parameters.

Parameters

Option	Description
Enable authentication via OIDC Identity Provider	The option enables authentication using the OpenID Connect protocol via an external Identity Provider. Login using a username and password remains available.
Login button name	The name of the authentication button for the Identity Provider. The button is displayed on the sign-in page of the Axidian Privilege console.
Match users by email on first login	**Compatibility mode** Enable the option to match users by email address if the identifier (`sub`) is not set in PAM. After sign-in, the identifier is saved and used for subsequent authentication. **Strict mode** Disable the option so that only users with a predefined identifier (`sub`) can sign in to PAM via OIDC.
Redirect URI	The address to which the Identity Provider redirects the user after authentication. Copy this value and specify it when registering PAM in the Identity Provider settings.
OIDC Provider URL	The OIDC server address from the Identity Provider settings. Example: `https://idp.company.ru`.

Option	Description
Authentication flow	**Available OIDC authentication flows** - **Authorization Code Flow** — the user is redirected to the authorization server and receives a code that is exchanged for an access token. - **Authorization Code Flow + PKCE (default)** — the recommended flow that uses the Proof Key for Code Exchange (PKCE) extension. An additional secret is generated for each authorization request and is verified when exchanging the code for an access token. - **Implicit Flow** — the authorization server returns the access token in the URL after user authentication. This flow is not recommended due to the risk of token interception.
Client ID	The client identifier created when registering PAM in the Identity Provider.
Client Secret	The client secret issued when registering PAM in the Identity Provider.
Claim	OIDC attribute that PAM uses to retrieve the user's email to match the user account. The default value is `email`.
Scope	The name of the OIDC scope used in the request to the OIDC provider to retrieve the claim containing the user's email. The default value is `email`.

3. Click **Save**.

After the setup, authentication via an external Identity Provider is available on the sign-in page of the Axidian Privilege console.

Manage authentication

After setting up authentication, make sure that for users who need access to PAM:

- OIDC authentication is allowed
- an email address (`email`) or identifier (`sub`) is set

OIDC authentication

To allow or deny a user to sign in via OIDC:

1. In the administrator console, go to the **Users** section and open the user profile.
2. Go to the **Authenticators** tab and, next to the **OIDC authentication** field, click ✎.
3. In the dialog that opens, select an option:
   - **Allow** — the user can sign in via an external Identity Provider (default).
   - **Deny** — the user cannot sign in via OIDC regardless of the configuration, the defined identifier (`sub`), and the email address (`email`).
4. Click **Save**.

Subject Identifier (`sub`)

> ⚠ **CAUTION**
> In strict mode, the identifier (`sub`) in Axidian Privilege must match the `sub` value in the Identity Provider. If the identifier (`sub`) is not set or is outdated in PAM, sign-in via OIDC is unavailable.

To set the identifier (`sub`):

1. In the administrator console, go to the **Users** section and open the user profile.
2. Go to the **Authenticators** tab and, next to the **Subject Identifier (sub)** field, click ✎.
3. In the dialog that opens, specify the identifier and click **Save**.

To delete the identifier (`sub`), next to the **Subject Identifier (sub)** field, click 🗑. If matching by email address is enabled in the configuration, a new identifier (`sub`) value is saved after the user signs in to the PAM console.

Email address (`email`)

To add or update the email address (`email`):

1. In the administrator console, go to the **Users** section and open the user profile.

2. Next to the **Email** field, click ✎ and specify the email address.

> ⓘ **INFO**
> If the user is from a directory service, change the email address in the directory — the data in Axidian Privilege is updated automatically.

3. Click **Save**.

Sign in to PAM via OIDC

> ⓘ **INFO**
> Authentication via an external Identity Provider is an additional sign-in method.
> Sign-in with login and password remains available.

1. Open the user console or the administrator console.
2. Proceed to authentication via the external Identity Provider.
   If the sign-in attempt fails, contact the PAM administrator.

RADIUS Configuring

> ⚠ **CAUTION**
> Please specify all URLs in lowercase.
>
> The JSON format does not allow comments in the file, so you need to remove lines starting with "//" characters.

> ⚠ **CAUTION**
> After changing the configuration file restart application pool IdP in IIS Manager.

Go to `C:\inetpub\wwwroot\idp` and edit file `appsettings.json`.

Section IdentitySettings

- `DirectoryMechanism` — Mechanism of authentication.
- `Authentication` — Authentication provider.

IdentitySettings section in appsettings.json configuration file

```
"IdentitySettings": {
...
"DirectoryMechanism": "Radius",
"Authentication": "Local",
...
}
```

Section Radius

- `Timeout` — timeout waiting for a RADIUS server response.

RemoteEndpoints:

- `Address` — RADIUS server address for connection.
- `Port` — RADIUS server port for connection (default port: 1812).
- `Secret` — secret for the additional authentication of the component.
- `AuthenticationScheme` — authentication scheme in RADIUS. Possible parameters: `PAP`, `CHAP`, `MSCHAPV2`. The `PAP` scheme is insecure.

- `AuthenticationUserName` — name format for authentication. Possible values:
  - `NameWithoutDomain` — name without domain (for authentication in FreeRadius).
  - `SamCompatibleName` — name in the format `AXIDIAN\\user`.
  - `PrincipalName` — name in the format user@axidian.domain.
- `CheckMessageAuthenticator` — enables or disables checking of the `Message-Authenticator` attribute in IDP. It is not recommended to disable it, as it reduces security.

Radius section in appsettings.json configuration file (one RADIUS server)

```
"Radius": {
    "Timeout": 60,
    "RemoteEndpoints": [
      {
        "Address": "PAM_RADIUS_SERVER_ADDRESS",
        "Port": 1812,
        "Secret": "PAM_RADIUS_SERVER_SECRET",
        "AuthenticationScheme": "MSCHAPV2",
        "AuthenticationUserName": "PrincipalName",
        "CheckMessageAuthenticator": true
      }
    ]
  },
```

You can specify multiple RADIUS servers to provide system fault tolerance. In this case, PAM sends the request to the RADIUS servers sequentially, in the order the servers are specified in the configuration file. In other words, if it was unable to connect to the first RADIUS server, then PAM will try to connect to the next one.

Radius section in appsettings.json configuration file (two RADIUS servers)

```
"Radius": {
   "Timeout": 10,
   "RemoteEndpoints": [
     {
       "Address": "10.11.4.28",
       "Port": 1812,
       "Secret": "123",
       "AuthenticationScheme": "MSCHAPV2",
       "AuthenticationUserName": "PrincipalName",
       "CheckMessageAuthenticator": true
     },
     {
       "Address": "10.11.4.128",
       "Port": 1812,
       "Secret": "123",
       "AuthenticationScheme": "MSCHAPV2",
       "AuthenticationUserName": "PrincipalName",
       "CheckMessageAuthenticator": true
     }
   ]
 },
```

Kerberos Authentication

Kerberos is a network authentication protocol that verifies the identity of a user or a host. A user obtains a ticket-granting ticket (TGT) from the Key Distribution Center (KDC), which runs on the domain controller. The user then uses the TGT to request a service ticket and presents that ticket to the service they want to access.

The Kerberos protocol lets Active Directory users sign in to the Axidian Privilege console with a domain account: the user doesn't need to enter a password, because authentication relies on the issued ticket.

> ⚠ **LIMITATIONS**
>
> - Kerberos authentication supports a single Active Directory domain. If other directories are connected, disable them in the Web Wizard.
> - When Kerberos authentication is configured, only internal users can sign in to PAM with a username and password.
> - The time on the Management Server, the domain controller, and the user's computer must be synchronized. If the time skew exceeds the maximum tolerance configured in the domain (5 minutes by default), the KDC rejects the tickets. For more information, see the Microsoft documentation.

Preparing the infrastructure

Select the scenario that matches your PAM deployment.

Management Server on Windows

If the Management Server runs on Windows, complete the following steps:

1. Verify the SPN for each address that users use to open the PAM console.
2. Configure authentication in the Web Wizard.
3. Configure the browser for Kerberos sign-in.

A Windows-based Management Server is joined to the domain, so no `keytab` file is required.

Verifying the SPN

A service principal name (SPN) is the unique identifier of a service instance. Kerberos authentication uses SPNs to associate a service instance with a service logon account.

Basic deployment

> **INFO**
> Perform these steps on a domain controller or on a domain-joined computer that has the Remote Server Administration Tools (RSAT) or the `Active Directory` module for PowerShell installed.

For the DNS name of the SPN management server, an SPN is automatically registered for the computer account if the following conditions are met:

- The Management Server is joined to the domain.
- In the Windows Authentication settings, the `useAppPoolCredentials` parameter is set to `False`, so the service ticket is decrypted with the key of the computer account.

If users open the PAM console through a load balancer address or through a DNS alias that doesn't match the DNS name of the Management Server, register the SPN manually.

Verify that the SPN for each PAM FQDN is registered to exactly one account:

1. Run PowerShell as an administrator.
2. Run the following command:

   ```
   setspn -Q */<PAM FQDN>
   ```

   The output must list a single account. In a basic deployment, this is the computer account of the Management Server, in the format `<domain>\<DNS name of the Management Server>$`.

   If the SPN isn't found, or if it's registered to more than one account, contact your domain administrator.

Load-balanced deployment

If users open the PAM console through the shared virtual address of a load balancer, you must manually register the SPN for the virtual name, because the virtual name doesn't match the DNS name of the Management Server.

To register the SPN:

1. Assign a service account as the identity of the `Axidian.Privilege.Idp` application pool.

   ▼ **How to assign the account**

   > ⓘ **NOTE**
   > Perform these steps on every Management Server.

   1. Open **IIS Manager**.
   2. In the Connections pane, select **Application Pools**.
   3. Right-click the `Axidian.Privilege.Idp` pool, and then select **Advanced Settings**.
   4. In the **Process Model** section, next to **Identity**, click ⋯.
   5. Select **Custom account**, and then specify the service account. Enter the username in the format `DOMAIN\Account name`.
   6. Click **OK**.

2. Configure IIS to use the application pool identity (`Axidian.Privilege.Idp`) for decrypting Kerberos service tickets.

▼ **How to configure `Axidian.Privilege.Idp` to validate tickets**

> **INFO**
> Perform these steps on every Management Server.

1. In the Connections pane, select **Sites** → **Default Web Site** → **idp**.
2. In the **Management** section, double-click **Configuration Editor**.
3. In the **Section** list, select `system.webServer` → `security` → `authentication` → `windowsAuthentication`.
4. Set the `useAppPoolCredentials` parameter to `True`.
5. In the **Actions** pane, click **Apply**.
6. In the **IIS** section, double-click **Authentication**.
7. Select **Windows Authentication**, and then in the **Actions** pane, click **Providers**.
8. Make sure that the authentication providers are listed in the following order:

   ```
   Negotiate
   NTLM
   ```

   If a provider isn't listed, select it in the **Available Providers** list, and then click **Add**.

   To change the order of the providers, use **Move Up** and **Move Down**.
9. Go to **Application Pools**, select `Axidian.Privilege.Idp`, and then in the **Actions** pane, click **Recycle**.

3. Register the SPN for the service account that the `Axidian.Privilege.Idp` application pool runs under.

How to register the SPN manually

> **INFO**
> Perform these steps on a domain controller or on a domain-joined computer that has the Remote Server Administration Tools (RSAT) or the `Active Directory` module for PowerShell installed.

To register the SPN:

1. Run PowerShell as an administrator.
2. Run the following command:

```
setspn -S HTTP/<PAM FQDN> <domain>\<AD account>
```

Example

```
setspn -S HTTP/pam.company.local PAM\pam-ad-user
```

The `-S` switch checks the forest for duplicate SPNs before it adds the SPN.

> **INFO**
> An SPN must be unique within the forest. Don't register the same SPN for another account.

What to do if the SPN is already registered

If `setspn` returns `Duplicate SPN found, aborting operation!`, the SPN is already registered to another account.

To resolve the conflict:

a. Run the following command:

```
setspn -Q HTTP/<PAM FQDN>
```

The output shows the account that the SPN is currently registered to.

b. Delete the SPN from that account:

> ⚠ **CAUTION**
> Coordinate the deletion with your domain administrator. The existing SPN might be in use by another service.

```
setspn -D HTTP/<PAM FQDN> <domain>\<current AD account>
```

c. Register the SPN for the new account:

```
setspn -S HTTP/<PAM FQDN> <domain>\<new AD account>
```

d. Verify that the conflict is resolved and that the SPN is registered to the intended account:

```
setspn -Q HTTP/<PAM FQDN>
```

The output shows the account that the SPN is now registered to.

3. List the SPNs registered to the account:

```
setspn -L <domain>\<AD account>
```

Management Server on Linux

If the Management Server runs on Linux, complete the following steps:

1. Prepare the service account that is used to validate tickets.
2. Register the SPN for each address that users use to open the PAM console.
3. Prepare the `keytab` file that is used to validate tickets.

   > ⚠ **WARNING**
   > The `keytab` file contains the keys of the service account. Treat this file as a secret: never share it or store it in shared file repositories, such as network shares or version control. If the file is compromised, reset the service account password and generate a new `keytab` file.

4. Configure authentication in the Web Wizard.
5. Configure the browser for Kerberos sign-in.

Preparing the Active Directory service account

A Linux-based Management Server isn't joined to the domain, so PAM has no domain account of its own to validate user tickets during Kerberos authentication. A dedicated Active Directory service account fills this role: you generate a `keytab` file for this account, and PAM uses the file to validate the tickets that users present when they sign in to the console.

> ⓘ **INFO**
> Perform these steps on a domain controller or on a domain-joined computer that has the Remote Server Administration Tools (RSAT) or the `Active Directory` module for PowerShell installed.

Active Directory

1. Open **Active Directory Users and Computers**.
2. Go to the appropriate organizational unit, and then create a dedicated service account for the Kerberos configuration.

3. Right-click the new account, and then select **Properties**.
4. On the **Account** tab, in **Account options**, do the following:
   - Select **This account supports Kerberos AES 256 bit encryption**.
   - Clear **Use only Kerberos DES encryption types for this account**.
5. Click **OK**.

PowerShell

1. Run PowerShell as an administrator.

2. Create a dedicated service account for the Kerberos configuration:

```
New-ADUser -Name "<AD account>" -SamAccountName "<AD account>" `
  -UserPrincipalName "<AD account>@<domain>" `
  -AccountPassword (Read-Host -AsSecureString "Password") `
  -PasswordNeverExpires $true -Enabled $true
```

Example command

```
New-ADUser -Name "pam-ad-user" -SamAccountName "pam-ad-user" `
  -UserPrincipalName "pam-ad-user@company.local" `
  -AccountPassword (Read-Host -AsSecureString "Password") `
  -PasswordNeverExpires $true -Enabled $true
```

3. Set the Kerberos AES-256 encryption type for the service account:

```
Set-ADUser <AD account> -KerberosEncryptionType AES256
```

Registering the SPN

A service principal name (SPN) is the unique identifier of a service instance. Kerberos authentication uses SPNs to associate a service instance with a service logon account.

Basic deployment

Determine the primary FQDN that users use to open the PAM console. Register an SPN for this address in the format `HTTP/<PAM FQDN>`, and map it to the dedicated Active Directory

service account.

Load-balanced deployment

If users open the PAM console through the shared virtual address of a load balancer, register the SPN for that shared address, and map it to the dedicated Active Directory service account.

> **INFO**
> Perform these steps on a domain controller or on a domain-joined computer that has the Remote Server Administration Tools (RSAT) or the `Active Directory` module for PowerShell installed.

To register the SPN:

1. Run PowerShell as an administrator.
2. Run the following command:

```
setspn -S HTTP/<PAM FQDN> <domain>\<AD account>
```

Example

```
setspn -S HTTP/pam.company.local PAM\pam-ad-user
```

The `-S` switch checks the forest for duplicate SPNs before it adds the SPN.

> **INFO**
> An SPN must be unique within the forest. Don't register the same SPN for another account.

What to do if the SPN is already registered

If `setspn` returns `Duplicate SPN found, aborting operation!`, the SPN is already registered to another account.

To resolve the conflict:

1. Run the following command:

   ```
   setspn -Q HTTP/<PAM FQDN>
   ```

   The output shows the account that the SPN is currently registered to.

2. Delete the SPN from that account:

   > ⚠ **CAUTION**
   > Coordinate the deletion with your domain administrator. The existing SPN might be in use by another service.

   ```
   setspn -D HTTP/<PAM FQDN> <domain>\<current AD account>
   ```

3. Register the SPN for the new account:

   ```
   setspn -S HTTP/<PAM FQDN> <domain>\<new AD account>
   ```

4. Verify that the conflict is resolved and that the SPN is registered to the intended account:

   ```
   setspn -Q HTTP/<PAM FQDN>
   ```

   The output shows the account that the SPN is now registered to.

3. List the SPNs registered to the account:

```
setspn -L <domain>\<AD account>
```

Preparing the `keytab` file

> ⓘ **NOTE**
> All Management Servers use the same `keytab` file. If you change the service account password or the PAM FQDN, generate a new `keytab` file.

The keytab file contains one or more Kerberos principal names and their corresponding secret keys, which are derived from the service account password. The Management Server uses these keys to decrypt and validate the service tickets that the browser presents.

Generating the `keytab` file

> ⓘ **INFO**
> Perform these steps on a domain controller or on a domain-joined computer that has the Remote Server Administration Tools (RSAT) or the `Active Directory` module for PowerShell installed.

Basic deployment

To generate the `keytab` file, Run PowerShell as an administrator, and then run the following command:

```
ktpass -princ HTTP/<PAM FQDN>@<REALM> `
  -mapuser <domain\AD account> `
  -crypto AES256-SHA1 `
  -ptype KRB5_NT_PRINCIPAL `
  -pass * `
  -out <path to save keytab>
```

Load-balanced deployment

If users open the PAM console through the shared virtual address of a load balancer, generate the `keytab` file for that shared address.

To generate the `keytab` file, Run PowerShell as an administrator, and then run the following command:

```
ktpass -princ HTTP/<Load Balancer FQDN>@<REALM> `
  -mapuser <domain\AD account> `
  -crypto AES256-SHA1 `
  -ptype KRB5_NT_PRINCIPAL `
  -pass * `
  -out <path to save keytab>
```

Store the resulting `keytab` file on a trusted host with restricted access.

Command example and parameters

Example command

```
ktpass -princ HTTP/pam.company.local@COMPANY.LOCAL `
  -mapuser PAM\pam-ad-user `
  -crypto AES256-SHA1 `
  -ptype KRB5_NT_PRINCIPAL `
  -pass * `
  -out http.keytab
```

Parameter	Description
`-princ`	The Kerberos principal that the keys are generated for. Specify the value in the format `HTTP/<PAM FQDN>@<REALM>`, where `REALM` is the Kerberos realm name. In most cases, the realm name is your Active Directory DNS domain name, written in uppercase. For example, `company.local` becomes `COMPANY.LOCAL`.
`-mapuser`	The Active Directory account that the principal is mapped to. The keys in the `keytab` file are derived from the password of this account. For example: `PAM\pam-ad-user`.
`-crypto`	The encryption type of the keys. Specify `AES256-SHA1`.
`-ptype`	The Kerberos principal type. Specify `KRB5_NT_PRINCIPAL`—the general principal type used for user and service accounts.
`-pass`	The password of the Active Directory account. Specify an asterisk (`*`) to be prompted for the password. Avoid passing the password in plain text. `ktpass` resets the account password to the value that you specify.
`-out`	The path or the file name to save the `keytab` file to. You can specify: • only a file name, for example, `http.keytab`. The file is created in the current folder. • a full path, for example, `C:\keytab\http.keytab`.

> ⚠ **WARNING**
>
> Avoid running `ktpass` more than once: each run resets the service account password and increments the Key Version Number (KVNO), which invalidates any `keytab` file generated earlier. Use only the `keytab` file that the most recent run produced.
>
> If you generate the file again, update the `keytab` file in PAM through the Web Wizard.

Validating the `keytab` file

> ⓘ **NOTE**
>
> Validate the file on a trusted Linux host that has restricted access and Kerberos utilities installed.

To validate the `keytab` file:

1. Copy the `keytab` file to the trusted host.
2. In the directory that contains the copy of the `keytab` file, create a `krb5.conf` file with the following structure:

```
[libdefaults]
  default_realm = <REALM>
  dns_lookup_realm = false
  dns_lookup_kdc = true
  rdns = false

[domain_realm]
  .<DNS domain> = <REALM>
  <DNS domain> = <REALM>
```

File example and parameters

Example file

```
[libdefaults]
  default_realm = COMPANY.LOCAL
  dns_lookup_realm = false
  dns_lookup_kdc = true
  rdns = false

[domain_realm]
  .company.local = COMPANY.LOCAL
  company.local = COMPANY.LOCAL
```

Parameter	Description
`default_realm`	The default Kerberos realm—your Active Directory DNS domain name in uppercase letters. The value must match the realm of the principal that is stored in the `keytab` file.
`dns_lookup_realm`	Specifies whether the Kerberos realm is resolved through DNS. Set this parameter to `false`.
`dns_lookup_kdc`	Specifies whether DNS SRV records are used to locate the KDC. Set this parameter to `true`.
`rdns`	Specifies whether reverse DNS lookups (PTR records) are used when host names are canonicalized. Set this parameter to `false`.
`[domain_realm]`	The rules that map DNS names to the Kerberos realm: ◦ `.<DNS domain> = <REALM>` — maps the subdomains of the DNS domain to the realm. ◦ `<DNS domain> = <REALM>` — maps the DNS domain itself to the realm.

3. In the directory that contains the `keytab` and `krb5.conf` files, run the following command to obtain a ticket-granting ticket (TGT) for the service principal:

```
KRB5_CONFIG=./krb5.conf \
KRB5CCNAME=FILE:./<ticket file>.ccache \
kinit -V -kt <keytab file> \
HTTP/<PAM FQDN>@<REALM>
```

For the `KRB5CCNAME` parameter, specify the credential cache file that the ticket is written to.

4. Verify that the ticket was obtained:

```
KRB5CCNAME=FILE:./<ticket file>.ccache klist
```

If the output lists a ticket, the `keytab` file contains valid keys: the keys match the current service account password and the Key Version Number (KVNO) in Active Directory.

If the command returns an error

Error	Possible cause and solution
`Preauthentication failed`	The keys in the `keytab` file don't match the current password or the Key Version Number (KVNO) on the domain controller. Generate the `keytab` file again.
`Keytab contains no suitable keys`	The `keytab` file doesn't contain a suitable key: either the file has no key for the specified principal, or it has no key of an encryption type that the domain controller supports. Check the contents of the file with `klist -kte <keytab file>`.
`Client not found in Kerberos database`	The domain controller has no principal that matches the value of the `-princ` parameter. Make sure that the principal name is correct and that the SPN is registered.
`Server not found in Kerberos database`	The domain controller has no `krbtgt` principal for the requested realm. Make sure that the `REALM` value is correct.
`Cannot find KDC for realm`	The host that runs the validation can't locate a domain controller for the specified realm. Check the DNS settings and the availability of the domain controller.

5. After the validation, destroy the credential cache:

```
KRB5CCNAME=FILE:./<ticket file>.ccache kdestroy
```

6. Delete the `krb5.conf` file and the copy of the `keytab` file from the trusted host.

Configuring authentication in the Web Wizard

You enable Kerberos authentication in the Web Wizard.

1. Launch the Web Wizard.

   How to launch the Web Wizard

   1. In the PAM distribution directory, run the following command to start the Web Wizard:

      ```
      sudo bash run-wizard.sh
      ```

   2. Open the URL that the script displays in the console.

   3. In the **Access code** field, enter the `AuthenticationCode` that the script displays in the console.

      For example: `vVHyTVRyKX5pxUKM6e1ZgCWEnOdXFdOy`.

      > ⚠ **TIME LIMIT**
      > The access code is valid for two hours.

   4. Click **Sign in**.

2. Select a scenario, such as Changing PAM configuration, and follow the instructions in the Web Wizard.

3. On the **Authentication** step, select the **Kerberos** authentication mechanism.

4. Continue to change the configuration by following the instructions in the Web Wizard.

When the Web Wizard finishes, Kerberos authentication is available on the sign-in page of the PAM console.

Configuring the browser

To sign in to the PAM console using the Kerberos protocol, the browser must send the user's domain credentials to the address where the PAM console is opened. To allow this, add the PAM address to the list of addresses allowed for Integrated Windows Authentication. The list is defined by the `AuthServerAllowlist` browser policy.

The `AuthServerAllowlist` policy is configured on a domain controller and distributed through Active Directory Group Policy to all domain-joined computers.

> **NOTE**
> Perform these steps on a domain-joined computer that has the Group Policy Management Tools installed or the `GroupPolicy` PowerShell module available.

1. Run PowerShell as an administrator.
2. Create a Group Policy Object (GPO):

```
New-GPO -Name "<GPO name>"
```

3. Configure the `AuthServerAllowlist` policy for the target browser.

Google Chrome

```
Set-GPRegistryValue -Name "<GPO name>" `
  -Key "HKLM\Software\Policies\Google\Chrome" `
  -ValueName AuthServerAllowlist -Type String -Value "<PAM addresses>"
```

Microsoft Edge

```
Set-GPRegistryValue -Name "<GPO name>" `
  -Key "HKLM\Software\Policies\Microsoft\Edge" `
  -ValueName AuthServerAllowlist -Type String -Value "<PAM addresses>"
```

For the `-Value` parameter, specify the addresses that users use to open the PAM console. You can define the list of allowed addresses in the following formats:

- `<PAM FQDN>` — an individual PAM address, for example, `pam.company.local`
- `*.<DNS domain>` — every PAM address in the domain, for example, `*.company.local`
- `*.<DNS domain>,<PAM FQDN>` — a combined list, for example, `*.company.local,pam.company.local`

Specify explicit PAM FQDNs whenever possible. Use the `*.<DNS domain>` wildcard only when necessary, because it applies the policy to every server in that DNS domain.

4. Link the GPO to the domain or to the organizational unit (OU) that contains the users' computers:

```
New-GPLink -Name "<GPO name>" -Target "<DN of domain or OU>"
```

For the `-Target` parameter, specify the distinguished name (DN) of the domain or OU, for example, `DC=company,DC=local` or `OU=Workstations,DC=company,DC=local`.

The policy takes effect at the next Group Policy refresh interval on the user's computer. To apply the policy immediately, close all browser processes on the target computer, and then run `gpupdate /force`.

How to verify that the policy has been applied

> **INFO**
> Verify the policy on the user's computer.

Google Chrome

1. Open **Google Chrome**, and then enter `chrome://policy` in the address bar. The browser policies page opens.
2. Verify that the **AuthServerAllowlist** policy is listed under **Chrome policies**.

Microsoft Edge

1. Open **Microsoft Edge**, and then enter `edge://policy` in the address bar. The browser policies page opens.
2. Verify that the **AuthServerAllowlist** policy is listed under **Microsoft Edge policies**.

3. (Optional) Run PowerShell as an administrator and purge the cached Kerberos tickets:

```
klist purge
```

4. (Optional) Request a service ticket for the PAM FQDN:

```
klist get HTTP/<PAM FQDN>
klist
```

The output lists the following Kerberos tickets:

- A ticket-granting ticket (TGT), which is used to request service tickets.
- A service ticket (also called a TGS ticket), which is used to authenticate to the PAM console.

Sign in to PAM

> **INFO**
>
> Users from the connected Active Directory domain can sign in only with Kerberos.
>
> Signing in with a username and password is available only for internal PAM users.

1. Open the PAM user console or administrator console.
2. Click **Sign in with domain account**.
3. (Optional) Provide your second authentication factor.

If the sign-in attempt fails, contact the PAM administrator.

TOTP Second Factor via Email Setup

This function allows you to receive the second factor via email. The email address is taken from account data in Active Directory.

If your server's OS is Windows, then go to the directory: `C:\inetpub\wwwroot\idp` and edit the file `appsettings.json`.

If your server's OS is Linux, then go to the directory: `/etc/axidian/axidian-privilege/idp` and edit the file `appsettings.json`.

Find the section **IdentitySettings** and replace **TOTP** to **EMAIL**:

IdentitySettings

```
"IdentitySettings": {
    ...
    "SecondFaType": "TOTP",
    ...
}
```

SMTP Section

```
"Smtp": {
    "Address": "PAM_SMTP_ADDRESS",
    "Port": 587,
    "SenderAddress": "PAM_SMTP_SENDER_ADDRESS",
    "Username": "PAM_SMTP_USERNAME",
    "Password": "",
    "EncryptionMethod": "TLS"
    "AllowedSslProtocols": "Tls12,Tls13"
}
```

- `Address` — SMTP server address.
- `Port` — SMTP server port.
- `SenderAddress` — the address from which the email will be sent.
- `Username` — login for authorization on the server.
- `Password` — password for authorization on the server (encrypted).
- `EncryptionMethod` — TLS supported only.
- `AllowedSslProtocols` — supported TLS versions.

Service Operations

Service Operations for Windows Resources

> ⚠ **CAUTION**
> If the management server components are installed on the Linux operating system, then the WinRM service must be configured over HTTPS on the Windows resource to perform service operations.

The following service operations are performed at Windows resources on behalf of the domain or local service account:

- Checking of connection to resources
- Synchronization of local accounts
- Checking of local account passwords
- Changing of local account passwords
- Getting data about operating system
- Getting list of security groups

Configuring a Domain Account as Service One

1. Log in to resource
2. Run the **Computer management** snap-in
3. Switch to **System tools** → **Local Users and Groups** → **Groups section**
4. Open the context menu of **Administrators** group
5. Select **Properties** item
6. Click **Add**
7. Select the domain account to be used as service one for the resource and click **OK**

Configuring a Local Account as Service One

If you plan to use local built-in administrator account as service account, then no additional configuration is required. Otherwise, proceed as follows:

1. Log in to resource

2. Run the **Computer management** snap-in
3. Switch to **System tools** → **Local Users and Groups** → **Groups** section
4. Open the context menu of **Administrators** group
5. Select **Properties** item
6. Click **Add**
7. Select the local account to be used as service one for the resource and click **OK**
8. Run **Windows registry editor** (RegEdit)
9. Expand
   the `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\` branch
10. Open the context menu of **System** section
11. Select **Create** → **DWORD (32-bit) Value**
12. Specify the parameter name — **LocalAccountTokenFilterPolicy**
13. Open the context menu of **LocalAccountTokenFilterPolicy** parameter
14. Select **Modify** item and set the **Value data:** equal to **1**

Registry editing is required due to restrictions on remote WinRM management for all local accounts except for built-in administrator account.

Configuring Axidian Privilege Core to Perform Service Operations on behalf of Local Resource Accounts

Service operations are performed using WinRM. To use local resource accounts as service one, you must add the resource to the **TrustedHosts** list of trusted ones on Axidian Privilege Core server.

Configuring the TrustedHosts List

1. Log in to the server on which Axidian Privilege Core will be installed
2. Run **Command line** (CMD) as Administrator
3. Execute the following command:

```
C:\>winrm s winrm/config/client @{TrustedHosts="Resource1.domain.local,
Resource2.domain.local"}
```

The specified resources shall be added to the TrustedHosts list.

> ⚠ **CAUTION**
>
> When adding new resources to the trusted list, you must specify previously added resources and new ones, since the new value overwrites the old one.

```
@{TrustedHosts="Resource1.domain.local, Resource2.domain.local, Resource3.domain.local"}
```

Service Operations in Directory Service

> ⚠ **CAUTION**
>
> If the management server components are installed on the Linux operating system, then LDAPS (LDAP over SSL) must be configured in the domain to perform service operations.

Account for service operations in Active Directory

1. Start the **Active Directory Users and Computers** snap-in.
2. Open the context menu of the Container or Organization Unit.
3. Select **Create** → **User** item.
4. Enter the name, for example, **IPAMADServiceOps**.
5. Fill in the required fields and complete the creation of the account.
6. Open the context menu of the container, organizational unit, or domain root.
7. Select the **Properties** item.
8. Go to the **Security** tab.

   > ⓘ **INFO**
   >
   > If there is no **Security** tab, then in the **View** menu, enable Advanced features.

9. Click **Add**.
10. Select **IPAMADServiceOps** account and click **OK**.
11. Click **Advanced**.

12. Select **IPAMADServiceOps** and click **Edit**.
13. For the field **Applies to:** set value **Descendant User objects**.
14. In the **Permissions:** section check **Reset password**.
15. Save all changes.

Service Operations for *nix Resources

The following service operations are performed at *nix resources on behalf of the local service account:

- Checking of connection to resource
- Searching for local accounts
- Checking of local account passwords
- Changing of local account passwords
- Getting data about operating system
- Getting list of security groups

Creating and Configuring a Service Account

1. Log in to resource.
2. Run **Terminal**.
3. Create a user, for example **IPAMService**:

```
adduser IPAMService
```

4. Add the user to **SUDO** group

```
usermod -aG sudo IPAMService
```

Configuring a Group of Privileged Accounts

Automatic searching and adding of Access accounts to Axidian Privilege is performed based on their permission to execute a SUDO command. To grant the permission to execute SUDO command, you may need to edit the `/etc/sudoers` file.

Administration

Management console

18 items

First Launch

License the product, specify network paths to storages and add all objects

Policy Setup

Select the sections that will be controlled by the policies

Configuring User Connections via SSH keys

Configuring User Connections via SSH keys

Dumping Passwords

Read about dumping passwords in an emergency

Usage of PostgreSQL and MSSQL Proxy

Explore Axidian Privilege PostgreSQL Proxy and MSSQL Proxy

Usage of Web Proxy

Learn about the capabilities of Web Proxy

Dashboard
Analyze user activity and system status in real time.

Management console

Administration of Axidian Privilege is performed using a special interface for Axidian Privilege Core — administrator console. It is available at:

- **Windows:** https://pam.domain.local/mc
- **Linux:** https://pam.domain.local/mc

> **INFO**
> The monitor screen resolution must be at least 1280 pixels wide, otherwise the elements of the administrator console interface will not be displayed correctly.

Authentication

To access the administrator console, the second authentication factor is required. To register your first authenticator, please proceed as follows:

1. Run the administrator console as the user, whose SID is specified in IDP configuration.
2. Read the instruction for authenticator registration.
3. Install the application to generate OTP and scan the QR-code.
4. Enter the obtained value to **Authenticator Code** field at the registration page.

After successful registration, you will be redirected to the Management Console. When reconnecting to the Management Console, you must enter a new TOTP code from the 2fa application.

> **TIP**
> After the first login, to enable management functions, you must add the user to the Administrator Role.

Login

1. Open the administrator console.
2. Enter Login. Examples of login format:
    - john.smith@space.local—UPN format login

- SPACE\john.smith—domain\user format login
- john.smith—no domain format login

> ⓘ **INFO**
> If there are several users in the company infrastructure with the same login: one from the user directory and one the internal user, then to log in as directory user enter the login with the domain.

3. Enter the password.
4. Click **Log in**.
5. Enter the second authentication factor.

Password Change

> ⚠ **CAUTION**
> This operation is only applicable for internal users.

Internal user can change their password on their own. To do so:

1. Authenticate in the Administrator Console.
2. In the upper right corner, click on login.
3. In the drop-down list, select **Change password**.
4. In the window that opens, enter the current password and the new password.
5. Optionally disable the **End all active sessions** option.
6. Click **Change password**.

Logout

1. Make sure you are authenticated in the administrator console.
2. In the upper right corner, click on your login.
3. In the drop-down list, click **Exit** and confirm the action.

Users

This section is intended for working with the following types of Axidian Privilege users:

- Users from directory service.
  For such users, the **Source** field indicates *Catalog*.
- Internal users.
  For such users, the **Source** field indicates *PAM*.

By default, 15 users are displayed. When this number is exceeded, a switcher will appear at the bottom of the page. Only 1000 users are available for viewing. The number of users displayed by default on the page can be changed in the configuration file:

- Windows: `C:\inetpub\wwwroot\mc\assets\config\config.prod.json`
- Linux: `/etc/axidian/axidian-privilege/mc/config.prod.json`

User search

Enter a first name, last name, phone number, or email address in the search string and click .

Click **Extended search**, set one or more filters and click **Search**.

> **INFO**
> Login search is not supported.

To find removed users:

1. Open the **Users** section and click **Extended search**.
2. Select the **Deleted** value for the **State** parameter.
3. Click **Search**.

Create an internal user

> ⚠ **WARNING**
>
> Do not close the window until you have passed the password to the user.
>
> Connection via RDS is not available for internal users.

1. Open the **Users** section.
2. Click **Create**.
3. Set the user's login. The login is used to access the user and administrator consoles.
4. Select the option:
   - **Set password manually** — the password is set manually.
   - **Generate** — the password will be generated by PAM.
5. Copy the password and pass it to the user.
6. Set the **Require password change on first login** option.
7. Set the user's Email.
8. Click **Optional fields** and fill in the fields: **First Name**, **Last Name**, **Phone**, **Description**.
9. Complete adding the user:
   - Click **Create** to stay in the **Users** section.
   - Click **Create and open** to navigate to the new user's profile.

User profile

For each user, the following is displayed:

- **Permissions** — list of granted permissions for the user to connect to the resource.
- **User groups** — list of groups the user belongs to.
- **Sessions** — list of active, ended, and aborted sessions.
- **Authenticators** — information about the user's configured authenticators.
- **Events** — records of operations related to the user.

Edit data in the profile

1. Open the user's profile.
2. Click ✎ next to the parameter to set or edit it.

Select a policy

1. Open the user's profile.
2. Click ✎ next to the **Policy** parameter.
3. Select a policy from the list and click **Select**.

Configure authenticator

The **Authenticators** tab displays information about the password, second factor, and SSH keys that allow connecting to SSH Proxy without a password.

For an internal PAM user, the date and time of the last password change, as well as the password expiration period, are displayed.

For all users, the authenticator status is displayed. The value *Not enrolled* indicates an unregistered authenticator. When the user first logs into the administrator console or user console, a page with instructions for registering the authenticator will open. After registration, the value *Enrolled* is displayed.

Add SSH key

SSH keys allow connecting to SSH Proxy without a password. A maximum of 10 SSH keys can be added to one user. Keys must be unique within a single user, but can be repeated across different users.

Supported key encryption algorithms:

- rsa-sha2-256
- rsa-sha2-512
- ecdsa-sha2-nistp256
- ecdsa-sha2-nistp384
- ecdsa-sha2-nistp521
- ssh-ed25519

Enabling or disabling the use of keys can be done in the Configuration section.

> ⚠ **WARNING**
> To add a key to a user, the administrator must have the *User.ManageSshAuthorizedKeys* privilege.

To add an SSH key:

- paste the copied string containing the encryption algorithm and key
- attach an X.509 certificate file

Key in text format

1. Open the user's profile.
2. Go to the **Authenticators** tab.
3. Click **Add**.
4. Paste the key in OpenSSH format into the **Public key** field. The key string must contain the encryption algorithm and the key. Optionally, the string may contain a comment, such as a username and a host. Example: ssh-ed25519 AAAAC3... user@host
5. Optionally enter a **Description**.
6. Click **Add**.

X.509 Certificate

1. Open the user's profile.
2. Go to the **Authenticators** tab.
3. Click **Add**.
4. Click **Upload certificate**.
5. Check the validity of the certificate dates. To do this, run one of the commands, depending on the OS used:

   Command for Windows

   ```
   certutil -verify -urlfetch "yourfilename.crt"
   ```

Command for Linux

```
openssl x509 -in "yourfilename.crt" -text -noout
```

Make sure that the period in which the key connection is planned falls within the date interval between `NotBefore` and `NotAfter`.

6. Upload the file in the **X.509 Certificate** field.

> ⚠ **CAUTION**
> Loading the certificate that contains the certificate chain is not supported.
>
> Please note that there is no automatic validation of the certificate dates. If the certificate has expired or is not yet valid, the key will be loaded and the session with such a key will open.

7. Optionally edit the **Description**.

8. Click **Add**.

> ⚠ **WARNING**
> The key cannot be recovered after deletion.

To delete an SSH key:

1. Open the user's profile.
2. Go to the **Authenticators** tab.
3. Select one or more keys.
4. Click **Remove**.

When an SSH key is deleted, a session opened using this key is not terminated.

> ⓘ **NOTE**
> If the same key is added to multiple users, deleting the key for one user will not result in the deletion of the same key for other users.

Two-factor authentication

1. Open the user's profile and go to the **Authenticators** tab.
2. Click ✎ next to the **Require 2FA** parameter and select one of the options:
   - **Default** — by default, the user is required to enter a second factor for authentication in the system.
   - **Enabled** — the user is required to enter a second factor for authentication in the system.
   - **Disabled** — the user is not required to enter a second factor for authentication in the system.
3. Click **Change**.

To reset the authenticator, click ✕ next to the desired authenticator.

X.509 certificate

> ⓘ **INFO**
>
> To add a `Subject` value for a user, the administrator must have the *Manage X.509 certificate Subject for users* claim.

Specify the `Subject` value for all users with X.509 certificate authentication enabled. If `Subject` is not set or entered incorrectly, the user will not be able to log into the console.

To add a certificate `Subject`:

1. In the admin console, go to the **Users** section.
2. Open the user profile and go to the **Authenticators** tab.
3. Next to the **Subject** field, click ✎ and select one of the options:
   - **Paste manually** — enter the certificate `Subject` value.

Example

Single line, comma-separated

```
CN=John Smith,OU=Development Department,O=Company
```

Multiline

```
CN=John Smith
OU=Development Department
O=Company
```

- **Upload certificate** — select and upload a certificate in .cer, .crt, .pem, or .der format. If the certificate is correct, the recognized `Subject` value will be displayed.

4. Click **Save**.

OIDC Identity Provider

Make sure that for users who need access to PAM via OIDC:

- OIDC authentication is allowed
- an email address (`email`) or identifier (`sub`) is set

OIDC authentication

To allow or deny a user to sign in via OIDC:

1. In the administrator console, go to the **Users** section and open the user profile.
2. Go to the **Authenticators** tab and, next to the **OIDC authentication** field, click ✎.
3. In the dialog that opens, select an option:
   - **Allow** — the user can sign in via an external Identity Provider (default).
   - **Deny** — the user cannot sign in via OIDC regardless of the configuration, the defined identifier (`sub`), and the email address (`email`).
4. Click **Save**.

Subject Identifier (`sub`)

> ⚠ **CAUTION**
> In strict mode, the identifier (`sub`) in Axidian Privilege must match the `sub` value in the Identity Provider. If the identifier (`sub`) is not set or is outdated in PAM, sign-in via OIDC is unavailable.

To set the identifier (`sub`):

1. In the administrator console, go to the **Users** section and open the user profile.
2. Go to the **Authenticators** tab and, next to the **Subject Identifier (sub)** field, click ✎.
3. In the dialog that opens, specify the identifier and click **Save**.

To delete the identifier (`sub`), next to the **Subject Identifier (sub)** field, click 🗑. If matching by email address is enabled in the configuration, a new identifier (`sub`) value is saved after the user signs in to the PAM console.

Email address (`email`)

To add or update the email address (`email`):

1. In the administrator console, go to the **Users** section and open the user profile.
2. Next to the **Email** field, click ✎ and specify the email address.

   > ⓘ **INFO**
   > If the user is from a directory service, change the email address in the directory — the data in Axidian Privilege is updated automatically.

3. Click **Save**.

Create permission

Permissions allow users to connect to resources.

To create a permission:

1. Open the user's profile and click **Create permission**.
2. (Optional) Select an organizational unit and click **Select**.
3. Define the permission composition. If necessary, modify the preset parameters.

More about permission scope

1. Select who gets access:
   - **Users** — the permission is granted to one or several selected users.
   - **User group** — the permission is granted to one selected user group.
2. Select what to get access to:
   - **Resources** — the permission is granted to one or several selected resources.
   - **Resource groups** — the permission is granted to one selected resource group.
   - **Ad hoc connections** — the permission is granted to Ad hoc resources with the selected connection type, including resources not registered in PAM. One shared account is used for all connection types.

     > ⚠ **LICENSE REQUIRED**
     > A special license is required to work with Ad hoc resources.
     >
     > A special license is required to create a permission for PostgreSQL or MSSQL. Before creating the permission, add an account from the DBMS to PAM. You need to specify it in the permission.
3. Click **Next**.
4. Select the account under which the user will open a session on the resource:
   - **Select account in PAM** — the permission is granted to an account added to Axidian Privilege.
   - **Use user account** — the permission is granted to an arbitrary account.
     The user needs to enter the login and password of the account on the resource. In RDP and SSH sessions, it is possible to log in using the current Axidian Privilege user credentials.

4. (Optional) Configure access to credentials.

More about access settings

You can grant access to credentials only at the permission creation step.

The following settings are available:

- **Credentials** — the option defines actions with credentials:
  - **Allow view account credentials** — users can view passwords of the accounts from this permission.
  - **Allow change account credentials** — users can change passwords of the accounts from this permission.
- **Allow running pamsu in SSH sessions** — the setting defines access to PamSU when connecting via SSH Proxy:
  - **Managed by policies** — access to PamSU is determined by the policy of the resource for which the permission is granted.
  - **Allowed** — the user can use PamSU regardless of policy settings.
  - **Denied** — the user is not allowed to use PamSU regardless of policy settings.

5. (Optional) Fill in the **Description** field.

6. (Optional) Configure time restrictions.

More about time restrictions

You can set a schedule according to which users are allowed to open sessions or change credentials. For example, you can grant permission to work only on weekdays from 8:00 to 17:00.

The following settings are available:

- **Validity period** — the time period during which the permission is valid. For example, you can grant permission for one day or month.
  - **Begin** — set the date and time when the permission becomes active.
    If only **Begin** is set, the permission will become active on the selected date, and its validity period will be unlimited.
  - **End** — set the date and time when the permission becomes inactive.
    If only **End** is set, the permission will become active at the moment of creation, but will be suspended on the specified date.

    > **INFO**
    > If the **Begin** and **End** parameters are not set, the permission will be valid indefinitely.

- **Access schedule** — restrictions by days of the week taking into account the specified schedule.
  - **Allow access only on selected days** — select the days of the week when the permission will be active.
  - **Allow access only during selected hours** — select the time when the permission will be active.

    > **INFO**
    > Access by days of week is granted according to the management server time zone.

After the validity period expires, the permission will transition to the *Restricted/Inactive* state, and the user session will be terminated.

7. In the **Connection source** setting, select the network address from which sessions to the resource are allowed to be opened. If no network locations are added to PAM, the value is set to **No restrictions** — the permission can be used from any device on the network.

8. Check the data and click **Create permission**.

Add and remove from group

To add a user to a group:

1. Open the user's profile and go to the **User Groups** tab.
2. Click **Add user group**.
3. Select one or more groups and click **OK**.

To remove a user from a group:

1. Open the user's profile and go to the **User Groups** tab.
2. Select one or more groups.
3. Click **Remove**.
4. In the pop-up window, click **Remove**.

To add multiple users to a group, in the **Users** section select the required users and click **Add to group**. Select one or more groups and click **OK**.

Set, reset, or request password

> ⚠ **WARNING**
> Available only for internal users.

1. Open the internal user's profile.
2. Click **Reset password**.
3. Select one of the checkboxes:
   - **Generate** — password is created automatically.
   - **Set password manually** — password is set in manual mode.
   - **Request password change** — password is requested by PAM upon system login.
4. Provide the password to the user. After closing the form, it will be impossible to retrieve the password.

5. Set the checkbox **Require password change on first login**.
6. Set the checkbox **Terminate all active sessions and log out**.
7. Click **Save**.

To reset the password for multiple users, in the **Users** section select the required users and click **Request password change**. You can terminate all active sessions of the selected users.

Block and unblock

Block a user if you need to restrict access to PAM. When blocked, access to the system is completely terminated: authentication in user and administrator consoles is unavailable, and all active sessions are terminated. A user can be unblocked at any time.

To block a user:

1. Go to the **Users** section.
2. Open the user's profile.
3. Click **Block**.
4. In the pop-up window, click **Block**.

To block multiple users, in the **Users** section select the required users and click **Block**.

To unblock a user:

1. Go to the **Users** section.
2. Open the blocked user's profile.
3. Click **Unblock**.
4. In the pop-up window, click **Unblock**.

To unlock multiple users, in the **Users** section, select the locked users and click **Unlock**.

Delete a user

> ⚠ **WARNING**
> This operation is only applicable to internal users.
>
> A deleted user cannot be restored. It is not possible to delete yourself or the first role administrator.

To delete a user:

1. Open the internal user's profile.
2. Click **Remove**.
3. Read the information in the pop-up window and click **Remove**.

To remove multiple PAM users, in the **Users** section, select the required users and click **Remove**.

Upon user deletion:

- The user will lose access to PAM and will no longer be able to authenticate.
- All active sessions will be terminated.
- All granted permissions will be revoked.
- The user will be removed from all user groups.
- The user will be removed from the scope of all policies.

Deleted users no longer appear in the **Users** section, but they can be viewed using extended search.

User Groups

The section presents working with permissions of user groups.

Add Axidian user group

1. Navigate to the **User Groups** section and click **Add**.
2. Fill in the **Name** and **Description** fields.
3. Click **Save**.

Add from catalog

1. Navigate to the **User Groups** section and click **Add from directory**.
2. Enter the directory name and click .
3. Select the group and click **Save**.

Group profile

For each user group, the following are displayed:

- **Users** — a list of users who are members of the group.
- **Permissions** — a list of granted permissions for the group to connect to resources.
- **Sessions** — a list of active, ended, and aborted sessions.
- **Events** — records of operations related to the group.

Add users to the group

> **INFO**
> Only for groups created via Axidian Privilege.

To add users to a group:

1. Open the user group profile.
2. Go to the **Users** tab and click **Add users**.

3. Select one or multiple users and click **OK**.
4. Confirm the selection and click **Add**.

Create permission

Permissions allow users to connect to resources.

To create a permission:

1. Open the group profile and click **Create permission**.
2. (Optional) Select an organizational unit and click **Select**.
3. Define the permission composition. If necessary, modify the preset parameters.

More about permission scope

1. Select who gets access:
   - **Users** — the permission is granted to one or several selected users.
   - **User group** — the permission is granted to one selected user group.
2. Select what to get access to:
   - **Resources** — the permission is granted to one or several selected resources.
   - **Resource groups** — the permission is granted to one selected resource group.
   - **Ad hoc connections** — the permission is granted to Ad hoc resources with the selected connection type, including resources not registered in PAM. One shared account is used for all connection types.

     > ⚠ **LICENSE REQUIRED**
     > A special license is required to work with Ad hoc resources.
     >
     > A special license is required to create a permission for PostgreSQL or MSSQL. Before creating the permission, add an account from the DBMS to PAM. You need to specify it in the permission.
3. Click **Next**.
4. Select the account under which the user will open a session on the resource:
   - **Select account in PAM** — the permission is granted to an account added to Axidian Privilege.
   - **Use user account** — the permission is granted to an arbitrary account.
     The user needs to enter the login and password of the account on the resource. In RDP and SSH sessions, it is possible to log in using the current Axidian Privilege user credentials.

4. (Optional) Configure access to credentials.

More about access settings

You can grant access to credentials only at the permission creation step.

The following settings are available:

- **Credentials** — the option defines actions with credentials:
  - **Allow view account credentials** — users can view passwords of the accounts from this permission.
  - **Allow change account credentials** — users can change passwords of the accounts from this permission.
- **Allow running pamsu in SSH sessions** — the setting defines access to PamSU when connecting via SSH Proxy:
  - **Managed by policies** — access to PamSU is determined by the policy of the resource for which the permission is granted.
  - **Allowed** — the user can use PamSU regardless of policy settings.
  - **Denied** — the user is not allowed to use PamSU regardless of policy settings.

5. (Optional) Fill in the **Description** field.

6. (Optional) Configure time restrictions.

More about time restrictions

You can set a schedule according to which users are allowed to open sessions or change credentials. For example, you can grant permission to work only on weekdays from 8:00 to 17:00.

The following settings are available:

- **Validity period** — the time period during which the permission is valid. For example, you can grant permission for one day or month.
  - **Begin** — set the date and time when the permission becomes active.
    If only **Begin** is set, the permission will become active on the selected date, and its validity period will be unlimited.
  - **End** — set the date and time when the permission becomes inactive.
    If only **End** is set, the permission will become active at the moment of creation, but will be suspended on the specified date.

    > **INFO**
    > If the **Begin** and **End** parameters are not set, the permission will be valid indefinitely.

- **Access schedule** — restrictions by days of the week taking into account the specified schedule.
  - **Allow access only on selected days** — select the days of the week when the permission will be active.
  - **Allow access only during selected hours** — select the time when the permission will be active.

    > **INFO**
    > Access by days of week is granted according to the management server time zone.

After the validity period expires, the permission will transition to the *Restricted/Inactive* state, and the user session will be terminated.

7. In the **Connection source** setting, select the network address from which sessions to the resource are allowed to be opened. If no network locations are added to PAM, the value is set to **No restrictions** — the permission can be used from any device on the network.

8. Check the data and click **Create permission**.

Synchronize user groups with directory

> ⓘ **INFO**
> Only for groups from directory service.

1. Open the user group profile.
2. Click **Sync** and confirm the action.

Select policy

1. Open the user group profile.
2. Click ✎ next to the **Policy** parameter.
3. Select a policy from the list and click **Select**.

Remove

1. Open the user group profile.
2. Click **Remove**.
3. Confirm the action by clicking **Remove**.

To remove multiple groups, in the **User Groups** section, select the required groups and click **Remove**.

Resources

The section is intended for working with resources — objects that need to be accessed on behalf of accounts stored in Axidian Privilege. Resources include Windows and Linux servers, workstations, DBMS, network equipment, websites, or client applications.

Resource profile

The following is displayed for each resource:

- **User connections** — the list of connections used to establish a connection to the resource. For each resource, you can create multiple user connections. This is required when the server hosts multiple applications that require privileged access.
- **Permissions** — the list of issued permissions for connecting to the resource.
- **Local accounts** — the list of accounts used to open a session on the resource.
- **Resource groups** — the list of groups the resource is added to.
- **Sessions** — the list of active, finished, and aborted sessions on the resource.
- **Events** — records of operations related to the resource.
- **Services** — the list of applications that can start automatically when the operating system starts. The tab is displayed if the associated resource has a service connection configured for Windows.

Find resource

Enter the resource name, DNS name, IP address, connection address, or tag in the search bar and click .

Click **Extended search**, set one or more filters and click **Search**.

Add resource

To connect to a resource, it must be added to Axidian Privilege. This can be done in the following ways:

- Manually in the PAM administrator console.
- Automatically using a CSV file, if you need to add multiple resources at once.

Add manually

1. Go to the **Resources** section and click **Add**.
2. Fill in the **Resource name** field.
   For resources with Windows OS, specify the computer name.
3. Fill in the **DNS name** and/or **IP address** field.
4. Enter a description and click **Next**.
5. Select the user connection type.
6. Select the connection address:
   - **Inherit from the resource** — the connection address duplicates the DNS name, URL, or IP address of the resource.
   - **Enter manually** — the connection address is set manually in the format `https://app.local:port` or `https://app.local`.
7. Fill in the **Port** field.
8. Specify additional parameters depending on the selected connection type:

   PostgreSQL or MSSQL

   Fill in the **Default database** field.
   Choosing a default database does not restrict the user's access to other databases on this resource. The available databases are determined by the rights of the DBMS account specified in the permission.

SSH

1. Set SSH key fingerprint:

   - **Get from resource** — use the SSH key fingerprint from the resource.
   - **Enter manually** — select the algorithm and enter the fingerprint in SHA256 format.

2. Specify the login formats for local and domain accounts:

   - **Default** — the format specified in the connection configuration.
   - **Set manually** — login formats are set manually.
     Use the required variable `%username%` and the optional variables `%location%`, `%location-dns%`.

     #### Examples

     Login format for john.smith@pam.local

     ```
     %username%@%location-dns%
     ```

     Login format for SPACE\john.smith

     ```
     %location%\%username%
     ```

     Login format for john.smith

     ```
     %username%
     ```

RDP

(Optional) Enable the **Run as administrator** option.
The RDP session will open with the `/admin` parameter. The user will have access to the administrative console and will be able to execute commands that require elevated privileges.

▼ **User connection**

> **INFO**
> You can add your own custom connection type in the Configuration → User connection section.

1. (Optional) In the **URL** field, specify the URL to go to when starting the web session.
2. (Optional) Enable the **Regular expression** option if query parameters are dynamically added to the URL when navigating to the specified page.
   In the **URL** field, specify the regular expression corresponding to the page address.

   ▼ **Example**

   The session opens at `https://app.org/mainpage` .

   When clicking on a link to a URL, the parameters `theme` and `page` are dynamically added.
   The page address takes the form `https://app.org/mainpage /?theme=dark&page=dashboard`.

   To go to the desired address, enable the **Regular expression** option and in the **URL** field, specify the regular expression corresponding to the page address.
   For example: `https://app.org/mainpage *`, where the character `*` replaces additional parameters in the query string.

9. (Optional) Enable the **Use connector for service connection** option and configure the service connection. On the next step, select the service account.
10. Click **Next**.
11. Check the entered data and click **Save**.

Add from file

1. Create a CSV file using the following template:

```
Name;Description;DNS name;IP address;UC type;UC address;UC port;UC matching url;UC
matching url is regex;SC account name;SC type;SC SSH template;SC address;SC port;Cisco
privilege mode password
```

Parameters

Parameter	Requirement	Description
`Name`	Required	Resource name
`Description`	Optional	Description
`DNS name` or `IP address`	Required	DNS name or IP address of the resource. Specify one of the parameters.
`UC type`	Required	User connection type. For more details, see User connection.
`UC address`	Optional	IP address or DNS name of the user connection
`UC port`	Optional	User connection port
`UC matching url`	Optional	Login page URL for a web resource
`UC matching url is regex`	Optional	Indicates whether the login page URL is a regular expression: ◦ `true` — yes ◦ `false` — no Specify if the `UC matching url` parameter is set.
`SC account name`	Optional	Service account name
`SC type`	Optional	Service connection type. For more details, see Service connection.

Parameter	Requirement	Description
`SC SSH template`	Optional	SSH connector template name. Specify if the service connection type is `SSH`.
`SC address`	Optional	IP address or DNS name of the service connection
`SC port`	Optional	Service connection port
`Cisco privilege mode password`	Optional	Cisco privileged mode password. Specify if the service connection type is `Cisco IOS`.

CSV file example

```
APP01;Application server;app01.local;;RDP;;;;;DOMAIN\svc_app;Windows;;;;
WEB01;Corporate
website;portal.local;;WebTemplate;https://portal.local/;;https://portal.local/login
;FALSE;DOMAIN\svc_web;Windows;;;;
SSH01;Linux server;;192.168.0.50;SSH;;;;;;;;;
```

2. In the administrator console, go to the **Resources** section.
3. Click **Add from file**.
4. In the window that opens, click **Select** and upload the CSV file.
5. (Optional) Enable the **Add with policy** option if a policy needs to be defined for the resources.
6. Click **Save**

Add resource to group

Groups allow you to organize work in the console. Group resources by the attribute you need, for example by department or connection type.

To add a resource to a group:

1. Open the resource profile and go to the **Resource groups** tab.
2. Click **Add resource group**.
3. Select a group and click **Next**.
4. Select one or more user connections and click **Next**.
5. Select one or more accounts for user connection and click **Next**.
6. Check the data and click **Add**.

Add service

> **INFO**
> The tab is displayed if the resource has a service connection configured for Windows.

Add to PAM the services that run on behalf of accounts managed by PAM. These services will automatically receive the current account password when it is changed through PAM.

To add a service:

1. Open the resource profile and **Services** tab.
2. Click **Add service**.
3. Enter the service name and description.
4. (Optional) Set the **Restart the service when the service password is changed** option and click **Next**.
5. Select account for service and click **Next**.
6. Check the data and click **Add**.

Select policy

A policy regulates user actions on a resource. For example, you can restrict the use of the clipboard or allow the execution of certain SSH commands.

One resource

To set a policy:

1. Open the resource profile and click ✎ next to the **Policy** parameter.
2. In the window that appears, select a policy and click **Select**.

Multiple resources

To set a policy for multiple resources:

1. Go to the **Resources** section and select the resources you need.
2. Click **Set policy**.
3. Select a policy and click **Select**.
4. Click **Set** to confirm the policy selection.

Set organizational unit

One resource

To set an organizational unit:

1. Go to the **Resources** section and open the resource profile.
2. Click **Move**.
3. In the window that appears, select an organizational unit and click **OK**.

Multiple resources

To set an organizational unit for multiple resources:

1. Go to the **Resources** section and select the resources you need.
2. Click **Set organizational unit**.
3. Select an organizational unit and click **OK**.
4. Click **Set** to confirm the organizational unit selection.

Add and delete tag

Tags help organize work in PAM. If you don't have any tags yet, create them in the Configuration section.

One resource

To add tags to a resource:

1. Open the resource profile and click + next to the **Tags** field.
2. Select one or more tags and click **Next**.
3. Check the data and click **Add**.

Multiple resources

To add tags to multiple resources:

1. In the **Resources** section, select the resources you need and click **Add tags**.
2. Select one or more tags and click **Next**.
3. Check the data and click **Add**.

To delete a tag, in the resource profile click ✕ next to the desired tag and confirm the action.

Add user connection

Add a user connection to open sessions over various protocols.

1. Open the resource profile.
2. On the **User connections** tab, click **Add user connection**.
3. Select the connection type.
4. Select the connection address:
    - **Inherit from the resource** — the connection address duplicates the DNS name, URL, or IP address of the resource.

- **Enter manually** — the connection address is set manually in the format `https://app.local:port` or `https://app.local`.

5. (Optional) Specify the port if it differs from the default port.

6. Specify additional parameters depending on the selected connection type:

> **PostgreSQL or MSSQL**
>
> Fill in the **Default database** field.
> Choosing a default database does not restrict the user's access to other databases on this resource. The available databases are determined by the rights of the DBMS account specified in the permission.

SSH

1. Set SSH key fingerprint:

   - **Get from resource** — use the SSH key fingerprint from the resource.
   - **Enter manually** — select the algorithm and enter the fingerprint in SHA256 format.

2. Specify the login formats for local and domain accounts:

   - **Default** — the format specified in the connection configuration.
   - **Set manually** — login formats are set manually.
     Use the required variable `%username%` and the optional variables `%location%`, `%location-dns%`.

     #### Examples

     Login format for john.smith@pam.local

     ```
     %username%@%location-dns%
     ```

     Login format for SPACE\john.smith

     ```
     %location%\%username%
     ```

     Login format for john.smith

     ```
     %username%
     ```

RDP

(Optional) Enable the **Run as administrator** option.
The RDP session will open with the `/admin` parameter. The user will have access to the administrative console and will be able to execute commands that require elevated privileges.

User connection

> **INFO**
> You can add your own custom connection type in the Configuration → User connection section.

1. (Optional) In the **URL** field, specify the URL to go to when starting the web session.
2. (Optional) Enable the **Regular expression** option if query parameters are dynamically added to the URL when navigating to the specified page.
   In the **URL** field, specify the regular expression corresponding to the page address.

   #### Example

   The session opens at `https://app.org/mainpage` .

   When clicking on a link to a URL, the parameters `theme` and `page` are dynamically added.
   The page address takes the form `https://app.org/mainpage /?theme=dark&page=dashboard`.

   To go to the desired address, enable the **Regular expression** option and in the **URL** field, specify the regular expression corresponding to the page address.
   For example: `https://app.org/mainpage *`, where the character `*` replaces additional parameters in the query string.

7. Click **Save**.

Create permission

Permissions allow users to connect to resources.

To create a permission:

1. Open the resource profile and click **Create permission**.
2. Select one or several user connections and click **Next**.
3. For each user connection, select an account:
    - **Select account in PAM** — the permission is granted to an account added to Axidian Privilege.
    - **Use user account** — the permission is granted to an arbitrary account.
      The user needs to enter the login and password of the account on the resource.
4. Click **Select**.
5. Define the permission composition. If necessary, modify the preset parameters.

More about permission scope

1. Select who gets access:
   - **Users** — the permission is granted to one or several selected users.
   - **User group** — the permission is granted to one selected user group.
2. Select what to get access to:
   - **Resources** — the permission is granted to one or several selected resources.
   - **Resource groups** — the permission is granted to one selected resource group.
   - **Ad hoc connections** — the permission is granted to Ad hoc resources with the selected connection type, including resources not registered in PAM. One shared account is used for all connection types.

     > ⚠ **LICENSE REQUIRED**
     > A special license is required to work with Ad hoc resources.
     >
     > A special license is required to create a permission for PostgreSQL or MSSQL. Before creating the permission, add an account from the DBMS to PAM. You need to specify it in the permission.
3. Click **Next**.
4. Select the account under which the user will open a session on the resource:
   - **Select account in PAM** — the permission is granted to an account added to Axidian Privilege.
   - **Use user account** — the permission is granted to an arbitrary account.
     The user needs to enter the login and password of the account on the resource. In RDP and SSH sessions, it is possible to log in using the current Axidian Privilege user credentials.

6. (Optional) Configure access to credentials.

More about access settings

You can grant access to credentials only at the permission creation step.

The following settings are available:

- **Credentials** — the option defines actions with credentials:
  - **Allow view account credentials** — users can view passwords of the accounts from this permission.
  - **Allow change account credentials** — users can change passwords of the accounts from this permission.
- **Allow running pamsu in SSH sessions** — the setting defines access to PamSU when connecting via SSH Proxy:
  - **Managed by policies** — access to PamSU is determined by the policy of the resource for which the permission is granted.
  - **Allowed** — the user can use PamSU regardless of policy settings.
  - **Denied** — the user is not allowed to use PamSU regardless of policy settings.

7. (Optional) Fill in the **Description** field.

8. (Optional) Configure time restrictions.

More about time restrictions

You can set a schedule according to which users are allowed to open sessions or change credentials. For example, you can grant permission to work only on weekdays from 8:00 to 17:00.

The following settings are available:

- **Validity period** — the time period during which the permission is valid. For example, you can grant permission for one day or month.
  - **Begin** — set the date and time when the permission becomes active.
    If only **Begin** is set, the permission will become active on the selected date, and its validity period will be unlimited.
  - **End** — set the date and time when the permission becomes inactive.
    If only **End** is set, the permission will become active at the moment of creation, but will be suspended on the specified date.

    > **INFO**
    > If the **Begin** and **End** parameters are not set, the permission will be valid indefinitely.

- **Access schedule** — restrictions by days of the week taking into account the specified schedule.
  - **Allow access only on selected days** — select the days of the week when the permission will be active.
  - **Allow access only during selected hours** — select the time when the permission will be active.

    > **INFO**
    > Access by days of week is granted according to the management server time zone.

After the validity period expires, the permission will transition to the *Restricted/Inactive* state, and the user session will be terminated.

9. In the **Connection source** setting, select the network address from which sessions to the resource are allowed to be opened. If no network locations are added to PAM, the value is set to **No restrictions** — the permission can be used from any device on the network.

10. Check the data and click **Create permission**.

Add account

> ⓘ **INFORMATION**
> When adding an account with a configured SSH connection, you can set a password and an SSH key.
> When adding Windows OS and DBMS accounts, you can only set a password.

Add to PAM the local resource accounts that can be used to provide access to the resource.

To add an account to Axidian Privilege:

1. Go to the **Local accounts** tab and click **Add local account**.

2. Enter the account name and description and click **Next**.

3. At the password setup step, select one of the options:

   - **Generate random password** — the password is created automatically and synchronized with the resource or domain.
   - **Set password manually** — the password is set manually.
     Enter the password and confirm it.
     To change the account password not only in PAM but also on the resource or domain, enable the **Change password on resource** or **Change password on domain** option.
   - **Not set** — the account is created without a password, which can be set later during editing.

4. Click **Next**.

5. At the SSH key setup step, select one of the options:

   - **Generate new SSH key** — the key is created automatically and synchronized with the resource or domain. Choose a cryptographic algorithm to generate the key: **Ed25519** or **RSA**.

- **Set SSH key manually** — the key is set manually. Select the SSH key file and enter its password. RSA keys in OpenSSH and PEM formats are supported, as well as Ed25519 keys in OpenSSH format.

  How to generate an SSH key?

  To create an SSH key and write it to a file, use the PuTTYgen program or one of the commands:

  The RSA key in the OpenSSH format

  ```
  ssh-keygen -t rsa -b 4096 -f id_rsa_openssh -C "RSA OpenSSH key"
  ```

  The RSA key in the PEM format

  ```
  ssh-keygen -t rsa -b 4096 -f id_rsa_pem -C "RSA PEM key" -m PEM
  ```

  The Ed25519 key in the OpenSSH format

  ```
  ssh-keygen -t ed25519 -f id_ed25519_openssh -C "Ed25519 OpenSSH key"
  ```

  To change the account SSH key not only in PAM but also on the resource or domain, enable the **Change SSH key on resource** or **Change SSH key on domain** option.

- **Not set** — the account is created without an SSH key, which can be set later during editing.

6. Click **Next**.

7. Check the data and click **Save**

Check connection

The network availability of the resource and the correctness of the address, name, and password of the service account are checked.

To check the availability of a resource, go to its profile and click **Check connection**.
To check multiple resources, in the **Resources** section select the resources you need and click **Check connection**.

Synchronize

Synchronization is available only for resources with a configured service connection and allows you to get:

- the correct resource name, operating system or DBMS version
- local accounts and the security groups they belong to

To synchronize a resource, go to its profile and click **Sync**.

If new accounts are found during synchronization, they are added to PAM and marked with ⚠. To continue working with these accounts, provide PAM with their passwords or reset them to a random value.
For more details, see the Accounts section.

Block

Blocking allows you to suspend all permissions that use this resource. A blocked resource is marked with 🔒, and the permissions issued for this resource are marked with ⚠.

To block a resource, go to its profile and click **Block**.

Remove resource

Before deleting a resource, you must delete all accounts that were added from the resource being removed.

> ⚠ **CAUTION**
> When a resource is removed, all services associated with it are also removed. Removed services cannot be restored, you can only view them via extended search in the **Services** section.

To delete a resource:

1. Open the resource profile.
2. Click **Remove**.

To remove multiple resources, in the **Resources** section select the resources you need and click **Remove**.

Rollback resource

> ⚠ **CAUTION**
>
> When restoring a resource, the services associated with it are not restored. You will need to add the services again. You can view the information about removed services via extended search in the **Services** section.

To restore a resource:

1. In the **Resources** section, click **Extended search**.
2. Enter the resource name, DNS name, or IP address.
3. In the **State** field, select **Removed** and click **Search**.
4. Open the resource profile and click **Rollback**.
5. Enter the reset reason and click **Rollback**.

Setting Up a Service Connection for Resources

For resources based on Windows OS, *nix OS and MS SQL Server, MySQL, OracleDB and PostgreSQL, you can configure a service connection that will allow you to perform the following operations:

- Checking the connection to the resource
- Synchronization of accounts
- Account password verification
- Resetting account passwords
- Synchronization of account security groups
- Synchronization of data about the OS or DBMS version

The service connection can be configured both when adding a resource or after adding it to Axidian Privilege, this article will consider examples of setting up a service connection for resources already added to the system.

> ⓘ **NOTE**
> Checking passwords of local resource accounts under Linux OS can be performed without setting up a service connection to the resource.

Adding Accounts

Service operations are performed on behalf of a service account. Both a local resource account and a domain account can be assigned to the service role. Before setting up a service connection, you must add a local or domain account to the system.

- Adding a Resource
- Adding local accounts
- Adding a Domain
- Adding domain accounts

Selecting and Setting Up a Service Connection

- Open the resource profile and click ✎ to the right of the **Service connection** option
- Enable the **Use connector for service connection** option

Setting Up a Service Connection for Windows

- Select **Connector** - **Windows**
- If the connection address is different from the DNS name/IP address, specify it by selecting the appropriate checkbox.

Selecting a Service Account

- Enter the **Name of the local** or **domain account** in whole or in part
- Select an account
- Complete the service connection setup

Setting Up a Service Connection for *nix

- Select **Connector** - **SSH**
- Select the connection **template**
- If the connection address is different from the DNS name/IP address, specify it by selecting the appropriate checkbox.
- Enter the port number if it is not the default. The **Template** field contains templates of service operations for OS *nix. By default, templates of service operations for OS * nix are absent in Axidian Privilege. To create and add a template, please contact Technical Support.

Selecting a Service Account

- Enter the **Name of the local account** in whole or in part
- Select an account
- Complete the service connection setup

Setting Up a Service Connection for MS SQL Server DBMS

- Select **Microsoft SQL Server** Connector
- If the connection address is different from the DNS name/IP address, specify it by selecting the appropriate checkbox.

Selecting a Service Account

- Enter the **Name of the domain account** or **DBMS account**.
- Select an account.
- Complete the service connection setup. If an instance of MS SQL Server is part of an Active Directory domain, then both domain and DBMS accounts can be used as a service one. If an instance of MS SQL Server is not part of an Active Directory domain, then only DBMS accounts can be used as a service one.

Setting Up a Service Connection for OracleDB

- Select **Oracle Database** Connector
- Check the **Use another connection address** option and enter **Connection address**, port and SID of the DBMS or DB instance

Selecting a Service Account

- Enter the **Name of the DBMS account** in whole or in part
- Select an account
- Complete the service connection setup

Setting Up a Service Connection for PostgreSQL

- Select **PostgreSQL** Connector
- If the connection address is different from the DNS name/IP address, specify it by selecting the appropriate checkbox.
- Enter the port number if it is not the default.

Selecting a Service Account

- Enter the **Name of the DBMS account** in whole or in part
- Select an account
- Complete the service connection setup

Setting Up a Service Connection for MySQL

- Select **MySQL** Connector
- If the connection address is different from the DNS name/IP address, specify it by selecting the appropriate checkbox.

- Enter the port number if it is not the default.

Selecting a Service Account

- Enter the **Name of the DBMS account** in whole or in part.
- Select an account.
- Complete the service connection setup.

> ⚠ **CAUTION**
> To perform service operations Axidian Privilege uses the **mysql_native_password** authentication type, other authentication types are not supported.

Setting Up a MySQL Service Account

- Open the MySQL service account profile and click ✎ to the right of the **Name** option.
- Fill in the **Enter new host for account** field.

Setting Up a Service Connection for Cisco IOS

- Select **Cisco IOS** Connector.
- If you need to set password for privileged EXEC mode, put the appropriate checkbox and specify it.
- If the connection address is different from the DNS name/IP address, specify it by selecting the appropriate checkbox.
- Enter the **Port** if it is not the default.

Selecting a Service Account

- Enter the name of the local **Account name** fully or partially.
- Select an account.
- Complete the service connection.

Setting Up a Service Connection for Inspur BMC

- Select **Inspur BMC** Connector.
- If the connection address is different from the DNS name/IP address, specify it by selecting the appropriate checkbox.
- Enter the **Port** if it is not the default.

Selecting a Service Account

- Enter the name of the local **Account name** fully or partially.
- Select an account.
- Complete the service connection.

Checking Key Fingerprints of SSH Server

Fingerprints are designed to verify the identity of a resource at the moment of connection. Using fingerprints helps protect the company infrastructure against MITM (Man in the Middle) attacks.

Only SHA256 format is supported for fingerprints.

Supported algorithms:

- Ed25519
- ECDSA
- RSA

> ⓘ **INFO**
> This verification is always enabled and cannot be disabled.
>
> You can select the verification mode in the **Authentication of resources using SSH server keys** parameter in the **Configuration → System settings → SSH connection settings** section.

Prerequisites

To work with SSH server key fingerprints, you need **Resource Management** privileges.

Types of Adding Fingerprints

There are three types for adding SSH server key fingerprints:

- **Automatically add key fingerprints to PAM**

  In this mode, the fingerprint value is added into the PAM without the participation of the administrator. The fingerprint is saved in PAM only if it has not been set before. The fingerprint is saved at the moment of using a service connection (connection check, password check/rotation, SSH key check/rotation, synchronization) or at the moment of using a user connection (when a

user opens a session). The fingerprint is added just once, after which it is only checked, it is not rewritten. Fingerprint verification always occurs.

- **Add fingerprints into PAM manually only**

  In this mode, adding the fingerprint in the PAM is performed by the PAM administrator. The PAM administrator can manually specify the fingerprint value by selecting one of three available algorithms or obtain a ready-made fingerprint value from a remote host. Fingerprint verification always occurs. If the fingerprint is not added into PAM, the connection is not available.

- **Add fingerprints into PAM only manually and check only if they are added**

  In this mode, adding the fingerprint in the PAM is performed by the PAM administrator. The PAM administrator can manually specify the fingerprint value by selecting one of three available algorithms or obtain a ready-made fingerprint value from a remote host. The difference between this mode and the previous one is that if the fingerprint is not added into PAM, the fingerprint verification will not be performed. That is, if the fingerprint is not added into PAM, connection to the resource is still available.

  It is not recommended to select this type, as it reduces the level of information security.

Selecting Resources to Add Fingerprints

1. Open the **Resources** section.
2. Open **Extended Search**.
3. Select one of the values in the **SSH Key Fingerprint** field:
   - **Does not match in Service Connection or User Connection**
     To find resources where the fingerprint value in PAM and the fingerprint value on the resource do not match.
   - **Have not set in Service Connection or User Connection**
     To search for resources for which the fingerprint is not set in PAM.

Adding Fingerprints

There are three ways to add fingerprints:

- manually
- automatically

- by group operation

Adding Fingerprints Manually

Enter the fingerprint value yourself

To add a fingerprint for a service connection, follow these steps:

1. Open the profile of the desired resource.
2. Click to the right of the **Service Connection** field.
3. In the **SSH Key Fingerprint** section, select **Specify Manually**.
4. Select **Algorithm**. It is recommended to select Ed25519 because it is the safest option.
5. Enter a value in the **Fingerprint** field.
6. Click **Next**.
7. Select the desired service account.
8. Click **Save**.

To add a fingerprint for a user connection, follow these steps:

1. Open the profile of the desired resource.
2. Find the desired connection with the SSH type and click **Edit**.
3. In the **SSH Key Fingerprint** section, select **Specify Manually**.
4. Select **Algorithm**. It is recommended to select Ed25519 because it is the safest option.
5. Enter a value in the **Fingerprint** field.
6. Click **Save**.

Get the fingerprint value from a resource

To add a fingerprint for a service connection, follow these steps:

1. Open the profile of the desired resource.
2. Click to the right of the **Service Connection** field.
3. In the **SSH Key Fingerprint** section, select **Get from resource**.
4. Click **Use fingerprint value from resource**.
5. Click **Next**.
6. Select the desired service account.
7. Click **Save**.

To add a fingerprint for a custom user connection, follow these steps:

1. Open the profile of the desired resource.
2. Find the desired connection with the SSH type and click **Edit**.
3. In the **SSH Key Fingerprint** section, select **Get from resource**.
4. Click **Use fingerprint value from resource**.
5. Click **Save**.

Adding Fingerprints Automatically

> ⚠ **CAUTION**
> This method only works if the **Automatically add key fingerprints to PAM** mode is selected in the SSH connection settings.

Fingerprints for the service connection are set automatically at the time of using the service connection, for example:

- connection check
- password or SSH key check/rotation
- synchronization

Fingerprints for a user connection are also set automatically at the time the user connection is used, that is, when the user opens a session.

> ⓘ **INFO**
> In automatic mode, fingerprints are only added, but not overwritten.

Adding Fingerprints by a Group Operation

This operation allows you to set fingerprints for multiple resources at once. To do this, follow these steps:

1. Open the **Resources** section.
2. Select one or more resources that have a service or user connection of type SSH and no key fingerprint specified.
3. Click **Get fingerprint from resource** and confirm the action with the **Next** button.

> **INFO**
> With this operation, fingerprints are only added if the fingerprint value was not specified, i.e. existing fingerprints are not overwritten.

Additional Information on SSH Key Fingerprints

- The **SSH Key Fingerprint** attribute is associated with a connection, not a resource. Therefore, both types of connections (service and user) have their own attribute for the SSH key fingerprint. This is done for cases when there is more than one SSH server installed on the remote host. The presence or absence of a fingerprint on one connection does not affect the operation of the other. Therefore, fingerprint values for different connections of the same resource may contain different values.

- The SSH key fingerprint is verified before authentication on the resource, i.e. before the credentials are transferred to the resource.

- If the **Add fingerprints to PAM only manually** mode is selected in the SSH connection settings and the attribute for the fingerprint in PAM is left unset, then connection to the resource will be unavailable. An event about an unsuccessful connection will appear in the log, and a red warning will appear on the resource page describing the cause of the error, listing the mismatched fingerprints, and indicating the connection type.

- If the **Add fingerprints to PAM only manually** mode is selected in the SSH connection settings, the attribute for the fingerprint in PAM is filled in, and the resource does not have a key for the specified algorithm or does not have any keys, then connection to the resource will be unavailable. An event about an unsuccessful connection will appear in the log, and a red warning will appear on the resource page describing the cause of the error, listing the mismatched fingerprints, and indicating the connection type.

- To correct the fingerprint mismatch error, you need to re-obtain the SSH key fingerprint from the remote host, for more details, see Adding Fingerprints.

Services

This section is designed for managing Windows services in Axidian Privilege.

Windows services are applications that can start automatically when the operating system starts.

Add services to PAM that run under accounts managed by PAM. These services will automatically receive the current account password when it is changed via PAM.

<details>
<summary>What if I don't add them?</summary>

The old account password will remain in the service properties.

The running service will continue to run until the next restart of the resource host. And after that, the service will not start because the account password specified in the service properties does not match the actual account password.

To start the service, you will need to connect to the resource and update the password in the service properties manually.
</details>

Prerequisites

To work with services, you need **Resource Management** privileges, and you also need to set up a service connection for Windows on the resource where the services are located.

Service Adding

1. Open the **Services** section.
2. Click **Add**.
3. Select a resource in the window that opens. The resource must have the status **Available**. The service will have the same organization unit as the selected resource.

> ⚠ **CAUTION**
> The resource field of the service cannot be modified once the service is created.

4. Fill in the required field **Name** of the service.
   The name you enter must match the name specified in the `Service Name` field of the Services snap-in on the resource.

   > ⚠ **CAUTION**
   > Do not use the name that is specified in the `Display name` field of the Services snap-in on the resource.
   >
   > Do not attempt to create a second service on the same resource with the same name. Duplicates are not allowed.

5. Optionally enter a **Description** of the service.
   The description you enter will only be displayed in PAM, it will not change the description displayed in the service properties on the resource.

6. Enable or disable the **Restart service when service password is changed** option.

   > ⓘ **INFORMATION**
   > For services with delayed start, it is recommended to leave the option disabled. The new password will be delivered to the service when the service is restarted.

7. In the next wizard window, select an account.

8. In the next wizard window, check that the entered data is correct and click **Add**.

Likewise, you can add a service from the **Resources** and **Accounts** sections.

Service Editing

> ⚠ **CAUTION**
> The resource field of the service cannot be modified, it is set only via service adding wizard.

The following service fields are available for editing:

- **Service name**
- **Description**
- **Service restart**
- **Account**

To edit a service, click on the service page to the right of the desired setting.

> **INFORMATION**
> Please note that no two services with the same name can exist on a resource. Do not enter the name of a service that already exists on this resource.

Service Password Changing

Services do not have their own passwords, their passwords are the passwords of the associated accounts.

There are two ways to change account passwords:

- manually
- on schedule

Setting a Password for a Service

This function allows you to initiate delivery of the current password of the associated account to its service on the resource. This allows you to synchronize the password of the account with the password specified in the service properties immediately, without the necessity to wait for the scheduled password change.

> **INFORMATION**
> If the **Restart service when service password is changed** option is enabled for the service, then this service will restart after performing the password setting function.

1. Open the service page.
2. Click **Set a new password in the service**.

Service Restart

Service restart is an option that is specified when creating or editing a service using the **Restart service when service password is changed** checkbox. If this option is enabled, then the service will restart when the password is changed or set.

For a service to restart successfully, the service must be in the **Running** state.

> **INFORMATION**
> If the service on the resource is in a state other than **Running**, the service will not restart. This situation creates an event with the INFO type *Service restart: Not required*. This scenario is considered a successful completion of the service restart. Accordingly, it does not cause new errors and resets previous ones.

If the service was in the **Running** state, but the error *The service could not be restarted* occurred, the reason may be that the timeout for waiting for the required status has expired. For more details, see the section Errors of services fixing.

Services Search

The search allows you to display only those services that meet the specified criteria. There are two types of search:

- Quick search is a search bar. You can only search by one criterion. Text input.
- Extended search is a form with several fields. You can search by several criteria at once. Dropdown lists.

Quick Search

In the search bar you can search by the following fields:

- **Service name**
- **Resource name**
- **Service description**
- **Account name**

Extended Search

You can search by one or several criteria. If you select several criteria, services that meet all of the listed criteria will be displayed. You can search by the following fields:

- **Service name**
- **Account name**
- **Resource**
- **State**

- **Services with errors only** checkbox

Values of the **State** field:

- **Managed**
- **Removed**

Removed Services Search

1. Open the **Services** section and click **Extended search**.
2. Select **Removed** for the **State** field.
3. Click **Search**.

Errors of services fixing

Errors may occur:

- when setting a password in the service
- when restarting the service

An error when setting a password in the service may occur for various reasons, here are some examples:

- internet connection is lost
- the host on which the resource is installed is frozen
- service connection stopped working

Restarting the service fails if the timeout expires while waiting for the required status. For example:

- the service was stopping for too long
- the service restarted and immediately stopped

You can find out what status was expected and what was received in the events of this service. This information will help you understand how to fix the error.

To fix the error you will need to connect to the resource. It is not possible to fix the error from the Axidian Privilege management console.

Service-removing

> ⚠ **CAUTION**
>
> The service cannot be restored once deleted.
>
> You can create a new one with the same name on the same resource.

Removing from the list of services

1. Open the **Services** section.
2. Select one or more services.
3. Click **Remove**.

Removing from service page

1. Open the service page.
2. Click **Remove**.

Removed services will no longer appear in the **Services** section, but can be viewed using extended search.

Resource Groups

The section is intended for grouping resources in order to quickly and conveniently issue permissions to the entire group at once, as well as view sessions and events in the group as a whole.

Resource Groups Search

Enter the resource group name in the search bar and click .

Click **Extended search**, set one or more filters and click **Search**.

Resource group profile

The following is displayed for each resource group:

- **Resources** — list of resources in the group.
- **Permissions** — the list of permissions issued to the group.
- **Sessions** — the list of active, finished, and aborted sessions.
- **Events** — records of operations related to the resource group.

Add resources

To work with resource groups, you must create a group and add resources to it.

1. Click **Add** in the **Resource groups** section
2. Select Organizational unit
3. Enter a Resource group **Name**, **Description** and save your changes.
4. Also, you can check **Add resources with account** option which means the type of Resource group. This option affects the creation of a permission for the resource group:
    1. If you check this option, then when adding each individual resource, you will need to specify a privileged **Account** to access the **Resource**.
    2. If you do not check this option, then you will not need to specify an account for each individual resource. Also, when creating a **Permission** for such a group, only domain **Accounts** will be available for choosing, or you may use the user account option instead.

5. Open the created resource group, in the **Resources** tab, click the **Add** button and add the necessary resources to the group.

Create permission

Permissions allow users to connect to resources.

To create a permission:

1. Open the resource group profile and click **Create permission**.
2. If the group contains resources without an account, select an account in the window that opens:
    - **Select account in PAM** — the permission is granted to an account added to Axidian Privilege.
    - **Use user account** — the permission is granted to an arbitrary account.
      The user needs to enter the login and password of the account on the resource.
3. Click **Select**.
4. Define the permission composition. If necessary, modify the preset parameters.

More about permission scope

1. Select who gets access:
   - **Users** — the permission is granted to one or several selected users.
   - **User group** — the permission is granted to one selected user group.
2. Select what to get access to:
   - **Resources** — the permission is granted to one or several selected resources.
   - **Resource groups** — the permission is granted to one selected resource group.
   - **Ad hoc connections** — the permission is granted to Ad hoc resources with the selected connection type, including resources not registered in PAM. One shared account is used for all connection types.

     > ⚠ **LICENSE REQUIRED**
     > A special license is required to work with Ad hoc resources.
     >
     > A special license is required to create a permission for PostgreSQL or MSSQL. Before creating the permission, add an account from the DBMS to PAM. You need to specify it in the permission.
3. Click **Next**.
4. Select the account under which the user will open a session on the resource:
   - **Select account in PAM** — the permission is granted to an account added to Axidian Privilege.
   - **Use user account** — the permission is granted to an arbitrary account.
     The user needs to enter the login and password of the account on the resource. In RDP and SSH sessions, it is possible to log in using the current Axidian Privilege user credentials.
5. (Optional) Configure access to credentials.

More about access settings

You can grant access to credentials only at the permission creation step.

The following settings are available:

- **Credentials** — the option defines actions with credentials:
  - **Allow view account credentials** — users can view passwords of the accounts from this permission.
  - **Allow change account credentials** — users can change passwords of the accounts from this permission.
- **Allow running pamsu in SSH sessions** — the setting defines access to PamSU when connecting via SSH Proxy:
  - **Managed by policies** — access to PamSU is determined by the policy of the resource for which the permission is granted.
  - **Allowed** — the user can use PamSU regardless of policy settings.
  - **Denied** — the user is not allowed to use PamSU regardless of policy settings.

6. (Optional) Fill in the **Description** field.

7. (Optional) Configure time restrictions.

More about time restrictions

You can set a schedule according to which users are allowed to open sessions or change credentials. For example, you can grant permission to work only on weekdays from 8:00 to 17:00.

The following settings are available:

- **Validity period** — the time period during which the permission is valid. For example, you can grant permission for one day or month.
  - **Begin** — set the date and time when the permission becomes active.
    If only **Begin** is set, the permission will become active on the selected date, and its validity period will be unlimited.
  - **End** — set the date and time when the permission becomes inactive.
    If only **End** is set, the permission will become active at the moment of creation, but will be suspended on the specified date.

    > **INFO**
    > If the **Begin** and **End** parameters are not set, the permission will be valid indefinitely.

- **Access schedule** — restrictions by days of the week taking into account the specified schedule.
  - **Allow access only on selected days** — select the days of the week when the permission will be active.
  - **Allow access only during selected hours** — select the time when the permission will be active.

    > **INFO**
    > Access by days of week is granted according to the management server time zone.

After the validity period expires, the permission will transition to the *Restricted/Inactive* state, and the user session will be terminated.

8. In the **Connection source** setting, select the network address from which sessions to the resource are allowed to be opened. If no network locations are added to PAM, the value is set to **No restrictions** — the permission can be used from any device on the network.

9. Check the data and click **Create permission**.

Since the permission is created for the entire group, all resources of the group become available to the user at once. Changing the content of the resource group for the user within the permission will also change the composition of the resources available for connection.

Remove resource group

1. Open the resource group profile.
2. Click **Remove**.
3. Confirm the action by clicking **Remove**.

To remove multiple groups, in the **Resource groups** section, select the required groups and click **Remove**.

Accounts

The section allows you to manage local and domain accounts.

Adding an account

To add an account to PAM, please follow these steps:

1. Go to the **Accounts** section and click **Add**.
2. Select the location of the account (resource or domain).
3. Enter an account name (required) and description (optional).
4. Set a password. Maximum password length is 4096 characters.
5. Check the entered data and save the account.

Password and SSH Key

> **INFO**
> When adding an account for a resource with an SSH connection type, you can configure not only a password, but also an SSH key.
>
> When adding Windows OS and DBMS accounts, you must set a password. SSH key configuration is not available for these types.

Password Settings

1. Select one of the options:
   - **Generate** — the password is created automatically and synchronized with the resource or domain.
   - **Set password manually** — the password is set manually.
     Enter the password and confirm it.
     To change the account password not only in PAM, but also on the resource or domain, enable the option **Change password on resource** or **Change password on domain**.
   - **Not set** — the account is created without a password, which can be set later during editing.
2. Click **Next**.

SSH Key Settings

1. Select one of the options:

   - **Generate new SSH key** — the key is created automatically and synchronized with the resource or domain. Choose a cryptographic algorithm to generate the key: **Ed25519** or **RSA**.

   - **Set SSH key manually** — the key is set manually. Select the SSH key file and enter its password. RSA keys in OpenSSH and PEM formats are supported, as well as Ed25519 keys in OpenSSH format.
     To create an SSH key and write it to a file, use the PuTTYgen program or one of the commands:

     The RSA key in the OpenSSH format

     ```
     ssh-keygen -t rsa -b 4096 -f id_rsa_openssh -C "RSA OpenSSH key"
     ```

     The RSA key in the PEM format

     ```
     ssh-keygen -t rsa -b 4096 -f id_rsa_pem -C "RSA PEM key" -m PEM
     ```

     The Ed25519 key in the OpenSSH format

     ```
     ssh-keygen -t ed25519 -f id_ed25519_openssh -C "Ed25519 OpenSSH key"
     ```

   - **Not set** — the account is created without an SSH key, it can be set later during editing.

2. Click **Next**.

3. Check the data and click **Save**.

Account Search

Enter an account name in whole or in part in the search bar.

Click **Extended search**, set one or more filters and click **Search**.

Account Page

The profile displays the data specified while adding the account:

- **Name** — is the account name
- **Location** — the name of the resource or domain, where the account resides
- **Description** — this can be an arbitrary text
- **Policy** — is the set of rules applied to sessions started with the account
- **Password** (or a Key) **checking date** — is date and time when the account password or SSH key was last checked
- **Synchronization date** — date and time of the last data synchronization
- **Date added** — is the date and time when the account was added to Axidian Privilege
- **Last change** — is the date and time when the account was last edited
- **Last password change date** — is the date and time when the account password was last changed in Axidian Privilege database
- **Last password change date on resource/domain** — is the date and time when the account password was last changed in the Axidian Privilege database and at the resource
- **Last SSH key change date** — the date and time of the SSH key change in the Axidian Privilege database
- **Last SSH key change date on resource** — the date and time of the SSH key change in the Axidian Privilege database and on the resource

Permissions

All permissions where the account is used are displayed in the **Permissions** tab. The following data is displayed for every permission:

- **#** — permission number.
- **User** — the Active Directory user, the permission is given to
- **Organizational unit** — OU's name that the resource belongs to
- **Resources** — the resources that RDP, SSH or web session can be started with the account specified in the permission

Sessions

All active and finished sessions for the account are available at the **Sessions** tab. The following data is displayed for every session:

- **User** — the Active Directory user who initiated the session
- **Account** — the account used to start RDP, SSH or web session
- **Organizational unit** — OU's name that the resource belongs to

- **Resource** — the resource that RDP, SSH or web session is started at under the account
- **Connection address** — the actual address used when opening the session
- **Duration** — is the session duration
- **Connection** — remote connection type (RDP, SSH, user types)
- **Connected to Axidian Privilege** — date and time when the session was started
- **Finished** — date and time when the session was finished
- **State** — this displays the current status of the session (active or finished)

To view detailed information about the session, click on it. To display all sessions for a given account, click **Show all**.

Events

The account events are displayed in the **Events** tab. The following data is displayed for every event:

- **Creation time** — date and time when the event was created
- **Code** — is the event code
- **Event** — is the event description
- **Component** — is the Axidian Privilege component that generated the event.
- **Initiator** — the account that initiated the generation of the event

To view detailed information about the event, click on it. To display all events for a given account, click the **Show all**.

Security Groups

The **Security groups** tab displays a list of groups to which the account has been added.

> ⓘ **NOTE**
> Built-in security groups are not displayed for domain accounts.

Services

> ⚠ **CAUTION**
> For local accounts, this tab is only displayed if the associated resource has a Windows service connection configured.

All added services are displayed on the **Services** tab.

For each service the following information is displayed:

- **Service name** — the value specified when the service was created. It matches the value of the **Service name** field of the Services snap-in on the resource.
- **Account** — the service runs on behalf of this account.
- **Description** — custom text.

Also on this tab you can add a service for this account, to do this click **Add**.

Setting a Policy for an Account

1. Open the account's profile.
2. Click to add or change a policy.

Account Operations

Account Editing

The function allows you to change the Account **Name**, **Description** or **Policy**

- Click ✎ in the account profile to the right of the desired option

Account Confirmation

Resource or Domain Synchronization function allows you to get local or domain accounts in automatic mode, but confirmation is required to work with the received accounts, since Axidian Privilege does not get their passwords.

- Click **Make managed** in the account page

Create Permission

Permissions allow users to connect to resources.

To create a permission:

1. Open the account page and click **Create permission**.
2. Select one or several user connections and click **Select**.
3. Define the permission composition. If necessary, modify the preset parameters.

More about permission scope

1. Select who gets access:
   - **Users** — the permission is granted to one or several selected users.
   - **User group** — the permission is granted to one selected user group.
2. Select what to get access to:
   - **Resources** — the permission is granted to one or several selected resources.
   - **Resource groups** — the permission is granted to one selected resource group.
   - **Ad hoc connections** — the permission is granted to Ad hoc resources with the selected connection type, including resources not registered in PAM. One shared account is used for all connection types.

     > ⚠ **LICENSE REQUIRED**
     > A special license is required to work with Ad hoc resources.
     >
     > A special license is required to create a permission for PostgreSQL or MSSQL. Before creating the permission, add an account from the DBMS to PAM. You need to specify it in the permission.
3. Click **Next**.
4. Select the account under which the user will open a session on the resource:
   - **Select account in PAM** — the permission is granted to an account added to Axidian Privilege.
   - **Use user account** — the permission is granted to an arbitrary account.
     The user needs to enter the login and password of the account on the resource. In RDP and SSH sessions, it is possible to log in using the current Axidian Privilege user credentials.

4. (Optional) Configure access to credentials.

More about access settings

You can grant access to credentials only at the permission creation step.

The following settings are available:

- **Credentials** — the option defines actions with credentials:
  - **Allow view account credentials** — users can view passwords of the accounts from this permission.
  - **Allow change account credentials** — users can change passwords of the accounts from this permission.
- **Allow running pamsu in SSH sessions** — the setting defines access to PamSU when connecting via SSH Proxy:
  - **Managed by policies** — access to PamSU is determined by the policy of the resource for which the permission is granted.
  - **Allowed** — the user can use PamSU regardless of policy settings.
  - **Denied** — the user is not allowed to use PamSU regardless of policy settings.

5. (Optional) Fill in the **Description** field.

6. (Optional) Configure time restrictions.

More about time restrictions

You can set a schedule according to which users are allowed to open sessions or change credentials. For example, you can grant permission to work only on weekdays from 8:00 to 17:00.

The following settings are available:

- **Validity period** — the time period during which the permission is valid. For example, you can grant permission for one day or month.
  - **Begin** — set the date and time when the permission becomes active.
    If only **Begin** is set, the permission will become active on the selected date, and its validity period will be unlimited.
  - **End** — set the date and time when the permission becomes inactive.
    If only **End** is set, the permission will become active at the moment of creation, but will be suspended on the specified date.

    > **INFO**
    > If the **Begin** and **End** parameters are not set, the permission will be valid indefinitely.

- **Access schedule** — restrictions by days of the week taking into account the specified schedule.
  - **Allow access only on selected days** — select the days of the week when the permission will be active.
  - **Allow access only during selected hours** — select the time when the permission will be active.

    > **INFO**
    > Access by days of week is granted according to the management server time zone.

After the validity period expires, the permission will transition to the *Restricted/Inactive* state, and the user session will be terminated.

7. In the **Connection source** setting, select the network address from which sessions to the resource are allowed to be opened. If no network locations are added to PAM, the value is set to **No restrictions** — the permission can be used from any device on the network.

8. Check the data and click **Create permission**.

Password and SSH Key

If a service connection of the SSH type is configured for the resource from which the account was added, then it will be possible to generate or manually add not only a password, but also an SSH key. Also, for such accounts it is possible not to set a password: the setup wizard will display an additional item when setting a password — **Not set**. Below we will consider an example of confirming an *nix account. When confirming Windows OS accounts, DBMS or domain accounts, the **Not set** item will be missing, and there will be no page for generating or manually setting an SSH Key.

Password Settings

1. Select one of the options:
   - **Generate** — the password is created automatically and synchronized with the resource or domain.
   - **Set password manually** — the password is set manually.
     Enter the password and confirm it.
     To change the account password not only in PAM, but also on the resource or domain, enable the option **Change password on resource** or **Change password on domain**.
   - **Not set** — the account is created without a password, which can be set later during editing.
2. Click **Next**.

SSH Key Settings

1. Select one of the options:

   - **Generate new SSH key** — the key is created automatically and synchronized with the resource or domain. Choose a cryptographic algorithm to generate the key: **Ed25519** or **RSA**.

   - **Set SSH key manually** — the key is set manually. Select the SSH key file and enter its password. RSA keys in OpenSSH and PEM formats are supported, as well as Ed25519 keys in OpenSSH format.

To create an SSH key and write it to a file, use the PuTTYgen program or one of the commands:

The RSA key in the OpenSSH format

```
ssh-keygen -t rsa -b 4096 -f id_rsa_openssh -C "RSA OpenSSH key"
```

The RSA key in the PEM format

```
ssh-keygen -t rsa -b 4096 -f id_rsa_pem -C "RSA PEM key" -m PEM
```

The Ed25519 key in the OpenSSH format

```
ssh-keygen -t ed25519 -f id_ed25519_openssh -C "Ed25519 OpenSSH key"
```

- **Not set** — the account is created without an SSH key, it can be set later during editing.

2. Click **Next**.

3. Check the data and click **Save**.

Rollback Password or SSH Key

The function allows you to return the saved state of the password or SSH key for the account

- Click **Rollback** on your account profile.
- Select a restore point, provide a reason and complete password recovery

Verification of Password or SSH Key

Credential verification allows you to compare the password and SSH key for an account as stored in PAM and on the resource, as well as to identify unmanaged SSH keys.

> **NOTE**
> To verify domain or local accounts on Linux resources, no service connection needs to be configured.

To verify an account:

1. Go to **Accounts** section and open the account profile.
2. Click **Check**.

> **Possible verification outcomes**
>
> The following outcomes are possible when verifying an account:
>
> - The credentials in PAM and on the resource match.
>
> For the account, the current credentials are verified, as well as any passwords and SSH keys previously stored in the PAM database. If the values from the PAM database match the current account credentials on the resource, the password or SSH key in PAM is updated to the current value.
>
> - Unmanaged SSH keys have been found on the resource for this account. You can remove these keys from the account profile in PAM.
>
> - The credentials in PAM and on the resource do not match.
>
> No matching password or SSH key exists in the PAM database. This can occur if a user has changed the password or SSH key for the account on the resource without updating them in PAM. In this case, the user must update the credentials manually.

To verify credentials for multiple accounts, select the desired accounts in the **Accounts** section and click **Check**.

Password Change

> ⚠ **CAUTION**
> When changing an account password, pay attention to whether there are services associated with the account. When you change the account password, the passwords of the associated services will also change.

The function allows you to change the password to a random value or enter a new password manually.

- Click **Change password** in the Account profile
- Select one of the following options **Generate random password** or **Set password manually**

- Enter the password or continue by selecting **Generate random password**
- Fill in the **Password change reason** and click **Save**

Scheduled Password Change

Changing account passwords on a schedule is configured via policies.

1. Open the **Policies** section.
2. Select the policy that controls the account you want to set scheduled password change for.
3. Open the **Accounts** section.
4. Enable the **Periodically change the account password and SSH key** option.
5. Specify the number of days in the **Password and SSH key change period** field. Automatic password or SSH key change will be performed once every specified number of days.

SSH Key Change

The function allows you to change the key to a random value or upload the new key manually.

- Click **Change SSH key** in the account profile
- Select one of the following options: **Generate new SSH key** or **Set SSH key manually**
- Select the SSH key file and enter its password or continue by selecting **Generate new SSH key**
- Fill in the **SSH key change reason** and click **Save**

Removing Unmanaged SSH Keys

If account has an error "Unmanaged SSH keys detected", the **Remove unmanaged SSH keys** button becomes available. Once clicked, only the unmanaged SSH Axidian Privilege keys will be removed.

Keys that were created or added to Axidian Privilege remain unchanged.

Synchronization

The function allows you to get the list of groups the account belongs to.

- Click **Sync** in the account profile

Blocking

The function allows you to suspend all permissions in which the account is used.

- Click **Block** in the account profile

> ⓘ **NOTE**
> The account will be marked with the symbol. All permissions in which the account is a member will be marked with the symbol.

Ignoring

The function allows you to put an account in a state in which it is stored without a password and cannot be used in permissions.

- Click **Ignore** in the account profile

> ⚠ **CAUTION**
> The account will be marked with the symbol. All permissions with this account will become inactive.

Removing an Account

- Click **Remove** on your account profile

> ⓘ **INFO**
> When removed, the account will disappear from all services associated with it. There will be a dash in the Account field in the service profile. The services will not be removed.

Rolling Back an Account

- Click **Extended search** in the **Accounts** section
- Enter your **Account name** in whole or in part
- Set the **State** field to Removed
- Select the resource or domain from which the account was added

- Open your account profile and click **Rollback**
- Select a password recovery point for your account
- Enter the reason for the recovery and click **Rollback**

> **INFO**
> When you restore an account, any previously existing associations between the account and services are not restored.

Bulk Operations for Accounts

Confirmation

- Switch to the **Accounts** section, check one or more accounts with **pending** state and click **Make managed**

> ⚠ **CAUTION**
> With bulk confirmation, random passwords are always generated for accounts, the generation of SSH keys is not performed.

Password or SSH Key Checking

- Switch to the **Accounts** section, check one or more accounts and click **Check**

Blocking

- Switch to the **Accounts** section, check one or more accounts and click **Block**

Ignoring

- Switch to the **Accounts** section, check one or more accounts and click **Ignore**

Axidian Privilege will not keep secrets of such account, also it cannot be selected when creating permissions.

Changing Policy

- Switch to the **Accounts** section, check one or more accounts and click **Set policy**
- Select a session policy

Removing

- Switch to the **Accounts** section, check one or more accounts and click **Remove**

Domains

The section is intended to work with Active Directory domains.

Domain Search

Enter the domain name or DNS name in whole or in part in the search bar.

Click **Extended search**, set one or more filters and click **Search**.

Domain Page

The page displays the data of the domain specified while adding it:

- **Domain name**
- **DNS name**
- **Service account** — domain account on behalf of which service operations will be performed
- **Policy** — is the set of rules applied to domain accounts added to Axidian Privilege
- **Resources synchronization date** — date and time of the last resources sync
- **Accounts synchronization date** — date and time of the last accounts sync

Domain Accounts

All domain accounts added are displayed in the **Domain accounts** tab.

Resource Containers

All containers selected for synchronization of domain computers are displayed in the **Resource containers** tab.

Privileged Groups

All security groups selected for synchronization of domain accounts are displayed in the **Privileged groups** tab.

Events

All events on the domain are displayed on the **Events** tab, the last 5 events are displayed here. To view detailed information about an event, you must expand it. To display all events for a given domain, click the **Show all**.

Setting a Policy for a Domain

1. Open the domain's profile.
2. Click ✎ to add or change a policy.

Adding a Domain

To manage domain access accounts and get domain computers, you must add the domain to Axidian Privilege.

- Click **Add** in the **Domains** section
- Enter **NetBIOS name** and **DNS name**
- Save changes

Configuring Service Connection for Domains

For Active Directory domains, you can configure a service connection that will allow you to perform the following operations:

- Domain connection check
- Synchronization of domain accounts
- Domain account password check
- Resetting password of domain accounts
- Synchronization of security groups of domain accounts
- Synchronization of domain computers

Adding Accounts

Service operations are performed on behalf of a service account. A domain account can be assigned to the service role. Before setting up a service connection, you must add a domain account to the system.

- Adding a Domain
- Adding domain accounts

Setting up a Service Connection

- Open your domain profile and click ✎ to the right of the **Service account** option
- Enter your **Account name** in whole or in part
- Select an account and complete the service connection setup

Domain Operations

Domain Editing

This function allows you to change **NetBIOS name**, **DNS name**, **Service account** or **Policy**.

- Click ✎ to the right of the required parameter in the domain profile

Adding an Account

The function allows adding domain resource accounts to Axidian Privilege that can be used to provide access to resources.

- Click **Add account** in the domain profile
- Enter an **Account Name** and **Description**

Password Setting

- Select **Not set**, **Generate random password** or **Set password manually**
- Enter your password or continue by selecting **Generate random password**

Domain Connection Check

The function allows you to check the network availability of the domain, the correctness of the NetBIOS name, address, name and password of the service account.

- Click **Check connection** in the domain profile

Import Resources

The function allows you to automatically add domain computers to Axidian Privilege.

Selection of Containers

- Switch to the **Resource containers** tab in your domain profile and click **Add**
- Enter the container name in whole or in part and select one or more containers

- Complete the container selection

Import

- Click **Import resources** in the domain profile.

Synchronizing Accounts

The function allows you to automatically add to Axidian Privilege domain accounts that are members of the selected Active Directory security groups.

Selecting Groups of Privileged Accounts

- Switch to the **Privileged groups** tab and click **Add**
- Enter the group name in whole or in part and select one or more groups
- Complete the group selection.

Synchronization

- Click **Sync accounts** in the domain profile

Remove / Rollback a Domain

Removing a Domain

- Click **Remove** on the domain profile

> ⓘ **NOTE**
> Before removing a domain, you must remove all accounts that were added from the removed domain.

Rolling Back Domains

- Click **Extended search** in the **Domains** section
- Enter the **NetBIOS name** or **DNS name** in whole or in part
- Select **Removed** for the **State** field and click **Search**
- Open the domain profile and click **Rollback**

- Enter the reason for the recovery and click **Rollback**

Bulk Operations for Domains

Checking the Connection to the Domains

- Switch to the **Domains** section, check one or more Domains and click **Check connection**.

Deleting Domains

- Switch to the **Domains** section, check one or more Domains and click **Remove**.

> **NOTE**
> Before deleting domains, you must delete all accounts that were added from the deleted domains.

Structure

This section is intended for creating Organizational Units (OU) of an organization. When creating OU, you can delimit the access of Axidian Privilege administrators to individual resources.

> ⓘ **NOTE**
> Axidian Privilege OUs are not related to Active Directory OUs/containers in any way.

Organizational Unit Types

An OU can be global (Root OU) or local. Also, Axidian Privilege objects can be global and local by belonging to an OU.

Immediately after installing Axidian Privilege, a Root OU already exists in the system. It owns all objects whose OU is not explicitly specified. Accordingly, after upgrading the Axidian Privilege version from version 2.6, all previously existing objects become global.

You can bind the Axidian Privilege administrator to the OU in the Role settings. A user can be in roles from the same OU. You cannot add a user to a role again by specifying other OUs.

The OU is specified when adding a Resource, Domain, or Resource Group.

The system recognizes whether a given object is local to a given OU through the objects' links to resources and domains. If an object is associated with a Resource and an Account, the OU is determined by the Resource.

Local Administrator

The local administrator is restricted in access and can only work with a set of objects that belong to his OU. The following objects are restricted — Accounts and Resources.

Exceptions:

- can read global domain accounts
- can read global policies
- can read Domains, but not their groups and containers

All objects created by the Local administrator automatically belong to his OU.

> ⓘ **NOTE**
> Only the Global Administrator can choose OU when creating objects.

Not available to the Local administrator:

- Objects related to other OUs
- Sections Structure, Roles, Notifications

The Management sections are read-only:

- Policies and their settings
- User connections and Service connections
- Configuration settings

Other sections are not available.

A local administrator cannot create permissions with view credentials for domain Accounts, including Application permissions.

> ⚠ **CAUTION**
> Operations with Organizational Units can be enabled or disabled in the Management Console configuration file.

Organizational Unit Enabling

Working with Organizational Units is enabled in the Management Console configuration file.

Path to configuration file:

- Windows: `C:\inetpub\wwwroot\mc\assets\config\`
- Linux: `/etc/axidian/axidian-pam/mc/`

To enable working with organizational units in PAM, set the value `true` for the `enableOrganizationalUnits` parameter in the `view` section:

```
"view": {
    "enableOrganizationalUnits": true
  }
```

Permissions

The section is intended to search, issue, revoke and suspend permissions.

Search

Enter a user, account, resource, or description in the search string and click 🔍.

Click **Extended search**, set one or more filters and click **Search**.

Create

> ⚠ **CAUTION**
> To be able to manage permissions you need the *Permissions management* privileges.

1. In the **Permissions** section, click **Create**.
2. (Optional) Select an organizational unit and click **Select**.
3. Define the permission scope.

More about permission scope

1. Select who gets access:
   - **Users** — the permission is granted to one or several selected users.
   - **User group** — the permission is granted to one selected user group.
2. Select what to get access to:
   - **Resources** — the permission is granted to one or several selected resources.
   - **Resource groups** — the permission is granted to one selected resource group.
   - **Ad hoc connections** — the permission is granted to Ad hoc resources with the selected connection type, including resources not registered in PAM. One shared account is used for all connection types.

     > ⚠ **LICENSE REQUIRED**
     > A special license is required to work with Ad hoc resources.
     >
     > A special license is required to create a permission for PostgreSQL or MSSQL. Before creating the permission, add an account from the DBMS to PAM. You need to specify it in the permission.
3. Click **Next**.
4. Select the account under which the user will open a session on the resource:
   - **Select account in PAM** — the permission is granted to an account added to Axidian Privilege.
   - **Use user account** — the permission is granted to an arbitrary account.
     The user needs to enter the login and password of the account on the resource. In RDP and SSH sessions, it is possible to log in using the current Axidian Privilege user credentials.

4. (Optional) Configure access to credentials.

More about access settings

You can grant access to credentials only at the permission creation step.

The following settings are available:

- **Credentials** — the option defines actions with credentials:
  - **Allow view account credentials** — users can view passwords of the accounts from this permission.
  - **Allow change account credentials** — users can change passwords of the accounts from this permission.
- **Allow running pamsu in SSH sessions** — the setting defines access to PamSU when connecting via SSH Proxy:
  - **Managed by policies** — access to PamSU is determined by the policy of the resource for which the permission is granted.
  - **Allowed** — the user can use PamSU regardless of policy settings.
  - **Denied** — the user is not allowed to use PamSU regardless of policy settings.

5. (Optional) Fill in the **Description** field.

6. (Optional) Configure time restrictions.

More about time restrictions

You can set a schedule according to which users are allowed to open sessions or change credentials. For example, you can grant permission to work only on weekdays from 8:00 to 17:00.

The following settings are available:

- **Validity period** — the time period during which the permission is valid. For example, you can grant permission for one day or month.
  - **Begin** — set the date and time when the permission becomes active.
    If only **Begin** is set, the permission will become active on the selected date, and its validity period will be unlimited.
  - **End** — set the date and time when the permission becomes inactive.
    If only **End** is set, the permission will become active at the moment of creation, but will be suspended on the specified date.

    > **INFO**
    > If the **Begin** and **End** parameters are not set, the permission will be valid indefinitely.

- **Access schedule** — restrictions by days of the week taking into account the specified schedule.
  - **Allow access only on selected days** — select the days of the week when the permission will be active.
  - **Allow access only during selected hours** — select the time when the permission will be active.

    > **INFO**
    > Access by days of week is granted according to the management server time zone.

After the validity period expires, the permission will transition to the *Restricted/Inactive* state, and the user session will be terminated.

7. In the **Connection source** setting, select the network address from which sessions to the resource are allowed to be opened. If no network locations are added to PAM, the value is set to **No restrictions** — the permission can be used from any device on the network.

8. Check the data and click **Create permission**.

Create copy

You can create a copy of any permission, while the original permission can be revoked or suspended. When copying, a creation window opens with the parameters of the original permission set. This selection can be edited: change the resource, remove users, or set restrictions.

> ⓘ **INFO**
> If a user, application, resource, or account from the original permission is unavailable, they will not be added to the new permission.

To copy a permission:

1. Go to the profile of the desired permission and click **Create copy**.
2. Select an action for the original permission:
   - **Keep** — the original permission will remain active.
   - **Suspend** — the original permission will become unavailable for use and will transition to the *Suspended* status.
   - **Revoke** — the original permission will be revoked and will transition to the *Revoked* status.
3. Make changes to the original permission.
4. Check the data and click **Create permission**.

Revoke

Click **Revoke** and revoke a permission that is no longer needed. Users lose access immediately, not after the session ends.

To revoke multiple permissions, in the **Permissions** section select the desired permissions and click **Revoke**.

> ⚠ **CAUTION**
> Revoked permissions cannot be restored.
>
> If you need to temporarily prohibit the use of a permission, suspend it.

Revoked permissions stop displaying in the **Permissions** section, but they can be found using search:

1. Go to the **Permissions** section.
2. Open **Extended search**.
3. Select the *Revoked* status and click **Search**.

Suspend

Click **Suspend** in the permission profile to temporarily prohibit using the permission. Users lose access immediately, not after the session ends.

To suspend multiple permissions, in the **Permissions** section select the required permissions and click **Suspend**.

Reactivate

Click Reactivate in the permission profile to activate a suspended permission. The permission will change to the *Valid* state.

To activate multiple permissions, in the **Permissions** section select the required permissions and click **Reactivate**.

Generate report

A report is an export of permissions based on specified filters. For example, you can generate a report on revoked permissions or export a list of all permissions for a specific user. By default, the report includes up to 50,000 records, but this limit can be increased.

To generate a report:

1. Go to the **Permissions** section.
2. (Optional) Enter a query in the search bar or apply extended search filters.

3. Click **Generate report**.
4. In the dialog that appears, select the CSV or XLSX format.

The report with the specified filters is generated in the background. Download the report in the Report history section.

Action Requests

The section is designed to work with requests for actions. This mechanism allows you to configure additional confirmation by a second person (Axidian Privilege Administrator) to connect to the target resource.

> ⚠ **CAUTION**
> The **SESSION REQUESTS MANAGEMENT** and **CREDENTIALS VIEWING REQUESTS MANAGEMENT** (SessionRequest.Confirm, CredentialsViewingRequest.Confirm) claims are required.

> **TIP**
> The session request timeout is configured in the Sessions policy section. The Password and SSH key viewing request timeout is configured in the Account policy section.

Action requests always display the historical values of the **User**, **Resource** and **Account** at the time of the request creation. Historical names in Requests and Sessions may be different because when opening a session, the current value of the **User**, **Resource**, **Account** is saved.

Search Action Requests

> **NOTE**
> Searching for **Action requests** by User finds Requests from users that request action.
>
> There is no search by the Administrator who confirms the **Action requests**.

Quick Search

Enter the **User**, **Account** or **Resource** in whole or in part in the search bar.

Extended Search

Click **Extended search** and enter one or more criteria, **Request number**, **creation time interval**, **Account**, **Resource**, **Resource group**, **Organizational unit**, **User**.

Select request state:

- Pending
- Confirmed
- Rejected
- Expired
- Canceled by user
- Used
- Not used

Select request type:

- Session
- Credentials

Action Request Functions

Action Request Confirmation

This feature allows the Axidian Privilege Administrator to confirm the User's request.

- Click **Confirm** in the request page, or by selecting the pending request's check box.

Action Request Rejection

This feature allows the Axidian Privilege Administrator to reject a User's request.

- Click **Reject** in the request page, or by selecting the pending requests check box.

Request Page

The request page displays the following data:

- **User** — the user of the Active Directory who created the request to open a session.
- **Account** — an account that is used to open an RDP, SSH or web session on the resources specified in the permission.
- **Resource** — resources on which RDP, SSH or a web session can be opened on behalf of the account specified in the permission.

- **User's IP** — The IP address from which the user was connecting to PAM Gateway, SSH proxy or RDP Proxy.
- **Connection type**
- **Reason** is arbitrary text entered by the user when creating a request.
- **State** — the current status of the request (Pending, Confirmed, Rejected, Expired, Canceled by user, Used, Not used).
- **Creation time** — date and time when the request was created by the user.

Active Sessions

The section is intended for automatic filtering and display of active Axidian Privilege sessions.

The following data is displayed for each session:

- **User** — Active Directory user who initiated the session
- **Account** — an account that is used to open an RDP, SSH or web session
- **Resource** — a resource on which an RDP, SSH or web session was opened on behalf of the account
- **Connection address** — the actual address used when opening a session.
- **Duration** — the duration of the session
- **Connection** — remote connection type (RDP, SSH, user types)
- **Connected to PAM** — date and time of session opening

If there are active sessions on the main sidebar to the right of the section title there will be an icon with number of active sessions.

All Sessions

This section is designed for searching and viewing active, completed, and aborted sessions. By default, the page displays 15 sessions, but this number can be changed in the configuration file:

- Windows: `C:\inetpub\wwwroot\mc\assets\config\config.prod.json`
- Linux: `/etc/axidian/axidian-privilege/mc/config.prod.json`

> **TABLE CUSTOMIZATION**
> You can customize the table in this section. To do so, click in the top-right corner and select the columns you want to show or hide.

Session search

Enter a username, resource, account, connection type, or reason in the search bar and click .

Click **Extended search**, set one or more filters and click **Search**.

Generate report

A report is a session export based on the specified filters. For example, you can export a user's sessions on a resource for a specified time period. By default, the report includes up to 50,000 records, but this limit can be increased.

To generate a report:

1. Go to the **All Sessions** section.
2. (Optional) Enter a query in the search bar or apply extended search filters.
3. Click **Generate report**.
4. In the dialog that appears, select the CSV or XLSX format.

The report is generated in the background. Download the report in the Report history section.

Abort a session

To forcibly abort a session, go to the active session profile and click **Abort**.

Refresh a session

To refresh the text log, screenshots, and files transferred to the server, go to the active session profile and click **Refresh**.

View and download session logs

The following logging types are available for sessions opened through PAM:

- Video — for RDP and SSH sessions opened through Axidian Privilege Gateway, and for client application sessions.
- Text log — for RDP and SSH sessions opened through Axidian Privilege Gateway and Axidian Privilege SSH Proxy.

  > ⓘ **INFO**
  > Text logging in RDP sessions is supported by the Axidian Privilege Agent component, the agent registers text input, intercepts the names of active windows and launched processes. Text logging in SSH sessions does not require the installation of separate components. Full input/output is logged in SSH sessions.

- Screenshots — for RDP and SSH sessions opened through Axidian Privilege Gateway, and for client application sessions.
- Files transferred to the server — for RDP sessions. Files transferred from mapped drives to the resource are intercepted and copied.

To download session logs, expand the **Videos**, **Text Log**, or **Screenshots** section and click **Download** / **Download all**.

To download transferred files, expand the **Transferred to the server files** section and follow the link to download the files.

Events

This section displays the history of events that occurred in Axidian Privilege.
A complete list of events is provided in the Reference section.

Event Search

> **INFO**
> If the PAM data is stored in a PostgreSQL database, the search by initiator name or component name is case-sensitive.

Enter an event code, component or initiator/user name in the search bar and click .

Click **Extended search**, set one or more filters and click **Search**.

Generate report

The report is an event upload based on the specified filters. For example, you can upload events that occurred on a resource during a selected time period.

To generate a report:

1. Go to the **Events** section.
2. (Optional) Enter a query in the search bar or apply extended search filters.
3. Click **Generate report**.
4. In the dialog that appears, select the CSV, XLSX, or PDF format.

The report with the specified filters is generated in the background. Download the report in the Report history section.

Reports history

> **PRIVILEGES REQUIRED**
> To work in this section, the administrator needs the claims *Read permissions*, *Read sessions*, or *Read events*.

The section contains reports on permissions, sessions, and events. Each report displays a status:

- ✅ — generated and ready for download.
- 🔄 — generating.
- ❌ — not generated, an error occurred.
  Increase the server response timeout or generate a smaller report.
- ⚠️ — generated and ready for download, but not all records were exported.
  By default, 50,000 records are exported. The limit can be increased in the configuration file.

Generate and download a report

1. In the administrator console, go to the **Permissions**, **All sessions**, or **Events** section.
2. (Optional) Enter a query in the search bar or apply advanced search filters.
3. Click **Generate report**.
4. In the dialog that appears, select the report format.
   The report with the specified filters is generated in the background.
5. Go to the **Report history** section and click **Download** next to the generated report.

Configuration settings

The following settings can be changed in the configuration file:

- the number of records exported to the report
- the server response timeout if an error occurs during report generation

> **NOTE**
> By default, 50,000 records are exported to each report.
> Maximum report size: 1,000,000 records.

Windows

To change the export limit or the server response timeout:

1. Open the Core component configuration file located at `C:\inetpub\wwwroot\idp\appsettings.json`.
2. In the `MaxTotalRecords` section, specify the number of records for each report type:
   - `Events` — events report
   - `Permissions` — permissions report
   - `Sessions` — sessions report
3. For the `CommandTimeout` parameter, specify the server response timeout.
   Change this parameter only if an error occurs during report generation.

   Configuration file example

   ```
   "Performance": {
     "SessionArtifactsRotation": {
       "MaxDegreeOfParallelism": 4
     },
     "Reports": {
       "CommandTimeout": "00:00:30",  // Server response timeout
       "MaxTotalRecords": {
         "Events": 50000,             // Number of records in the events report
         "Permissions": 50000,        // Number of records in the permissions report
         "Sessions": 50000            // Number of records in the sessions report
       }
     }
   ```

4. Save the file.

After editing the configuration file, restart the IIS server:

1. Run PowerShell as administrator.
2. Launch IIS Manager:

   ```
   start inetmgr
   ```

3. In the left panel, click the required server.

4. In the right panel, click **Restart**.

Linux

To change the export limit or the server response timeout:

1. Open the Core component configuration file located at `/etc/axidian/axidian-privilege/core/appsettings.json`.
2. In the `MaxTotalRecords` section, specify the number of records for each report type:
   - `Events` — events report
   - `Permissions` — permissions report
   - `Sessions` — sessions report
3. For the `CommandTimeout` parameter, specify the server response timeout.
   Change this parameter only if an error occurs during report generation.

   Configuration file example

```
"Performance": {
  "SessionArtifactsRotation": {
    "MaxDegreeOfParallelism": 4
  },
  "Reports": {
     "CommandTimeout": "00:00:30",  // Specify the server response timeout
    "MaxTotalRecords": {
       "Events": 50000,             // Specify the number of records in the events report
       "Permissions": 50000,        // Specify the number of records in the permissions report
       "Sessions": 50000            // Specify the number of records in the sessions report
    }
  }
```

4. Save the file.
5. Navigate to the PAM scripts folder and restart the component:

```
cd /etc/axidian/axidian-privilege/scripts/
```

```
bash restart-pam.sh core
```

Notifications

In this section, mail notifications for the specified log events are configured.

Presetting

At first, specify the mail settings: go to the **SMTP server** section, enter the mail server address, port, authorization credentials and save the changes.

To test the settings, click the **Send test email** button.

Configuring Notifications

To set up notifications, follow these steps:

1. Create recipient groups — lists of addresses for sending notifications about the registration of selected events in the log.
    1. Open the **Distribution groups** section, click the **Add** button, enter a name and description for the recipient group, click **Save**
    2. Go to the created distribution group, click the **Add email** button, enter the employee's email address.
2. In the **Notifications** section, add the events for which you want to send notifications and the corresponding distribution groups.

Removing Distribution Groups or Notifications

To remove items, go to the appropriate section, select the required items and click the **Remove** button.

Configuration

This section contains parameters for configuring PAM.

System Settings

In this section global system settings are specified. Fine-tuning is performed in the Policies section.

Scheduled jobs

Option	Description
Account checking start time	At this time Axidian Privilege will start checking all active accounts in the *Managed* state
Resources and accounts syncing start time	At this time Axidian Privilege will start resource information syncing and accounts syncing for resources and domains
Account password reset start time	At this time Axidian Privilege will generate new passwords for accounts
Service connection checking start time	At this time Axidian Privilege will start checking service connection to resources and domains
Session artifact rotation start time	At this time Axidian Privilege will start session artifact rotation
Synchronization interval for user groups from the directory	The PAM system updates the list of members of user groups from the directory at a specified interval

Video

Option	Description
Video recording codec options	The libx264 codec is used by default with the following settings: libx264 -preset medium -tune zerolatency.
Video streaming codec options	The libx264 codec is used by default with the following settings: libx264 -g 10 -tune zerolatency.

Option	Description
The duration of the recorded video segment, sec.	You can set the duration at which the video will be saved as an independent segment, the default is 3600 seconds (1 hour).

Sessions

Option	Description
Gateway connection timeout, sec.	Time after which connection will be closed if gateway isn't responding. Set the value to 0 if you do not want the connection to be interrupted.
Time to connect, min.	Close session on the Gateway if a user did not connect to the resource.
Legal notice	That text will be shown to user before session. Leave it empty if you don't need it.
Maximum amount of sessions per user	Limiting the number of concurrent open sessions per user, 0 is the default with no limit.
Notify user about session termination	The user will be notified before the session ends.
Notifications threshold	Notification will be shown for the specified time before the session expires.
Notification interval	Interval between notifications about expiring session.

Gateway connections

The setting defines the main parameters of the Gateway component that are used by default for all connections to the RDS Access Server. To route a specific connection to another proxy server instance, override the Gateway parameters through policies.

Option	Description
RDCB address	IP address or DNS name of the server with the Remote Desktop Connection Broker role.
RDCB collection name	Name of the Remote Desktop Connection Broker collection. The collection is used for load balancing when connecting through Axidian Privilege Gateway.

Option	Description
Use RDGW	Allows the RDP client to connect to Axidian Privilege Gateway through the Remote Desktop Gateway.
RDGW address	IP address or DNS name of the Remote Desktop Gateway server.

RDP file parameters	Parameters that are automatically added when the RDP file is generated in the User Console. The specified parameters are used when connecting to the RDS Access Server.
	`# Example`
	`screen mode id:i:2`
	`authentication level:i:2`
	Limitations
	The following parameters cannot be overridden through the configuration settings:
	• `full address`
	• `redirectprinters`
	• `redirectcomports`
	• `redirectsmartcards`
	• `redirectposdevices`
	• `drivestoredirect`
	• `gatewayhostname`
	• `gatewayusagemethod`
	• `gatewayprofileusagemethod`
	• `loadbalanceinfo`
	• `shell working directory`
	• `alternate shell`
	• `remoteapplicationprogram`
	• `remoteapplicationcmdline`

RDP Proxy

The setting defines the main parameters of the RDP Proxy component that are used by default for all connections to this proxy server. To route a specific connection to another proxy server instance, override the RDP Proxy parameters through policies.

Option	Description
RDP Proxy Address	IP address or DNS name of the server with the RDP Proxy. If the port is not specified, the default value (3390) is used.

RDP file parameters	Parameters that are added when the RDP file is generated in the User Console. The specified parameters are used when connecting to the RDP Proxy server.
	`# Example`
	`screen mode id:i:2`
	`authentication level:i:2`
	Limitations
	The following parameters cannot be overridden through the configuration settings:
	• `full address`
	• `redirectprinters`
	• `redirectcomports`
	• `redirectsmartcards`
	• `redirectposdevices`
	• `drivestoredirect`
	• `gatewayhostname`
	• `gatewayusagemethod`
	• `gatewayprofileusagemethod`
	• `loadbalanceinfo`
	• `shell working directory`
	• `alternate shell`
	• `remoteapplicationprogram`
	• `remoteapplicationcmdline`

Web Proxy

The setting defines the main address of the Web Proxy component that is used by default for all connections to this proxy server. To route a specific connection to another proxy server instance, override the Web Proxy address through policies.

Option	Description
Web Proxy Address	IP address or DNS name of the server with the Web Proxy. If the port is not specified, the default value (5444) is used.

PostgreSQL Proxy

The setting defines the main address of the PostgreSQL Proxy component that is used by default for all connections to this proxy server. To route a specific connection to another proxy server instance, override the PostgreSQL Proxy address through policies.

Option	Description
PostgreSQL Proxy Address	IP address or DNS name of the server with the PostgreSQL Proxy. If the port is not specified, the default value (5433) is used.

MSSQL Proxy

The setting defines the main address of the MSSQL Proxy component that is used by default for all connections to this proxy server. To route a specific connection to another proxy server instance, override the MSSQL Proxy address through policies.

Option	Description
MSSQL Proxy Address	IP address or DNS name of the server with the MSSQL Proxy. If the port is not specified, the default value (1432) is used.

SSH connection settings

The setting defines the main parameters of the SSH Proxy component that are used by default for all connections to this proxy server. To route a specific connection to another proxy server instance, override the SSH Proxy parameters through policies.

Option	Description
SSH Proxy address	IP address or DNS name of the server with the SSH Proxy. If the port is not specified, the default value (2222) is used.
Authentication of resources using SSH server keys	The mode for adding SSH server key fingerprints. For more information about working with fingerprints, see the Checking SSH server key fingerprints section.

Web terminal

Activate the Web Terminal using the **Enable Web Terminal** option.
The Web Terminal allows you to open SSH and RDP sessions in a browser without installing third-party clients. You can open a session via the user's console.

Syslog

The Syslog server is used for integration with a SIEM system and serves as a unified data storage for PAM event records or text session logs. Data is updated in real time: during an active remote connection, not after its completion.

To send text logs of sessions, fill in the Syslog server data.
Sending events to the Syslog server is configured via configuration files.

Option	Description
Syslog server	IP address or DNS name of Syslog server
Port	Syslog server port
Protocol	Network protocol for connection to Syslog server: TCP, UDP
Format	Event format used by syslog server: CEF, LEEF
Syslog version	IETF standard of Syslog protocol: RFC3164, RFC5424

User Authentication

This section specifies the global authentication settings. Fine-tuning authentication is configured in the Policies section.

User Blocking

If the user enters the wrong password or OTP several times in a row, their account will be blocked for the specified time.

Option	Description
Number of Attempts	If this value is exceeded, the user will be temporarily blocked. If the value is 0, the blocking does not apply.
Blocking Time	Defines the period of time after which the user will be unlocked and will be able to enter the password or OTP again.

Automatic logout on inactivity

The **Inactivity period in MC/UC interface** parameter sets the time after which the user and administrator consoles are automatically logged out. The setting does not affect user access to resources.

Automatic exit occurs if the user:

- authenticated in the user or administrator console via IDP;
- did not perform any actions in any browser tab during the specified period of inactivity.

Set the period of inactivity from 0 to 480 minutes, where 0 — means automatic logout is disabled. Background browser operations, such as updating data or checking system status, are not considered user actions.

SSH Key Authentication

If the **Allow users to connect to SSH Proxy using SSH keys** option is enabled, users can connect to SSH Proxy without passwords using SSH keys added to Axidian PAM. The requirement to enter OTP remains. If this option is disabled, users can only authenticate using a password.

Session opening without re-authentication

This setting allows you to disable re-authentication when running RDP, SSH, and SQL sessions. A code is added to the connection string or RDP file, which is used to authenticate the user without requesting a password or a second authentication factor. The code is valid only once and for a limited time.

For Web Proxy, this setting does not apply: a code is always used.

How to set the number of authentication codes?

The number of codes is set in the component configuration file Axidian Privilege IdP:

- Windows OS: `C:\inetpub\wwwroot\idp\appsettings.json`
- Linux OS: `/etc/axidian/axidian-privilege/idp/appsettings.json`

Set the value from 1 to 100 for the `MaxAuthCodesPerUser` parameter:

```
"DirectoryMechanism": "Ldap",
"Authentication": "Local",
"UseDeveloperSigningCredential": false,
 "MaxAuthCodesPerUser": 100,
"QaToolClientSecret": "secret"
```

Option	Description
Allow session opening without re-authentication	If this option is enabled, a one-time authentication code is added to the connection string or RDP file.
Authentication code lifetime	Determines the validity period of the authentication code. If you start a session with an expired code, the user will need to enter a password and a second authentication factor. Default value: 60 seconds. Minimum value: 5 seconds. Maximum value: 300 seconds.

X.509 certificate authentication

Allows authenticating users in the admin and User Consoles using X.509 client certificates issued by trusted certification authorities. To add this login method, see the X.509 Certificate section.

Authentication modes

- **Enabled (optional)** — users can log in using a certificate or a username and password.
- **Mandatory for users with specified certificate Subject** — users with a specified certificate `Subject` can log in only using a certificate. Other users log in via login and password.
- **Mandatory for all users** — console login is only possible using a certificate.

  > ⚠ **CAUTION**
  > When selecting the **Mandatory for all users** mode, ensure that users have the Subject field filled in correctly, otherwise they will not be able to log into the console.

- **Disabled** — certificate authentication is not used.

Authentication via OIDC Identity Provider

The setting allows you to enable authentication via an external Identity Provider using the OpenID Connect protocol.
To add this login method, see the OpenID Connect Protocol section.

Parameters

Option	Description
Enable authentication via OIDC Identity Provider	The option enables authentication using the OpenID Connect protocol via an external Identity Provider. Login using a username and password remains available.
Login button name	The name of the authentication button for the Identity Provider. The button is displayed on the sign-in page of the Axidian Privilege console.
Match users by email on first login	**Compatibility mode** Enable the option to match users by email address if the identifier (`sub`) is not set in PAM. After sign-in, the identifier is saved and used for subsequent authentication. **Strict mode** Disable the option so that only users with a predefined identifier (`sub`) can sign in to PAM via OIDC.
Redirect URI	The address to which the Identity Provider redirects the user after authentication. Copy this value and specify it when registering PAM in the Identity Provider settings.
OIDC Provider URL	The OIDC server address from the Identity Provider settings. Example: `https://idp.company.ru`.

Option	Description
Authentication flow	**Available OIDC authentication flows** • **Authorization Code Flow** — the user is redirected to the authorization server and receives a code that is exchanged for an access token. • **Authorization Code Flow + PKCE (default)** — the recommended flow that uses the Proof Key for Code Exchange (PKCE) extension. An additional secret is generated for each authorization request and is verified when exchanging the code for an access token. • **Implicit Flow** — the authorization server returns the access token in the URL after user authentication. This flow is not recommended due to the risk of token interception.
Client ID	The client identifier created when registering PAM in the Identity Provider.
Client Secret	The client secret issued when registering PAM in the Identity Provider.
Claim	OIDC attribute that PAM uses to retrieve the user's email to match the user account. The default value is `email`.
Scope	The name of the OIDC scope used in the request to the OIDC provider to retrieve the claim containing the user's email. The default value is `email`.

Password Requirements for Internal Users

Option	Description
Password Validity Period	Minimum value: 0—no restrictions. Default value: 45 days. Maximum value: 999 days.

Option	Description
Minimum password length	Minimum value: 4 characters. Default value: 8 characters. Maximum value: 255 characters.
Lowercase letters	If the option is enabled, the password must contain at least one lowercase Latin letter.
Uppercase letters	If the option is enabled, the password must contain at least one Latin capital letter.
Digits	If the option is enabled, the password must contain at least one digit 0–9.
Special characters	If the option is enabled, the password must contain at least one special character from the list: ~!@#$%^&*()_-+={}|[] \:;"'<>,.?/

User Connection

> ⚠ **CAUTION**
> **Manage User Connections** privileges are required to work with user connections (UserConnectionType.Create, UserConnectionType.Read, UserConnectionType.Update, UserConnectionType.Delete).

Axidian Privilege has the following built-in user connection types:

- RDP
- SSH
- Telnet
- PostgreSQL
- MSSQL
- Web

Built-in types cannot be changed or deleted.

It is also possible to add custom user connection types.

Adding Custom User Connection Types

Add your custom type of user connection and open sessions in the browser without using third-party applications.

Web application

1. Go to the **Configuration** → **User Connection** section.
2. Click **Add**.
3. Enter a name of the user connection.
4. Set the login format or leave the default value.
5. Select the **Web Application** type and click **Next**.
6. Select Session opening method:
   - In browser — the session will open in a new browser tab.
     Access is provided via Web Access Server.
   - Via RDP — the session will open via a downloaded RDP file.
     Select a browser and enable the **Run browser in kiosk mode** option. Access is provided via RDS Access Server by publishing the selected browser.
7. Click **Next**.
8. Configure the **Auto-fill user credentials (SSO)** option.
   This option allows automatic filling of the login and password on the target resource using privileged account data. After enabling the option, download the SSO template in JSON format for connecting via the browser, and in XML format for the RDP file.
9. Click **Create**.

Windows application

> **INFO**
> To add a new connection type, you need to research the client application and develop a template for Axidian Privilege ESSO Agent. The new connection type is unique for each application, for development please contact Technical Support.

1. Go to the **Configuration** → **User Connection** section.
2. Click **Add**.
3. Enter a name of the user connection.
4. Set the login format or leave the default value.

5. Select the **Windows Application** type and click **Next**.
6. In the **Path to executable file** field, specify the path to the Windows application.
7. In the **Command line arguments** field, enter the required arguments and click **Next**.
8. Configure the **Auto-fill user credentials (SSO)** option.
   This option allows automatic filling of the login and password on the target resource using privileged account data. After enabling the option, download the SSO template in XML format.
9. Click **Create**.

Auto-fill user credentials (SSO)

SSO (Single Sign-On) is a method that allows users to authenticate to multiple web resources with a single set of credentials. To fill in the credentials automatically, create an SSO template file with the login form data.

To connect to a user using the browser session opening method, download the SSO template in JSON format, and to connect via RDP, download it in XML format. To configure the SSO template in XML format, contact technical support.

An example of an SSO template is located in the PAM distribution package `\axidian-pam-tools\sso-templates` folder.

> ⚠ **CAUTION**
> The credentials for authentication on the web resource must match the data of the privileged account.

The structure of the SSO template in JSON format

```
{
  "username-field": "input[id='login']",
  "password-field": "input[id='password']",
  "submit": "button[type='submit']",
  "cannot-submit": "div[class='v-messages__message']"
}
```

To automatically authenticate to a web resource, change the values of the CSS selectors:

- `username-field` — account login, for example: `"input[data-marker='login-form/login/input']"`
- `password-field` — account password, for example: `"input[type='password']"`

- `submit` — login button, for example: `"button[data-marker='login-form/login-button']"`
- `cannot-submit` — authentication error, for example: `"div[data-marker='login-form/error']"`

> **HOW TO DETERMINE A CSS SELECTOR NAME**
>
> Launch the web resource in a browser and navigate to the authentication page. Open **DevTools** and switch to the **Elements** panel. Find the desired CSS selector and insert the value into the SSO template.

Login format for SSH connections

Change the login format for a domain or local account if the login in UPN or DOMAIN\user format is used when connecting to a resource via SSH.

To set the default login format:

1. Go to the **Configuration** → **User Connection** section.
2. In the **SSH** connection settings, click **Edit**.
3. Specify the login formats for local and domain accounts.
   Use the required variable `%username%` and the optional variables `%location%`, `%location-dns%`.

   Examples

   Login format for john.smith@pam.local

   ```
   %username%@%location-dns%
   ```

   Login format for SPACE\john.smith

   ```
   %location%\%username%
   ```

   Login format for john.smith

   ```
   %username%
   ```

4. Click **Save**.

Service Connection

> ⚠ **CAUTION**
>
> **Manage Service Connection Types** privileges are required to work with service connections (ServiceConnectionType.Create, ServiceConnectionType.Read, ServiceConnectionType.Update, ServiceConnectionType.Delete).

Axidian Privilege has the following built-in service connection types:

- Windows
- SSH
- Microsoft SQL Server
- MySQL
- PostgreSQL
- Oracle Database
- Cisco IOS
- Inspur BMC

Built-in types cannot be changed or deleted.

It is also possible to add custom service connection types.

Adding Custom Service Connection Types

> ⚠ **CAUTION**
>
> If your PAM installation's management server is installed on a Windows host, you can only add connectors with a powershell template.
>
> If your PAM installation's management server is installed on a Linux host, you can only add connectors with a bash template.

1. Open the **Configuration** → **Service Connection** section.
2. Click **Add Service Connection** Type.
3. In the window that opens, upload the ZIP archive with the connector file.
4. Specify the **Name** of the service connection or use the value loaded from the metadata.
5. Enter the **Description** of the service connection. Optional.
6. Finish operation by clicking **Add**.

Connectors preparation

To prepare a ZIP archive with the connector file, use the Connector Creation Tool.

Editing Custom Service Connection Types

Upload new connector

1. Open the **Configuration** → **Service Connection** section.
2. Click **Edit** next to the desired service connection type.
3. Click **Download archive** and select a folder on your computer to save the current ZIP archive with the connector file. This archive will be needed to restore the previous state of the service connection if an error occurs when loading a new archive.
4. Upload a new ZIP archive with connector file.
5. If necessary, edit **Name** or **Description**.
6. Finish editing by clicking **Save**.

Edit name or description

1. Open the **Configuration** → **Service Connection** section.
2. Click **Edit** next to the desired service connection type.
3. Edit **Name** or **Description**.
4. Finish editing by clicking **Save**.

Connector Script Code Viewing

1. Open the **Configuration** → **Service Connection** section.
2. Click **Show script code** next to the desired service connection type.

Custom Connection Types Deleting

1. Open the **Configuration** → **Service Connection** section.
2. Click **Delete** next to the desired service connection type.

> **INFO**
> A service connection type cannot be deleted if a resource with that type exists.

Uploading the SSH Connector Template

The service operations template is unique for each *nix distribution. The PAM distribution includes templates for the *nix distributions listed below. Path to the templates in the PAM distribution: `AxidianPAM_3.5\axidian-pam-tools\ssh-templates\`.

SSH connector templates included in Axidian Privilege distribution

- CentOS
- Debian
- FreeBSD
- Gentoo
- Oracle
- RHEL
- Rocky
- SLES
- Ubuntu

To add a template to Axidian Privilege:

1. Open the **Configuration** → **Service Connection** section.
2. Inside the SSH block, click **Add**.
3. Select the file with the SSH connector template you need from the distribution by path `AxidianPAM_3.5\axidian-pam-tools\ssh-templates\`.

If you need help with development of the new template, please contact Technical Support.

Network Location

The section contains information about adding network locations to limit the use of resources issued by addresses.

To add a network location:

1. Click **Add**.
2. Enter a **Name**.
3. Add the **Network addresses** of the resources to which you want to issue a limited connection.

Tags

This section displays all the tags that have been created. By default, tags are sorted alphabetically in direct order. To sort them in reverse order, click on the table header, the **Tags** column.

To create a tag:

1. Click **Create**.
2. Enter tag **Name**. It can contain from 2 to 50 characters and can consist only of Latin and Cyrillic letters, numbers and special characters. The tag name must be unique regardless of case. For example, if you already have an "important" tag, you won't be able to create an "IMPORTANT" tag.
3. Select a color.
4. Leave the **Display tag in User Console (UC)** option enabled. If you disable this option, only PAM administrators will be able to use the tag in management console.
5. Finish adding by clicking **Save**.

To find the tag:

1. Specify the tag name in the search bar in whole or in part.
   In PAM installations with PostgreSQL database, the search is case-sensitive. For example, if you have an "important" tag, it won't appear when you type "IMPORTANT". In PAM installations with Microsoft SQL database, the search is case-insensitive, that is, the tag will be displayed when you enter its name with both uppercase and lowercase letters.
2. Press ENTER or .

To edit the tag:

1. Select the tag from the list.
2. Click **Edit**.
3. Make the changes. It is possible to change the tag name, color and visibility of the tag in the User Console.
4. Finish editing by clicking **Save**.

To remove one or more tags:

1. Select one or more tags from the list.
2. Click **Remove**.
3. In the pop-up window, click **Remove**.

> **INFO**
> When tag is removed from PAM, the tag will be removed from all the resources to which it was applied.

Monitoring

Axidian Privilege automatically detects unused permissions. Administrator can revoke such permissions to minimize redundant privileges.

Parameter **Consider permission unused if it has not been used for more than** sets the number of days of inactivity on the permission, beyond which the permission is considered unused.

The following actions are considered to be the use of the permission:

- successful start of the session
- viewing or changing credentials
- checking the permission to use pamsu

Licenses

This section displays data on registered, available, and used licenses. For more information about licenses, see the section Licensing.

Getting

1. Open the **Configuration** → **Licenses** section.
2. Copy the value from the **Installation ID** field.
3. Send this value to technical support and ask them to generate a license file.
4. Wait for a response from technical support with a license file in the `PAM_yyyy.mm.dd.lic` format.

Adding

1. Open the **Configuration** → **Licenses** section.
2. Click **Add** and select a license file.

Removing

1. Open the **Configuration** → **Licenses** section.
2. Select one or more licenses and click **Remove**.

Specifying the Length of a Video Segment when Recording an RDP Session

During an RDP session, video is recorded from the desktop of the remote resource. The RDP session video is divided into segments.

The longer the video segment is, the more CPU is loaded in an open session.

To reduce CPU load, set a smaller value of the following parameter in the PAM administrator console:

Configuration → System Settings → The duration of the recorded video segment, sec

Connector Creation Tool Usage

Connector Creation Tool (CCT) is a command-line utility for creating and debugging custom service connection types. The archive created with this utility is loaded into PAM in the Configuration → Service Connection section.

Prerequisites

There are no additional requirements to run on Windows.
To run on Linux, you need to have Microsoft .NET Core 8 and Docker installed.

Connector Development

1. To make it easier to work with the Connector Creation Tool (CCT), add an alias for it using the command below. Before running the command, replace `<path to CCT>` with the location on the file system where you have the Connector Creation Tool.

   After executing the command below, close the terminal and open it again.

   Windows

   Adding the path to CCT to the environment variable

   ```
   "New-Alias cct <path to CCT>\Pam.Tools.ConnectorCreationTool.exe" | Add-Content $PROFILE
   ```

   Linux

   Adding the path to CCT to the environment variable

   ```
   echo 'alias cct="<path to CCT>/run-cct.sh"' >> ~/.bashrc
   ```

2. Create a folder for the connector and navigate to it:

   Connector Folder Creation

```
mkdir my_connector
cd my_connector
```

3. Create a connector template using the `new` command:

Connector Template Creation

```
cct new
```

The connector type is selected depending on the OS: ps1 for Windows, sh for Linux. If necessary, you can change the type in the options of the `new` command, for more information see the command reference.

After executing the command, the main files of the connector will appear in the directory. For more information, see connector structure.

4. The `connector.ps1/sh` file contains methods that need to be implemented. Initially such methods return an error when called, but the file also contains working examples in commented code. Implement these methods.

> ⓘ **INFO**
> The main script of the connector must be written in bash or powershell, depending on the selected connector type. At the same time, to implement the methods, you can use any languages and technologies, depending on what is more convenient to access the resource. In this case, you will need to call your scripts or executables created in other languages in the main `connector.ps1/sh` script.

5. Go to connector debugging.

Connector Debugging

Once the methods in the script are implemented, you can check their execution using the `run` command. For more information on the `run` command, see the command reference.

1. Check the connection to the connector.

Checking the connection to the connector

```
cct run test_connection -a <DNS or IP of the connector>
```

2. Check the command of setting the password for the user.

Setting the password for the user

```
cct run set_user_password -a <DNS or IP of the connector> --user <user> --new-password <new password>
```

3. Check the command of setting the key for the user.

Setting the key for the user

```
cct run set_user_key -a <DNS or IP of the connector> --user <user> --old-key-path <old key path> --new-key-path <new key path>
```

4. Check the user password verification command.

User password verification

```
cct run test_password -a <DNS or IP of the connector> --user <user> --password <password>
```

5. Check the user key verification command.

User key verification

```
cct run test_key -a <DNS or IP of the connector> --user <user> --key-path <key path>
```

6. Check the command of checking for unmanaged keys.

Checking for unmanaged keys

```
cct run test_unmanaged_keys -a <DNS or IP of the connector> --user <user> --key-path <key path>
```

7. Check the unmanaged key removal command.

Removing unmanaged keys

```
cct run remove_unmanaged_keys -a <DNS or IP of the connector> --key-path <key path>
```

8. Check the command of getting information about a resource.

Getting information about a resource

```
cct run get_resource_info -a <DNS or IP of the connector>
```

9. Check the command of getting information about an account.

Getting information about an account

```
cct run get_account_info -a <DNS or IP of the connector> --user <user>
```

10. Check the command of getting the list of users.

Getting a list of users

```
cct run get_users -a <DNS or IP of the connector>
```

11. After checking all service operations, go to packing the connector.

Connector Packing

Connector files need to be packed into a ZIP archive for further uploading into PAM. To do this, run the following command in the same directory:

Connector packing

```
cct pack
```

For more information on the `pack` command, see the command reference.

ZIP archive will be placed to the parent directory. Next, go to PAM in the Configuration → Service connection section to upload the ZIP archive file of the connector.

Connector Structure

There are three main files in the ZIP archive file of the connector:

- `info.json`—connector metadata
- `info.schema.json`—JSON schema of info.json file
- `connector.ps1/sh`—script performing service operations

In addition to the main files, the connector may contain any other files, including binary ones. Except for files named `wrapper.ps1` and `wrapper.sh`. These file names are reserved for PAM for an additional script to start the connector.

The maximum size of the ZIP archive file of the connector is 100 MB.

Example of info.json file

```
{
  "$schema": "info.schema.json",
  "Id": "TestBashConnector",
  "Name": "Test Bash connector",
  "Description": "This is a test connector",
  "Version": "1.0",
  "CreatedAt": "2024-12-05 14:45:03Z",
  "ConnectorType": "sh",
  "ScriptTimeout": 30,
  "IsKeyServiceOperationSupported": false,
  "LinuxSandbox": {
    "Image": "my-test-connector:1.0",
    "CpuLimit": "0.5",
    "MemoryLimitMb": "512",
    "StorageLimitMb": "1024",
    "PidCountLimit": "8"
  }
}
```

- `$schema`—JSON schema file name.
- `Id`—connector identifier, must be unique within PAM installation.
- `Name`—connector name that will be displayed in PAM, must be unique within PAM installation.
- `Description`—description of the connector that can be viewed in the connector details in PAM. Optional.
- `Version`—connector version.
- `CreatedAt`—connector creation time, specified automatically when packaging the connector.
- `ConnectorType`—connector type (sh or ps1).

- `ScriptTimeout`—timeout for attempting to perform a service operation by the connector in seconds. If the script does not complete within the specified time during the execution of a service operation, the operation will time out.
- `IsKeyServiceOperationSupported`—flag indicating whether the connector supports working with SSH keys. If the script implements operations with SSH keys, then specify true.
- `LinuxSandbox`—optional section. Contains settings to override the default Docker sandbox settings specified in Core/appsettings.json.
- `Image`—Docker image tag for sandbox execution.
- `CpuLimit`—CPU limit of one sandbox container.
- `MemoryLimitMb`—memory limit of one sandbox container.
- `StorageLimitMb`—temporary storage limit of one sandbox container.
- `PidCountLimit`—number of processes limit of one sandbox container.

> **INFO**
> There is no sandbox for PowerShell connectors.

Command Reference

new

Creates a template for a new connector. This command creates `info.json`, `info.schema.json` and `connector.ps1/sh` files in the specified directory.

Windows

Example

```
<path to CCT>\Pam.Tools.ConnectorCreationTool.exe new -t ps1 -p
C:\Users\user\documents\folder1\
```

Linux

Example

```
bash <path to CCT>/run-cct.sh new -t ps1 -p /home/user/documents/folder1/
```

Parameters of the command new

Parameter	Required	Description
`-v`, `--verbose`	—	Enable display of additional logs.
`-p`, `--path`	—	Path to the directory where the `info.json`, `info.schema.json` and `connector.ps1/sh` files will be created. If not specified, the files will be created in the current folder.
`-t`, `--type`	—	Script type. Possible values: • `sh` — only run on Linux (bash) • `ps1` — only run on Windows (powershell)
`-h`, `--help`	—	Usage information and help.

pack

Creates a ZIP archive of the connector for further uploading into PAM.

Windows

Example

```
<path to CCT>\Pam.Tools.ConnectorCreationTool.exe pack -p C:\Users\user\documents\folder1\ -
n b80d094b715aa08375b87e9.1.1
```

Linux

Example

```
bash <path to CCT>/run-cct.sh pack -p /home/user/documents/folder1/ -n
b80d094b715aa08375b87e9.1.1
```

Parameters of the command pack

Parameter	Required	Description
`-v`, `--verbose`	—	Enable display of additional logs.
`-p`, `--path`	—	Path to the connector.
`-n`, `--name`	—	The name of the ZIP file without the .zip extension. By default, the name consists of the values of the ID and Version fields of the info.json file.
`-h`, `--help`	—	Usage information and help.

hash

Calculates the SHA-256 hash of a file. Used to ensure file integrity.

Windows

Example

```
<path to CCT>\Pam.Tools.ConnectorCreationTool.exe hash -p C:\Users\user\documents\folder1\
```

Linux

Example

```
bash <path to CCT>/run-cct.sh hash -p /home/user/documents/folder1/
```

Parameters of the command hash

Parameter	Required	Description
`-v`, `--verbose`	—	Enable display of additional logs.
`-p`, `--path`	Yes	Path to the connector (ZIP archive).

Parameter	Required	Description
`-h`, `--help`	—	Usage information and help.

run

Launches the connector, executes the connector script in the specified directory.

Windows

Example

```
<path to CCT>\Pam.Tools.ConnectorCreationTool.exe run test_connection -p
C:\Users\user\documents\folder1\ -a 192.168.5.1
```

Linux

Example

```
bash <path to CCT>/run-cct.sh run test_connection -p /home/user/documents/folder1/ -a
192.168.5.1
```

Parameters of the command run

Parameter	Required	Description
`-v`, `--verbose`	—	Enable display of additional logs.
`-p`, `--path`	—	Path to the connector (ZIP archive or directory).
`-a`, `--address`	Yes	DNS or IP of the connector.
`--port`	—	Connector port.
`-sa`, `--service-account`	—	Service account name.
`-sp`, `--service-account-password`` password``	—	Service account password.

Parameter	Required	Description
`-skp`, `--service-account-key-path`	—	service account key path.
`-slt`, `--service-account-location-type`	—	Service account location type. Possible values: `Domain`, `Local`.
`--disable-sandbox`	—	Disable sandbox.
`-h`, `--help`	—	Usage information and help.

Commands that can be launched with run command

Command	Description
`test_connection`	Check the connection to the connector.
`set_user_password`	Set a password for the user.
`set_user_key`	Set a key for the user.
`test_password`	Check user password.
`test_key`	Check user key.
`test_unmanaged_keys`	Check for unmanaged keys.
`remove_unmanaged_keys`	Remove unmanaged keys.
`get_resource_info`	Get information about a resource.
`get_account_info`	Get information about an account.
`get_users`	Get a list of users.

Roles

This section is for configuring privileges for Axidian Privilege administrator users in the Axidian Privilege Management Console.

Presetting

Add the current user to the Administrator role after first login

1. Go to the **Roles** section
2. Open the **Administrator** role and go to the **Members** subsection
3. Click **Add**, select the current user and add him to the role
4. Re-enter the management console and make sure that all other sections appear in the console

Built-in Roles

The **Administrator**, **Operator** and **Supervisor** roles will be available right after the installation.

> ⚠ **CAUTION**
> Attention! After upgrading to the new version, it is necessary to check the set of claims for all roles added.

All claims are enabled for the **Administrator** role.

The **Operator** role includes claims that allow you to create or revoke permissions (for example, process access requests), as well as check privileged Accounts and the availability of target Resources.

The **Supervisor** role is for finding and viewing values, except for Account passwords. The claims to add and modify values are disabled. The role will be useful for monitoring the work of Axidian Privilege administrators.

Creating New Roles

> ⓘ **NOTE**
>
> To perform operations on roles, you should have the claims to manage access roles.

Follow these steps:

1. Go to the **Roles** section, click the **Add** button and provide a name for the new role. The new role is added to the list of roles.
2. Open the created role, go to the **Claims** section, select the required set of claims, save the changes.

Adding Users to a Role

Follow these steps to assign claims to the management console users:

1. Go to the **Roles** section, open the required role.
2. Go to the **Members** section and add the required users.

> ⚠ **CAUTION**
>
> If a user is added to several roles, then he receives the sum of privileges from all his roles.

Removing Roles

Go to the **Roles** section, select the required roles, click **Remove**.

Applications

An Application is third-party software for automation and task execution. When launched, an application requests authentication using account credentials. Typically, this data is stored unencrypted in scripts or configuration files, increasing the risk of interception by third parties.

To enhance security, use the method of automatic credential retrieval — Application to Application Password Management (AAPM). In this case, passwords and SSH keys of accounts are stored in Axidian Privilege and requested by the application only at the moment of task execution. This allows controlling access to credentials, avoiding their storage in an open format, and automatically updating them.

To configure AAPM operation:

1. Add the application to Axidian Privilege and configure authentication.
2. Grant permission and select those accounts whose passwords or SSH keys are required for AAPM operation.
3. Verify the application's operation and retrieve credentials in a convenient way.

> ⓘ **INFO**
> An AAPM license is required to work with applications.

Application profile

For each application, the following are displayed:

- **Administrators** — a list of users who can view the application's credentials.
- **Permissions** — a list of granted permissions to use account credential data.
- **Events** — records of operations related to the application.

Add application

> ⚠ **RESTRICT ACCESS**
> To improve security, it is recommended to create an application for a specific task and control the permissions granted.

1. Go to the **Applications** section in the admin console.
2. Click **Add**.
3. Fill in the **Name** and **Description** fields and click **Save**.

Authentication

Before starting work in Axidian Privilege, applications and users are authenticated in the IdP.
The following authentication methods are supported for applications:

- **Password** — mandatory and automatically generated when adding an application to PAM. In the admin console, the password cannot be viewed but can be reset. The application administrator can view the password in the user console.
- **IP address** — set additionally if verification of the IP address from which the token request originates is required.
- **Certificate** — set additionally if verification of the client certificate fingerprint is required.

Create permission

Permissions allow the application to use passwords or SSH keys of Axidian Privilege accounts.

To create a permission:

1. Open the application profile and click **Create permission**.
2. (Optional) Select an organizational unit and click **Select**.
3. Define the permission composition:
    1. Select an application or keep the preset value.
    2. Select one or several accounts whose credentials are required for the application to work.
4. (Optional) Set the **Allow change account credentials** option. If the option is enabled, users can change the password of the privileged accounts used in the permission.
5. (Optional) Fill in the **Description** field.
6. (Optional) Configure time restrictions.

More about time restrictions

You can set a schedule according to which users are allowed to open sessions or change credentials. For example, you can grant permission to work only on weekdays from 8:00 to 17:00.

The following settings are available:

- **Validity period** — the time period during which the permission is valid. For example, you can grant permission for one day or month.
  - **Begin** — set the date and time when the permission becomes active.
    If only **Begin** is set, the permission will become active on the selected date, and its validity period will be unlimited.
  - **End** — set the date and time when the permission becomes inactive.
    If only **End** is set, the permission will become active at the moment of creation, but will be suspended on the specified date.

    > **INFO**
    > If the **Begin** and **End** parameters are not set, the permission will be valid indefinitely.

- **Access schedule** — restrictions by days of the week taking into account the specified schedule.
  - **Allow access only on selected days** — select the days of the week when the permission will be active.
  - **Allow access only during selected hours** — select the time when the permission will be active.

    > **INFO**
    > Access by days of week is granted according to the management server time zone.

After the validity period expires, the permission will transition to the *Restricted/Inactive* state, and the user session will be terminated.

7. Check the data and click **Create permission**.

Reset password

When adding an application, Axidian Privilege assigns it a random password. In the admin console, this password cannot be viewed, but it can be reset and a new one set. Follow these steps:

1. Go to the application profile and click **Reset password**.
2. In the window that appears, specify a reason to reset the application password.
3. Click **Reset**.

After the old password is reset, Axidian Privilege will generate a new one.

Add or remove an administrator

Administrators can view application passwords in the user console.
To add an administrator:

1. Open the application profile and go to the **Administrators** tab.
2. Click **Add Administrator**.
3. Select one or more users and click **OK**.
4. Confirm the action and click **Add**.

To remove an administrator:

1. Open the application profile and go to the **Administrators** tab.
2. Select one or more users and click **Remove**.
3. Confirm the action and click **Remove**.

Delete application

> ⚠ **CAUTION**
> After deleting application, it will no longer be able to receive passwords or SSH keys from Axidian Privilege accounts.

To remove the application:

1. Go to the application profile.
2. Click **Delete** and confirm the action.

To delete multiple applications, select the required applications in the **Applications** section and click **Remove**.

First Launch

After the first login, go to the **Roles** section and add the current user to the *Administrator* role, refresh the page and make sure all the sections of the administrator console are available to you.

Check users presence

1. Go to the **Users** section.
2. Click .
3. Make sure that all users from the specified organizational unit are displayed correctly.

License the installation

1. Go to **Configuration** → **Licenses** section.
2. Copy the value from the **Installation ID** field.
3. Send this value to technical support and ask them to generate a license file.
4. Wait for a response from technical support with a license file in the `PAM_yyyy.mm.dd.lic` format.
5. In the **Configuration** → **Licenses** section, click **Add** and attach the received license file.

Fill in the component addresses

1. Go to **Configuration** → **System Settings** section.
2. In the **Connect to Gateway** section, specify the **RDCB Address** and **RDCB Collection Name**.
3. In the **RDP Proxy** section, specify **RDP Proxy Address**.
4. In the **PostgreSQL Proxy** section, specify the **PostgreSQL Proxy Address**.
5. In the **SSH Connection Settings** section, specify the **SSH Proxy Address**.
6. Save the changes.

Check events

1. Go to the **Events** section.
2. Make sure the event of configuration settings change is displayed.

Define the operation of text logging

If you chose not to install the Axidian PAM Agent component, go to **Policies** → **Sessions** → **Artifacts** and perform one of the following:

- disable the **Save text session logs** option
- enable the option **Continue RDP session without logging if unable to get text log**

If there are no errors, then you can proceed to adding objects.

Adding the Domain

1. Go to **Domains** section, click **Add**.
2. Enter the domain name (for example AXIDIAN-PRIVILEGE) and its DNS name (for example axidian-privilege.local), click **Save**.
3. Open the domain page.
4. Click **Add account**, enter the service account name (for example, **IPAMADServiceOps**)
5. Set the password manually and click **Save**.
6. Click the pencil icon next to **Service account** and select the service account (**IPAMADServiceOps**).
7. Click **Check connection** and check if the connection was successful.
8. Here, on the domain page, go to the **Resource container** tab and add an AD container that contains the required domain resources (for example, **Computers**).
9. Here, on the domain page, go to the **Privileged groups** tab and specify the security groups that contain the accounts which users will use to access domain resources (for example, **IPAMPrivilegedAccounts**).
10. Here, on the domain page, click the **Import Resources** and **Sync accounts** buttons. After that, all available resources and accounts will be added to the corresponding sections of the console.
11. If necessary, go to the **Events** tab to view detailed information about domain events.

Add and Take Control of Accounts

In the **Accounts** section, check the imported domain accounts: they begin with the domain name, are marked with a question mark, and have a **Pending** state. At the top, click the **Make managed** button. Then, the password for the selected accounts will be reset to a new one in accordance with the policy.

Adding Non-Domain Resources

1. Go to the **Resources** section, click **Add**.
2. Enter the **Resource name**, **DNS name** or **IP address**.
3. At the **User connection** step, select the connection type, specify the connection address and port if necessary.
4. At the **Service connection** step, uncheck the **Use connector for service connection** checkbox (since local accounts have not been added yet), finish adding the resource. The new resource appears in the resource list.
5. Open the resource page, click **Add account**, set the password manually.

The resource is ready to use: you can create permissions for it.

To perform service operations (searching and adding accounts, automatically changing passwords, updating resource information), it is necessary to set up a service connection.

Policy Setup

Policies

A policy is a set of options and restrictions applied to various objects: users, accounts, resources, or domains. For example, using configured policies, you can set forbidden SSH commands for the user, request reasons for opening a session, or restrict the operation of the clipboard between the workplace and the resource. You can assign only one policy for each object.

The **default policy** contains a set of parameters for all available sections and applies to all new objects, so it is advisable to start configuring there.

> ⓘ **NOTE**
> The default policy also applies to sessions opened on behalf of user accounts, unless other policies are explicitly applied to these users.

Open the policy page, set the desired parameters for the **Accounts**, **Sessions**, **RDP** sections, save settings.

Adding New Policy

> ⚠ **CAUTION**
> To add, view, edit and delete policies, you may need the appropriate claims from the **POLICIES MANAGEMENT** section (Policy.Create, Policy.Read, Policy.Update, Policy.Delete).

Click **Add** in the **Policies** section, fill in the Policy **Name**, **Description**, and **Priority** fields. The new policy will appear in the list.

General Information

Open the policy page, review the general information, edit **Name**, **Description**, or **Priority** if necessary by clicking the pencil icon

- **Name** — the name of the policy, it is set when creating a new policy. It can be changed at any time.
- **Description** — policy description.

- **Priority** — a number indicating the order in which a particular policy is applied. Zero priority is the default policy that is applied last.
- **Created by** — Axidian Privilege administrator name.
- **Date created** — date and time when the policy was created.
- **Changed by** — name of Axidian Privilege administrator who saved the policy settings.
- **Date changed** — date and time when the policy settings were saved.

To edit **Name**, **Description** and **Priority** click ✎

Sections

Go to the **Sections** and mark the sections which will be determined by the policy, save the changes. The corresponding sections will become available for setting up.

> ⓘ **NOTE**
> For unchecked sections, other policies will be applied by priority.

Scope

> ⚠ **CAUTION**
> To assign policies you may need the appropriate claims (User.SetPolicy, UsersGroup.SetPolicy, Account.SetPolicy, Resource.SetPolicy, Domain.SetPolicy).

Contains information about which users, user groups, accounts, resources, or domains the policy is applied to.

To apply a policy to an object, click **Add**, select the type of object to apply the policy, select the objects.

To remove the policy from objects, select the required objects and click **Remove**.

Creating a Copy of the Policy

Check the policy in the **Policies** section and click **Create copy**, fill in the **Policy name**, **Description** and **Priority** fields. The copied policy will appear in the list.

Removing Policy

Before removing a policy, make sure that it does not apply to any objects.

Check the required policies in the **Policies** section and click **Remove**.

> **NOTE**
> The **Default policy** cannot be removed.

Changing the Priority of a Policy

Check one policy under **Policies**, click **Change priority** and enter a number for the policy priority value.

You can also change the priority by opening the required policy and in the **General Information** section click the pencil icon next to the priority value.

Policy Sections

Accounts

Credential privacy settings

Option	Description
Reset account password and SSH key after showing	If this option is enabled, the password and SSH key of the privileged account will be reset every time the user views it in his self service (User Console).
Reset password and SSH key after X minutes	After viewing, the password and SSH key will be reset to a random value after the specified number of minutes.
Require a reason of password and SSH key viewing	If this option is enabled, the directory user must provide a reason before viewing the password or SSH key of the privileged account.
Password and SSH key viewing must be confirmed by Axidian Privilege administrator	Before each credential is viewed by the user, it must be confirmed by the Axidian Privilege administrator
Password and SSH key confirmation timeout, min.	Timeout of waiting for confirmation of password and SSH key viewing, from 1 to 180 minutes.

Option	Description
Encrypt SSH key using generated password before showing to user	If this option is enabled, the SSH key will be shown in encrypted form, and the generated encryption password will be hidden. The encryption key and password is generated by Axidian Privilege every time the data is viewed.

Set credential settings

Option	Description
Allow Axidian Privilege users to set credentials for accounts if they are not set	If this option is enabled, Axidian Privilege users can set password/SSH keys for privileged account before connection.

Check and Reset Credentials Settings

Option	Description
Periodically synchronize resources and accounts	If this option is enabled, then an automatic search for data and privileged accounts on resources will be performed.
Synchronize resources and accounts once in X days	Automatic search for resource data and privileged accounts will be performed once every specified number of days, from 1 to 10,000 days
Periodically check account password and SSH key	If this option is enabled, then passwords and SSH keys will be automatically checked for privileged accounts.
Check password and SSH key once in X days	Automatic check of the password and SSH key of privileged accounts will be performed once every specified number of days, from 1 to 10,000 days.
Reset password and SSH key if a mismatch is detected	If this option is enabled, then passwords and SSH keys will be automatically reset in case of mismatch between Axidian Privilege and resources.
Remove SSH keys unmanaged by Axidian Privilege	If there is no SSH key for the added account in Axidian Privilege, but there is one on the resource, then all discovered keys from the resource will be removed.

Option	Description
Check password and SSH key if it's set manually	If this option is enabled, a check will be performed when setting or changing a password or SSH key.
Periodically change account password and SSH key	If this option is enabled, the password or SSH key will be automatically changed to a random value for privileged accounts.
Change password and SSH key every X days	Automatic change of password or SSH key for privileged accounts will be performed once every specified number of days.

Password Generator Requirements

Option	Description
Generated password length	Total number of characters for automatically generated and manually entered passwords.
Lowercase letters	If this option is enabled, then automatically generated passwords will consist of lowercase letters. When combined with other settings, the password will contain at least one lowercase letter.
Uppercase letters	If this option is enabled, then automatically generated passwords will consist of capital letters. When combined with other settings, the password will contain at least one uppercase letter.
Digits	If this option is enabled, then automatically generated passwords will consist of digits. When combined with other settings, the password will contain at least one digit.
Special characters	If this option is enabled, then automatically generated passwords will consist of special characters. When combined with other settings, the password will contain at least one special character.
Prohibit the use of special characters at the beginning of the password	If this option is enabled, then the password will start with a letter or a number.

Option	Description
Maximum number of consecutive special characters	This parameter determines how many special characters are allowed to be used one after another. For example, if you specify a value of 1, then the `password#!` password will not be valid. But the `passwor#d!` password will be valid, because the special characters are not consecutive, they are separated by a letter. To allow any number of consecutive special characters, specify 0.
Prohibited characters	Characters that should not be used by the password generator when generating passwords. The field may be empty. In this case, no restrictions apply.
Required characters	Characters, at least one of which will definitely be used when generating a password. The field may be empty. In this case, no restrictions apply.
Number of passwords that should not be repeated	The number of previous passwords for the account with which the new password should not match.

Password Requirements for Manual input

Option	Description
Minimum password length	Minimum number of characters for manual password entry.
Limit characters for manual password entry	If the option is enabled, the settings described in this table are available for being set. If the option is disabled, any characters are allowed in passwords.
Lowercase letters	If this option is enabled, the password must contain at least one lowercase letter.
Uppercase letters	If this option is enabled, the password must contain at least one uppercase letter.
Digits	If this option is enabled, the password must contain at least one digit.

Option	Description
Special characters	If this option is enabled, the password must contain at least one special character.
Allow white space	If this setting is enabled, white spaces are allowed in the password, but are not required. You cannot enter a space in the **Prohibited Characters** and **Required Characters** fields.
Prohibit the use of special characters at the beginning of the password	If this option is enabled, the password must start with a letter or a digit.
Maximum number of consecutive special characters	This parameter determines how many special characters are allowed to be used one after another. For example, if you specify a value of 1, then the `password#!` password will not be valid. But the `passwor#d!` password will be valid, because the special characters are not consecutive, they are separated by a letter. To allow any number of consecutive special characters, specify 0.
Prohibited characters	Characters that should not be used in passwords. You cannot enter a white space in this field. The field may be empty. In this case, no restrictions apply.
Required characters	Characters, at least one of which must be used in passwords. You cannot enter a white space in this field. The field may be empty. In this case, no restrictions apply.
Number of passwords that should not be repeated	The number of previous passwords for the account with which the new password should not match.

Sessions

General

Option	Description
User must specify the connection reason	If the option is enabled, then when connecting to the resource, the user must enter the reason for starting the session. **Attention!** If you use PostgreSQL Proxy, warn users that they will need to enter the reason in the same field as the account name. For more information, see Connection to the PostgreSQL Proxy section.
The message that the user will see when the reason is requested	If the **User must specify the connection reason** option is enabled, then the message is required to be filled in. Default value: "Specify the connection reason:". You can change the text of the message to tell the user what exactly the information to enter when connecting. For example, if you need to specify the task number in the ticket system to connect, then enter: "Specify the task number to perform the task on this resource:". Maximum allowed message length: 100 characters.
Maximum session duration	The option enables the session duration limit in hours and minutes, after which the session will end automatically.
Enforce exclusive usage of account	If the option is enabled, then only one active session can be opened for the account
Start of the session must be confirmed by Axidian Privilege administrator	If this option is enabled, then manual confirmation by the Axidian Privilege administrator is required for each opened session. **Attention!** Leave this option disabled if you use PostgreSQL Proxy, otherwise it will be impossible to open an SQL session.
Session confirmation timeout, min.	Timeout for confirmation by the Axidian Privilege administrator, in the range from 1 to 180 minutes

Option	Description
Terminate session when there is no user activity	If the option is enabled, then if the user is inactive for a specified period of time, their session is terminated. For existing policies this option is disabled by default, and for new ones it is enabled by default. User activity refers to user interaction with the screen or session terminal, as well as file transfer operations. This option only applies to sessions opened via SSH Proxy and RDP Proxy.
Session termination timeout, min.	Minimum value: 1 minute Default value: 30 minutes Maximum value: 720 minutes
Reset password and SSH key at the end of the session	If the option is enabled, the password and SSH key will be reset after each session.

Session Artifacts

Option	Description
Save session text logs	If the option is enabled, then after the session, a text log will be available for viewing and downloading

Option	Description
Proceed with the RDP session without logging if the text log could not be retrieved	When option is enabled: If connection with the PAM agent is lost, the session is not terminated, users can continue working in this session. The event "Lost connection with PAM Agent" is entered into the log once. The line "WARNING: Lost connection with PAM Agent" is written once into the text session log. When the connection with the PAM agent is restored, the event "Connection with PAM Agent restored" is entered into the log once, and the line "INFO: Connection with PAM Agent restored" is written once into the text session log. When option is disabled (by default): If connection with the PAM agent is lost, the session is terminated.
Text log rotation	If this option is enabled, text session logs are deleted based on the configured number of days.
Remove text logs older than	The storage period of the text logs of the session (in days). Specify a value from 1 to 3650.
Save video	If the option is enabled, then after the session is completed, video recording will be available
Frames per second	The setting determines the frame rate for video recording. Specify a value from 1 to 10.
Video resolution	The setting allows you to set the resolution for video recording. Available values: • No change • Reduce 1.5 times • Reduce 2 times (recommend scaling for web sessions)
Video log rotation	If this option is enabled, video recordings are deleted based on the configured number of days.

Option	Description
Remove video older than	The storage period of the video recordings (in days). Specify a value from 1 to 3650.
Save screenshots	If this option is enabled, then screenshots of the session will be saved
Screenshots interval, sec.	Saving a screenshot after a specified number of seconds. Minimum interval is 60 seconds.
Screenshots resolution	Setting allows you to set the resolution of the screenshot. Available values: • No change • Reduce 1.5 times • Reduce 2 times (recommend scaling for web sessions)
Screenshots log rotation	If this option is enabled, screenshots are deleted based on the configured number of days.
Remove screenshots older than	The storage period of the screenshots (in days). Specify a value from 1 to 3650.
Save transferred files	If the option is enabled, then files when transferred from the local machine to the resource will be duplicated in the specified network folder. Supported only for Windows resources with disk forwarding enabled.
Transferred files rotation	If this option is enabled, transferred files are deleted based on the configured number of days.
Remove transferred files older than	The storage period of the transferred files (in days). Specify a value from 1 to 3650.

Sending Text Log via Syslog

Option	Description
Send text logs via syslog	The text log lines will be sent via syslog using the specified keywords. A keyword can be a regular expression.

Connection settings

The connection settings allow you to override the proxy server parameters specified in the Configuration → System Settings section. If your infrastructure uses multiple proxy server instances, you can specify individual settings for each one.

> ⓘ **HOW TO APPLY THE SETTINGS**
>
> To apply the settings when a session starts, assign the policy to a resource, account, or user.

Option	Description
Override Gateway settings	If this option is enabled, the Gateway component parameters used when connecting to the RDS Access Server are overridden according to the policy.

Option	Description

	Settings and limitations
	
	- **RDCB address** — IP address or DNS name of the server with the Remote Desktop Connection Broker role.
	- **RDCB collection name** — name of the Remote Desktop Connection Broker collection. The collection is used for load balancing when connecting through Axidian Privilege Gateway.
	- **Use RDGW** — allows the RDP client to connect to Axidian Privilege Gateway through the Remote Desktop Gateway.
	- **RDGW address** — IP address or DNS name of the Remote Desktop Gateway server.
	- **RDP file parameters** — parameters that are automatically added when the RDP file is generated in the User Console. The specified parameters are used when connecting to the RDS Access Server.
	
	`# Example`
	`screen mode id:i:2`
	`authentication level:i:2`

Option	Description
	Limitations The following parameters cannot be overridden through a policy: - `full address` - `redirectprinters` - `redirectcomports` - `redirectsmartcards` - `redirectposdevices` - `drivestoredirect` - `gatewayhostname` - `gatewayusagemethod` - `gatewayprofileusagemethod` - `loadbalanceinfo` - `shell working directory` - `alternate shell` - `remoteapplicationprogram` - `remoteapplicationcmdline`
Override SSH Proxy settings	If this option is enabled, the SSH Proxy component address is overridden according to the policy. In the **New address** field, enter the IP address or DNS name of the SSH Proxy server. This address is automatically added to the command used to connect to the resource.
Override RDP Proxy settings	If this option is enabled, the RDP Proxy component parameters are overridden according to the policy.

Option	Description
	Settings and limitations - **New address** — IP address or DNS name of the RDP Proxy server. This address is added to the RDP file. - **RDP file parameters** — parameters that are automatically added when the RDP file is generated in the User Console. The specified parameters are used when connecting to the RDP Proxy server. ``` # Example screen mode id:i:2 authentication level:i:2 ``` **Limitations** The following parameters cannot be overridden through a policy: - `full address` - `redirectprinters` - `redirectcomports` - `redirectsmartcards` - `redirectposdevices` - `drivestoredirect` - `gatewayhostname` - `gatewayusagemethod` - `gatewayprofileusagemethod` - `loadbalanceinfo` - `shell working directory` - `alternate shell` - `remoteapplicationprogram` - `remoteapplicationcmdline`

Option	Description
Override Web Proxy settings	If this option is enabled, the Web Proxy component address is overridden according to the policy. In the **New address** field, enter the IP address or DNS name of the Web Proxy server. This address is automatically substituted when a web session starts.
Override PostgreSQL Proxy settings	If this option is enabled, the PostgreSQL Proxy component address is overridden according to the policy. In the **New address** field, enter the IP address or DNS name of the PostgreSQL Proxy server. This address is automatically added to the command used to connect to the resource.
Override MSSQL Proxy settings	If this option is enabled, the MSSQL Proxy component address is overridden according to the policy. In the **New address** field, enter the IP address or DNS name of the MSSQL Proxy server. This address is automatically added to the command used to connect to the resource.

RDP

Connection parameters

> **INFO**
> The settings are added to the RDP file and are applied by the RDP client—the Remote Desktop Connection application or the Web Terminal—when the session is started.

Option	Description
Printers	If this option is enabled, the user can redirect a printer from their workplace to the Windows resource. This setting applies when connecting through Gateway and RDP Proxy.

Option	Description
Clipboard	If this option is enabled, the user can: • use the clipboard between their workplace and the resource • drag and drop files between the workstation and the resource when the RDP session is opened through the Web terminal This setting applies when connecting through Gateway and RDP Proxy.
Smart cards	If this option is enabled, the user can redirect a smart card from their workplace to the Windows resource. This setting applies when connecting through Gateway and RDP Proxy.
Ports	If this option is enabled, the user can redirect COM ports from their workplace to the Windows resource. This setting applies when connecting through Gateway and RDP Proxy.
Local drives	If this option is enabled, the user can: • redirect local drives from their workplace to the resource • exchange files between the resource and their workplace through the forwarded drives in RDP sessions opened through the Web terminal This setting applies when connecting through Gateway and RDP Proxy.
Require a trusted resource certificate to open an RDP session	The certificate is verified by the user's local RDP client when the RDP file is opened: • If this option is enabled and the resource certificate is invalid, the session does not open. • If this option is disabled, the session will open with any certificate. This setting applies when connecting through Gateway and RDP Proxy.

RDP file parameters	Parameters that are added when the RDP file is generated. This setting applies when connecting through Gateway and RDP Proxy.
	`# Example`
	`screen mode id:i:2`
	`use multimon:i:1`

Option	Description
	Limitations The following parameters cannot be overridden through a policy: • `full address` • `password` • `redirectprinters` • `redirectcomports` • `redirectsmartcards` • `redirectclipboard` • `redirectposdevices` • `server port` • `drivestoredirect` • `username` • `authentication level`

Activity control

Activity control allows you to track user actions within an RDP session and respond to them. For example, you can block a user in Axidian Privilege if they launch a specific application, switch to another window, or type a specific word on the keyboard.

User actions are tracked by analyzing text logs—when data appears in the logs, PAM reacts according to the configured rules.

> **HOW TO ENABLE LOG COLLECTION**
> For PAM to collect and analyze session logs, in the policy, go to **Sessions** → **Session Artifacts** section and enable the **Save session text logs** option.
>
> If the **Proceed with the RDP session without logging if the text log could not be retrieved** option is enabled, the session is not interrupted, but activity control is paused until log collection is restored.

Add rule

Add the necessary rules before the user connects to the resource. New rules apply only to sessions opened after the rules are added.

To add a new rule:

1. In the policy, in the **RDP** section, click **Add**.

2. Select the monitored action and fill in the additional parameters.

How to select and configure the action type

Process launch

With the selected action type, PAM tracks what the user launches. This can be applications, browsers, or system utilities.

1. In the **Executable path** field, enter a regular expression to match the executable file path. In the log, the file path follows `Executable path`.
2. (Optional) In the **Command line arguments** field, enter a regular expression to match the file startup parameters. In the log, the arguments follow `command line`.

> **INFO**
> Regular expressions are case-insensitive.
>
> The **Command line arguments** field is intended for startup parameters only. If the log duplicates the executable path after `command line`, do not include the path in this field.

Examples

Launching Google Chrome

To track Google Chrome launches, fill in the following fields:

- In the **Executable path** field, specify `.*\\chrome\.exe`.
- In the **Command line arguments** field, specify `.*`.

Text log example

```
2026-05-25 00:52:09 Executable path: C:\Program
Files\Google\Chrome\Application\chrome.exe, command line: "C:\Program
Files\Google\Chrome\Application\chrome.exe" --type=renderer --no-pre-
read-main-dll --disable-gpu-compositing --video-capture-use-gpu-memory-
buffer --lang=ru --device-scale-factor=1 --num-raster-threads=2 --enable-
main-frame-before-activation --renderer-client-id=35 --time-ticks-at-
unix-epoch=-1763427056801309 --launch-time-ticks=16232471832426 --
metrics-shmem-
handle=3048,i,5665439599788436001,8804099441798368138,2097152 --field-
trial-handle=1900,i,6741951583612309079,9546513817746230192,262144 --
variations-seed-version=20260524-030033.420000-production --
pseudonymization-salt-
handle=1904,i,9758245334007145095,8031267275877605306,4 --trace-process-
track-uuid=3190709019108336209 --mojo-platform-channel-handle=6232
/prefetch:1
```

Detecting a PowerShell execution policy bypass

To detect a PowerShell execution policy bypass, fill in the following fields:

- In the **Executable path** field, specify `.*\\powershell\.exe`.
- In the **Command line arguments** field, specify `.*-ExecutionPolicy\s+Bypass.*`.

Text log example

```
2026-05-25 10:14:32 Executable path:
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe, command line:
"powershell.exe" -ExecutionPolicy Bypass -WindowStyle Hidden -File
C:\Temp\install.ps1
```

Active window change

With the selected action type, PAM tracks which windows the user switches to, for example, Task Manager or a browser window.

In the **Active window title** field, enter a regular expression to match the window title that you want to track. In the log, the window title follows `Active window changed to`.

> **INFO**
> Regular expressions are case-insensitive.

Example

Switching to a Google Chrome browser window

To track switching to the Google Chrome browser window, in the **Active window title** field, specify `[^']*Google Chrome`.

Text log example

```
2026-05-25 00:30:27 Active window changed to 'New Tab - Google Chrome' 2026-05-25 00:30:27 Executable path: C:\Windows\system32\TSTheme.exe, command line: C:\Windows\system32\TSTheme.exe -Embedding
```

Keyboard input

With the selected action type, PAM tracks the text the user types on the keyboard. The rule does not apply to password input, because that field is masked.

In the **Entered text** field, enter a regular expression to match the text the user types on the keyboard. In the log, keyboard input follows `Keyboard`.

> **INFO**
> Regular expressions are case-insensitive.

⚠ **LIMITATIONS**

The rule applies to the sequence of keystrokes from the log, not to the final text the user entered.

When the rule will not trigger

The rule will not trigger in the following cases:

- Executing a command from history with the **Up+Enter** shortcut. The log contains only `[Up][Enter]` without the command text.
- Editing text with the **Backspace**, **Delete**, **Home** keys, or the **Left** and **Right** arrow keys.
- Entering characters with the **Shift** key. For example, entering the path `C:\Temp` appears in the log as `[Shift+c][Shift+;]\[Shift+t]emp`.
- Tracking text pasted from the clipboard.
- Selecting or replacing already entered text.
- Switching between input fields with the mouse.

Example

Entering a specific word

To track the entry of a word, for example `confidential`, in the **Entered text** field, specify `confidential`.

Text log example

```
2026-05-25 00:41:44 Keyboard: confidential[Enter]
```

Using the clipboard with Ctrl+V

To track when the user presses **Ctrl+V**, in the **Entered text** field, specify `\[Control\+v\]`.

Text log example

```
2026-05-25 09:15:02 Keyboard: [Control+v]
```

Opening print with Ctrl+P

To track when the user presses **Ctrl+P**, in the **Entered text** field, specify `\[Control\+p\]`.

Text log example

```
2026-05-25 09:16:20 Keyboard: [Control+p]
```

3. Select how PAM reacts when the user performs the tracked action.

Reactions and their priorities

> ⚠ **REACTION PRIORITY**
> If multiple rules apply to a single log entry, the rule with the higher priority is applied.

PAM reaction	Priority	Description
Log event only	1	◦ The user action is recorded in the log ◦ The current RDP session is not aborted ◦ The user is not blocked in PAM
Abort session	2	◦ The user action is recorded in the log ◦ The current RDP session is aborted ◦ The user is not blocked in PAM
Block user in PAM	3	◦ The user action is recorded in the log ◦ All user sessions are aborted ◦ The user is blocked in PAM

4. (Optional) Fill in the **Description** field. We recommend describing what the rule is for.
5. Click **Create**.

Edit rule

> ⓘ **INFO**
> The changes will take effect when the user ends the current session and starts a new one.

To edit an existing rule:

1. Select a rule from the list and click **Edit**.
2. Make the necessary changes and click **Save**.

Remove rule

If you remove a rule, PAM no longer reacts to the previously tracked action in the RDP session. A removed rule cannot be restored.

To remove a rule, select one or more rules and click **Remove**.

SSH

Session Parameters

Option	Description
Use PTY	Requests a pseudo-terminal (PTY) for the session. When disabled, only non-interactive commands are available.
Allow local port forwarding	Users can forward local ports in sessions opened via SSH Proxy. This allows using the SSH session to connect to other systems available on the target resource's network. When disabled, port forwarding is not allowed in the session. Dynamic and remote forwarding aren't supported in SSH Proxy sessions.

Privilege Elevation

Option	Description
Allow run pamsu	Support for executing commands with root privileges on resources with the PamSu component installed.

> **INFO**
> Allowing to use PamSu while creating the permission takes priority over the setting in the policy.

Allowed and Forbidden Commands

Option	Description
Prompt	Regular expression to correctly recognize command input. When entering a regular expression, note that you do not need to escape the `<` and `>` characters, as they are not included in the list of special characters: `.[{}()*+?|^$`. The `]` character is also special, but only when entered after `[`. For more information about the Boost regular expression syntax, see the Boost documentation.

Option	Description
Reaction to forbidden command	Terminal behavior in response to a forbidden command: CTRL + C (cancel execution) or Abort the session.
SSH commands	List of commands allowed or prohibited to execute in an SSH session.

Creating a list of controlled commands:

1. Click the **Add** button.
2. Enter the command or regular expression.

   When entering a regular expression, note that you do not need to escape the `<` and `>` characters, as they are not included in the list of special characters: `.[{}()\*+?|^$`. The `]` character is also special, but only when entered after `[`.

   For more information about the Boost regular expression syntax, see the Boost documentation.
3. Select the status **Allowed** or **Forbidden**.

> **INFO**
> Restricting command execution takes priority over permission.
>
> Without explicit permission, commands will be considered forbidden, so it is not recommended to remove the last rule that allows command execution.

To allow or prohibit several commands at once, select them with the check boxes and click the appropriate button.

When working with the list of commands, as well as when trying to execute a prohibited command, the corresponding events are recorded in the Events section.

Data Transfer

Option	Description
SCP	SCP file transfer settings.

Option	Description
	Available values - **Allowed in both directions** — files can be transferred both from and to the resource - **Allowed to the resource only** — files can be transferred only to the resource - **Allowed from the resource only** — files can be transferred only to the user's workplace - **Forbidden** — file transfer between the resource and the user's workplace is not available
SFTP	SFTP file transfer settings. **Available values** - **Allowed in both directions** — files can be transferred both from and to the resource - **Allowed to the resource only** — files can be transferred only to the resource - **Allowed from the resource only** — files can be transferred only to the user's workplace - **Forbidden** — file transfer between the resource and the user's workplace is not available
Maximum file size, MB	If the file size exceeds the specified value, the user cannot transfer the file during the session.

Configuring User Connections via SSH keys

Users can connect to SSH Proxy using SSH keys. This ensures secure and fast login to SSH Proxy without the need to use passwords.

Prerequisites

In the Configuration → User Authentication → SSH Key Authentication section, enable the **Allow users to connect to SSH Proxy using SSH keys** option.

Add the *User.ManageSshAuthorizedKeys* privilege to the role for the administrator who will add keys to users.

Getting and Adding Keys

Key in text format

1. Ask the user to generate an SSH key.

   Supported key encryption algorithms:

   - rsa-sha2-256
   - rsa-sha2-512
   - ecdsa-sha2-nistp256
   - ecdsa-sha2-nistp384
   - ecdsa-sha2-nistp521
   - ssh-ed25519
2. Request the public key from the user. The key string must contain the encryption algorithm and the key. Optionally, the string may contain a comment, such as a username and a host. Example: ssh-ed25519 AAAAC3... user@host.
3. Add the received key to this user in the Axidian Privilege administrator console.

X.509 Certificate

1. Ask the user to generate an X.509 certificate that does not have a certificate chain.

   Supported key encryption algorithms:

   - rsa-sha2-256
   - rsa-sha2-512
   - ecdsa-sha2-nistp256
   - ecdsa-sha2-nistp384
   - ecdsa-sha2-nistp521
   - ssh-ed25519
2. Request the certificate file from the user. Supported file extensions: PEM, DER, CRT.
3. Add the received file to this user in the Axidian Privilege administrator console.

Dumping Passwords

In an emergency, if the Axidian Privilege components fail, you can dump the privileged account passwords from the Axidian Privilege database.

Location of dump utility: `AxidianPAM_3.5\axidian-pam-tools\dump\Pam.Tools.Dump.exe`.

Editing the Configuration File

At first, open the utility config file `AxidianPAM_3.5\axidian-pam-tools\dump\appsettings.json` and specify the access parameters for the Core database:

`Database` section:

- `Database` — DBMS provider
  - `mssql` — Microsoft SQL Server
  - `pgsql` — PostgreSQL
- `PamCore` — DBMS connection string

MicrosoftSQL connection string

- `Data Source` — the name of the DBMS server or named instance
- `Initial Catalog` — database name
- `User ID` — database connection account
- `Password` — account's password

Other options available, see documentation for SqlClient 3.0 .NET Core

```
"PamCore": "Data Source=sql.domain.local; Initial Catalog=IPAMCore; Integrated
Security=False; User ID=IPAMSQLService; Password=password"
```

> ⚠ **CAUTION**
> If using a Named Instance of Microsoft SQL Server, the value of the Server parameter must be specified in the Server Name\Named instance format.
>
> ```
> "PamCore": "Data Source=sql\\instance; ..."
> ```

PostgreSQL connection string

- `Host` — the name of the DBMS server or named instance
- `Database` — database name
- `Username` — database connection account
- `Password` — account's password

Other options available, see documentation for Npgsql connection string

```
"PamCore": "Host=sql.domain.local; Database=IPAMCore; Integrated Security=False;
Username=IPAMSQLService; Password=password"
```

`Encryption` section:

- `Algorithm` — Core database encryption algorithm
- `Key` — Core database encryption key

Launching the Utility

The utility can be executed with the following arguments:

- `decrypt-ssh-key` — decrypting encrypted exported ssh key of the account
- `decrypt-password` — decrypting encrypted exported password of the account
- `decrypt-secrets` — decrypting credentials of accounts from specified or chosen folder
- `ssh-key` — dumping the SSH key of the account, you must specify the account, for example:
  `Pam.Tools.Dump.exe ssh-key --name res2\administrator`
- `password` — dumping the password of a privileged account, you must specify an account, for example:
  `Pam.Tools.Dump.exe password --name res2\administrator`
- `all-secrets` — dumping all credentials to the `.\Results` folder, or to the specified one. Passwords will be dumped to `accounts.csv` file, keys will be dumped to `sshKeys` folder in separate files. Example command:
  `Pam.Tools.Dump.exe all-secrets --output c:\temp`
- `help` — displaying more information of a specific command
- `version` — displaying version information

Usage of PostgreSQL and MSSQL Proxy

The MSSQL Proxy and PostgreSQL Proxy components allow opening SQL sessions through console and graphical clients. Text logging of SQL sessions is supported, which simplifies incident investigation.

> **INFO**
> A special license is required to connect to MSSQL and PostgreSQL resources.

DBMS Client Configuration

When connecting to a server and working with it through an SQL client, multiple sessions may be created. In this case, multiple sessions are also created in PAM, which causes inconvenience when viewing logs. To have one session within a single connection to the server, you need to configure the SQL client.

Configuration using the DBeaver client as an example:

1. Install the DBeaver client.
2. In the left part of the screen in the **Database Navigator** window, find the required server in the list of available connections.
   Right-click on it and select **Edit Connection** from the context menu.
3. In the window that opens, go to the **Metadata** tab and select the **Datasource <servername> settings** check box.
4. For the **Open separate connection for metadata read** parameter, select **Never** from the drop-down list.
5. Go to the **SQL Editor** tab and select the **Datasource <servername> settings** check box.
6. For the **Open separate connection for each editor** parameter, select the **Never** check box from the drop-down list.
7. Click **OK**.
8. Repeat the listed actions for all database servers.

Configure SSL encryption

> ⚠ **CAUTION**
> For correct operation, it is necessary to configure SSL both for the proxy and on the server.

PostgreSQL Proxy

To configure PostgreSQL Proxy operation via SSL, enable SSL usage in PostgreSQL Proxy and on the PostgreSQL Server. Follow these steps:

1. Open the PostgreSQL Proxy configuration file at `/etc/axidian-privilege/sql-proxy/appsettings.json`.
2. Set the `SslIsRequired` parameter value to `true` and save the changes.
3. Open the PostgreSQL Server configuration file `postgresql.conf`.
4. Set the `ssl` parameter value to `on`.
5. For the `ssl_cert_file =` parameter, specify the path to the SSL certificate.
6. Save the changes.

MSSQL Proxy

To configure MSSQL Proxy operation via SSL, enable SSL usage in MSSQL Proxy and on the Microsoft SQL Server. Follow these steps:

1. Open the MSSQL Proxy configuration file at `/etc/axidian/axidian-privilege/tsql-proxy/appsettings.json`.
2. Set the `SslIsRequired` parameter value to `true` and save the changes.
3. Open the SQL Server Configuration Manager client.
4. Expand the **SQL Server Network Configuration** tab and select the protocol for your SQL Server instance.
5. Set the **Force Encryption** parameter value to **Yes**.
6. Go to the **Certificate** tab and upload the SSL certificate.
7. Click **Apply** and **OK**.

Is interaction without SSL possible?

Yes, to do this, disable SSL usage in the proxy and on the server.

Specify MSSQL and PostgreSQL Proxy addresses

1. Go to **Configuration** → **System settings**.
2. Specify the proxy address in the PostgreSQL Proxy Address or MSSQL Proxy Address.

Open SQL session

To open an SQL session, go to the user console and connect to the resource via MSSQL Proxy or PostgreSQL Proxy.

Viewing Text Logs of SQL Sessions

> **INFO**
> SQL clients may save SQL query text differently. For example, psql cuts out comments from SQL queries, while pgAdmin keeps them.
>
> Only outgoing SQL queries (client → server) are captured in the text log, and their results are not saved.

To view text logs of a session opened via MSSQL Proxy or PostgreSQL Proxy:

1. Open the administrator console and go to the **Active sessions** section.
2. Select the required session.
3. Click **Text Log**.

To get the current text log, click **Refresh**.

If problems or errors occur during operation, collect PostgreSQL Proxy or MSSQL Proxy logs and contact technical support.

Limitations

- A user can open sessions via MSSQL Proxy and PostgreSQL Proxy only on behalf of a service account added to PAM with a password. The connection will not be established if the permission has selected:
  - a service account added to PAM without a password
  - a user service account for which credentials are requested when opening a session
- Two-factor authentication is supported only for installations with authentication through RADIUS, where the second factor is request confirmation in the application.
- For installations with authentication through PAM, the **Use two-factor authentication** parameter is ignored, meaning the second factor is not requested during connection.
- The user does not need confirmation from the administrator to open a session. Disable the Start of the sessions must be confirmed by PAM administrator parameter in the session policy, otherwise it is impossible to open an SQL session.
- When opening a session, users are required to enter the reason for connection if the User must specify the connection reason check box is selected in the session policy.

Usage of Web Proxy

The Web Proxy component provides secure access to web applications and websites through a browser without the need to use Microsoft RDS. An administrator can upload an SSO template to automatically fill in the login form on a web resource. This provides convenient access and does not reveal the password to the user.

No special licenses are required to work with Web Proxy.

Preliminary actions

1. Go to the **Configuration** → **System Settings** section and fill in the Web Proxy Address field.
2. Go to the **User Connection** subsection and add a user connection with the **Web Application** type and **In Browser** session opening method.
3. In the **Resources** section, open the resource profile and add the created user connection. You can add multiple connections with different URLs.
   Add a new resource if there is no suitable one in PAM.
4. In the resource profile, open the **Permissions** tab and make sure that permission has been granted for the resource. If permission has not been granted or you need to change the composition of users or the service account for connection, create a new permission.

Configure HTTPS connection

> ⓘ **INFO**
> The web resource certificate must be issued by a trusted CA.

To work with Web Proxy, a secure HTTPS connection is required. If a web resource has a self-signed certificate, this certificate is not trusted. When attempting to access such a resource, Web Proxy blocks the connection as it considers it unsafe.

To configure a secure connection:

1. Add the web resource's certification authority certificate to the folder `/etc/axidian/axidian-privilege/ca-certificates`.

2. Go to the folder with PAM scripts and restart the Web Access Server:

```
cd /etc/axidian/axidian-privilege/scripts/
```

```
sudo bash restart-pam.sh web-proxy
```

Open a session through the user console and connect to the web resource.

3. Verify that an HTTPS connection is established and the web resource opens.

Open a session through Web Proxy

To open a web session in a new browser tab or through an RDP file, go to the user console and connect to the resource through Web Proxy.

View logs

> **INFORMATION**
> Only video logging of the session is supported.

To view the video of a web session:

1. Open the administrator console and go to the **Active Sessions** section.
2. Select the desired session.
3. Expand the **Video** section.

If problems or errors occur when working with Web Proxy, collect the component logs and contact technical support.

Limitations

- The user does not need confirmation from the administrator to open a session.
- The clipboard is intended for text data only.
- Working with PDF files is not supported in web sessions. The file cannot be opened or sent to print.
- The settings Terminate session when there is no user activity and Opening sessions without re-authentication do not apply to web sessions.

- The address string in the web session is not available for editing. You won't be able to navigate to an arbitrary URL.
- There is no restriction on following links within a web session.
- HTTP Strict Transport Security (HSTS) cannot be configured for connections.
- Sessions opened through Web Proxy are not adapted for touch screens and mobile browsers.

Dashboard

The dashboard allows you to analyze user activity in real time. The dashboard contains widgets that display PAM summary data. The widgets allow you to navigate to other sections of the administrator console for more detailed analysis.

List of widgets

The following widgets are available in Axidian Privilege 3.5:

- Sessions
- PAM servers
- Permissions
- Accounts
- License usage
- Activity monitoring

INFO

To view and edit the dashboard, enable the claims *View page* and *Update page configuration*.

Sessions

The widget shows changes in the number of sessions, authentication errors, and credentials views. Analyze sessions and user actions to identify potential incidents, such as activity during non-working hours or recurring errors in sessions.

The graph can display data for an hour, day, or week and show the number of:

- Total sessions — total number of sessions.
- Sessions ended due to error — number of sessions terminated due to an error.
- Authentication errors — number of authentication errors in the user and administrator consoles.
- Credentials views — number of credentials views in the user console.

To go to the list of all sessions or sessions terminated due to an error, click Go to Sessions.

To go to the list of failed authentication attempts or credentials views, click Go to Events.

PAM servers

The widget shows the number of servers with installed Axidian Privilege components and their server state. It is important to monitor the health status of PAM components — in case of failure, you can promptly detect, alert, and remediate the issue.

For each Axidian Privilege component, a status is displayed:

- *Healthy* — all server components are functioning correctly.
- *Error* — a failure occurred in one or several components.
- *Pending* — checking the operation of an added or modified server.

To analyze component states in detail, go to the **PAM servers** widget and in the left menu select the desired server. If a component failure occurs, reveal the error and resolve it.

Add server to widget

If a new server with installed PAM components appears, add the server to the widget to monitor its state. To display the server state in the widget:

1. Go to the **PAM servers** widget.
2. In the left menu, click **Add PAM server**.
3. In the **Server address** field, specify the DNS name or IP address of the server.
4. Select the server's operating system.
5. Depending on the operating system, assign one or multiple roles to the server.
6. (Optional) Expand the setting **Change ports** and specify ports for each selected role.

   > ⚠ **CAUTION**
   > Ports are used to check the server's availability via the Healthcheck method. Change the ports only if non-default ports are specified in the PAM component configuration files.

7. Click **Check connection** and make sure the connection to the server is established. If an error occurs, ensure that the PAM components are installed on the server and the correct roles are selected.
8. Click **Add**.

The added server is displayed in the widget with the status *Pending*. Within a minute, the widget will display the server state and its components.

Edit Server Data

When changing the server configuration, such as adding a new role or updating the DNS name, enter the new data into the widget.

To modify server data:

1. Go to the **PAM Servers** widget.
2. Navigate to the tab with the required server and press **Edit**.
3. Make the necessary changes.

   > ⚠ **CAUTION**
   > Ports are used to check the server's availability via the Healthcheck method. Change the ports only if non-default ports are specified in the PAM component configuration files.

4. Click **Check Connection** and ensure that the connection to the server is established. If an error occurs, ensure that the PAM components are installed on the server and the correct roles are selected.
5. Click **Save**.

After editing, the server is displayed in the widget with the status *Pending*. Within a minute, the widget will display the server state and its components.

Remove a server from the widget

Removing a server only affects the widget display — the status of the removed server is not tracked.
To not display a server in the widget:

1. Navigate to the **PAM Servers** widget.
2. Navigate to the tab with the required server and press **Remove**.
3. In the confirmation window, click **Remove**.

Permissions

The widget shows the number of problematic or unused permissions. Keep permissions up to date: this ensures control over privileged access and reduces the risks of unauthorized actions.

What is tracked:

- Restricted permissions — the number of permissions with errors. Users cannot open sessions using such permissions. Restrictions occur for several reasons: no license, SSH fingerprint not set, user or service account unavailable. Fix the errors, revoke or recreate the permissions.
- Unused permissions — the number of permissions that have not been used within a specified time period. Revoke such permissions. The period after which permissions are considered unused can be configured in the Monitoring section.

To go to the detailed list of permissions, click ↗.

Service accounts

The widget shows the number and status of service accounts. Make sure that the necessary service accounts are under PAM management, and their passwords and SSH keys are updated in a timely manner. This will protect service accounts from unauthorized use bypassing PAM.

What is tracked:

- Pending — service accounts in the *Awaiting decision* state. PAM does not manage such service accounts. They can be used outside the system and bypass access control. Go to the service account profile and change its state to *Managed* or *Ignored*.
- Accounts with errors — service accounts that encountered errors when working with PAM. This could be a failure during password change or errors with SSH keys. Such service accounts are not updated and may not work as expected. Check the details and resolve the issue.
- Password and SSH key rotation not enabled in policy — service accounts for which credentials are not rotated. Such service accounts are vulnerable. Select the check box Periodically rotate service account password and SSH key.

To go to the detailed list of service accounts, click ↗.

Other service account states

Service account states:

- Managed — managed service account. PAM can store the password and SSH key for this account, grant permissions and launch sessions. When a service connection is available, credentials for this service account are checked and changed.
- Ignored — the service account does not participate in operations and synchronization. PAM knows about the existence of the service account, but does not store or manage its credentials.
- Blocked — the service account is unavailable for use.

Licenses

The widget shows the number of used and available licenses. Monitor the remaining licenses and their expiration date: without them, users cannot open sessions, and administrators cannot grant permissions.

For more information about licenses, see the Licensing section.

The following licenses are tracked:

- User — determines the number of users who can use Axidian Privilege.
- Resource — defines the number of resources that can be added to Axidian Privilege.
- AAPM — the number of accounts that can be granted permissions using the AAPM mechanism.
- SQL Proxy — defines the number of active permissions for resources with PostgreSQL or MSSQL type.
- Ad hoc resources — defines the number of custom resources for connection.

To go to the license list, click **More** in the upper right corner of the widget.

Activity control

The widget shows the number of inactive users. A user is considered inactive if they have not used their permissions within the period set by the administrator.

To go to the detailed list of users, click ↗

User Manual

User Console

Gain access to the User Console

Connection to the Resource

2 items

Authentication in SSH Proxy via SSH key

Authentication in SSH Proxy via SSH key

Additional Utilities

2 items

User Console

The User Console is a web application for accessing Axidian Privilege protected objects. Through the console, you can connect to a resource and open a session using active permissions. The console URL is formed from the Axidian Privilege domain name. Example address: `https://pam.domain.local/uc`.

The User Console contains several sections:

- **Resources** is the main section where permissions to connect to resources are displayed.
- **Accounts** is a list of account entries with the ability to view and edit passwords and SSH keys. The section displays only those account entries for which the **View account credentials** and/or **Manage account credentials** options are enabled in the permissions.
- **Applications** is a list of applications added to Axidian Privilege with the ability to view account data.
  Only application administrators can view passwords.

Two-factor authentication (2FA)

1. Open the User Console.
2. Enter the login in one of the formats:
   - john.smith@space.local — UPN format
   - SPACE\john.smith — domain\user format
   - john.smith — without the domain part

   If a user's login from an external directory matches an internal user's login, specify the login along with the domain to log in under the catalog account.
3. Enter the password and click **Log In**.
4. Enter the second factor of authentication and click **Log In**.

How to configure two-factor authentication

Set up two-factor authentication on your first login to the console.
To register an authenticator:

1. Install an OTP generation application.
2. Scan the QR code or enter the access key.
3. In the User Console, enter the one-time authentication code.
4. Click **Register**.

After registration, the console login form will appear. Enter the new code from the OTP generation application.

> ⚠ **CAUTION**
> After exceeding the number of incorrect OTP entry attempts, the user is blocked for 10 minutes by default. The number of attempts and the blocking time are set by the administrator in the Configuration → User Authentication section.

To exit the console, in the top right corner, click on the login and select **Sign Out**.

Change PAM User Password

An internal Axidian Privilege user can independently change their password.
To change the password:

1. Authenticate in the User Console.
2. In the top right corner, click on the login.
3. In the drop-down list, select **Change Password**.
4. In the window that opens, enter the current and new password.
5. (Optional) Set the **Terminate all active sessions** option.
6. Click **Change Password**.

Working with Folders

Folders help organize work in the console. Group resources by the desired attribute, for example, by department or connection type. To display the menu with folders, in the Resources section click » and select the required action:

- — create a new folder
- — edit the name of the selected folder
- — delete the selected folder

To add a resource to a folder:

1. Go to the **Resources** section and click **All Resources** or **Resources without a folder**.
2. Select one or more resources and click **Move**.

> **INFO**
> Ad hoc resources cannot be added to a folder.

3. Select the required folder and click **Save**.

Find a resource, account, or application

To find a resource:

1. Go to the **Resources** section.
2. Click » and in the expanded menu select where to search for the resource.
3. In the search bar, enter the resource name, account name, type, connection address, or tag.

> **INFO**
> Ad hoc resources can be found by the query «adhoc».

To find an account or application:

1. Go to the **Accounts** or **Applications** section.
2. In the search bar, enter the account or application name.

View credentials

In the user console, viewing of passwords and SSH keys for accounts that have the **Allow view account credentials** permission enabled is available. To view credentials:

1. Go to the **Accounts** section.
2. Click **View credentials** next to the required account.
3. Enter the reason for viewing and click **View credentials**.

Only their administrators can view application credentials.
To view an application password:

1. Go to the Applications section.
2. Click **View credentials** next to the required application.
3. Enter the reason for viewing and click **View credentials**.

Change a password or SSH key

If a user has manually changed the password or SSH key for an account on the resource, these credentials must be updated in the PAM database. Access to the resource is only possible with valid credentials—if the data stored in PAM is outdated, the session will not be established.

> ⓘ **INFO**
> The user console does not allow changing the password or SSH key on the resource itself: only the credentials stored in PAM can be updated.
>
> Credentials can only be updated for accounts that have the **Allow change account credentials** option enabled in the permission.

To update credentials:

1. Go to the **Accounts** section.
2. Click ▼ and select the required action:
    - **Change password** — enter the new password and confirm it.

- **Change SSH key** — select the SSH key file and enter its password.
  RSA keys in OpenSSH and PEM formats are supported, as well as Ed25519 in OpenSSH format.

  How to generate an SSH key

  To create an SSH key and save it to a file, use the PuTTYgen program or one of the commands:

  The RSA key in the OpenSSH format

  ```
  ssh-keygen -t rsa -b 4096 -f id_rsa_openssh -C "RSA OpenSSH key"
  ```

  The RSA key in the PEM format

  ```
  ssh-keygen -t rsa -b 4096 -f id_rsa_pem -C "RSA PEM key" -m PEM
  ```

  The Ed25519 key in the OpenSSH format

  ```
  ssh-keygen -t ed25519 -f id_ed25519_openssh -C "Ed25519 OpenSSH key"
  ```

3. Specify the reason for changing the password or SSH key and click **Save**.

Connection to the Resource

RDP, SSH, Web and SQL Connection

Learn about ways to connect to resources

SCP/SFTP Connection to the Resource

3 items

RDP, SSH, Web and SQL Connection

The Axidian Privilege user console displays permissions to access resources. Sorting is available for each column except the **Tags** column. When searching, matches are displayed across all columns.

If the user has access to ad hoc resources, they are displayed at the top of the list.

Connection to a Resource via RDP

Connect to a resource using an RDP file or open a session in a new browser tab through the Web terminal.

RDP file

1. Click ▼ next to the permission and select **Download RDP connection file**.
2. Open the downloaded file and authenticate as an Axidian Privilege user.
   If the administrator has enabled an authentication code, credentials do not need to be entered.
3. (Optional) Specify a reason for the connection if required by the policy.
4. Authenticate on the resource:
   - If the permission specifies an account, login is performed on behalf of that account.
   - If the permission is granted for a user account and authentication in Axidian Privilege was completed as a PAM user, their login and password are auto-filled in the resource login form.

> ⓘ **NOTE**
> If authentication codes are enabled, enter the user password when reusing the RDP file.

Web Terminal

1. Click ▼ next to the permission and select **Open via Web terminal**.
2. Authenticate as an Axidian Privilege user.
   If the administrator has enabled an authentication code, credentials do not need to be entered.
3. (Optional) Specify a reason for the connection if required by the policy.

4. Authenticate on the resource:
    - If the permission specifies an account, login is performed on behalf of that account.
    - If the permission is granted for a user account and authentication in Axidian Privilege was completed as a PAM user, their login and password are auto-filled in the resource login form.

The session opens in a new browser tab. To terminate the session, close the tab.

> **CLIPBOARD AND FILE TRANSFER**
> The clipboard supports text data only.
> You can transfer files between your workplace and a Windows resource by using drag-and-drop.
>
> **How to transfer files through the Web terminal**
>
> **Upload a file to the resource**
>
> Drag the files or folders you need from your workplace into the RDP session area. The files appear on the forwarded drive `G:`, from where you can move them to the required location on the resource.
>
> **Download a file from the resource**
>
> On the resource, open the Web terminal forwarded drive, go to `G:\Download`, and move the files or folder you need there. The browser automatically downloads the files to the `Downloads` folder on your workplace.

Connection to the Access Gateway

The access gateway accepts the user's connection and displays a list of resources available for launching a session.

RDS gateway

1. Click **Connect to the access gateway**, the download of the RDP file will begin.
2. Run this RDP file.

3. Authenticate and set up the connection.

SSH gateway

Connect to the SSH gateway from the command line or using an SSH client.

Command line

1. Open the console utility.
2. Enter the IP address or DNS name to connect to the SSH access server or load balancer. To find out the address, go to the user console and copy the SSH command to any resource. Use the value specified after the `@` symbol. If required, specify the path to the private key.

   Template of SSH Proxy Connection Command

   ```
   ssh <user login>@<IP address or DNS name> -p <port number> -i <path to private key>
   ```

   Example of SSH Proxy Connection Command

   ```
   ssh user@axidianproxy -p 2222 -i "C:\Users\user\.ssh\id_ed25519"
   ```

3. Complete authentication. If SSH key authentication is configured, skip this step.
4. Select a resource and connect.

PuTTY

Authentication via Password

1. Open the PuTTY app.
2. In the **Host Name (or IP address)** field, enter the SSH Proxy or the load balancer address. You can use an IP address or DNS. To find out the SSH Proxy address, copy the SSH command of any resource in the user console and take the value specified after the @ character.
3. Optionally specify the port in the **Port** field.
4. In the **Connection type** field, select *SSH*.

5. Click **Open**.
6. Enter user login.
7. Enter the password.
8. Enter OTP.
9. Select a resource and connect.

Authentication via SSH Key

> ⚠ **CAUTION**
> This method is possible only if SSH key authentication is configured and the key is generated by the PuTTYgen utility.

1. Open the PuTTY app.
2. In the **Host Name (or IP address)** field, enter the SSH Proxy or the load balancer address. You can use an IP address or DNS. To find out the SSH Proxy address, copy the SSH command of any resource in the user console and take the value specified after the @ character.
3. Optionally specify the port in the **Port** field.
4. In the **Connection type** field, select *SSH*.
5. Open **Connection** → **Data**. Enter user login in **Auto-login-username** field.
6. Open **Connection** → **SSH** → **Auth** → **Credentials**. Specify the private key in the **Private key file for authentication** field.
7. Click **Open**.
8. Enter OTP.
9. Select a resource and connect.

Certificate Authentication

> ⚠ **CAUTION**
> This method is available only if SSH key authentication is configured and PuTTY CAC is installed.

1. Open the PuTTY app.
2. In the **Host Name (or IP address)** field, enter the SSH Proxy or the load balancer address. You can use an IP address or DNS. To find out the SSH Proxy address, copy the SSH command of any resource in the user console and take the value specified after the @ character.

3. Optionally specify the port in the **Port** field.
4. In the **Connection type** field, select *SSH*.
5. Open **Connection** → **Data**. Enter user login in **Auto-login-username** field.
6. Open **Connection** → **SSH** → **Certificate**. Click **Set CAPI Cert**.
7. Click **Open**.
8. Enter OTP.
9. Select a resource and connect.

MobaXterm

> ⚠ **CAUTION**
> In MobaXterm versions earlier 23.0, you need to disable the **Fix connection issues** option in the **Settings** → **Configuration** → **SSH** section.

Authentication via Password

1. Open the MobaXterm app.
2. Click **Sessions** → **New Session**.
3. Select **SSH**.
4. In **Remote host** specify the SSH Proxy or the load balancer address. You can use an IP address or DNS. To find out the SSH Proxy address, copy the SSH command of any resource in the user console and take the value specified after the @ character.
5. Enable the **Specify username** option and enter the username.
6. Optionally specify the port in the **Port** field.
7. Click **OK**.
8. Enter the password.
9. Enter OTP.
10. Select a resource and connect.

Authentication via SSH Key

> ⚠ **CAUTION**
> This method is possible only if SSH key authentication is configured.

1. Open the MobaXterm app.
2. Click **Sessions** → **New Session**.

3. Select **SSH**.
4. In **Remote host** specify the SSH Proxy or the load balancer address. You can use an IP address or DNS. To find out the SSH Proxy address, copy the SSH command of any resource in the user console and take the value specified after the @ character.
5. Enable the **Specify username** option and enter the username.
6. Optionally specify the port in the **Port** field.
7. Click the **Advanced SSH Settings** tab.
8. Enable the **Use private key** option and specify the private key in this field.
9. Click **Expert SSH settings**.
10. In the **SSH protocol version** field, specify *SSHv2*.
11. Click **OK**.
12. Enter OTP.
13. Select a resource and connect.

SecureCRT

Authentication via Password

1. Open the SecureCRT app.
2. Click **File** → **Quick Connect**.
3. In the **Protocol** field, select *SSH2*.
4. In the **Hostname** field, specify the SSH Proxy or the balancer address. You can use an IP address or DNS. To find out the SSH Proxy address, copy the SSH command of any resource in the user console and take the value specified after the @ character.
5. Optionally specify the port in the **Port** field.
6. In the **Username** field, enter the username.
7. Click **Connect**.
8. Enter the password.
9. Enter OTP.
10. Select a resource and connect.

Authentication via SSH Key

1. Open the SecureCRT app.
2. Click **File** → **Quick Connect**.
3. In the **Protocol** field, select *SSH2*.

4. In the **Hostname** field, specify the SSH Proxy or the balancer address. You can use an IP address or DNS. To find out the SSH Proxy address, copy the SSH command of any resource in the user console and take the value specified after the @ character.
5. Optionally specify the port in the **Port** field.
6. In the **Username** field, enter the username.
7. In the **Authentication** group, enable the **PublicKey** option and disable all others.
8. Select **PublicKey** with the mouse and click ⚙.
9. Select the **Use session public key setting** option.
10. Specify the private key in the **Use identity or certificate file** field.
11. Click **OK**.
12. Click **Connect**.
13. Enter OTP.
14. Select a resource and connect.

Connection to a Resource via SSH

Connect to the resource using the command line, SSH client, or start an SSH session in a new browser tab via a Web Terminal.

Command Line

1. Click ▼ next to the permission and select **Copy SSH command**.
2. Run the copied command in the terminal.
   If you need to specify a reason for the connection, add it to the command after the username.

   Example command with a reason

   ```
   ssh "pamadmin@pam.local#10.10.1.191#LINUX-PAM.LOCAL\pam-admin#reason-for-connection#@pam.axidian-id.hq" -p 2222
   ```

3. Authenticate as an Axidian Privilege user.
   If the administrator has enabled an authentication code, credentials do not need to be entered.

Example command with a reason and an authentication code

```
ssh "pamadmin@pam.local#10.10.1.191#LINUX-PAM.LOCAL\pam-admin#reason-for-connection#ZO3nNVdBFMKIGEs@pam.axidian-id.hq" -p 2222
```

4. Authenticate on the resource:

   - If the permission specifies an account, login is performed on behalf of that account.
   - If the permission is granted for a user account and authentication in Axidian Privilege was completed as a PAM user, their login and password are auto-filled in the connection string.
     To log in to the resource, press **Enter** twice.

> **NOTE**
> If authentication codes are enabled, enter the user password when reusing the command.

Connection using a command with additional parameters

You can write an SSH command manually using the template below.

1. Write an SSH command using the following template:

   SSH command template

   ```
   ssh [user-name]#[resource]#[account-name]#[reason]@[proxy-address]
   ```

   - `user-name` — username
   - `resource` — IP address or DNS name of the resource
   - `account-name` — name of the privileged account
   - `reason` — connection reason text; if the reason contains spaces, enclose it in quotes
   - `proxy-address` — IP address or DNS name of the SSH Proxy server

   Any parameter except `proxy-address` can be omitted. In this case, SSH Proxy will prompt for these parameters separately.

2. Run the command in the terminal.

3. Authenticate.

Web terminal

To open an SSH session in a new browser tab:

1. Click ▼ next to the permission and select **Open via Web terminal**.
2. Authenticate as an Axidian Privilege user.
   If the administrator has configured an authentication code, credentials do not need to be entered.
3. (Optional) Specify a reason for the connection if required by the policy.
4. Authenticate on the resource:
   - If the permission specifies an account, login is performed on behalf of that account.
   - If the permission is granted for a user account and authentication in Axidian Privilege was completed as a PAM user, their login and password are auto-filled in the connection string.
     To log in to the resource, press **Enter** twice.

The session opens in a new browser tab. To terminate the session, close the tab.

> ⓘ **CLIPBOARD LIMITATIONS**
> The clipboard supports text data only.

PuTTY

1. In the user console, to the right of the permission to the SSH resource, click **Copy SSH command**.
2. Open the PuTTY app.
3. Paste the copied line in the **Host Name (or IP address)** field. Remove the ssh, quotes, and port from this line.
4. Specify the port in the **Port** field.
5. Click **Open**.
6. Enter your password and OTP.

MobaXterm

1. Open the MobaXterm app.
2. Click **Sessions** → **New Session**.

3. Select **SSH**.
4. In **Remote host** specify the SSH Proxy or the load balancer address. You can use an IP address or DNS. To find out the SSH Proxy address, copy the SSH command of any resource in the user console and take the value specified after the @ character.
5. Enable the **Specify username** option.
6. Enter username. You can specify it in the format:
   `[user-name]#[resource]#[account-name]#[reason]`

   Example of specifying additional parameters in a username

   ```
   VDD\alex.shushkin#cent9en.vdd.com#CENT9EN\local##
   ```

7. Optionally specify the port in the **Port** field.
8. Click **OK**.
9. Enter your password and OTP.

SecureCRT

1. Open the SecureCRT app.
2. Click **File** → **Quick Connect**.
3. In **Protocol** field select *SSH2*.
4. In the **Hostname** field, specify the SSH Proxy or the balancer address. You can use an IP address or DNS. To find out the SSH Proxy address, copy the SSH command of any resource in the user console and take the value specified after the @ character.
5. In the **Username** field, specify the username.
   You can specify it in the format: `[user-name]#[resource]#[account-name]#[reason]`

   Example of specifying additional parameters in a username

   ```
   VDD\alex.shushkin#cent9en.vdd.com#CENT9EN\local##
   ```

6. Click **Connect**.
7. Enter your password and OTP.

Connection to a Resource via PostgreSQL Proxy

> ⚠ **CAUTION**
>
> A special license is required to connect to the PostgreSQL resource.

Psql CLI

1. Click ▼ next to the permission and select **Copy Psql connection command**.
2. Run the copied command in the terminal.
   If you need to specify a reason for connection, enter it in the command after the username.

   Example of a command without a reason

   ```
   psql "postgresql://pamadmin%40pam.local%2310.10.1.105%23POSTGRESQL%5CAdmin@pam.axidian-id.hq:5432/postgres"
   ```

   Example command with a reason

   ```
   psql "postgresql://pamadmin%40pam.local%2310.10.1.105%23POSTGRESQL%5CAdmin%23reason-for-connection@pam.axidian-id.hq:5432/postgres"
   ```

3. Complete authentication. If the administrator has configured session opening without re-authentication, credentials do not need to be entered.

   Example command with a reason and an authentication code

   ```
   psql "postgresql://pamadmin%40pam.local%2310.10.1.105%23POSTGRESQL%23reason-for-connection%230C6XI9IrGx:nopassword@pam.axidian-id.hq:5432/postgres"
   ```

   > ⓘ **INFO**
   >
   > If authentication codes are enabled, when you reuse the command, remove the authentication code and the `:nopassword` argument from it. When you connect to the resource, you will be prompted for the user's password.

GUI DBMS Client

1. Open the user console of Axidian PAM.
2. Click **Show connection credentials**.
3. Open your DBMS client and enter into its connection form the data you received in the previous step:
   - **Connection Address**
   - **Connection Port**
   - **Account Name**
   - **Default Database**
4. If the **User must specify the connection reason** option is enabled in the session policy, then add the connection reason text to the **Account Name** field.

   Example: if the **Account Name** value was `admin@company.local#1.1.1.1#MYCOMPANY\test-admin`, after the reason was added it will read as: `admin@company.local#1.1.1.1#MYCOMPANY\test-admin#"my reason to connect"`.

   If this option is disabled, skip this step.
5. In the connection form, enter the password of your PAM account.

Connection to a Resource via MSSQL Proxy

> ⚠ **CAUTION**
> A special license is required to connect to the MSSQL resource.

Sqlcmd CLI

1. Click ▼ next to the permission and select **Copy sqlcmd connection command**.
2. Run the copied command in the terminal.
   If you need to specify a reason for connection, enter it in the command after the username.

Example of a command without a reason

```
sqlcmd -S pam.local,8081 -U ivan.ivanov#SQL -d master
```

Example command with a reason

```
sqlcmd -S pam.local,8081 -U ivan.ivanov#SQL#MSSQLuser#reason-for-connection -d master
```

3. Complete authentication. If the administrator has configured session opening without re-authentication, credentials do not need to be entered.

Example command with a reason and an authentication code

```
sqlcmd -S pam.local,8081 -U ivan.ivanov#SQL#MSSQLuser#reason-for-
connection#C6XI9IrGx:nopassword -d master
```

> **INFO**
> If authentication codes are enabled, when you reuse the command, remove the authentication code and the `:nopassword` argument from it. When you connect to the resource, you will be prompted for the user's password.

GUI DBMS Client

1. Open the user console of Axidian PAM.
2. Click **Show connection credentials**.
3. Open your DBMS client and enter into its connection form the data you received in the previous step:
   - **Connection Address**
   - **Connection Port**
   - **Account Name**
   - **Default Database**
4. If the **User must specify the connection reason** option is enabled in the session policy, then add the connection reason text to the **Account Name** field.

Example: if the **Account Name** value was `admin@company.local#1.1.1.1#MYCOMPANY\test-admin`, after the reason was added it will read as: `admin@company.local#1.1.1.1#MYCOMPANY\test-admin#"my reason to connect"`.

If this option is disabled, skip this step.

5. In the connection form, enter the password of your PAM account.

Connection to a Resource via Web Proxy

Connect to the web application or website via a Web Proxy from the user's console.

Open in new tab

To open a web resource in a new browser tab:

1. Click **Open in new tab** next to the required permission.
2. Specify the reason for the connection and click **Confirm**.

The session opens in a new browser tab. To terminate the session, close the tab.

> **CLIPBOARD LIMITATIONS**
> The clipboard supports text data only.

RDP file

1. Click ▼ next to the permission and select **Download RDP connection file**.
2. Open the downloaded file and authenticate as an Axidian Privilege user.
   If the administrator has enabled an authentication code, credentials do not need to be entered.
3. (Optional) Specify a reason for the connection if required by the policy.
4. Authenticate on the resource:
   - If the permission specifies an account, login is performed on behalf of that account.
   - If the permission is granted for a user account and authentication in Axidian Privilege was completed as a PAM user, their login and password are auto-filled in the resource login form.

> ⓘ **NOTE**
> If authentication codes are enabled, enter the user password when reusing the RDP file.

Connection to an Ad Hoc Resource

Ad hoc resources are resources that are not registered in the Axidian Privilege system. This type of connection makes it possible to connect to any resources according to connection types predefined by the PAM administrator.

> ⚠ **CAUTION**
> A special license is required to connect to the ad hoc resource.

1. Click **Specify connection address** to the right of the required permission to the ad hoc resource.
2. Select **Connection type**.

   > ⓘ **INFO**
   > The available connection types are determined by the PAM administrator when granting permissions.

3. Enter **Connection address**.
4. Depending on the selected connection type, click one of the buttons: **Copy SSH command** or **Download RDP file**.

> ⓘ **INFO**
> If you have several permissions (with different connection types) to an ad hoc resource, and in the **Connection to an ad hoc** resource window in the **Connection type** field there are no required options, then check the **Permission Access Schedule**.
>
> The connection type will not be displayed in the **Connection type** field if you are trying to connect via permission outside the hours specified in the **Permission Access Schedule**.

Setting a Password During Connection

When connecting to the resource, you may be asked for a password.

This means that the account on whose behalf you are granted access to the resource does not have a password. You cannot connect to the resource with such an account. Contact your PAM administrator, as only an administrator can set an account password.

Ending a Session

To end the session, close the remote connection window or log off the resource.

SCP/SFTP Connection to the Resource

Command Line

Connection via SCP, SFTP, PSCP, PSFTP

WinSCP

Connection via WinSCP

FileZilla

Connection via FileZilla

Command Line

SCP

> **NOTE**
> On devices running Windows Server 2019, Windows 10 1809 and higher, the SCP command is included in the pre installed OpenSSH client.

For transferring files using SCP protocol, you can use **scp** utility built into the OS. Use the standard command to copy, but instead of the resource address, specify the SSH Proxy address:

For Windows:

```
scp -r C:\temp\configs\ james.miller.axidian.local:/tmp

scp -r C:\path_to_local_file user_name@address_ssh_proxy:/path_to_copy_on_resource
```

For Linux:

```
scp -r /tmp james.miller@sshproxy.axidian.local:/tmp

scp -r /path_to_local_file user_name@address_ssh_proxy:/path_to_copy_on_resource
```

Parameter -r means recursive copying. i.e. copy entire directories.

In the next step, after successful authentication, select the resource for file transfer.

SFTP

For transferring files you can use **sftp** utility on devices running on Windows

For transferring files:

1. Run a Command Line
2. Connect to the SSH Proxy server

```
sftp james.miller@sshproxy.axidian.local
```

3. Select a resource for connection
4. Transfer files using the command:

```
put -r C:\temp\configs\ /tmp
put -r path_to_local_files path_to_files_on_resource
```

Parameter -r means recursive copying. i.e. copy entire directories.

PSCP

> ⓘ **NOTE**
> For the PSCP and PSFTP commands the PuTTY package must be installed on the device

For transferring files you can use **pscp** utility on devices running on Windows

Command for transferring files:

```
pscp -r C:\temp\configs\ james.miller@sshproxy.axidian.local:/tmp

pscp -r C:\path_to_local_file user_name@address_ssh_proxy:/path_to_copy_on_resource
```

Parameter -r means recursive copying. i.e. copy entire directories.

PSFTP

For transferring files you can use **psftp** utility on devices running on Windows

1. Run a Command Line
2. Enter command psftp
3. Connect to the SSH Proxy server

```
open james.miller@sshproxy.axidian.local
```

4. Select a resource for connection
5. Transfer files using the command:

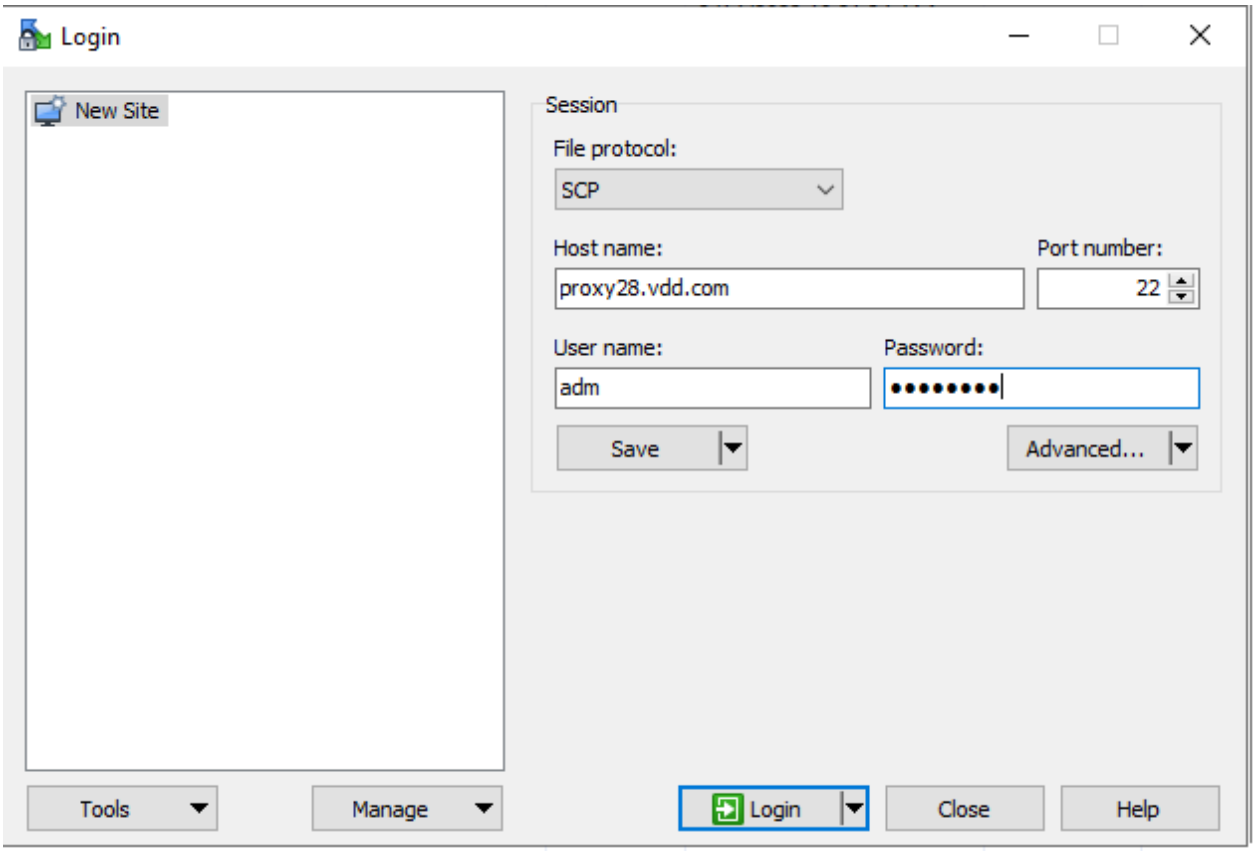
```
put -r C:\temp\configs\ /tmp/configs
put -r path_to_local_files path_to_files_on_resource
```

Parameter -r means recursive copying. i.e. copy entire directories. Also necessary to specify the name of the file that will be saved on the resource.

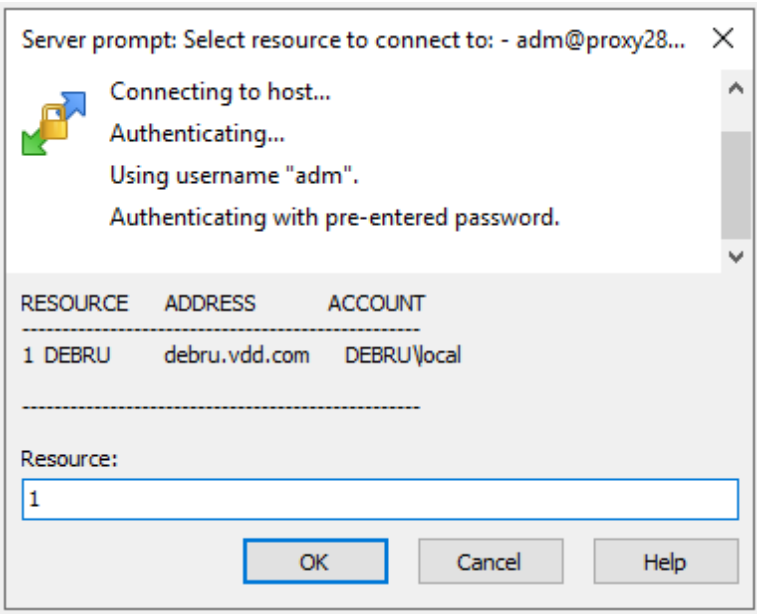
WinSCP

Connecting via Access Gateway

1. Open WinSCP client.
2. Select "File protocol" **SCP** or **SFTP**. Enter the address and port of the SSH Proxy server in the "Host Name" and "Port number". Enter login and password in the "User name" and "Password".



3. Click **Login** button and select a resource to connect to.

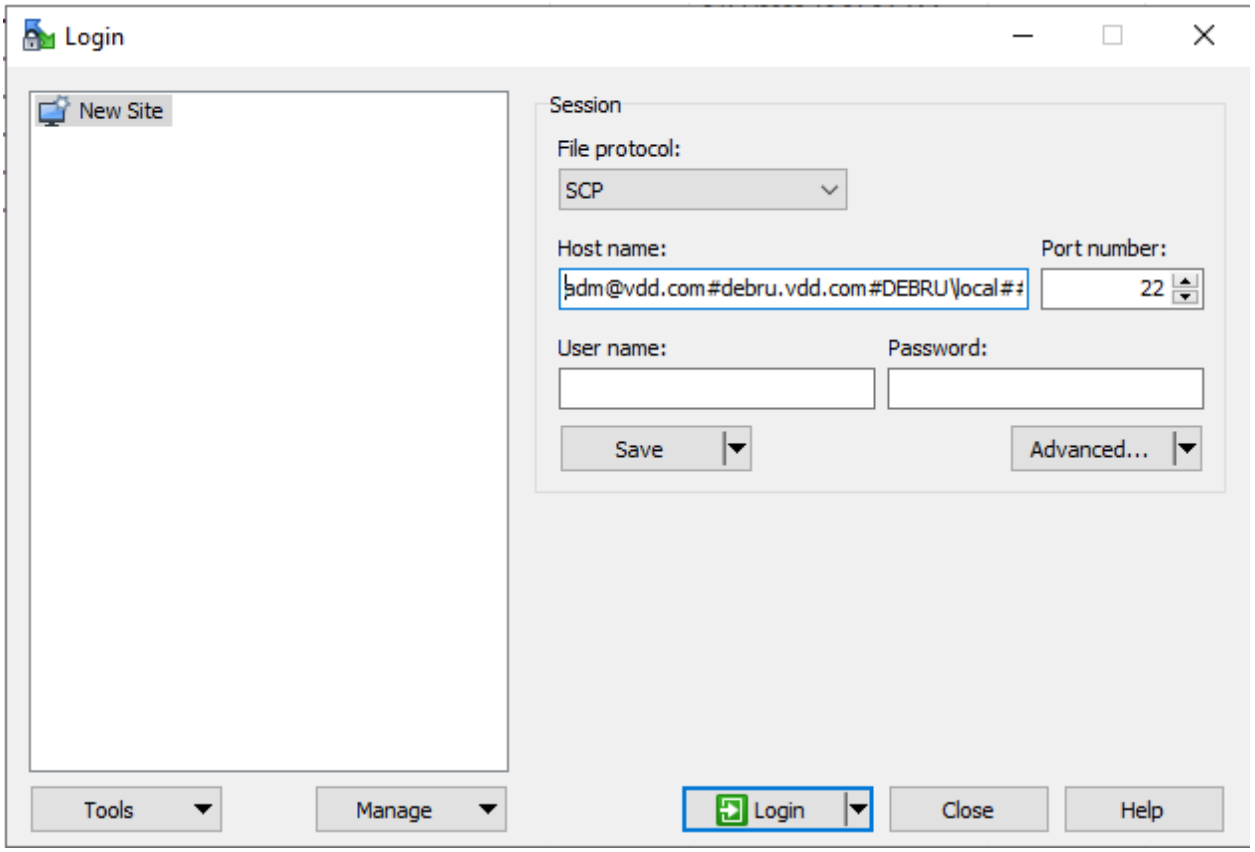


Direct Connection to the Resource

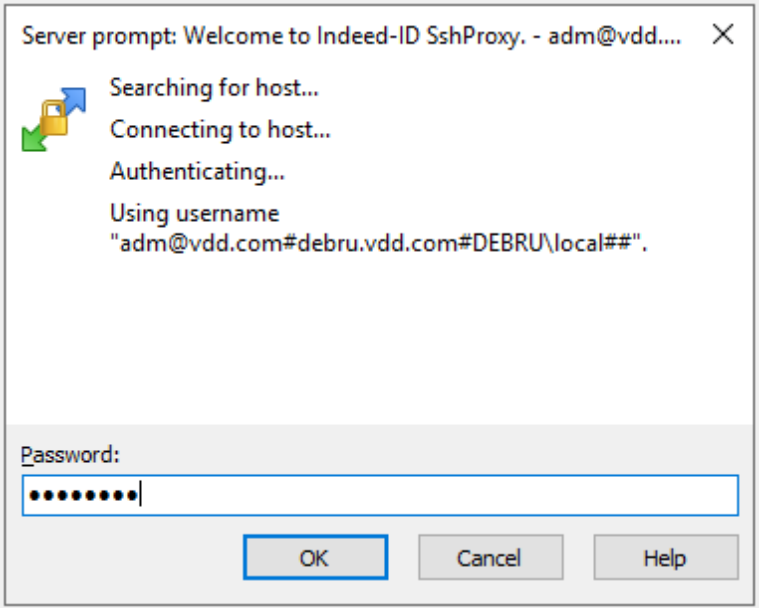
1. Open **User Console** and copy connection string to the resource.

2. Select "File protocol" **SCP** or **SFTP**. Insert the connection string into the "Host name", removing the quotes and "ssh" from the string. The connection string should look like this:

```
adm@vdd.com#debru.vdd.com#DEBRU\local##@proxy28.vdd.com
```



3. Enter the password.



FileZilla

SFTP Connection to a Resource

To configure SFTP connection in FileZilla follow these steps:

1. Go to **File** → **Site Manager** → **New site.**
2. Fill the **General** section:
    - Protocol: SFTP — SSH File Transfer Protocol
    - Host: Address of SSH Proxy server
    - Port: Port of SSH Proxy server
    - Logon Type: Interactive
    - User: connection string, copied from UC to connect to the resource. ("SSH" and quotation marks must be removed from the string)
3. Open **Transfer Settings** section and enable **Limit number of simultaneous connections** parameter. Set value of **Maximum number of connections** equal 1.
4. Click the **Connect** button.

> ⓘ **NOTE**
> FileZilla does not support TCP connection.

Authentication in SSH Proxy via SSH key

Users can connect to SSH Proxy using SSH keys. This method ensures secure and fast login to SSH Proxy without the need to use passwords. To check if this authentication method is available to you, contact your PAM administrator.

SSH key in text format

To connect to SSH Proxy, you need to generate an SSH key and pass a public key to the PAM administrator. The method of generation depends on the client used to connect to SSH Proxy. When using cmd, generate a key with the ssh-keygen utility. When using PuTTY, generate a key with the PuTTYgen utility. When using MobaXterm, any method is suitable.

Key generation with the ssh-keygen utility

1. Generate an SSH key.

   Supported key encryption algorithms:

   - rsa-sha2-256
   - rsa-sha2-512
   - ecdsa-sha2-nistp256
   - ecdsa-sha2-nistp384
   - ecdsa-sha2-nistp521
   - ssh-ed25519

Template and example command for generating an SSH key

Template

```
ssh-keygen -t <algorithm>
```

Example

```
ssh-keygen -t ssh-ed25519
```

2. Pass the public key to the PAM administrator. The key string must contain the encryption algorithm and the key. Optionally, the string may contain a comment, such as a username and a host. Example: ssh-ed25519 AAAAC3... user@host.

3. Wait for the administrator to configure the connection via an SSH key.

4. Connect to SSH Proxy.

> **INFO**
> It is recommended to place the SSH key in the `.ssh` folder. For example, `C:\Users\user\.ssh` for Windows and `/home/user/.ssh` for Linux.
>
> It is recommended to keep the default name of the key. For example, *id_rsa*, *id_ecdsa*, *id_ed25519*.
>
> If the key files are located in a different place or their names differ from the standard ones, then when connecting to SSH Proxy, you need to specify the path to the private key.

Key generation with the PuTTYgen utility

1. Open PuTTYgen.
2. In the **Type of key to generate** field select one of the values: RSA, ECDSA nistp-256, ECDSA nistp-384, ECDSA nistp-521, EdDSA Ed25519.
3. Click **Generate**.
4. Move the mouse in the empty area of the PuTTYgen window until the key generation is complete.

5. Clear the **Key comment** field and enter the username and host in the user@host format. To find out the username and host, run the command in the terminal:

   ```
   whoami
   ```

6. Save the text from the **Public key for pasting into OpenSSH authorized keys file** field.
7. Click **Save private key**.
8. In the pop-up window, click **Yes**.
9. Specify a file name, for example *key-private*.
10. Then click **Save**.
11. Pass the public key to the PAM administrator. The key string must include the encryption algorithm, key, username, and host. Example: ssh-ed25519 AAAAC3... user@host.
12. Wait for the administrator to configure the connection via an SSH key.
13. Connect to SSH Proxy.

X.509 certificate

To connect to SSH Proxy, you need to generate a certificate with an SSH key and pass a public key to the PAM administrator.

1. Generate an X.509 certificate that does not have a certificate chain.

   Generation Instructions

   1. Open the Manage user certificates snap-in, and then open **Personal** → **Certificates**.
   2. Right-click the Certificates folder. Select **All Tasks** → **Request a new certificate**.
   3. Click **Next**.
   4. Select a certificate enrollment policy and click **Next**.
   5. Select a certificate.
   6. Click **Request**.

2. Export the certificate.

Export Instructions

1. Open the Manage user certificates snap-in, and then open **Personal** → **Certificates**.
2. Right-click on the certificate that was generated in the previous step. Select **All Tasks** → **Export**.
3. In the window that opens, click **Next**.
4. Select the **X.509 Files option (.CER) encoded DER**.
5. Select the file location and fill in **File Name**. Click **Next**.
6. Check your entered data and click **Done**.

3. Pass the certificate file to the PAM administrator. Supported file extensions: PEM, DER, CRT.

4. Wait for the administrator to configure the connection via an SSH key.

5. Connect to SSH Proxy.

Additional Utilities

Usage of PamSu

Learn how to run a command if sudo is needed

Usage of Desktop Console

Learn about Axidian Privilege Desktop Console

Usage of PamSu

To execute commands with root privilege, the pamsu command is used similarly to sudo. The difference is that authentication will be requested from the Axidian Privilege user, and not by the privileged account.

The command with arguments must be preceded by two hyphens. For example:

```
[administrator@centos7 ~]$ pamsu -- ls -la /etc/ssl
Password for axidian\james.miller:
total 12
drwxr-xr-x. 4 root root 68 Sep 22 19:20 .
drwxr-xr-x. 75 root root 8192 Sep 22 17:49 ..
drwxr-xr-x. 2 root root 123 Sep 22 19:30 CA
lrwxrwxrwx. 1 root root 21 Sep 22 15:51 cert.pem -> /etc/pki/tls/cert.pem
lrwxrwxrwx. 1 root root 16 Nov 23 2020 certs -> ../pki/tls/certs
[administrator@centos7su ~]$
[administrator@centos7su ~]$ pamsu vi /etc/resolv.conf
```

Usage of Desktop Console

To learn how to install and setup Desktop Console utility, read this article.

To start Desktop Console utility, make sure you are logged on with Active Directory account (otherwise, run Desktop Console utility as an Active Directory user account), double-click the **Axidian Privilege Desktop Console** shortcut, Axidian Privilege authentication window appears. Register or enter TOTP code. After successful authentication you will see the available resources in the **Connections** pane.

To open connection double-click the desired resource (also you can right-click it and choose **Connect** menu item) and complete the authentication. You can open multiple connections at the same time.

Automation

Integration with Ansible

2 items

AAPM Reference

3 items

ConsoleApp

The utility allows you to automatically manage Axidian Privilege objects and configure access permissions

Integration with Ansible

Ansible Lookup Plugin

The plugin allows you to manage Axidian Privilege credentials directly in Ansible playbooks

Connecting via SSH Proxy

Configuring Ansible connections to resources through the Axidian Privilege proxy server

Ansible Lookup Plugin

With Lookup Plugin, you can manage Axidian Privilege credentials directly in Ansible playbooks. All requests to retrieve and view credentials are logged in the Events journal.

> **NOTE**
> Application to Application Password Management (AAPM) method is used to manage Axidian Privilege account credentials.

Requirements

The following is required to work with Ansible Lookup Plugin:

- Python 3.9 or higher
- Ansible 2.14 or higher
- AAPM license

Prerequisites

To set up Ansible Lookup Plugin:

1. Go to the AAPM Python SDK package folder at `AxidianPAM_3.5/axidian-pam-tools/aapm` and execute the command:

   ```
   pip install pam_aapm-3.5.0-py3-none-any.whl
   ```

2. Go to the Lookup Plugin distribution directory at `AxidianPAM_3.5/axidian-pam-tools/ansible-lookup-plugin` and run the command:

   ```
   ansible-galaxy collection install axidian-ansible-lookup-plugin-3.5.0.tar.gz
   ```

3. Open the Axidian Privilege administrator console and add an application.

4. For the application, create a permission with the **Allow view account credentials** option enabled.
   The permission allows the application to use passwords and SSH keys of PAM accounts.

5. Assign application administrators who can view the application password.

6. Open the Axidian Privilege user console and go to the **Applications** tab.

7. View the application password and save it.

Next, configure Ansible to gain access to the Axidian Privilege server.

Ansible Configuration

To establish a connection to the Axidian Privilege server and obtain access tokens, configure Ansible using one of the following methods:

- Configuration file `ansible.cfg` — specify the variables in the file if the configuration does not change between scenario runs. It is recommended to encrypt credentials or pass them through environment variables.
- Environment variables — specify the variables in the terminal before running the scenario. Variables exist only within the current session. Recommended for use in CI/CD automations.
- Ansible playbook — pass parameters as named arguments when calling the `lookup()` function. This method is suitable when you need to connect to a different server or override a parameter, such as `ca_cert`.

For more details on how the scenario works when the configuration is defined in multiple places, see the Ansible documentation.

Configuration parameters

Parameter	Environment variable	Requirement	Description
`idp_server`	`PAM_IDP_SERVER`	Required	URL of the Axidian Privilege IdP component
`core_server`	`PAM_CORE_SERVER`	Required	URL of the Axidian Privilege Core component
`username`	`PAM_USERNAME`	Required	Application name
`password`	`PAM_PASSWORD`	Required	Password of the specified application. The application administrator can view the password in the user console.
`timeout`	`PAM_TIMEOUT`	Optional	Request response timeout, sec. Default value: `30.0`.
`verify_ssl`	`PAM_VERIFY_SSL`	Optional	Server SSL certificate verification: • `True` — required • `False` — not required Default value: `True`. **Note:** Enabled verification reduces the risk of data interception. If you have disabled verification, it is recommended to note this in the script and leave a comment.

Parameter	Environment variable	Requirement	Description
`ca_cert`	`PAM_CA_CERT`	Optional	Path to the certificate for SSL connection verification. Specify if the PAM server uses a certificate signed by an internal CA. The certificate must be in PEM format. Example: `ca_cert="/path/to/ca.crt"`. Default value: `None`.

Examples

ansible.cfg file

```
[pam]
idp_server = https://pam.company.com/idp
core_server = https://pam.company.com/core
username = my-app
password = your-app-password
timeout = 30
verify_ssl = true
ca_cert = /path/to/ca.crt
```

Environment variables

```
export PAM_IDP_SERVER="https://pam.company.com/idp"
export PAM_CORE_SERVER="https://pam.company.com/core"
export PAM_USERNAME="my-app"
export PAM_PASSWORD="your-app-password"
export PAM_VERIFY_SSL="true"
export PAM_CA_CERT="/path/to/ca.crt"
export PAM_TIMEOUT="30"
```

Ansible playbook

```
- name: Retrieve password with explicit server specification
  ansible.builtin.set_fact:
    db_password: "{{ lookup('axidian.pam.get_password', 'SERVER/admin',
                            idp_server='https://pam.company.com/idp',
                            core_server='https://pam.company.com/core',
                            username='my-app',
                            password='app-password') }}"
  no_log: true
```

After configuring access, use plugins to retrieve credentials.

Plugins

> **NOTE**
>
> Use the `no_log: true` parameter to prevent credentials from being displayed in the console after the task is completed.

Ansible plugins are called through the `lookup()` function and allow you to retrieve the following from Axidian Privilege:

- account password
- account SSH key
- list of available accounts

`get_password`

The plugin is used to retrieve a PAM account password.

`get_password` parameters

Parameter	Requirement	Description
`_terms`	Required	Account name in the format: • `LOCATION/username` — recommended format • `LOCATION\username` — requires escaping in Python scripts, e.g. `"SERVER\\admin"` Passed as the second argument after the plugin name.
`reason`	Optional	Reason for retrieving credentials. Whether a reason is required is determined by the policy applied to the account.
`errors`	Optional	Error handling mode: • `strict` — outputs an error and aborts task execution. Use when the scenario cannot proceed without the password. • `warn` — outputs a warning and assigns an empty string to the variable. Use when the absence of a password does not affect the scenario. • `ignore` — outputs no messages and assigns an empty string to the variable. Use when you handle errors yourself.

```
- name: Retrieve administrator password
  ansible.builtin.set_fact:
    admin_password: "{{ lookup('axidian.pam.get_password', 'PROD-SERVER/admin',
                               reason='Maintenance', errors='strict') }}"
  no_log: true
```

`get_key`

The plugin is used to retrieve a PAM account SSH key.

`get_key` parameters

Parameter	Requirement	Description
`_terms`	Required	Account name in the format: • `LOCATION/username` — recommended format • `LOCATION\username` — requires escaping in Python scripts, e.g. `"SERVER\\admin"` Passed as the second argument after the plugin name.
`decrypt`	Optional	Return the decrypted SSH key: • `True` — return • `False` — do not return Default value: `True`.
`reason`	Optional	Reason for retrieving credentials. Whether a reason is required is determined by the policy applied to the account.
`errors`	Optional	Error handling mode: • `strict` — outputs an error and aborts task execution. Use when the scenario cannot proceed without the SSH key. • `warn` — outputs a warning and assigns an empty string to the variable. Use when the absence of an SSH key does not affect the scenario. • `ignore` — outputs no messages and assigns an empty string to the variable. Use when you handle errors yourself.

Response parameters

Parameter	Description
If `decrypt=True` in the request	
`key`	Account SSH key in PEM format
If `decrypt=False` in the request	
`key`	Encrypted SSH key
`passphrase`	Encrypted key passphrase

```
# Decrypted key (default)
- name: Deploy SSH key
  ansible.builtin.copy:
    content: "{{ lookup('axidian.pam.get_key', 'LINUX-SERVER/automation',
                              reason='Maintenance', errors='warn') }}"
    dest: /home/deploy/.ssh/id_rsa
    mode: '0600'
  no_log: true

# Encrypted key with passphrase
- name: Retrieve SSH key and its passphrase
  ansible.builtin.set_fact:
    ssh_creds: "{{ lookup('axidian.pam.get_key', 'LINUX-SERVER/automation',
                          decrypt=false) }}"
  no_log: true
```

`get_accounts`

The plugin is used to retrieve the list of available PAM accounts and does not require additional parameters.

Response parameters

The response contains a list of accounts in dictionary format with the parameters from the table.

Parameter	Description
`display_name`	Account name
`requires_reason`	Whether a reason for viewing credentials is required according to the policy: • `true` — required • `false` — not required

```
- name: Show available accounts
  ansible.builtin.debug:
    msg: "{{ lookup('axidian.pam.get_accounts') }}"

- name: Show account names only
  ansible.builtin.debug:
    msg: "{{ lookup('axidian.pam.get_accounts') | map(attribute='display_name') | list }}"
```

Using Ansible Vault

It is recommended not to store credentials in plain text and to encrypt them using the Ansible Vault component.

To encrypt the application password:

1. Open a terminal and run the command to encrypt the password:

   ```
   ansible-vault encrypt_string --ask-vault-pass '<password>' --name '<variable>'
   ```

   - `password` — the Axidian Privilege application password to encrypt
   - `variable` — the variable name for encryption

2. Enter the password that will be used to decrypt the variable when running the playbook.
   As a result, the encrypted variable will be displayed in the terminal.

3. Create a file in YAML or JSON format and save the command output to it.

YAML

```
vault_pam_password: !vault |
          $ANSIBLE_VAULT;1.1;AES256

316438643866643766396561623466643139376330353466386561393761386561633766386561
64

633766396138396466613763393062643965663766613766 0a313233343536373839306162636465
```

JSON

```
{
    "vault_pam_password":
"$ANSIBLE_VAULT;1.1;AES256\n316438643866643766396561623466643139376330353466386561393761
386561633766386561 64\n633766396138396466613763393062643965663766613766 0a31323334353637"
}
```

4. Specify the variable in the playbook:

   - For the `vars_files` parameter, specify the path to the file containing the encrypted variable.
   - For the `password` parameter, specify the variable name.

Example

```
- name: Retrieve password using Vault
  hosts: localhost
  gather_facts: false
  vars_files:
    - ./vault.yml
  tasks:
    - name: Request account password from PAM
      ansible.builtin.set_fact:
        db_password: "{{ lookup('axidian.pam.get_password',
                                'SERVER/admin',
                                idp_server='https://pam.company.com/idp',
                                core_server='https://pam.company.com/core',
                                username='my-app',
                                password=vault_pam_password) }}"
      no_log: true
```

Security Recommendations

1. Use the `no_log: true` parameter to prevent credentials from being displayed in the console when a task completes.
2. Do not store passwords in plain text — use Ansible Vault to encrypt credentials.
3. SSL connection verification is enabled by default. Disable it only for testing in isolated environments.
4. When running a scenario simultaneously on different hosts, it is recommended to include the host address in the connection reason.
   Example: `reason='host={{ ansible_host }}; operation=maintenance'`.

Connecting via SSH Proxy

Axidian Privilege supports connecting Ansible to resources through a proxy server. In this scenario, Ansible connects to the SSH Proxy component, which provides access to resources via SSH, SCP, and SFTP protocols.

The component establishes a connection to the resource on behalf of the specified account, controls access to it, and logs all actions on the resource in the Events, Active Sessions, and All Sessions journals.

> ⓘ **LIMITATIONS**
> Two-factor authentication is not supported in the Ansible via SSH Proxy scenario.

Requirements

The following is required to use Ansible via SSH Proxy:

- Ansible 2.14 or higher
- Access to the Axidian Privilege SSH Proxy component
- An Axidian Privilege user account with access to the target resource
- AAPM license, if using Ansible Lookup Plugin

Connection Configuration

To configure a connection from an Ansible playbook through SSH Proxy:

1. Construct the SSH Proxy connection string in UTF-8 encoding using the following template:

   ```
   <pam_user>#<resource_address>#<account_name>#[reason]
   ```

   - `pam_user` — Axidian Privilege username for authentication in SSH Proxy
   - `resource_address` — IP address or DNS name of the target resource
   - `account_name` — account name used to connect to the target resource
   - `reason` — reason for connecting to the resource, if required by the policy

   Example: `pam.admin#192.168.0.100#PAM.LOCAL\pam-admin#Maintenance`

2. Configure Ansible for connecting to Axidian Privilege in one of the following files:

    - Ansible playbook — specify the parameters in the `vars` section.
    - `inventory.yml` — specify the parameters in the `hosts` section.

Configuration parameters

Parameter	Requirement	Description
`ansible_host`	Required	DNS name or IP address of the SSH Proxy component
`ansible_port`	Required	SSH Proxy component port. Default port: `2222`
`ansible_user`	Required	SSH Proxy connection string. Example: `pam.admin#10.0.0.1#DOMAIN\admin`.
`ansible_password`	Optional	PAM user password. Specify if password authentication is configured. It is recommended to encrypt the password using Ansible Vault.
`ansible_ssh_private_key_file`	Optional	Path to the PAM user SSH key. Specify if SSH key authentication is configured. Example: `/home/user/.ssh/id_rsa`.
`ansible_ssh_retries`	Optional	Number of connection retry attempts. Specify to reconnect after a connection drop or session closure from the administrator console.
`ansible_ssh_extra_args`	Optional	Allows passing additional command-line arguments to the SSH client. Use to configure SCP and SFTP connections.

Examples

Ansible playbook

```yaml
- name: Execute command via PAM SSH Proxy
  hosts: all
  gather_facts: false

  vars:
    ansible_host: "pam.company.com"
    ansible_port: 2222
    ansible_user: "pam.admin#192.168.0.100#DOMAIN\\admin"
    ansible_password: "{{ pam_password }}"

  tasks:
    - name: Get system information
      ansible.builtin.raw: uname -a
      register: result
      changed_when: false

    - name: Show result
      ansible.builtin.debug:
        msg: "{{ result.stdout | trim }}"
```

inventory file

Single resource

```yaml
---
all:
  hosts:
    target_server:
      ansible_host: pam.company.com
      ansible_port: 2222
      ansible_user: "pam.admin#192.168.0.100#DOMAIN\\admin"
      ansible_password: "{{ vault_pam_password }}"
```

Multiple resources

```yaml
---
all:
  vars:
    ansible_port: 2222
    ansible_host: pam.company.com
    ansible_password: "{{ vault_pam_password }}"

  hosts:
    web_server:
      ansible_user: "pam.admin#10.11.5.10#DOMAIN\\web-admin"

    db_server:
      ansible_user: "pam.admin#10.11.5.20#DOMAIN\\db-admin"

    app_server:
      ansible_user: "pam.admin#190.160.1.100#LINUX-SERVER\\db-admin#Maintenance"
```

Running a Scenario

To start a session, open a terminal and run the command to connect to the resource via SSH Proxy:

```
ansible-playbook <playbook> [-i <inventory>] [-e <variable>]
```

- `playbook` — name of the Ansible playbook
- `inventory` — name of the configuration file with connection settings
- `variable` — name of the environment variable

Launch command examples

Connection settings specified in the playbook

```
ansible-playbook playbook.yml
```

Connection settings specified in the configuration file

```
ansible-playbook playbook.yml -i inventory.yml
```

Using an environment variable

```
ansible-playbook playbook.yml -i inventory.yml -e "pam_password=${PAM_PASSWORD}"
```

Using Ansible Vault

It is recommended to encrypt credentials using the Ansible Vault component rather than storing them in plain text.

To encrypt the PAM user password:

1. Open a terminal and run the command to encrypt the password:

   ```
   ansible-vault encrypt_string --ask-vault-pass '<password>' --name '<variable>'
   ```

   - `password` — the Axidian Privilege user password to encrypt
   - `variable` — the variable name for encryption

2. Enter the password that will be used to decrypt the variable when running the playbook.
   As a result, the encrypted variable will be displayed in the terminal.

3. Create a file in YAML or JSON format and save the command output to it.

YAML

```
vault_pam_password: !vault |
          $ANSIBLE_VAULT;1.1;AES256

316438643866643766396561623466643139376330353466386561393761386561633766386561 64

633766396138396466613763393062643965663766613766 0a313233343536373839306162636465
```

JSON

```
{
    "vault_pam_password":
"$ANSIBLE_VAULT;1.1;AES256\n316438643866643766396561623466643139376330353466386561393761
386561633766386561 64\n633766396138396466613763393062643965663766613766 0a3132333435363738
39306"
}
```

4. Specify the variable in the playbook:
    - For the `vars_files` parameter, specify the path to the file containing the encrypted variable.
    - For the `password` parameter, specify the variable name.

Example

```
---
- name: Execute command via PAM SSH Proxy using Ansible Vault
  hosts: all
  gather_facts: false
   vars_files:
     - ./vault.yml

  vars:
      ansible_host: "pam.company.com"
      ansible_port: 2222
      ansible_user: "pam.admin#192.168.0.100#PAM.LOCAL\\pam-admin"
       ansible_password: "{{ vault_pam_password }}"

  tasks:
    - name: Verify connection
      ansible.builtin.raw: id
      register: result
      changed_when: false
      no_log: true
```

File Transfer via SCP and SFTP

Files can be transferred from the host running the playbook to an SSH resource using the following protocols:

- SCP — for quick transfer of a single file to the resource
- SFTP — for CI/CD automation or transferring multiple files to the resource

> **LIMITATIONS**
>
> Use the `ansible.builtin.shell` module and the sshpass utility to transfer files.
>
> The `ansible.builtin.copy` module is not suitable for file transfer via SSH Proxy. The module creates a temporary directory on the resource, uploads the file there, moves it to the target directory, sets access permissions, and removes the temporary directory. This requires a separate communication channel, but SSH Proxy only allows file transfer via SCP and SFTP and terminates the session immediately after the file is transferred.

Prerequisites

In the Axidian Privilege administration console, perform the following steps:

1. Go to the **Policies** section and click on the required policy.
2. Go to the **SSH** → **Data Transfer** subsection.
3. For the SCP and SFTP protocols, select the **Allowed to resource only** or **Allowed in both directions** option.
4. Click **Save**.

Host Configuration

On the host from which you plan to connect to the SSH resource, perform the following steps:

1. Install the sshpass utility, which allows automatically filling in the password for SSH connections.

RPM

```
sudo dnf install sshpass
```

DEB

```
sudo apt install sshpass
```

2. Configure the connection to the SSH resource using one of the following methods:

   - Specify the parameters in the `ssh_config` file and pass the file path in the `ansible_ssh_extra_args` variable — the recommended method. This allows you to avoid escaping the connection string.
   - Specify the parameters directly in `ansible_ssh_extra_args` in the `inventory.yml` file or Ansible playbook.

     > ⓘ **ESCAPING SPECIAL CHARACTERS**
     > The SSH Proxy connection string contains special characters `#` and `\` that must be escaped. When configuring in a YAML file, specify the connection string in single quotes.
     >
     > When substituting variables into a command, such as `src_file` or `ansible_user`, use the `quote` filter to handle spaces and special characters.

Parameters

Parameter	Description
`HostName`	DNS name or IP address of the SSH Proxy component. Can be specified in the `ansible_host` parameter in `inventory.yml` or in the playbook.
`Port`	SSH Proxy component port. Default port: `2222`. Can be specified in the `ansible_port` parameter in `inventory.yml` or in the playbook.
`User`	SSH Proxy connection string. Example: `pamadmin@pam.local#ssh-host.example.com#RESOURCE\user##`. Can be specified in the `ansible_user` parameter in `inventory.yml` or in the playbook.
`PreferredAuthentications`	Priority order of authentication methods used when connecting to the proxy server. Possible values: ▪ `keyboard-interactive` — interactive authentication (challenge-response) ▪ `password` — password authentication ▪ `publickey` — SSH key authentication Example: `publickey,keyboard-interactive` — the SSH key is checked first; if it does not match, the server requests a password.
`KbdInteractiveAuthentication`	Enable interactive authentication using the `keyboard-interactive` method. Possible values: ▪ `true` ▪ `false`
`PubkeyAuthentication`	Enable SSH key authentication. Possible values: ▪ `true` ▪ `false`

Parameter	Description
`NumberOfPasswordPrompts`	Number of password entry attempts. If exceeded, the connection to the proxy server is terminated.
`UserKnownHostsFile`	Path to the `known_hosts` file
`StrictHostKeyChecking`	Server SSH key verification: ▪ `yes` — strict verification. If the server key is not found in the `known_hosts` file or does not match the saved key for this host, the connection is terminated with an error. ▪ `no` — verification disabled. If the key is not in the `known_hosts` file, it is added automatically. ▪ `accept-new` — verification for new hosts only. If the key is not in `known_hosts`, it is added automatically and the connection is established. If the specified key does not match the key in `known_hosts`, the connection is terminated. Keys for hosts in `known_hosts` are not overwritten.
`ConnectTimeout`	Timeout (in seconds) for establishing a TCP connection to the server

Examples

inventory.yml

Parameters defined in inventory.yml

```
all:
 hosts:
   pam_target:
     ansible_connection: ssh
     ansible_host: pam.example.com
     ansible_port: 2222
     ansible_user: 'pamadmin@pam.local#ssh-host.example.com#RESOURCE\pam-
user##'
     ansible_password: "{{ vault_pam_password }}"
     ansible_ssh_extra_args: >-
       -tt
       -o PreferredAuthentications=keyboard-interactive,password
       -o KbdInteractiveAuthentication=yes
       -o PubkeyAuthentication=no
       -o NumberOfPasswordPrompts=1
       -o StrictHostKeyChecking=yes
       -o UserKnownHostsFile=./known_hosts
       -o ConnectTimeout=10
```

Path to ssh_config specified in inventory.yml

```
all:
  hosts:
    pam_target:
      ansible_connection: ssh
      ansible_password: "{{ vault_pam_password }}"
      ansible_ssh_extra_args: '-tt -F ./ssh_config'
```

ansible.cfg

Path to ssh_config specified in ansible.cfg

```
[defaults]
inventory = ./inventory.yml

[ssh_connection]
pipelining = False
ssh_args = -F ./ssh_config
```

Ansible playbook

Parameters specified in the playbook

```
- block:
  - name: Transfer file via SSH Proxy using SFTP protocol
    delegate_to: localhost
    environment:
      SSHPASS: "{{ ansible_password }}"
    ansible.builtin.shell: >-
      sshpass -e sftp
      -P {{ ansible_port }}
      -o PreferredAuthentications=keyboard-interactive,password
      -o KbdInteractiveAuthentication=yes
      -o PubkeyAuthentication=no
      -o NumberOfPasswordPrompts=1
      -o StrictHostKeyChecking=accept-new
      -o UserKnownHostsFile=./known_hosts
      -o ConnectTimeout=10
      -o BatchMode=no
      -b {{ sftp_batch_file.path | quote }}
      {{ ansible_user | quote }}@{{ ansible_host }}
    register: sftp_result
    no_log: true
```

Path to ssh_config specified in the playbook

```
ansible.builtin.shell: >-
  sshpass -e sftp
  -F ./ssh_config
  -o BatchMode=no
  -b {{ sftp_batch_file.path | quote }}
  {{ inventory_hostname }}
```

ssh_config file example

```
Host pam_target
 HostName pam.example.com
 Port 2222
 User pamadmin@pam.local#ssh-host.example.com#RESOURCE\pam-user##
 PreferredAuthentications keyboard-interactive,password
 KbdInteractiveAuthentication yes
 PubkeyAuthentication no
 NumberOfPasswordPrompts 1
 UserKnownHostsFile ./known_hosts
 StrictHostKeyChecking yes
 ConnectTimeout 10
```

3. Add the public key of the SSH Proxy component to the `known_hosts` file.

> ⚠ **CAUTION**
> This step is required if `StrictHostKeyChecking` is set to `yes`. If the proxy server fingerprint is not recorded before the first run, the playbook will fail with an error.

```
ssh-keyscan [-p <port>] <host> >> ./known_hosts
```

- `port` — SSH Proxy component port
- `host` — DNS name or IP address of the SSH Proxy component

To confirm the fingerprint, type `yes` in the terminal.

4. Run the playbook to transfer files from the host to the SSH resource using the selected protocol.

```
ansible-playbook <playbook> \
   -e src_file=<source_path> \
   -e dest_dir=<destination_dir> \
   --ask-vault-pass
```

- `playbook` — name of the Ansible playbook
- `source_path` — path to the file to be transferred from the host to the target resource
- `dest_dir` — directory on the target resource where the file will be transferred
- `ask-vault-pass` — prompt for the password to decrypt variables in the playbook

Playbook example

SCP

```
---
- name: Transfer file via SSH Proxy using SCP protocol
  hosts: all
  gather_facts: false

  vars:
    src_file: /tmp/file.txt
    dest_dir: /home/user
    dest_file: "{{ dest_dir }}/{{ src_file | basename }}"

  tasks:
    - name: Transfer file via SSH Proxy using SCP protocol
      delegate_to: localhost
      environment:
        SSHPASS: "{{ ansible_password }}"
      ansible.builtin.shell: >-
        sshpass -e scp
        -F ./ssh_config
        -O
        {{ src_file | quote }}
        {{ inventory_hostname }}:{{ dest_file | quote }}
      register: scp_result
      failed_when: false

    - name: Verify file exists on target
      ansible.builtin.raw: "test -f {{ dest_file | quote }} && echo OK"
      register: verify_result
      changed_when: false
      failed_when: "'OK' not in verify_result.stdout"
```

SFTP

```
---
- name: Transfer file via SSH Proxy using SFTP protocol
  hosts: all
  gather_facts: false

  vars:
    src_file: /tmp/file.txt
    dest_dir: /home/user
    dest_file: "{{ dest_dir }}/{{ src_file | basename }}"

  tasks:
    - name: Create temporary batch file
      delegate_to: localhost
      ansible.builtin.tempfile:
        state: file
        suffix: .sftp
      register: sftp_batch_file

    - name: Write SFTP batch commands
      delegate_to: localhost
      ansible.builtin.copy:
        dest: "{{ sftp_batch_file.path }}"
        content: "put {{ src_file }} {{ dest_file }}\n"

    - block:
        - name: Transfer file via SSH Proxy using SFTP protocol
          delegate_to: localhost
          environment:
            SSHPASS: "{{ ansible_password }}"
          ansible.builtin.shell: >-
            sshpass -e sftp
            -F ./ssh_config
            -o BatchMode=no
            -b {{ sftp_batch_file.path | quote }}
            {{ inventory_hostname }}
          register: sftp_result
          no_log: true

        - name: Verify file exists on target
          ansible.builtin.raw: "test -f {{ dest_file | quote }} && echo OK"
          register: verify_result
          changed_when: false
          failed_when: "'OK' not in verify_result.stdout"
      always:
        - name: Remove temporary batch file
          delegate_to: localhost
          ansible.builtin.file:
            path: "{{ sftp_batch_file.path }}"
            state: absent
```

Security Recommendations

1. For server authentication and automation scenarios, before the first connection to PAM, add the public key of the SSH Proxy component to the `known_hosts` file:

   ```
   ssh-keyscan [-p <port>] <host> >> ~/.ssh/known_hosts
   ```

   - `port` — SSH Proxy component port
   - `host` — DNS name or IP address of the SSH Proxy component

   > ⚠ **CAUTION**
   > Verify the key authenticity: the `ssh-keyscan` command uses the Trust on first use (TOFU) mechanism, where the key is added without verification.

2. When configuring the connection, enable public key verification: set the `StrictHostKeyChecking` parameter to `yes`.

3. Do not store passwords in plain text — use Ansible Vault to encrypt credentials.

4. Use the `no_log: true` parameter to prevent credentials from appearing in Ansible logs when a task completes.

5. In CI/CD scenarios, pass the password and SSH key through environment variables.

6. The `ssh_config` file contains connection data. It is recommended to restrict file permissions using the command:

   ```
   chmod 600 ~/.ssh/config
   ```

7. To enhance security, it is recommended to use the following parameters:

   - `gather_facts: false` — disables host information gathering, which prevents Python script launch commands from appearing in logs.
   - `no_log: true` — disables output to the console and Ansible logs. Use for tasks involving credentials.
   - `become: true` and `become_method: sudo` — elevates privileges for executing commands that require `root` permissions.

- `raw` module — allows executing commands through SSH Proxy without installing Python on the target resource and enables displaying an informative log in the session profile in the administrator console.

Scenario example

```yaml
---
- name: Execute command via PAM SSH Proxy
  hosts: all
  gather_facts: false
  become: true
  become_method: sudo

  vars:
    ansible_host: "pam.company.com"
    ansible_port: 2222
    ansible_user: "pam.admin#10.10.5.190#PAM.LOCAL\\pam-admin"
    ansible_password: "{{ pam_password }}"

  tasks:
    - name: Execute command (credentials hidden)
      ansible.builtin.raw: uname -a
      register: result
      changed_when: false
      no_log: true

    - name: Show command result (log displayed)
      ansible.builtin.debug:
        msg: "{{ result.stdout | trim }}"
      no_log: false
```

AAPM Reference

Python SDK

Integrating Axidian Privilege into Python applications and automation scripts

AAPM API

Interaction with AAPM via API

Console Tool

The utility allows an application to retrieve account passwords and SSH keys from Axidian Privilege

Python SDK

Python SDK provides an API for retrieving passwords and SSH keys of Axidian Privilege accounts. The solution is suitable for integrating PAM into CI/CD automations, Python scripts, orchestration systems, and other processes that require secure credential management.

All requests to retrieve and view credentials are logged in the Events section.

> ⚠ **REQUIREMENTS**
> Python 3.9 or higher is required to work with Python SDK.

Prerequisites

To set up Python SDK, perform the following steps:

1. Go to the AAPM Python SDK package folder at `AxidianPAM_3.5/axidian-pam-tools/aapm` and execute the command:

   ```
   pip install pam_aapm-3.5.0-py3-none-any.whl
   ```

2. Go to the Axidian Privilege administrator console and add an application.

3. For the application, create a permission with the **Allow view account credentials** option enabled.
   The permission will allow the application to use passwords and SSH keys of PAM accounts.

4. Assign application administrators who can view its password.

5. Open the Axidian Privilege user console and go to the **Applications** tab.

6. View the application password and save it.

Next, open any Python development environment and configure access to the Axidian Privilege server.

Quick start

```python
from pam_aapm import PamClient

# Using a context manager (recommended)
with PamClient(
    idp_url="https://pam.company.com/idp",
    core_url="https://pam.company.com/core",
    username="my-app",
    password="app-password",
) as client:
    # Retrieving a password
    db_password = client.get_password("DB-SERVER/admin")

    # Retrieving an SSH key
    ssh_key = client.get_ssh_key("LINUX-SERVER/deploy")

    # Retrieving a list of available accounts
    accounts = client.get_accounts()
    for account in accounts:
        print(f"{account.display_name}: password={account.has_password}, key=
{account.has_key}")
```

Authentication

`PamClient` is the main Python SDK class for interacting with Axidian Privilege. It provides an API for authentication and credential retrieval. To establish a connection to the PAM server and obtain access tokens, specify the parameters from the table for the `PamClient` class.

`PamClient` parameters

Parameter	Environment variable	Required	Description
`idp_url`	`PAM_IDP_SERVER`	Required	URL of the Axidian Privilege IdP component
`core_url`	`PAM_CORE_SERVER`	Required	URL of the Axidian Privilege Core component
`username`	`PAM_USERNAME`	Required	Application name
`password`	`PAM_PASSWORD`	Required	Password of the specified application. The application administrator can view the password in the user console.
`client_id`	—	Optional	Identifier of the client application requesting the token. Default: `"aapm-tool"`.
`scope`	—	Optional	API access request via the OAuth2 protocol. Default: `"pam-api"`.

Parameter	Environment variable	Required	Description
`verify_ssl`	`PAM_VERIFY_SSL`	Optional	Server SSL certificate verification: • `True` — required • `False` — not required Default: `True`. **Note:** Enabled verification reduces the risk of data interception. If you have disabled verification, it is recommended to highlight this in the script and leave a comment.
`ca_cert`	`PAM_CA_CERT`	Optional	Path to the certificate for SSL connection verification. Specify if the PAM server uses a certificate signed by an internal CA. The certificate must be in PEM format. Example: `ca_cert="/path/to/ca.crt"`. Default: `None`.
`timeout`	—	Optional	Response timeout for a request, in seconds. Default: `30.0`.
`accounts_cache_ttl`	—	Optional	Time-to-live (TTL) for the accounts cache, in seconds. Default: `300`.

After configuring access, call one of the methods to retrieve credentials.

> **NOTE**
>
> It is recommended to use the `with` context manager.
>
> In this case, the connection to PAM is closed automatically and access tokens are deleted.

Example with authentication parameters

```python
from pam_aapm import PamClient

with PamClient(
    idp_url="https://pam.company.com/idp",
    core_url="https://pam.company.com/core",
    username="my-app",
    password="app-password",
) as client:
    password = client.get_password("SERVER/account")
```

Example with environment variables (recommended for CI/CD automations)

```python
import os
from pam_aapm import PamClient

with PamClient(
    idp_url=os.environ["PAM_IDP_SERVER"],
    core_url=os.environ["PAM_CORE_SERVER"],
    username=os.environ["PAM_USERNAME"],
    password=os.environ["PAM_PASSWORD"],
    verify_ssl=os.environ.get("PAM_VERIFY_SSL", "true").lower() == "true",
    ca_cert=os.environ.get("PAM_CA_CERT"),
) as client:
    password = client.get_password("SERVER/account")
```

Methods

Python SDK methods allow you to retrieve the following from Axidian Privilege:

- account password
- account SSH key
- list of available accounts

`get_password()`

The method is used to retrieve a PAM account password.

```
get_password(account_name, reason=None)
```

`get_password()` parameters

Parameter	Required	Description
`account_name`	Required	Account name in the following format: • `LOCATION/username` — recommended format • `LOCATION\username` — requires escaping in Python scripts, for example `"DB-SERVER\\admin"`
`reason`	Optional	Reason for retrieving credentials. Whether a reason is required is determined by the policy applied to the account. Default: `None`.

```python
from pam_aapm import PamClient

with PamClient(
    idp_url="https://pam.company.com/idp",
    core_url="https://pam.company.com/core",
    username="my-app",
    password="app-password",
) as client:
    # Retrieving a password
    password = client.get_password("DB-SERVER/db_admin")

    # Retrieving a password when a reason is required
    password = client.get_password(
        "PROD-SERVER/admin",
        reason="Scheduled maintenance"
    )
```

`get_ssh_key()`

The method is used to retrieve a PAM account SSH key.

```
get_ssh_key(account_name, decrypt=True, reason=None)
```

`get_ssh_key()` parameters

Parameter	Required	Description
`account_name`	Required	Account name in the following format: • `LOCATION/username` — recommended format • `LOCATION\username` — requires escaping in Python scripts, for example `"DB-SERVER\\admin"`
`decrypt`	Optional	Return the decrypted SSH key: • `True` — return • `False` — do not return Default: `True`.
`reason`	Optional	Reason for retrieving credentials. Whether a reason is required is determined by the policy applied to the account. Default: `None`.

Response parameters

Parameter	Description
If `decrypt=True` in the request	
`key`	Account SSH key in PEM format
If `decrypt=False` in the request	
`key`	Encrypted SSH key
`passphrase`	Passphrase of the encrypted key
`file_name`	Key file name

```python
from pam_aapm import PamClient

with PamClient(
    idp_url="https://pam.company.com/idp",
    core_url="https://pam.company.com/core",
    username="my-app",
    password="app-password",
) as client:
    # Decrypted key
    key = client.get_ssh_key("LINUX-SERVER/automation")

    # Encrypted key with passphrase
    key_data = client.get_ssh_key("LINUX-SERVER/automation", decrypt=False)
    print(f"Key: {key_data.key}")
    print(f"Passphrase: {key_data.passphrase}")
```

`get_accounts()`

The method is used to retrieve a list of available PAM accounts.

```python
get_accounts(force_refresh=False)
```

`get_accounts()` parameters

Parameter	Required	Description
`force_refresh`	Optional	Force cache refresh: • `True` — reset cache • `False` — do not reset Default: `False`.

Response parameters

Parameter	Description
`id`	Account identifier
`display_name`	Account name
`requires_reason`	A reason for viewing credentials is required: • `true` — required • `false` — not required Whether a reason is required is determined by the policy applied to the account.
`has_password`	Account password: • `true` — set • `false` — not set
`has_key`	Account SSH key: • `true` — set • `false` — not set
`is_key_supported`	Adding an SSH key is available for the account: • `true` — available • `false` — not available

```python
from pam_aapm import PamClient
with PamClient(
    idp_url="https://pam.company.com/idp",
    core_url="https://pam.company.com/core",
    username="my-app",
    password="app-password",
) as client:
    accounts = client.get_accounts(force_refresh=False)

    for account in accounts:
        print(f"Account: {account.display_name}")
        print(f"  - Has password: {account.has_password}")
        print(f"  - Has SSH key: {account.has_key}")
        print(f"  - Requires reason: {account.requires_reason}")
```

`close()`

The method releases system resources and is called automatically when the `with` context manager is used.

If the context manager is not used, call `close()` when the connection to PAM is no longer needed.

```
close()
```

Example without using a context manager

```python
from pam_aapm import PamClient

# Creating a client instance
client = PamClient(
    idp_url="https://pam.company.com/idp",
    core_url="https://pam.company.com/core",
    username="my-app",
    password="app-password",
)

password = client.get_password("DB-SERVER/db_admin")

client.close()
```

Exceptions and error handling

Exceptions are events that report errors during script execution. Exception handling allows you to intercept an error without forcefully terminating the program.

Exception list

Exception	Description
`AuthenticationError`	Authentication error in Axidian Privilege. Change the credentials or refresh the access token.
`AccountNotFoundError`	The account was not found or is unavailable. Make sure the account has not been deleted in Axidian Privilege or that the account name in the request is correct.
`PasswordNotSetError`	The password for the account is not set. Occurs when calling the `get_password()` method if the account does not have a password configured.
`SshKeyNotSetError`	The SSH key for the account is not set. Occurs when calling the `get_ssh_key()` method if the account does not have an SSH key configured.
`ReasonRequiredError`	A request reason is required according to the policy. Fill in the `reason` parameter in the request.
`ConfigurationError`	Configuration error. Make sure the URLs for IdP and Core are specified correctly, or add the missing parameters to the request.
`ApiError`	API server error. Review the HTTP response code.
`PamConnectionError`	Server connection error. Check the availability of the IdP and Core components.
`ValidationError`	Input data processing error. Make sure the IdP and Core components are accessible and the request parameters are specified correctly.

Exception handling example

```python
from pam_aapm import (
    PamClient,
    AuthenticationError,
    AccountNotFoundError,
    PasswordNotSetError,
    ReasonRequiredError,
    SshKeyNotSetError,
    PamConnectionError,
    PamError,
)

try:
    with PamClient(
        idp_url="https://pam.company.com/idp",
        core_url="https://pam.company.com/core",
        username="my-app",
        password="app-password",
    ) as client:
        password = client.get_password("SERVER/account")

except AuthenticationError as e:
    print(f"Authentication error: {e}")
except AccountNotFoundError as e:
    print(f"Account not found: {e.account_name}")
except PasswordNotSetError as e:
    print(f"Password not set: {e.account_name}")
except ReasonRequiredError as e:
    print(f"Reason required: {e.account_name}")
except SshKeyNotSetError as e:
    print(f"SSH key not set: {e.account_name}")
except PamConnectionError as e:
    print(f"Connection error: {e}")
except PamError as e:
    print(f"PAM error: {e}")
```

Security recommendations

1. Do not store credentials in scripts. For improved security, use environment variables or secret vaults.
2. Use the `with` context manager. In this case, the connection to Axidian Privilege is closed automatically and access tokens are deleted after the request is processed.
3. SSL connection verification is enabled by default. Disable verification only for testing in isolated environments.

4. When logging exceptions, avoid recording account names so that they are not persisted in the logs.

AAPM API

Axidian Privilege supports interaction with Application to Application Password Management (AAPM) through the API.
Requests for retrieval and viewing of account data are logged in the Events section.

To obtain a list of accounts or their data, authenticate and obtain an access token.

> **INFO**
> To add an application and grant it access to account data, read the Applications section.

Authentication and Token Retrieval

Authentication and token acquisition occur via the OpenID Connect (OIDC) protocol using the Resource Owner Password Credentials (ROPC) mechanism. The application sends the login and password to the IdP component, and the IdP returns an access token.

To authenticate and obtain a token, send a POST request to the management server:

```
POST https://<PAM FQDN>/idp/connect/token
```

Request Parameters

Parameters	Description
`Content-Type`	Format for reading, processing, and outputting data. For working with data in JSON format, specify `application/json`.
`grant_type`	Method of authentication and token acquisition. For application authentication by login and password, specify `password`.
`username`	Name of the application added to Axidian Privilege
`password`	Password of the specified application. The application administrator can view the password in the user console.
`scope`	API access request. For access to Axidian Privilege API, specify `pam-api`.
`client_id`	Identifier of the client application requesting the token. For application authentication on the IdP server, specify `aapm-tool`.

Example of a token request

```
POST https://pam.server/idp/connect/token
Content-Type: application/x-www-form-urlencoded
grant_type=password&username=MyApp&password=a4dGs22TfDpm31&scope=pam-api&client_id=aapm-tool
```

The response contains an `access_token` field, which contains the access token. Use it in requests to obtain:

- a list of available accounts
- passwords and SSH keys of accounts stored in Axidian Privilege

Response Parameters

Parameters	Description
`access_token`	Token for access to Axidian Privilege API
`expires_in`	Token validity period in seconds
`token_type`	Access token type: `Bearer` — any user possessing the token can use it.
`scope`	API access permission: `pam-api` — the token is valid only for Axidian Privilege API calls.

Response example

```
{
    "access_token": "BB984E803AFAA449FD8C1",
    "expires_in": 60,
    "token_type": "Bearer",
    "scope": "pam-api"
}
```

Retrieving Account Data

The request is sent to the Core component using the access token from the request to IdP.
To obtain account data, send a POST request to the management server:

```
POST https://<PAM FQDN>/core/accounts/<account identifier>/credentials-view
```

Copy the account entry identifier from the account profile URL.

Request Parameters

Parameters	Description
`Content-Type`	Format for reading, processing, and outputting data. For working with data in JSON format, specify `application/json`.
`Authorization`	User authentication and access verification. Specify the Bearer authentication method and the access token obtained in the request to IdP.
`account-id`	Application identifier for which account data is requested. The identifier is displayed in the URL address in the application profile.
`UserId`	Service attribute in UUID format. Specify `00000000-0000-0000-0000-000000000000`.
`Reason`	Reason for obtaining account data. The reason specification is defined by the policy that applies to the account.

Example of a request to obtain credentials

```
POST https://pam.server/core/accounts/5e852968-26ed-498c/credentials-view
Content-Type: application/json
Authorization: Bearer BB984E803AFAA449FD8C1
{
 "UserId": "00000000-0000-0000-0000-000000000000",
 "Reason": "get-data"
}
```

The response to the request contains account data: password, SSH key and their settings.

Response Parameters

Parameters	Description
`Password`	Account password
`Key`	Account SSH key
`KeyPassphrase`	Generated password for SSH key. Password generation is defined by the policy that applies to the account. If the **Encrypt SSH key using generated password before showing to user** option is disabled, the field indicates `null`.
`ResetCredentialsAfterShowing`	Password reset setting after viewing: • `true` — password is reset • `false` — password is not reset The setting is specified in the **Credential privacy settings** in the policy that applies to the account.
`ResetCredentialsAfterShowingAfterMin`	Time after which the password is reset in minutes

Response example

```
{
    "Password": "Q1w2e3r4",
    "Key": "",            // SSH key can be set for the account, but it is not added at the
moment
    "KeyPassphrase": null,
    "KeyFileName": "AXIDIAN-ID\\Administrator_20221013_160621Z.pem",
    "ResetCredentialsAfterShowing": false,
    "ResetCredentialsAfterShowingAfterMin": 60
}
```

Getting a list of accounts

The request is executed to the Core component using the access token from the request to IdP.
To get a list of accounts, send a GET request to the management server:

```
GET https://<PAM FQDN>/core/users/permitted-accounts
```

Request Parameters

Parameters	Description
`Content-Type`	Format for reading, processing, and outputting data. For working with data in JSON format, specify `application/json`.
`Authorization`	User authentication and access verification. Specify the `Bearer` authentication method and the access token obtained in the request to IdP.

Example of a request to get a list of accounts

```
GET https://pam.server/core/users/permitted-accounts
Content-Type: application/json
Authorization: Bearer BB984E803AFAA449FD8C1
```

The response to the request contains a list of accounts with settings of active permissions and policies.

Response Parameters

Parameters	Description
`Account` — account data	
`Id`	Account identifier
`DisplayName`	Account name
`IsKeySupported`	For the account, adding an SSH key is available: • `true` — available • `false` — unavailable
`NextCredentialsReset`	Account password and SSH key are reset the specified time after being displayed. `null` — account data reset is not set by the policy.
`AreCredentialsResettingNow`	During the request, the account password and/or SSH key is being changed: • `true` — account data is currently being changed • `false` — account data is not being changed
`HasPassword`	Account password: • `true` — set • `false` — not set
`HasKey`	Account SSH key: • `true` — set • `false` — not set
`PolicySettings` — policy parameters that apply to the account	

Parameters	Description
`RequireCredentialsViewingReason`	Require to specify the reason for viewing password and SSH key: • `true` — required • `false` — not required
`IsCredentialsViewingConfirmationRequired`	Viewing password and SSH key requires administrator confirmation: • `true` — password is available after request confirmation by administrator • `false` — not required
`CredentialsViewingConfirmationTimeout`	Waiting time for confirmation of password and SSH key viewing in minutes
`EncryptKeyBeforeShowing`	Encrypt SSH key with generated password before showing to user: • `true` — encrypt • `false` — do not encrypt
`IsUserCanSetAccountCredentialsIfNotSet`	Allow PAM users to set account data for accounts if they are not set: • `true` — allowed • `false` — not allowed
`PermissionSettings` — permission settings	
`IsCredentialsViewAllowed`	Allow user to view account credentials: • `true` — user is added to application administrators and can view application password in user console • `false` — user is not added to the administrators and cannot view the password

Parameters	Description
`IsCredentialsChangeAllowed`	Allow user to manage account data: • `true` — user is added to permission and can reset application password • `false` — user cannot reset the password because they are not added to the permission or this option is not enabled in their permission

Response example


```
{
    "Accounts": [
        {
            "Account": {
                "Id": "7c0616f5-9c60-432b-a644-b57bbd176e65",
                "DisplayName": "UBUNTU-PAM.PAM-AD1.LOCAL\\root",
                "IsKeySupported": true,
                "NextCredentialsReset": null,
                "AreCredentialsResettingNow": false,
                "HasPassword": true,
                "HasKey": false
            },
            "PolicySettings": {
                "RequireCredentialsViewingReason": false,
                "IsCredentialsViewingConfirmationRequired": false,
                "CredentialsViewingConfirmationTimeout": "00:07:00",
                "EncryptKeyBeforeShowing": false,
                "IsUserCanSetAccountCredentialsIfNotSet": false
            },
            "PermissionSettings": {
                "IsCredentialsViewAllowed": true,
                "IsCredentialsChangeAllowed": false
            }
        }
    ]
}
```

Console Tool

The Pam.Tools.Aapm console utility allows the application to retrieve passwords and SSH keys for account records stored in Axidian Privilege. Install and configure the utility on the server from which the application runs.
Requests for retrieval and viewing of account data are logged in the Events section of the journal.

> **INFO**
> To add an application and grant it access to account data, read the Applications section.

Configuration

1. Go to the AAPM distribution and open the utility's configuration file `appsettings.json`.
2. In the `Auth` and `Endpoints` sections, specify values for the parameters:
   - `Username` and `Password` — the application name and password.
     The application administrator can view this data in the user console.
   - `CoreUrl` — the address of the Core component.
   - `IdpUrl` — the address of the IdP component.
   - `Certificate` — the certificate identifier.
     Specify if client certificate fingerprint verification is configured.

Configuration file example

```
{
  "$schema": "appsettings.schema.json",
  "Auth": {
    "Username": "124",
    "Password": "2cenQ>(/Q)+gxGN5h@!P-Sa=7]~qEl",
    "Certificate": ""
  },
  "Endpoints": {
    "CoreUrl": "https://pam.server/core",
    "IdpUrl": "https://pam.server/idp"
  },
  "NLog": {
    "variables": {
      "maxArchiveFilesPerCategory": 770
    },
    "rules": {
      "0_MicrosoftExtensionsIgnored": {
        "logger": "Microsoft.Extensions.*",
        "maxLevel": "Info",
        "final": true
      },
      "0_MicrosoftEfCoreIgnored": {
        "logger": "Microsoft.EntityFrameworkCore*",
        "maxLevel": "Debug",
        "final": true
      },
      "0_SystemIgnored": {
        "logger": "System.*",
        "maxLevel": "Info",
        "final": true
      },
      "1_File": {
        "logger": "*",
        "writeTo": "appdomainFile"
      }
    }
  }
}
```

Launching the utility

Windows

1. Run PowerShell as administrator.

2. Go to the folder with the utility at `AxidianPAM_3.5\axidian-pam-tools\aapm`.

3. Run the utility with the required parameter:

```
.\Pam.Tools.Aapm.exe <parameter>
```

- `get-accounts` — list of account records whose data the application knows and can use.
- `get-ssh-key` — SSH key for the specified account record.
- `get-password` — password for the specified account record.
- `help` — information about the specified command.
- `version` — the utility version number.

Command examples

Outputs a list of accounts from permissions

```
.\Pam.Tools.Aapm.exe get-accounts
```

Outputs the password of the Axidian\ServiceOps account

```
.\Pam.Tools.Aapm.exe get-password -n Axidian\ServiceOps
```

Stores the command result in a variable and outputs the result

```
$result = .\Pam.Tools.Aapm.exe get-ssh-key -n Axidian\ServiceOps
echo $result
```

Linux

> ⚠ **CAUTION**
> To use the utility, install dotnet-runtime-8.0.

1. Go to the folder with the utility at `AxidianPAM_3.5/axidian-pam-tools/aapm`.

2. From the directory, open a terminal and run the utility with the required parameter:

```
dotnet ./Pam.Tools.Aapm.dll <parameter>
```

- `get-accounts` — list of account records whose data the application knows and can use.
- `get-ssh-key` — SSH key for the specified account record.
- `get-password` — password for the specified account record.
- `help` — information about the specified command.
- `version` — the utility version number.

Command examples

Outputs a list of accounts from permissions

```
dotnet ./Pam.Tools.Aapm.dll get-accounts
```

Outputs the password of the Axidian\ServiceOps account

```
dotnet ./Pam.Tools.Aapm.dll get-password -n Axidian\ServiceOps
```

Stores the command result in a variable and outputs the result

```
result=$(dotnet ./Pam.Tools.Aapm.dll get-ssh-key -n Axidian\ServiceOps)
echo $result
```

ConsoleApp

The built-in ConsoleApp utility allows you to automatically manage Axidian Privilege objects and configure access permissions. For example, you can use the utility to create multiple resources or accounts at once, as well as revoke all unused permissions.

> **INFO**
> All operations performed by the utility are logged in the Events journal.

Authentication

Before using the utility, configure authentication to access Axidian Privilege. ConsoleApp supports the following OAuth 2.0 authentication modes:

- Resource Owner Password Flow (ROPC) — the utility obtains an access token on behalf of a PAM user and sends their credentials to the Axidian Privilege IDP component. All actions performed through the utility are executed on behalf of the PAM user, and the available operations are limited by the privileges of the specified user.
- Client Credentials Flow — the utility authenticates in PAM on its own behalf in Machine-to-Machine (M2M) mode. All actions performed through the utility are executed on behalf of the `Console Application` service client, and the available operations are limited by the privileges of this client.

Resource Owner Password Flow

> **INFO**
> For ROPC authentication, do not fill in the `clientSecret` parameter — leave the value empty.

To configure authentication:

1. Navigate to the utility folder and open the `appsettings.json` configuration file.
2. For the `coreUrl` parameter, specify the Core component address.
3. For the `idpUrl` parameter, specify the IdP component address.
4. For the `authUsername` parameter, specify the PAM user login.
   If the parameter is not specified, the login will be requested when the utility starts.

5. For the `authPassword` parameter, specify the PAM user password.
   If the parameter is not specified, the password will be requested when the utility starts.

When the utility starts, authentication is performed on behalf of the specified PAM user. If two-factor authentication is configured for the user, the utility will request an OTP code.

Client Credentials Flow

> ⚠ **CAUTION**
> It is not recommended to use this authentication method — all users working with the utility perform operations on behalf of the service client and have the same set of privileges. To differentiate permissions and improve security, use ROPC authentication.

To configure authentication:

1. Navigate to the utility folder and open the `appsettings.json` configuration file.
2. For the `clientSecret` parameter, specify the `Console Application` client secret.

When the utility starts, authentication is performed on behalf of the service client, and the OTP code is not requested.

> **WHERE TO FIND THE CLIENT SECRET?**
> Open the IdP component configuration file at:
>
> - Windows: `C:\inetpub\wwwroot\idp\appsettings.json`
> - Linux: `/etc/axidian/axidian-pam/idp/appsettings.json`
>
> In the `IdentitySettings` section, the `ConsoleAppClientSecret` parameter contains the client secret.

Configuration file example

Resource Owner Password Flow

```
{
  "coreUrl": "https://pam.example.local/core",
  "idpUrl": "https://pam.example.local/idp",
  "clientSecret": "",
  "authUsername": "ConsoleAppUser",
  "authPassword": "#123QwerTy!",
  "skipErrorsInBulkProcessing": true,
  "NLog": {
    "variables": {
      "minLevel": "Trace",
      "dbMinLevel": "Info",
      "maxArchiveFilesPerCategory": 23
    },
    "rules": {
      "1": {
        "logger": "*",
        "minLevel": "Trace",
        "writeTo": "processFile"
      }
    }
  }
}
```

Client Credentials Flow

```
{
  "coreUrl": "https://pam.example.local/core",
  "idpUrl": "https://pam.example.local/idp",
  "clientSecret": "NPW8dALzsjzpSGDlTGIEMt5o6sjM8x3sz",
  "authUsername": "",
  "authPassword": "",
  "skipErrorsInBulkProcessing": true,
  "NLog": {
    "variables": {
      "minLevel": "Trace",
      "dbMinLevel": "Info",
      "maxArchiveFilesPerCategory": 23
    },
    "rules": {
      "1": {
        "logger": "*",
        "minLevel": "Trace",
        "writeTo": "processFile"
      }
    }
  }
}
```

Account operations

Create an account

Single account

To create an account in Axidian Privilege:

1. Navigate to the utility folder.
2. Run the utility with the parameters from the table:

Windows

```
.\Pam.ConsoleApp.exe create-account <parameter> <value>
```

Linux

```
dotnet ./Pam.ConsoleApp.dll create-account <parameter> <value>
```

Parameters

Parameter	Requirement	Description
`--username`	Required	Account name
`--resource` or `--domain`	Required	Account location: ◦ `--resource` — resource name ◦ `--domain` — domain name Specify one of the parameters.
`--password`	Optional	Account password
`--description`	Optional	Description
`--policy`	Optional	Policy to apply to the account
`--key-file`	Optional	Path to the SSH key file, for example: `.\id_rsa`
`--key-passphrase`	Optional	SSH key file passphrase

Command examples

Windows

Create an account

```
.\Pam.ConsoleApp.exe create-account `
--username Administrator `
--resource app01.local `
--password "Pass123$" `
--description "Local admin" `
--policy Default
```

Create a domain account

```
 .\Pam.ConsoleApp.exe create-account --username Administrator --domain
dev.local
```

Create an account with an SSH key

```
 .\Pam.ConsoleApp.exe create-account `
 --username root `
 --resource linux01.local `
 --password "Pass123$" `
 --key-file .\id_rsa `
 --key-passphrase "Passphrase"
```

Linux

Create an account

```
 dotnet ./Pam.ConsoleApp.dll create-account `
--username Administrator `
--resource app01.local `
--password "Pass123$" `
--description "Local admin" `
--policy Default
```

Create a domain account

```
 dotnet ./Pam.ConsoleApp.dll create-account --username Administrator --domain
dev.local
```

Create an account with an SSH key

```
dotnet ./Pam.ConsoleApp.dll create-account `
--username root `
--resource linux01.local `
--password "Pass123$" `
--key-file .\id_rsa `
--key-passphrase "Passphrase"
```

Multiple accounts

To create multiple accounts in Axidian Privilege:

1. Create a CSV file using the following template:

```
Location type;Location Name;Username;Set password;Password;Description;SSH key file
path;SSH key passphrase
```

Parameters

Parameter	Requirement	Description
`Location type`	Required	Account type: ◦ `Local` — resource account ◦ `Domain` — domain account
`Location Name`	Required	Resource or domain name
`Username`	Required	Account name
`Set password`	Required	Set a password for the account: ◦ `true` — set a password ◦ `false` — create the account without a password
`Password`	Optional	Account password. Specify if `Set password` is set to `true`.
`Description`	Optional	Description
`SSH key file path`	Optional	Path to the SSH key file, for example: `.\id_rsa`
`SSH key passphrase`	Optional	SSH key file passphrase

CSV file example

```
Local;dc.dev.local;root;true;root;Local account;;
Local;raspberrypi;root;true;root;SSH key example;id_rsa;passphrase
Domain;dev.local;Administrator;false;;Domain admin;;
```

2. Navigate to the utility folder and run the command:

Windows

```
.\Pam.ConsoleApp.exe create-accounts-from-file --file <file path>
```

Linux

```
dotnet ./Pam.ConsoleApp.dll create-accounts-from-file --file <file path>
```

Delete an account

To delete an account from Axidian Privilege:

1. Navigate to the utility folder.
2. Run the command, specifying the account name or its identifier:

Windows

```
.\Pam.ConsoleApp.exe delete-account --name <account name>
```

```
.\Pam.ConsoleApp.exe delete-account --id <account identifier>
```

Linux

```
dotnet ./Pam.ConsoleApp.dll delete-account --name <location\account name>
```

```
dotnet ./Pam.ConsoleApp.dll delete-account --id <account identifier>
```

The identifier is displayed in the URL in the account profile.

Command examples

Windows

Delete an account by name

```
.\Pam.ConsoleApp.exe delete-account --name app01.local\User
```

Delete an account by identifier

```
.\Pam.ConsoleApp.exe delete-account --id a988f1b0-b871-43fa-a40c-6f4ac75f904c
```

Linux

Delete an account by name

```
dotnet ./Pam.ConsoleApp.dll delete-account --name app01.local\Administrator
```

Delete an account by identifier

```
dotnet ./Pam.ConsoleApp.dll delete-account --id a988f1b0-b871-43fa-a40c-
6f4ac75f904c
```

Resource operations

Create a resource

Single resource

To create a resource in Axidian Privilege:

1. Navigate to the utility folder.

2. Run the utility with the parameters from the table:

Windows

```
.\Pam.ConsoleApp.exe create-resource <parameter> <value>
```

Linux

```
dotnet ./Pam.ConsoleApp.dll create-resource <parameter> <value>
```

Parameters

Parameter	Requirement	Description
`--name`	Required	Resource name
`--description`	Optional	Description
`--dns-name` or `--ip-address`	Required	Resource address: • `--dns-name` — DNS name • `--ip-address` — IP address Specify one of the parameters.
`--user-connection-type`	Required	User connection type. For more details, see User connection.
`--user-connection-address`	Optional	IP address or DNS name of the user connection
`--user-connection-port`	Optional	User connection port
`--user-connection-matching-url`	Optional	Login page URL for a web resource
`--user-connection-matching-url-is-regex`	Optional	Indicates whether the login page URL is a regular expression: • `true` — yes • `false` — no Specify if the `UC matching url` parameter is set.

Parameter	Requirement	Description
`--service-account`	Optional	Service account name
`--service-connection-type`	Optional	Service connection type. For more details, see Service connection.
`--service-connection-port`	Optional	Service connection port
`--service-ssh-template`	Optional	SSH connector template name. Specify if the service connection type is `SSH`.
`--cisco-privilege-mode-password`	Optional	Cisco privileged mode password. Specify if the service connection type is `Cisco IOS`
`--policy`	Optional	Policy to apply to the resource

Command examples

Windows

Create a resource

```
.\Pam.ConsoleApp.exe create-resource `
--name APP01 `
--description "Application server" `
--dns-name app01.local `
--user-connection-type RDP `
--user-connection-port 3389 `
--service-account DOMAIN\svc_app `
--service-connection-type Windows
```

Linux

Create a resource

```
dotnet ./Pam.ConsoleApp.dll create-resource `
--name APP01 `
--description "Application server" `
--dns-name app01.local `
--user-connection-type RDP `
--user-connection-port 3389 `
--service-account DOMAIN\svc_app `
--service-connection-type Windows
```

Multiple resources

To create multiple resources in Axidian Privilege:

1. Create a CSV file using the following template:

```
Name;Description;DNS name;IP address;UC type;UC address;UC port;UC matching url;UC
matching url is regex;SC account name;SC type;SC SSH template;SC address;SC port;Cisco
privilege mode password
```

Parameters

Parameter	Requirement	Description
`Name`	Required	Resource name
`Description`	Optional	Description
`DNS name` or `IP address`	Required	DNS name or IP address of the resource. Specify one of the parameters.
`UC type`	Required	User connection type. For more details, see User connection.
`UC address`	Optional	IP address or DNS name of the user connection
`UC port`	Optional	User connection port
`UC matching url`	Optional	Login page URL for a web resource
`UC matching url is regex`	Optional	Indicates whether the login page URL is a regular expression: ◦ `true` — yes ◦ `false` — no Specify if the `UC matching url` parameter is set.
`SC account name`	Optional	Service account name
`SC type`	Optional	Service connection type. For more details, see Service connection.

Parameter	Requirement	Description
`SC SSH template`	Optional	SSH connector template name. Specify if the service connection type is `SSH`.
`SC address`	Optional	IP address or DNS name of the service connection
`SC port`	Optional	Service connection port
`Cisco privilege mode password`	Optional	Cisco privileged mode password. Specify if the service connection type is `Cisco IOS`.

CSV file example

```
APP01;Application server;app01.local;;RDP;;;;;DOMAIN\svc_app;Windows;;;;
WEB01;Corporate
website;portal.local;;WebTemplate;https://portal.local/;;https://portal.local/login
;FALSE;DOMAIN\svc_web;Windows;;;;
SSH01;Linux server;;192.168.0.50;SSH;;;;;;;;;
```

2. Navigate to the utility folder and run the command:

Windows

```
.\Pam.ConsoleApp.exe create-resources-from-file --file <file path>
```

Linux

```
dotnet ./Pam.ConsoleApp.dll create-resources-from-file --file <file path>
```

Delete a resource

To delete a resource from Axidian Privilege:

1. Navigate to the utility folder.
2. Run the command, specifying the resource name or its identifier:

Windows

```
.\Pam.ConsoleApp.exe delete-resource --name <resource name>
```

```
.\Pam.ConsoleApp.exe delete-resource --id <resource identifier>
```

Linux

```
dotnet ./Pam.ConsoleApp.dll delete-resource --name <resource name>
```

```
dotnet ./Pam.ConsoleApp.dll delete-resource --id <resource identifier>
```

The identifier is displayed in the URL in the resource profile.

Command examples

Windows

Delete a resource by name

```
.\Pam.ConsoleApp.exe delete-resource --name app01.local
```

Delete a resource by identifier

```
.\Pam.ConsoleApp.exe delete-resource --id a988f1b0-b871-43fa-a40c-6f4ac75f904c
```

Linux

Delete a resource by name

```
dotnet ./Pam.ConsoleApp.dll delete-resource --name app01.local
```

Delete a resource by identifier

```
dotnet ./Pam.ConsoleApp.dll delete-resource --id a988f1b0-b871-43fa-a40c-
6f4ac75f904c
```

Permission operations

Create a permission

Single permission

To create a permission in Axidian Privilege:

1. Navigate to the utility folder.

2. Run the utility with the parameters from the table:

Windows

```
.\Pam.ConsoleApp.exe create-permission <parameter> <value>
```

Linux

```
dotnet ./Pam.ConsoleApp.dll create-permission <parameter> <value>
```

Parameters

Parameter	Requirement	Description
`--user`	Required	PAM user name in UPN format
`--account`	Optional	PAM account name for connecting to the resource. If not specified, the user will be prompted to enter the account credentials when starting a session.
`--resources` or `--resources-group`	Required	Resource or resource group name. Specify in the format: ◦ `<resource name>:<connection type>` — for one or more resources ◦ `<group name>` — for a resource group
`--active-from`	Optional	Date and time when the permission becomes active. Specify in the format `DD.MM.YYYY HH:MM` or `DD.MM.YYYY`.
`--active-to`	Optional	Date and time when the permission is suspended. Specify in the format `DD.MM.YYYY HH:MM` or `DD.MM.YYYY`.
`--schedule-time-from`	Optional	Time when the permission can be used. Specify in the format `HH:MM`.
`--schedule-time-end`	Optional	Time when the permission cannot be used. Specify in the format `HH:MM`.

Parameter	Requirement	Description
`--schedule-time-utc`	Optional	Do not convert the specified access time from the current time zone to UTC: ◦ `true` — do not convert to UTC ◦ `false` — convert to UTC
`--allow-to-view-creds`	Optional	Allow the user to view the credentials of accounts added to the permission: ◦ `true` — allow ◦ `false` — deny
`--allow-to-change-creds`	Optional	Allow the user to change the credentials of accounts added to the permission: ◦ `true` — allow ◦ `false` — deny

Command examples

Windows

Create a permission for multiple resources

```
.\Pam.ConsoleApp.exe create-permission `
  --user ivanov@domain.local `
  --account DOMAIN\Administrator `
  --resources srv01.local:RDP,srv02.local:SSH
```

Create a permission for a resource group

```
.\Pam.ConsoleApp.exe create-permission `
  --user ivanov@domain.local `
  --account DOMAIN\Administrator `
  --resources-group PROD-SERVERS
```

Create a permission with time restrictions

```
.\Pam.ConsoleApp.exe create-permission `
  --user ivanov@domain.local `
  --resources srv01.local:SSH `
  --active-from "01.08.2026 09:00" `
  --active-to "31.08.2026 18:00" `
  --schedule-time-from 08:00 `
  --schedule-time-end 21:59 `
  --schedule-time-utc true `
  --allow-to-view-creds true `
  --allow-to-change-creds true
```

Linux

Create a permission for multiple resources

```
dotnet ./Pam.ConsoleApp.dll create-permission `
  --user ivanov@domain.local `
  --account DOMAIN\Administrator `
  --resources srv01.local:RDP,srv02.local:SSH
```

Create a permission for a resource group

```
dotnet ./Pam.ConsoleApp.dll create-permission `
  --user ivanov@domain.local `
  --account DOMAIN\Administrator `
  --resources-group PROD-SERVERS
```

Create a permission with time restrictions

```
dotnet ./Pam.ConsoleApp.dll create-permission `
  --user ivanov@domain.local `
  --account resource\Administrator `
  --resources srv01.local:SSH `
  --active-from "01.08.2026 09:00" `
  --active-to "31.08.2026 18:00" `
  --schedule-time-from 08:00 `
  --schedule-time-end 21:59 `
  --schedule-time-utc true `
  --allow-to-view-creds true `
  --allow-to-change-creds true
```

Multiple permissions

To create multiple permissions in Axidian Privilege:

1. Create a CSV file using the following template:

```
UserPrincipalName;AccountName;Resource1[:ConnectionType];Resource2[:ConnectionType];...;
ResourceN[:ConnectionType]
```

Parameters

Parameter	Requirement	Description
`UserPrincipalName`	Required	PAM user name in UPN format
`AccountName`	Required	Account name in the DOMAIN\user format. If not specified, the user will be prompted to enter the account credentials when starting a session.
`Resource[:ConnectionType]`	Required	Resource name and user connection type. Multiple resources can be specified. Example: `srv01.local:RDP;srv02.local:SSH`. If the resource has only one user connection, the connection type can be omitted.

CSV file example

```
ivanov@domain.local;DOMAIN\Administrator;srv01.local:RDP;srv02.local:SSH
petrov@domain.local;;linux01.local:SSH
```

2. Navigate to the utility folder and run the command:

Windows

```
.\Pam.ConsoleApp.exe create-permissions-from-file --file <file path>
```

Linux

```
dotnet ./Pam.ConsoleApp.dll create-permissions-from-file --file <file path>
```

Revoke a permission

> ⚠ **CAUTION**
> Revoked permissions cannot be restored. If you need to temporarily restrict the use of a permission, suspend it instead.

Single permission

To revoke a permission:

1. Navigate to the utility folder.
2. Run the following command:

Windows

Revoke a permission by number

```
.\Pam.ConsoleApp.exe revoke-permissions --permissions <permission numbers>
```

Revoke a user permission

```
.\Pam.ConsoleApp.exe revoke-permissions-by-user <parameter> <value>
```

Linux

Revoke a permission by number

```
dotnet ./Pam.ConsoleApp.dll revoke-permissions --permissions <permission numbers>
```

Revoke a user permission

```
dotnet ./Pam.ConsoleApp.dll revoke-permissions-by-user <parameter> <value>
```

Parameters

Parameter	Requirement	Description
`--user`	Required	PAM user name in UPN format
`--account`	Optional	Account name
`--resources` or `--resources-group`	Required	Resource or resource group name. Specify one of the parameters.

Command examples

Windows

Revoke user permissions by resources

```
.\Pam.ConsoleApp.exe revoke-permissions-by-user `
  --user ivanov@domain.local `
  --account DOMAIN\Administrator `
  --resources srv01.local:RDP,srv02.local:SSH
```

Revoke user permissions by resource group

```
.\Pam.ConsoleApp.exe revoke-permissions-by-user `
  --user ivanov@domain.local `
  --account DOMAIN\Administrator `
  --resources-group PROD-SERVERS
```

Linux

Revoke permissions for a resource

```
dotnet ./Pam.ConsoleApp.dll revoke-permissions-by-user `
  --user ivanov@domain.local `
  --account DOMAIN\Administrator `
  --resources srv01.local:RDP,srv02.local:SSH
```

Revoke user permissions for a resource group

```
dotnet ./Pam.ConsoleApp.dll revoke-permissions-by-user `
  --user ivanov@domain.local `
  --account DOMAIN\Administrator `
  --resources-group PROD-SERVERS
```

Multiple permissions

To revoke multiple permissions in Axidian Privilege:

1. Create a CSV file using the following template:

```
UserPrincipalName;AccountName;Resource1[:ConnectionType];Resource2[:ConnectionType];...;
ResourceN[:ConnectionType]
```

Parameters

Parameter	Requirement	Description
`UserPrincipalName`	Required	PAM user name in UPN format
`AccountName`	Required	Account name in the DOMAIN\user format. If not specified, the user will be prompted to enter the account credentials when starting a session.
`Resource[:ConnectionType]`	Required	Resource name and user connection type. Multiple resources can be specified. Example: `srv01.local:RDP;srv02.local:SSH`

CSV file example

```
ivanov@domain.local;DOMAIN\Administrator;srv01.local:RDP;srv02.local:SSH
petrov@domain.local;;linux01.local:SSH
```

2. Navigate to the utility folder and run the command:

Windows

```
.\Pam.ConsoleApp.exe revoke-permissions-from-file --file <file path>
```

Linux

```
dotnet ./Pam.ConsoleApp.dll revoke-permissions-from-file --file <file path>
```

After the command is executed, the specified permissions are set to the *Revoked* state.

Suspend a permission

An unused permission is a permission that has not been used within the period specified in the Monitoring settings. It is recommended to revoke or suspend such permissions.

To suspend unused permissions:

1. Navigate to the utility folder.
2. Run the following command:

Windows

```
.\Pam.ConsoleApp.exe suspend-unused-permissions
```

Linux

```
dotnet ./Pam.ConsoleApp.dll suspend-unused-permissions
```

After the command is executed, all unused permissions are set to the *Suspended* state.
The permission can be resumed at any time.

Troubleshooting

Certificate issues

What to do if certificates have expired or need to be replaced

Technical Support

Learn how to create a technical support request

Logs

2 items

Certificate issues

A certificate provides a secure HTTPS connection. If there are problems with the certificate, the browser cannot guarantee secure data exchange with the server, and the risk of data interception increases.

When it is necessary to replace a certificate:

- Outdated certificate data — the certificate contains outdated data, for example, the domain name, SAN (Subject Alternative Names), or server IP address.
  If the old certificate is retained, PAM will become unavailable.
- Compromise of the server's private key — the key becomes known and can be used by third parties.
  Replace certificates even if they have not yet expired.
- Expiration — the most common reason for certificate replacement.
  We recommend replacing certificates before they expire, otherwise PAM will become unavailable and the connection will be insecure for users.

  How to check when the certificate expires?

  If the user or administrator console does not open, and the browser address bar displays the error **Not secure**, check the certificate expiration date. Click on the warning in the address bar of your browser:

  - Microsoft Edge: go to **Not secure** → **Your connection to this site isn't secure** → .
  - Google Chrome: go to **Not secure** → **Certificate details**.

Root certificate of the CA

The CA root certificate must be replaced on all PAM servers, including the load balancer.
The certificate must be in PEM format with Base-64 encoding and use the SHA-256 signature algorithm. When replacing certificates, preserve the original file names.

> **INFO**
> If the new CA certificate is created with the same private keys, replacing certificates in the PAM installation is not required. When creating a certificate with a new key pair, it is necessary to replace all previously issued certificates throughout the entire PAM installation.

Windows

1. Export the root certificate without the private key with the extension .cer or .crt.
2. Right-click on the certificate file and select **Install Certificate** from the context menu.
3. In the certificate import wizard, for the **Store Location** parameter, select **Local Machine** and click **Next**.
4. Select **Place all certificates in the following store** and click **Browse**.
5. In the window that opens, select **Trusted Root Certification Authorities** and click **OK**.
6. Click **Next**.
7. Click **Finish** in the confirmation dialog.

Linux

1. Export the root certificate without the private key with the extension .crt.

   > **CAUTION**
   > The root certificate for the load balancer must be named `ca.crt`.

2. Place the certificate at the path `/etc/axidian/axidian-privilege/ca-certificates/`.

3. Open the terminal and navigate to the folder `/etc/axidian/axidian-privilege/` with elevated privileges:

   ```
   sudo -i
   ```

   ```
   cd /etc/axidian/axidian-privilege/
   ```

4. Stop all components:

   ```
   bash scripts/stop-pam.sh
   ```

5. Update permissions for the replaced files:

> ⚠ **CAUTION**
> It is necessary to run the command from the folder `/etc/axidian/axidian-privilege/`.

```
bash scripts/set-permissions.sh
```

6. Start the stopped components:

```
bash scripts/run-pam.sh
```

Server certificate

Replace the certificates on the target server. New certificates must meet the requirements and preserve the original file names.

Windows

1. Export the private key certificate in .pfx format.
2. Place the server certificate in the computer's personal certificates:
    1. Right-click on the certificate file and select **Install Certificate** from the context menu.
    2. In the certificate import wizard, for the **Store Location** parameter, select **Local Machine** and click **Next**.
       Enter the certificate password.
    3. Select **Place all certificates in the following store** and click **Browse**.
    4. In the window that opens, select **Personal** and click **OK**.
    5. Click **Finish** in the confirmation dialog.
3. Launch IIS Manager.
4. In the left **Connections** panel expand <FQDN> → **Sites** → **Default Web Site**.
5. Select **Default Web Site** and in the right **Actions** panel, click **Bindings**.

6. In the window that opens, replace the certificate for all bindings with type HTTPS and port 443:
    1. Select the binding and click **Edit**.
    2. In the window that opens, click **Select** and choose the imported certificate.
7. After replacing the certificates, in the left **Connections** panel, click on the server FQDN.
8. In the right Actions panel, click **Restart**.
9. Open the configuration file `C:\Program Files\Axidian\Axidian Privilege\Gateway\Pam.Gateway.Service\appsettings.json` with administrator rights
10. In the `Kestrel` section, specify the `Subject` value of the new certificate for the `Subject` parameter.

    Configuration file structure

    ```
    "Kestrel": {
      "Endpoints": {
        "HttpsInlineCertStore": {
          "Url": "https://0.0.0.0:5443",
          "Certificate": {
            "Subject": "dc.axidian.local", // Specify the value from the new certificate
            "Store": "My",
            "Location": "LocalMachine",
            "AllowInvalid": "False"
          }
        }
      }
    }
    ```

    If the server IP address is not specified in the SAN field of the new certificate, update the ProxyApp configuration:

    - Open the configuration file `C:\Program Files\Axidian\Axidian Privilege\Gateway\ProxyApp\appsettings.json`.
    - In the `GatewayService` section, replace the IP address with the server name in FQDN format.

Configuration file structure

```
"GatewayService": {
  "Url": "https://dc.axidian.local:5443" // Specify the server name in FQDN format
}
```

Linux

1. Export the public key certificate in PEM (Base-64) format with .crt extension.
2. Export the private key certificate in PEM (Base-64) format with .pem or .pfx extension.
   For a certificate with .pem extension, no preliminary preparation is required.

   If the certificate has .pfx extension, extract the keys from it using the commands:

   Key extraction

   ```
   openssl pkcs12 -in <public key certificate> -nocerts -out <private key certificate> -
   nodes -passin pass:<password>
   ```

   Certificate extraction

   ```
   openssl pkcs12 -in <private key certificate> -clcerts -nokeys -out <public key
   certificate> -passin pass:<password>
   ```

   - `<public key certificate>` — name of the exported certificate with .crt extension
   - `<private key certificate>` — name of the exported certificate with .pem or .pfx extension
   - `<password>` — password set when exporting the certificate
3. Place the certificates in the appropriate component folders:
   - Management Server: `/etc/axidian/axidian-privilege/certs`
     Replace the `pam.crt` and `pam.key` certificates. If the `pam-selfsigned.key` and `pam-selfsigned.crt` certificates are located in the folder, you do not need to change them.
   - RDP Proxy: `/etc/axidian/axidian-privilege/keys/rdp-proxy`
   - PostgreSQL Proxy: `/etc/axidian/axidian-privilege/keys/sql-proxy`
   - MSSQL Proxy: `/etc/axidian/axidian-privilege/keys/tsql-proxy`

- Web Proxy: `/etc/axidian/axidian-privilege/keys/web-proxy`

4. Open the terminal and navigate to the folder `/etc/axidian/axidian-privilege/` with elevated privileges:

```
sudo -i
```

```
cd /etc/axidian/axidian-privilege/
```

5. Stop all components:

```
bash scripts/stop-pam.sh
```

6. Update permissions for the replaced files:

> ⚠ **CAUTION**
> It is necessary to run the command from the folder `/etc/axidian/axidian-privilege/`.

```
bash scripts/set-permissions.sh
```

7. Start the stopped components:

```
bash scripts/run-pam.sh
```

RDS access server certificate

RDS access server certificates are managed through Server Manager, as they are used by the following services:

- RD Connection Broker: SSO
- RD Connection Broker: Publishing

To replace the certificate:

1. Export two private key certificates in .pfx format.
   Certificates must meet the requirements.

2. Open Server Manager.
3. Go to **Remote Desktop Services**.
4. In the **Deployment Overview** window, click **Tasks** and select **Edit Deployment Properties** from the drop-down list.
5. In the window that opens, select **Certificates**.
6. In the **Role Service** window, select **RD Connection Broker - Enable Single Sign On**.
7. Click **Select existing certificate...**.
8. Select **Choose a different certificate** and click **Browse**.
9. In the window that opens, select the certificate to import and click **Open**.
10. In the **Password** field, enter the certificate password.
11. Enable the **Allow the certificate to be added to the Trusted Root Certification Authorities certificate store on the destination computers** checkbox.
12. Click **OK** and **Apply**.
13. Repeat steps 6-12 for the **RD Connection Broker - Publishing role service**.

Technical Support

If you can't find the answer to your question in the documentation or knowledge base, you can contact support for help.

If you contact support to resolve a problem, please provide as much information as possible, including files, screenshots and logs. This will help to solve the problem quickly.

To submit a support request, please follow these steps:

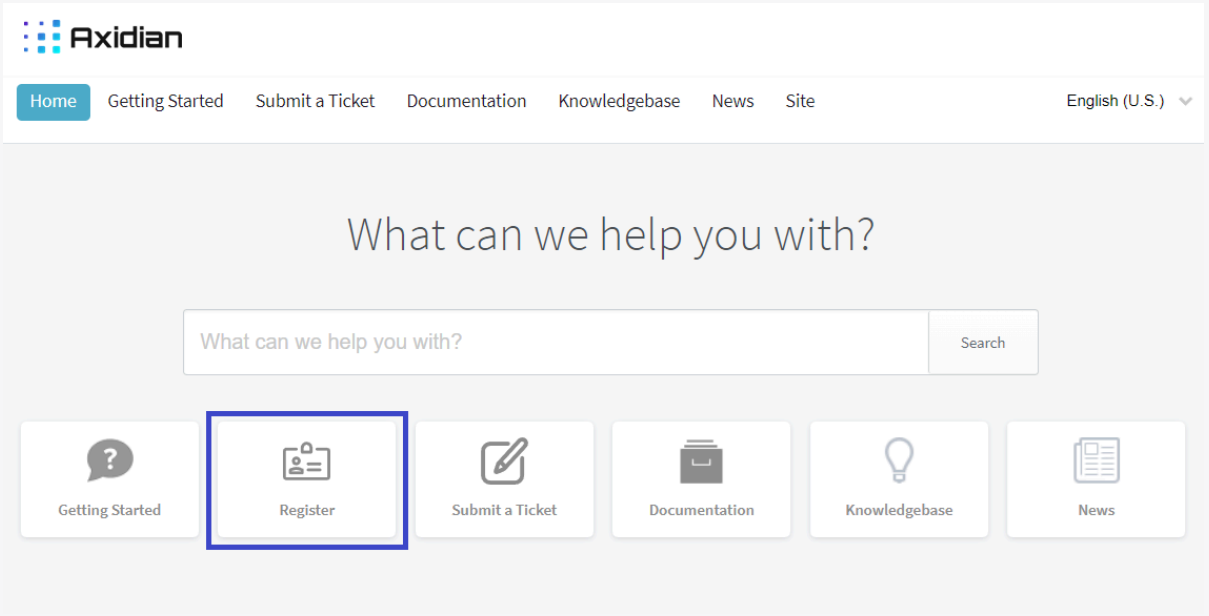
1. Open Technical Support Portal.
2. Enter your email address and password and click **Login**.

If you do not have a login and password

You can register on the support portal yourself or submit a registration request.

To register yourself:

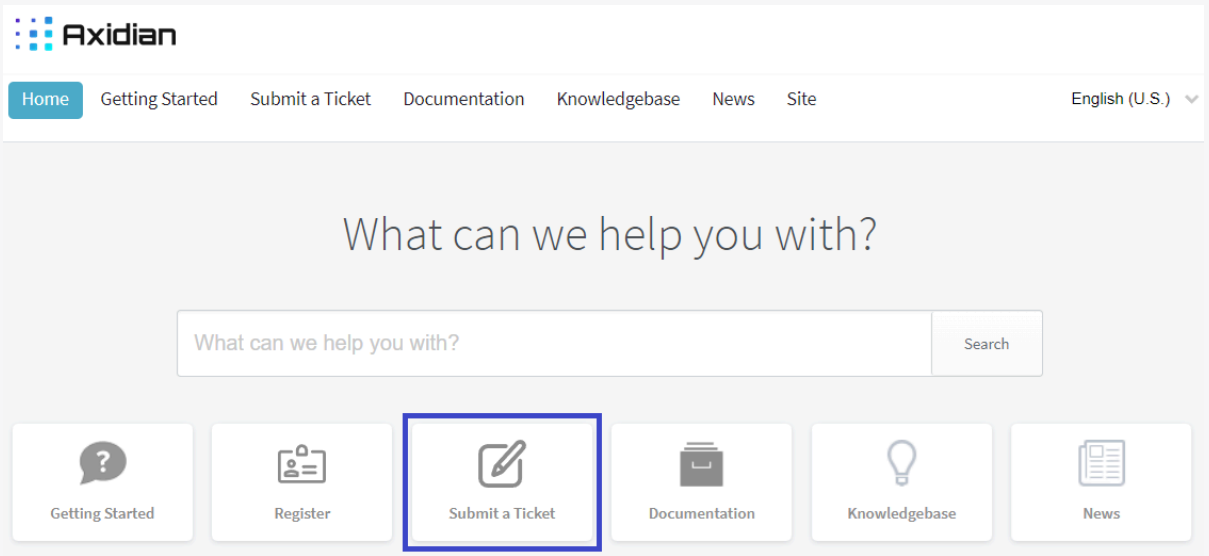
1. Click **Register**.



2. A registration form will appear. Fill in the fields and click **Register**.
3. Check the inbox of the specified email address. You will receive an email with a link to activate your account. Follow the link.

To submit a registration request:

1. Click **Submit a Ticket**.



2. A request form will appear. Indicate that this is an account creation request.
3. Check the inbox of the specified email address. You will receive an email with a link to activate your account. Follow the link.

3. Click **Submit a Ticket**.
4. Select department and click **Next**.
5. Fill in the fields and click **Submit**.

Logs

Collecting Logs of Server Components

Logs of Core Server, IDP, MC, UC, Log Server, Gateway, ProxyApp, SSH Proxy, PostgreSQL Proxy and RDP Proxy

Collecting Logs of Client Components

Logs of PamSU and Desktop Console

Collecting Logs of Server Components

Logging Levels

Depending on how detailed the information about the component's operation needs to be, different logging levels can be set. They determine how important and detailed the information will be recorded in log files. This allows for more efficient filtering and analysis of logs.

It is recommended to use the `Trace` logging level as the most detailed.

Logging Levels

Logging Level	Sequential Number	Description
Trace	0	Most detailed level. All information about the component's operation processes is recorded, including details about API method calls.
Debug	1	Details about the component's operation progress, significant variables, and other data that may be useful in detecting and fixing errors are recorded.
Info	2	Informational messages are recorded that notify about normal component functioning. They may include events such as starting or stopping processes, editing user profiles, and others.
Warn	3	Warnings and notifications about potential errors and abnormal situations are recorded. Events are not critical but require attention. At the same time, the component can continue operating.
Error	4	Errors that have led to incorrect component operation or the occurrence of serious problems are recorded. Logs indicate problems that require intervention and correction.
Fatal	5	The least detailed logging level. Only the most critical errors and problems that lead to immediate termination of the component or other serious consequences are recorded. Logs usually indicate serious failures that require immediate intervention and correction.

Collecting installation script logs

The installation script `run-deploy.sh` may terminate with an error. In this case, you need to send the log files to technical support.

Path to log files: `AxidianPAM_3.5/axidian-pam/logs/web-wizard/`

Example

```
Failed: Ansible playbook returned error code: 2
```

Axidian Privilege Core

Windows

Enabling Logging

1. Open the configuration file `C:\inetpub\wwwroot\core\appsettings.json`.
2. Edit the `NLog` section:
   - set the `minlevel` parameter to `Trace`.
   - set the `dbMinLevel` parameter to `Trace`.

   Example

   ```
   "NLog": {
     "variables": {
       "minLevel": "Trace",
       "dbMinLevel": "Trace",
       "maxArchiveFilesPerCategory": 23
   }
   ```

3. Save the file.

After editing the configuration file, restart the application pool:

1. Run PowerShell as administrator.
2. Execute the command:

```
C:\Windows\System32\inetsrv\appcmd.exe recycle apppool Axidian.Privilege.Core
```

Collecting Logs

1. Clear the existing Privilege Core server logs in the folder `C:\inetpub\wwwroot\core\Logs`.
2. Reproduce the problem.
3. Collect an archive with logs and send it to technical support. Describe the user's actions and specify the exact time when the problem occurred.

Linux

Enabling Logging

1. Open the configuration file `/etc/axidian/axidian-privilege/core/appsettings.json`.
2. Edit the `NLog` section:
   - set the `minlevel` parameter to `Trace`.
   - set the `dbMinLevel` parameter to `Trace`.

Example

```
"NLog": {
  "variables": {
    "minLevel": "Trace",
    "dbMinLevel": "Trace",
    "maxArchiveFilesPerCategory": 23
  }
```

3. Save the file.
4. Go to the folder with PAM scripts and restart the component:

```
cd /etc/axidian/axidian-privilege/scripts/
```

```
bash restart-pam.sh core
```

Collecting Logs

1. Clear existing logs in the folder `/etc/axidian/axidian-privilege/logs/core`.
2. Reproduce the problem.
3. Collect an archive with logs and send it to technical support. Describe the user's actions and specify the exact time when the problem occurred.

Axidian Privilege Idp

Windows

Enabling Logging

1. Open the configuration file `C:\inetpub\wwwroot\idp\appsettings.json`.
2. Edit the `NLog` section:
   - set the `minlevel` parameter to `Trace`.
   - set the `dbMinLevel` parameter to `Trace`.

   Example

   ```
   "NLog": {
     "variables": {
       "minLevel": "Trace",
       "dbMinLevel": "Trace",
       "maxArchiveFilesPerCategory": 23
   }
   ```

3. Save the file.

After editing the configuration file, restart the application pool:

1. Run PowerShell as administrator.
2. Execute the command:

   ```
   C:\Windows\System32\inetsrv\appcmd.exe recycle apppool Axidian.Privilege.Idp
   ```

Collecting Logs

1. Clear existing logs in the folder `C:\inetpub\wwwroot\idp\Logs`.

2. Reproduce the problem.
3. Collect an archive with logs and send it to technical support. Describe the user's actions and specify the exact time when the problem occurred.

Linux

Enabling Logging

1. Open the configuration file `/etc/axidian/axidian-privilege/idp/appsettings.json`.
2. Edit the `NLog` section:
   - set the `minlevel` parameter to `Trace`.
   - set the `dbMinLevel` parameter to `Trace`.

Example

```
"NLog": {
  "variables": {
    "minLevel": "Trace",
    "dbMinLevel": "Trace",
    "maxArchiveFilesPerCategory": 23
}
```

3. Save the file.
4. Go to the folder with PAM scripts and restart the component:

```
cd /etc/axidian/axidian-privilege/scripts/
```

```
bash restart-pam.sh idp
```

Collecting Logs

1. Clear existing logs in the folder `/etc/axidian/axidian-privilege/logs/idp`.
2. Reproduce the problem.
3. Collect an archive with logs and send it to technical support. Describe the user's actions and specify the exact time when the problem occurred.

Axidian Privilege Log Server

Windows

Enabling Logging

1. Open the configuration file `C:\inetpub\wwwroot\ls\appsettings.json`.
2. Edit the `NLog` section:
   - set the `minlevel` parameter to `Trace`.
   - set the `dbMinLevel` parameter to `Trace`.

   Example

   ```
   "NLog": {
     "variables": {
       "minLevel": "Trace",
       "dbMinLevel": "Trace",
       "maxArchiveFilesPerCategory": 23
   }
   ```

3. Save the file.

After editing the configuration file, restart the application pool:

1. Run PowerShell as administrator.
2. Execute the command:

   ```
   C:\Windows\System32\inetsrv\appcmd.exe recycle apppool Axidian.Privilege.LS
   ```

Collecting Logs

1. Clear existing logs in the folder `C:\inetpub\wwwroot\ls\Logs`.
2. Reproduce the problem.
3. Collect an archive with logs and send it to technical support. Describe the user's actions and specify the exact time when the problem occurred.

Linux

Enabling Logging

1. Open the configuration file `/etc/axidian/axidian-privilege/ls/appsettings.json`.
2. Edit the `NLog` section:
   - set the `minlevel` parameter to `Trace`.
   - set the `dbMinLevel` parameter to `Trace`.

Example

```
"NLog": {
  "variables": {
    "minLevel": "Trace",
    "dbMinLevel": "Trace",
    "maxArchiveFilesPerCategory": 23
}
```

3. Save the file.
4. Go to the folder with PAM scripts and restart the component:

```
cd /etc/axidian/axidian-privilege/scripts/
```

```
bash restart-pam.sh ls
```

Collecting Logs

1. Clear existing logs in the folder `/etc/axidian/axidian-privilege/logs/ls`.
2. Reproduce the problem.
3. Collect an archive with logs and send it to technical support. Describe the user's actions and specify the exact time when the problem occurred.

Axidian Privilege Gateway Service

Windows

Enabling Logging

1. Open the configuration file `C:\Program Files\Axidian\Axidian Privilege\Gateway\Pam.Gateway.Service\appsettings.json`.
2. Edit the `NLog` section:
   - set the `minlevel` parameter to `Trace`.
   - set the `dbMinLevel` parameter to `Trace`.

   Example

   ```
   "NLog": {
     "variables": {
       "minLevel": "Trace",
       "dbMinLevel": "Trace",
       "maxArchiveFilesPerCategory": 23
   }
   ```

3. Save the file.

After editing the configuration file, restart Pam.Gateway.Service:

1. Open the **Services**.
2. Find **Pam.Gateway.Service** in the services list.
3. Right-click the service and select **Restart**.

Collecting Logs

1. Clear existing logs in the folder `C:\Program Files\Axidian\Axidian Privilege\Gateway\Pam.Gateway.Service\logs`.
2. Reproduce the problem.
3. Collect an archive with logs and send it to technical support. Describe the user's actions and specify the exact time when the problem occurred.

Linux

Enabling Logging

1. Open the configuration file `etc/axidian/axidian-privilege/gateway-service/appsettings.json`.
2. Edit the `NLog` section:
   - set the `minlevel` parameter to `Trace`.
   - set the `dbMinLevel` parameter to `Trace`.

Example

```
"NLog": {
  "variables": {
    "minLevel": "Trace",
    "dbMinLevel": "Trace",
    "maxArchiveFilesPerCategory": 23
}
```

3. Save the file.
4. Go to the folder with PAM scripts and restart the component:

```
cd /etc/axidian/axidian-privilege/scripts/
```

```
bash restart-pam.sh gw-service
```

Collecting Logs

1. Clear existing logs in the folder `/etc/axidian/axidian-privilege/logs/gateway-service`.
2. Reproduce the problem.
3. Collect an archive with logs and send it to technical support. Describe the user's actions and specify the exact time when the problem occurred.

Axidian Privilege ProxyApp

Enabling Logging

1. Open the configuration file `C:\Program Files\Axidian\Axidian Privilege\Gateway\ProxyApp\appsettings.json`.
2. Set the `defaultMinLevel` parameter to `Trace`.

Example

```
"NLog": {
  "variables": {
    "defaultMinLevel": "Trace",
    "maxArchiveFilesPerCategory": 23
}
```

3. Save the file.

After editing the configuration file, restart Pam.Service:

1. Open the **Services**.
2. Find **Pam.Service** in the services list.
3. Right-click the service and select **Restart**.

Collecting Logs

1. Clear existing logs in the folder `C:\Program Files\Axidian\Axidian Privilege\Gateway\ProxyApp\logs`.
2. Reproduce the problem.
3. Collect an archive with logs and send it to technical support. Describe the user's actions and specify the exact time when the problem occurred.

Privilege SSH Proxy

Enabling Logging

1. Open the configuration file `/etc/axidian/axidian-privilege/ssh-proxy/appsettings.json`.
2. Set the `LogLevel` parameter to `Trace`.

Example

```
"LogLevel": "TRACE",
"LogStream": "FILE",
"MaxLogFiles": 100,
"MaxLogFileSize": 10000000,
```

3. Save the file.

4. Go to the folder with PAM scripts and restart the component:

```
cd /etc/axidian/axidian-privilege/scripts/
```

```
bash restart-pam.sh ssh-proxy
```

Collecting Logs

1. Clear existing logs in the folder `/etc/axidian/axidian-privilege/logs/ssh`.
2. Reproduce the problem.
3. Collect an archive with logs and send it to technical support. Describe the user's actions and specify the exact time when the problem occurred.

Axidian Privilege PostgreSQL Proxy

Enabling Logging

1. Open the configuration file `/etc/axidian/axidian-privilege/sql-proxy/appsettings.json`.

2. Set the `LogLevel` parameter to `Trace`.

Example

```
"LogLevel": "TRACE",
"LogStream": "FILE",
"MaxLogFiles": 100,
"MaxLogFileSize": 10000000,
```

3. Save the file.

4. Go to the folder with PAM scripts and restart the component:

```
cd /etc/axidian/axidian-privilege/scripts/
```

```
bash restart-pam.sh sql-proxy
```

Collecting Logs

1. Clear existing logs in the folder `/etc/axidian/axidian-privilege/logs/sql`.
2. Reproduce the problem.
3. Collect an archive with logs and send it to technical support. Describe the user's actions and specify the exact time when the problem occurred.

Axidian Privilege MSSQL Proxy

Enabling Logging

1. Open the configuration file `/etc/axidian/axidian-privilege/tsql-proxy/appsettings.json`.
2. Set the `LogLevel` parameter to `Trace`.

   Example

   ```
   "LogLevel": "TRACE",
   "LogStream": "FILE",
   "MaxLogFiles": 100,
   "MaxLogFileSize": 10000000,
   ```

3. Save the file.
4. Go to the folder with PAM scripts and restart the component:

   ```
   cd /etc/axidian/axidian-privilege/scripts/
   ```

   ```
   bash restart-pam.sh tsql-proxy
   ```

Collecting Logs

1. Clear existing logs in the folder `/etc/axidian/axidian-privilege/logs/tsql`.
2. Reproduce the problem.
3. Collect an archive with logs and send it to technical support. Describe the user's actions and specify the exact time when the problem occurred.

Axidian Privilege RDP Proxy

Enabling Logging

1. Open the configuration file `/etc/axidian/axidian-privilege/rdp-proxy/appsettings.json`.
2. Set the `LogLevel` parameter to `Trace`.

Example

```
"LogLevel": "TRACE",
"LogStream": "FILE",
"MaxLogFiles": 100,
"MaxLogFileSize": 10000000,
```

3. Save the file.
4. Go to the folder with PAM scripts and restart the component:

```
cd /etc/axidian/axidian-privilege/scripts/
```

```
bash restart-pam.sh rdp-proxy
```

Collecting Logs

1. Clear existing logs in the folder `/etc/axidian/axidian-privilege/logs/rdp`.
2. Reproduce the problem.
3. Collect an archive with logs and send it to technical support. Describe the user's actions and specify the exact time when the problem occurred.

Axidian Privilege Web Proxy

Enabling Logging

1. Open the configuration file `/etc/axidian/axidian-privilege/web-proxy/appsettings.json`.
2. Set the `LogLevel` parameter to `Trace`.

Example

```
"Settings": {
  "CoreUrl": "PAM_CORE_URL",
  "IdpUrl": "PAM_IDP_URL",
  "ClientSecret": "PAM_WEB_PROXY_SECRET",
  "LogLevel": "TRACE",
  "LogStream": "FILE",
  "MaxLogFiles": 30,
  "MaxLogFileSize": 10000000,
  "RateLimit": {
    "VolumePerTimeMBytes": 100,
    "TimeForFullVolumeSec": 60,
    "TimeForOneAdditionSec": 1
}
```

3. Save the file.

4. Go to the folder with PAM scripts and restart the component:

```
cd /etc/axidian/axidian-privilege/scripts/
```

```
bash restart-pam.sh web-proxy
```

Collecting Logs

1. Clear existing logs in the folder `/etc/axidian/axidian-privilege/logs/web`.
2. Reproduce the problem.
3. Collect an archive with logs and send it to technical support. Describe the user's actions and specify the exact time when the problem occurred.

Collecting Logs of Client Components

Axidian Privilege PamSU

Enabling Logging

1. Open the configuration file `/etc/pamsu.conf`.
2. Set the `Set log_level` parameter to `INFO`.

Example

```
# Log level is minimum level of logging
# You can choose between
# INFO, WARN ERROR and FATAL
Set log_level INFO
```

3. Save the file.

Collecting Logs

1. Clear existing logs in the folder `/opt/Axidian-Privilege/pamsu/logs/`.
2. Reproduce the problem.
3. Collect an archive with logs and send it to technical support. Describe the user's actions and specify the exact time when the problem occurred.

Axidian Privilege Desktop Console

Enabling Logging

1. Run **Axidian Privilege Desktop Console** as administrator.
2. Click **Tools** and go to **Options** section.
3. Go to the **Notifications** section in the left menu.
4. Select the **Log to application directory** checkbox and do not change the current file path.
5. Enable the **Debug**, **Information**, **Warnings**, and **Errors** logging levels.
6. Click **OK**.
7. Restart the **Axidian Privilege Desktop Console** application.

Collecting Logs

1. Clear existing logs in the folder `C:\Users\[Username]\AppData\Roaming\Axidian Privilege Desktop Console`.
2. Reproduce the problem.
3. Collect an archive with logs and send it to technical support. Describe the user's actions and specify the exact time when the problem occurred.

Axidian Privilege Web Terminal

Enabling Logging

1. Open the configuration file `/etc/axidian/axidian-privilege/web-terminal-proxy/appsettings.json`.
2. Set the `LogLevel` parameter to `Trace`.

Example

```
{
  "Settings": {
     "Port": "4822",
     "LogLevel": "TRACE",
     "LogStream": "BOTH",
     "MaxLogFiles": 10,
     "MaxLogFileSize": 1000000
     "Host": "0.0.0.0",
  }
}
```

3. Save the file.
4. Go to the folder with PAM scripts and restart the component:

```
cd /etc/axidian/axidian-privilege/scripts/
```

```
bash restart-pam.sh web-terminal-proxy
```

Collecting Logs

1. Clear existing logs in the folder `/etc/axidian/axidian-privilege/logs/web-terminal`.
2. Reproduce the problem.

3. Collect an archive with logs and send it to technical support. Describe the user's actions and specify the exact time when the problem occurred.

References

Events

Events of Axidian Privilege

Claims

List of privileges that can be included in roles

Mapping user directory and PAM attributes

List of default values for user directory attributes and mapping Axidian Privilege attributes

Events

This section contains a list of Axidian Privilege events.

Axidian Privilege keeps records of the following types of events:

- information is a message with information about changes to any data in the PAM, while the PAM is working correctly
- error — notification of a problem that requires the intervention of the PAM administrator
- warning — informing that a problem or error may appear in the future, the attention of the PAM administrator is recommended

Info

Code	Event
1000	Account successfully registered
1003	Account name successfully changed
1004	Account successfully restored
1008	Account password successfully added
1009	Account successfully disabled
1010	Permission successfully created
1013	Permission successfully revoked
1014	Resource successfully registered
1015	Resource successfully removed
1016	Resource info successfully updated
1017	Session successfully opened
1018	User closed the session

Code	Event
1021	Configuration successfully updated
1022	Domain successfully registered
1023	Domain successfully removed
1024	Domain successfully updated
1025	Session successfully aborted
1026	Account successfully enabled
1027	Account successfully removed
1028	Resource successfully disabled
1029	Resource successfully enabled
1033	No unregistered accounts detected
1034	Account password successfully reset
1035	Account successfully ignored
1036	Policy was successfully created
1037	Policy name successfully changed
1038	Policy settings successfully updated
1039	Policy was successfully created by copying
1040	Account policy successfully changed
1041	Domain successfully enabled
1042	Domain successfully restored
1043	Resource successfully restored
1044	User is successfully authenticated by two factor

Code	Event
1045	Account is successfully made managed
1046	Account SSH key successfully checked
1048	Account SSH key successfully added
1049	Account SSH key successfully reset
1052	Accounts synchronization job has been started
1053	Accounts synchronization job has been finished
1055	Change credentials job has been started
1056	Change credentials job has been finished
1057	Credentials verification job has been started
1058	Credentials verification job has been finished
1059	Service connection testing job has been started
1060	Service connection testing job has been finished
1064	SSH template successfully added
1065	SSH template successfully removed
1066	SSH template successfully updated
1067	User connection successfully added
1068	User connection successfully removed
1069	User connection successfully updated
1070	User viewed account credentials
1071	License for users and resources successfully registered
1072	Session artifacts rotation job has been started

Code	Event
1073	Session artifacts rotation job has been completed
1074	Session video has been removed according to the rotation policy configuration
1075	Session screenshots have been removed according to the rotation policy configuration
1077	Resources synchronization has been started
1078	Resources synchronization has been finished
1080	Found changes of groups for account
1081	Session transferred files have been removed according to the rotation policy configuration
1082	User enrolled two factor authenticator
1083	User authenticator successfully reset
1085	Permission successfully reactivated
1086	Permission successfully suspended
1088	Domain privileged groups successfully registered
1089	Container list for searching domain resources successfully changed
1090	Domain resources synchronization job has been started
1091	Domain resources synchronization job has been finished
1095	New role is added
1096	Role is removed
1097	Set of role privileges is changed
1098	Role name is changed
1099	New member is added to role
1100	Member is removed from role

Code	Event
1101	Resource group successfully created
1102	Resource group successfully removed
1103	Resource group info successfully updated
1104	Resource is successfully added to resource group
1105	Resource is successfully removed from resource group
1106	Confirmation of request for a session is successfully used
1107	Request for a session is rejected
1108	User sent request for a session
1109	Request to open a session is confirmed
1110	User canceled request for a session
1111	Confirmation of request for a session is timed out
1112	Request for a session is timed out
1114	Session policy successfully set for user
1115	Policy successfully removed
1117	License for sessions successfully registered
1118	Request to view credentials is rejected
1119	User sent credentials viewing request
1120	Request to view credentials is confirmed
1121	User canceled credentials viewing request
1122	Confirmation of credentials viewing request is timed out
1123	Request to view credentials is timed out

Code	Event
1124	User connection successfully added to resource
1125	Resource user connection successfully updated
1126	User connection successfully removed from resource
1127	Policy of object successfully changed
1128	Account password successfully fixed
1129	Account SSH key successfully fixed
1130	Priority of policy successfully changed
1131	Set of sections for the policy successfully changed
1132	Policy name successfully changed
1135	Unmanaged SSH keys successfully removed
1136	Container for searching domain resources successfully removed
1137	Domain privileged group successfully removed
1138	Administrator is successfully added to application
1139	Application name successfully changed
1140	Application successfully added
1141	Administrator is successfully removed from application
1142	Application successfully removed
1143	Application password successfully reset
1144	Application description successfully changed
1145	User viewed application credentials
1146	Organizational unit was successfully created

Code	Event
1147	Organizational unit name successfully changed
1148	Organizational unit successfully removed
1149	2FA requirement for a user successfully changed
1150	Application successfully received account credentials
1151	Application IP address successfully changed
1152	Application certificate successfully changed
1153	Organizational unit of object successfully changed
1154	License for AAPM successfully registered
1155	License for users successfully registered
1156	License for resources successfully registered
1157	User group successfully created
1158	User group successfully removed
1159	User group info successfully updated
1160	User is successfully added to user group
1161	User is successfully removed from user group
1162	User is successfully authenticated
1163	Application is successfully authenticated
1164	Account password successfully removed
1165	Account SSH key successfully removed
1166	License for sessions successfully removed
1167	License for AAPM successfully removed

Code	Event
1168	License for users successfully removed
1169	License for resources successfully removed
1170	Network location was successfully created
1171	Network location was successfully updated
1172	Network location successfully removed
1173	Catalog group synchronization completed
1174	Catalog groups synchronization job has been started
1175	Catalog groups synchronization job has been finished
1176	Session successfully created
1178	User successfully activated
1179	User successfully blocked
1181	Connection with PAM Agent restored
1182	Service successfully registered
1183	Service successfully removed
1184	Service successfully updated
1185	Service log on account password successfully set
1186	Service restart: Successful
1187	Service restart: Not required
1188	Custom service connection type successfully created
1189	Custom service connection type successfully updated
1190	Custom service connection type successfully removed

Code	Event
1191	User is successfully created
1192	Tag was successfully created
1193	Tag successfully removed
1194	Tag was successfully updated
1195	User info successfully updated
1196	User successfully removed
1197	License for Ad hoc resources successfully registered
1198	License for Ad hoc resources successfully removed
1199	License for SQL Proxy successfully registered
1200	License for SQL Proxy successfully removed
1201	Public key successfully added for user
1202	Public key successfully deleted from user
1203	The user password has been successfully reset
1204	Password change is forced for the user at the next login
1205	User has successfully changed their password
1209	PAM server added to monitoring
1210	PAM server information updated in monitoring
1211	PAM server removed from monitoring
1212	Certificate Subject for user successfully changed
1214	Server operation restored
1215	User's Subject Identifier from the external Identity Provider successfully deleted

Error

Code	Event
2000	Failed to register account
2003	Failed to change account name
2004	Failed to restore account
2008	Failed to add account password
2009	Failed to disable account
2010	Failed to create permission
2013	Failed to revoke permission
2014	Failed to register resource
2015	Failed to remove resource
2016	Failed to update resource info
2017	Failed to open session
2018	An error occurred during the closing of the session
2019	Failed to save session text log
2020	Failed to save session video stream
2021	Failed to update configuration
2022	Failed to register domain
2023	Failed to remove domain
2024	Failed to update domain info
2025	Failed to abort session

Code	Event
2026	Failed to enable account
2027	Failed to remove account
2028	Failed to disable resource
2029	Failed to enable resource
2030	Failed to save session screenshot
2031	Failed to check account password
2032	Failed to perform accounts search
2034	Failed to reset account password
2035	Failed to ignore account
2036	Failed to create policy
2037	Failed to change policy name
2038	Failed to update policy settings
2039	Failed to copy policy
2040	Failed to change account policy
2041	Failed to enable domain
2042	Failed to restore domain
2043	Failed to restore resource
2044	User is failed to authenticate by two factor
2045	Failed to make account managed
2046	Failed to check account SSH key
2048	Failed to add account SSH key

Code	Event
2049	Failed to reset account SSH key
2051	Can not open service connection to resource
2053	Failed to complete accounts synchronization
2054	Can not open service connection to domain
2056	Failed to complete change credentials job
2058	Failed to complete credentials verification job
2060	Failed to complete service connection testing job
2064	Failed to add SSH template
2065	Failed to remove SSH template
2066	Failed to update SSH template
2067	Failed to add user connection
2068	Failed to remove user connection
2069	Failed to update user connection
2070	Failed to provide account credentials for user
2071	Failed to register license
2073	Failed to complete session artifacts rotation job
2076	Failed to remove the session logs
2078	Failed to complete resources synchronization
2079	The server storage is unavailable
2080	Failed to change account groups
2082	User is failed to enroll two factor authenticator

Code	Event
2083	Failed to reset user authenticator
2085	Failed to reactivate permission
2086	Failed to suspend permission
2087	Failed to synchronize resource info
2088	Failed to register domain privileged groups
2089	Failed to change container list for searching domain resources
2091	Failed to complete domain resources synchronization job
2092	Failed to perform domain resources search
2095	Failed to create role
2096	Failed to remove role
2097	Failed to change role privileges
2098	Failed to change role name
2099	Failed to add new member to role
2100	Failed to remove member from role
2101	Failed to create resource group
2102	Failed to remove resource group
2103	Failed to update resource group info
2104	Failed to add resource to resource group
2105	Failed to remove resource from resource group
2106	Failed to use confirmation of the request for a session
2107	Failed to reject the request for a session

Code	Event
2108	Failed to send request for a session
2109	Failed to confirm the request for a session
2110	Failed to cancel request for a session
2114	Failed to set session policy for user
2115	Failed to remove policy
2118	Failed to reject the credentials viewing request
2119	Failed to send credentials viewing request
2120	Failed to confirm the credentials viewing request
2121	Failed to cancel credentials viewing request
2124	Failed to add user connection to resource
2125	Failed to update resource user connections
2126	Failed to remove user connection from resource
2127	Failed to change policy of object
2130	Failed to change policy priority
2131	Failed to change set of sections for the policy
2132	Failed to change policy name
2133	Failed to check account unmanaged SSH keys
2135	Failed to remove unmanaged SSH keys
2136	Failed to remove container for searching domain resources
2137	Failed to remove domain privileged group
2138	Failed to add administrator to application

Code	Event
2139	Failed to change application name
2140	Failed to create application
2141	Failed to remove administrator from application
2142	Failed to remove application
2143	Failed to reset application password
2144	Failed to change application description
2145	Failed to view application credentials
2146	Failed to create organizational unit
2147	Failed to change organizational unit name
2148	Failed to remove organizational unit
2149	Failed to change 2FA requirement state
2150	Failed to provide account credentials for application
2151	Failed to change application IP address
2152	Failed to change application certificate
2153	Failed to change organizational unit of object
2157	Failed to create user group
2158	Failed to remove user group
2159	Failed to update user group info
2160	Failed to add user to user group
2161	Failed to remove user from user group
2162	User is failed to authenticate

Code	Event
2163	Application is failed to authenticate
2164	Failed to remove account password
2165	Failed to remove account SSH key
2170	Failed to create network location
2171	Failed to update network location
2172	Failed to remove network location
2173	Failed to synchronize catalog user group
2175	Failed to complete Catalog groups synchronization
2176	Failed to create session
2178	Failed to activate user
2179	Failed to block user
2182	Failed to register service
2183	Failed to remove service
2184	Failed to update service info
2185	Failed to set service log on account password
2186	Service restart: Failed
2188	Failed to create service connection type
2189	Failed to update service connection type
2190	Failed to remove service connection type
2191	Failed to create user
2192	Failed to create tag

Code	Event
2193	Failed to remove tag
2194	Failed to update tag
2195	Failed to update user info
2196	Failed to remove user
2201	Failed to add public key for user
2202	Failed to delete user public key
2203	Failed to reset user password
2204	Failed to enable user password change at next login
2205	Failed to change user password
2207	Failed to check account secrets rotation
2209	Failed to add PAM server to monitoring
2210	Failed to update PAM server information
2211	Failed to remove PAM server from monitoring
2212	Failed to change user certificate Subject
2213	Server failure detected
2215	Failed to delete the user's Subject Identifier from the external Identity Provider

Warning

Code	Event
3047	Account SSH key is invalid
3061	Account was not found

Code	Event
3084	User is locked
3087	Resource information has been updated
3093	Unregistered accounts detected
3094	Account password is invalid
3113	Attempt to execute forbidden command
3116	Session interrupted
3134	Unmanaged SSH keys detected
3177	User group was not found in catalog
3180	Lost connection with PAM Agent
3206	Inactive users detected
3208	Unused permissions detected

Claims

This section contains a list of privileges that can be included in roles.

ID	Name
Users management	
User.Create	Create new users
User.Read	Read users
User.Update	Update users
User.Delete	Delete users
User.Reset2FA	Reset 2FA for user
User.SetPolicy	Set policy for user
User.ManageSshAuthorizedKeys	Manage SSH authorized keys
User.PasswordManagement	Manage password for internal user
User.ManageX509Certificate	Manage X.509 certificate Subject for users
User groups management	
UsersGroup.Create	Create user groups
UsersGroup.Delete	Delete user groups
UsersGroup.Read	Read user groups
UsersGroup.Update	Update user groups
UsersGroup.SetPolicy	Set policy for user groups
Permissions management	

ID	Name
Permission.Create	Create permissions
Permission.Read	Read permissions
Permission.Revoke	Revoke permissions
Permission.Suspend	Suspend and reactivate permissions
Accounts management	
Account.Create	Create accounts
Account.Read	Read accounts
Account.Update	Update accounts
Account.Restore	Restore credentials of accounts to previously used ones
Account.Delete	Delete accounts
Account.Block	Block accounts
Account.Manage	Make accounts managed
Account.Ignore	Ignore accounts
Account.SetPolicy	Set policy for account
Account.Credentials.Check	Check account credentials
Account.Credentials.Update	Update account credentials
Resources management	
Resource.Create	Create resources
Resource.Read	Read resources
Resource.Update	Update resources

ID	Name
Resource.Restore	Restore deleted resources
Resource.Delete	Delete resources
Resource.Block	Block resources
Resource.CheckConnection	Check connection to resource
Resource.Sync	Synchronize resources
Resource.SetPolicy	Set policy for resource
Resource.SetOrganizationalUnit	Set organizational unit for resource
Resource.TagManagement	Resource tags management
Resource groups management	
ResourcesGroup.Create	Create resource groups
ResourcesGroup.Read	Read resource groups
ResourcesGroup.Update	Update resource groups
ResourcesGroup.Delete	Delete resource groups
ResourcesGroup.SetOrganizationalUnit	Set organizational unit for resource group
Domains management	
Domain.Create	Create domains
Domain.Read	Read domains
Domain.Update	Update domains
Domain.Restore	Restore deleted domains
Domain.Delete	Delete domains

ID	Name
Domain.CheckConnection	Check connection to domain
Domain.AccountsSync	Synchronize domain accounts
Domain.ResourcesImport	Import resources from domain
Domain.SetPolicy	Set policy for domain
Domain.PrivilegedGroups.Create	Create privileged groups on domain
Domain.PrivilegedGroups.Read	Read privileged groups on domain
Domain.PrivilegedGroups.Delete	Delete privileged groups on domain
Domain.ResourceContainer.Create	Create resource containers on domain
Domain.ResourceContainer.Read	Read resource containers on domain
Domain.ResourceContainer.Delete	Delete resource containers on domain
Sessions management	
Session.Read	Read sessions
Session.Abort	Abort sessions
Session requests management	
SessionRequest.Read	Read session requests
SessionRequest.Confirm	Confirm sessions
Credentials viewing requests management	
CredentialsViewingRequest.Read	Read credentials viewing requests
CredentialsViewingRequest.Confirm	Confirm account credentials viewing requests

ID	Name
Event Log	
Event.Read	Read events
Policies management	
Policy.Create	Create policies
Policy.Read	Read policies
Policy.Update	Update policies
Policy.Delete	Delete policies
System settings management	
SystemSettings.Read	Read system settings
SystemSettings.Update	Update system settings
Licenses management	
License.Create	Add licenses
License.Read	Read licenses
License.Delete	Delete licenses
SSH templates management	
SshTemplate.Create	Import SSH templates
SshTemplate.Read	Read SSH templates
SshTemplate.Delete	Delete SSH templates

ID	Name
User connection types management	
UserConnectionType.Create	Create user connection types
UserConnectionType.Read	Read user connection types
UserConnectionType.Update	Update user connection types
UserConnectionType.Delete	Delete user connection types
Roles management	
Role.Create	Create roles
Role.Read	Read roles
Role.Update	Update roles
Role.Delete	Delete roles
Role.Members	Manage role membership of users
Role.Claims	Manage role claims
Subscription groups management	
SubscriptionGroup.Create	Create subscription groups
SubscriptionGroup.Read	Read subscription groups
SubscriptionGroup.Update	Update subscription groups
SubscriptionGroup.Delete	Delete subscription groups
Notifications management	
EventSubscription.Create	Create notifications

ID	Name
EventSubscription.Read	Read notifications
EventSubscription.Delete	Delete notifications
Applications management	
Application.Create	Create new application
Application.Read	Read applications
Application.Update	Update applications
Application.Delete	Delete application
Organizational units management	
OrganizationalUnit.Create	Create organizational units
OrganizationalUnit.Read	Read organizational units
OrganizationalUnit.Update	Update organizational units
OrganizationalUnit.Delete	Delete organizational units
Network locations management	
NetworkLocation.Create	Create network locations
NetworkLocation.Update	Update network locations
NetworkLocation.Delete	Delete network locations
Tags management	
Tag.Create	Create tags
Tag.Update	Update tags

ID	Name
Tag.Delete	Delete tags
Dashboard page	
Dashboard.Edit	Update page configuration
Dashboard.View	View page
Service connection types management	
ServiceConnectionType.Create	Create service connection types
ServiceConnectionType.Read	Read service connection types
ServiceConnectionType.Update	Update service connection types
ServiceConnectionType.Delete	Delete service connection types

Mapping user directory and PAM attributes

This section contains a list of default values for user directory attributes and their mapping Axidian Privilege attributes.

Active Directory and Samba DC

Directory attribute	Axidian Privilege attribute	Description
Users		
`objectGUID`	`ID`	Entity identifier
`name`	`Name`	User name
`userPrincipalName`	`PrincipalName`	Login with domain in the format `username@domain` Example: `pamadmin@company.local`
`objectSID`	`SID`	Unique entity identifier in the directory in SID format Example: `S-1-5-21-2418255240-4279612882-1152719259`
`distinguishedName`	`DistinguishedName`	Path to the entity in the directory in DN format Example: `'cn=pamadmin,cn=users,cn=accounts,dc=my,dc=company'`
`sAMAccountName`	`SamAccountName`	User login name Example: `pamadmin`
`thumbnailPhoto`	`ThumbnailPhoto`	User thumbnail photo in JPEG or binary file format.
`jpegPhoto`	`JpegPhoto`	User photo in JPEG format.
User Groups		
`objectGUID`	`ID`	Entity identifier

Directory attribute	Axidian Privilege attribute	Description
`name`	`Name`	Group name
`canonicalName`	`CanonicalName`	Full path to the group in the directory
`objectSID`	`SID`	Unique entity identifier in the directory in SID format Example: `S-1-5-21-2418255240-4279612882-1152719259`
`distinguishedName`	`DistinguishedName`	Path to the entity in the directory in DN format Example: `'cn=pamadmins,cn=users,cn=accounts,dc=my,dc=company'`
`sAMAccountName`	`SamAccountName`	Unique Group name

FreeIPA

Directory attribute	Axidian Privilege attribute	Description
Users		
`entryUUID`	`ID`	Entity identifier
`cn`	`Name`	User name
`krbPrincipalName`	`PrincipalName`	Login with domain in the format `username@domain` Example: `pamadmin@company.local`
`ipaNTSecurityIdentifier`	`SID`	Unique entity identifier in the directory in SID format Example: `S-1-5-21-2418255240-4279612882-1152719259`
`ipaUniqueID`	`GUID`	Unique Entity identifier in the directory in GUID format Example: `176f69c4-3f2b-11eb-89aa-005056980f49`
`entrydn`	`DistinguishedName`	Path to the entity in the directory in DN format Example: `'uid=pamadmin,cn=users,cn=accounts,dc=my,dc=company'`

Directory attribute	Axidian Privilege attribute	Description
`uid`	`SamAccountName`	User login name Example: `pamadmin`
`jpegPhoto`	`ThumbnailPhoto`	User thumbnail photo in JPEG or binary file format.
`jpegPhoto`	`JpegPhoto`	User photo in JPEG format.
User Groups		
`ipaUniqueID`	`ID`	Entity identifier
`cn`	`Name`	Group name
`cn`	`CanonicalName`	Full path to the group in the directory
`ipaNTSecurityIdentifier`	`SID`	Unique entity identifier in the directory in SID format Example: `S-1-5-21-2418255240-4279612882-1152719259`
`ipaUniqueID`	`GUID`	Unique Entity identifier in the directory in GUID format Example: `176f69c4-3f2b-11eb-89aa-005056980f49`
`entryDn`	`DistinguishedName`	Path to the entity in the directory in DN format Example: `'uid=pamadmin,cn=users,cn=accounts,dc=my,dc=company'`
`cn`	`SamAccountName`	Unique Group name

OpenLDAP

Directory attribute	Axidian Privilege attribute	Description
Users		
`entryUUID`	`ID`	Entity identifier

Directory attribute	Axidian Privilege attribute	Description
`cn`	`Name`	User name
`entrydn`	`DistinguishedName`	Path to the entity in the directory in DN format Example: `'uid=pamadmin,cn=users,cn=accounts,dc=my,dc=company'`
`uid`	`SamAccountName`	User login name Example: `pamadmin`
`photo`	`ThumbnailPhoto`	User thumbnail photo in JPEG or binary file format.
`photo`	`JpegPhoto`	User photo in JPEG format.
User Groups		
`entryUUID`	`ID`	Entity identifier
`cn`	`Name`	Group name
`cn`	`CanonicalName`	Full path to the group in the directory
`entryDn`	`DistinguishedName`	Path to the entity in the directory in DN format Example: `'uid=pamadmin,cn=users,cn=accounts,dc=my,dc=company'`
`cn`	`SamAccountName`	Unique Group name

What's new

This section provides a brief description of changes and improvements in the Axidian Privilege by version.

3.5

Authentication

- Added Kerberos authentication support for installations with a Linux-based management server.
- Added a strict authentication mode for sign-in via an external Identity Provider.

Sessions and components

- Enhanced the Web Terminal component — you can now open sessions in Remote Desktop Services (RDS) mode directly from the browser. Access is granted to a remote desktop or to a published RemoteApp application.
- Added file transfer between a resource and a user's workstation in RDP sessions opened via Web Terminal.

Policies

- Added activity control for user actions in RDP sessions.
- Added the ability to automatically delete session text logs.
- Added the ability to override proxy component settings.
- Added support for local port forwarding in sessions opened via SSH Proxy.

Interface

- Redesigned the permission wizard—all settings are now on a single page.
- In the All sessions section, added the ability to show and hide table columns.
- Added automatic refresh of dashboard widgets: data is updated every 10 seconds.

Other changes

- Added case-insensitive search when Axidian Privilege data is stored in a PostgreSQL database. Exception: searching events by component or initiator is case-sensitive.
- The configuration wizard now supports installing Axidian Privilege from a backup file.

3.4

Authentication

- Added support for the Kerberos authentication protocol for sessions opened via RDP Proxy.
- Added support for X.509 certificate authentication.
- Added support for authentication via the OpenID Connect protocol.
- Improved authentication in RDP and SSH sessions: if a permission is granted for a user account and the user has authenticated in Axidian Privilege, their login and password are automatically filled in the sign-in form on the resource.
- Added the ability to specify the login format for accounts when connecting via SSH.
- The ConsoleApp utility now supports sign-in on behalf of a specific Axidian Privilege user, enabling individual privileges and access control differentiation.

Integrations

- Extended AAPM functionality — added integrations with Ansible Lookup Plugins and Python SDK for managing Axidian Privilege credentials.
- Added the ability to launch SSH sessions from an Ansible playbook.

Other changes

- Added clipboard support for sessions opened via Web Proxy.
- Added a health check mechanism for Axidian Privilege servers, components, and services. Results are displayed on the dashboard in the new PAM servers widget.
- Improved the report generation mechanism — reports on sessions, events, and permissions are now generated in the background. Generated reports can be downloaded in the Reports history section.
- Added access server information to session and event cards.

3.3

- Open web sessions with the new Web Proxy component.
- Open RDP and SSH sessions in a browser with the new Web Terminal component.
- A new Dashboard section is added.
- Session opening without re-authentication is added.
- Set the days of the week in permissions.

- Configuration now includes the ability to set automatic logout on inactivity from user and management consoles.
- Support for the Ed25519 algorithm for SSH keys is added.
- Improved blocking mechanism: blocking now applies not only to users, but also to PAM administrators. When blocked, access to the system is completely terminated.
- Support for Microsoft SQL Server in SQL Proxy is added.

3.2

- Authentication by SSH keys in SSH Proxy is added.
- Creation of internal users is added.
- Licensing is changed. To connect to ad hoc resources and PostgreSQL Proxy, special licenses are now required. Connecting to PostgreSQL Proxy works in early access mode until December 31, 2026, after which you need to purchase licenses.
- Automatic detection of permissions that have not been used for a long time is added. The validity period of permissions is determined in the configuration.

3.1

- Now administrators can add tags to resources.
- Now you can change the text of the connection reason prompt. This option is set in the session policy.
- Session search is improved. Now it is possible to search by session termination state and reason.

3.0

- Managing windows services.
- Copying permissions.
- Proxying SQL sessions for PostgreSQL.
- Session termination when user is inactive.
- Boost library is now linked to work with regular expressions. In this regard, there are small changes in the syntax of regular expressions when specifying a list of allowed and prohibited commands in SSH sessions.

- New settings in policies to manage requirements for generated passwords and manually entered passwords.
- RDP sessions without local disk redirection.
- SSH server key fingerprints verification.
- Operations with custom service connection types.
- New installation, upgrade and configuration wizard.

2.10

- OpenLDAP support.
- Blocking a user.
- Changing encryption key and/or encryption algorithm of PAM database without stopping PAM.
- Specifying multiple RADIUS servers to authenticate PAM users.
- Setting policy for user groups.
- Connecting to ad hoc resources.
- Native SIEM support via CEF and LEEF log format.
- Maximum account password length is increased up to 4096 symbols.
- Blocking settings for incorrect OTP input.
- S3 storage support.
- Enabling Restart of Proxy Service Containers.