Documentation of Axidian Privilege 3.2

Table of contents:

- Certificates
- Databases
- Data Storage
- User Directories
- Role Administrators
- User Authentication
- Access Server
- Logging
- Syslog Events
- Backup
- Installation

- Fault Tolerant on Linux
  - Wizard Launch
  - Scenario
  - Hosts Scheme
  - Ports
  - Certificates
  - Databases
  - Data Storage
  - User Directories
  - Role Administrators
  - User Authentication
  - Access Server
  - Logging
  - Syslog Events
  - Backup
  - Installation
  - IIS Setup
  - Additional Components Setup
  - RADIUS Configuring
  - RDP File Signature Configuring
  - TOTP Second Factor via Email Setup
  - Enabling Restart of Proxy Service Containers
  - Integration with User Directories
  - Configuring PAM for use with NFS
- IIS Setup
- Additional Components Setup
  - PamSu

- Event Log
- System Services
- File System
  - %SystemRoot%\System32\config
  - %SystemRoot%\System32\config\RegBack
- Registry
  - MACHINE\SOFTWARE
  - MACHINE\SYSTEM
  - MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg
- Advanced Audit Configuration
  - Account Logon
  - Account Management
  - Logon/Logoff
  - Object Access
  - Policy Change
  - Privilege Use
  - System
- Administrative Templates Section
  - Connections
  - Device and Resource Redirection
  - Remote Session Environment
  - Security
  - Session Time Limits
  - Temporary Folders
- Policies Import Procedure

- Access Server Security Settings
  - Applying Settings Using the Utility
  - Verifying that the Access Server Security Settings have been Successfully Applied
  - Applying Settings Manually
- Changing the Encryption Key of the PAM Database
- Service Operations
  - Service Operations for Windows Resources
    - Configuring a Domain Account as Service One
    - Configuring a Local Account as Service One
    - Configuring Axidian Privilege Core to Perform Service Operations on behalf of Local Resource Accounts
      - Configuring the TrustedHosts List
  - Service Operations in Active Directory

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.

Terms

User Directory

Active Directory container or organization unit (OU) from which Axidian Privilege receives employee data. It is possible to work with multiple Active Directory domains.

> **INFO**
>
> In addition to Active Directory, the following directory services are supported:
>
> - FreeIPA (PAM 2.9 and higher)
> - OpenLDAP (PAM 2.10 and higher)
>
> Axidian Privilege version 3.2 allows you to work with internal users without connecting to a directory service.

Users

Active Directory users that are members of container or Organization Unit defined as User Directory.

Accounts

Accounts of Windows OS, *nix OS, DBMS, Active Directory, web applications or client applications on behalf of which sessions will be opened in controlled systems.

Resources

The various systems that should be remotely accessed on behalf of the accounts.

Domains

Domains are intended for obtaining and automatically adding domain computers and domain accounts to Axidian Privilege.

Structure

Structure contains organizational units. An organizational unit (OU) combines users, resources, accounts, permissions to access protected objects in Axidian Privilege. OUs are designed to separate the privileges of Axidian Privilege administrators, which allows you to operate only within a specific OU without having access to operate with objects of other OUs.

Data Storage

For data storage Axidian Privilege can use different DBMS:

- Microsoft SQL Server
- PostgreSQL
- PostgreSQL Pro
- Jatoba

Service Connection

Service connection to a resource allows you to perform the following operations:

- Checking the connection to the resource
- Synchronizing accounts
- Account Security Groups synchronization
- Control of passwords (SSH keys) of accounts
- Changing the passwords (SSH keys) of accounts
- Synchronizing resource OS version or DBMS version
- Synchronizing domain computers in Active Directory

Service connections are supported for the following resources:

- Microsoft Active Directory
- Windows

- *nix
- Microsoft SQL Server
- MySQL
- PostgreSQL
- OracleDB
- Cisco (IOS XE)
- Inspur BMC (IPMI)

It is also possible to add your own service connection types.

User Connection

The User connection allows you to open sessions on resources or run individual RemoteApp applications. The following types of connections are supported:

- RDP
- SSH
- Telnet
- RemoteApp
- PostgreSQL

A resource can have one or more user connection types.

It is also possible to add your own user connection types.

Permissions

Permissions are used to manage privileged access. Any Active Directory user can be given permission to access the resource.
Contents of the permission:

- **User** — an employee whose personal account is part of the User Directory.
- **Account** — local or domain account used by Active Directory user to start a session at the resource.
- **Resource** — the resource on which the session will be opened.

> ⚠ **CAUTION**
>
> **Permission** cannot be modified while used. Revoked permissions cannot be restored.

Policies

A policy is a set of settings that is propagated to multiple system objects. A single object can be assigned only one policy of the certain type.

Components

Management Server

Axidian Privilege Core

This is the central component that manages the logic of Axidian Privilege operation.

Environment:

- Windows Server 2016 – 2022 → Internet Information Services (IIS)
- Linux Web Server → Docker → Nginx Web Server

Consists of:

- Web application — core

Tasks:

- Managing users, privileged accounts, access, passwords, etc.

Axidian Privilege IdP

User and Component Identification Center.

Environment:

- Windows Server 2016 – 2022 → Internet Information Services (IIS)
- Linux Web Server → Docker → web server → Nginx Web Server

Consists of:

- Web application — idp

Tasks:

- User authentication management, 2fa issuance and verification, Axidian Privilege component authentication

Axidian Privilege Management Console

An administrative interface for management of Axidian Privilege.

Environment:

- Windows Server 2016 – 2022 → Internet Information Services (IIS)
- Linux Web Server → Docker → Nginx Web Server

Consists of:

- Web application — mc

Tasks:

- The task list is available in Administration section.

Axidian Privilege User Console

User interface for accessing protected Axidian Privilege objects.

Environment:

- Windows Server 2016 – 2022 → Internet Information Services (IIS)
- Linux Web Server → Docker → Nginx Web Server

Consists of:

- Web application — uc

Tasks:

- The task list is available in User's Manual section.

Axidian Privilege Log Server

This is a uniform event log that collects and stores the Axidian Privilege events.

Environment:

- Windows Server 2016 – 2022 → Internet Information Services (IIS)

- Linux Web Server → Docker → Nginx Web Server

Consists of:

- Web application — ls

Tasks:

- Collecting, storing and issuing events.

Axidian Privilege EventLog

An add-on for Axidian Privilege Log Server.

Environment:

- Windows Server 2016 – 2022

Consists of:

- Files and Libraries for Log Server

Task:

- Implements event logging in Windows Event Log.

Access Server

Axidian Privilege Gateway

A set of components implementing jump server functions, session auditing tools and protection mechanisms.

Environment:

- Windows Server 2016 – 2022

Consists of:

- Windows desktop application — ProxyApp.exe
- File System Driver — Pam.FsFilter

- Windows service for interacting with a file system filter — Pam.Service
- Modified SSH Client — Putty.exe
- Extension for mstsc.exe
- A set of utilities and libraries — FFmpeg
- Process Control Libraries

Tasks:

- Providing access to target resource via the RDP/SSH/Telnet protocols and others in RemoteApp mode
- Recording videos and screenshots, text interception and interception of transmitted files.
- Processing and saving session artifacts.
- Checking the status of client components.
- Process startup control, file system access control.

Axidian Privilege SSH Proxy

Proxy server for SSH sessions.

Environment:

- Linux → Docker

Consists of:

- Application — Pam.SshProxy.Service (Linux)

The component tasks are:

- Providing access via SSH/SCP/SFTP protocols
- Providing port forwarding with the target resources
- Interception of text and transmitted files
- Processing and saving session artifacts.

Axidian PAM PostgreSQL Proxy

Proxy server for PostgreSQL sessions.

Environment:

- OC Linux → Docker

Consists of:

- Application — Pam.PostgreSQLProxy.Service (Linux)

The component tasks are:

- Interception of the text of SQL queries launched by the user.

Axidian Privilege RDP Proxy

Proxy server for RDP sessions.

Environment:

- Linux → Docker

Consists of:

- Application — Pam.RdpProxy.Service (Linux)

The component tasks are:

- Providing access via RDP protocols
- Interception of text, video, screenshots and transmitted files
- Processing and saving session artifacts

Axidian Privilege ESSO Agent and Axidian Privilege Admin Pack

A set of components for implementing SSO access.

Environment:

- Windows Server 2016 – 2022

Consists of:

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

Tasks:

- Interception and autofill of authentication forms for web-based applications and Windows desktop applications

Windows Resources

Axidian Privilege Agent

The component is intended to capture text logs during RDP session.

Environment:

- Windows Server 2016 – 2022/Windows XP SP3 X64 – Windows 11

Consists of:

- Windows application — Pam.Proxy.WindowsAgent.exe

Tasks:

- Recording changes of active windows, process launches and keyboard input
- Sending heartbeat messages to Axidian Privilege Gateway to register its activity

> **INFO**
>
> The Axidian Privilege Agent component is optional, as Axidian Privilege is a completely agentless solution. You can disable text logs in RDP sessions to work without Axidian Privilege Agent.

Linux Resources

PAMSU Component

A component for executing commands with root privilege similar to the sudo command. The difference is that authentication will be requested from the Axidian Privilege user, not from the privileged account on behalf of which the session was opened on the resource.

Environment:

- Linux

Consists of:

- .deb or .rpm packages

Tasks:

- Running elevated commands as a PAM user

> **INFO**
>
> The PAMSU component is optional, as Axidian Privilege is a completely agentless solution. You can disable pamsu feature in SSH sessions to work without PAMSU.

User's Workplace

Axidian Privilege Desktop Console

Additional tool for connecting to target resources via **Axidian Privilege**.

Consists of:

- Modified mRemoteNG utility

Tasks:

- The task list is available in User's Manual section.

Simplified on Windows

To explore Axidian Privilege

Simplified on Linux

To explore Axidian Privilege

Basic

For implementation and operation in production

Fault Tolerant

For implementation and operation in production, with server balancing

Simplified on Windows

All Axidian Privilege components are installed on two servers. Recommended for review and testing.

Components

Management Server / Access Server (RDP/RemoteApp)

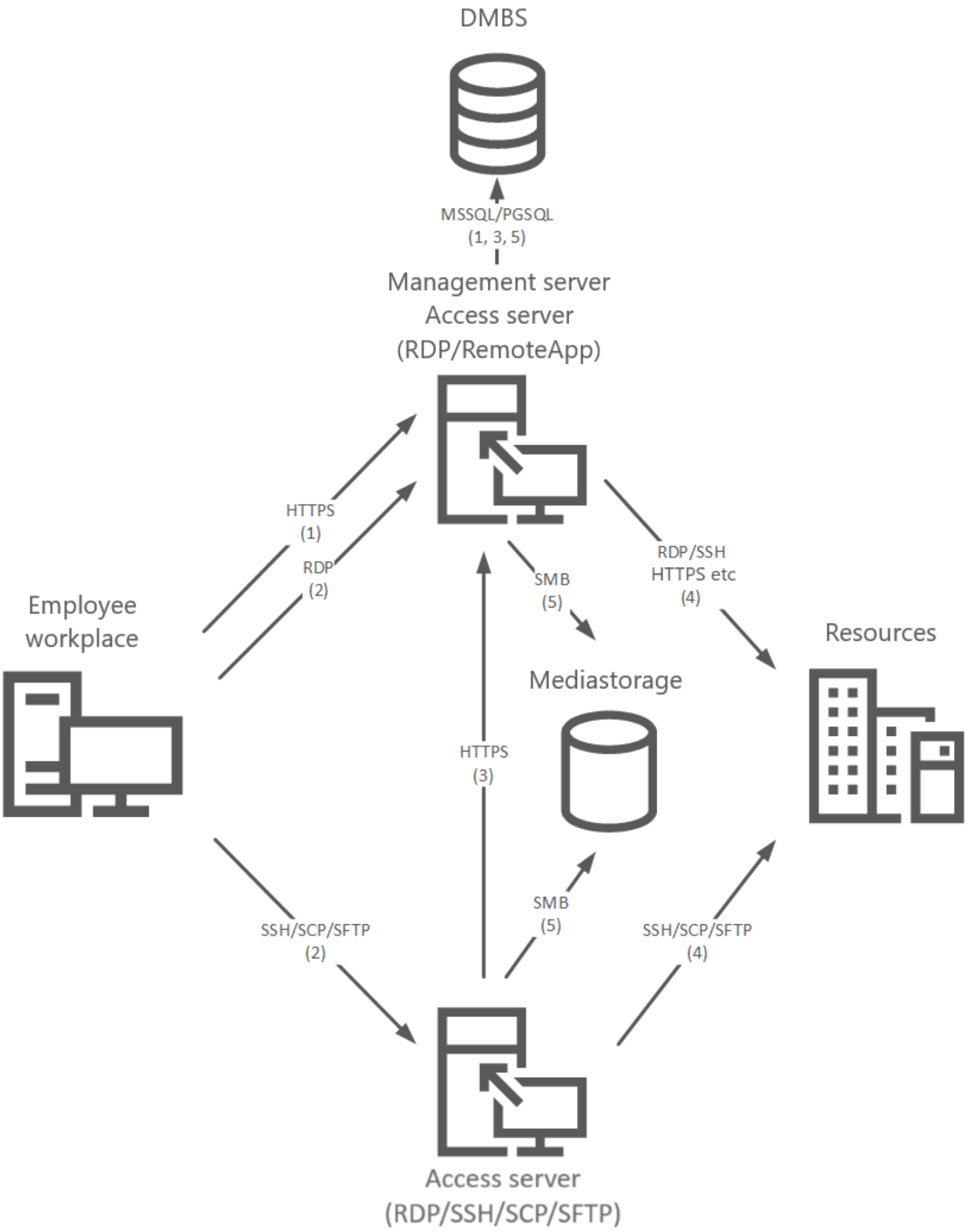
- Axidian Privilege Core
- Axidian Privilege IdP
- Axidian Privilege Management Console
- Axidian Privilege User Console
- Axidian Privilege Log Server
- Axidian Privilege EventLog
- Axidian Privilege Gateway
- Axidian Privilege ESSO Admin Pack
- Axidian Privilege ESSO Agent

Access Server (SSH/SCP/SFTP)

- Axidian Privilege SSH Proxy
- Axidian Privilege RDP Proxy
- Axidian Privilege PostgreSQL Proxy

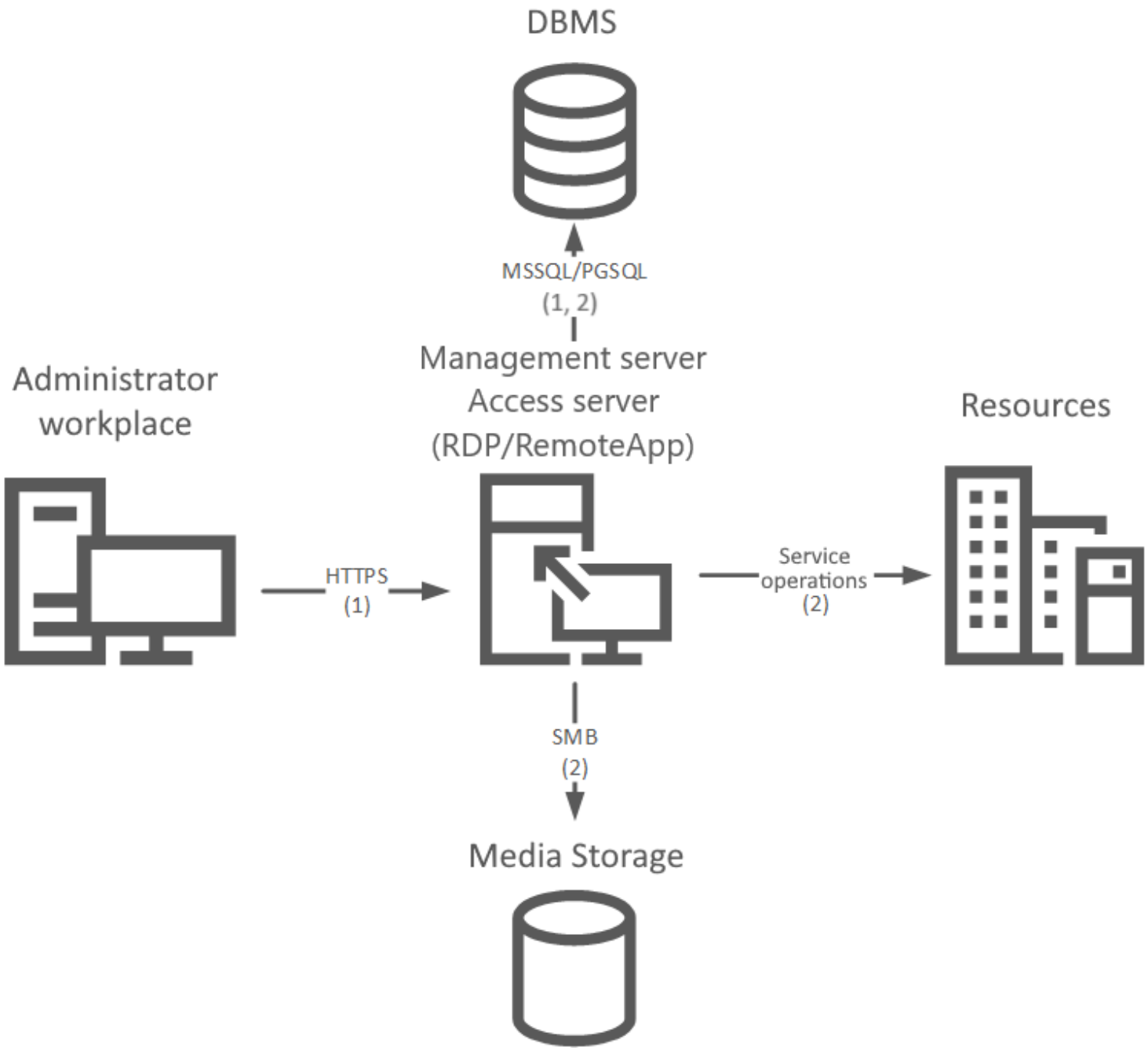
Work Scenarios

User Scenario


DMBS
MSSQL/PGSQL
(1, 3, 5)
Management server
Access server
(RDP/RemoteApp)
HTTPS
(1)
RDP
(2)
SMB
(5)
RDP/SSH
HTTPS etc
(4)
Employee
workplace
Mediastorage
Resources
HTTPS
(3)
SMB
(5)
SSH/SCP/SFTP
(2)
SSH/SCP/SFTP
(4)
Access server
(RDP/SSH/SCP/SFTP)

1. Connection to the user's self service via a browser or Axidian Privilege Desktop Console. Domain authentication and second factor authentication. Checking the user in the IdP database. Getting a list of resources from the Core database. Obtaining an RDP file to connect to a resource.
2. Connection to Access server (RDP/RemoteApp) using an RDP file, Axidian Privilege Desktop Console or connection to Access server (RDP/SSH/SCP/SFTP) using a separate RDP file or SSH client.
3. Domain authentication and second factor authentication. Checking the user of the IdP database. Checking the permission to access the Core database. Retrieving service account credentials from the DBMS to work with media storage. Retrieving privileged account credentials from the DBMS for connecting to a resource.
4. Connecting to a resource.
5. Saving videos and screenshots in the media storage. Saving a text log to the Core database.

Administrator Scenario



1. Connection to the administrator's self service. Domain authentication and second factor authentication. Checking the user in the IdP database.
2. Getting, adding and editing system objects. Performing service operations.

Simplified on Linux

All Axidian Privilege components are installed on two servers. Recommended for review and testing.

Components

Management Server / Access Server (RDP/SSH/SCP/SFTP)

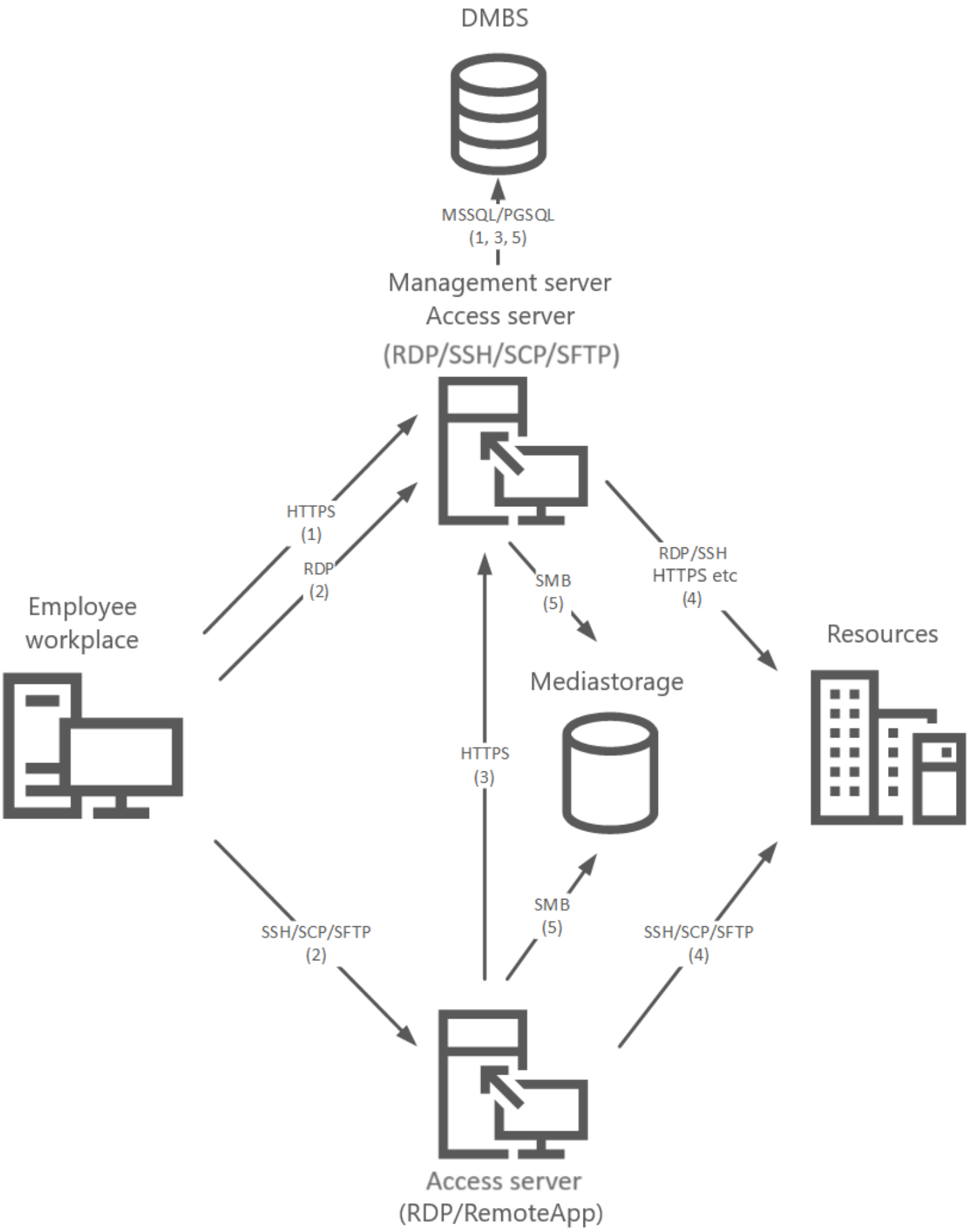
- Axidian Privilege Core
- Axidian Privilege IdP
- Axidian Privilege Management Console
- Axidian Privilege User Console
- Axidian Privilege Log Server
- Axidian Privilege SSH Proxy
- Axidian Privilege RDP Proxy
- Axidian Privilege PostgreSQL Proxy

Access Server (RDP/RemoteApp)

- Axidian Privilege Gateway
- Axidian Privilege ESSO Admin Pack
- Axidian Privilege ESSO Agent

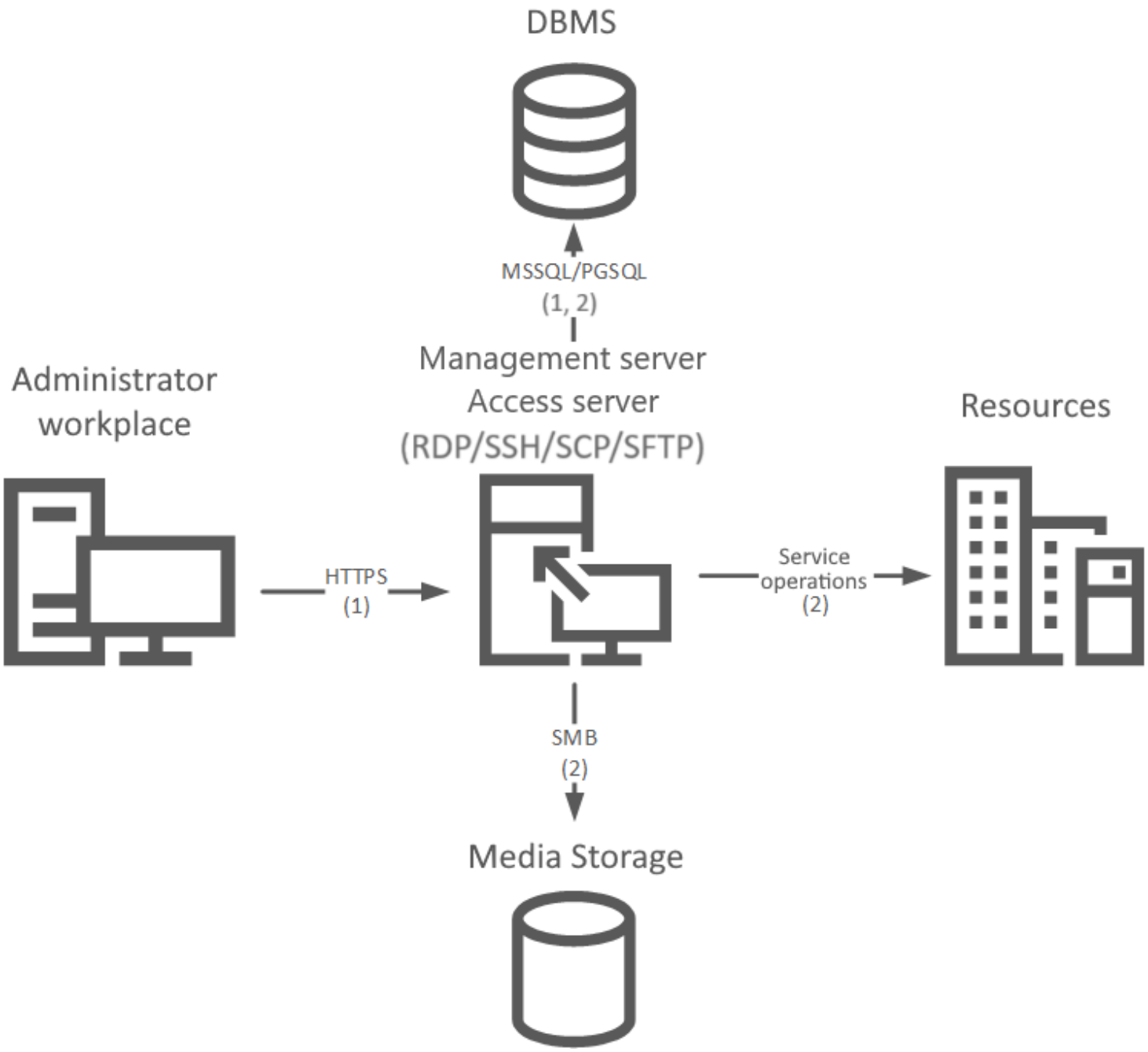
Work Scenarios

User Scenario


DMBS
MSSQL/PGSQL
(1, 3, 5)
Management server
Access server
(RDP/SSH/SCP/SFTP)
HTTPS
(1)
RDP
(2)
SMB
(5)
RDP/SSH
HTTPS etc
(4)
Employee
workplace
Mediastorage
Resources
HTTPS
(3)
SMB
(5)
SSH/SCP/SFTP
(2)
SSH/SCP/SFTP
(4)
Access server
(RDP/RemoteApp)

1. Connection to the user's self service via a browser or Axidian Privilege Desktop Console. Domain authentication and second factor authentication. Checking the user in the IdP database. Getting a list of resources from the Core database. Obtaining an RDP file to connect to a resource.
2. Connection to Access server (RDP/RemoteApp) using an RDP file, Axidian Privilege Desktop Console or connection to Access server (RDP/SSH/SCP/SFTP) using a separate RDP file or SSH client.
3. Domain authentication and second factor authentication. Checking the user of the IdP database. Checking the permission to access the Core database. Retrieving service account credentials from the DBMS to work with media storage. Retrieving privileged account credentials from the DBMS for connecting to a resource.
4. Connecting to a resource.
5. Saving videos and screenshots in the media storage. Saving a text log to the Core database.

Administrator Scenario



1. Connection to the administrator's self service. Domain authentication and second factor authentication. Checking the user in the IdP database.
2. Getting, adding and editing system objects. Performing service operations.

Basic

Axidian Privilege components are installed on three different servers. This type of installation allows you to decouple the Core of the system from the components that provide Access. Recommended for implementation and operation in a production environment.

Components

Management server

- Axidian Privilege Core
- Axidian Privilege IdP
- Axidian Privilege Management Console
- Axidian Privilege User Console
- Axidian Privilege Log Server
- Axidian Privilege EventLog

Access server (RDP/RemoteApp)

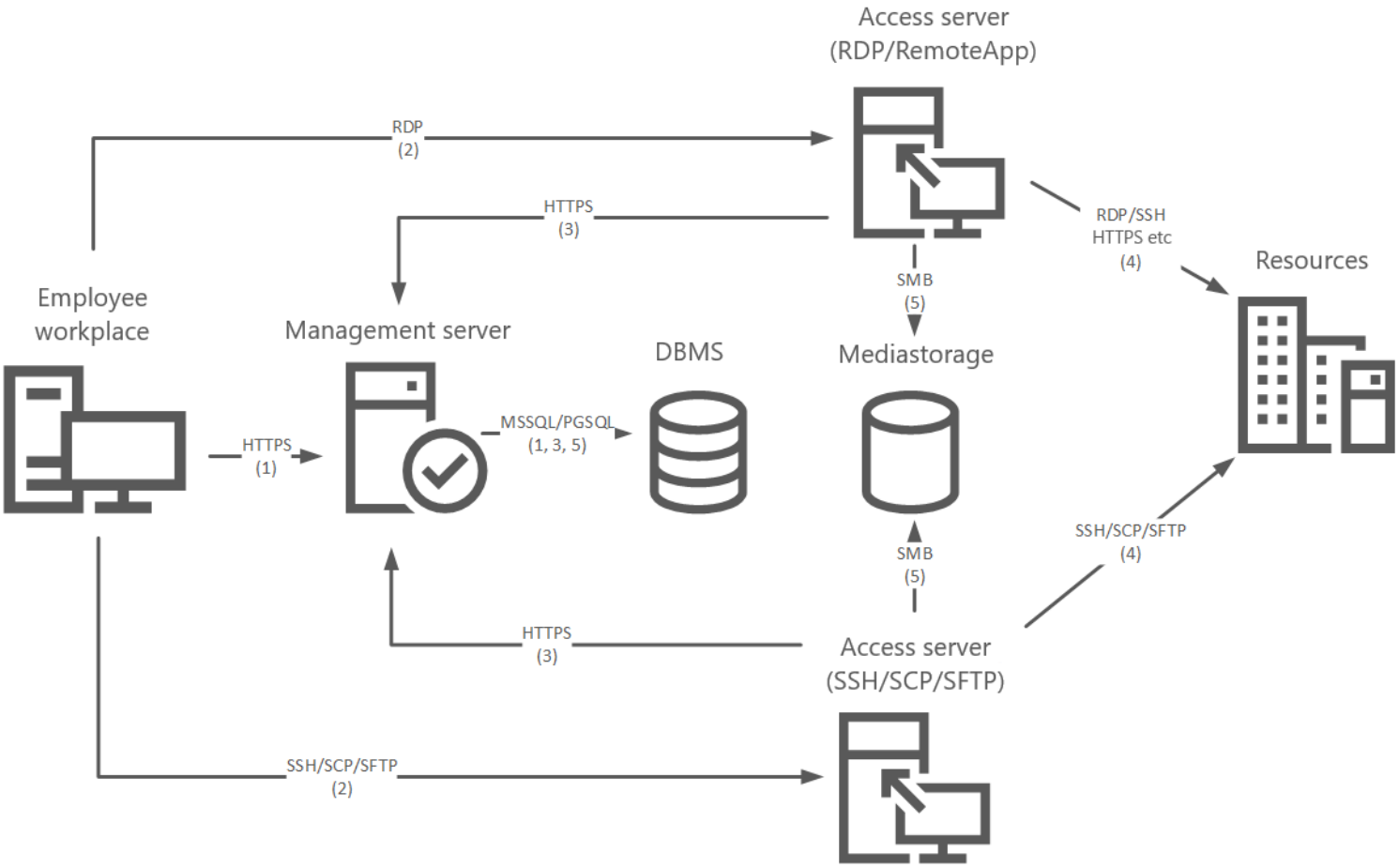
- Axidian Privilege Gateway
- Axidian Privilege ESSO Admin Pack
- Axidian Privilege ESSO Agent

Access server (RDP/SSH/SCP/SFTP)

- Axidian Privilege SSH Proxy
- Axidian Privilege RDP Proxy
- Axidian Privilege PostgreSQL Proxy

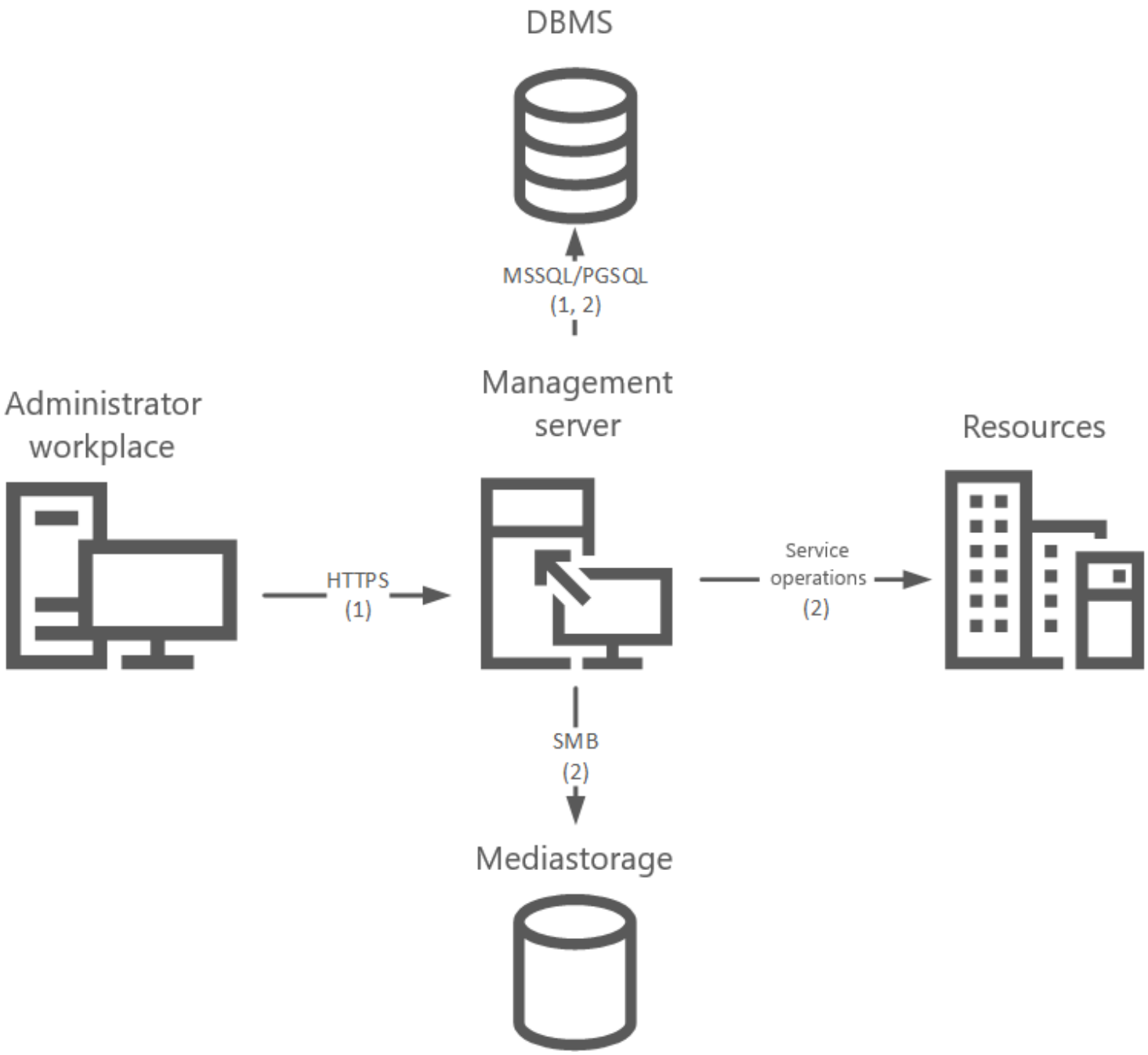
Work Scenarios

User Scenario



1. Connection to the user's self service via a browser or Axidian Privilege Desktop Console. Domain authentication and second factor authentication. Checking the user in the IdP database. Getting a list of resources from the Core database. Obtaining an RDP file to connect to a resource.
2. Connection to Access server (RDP/RemopteApp) using an RDP file, Axidian Privilege Desktop Console or connection to Access server (SSH/SCP/SFTP) using a separate SSH client.
3. Domain authentication and second factor authentication. Checking the user of the IdP database. Checking the permission to access the Core database. Retrieving service account credentials from the DBMS to work with Mediastorage. Retrieving privileged account credentials from the DBMS for connecting to a resource.
4. Connecting to a resource.
5. Saving videos and screenshots in the media storage. Saving a text log to the Core database.

Administrator Scenario



1. Connection to the administrator's self service. Domain authentication and second factor authentication. Checking the user in the IdP database.
2. Getting, adding and editing system objects. Performing service operations.

Fault Tolerant

Axidian Privilege components are installed on different servers, each server is duplicated to provide fault tolerance. Recommended for implementation and operation in a production environment.

Components

Management Server

- Axidian Privilege Core
- Axidian Privilege IdP
- Axidian Privilege Management Console
- Axidian Privilege User Console
- Axidian Privilege Log Server
- Axidian Privilege EventLog

Access Server (RDP/RemoteApp)

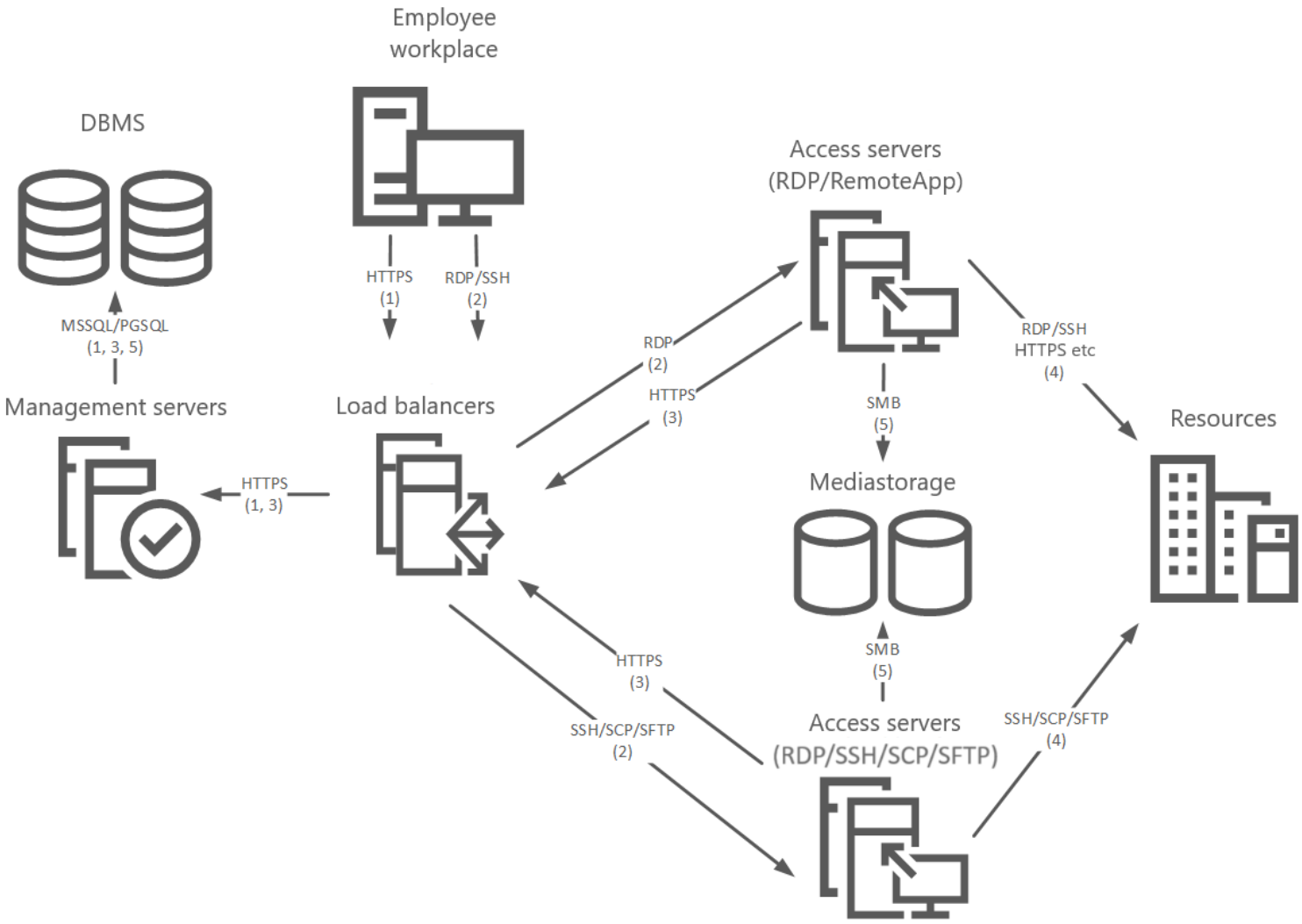
- Axidian Privilege Gateway
- Axidian Privilege ESSO Admin Pack
- Axidian Privilege ESSO Agent

Access Server (RDP/SSH/SCP/SFTP)

- Axidian Privilege SSH Proxy
- Axidian Privilege RDP Proxy
- Axidian Privilege PostgreSQL Proxy

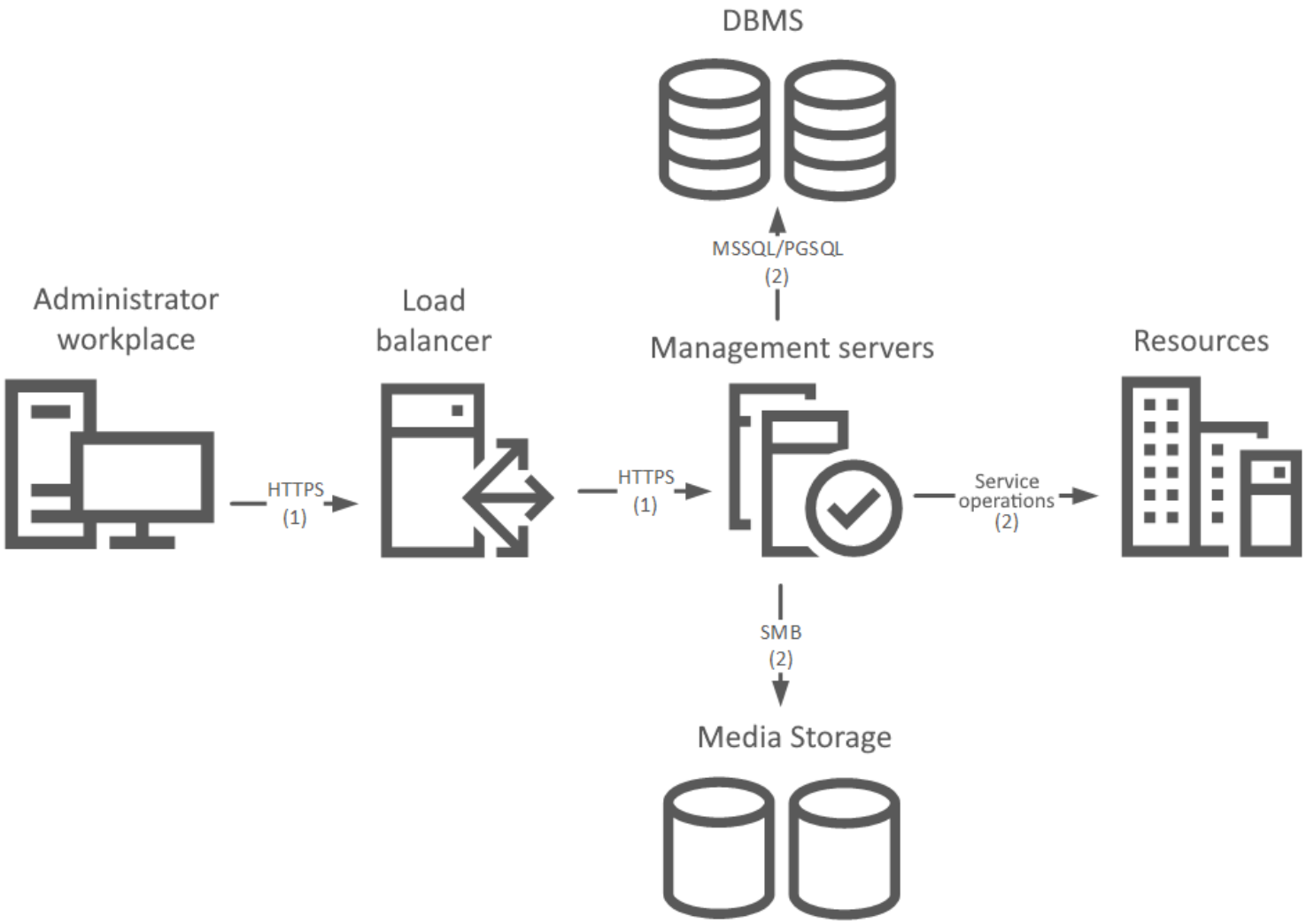
Work Scenarios

User Scenario



1. Connection to the user's self service via a browser or Axidian Privilege Desktop Console. Domain authentication and second factor authentication. Checking the user in the IdP database. Getting a list of resources from the Core database. Obtaining an RDP file to connect to a resource.
2. Connection to Access server (RDP/RemoteApp) server using an RDP file, Axidian Privilege Desktop Console or connection to Access server (RDP/SSH/SCP/SFTP) using a separate SSH client.
3. Domain authentication and second factor authentication. Checking the user of the IdP database. Checking the permission to access the Core database. Retrieving service account credentials from the DBMS to work with media storage. Retrieving privileged account credentials from the DBMS for connecting to a resource.
4. Connecting to a resource.
5. Saving videos and screenshots in the media storage. Saving a text log to the Core database.

Administrator Scenario



1. Connection to the administrator's self service. Domain authentication and second factor authentication. Checking the user in the IdP database.
2. Getting, adding and editing system objects. Performing service operations.

Windows Environment

Hardware and software requirements for installing Axidian Privilege on Windows OS

Linux Environment

Hardware and software requirements for installing Axidian Privilege on Linux OS

DBMS Environment

Hardware requirements for DBMS

Windows Environment

Management Server

Hardware Requirements

Device	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 Gbit	1 Gbit	1 Gbit

Software Requirements

Operating system:

- Windows Server 2016 – 2022

Domain:

- Microsoft Active Directory member

Web server:

- Internet Information Services 8.5 – 10.0

Modules for the Internet Information Services web server:

- Basic Authentication
- Windows Authentication
- Static Content
- HTTP Redirection

- ASP.NET
- ISAPI Extensions
- .NET Extensibility
- ISAPI Filters
- IIS Management Console

Additional Microsoft components:

- Microsoft .NET Core 8
- URL Rewrite

Network Connectivity

Incoming **Outgoing**

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

Access Server (RDP)

Hardware Requirements

Device	10 RDP/SSH sessions	50 RDP/SSH sessions	100 RDP/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 Gbit	1 Gbit	1 Gbit

> ⚠ **CAUTION**
>
> **Please pay attention to the information provided below.**
>
> Requirements are calculated for a dedicated physical server. Performance testing was conducted with RDP and SSH sessions.
>
> The declared number of concurrent sessions requires Simultaneous MultiThreading (AMD) or Hyper-Threading (Intel) supported CPUs.
>
> The declared number of concurrent sessions is supported when capturing video from a single monitor in HD resolution. The video resolution is determined by the monitor settings on the user's side. If you increase the resolution or the number of monitors, the declared number of concurrent sessions will decrease.
>
> Using client applications launched from the Axidian Privilege server in RemoteApp mode reduces the number of concurrent sessions. The impact of each application on the number of concurrent sessions is individual, this can only be determined during testing.
>
> If the deployment is in a concurrent virtual environment, then the number of concurrent sessions may be less. To support the declared number of concurrent sessions, the virtual server must have reserved CPU frequency and RAM equivalent to the physical server.

Software Requirements

Operating system:

- Windows Server 2016 – 2022

Domain:

- Microsoft Active Directory member

Additional Microsoft components:

- Microsoft .NET Desktop Runtime x64 version 8
- Microsoft C++ 2015 – 2019 Redistributable

Browser:

- Google Chrome
- Microsoft Edge

Roles:

- Remote Desktop Services Broker (RDCB)
- Remote Desktop Services Host (RDSH)
- Remote Desktop Web Access (RDWA)

Network Connectivity

Incoming **Outgoing**

Protocol	Port	Description
TCP	3389	Connection to the Access server
TCP	5443	Reading a session stream

Other Requirements

Employees with access to the administrator console or user console must have a monitor width resolution of at least 1280 pixels, otherwise the console interface elements will not display correctly.

Linux Environment

Management Server

Hardware Requirements

Device	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 Gbit	1 Gbit	1 Gbit

Software Rquirements

Operating system:

- Linux

Container engine:

- Docker 18.09 and higher
- Docker Compose 1.29.2 and higher

> ⚠ **CAUTION**
>
> Docker must be installed from the distribution's repository.

<details>
<summary>Alternative way to install Docker (not recommended)</summary>

As an exception (in cases when there is no access to the operating system and Docker repositories) it is possible to install Docker from static binary files.
</details>

If you are using an operating system other than those listed by the link, then the required package with the SELinux module will not be installled during the Docker installation. This package is required for Axidian Privilege to function properly. On most systems this package is called **container-selinux**.

Install it manually according to the documentation of the operating system you are using. This must be done **before** running the installation script **run-deploy.sh**.

Network Connectivity

Incoming **Outgoing**

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

Access Server (SSH)

Hardware Requirements

Device	50 SSH sessions	100 SSH sessions	200 SSH sessions
CPU	2 Cores	2 Cores	2 Cores
RAM	2 GB	2 GB	4 GB
HDD/SSD	120 GB	120 GB	120 GB
Network adapter	1 Gbit	1 Gbit	1 Gbit

Software Requirements

Operating system:

- Linux

Container engine:

- Docker 18.09 and higher
- Docker Compose 1.29.2 and higher

Network Connectivity

Incoming **Outgoing**

Protocol	Port	Description
TCP	2222	Connection to the Access server

Access Server (RDP)

Hardware Requirements

Device	10 RDP sessions	50 RDP sessions	100 RDP sessions
CPU	4 Cores	12 Cores	16 Cores
RAM	4 GB	12 GB	40 GB
HDD/SSD	120 GB	120 GB	120 GB
Network adapter	1 Gbit	1 Gbit	1 Gbit

Software Requirements

Operating system:

- Linux

Container engine:

- Docker 18.09 and higher
- Docker Compose 1.29.2 and higher

Network Connectivity

Incoming **Outgoing**

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

CIS Benchmark Security Settings

PAM servers must have CIS Benchmark security settings applied.

Other Requirements

Employees with access to the administrator console or user console must have a monitor width resolution of at least 1280 pixels, otherwise the console interface elements will not display correctly.

DBMS Environment

Supported DBMS

- Microsoft SQL Server 2012SP2 – 2022 with support for Full-Text and Semantic Extractions for Search
- PostgreSQL 12–16
- Postgres Pro Standard 12–16
- Postgres Pro Enterprise
- Jatoba 4–5

> ⚠ **CAUTION**
>
> If you use Microsoft SQL Server you need to install an additional module: Full-Text and Semantic Extractions for Search.

Hardware Requirements

Device	50 sessions	100 sessions	200 sessions
CPU	2 Cores	2 Cores	2 Cores
RAM	2 GB	4 GB	4 GB
HDD	1 TB	1 TB	1 TB
Network adapter	1 Gbit	1 Gbit	1 Gbit

Software Requirements

- In accordance with the official documentation of the manufacturer

Network Connectivity

- In accordance with the official documentation of the manufacturer

Licensing

Axidian Privilege has two licensing schemes:

- Licensing by users and resources.
- Licensing by sessions (simultaneous connections).

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

Additionally, regardless of the licensing scheme, you can purchase a license for Application to Application Password Management (AAPM). This license only affects access to AAPM features and does not affect the ability of users to establish a session through PAM or the ability of an administrator to add a permission to a user.

Licensing by Users and Resources

When selecting this licensing scheme, you will need to determine the number of users and the number of resources in your Axidian Privilege installation.

They are set by the number of licenses of the following types:

- User — determines the number of users who can use PAM.
- Resource — determines the number of resources that can be created in PAM.

When selecting this licensing scheme, the number of sessions (simultaneous connections) is not limited. User licenses can be redistributed between employees (revoke licenses from some employees and allocate them to others). Resource licenses can be freed and then taken by other resources.

> **TIP**
>
> Any licenses can be purchased additionally. You can increase the number of licenses of any type at any time.

Issuance of a License

User License

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

Resource License

To issue a resource license, create or restore the 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 (Release) of a License

User License

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

- Revocation
- Suspension
- Expiration

Resource License

The resource license is released when the resource is deleted.

License Validity Period

Types of licenses according to the validity period:

- Not time limited
- Limited by a specific calendar date
  - Trial period
  - Subscription

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

- Add a resource
- Add a user (even if not taken licenses are available)

- Open a session (connect to a resource)

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

Licensing by Session

When selecting this licensing scheme, you will need to determine the number of sessions (simultaneous connections that can be opened via Axidian Privilege).

When selecting this licensing scheme, the number of users and resources is not limited.

Issuance and Release of a License

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).

License Validity Period

- Types of licenses according to the validity period:
- Not time limited
- Limited by a specific calendar date
  - Trial period
  - Subscription

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

After the license expires, the following operations will remain available:

- Permissions editing
- Created resources editing
- Account editing

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

Application to Application Password Management License

The AAPM 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 the AAPM.

The number of applications, application users and permissions is unlimited.

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

Issuance and Release of a License

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

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

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

License Validity Period

Types of licenses according to the validity period:

- Not time limited
- Limited by a specific calendar date
  - Trial period
  - Subscription

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

- Add new permissions to applications

- Use scenarios for third-party applications to 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 scheme.
>
> 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;
- limited by a specific calendar date:
  - trial period;
  - subscription.

When the license expires, the previously created permissions will get the Inactive state, and the following operations will no longer be available:

- add or renew permissions to connect to ad hoc resources;
- open a session to ad hoc resource.

SQL Proxy License

This license allows you to connect to resources of the PostgreSQL type. This license defines the number of active permissions for resources with the PostgreSQL type.

> **INFO**
>
> The SQL Proxy license is independent of the selected licensing scheme.

> The SQL Proxy license can be purchased or removed at any time.

Issuance

To occupy the SQL Proxy license, add to the user at least one active permission to the resource with PostgreSQL type. If all SQL Proxy licenses are occupied, you cannot add permission to a new user for a resource of the PostgreSQL type.

Revocation

The SQL Proxy license is released as a result of such actions with permissions to a resource with PostgreSQL type, as:

- revocation;
- suspension;
- expiration.

Validity Period

Types of licenses according to the validity period:

- not time limited;
- limited by a specific calendar date:
  - trial period;
  - subscription.

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

- add or renew permissions to connect to resources of the PostgreSQL type;
- add users to the user group for which there is an active permission to the resource with the PostgreSQL type;
- add resources to the resource group for which there is an active permission to the resource with the PostgreSQL type;
- select the PostgreSQL type when editing the user connection of the resource for which there is an active permission;
- open a session for the resource with the PostgreSQL type.

General Plan of Implementation

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 on session basis.
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:
    i. Installation of Microsoft SQL Server/PostgreSQL Pro or providing access to an existing Microsoft SQL Server/PostgreSQL Pro instance.
    ii. Creation of databases and configuration of service account or provision of access to an existing account.
6. Definition of LDAP paths to containers and organization units in the Active Directory hierarchy to place Axidian Privilege end users to.
7. Creation and configuration of service account for use with Active Directory user directory or provision of access to an existing account.
8. Creation and configuration of service account to use for service operations in Active Directory or provision of access to an existing account.

Installation and Configuration of Axidian Privilege Server Components

Windows

1. Management Server (Windows)
2. Access Server (RDP\RemoteApp)
3. Access Server (SSH Proxy)

Linux

1. Management Server (Linux)

2. Access Server (RDP/RemoteApp)
3. Access Server (SSH Proxy)

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. Operability check for server and client components.
2. Check of system functions and customer scenarios:
    i. Configuration of service operations for Windows resources.
    ii. Configuration of service operations for *nix resources.
    iii. Configuration of user connections.
3. Troubleshooting.

Final Step

1. Demonstration of operation.
2. Training to use the Axidian Privilege.
3. Testing.

User Directory Accounts

Create accounts to work with user directory and for service operations

Certificates

Create management server certificates

Databases

Create databases and accounts to work with the data storage

Media Storage

Create and configure media storage

Servers

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

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 | **FreeIPA** | **OpenLDAP**

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.

Account for Service Operations in Active Directory

Active Directory | **FreeIPA** | **OpenLDAP**

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.

Certificates

Please prepare your 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.

Installation without balancing | **Fault-tolerant installation with HAProxy** | **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.
- FQDN PAM certificate with private key in `.pfx` format.
- Certificates for all RDP, RDS and PostgreSQL access servers with a private key in `.pfx` format. Except when the access server is installed on the same host as the management server.

> ⓘ **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 *..PAM_3.2\axidian-pam\state\ca-certificates* before running the wizard.

Databases

To store data, Axidian Privilege uses the following databases:

- **Core** — Axidian Privilege Core component database is used to store Axidian Privilege privileged accounts, resources, permissions, and other service data.
- **CoreJobs** — Axidian Privilege Core component database is used to store scheduled jobs.
- **Idp** — IdP component database is used to store authenticators of Axidian Privilege users and administrators.
- **IdpJobs** — IdP component database is used to store scheduled jobs.
- **ILS** — Log Server component database is used to store the Axidian Privilege events.

Database Creation

MSSQL **PostgreSQL**

1. Launch **Microsoft SQL Management Studio** (SSMS) and connect to Microsoft SQL Server instance.
2. Open the context menu of **Databases** item.
3. Select the **New Database** item.
4. Specify a database name, for example **Core**, **CoreJobs**, **Idp**, **IdpJobs**, **ILS**.
5. Click **OK**.

Creating a Service Account to Work with Data Storage

MSSQL **PostgreSQL**

1. Start **Microsoft SQL Management Studio** (SSMS) and connect to the Microsoft SQL Server instance.
2. Expand the **Security** item.
3. Open the context menu of **Logins item**.
4. Select the **Create login item**.

5. Enter the name, for example **IPAMSQLServiceOps**.
6. Select **SQL Server authentication** item and fill in the required fields.
7. Switch to **User Mapping item**.
8. Check **Core**, **CoreJobs**, **Idp**, **IdpJobs** and **ILS** databases.
9. Check database roles **db_owner**, **db_datareader** and **db_datawriter**.
10. Click **OK**.

> ⓘ **NOTE**
>
> The grants **db_owner** for Microsoft SQL Server is required only for the first access to the database.

> ⓘ **NOTE**
>
> A certificate for the MSSQL instance is required for Axidian Privilege.

Media Storage

File storages are necessary for aggregation and long-term storage of videos, screenshots and files transferred in sessions.

File Storage Account

> ⚠ **CAUTION**
>
> A domain account is required to work with file storage, recommended to use the already created **IPAMStorageOps** account.

Creating and Configuring File Storage

1. Log in to the server, which will act as a file storage.
2. Create a directory, for example **IPAMStorage**.
3. Right click on the folder you created, select the item **Give access to** → **Specific people**.
4. Enter the username, for example **IPAMStorageOps** and click **Add**.
5. In the **Permission level** column, click the **Read** value next to the **IPAMStorageOps** user and select **Read/Write** from the menu.
6. Finish by clicking **Share**.

Servers

Windows | Linux

All servers on which you plan to install Axidian Privilege components must be located in the same domain, on the same network and access the same DNS server.

Access Server

The access server accepts remote connections from Axidian Privilege users and automatically opens remote connections to target resources on behalf of privileged accounts.

To deploy the RDS role, it is recommended to use a "clean" Windows Server in the domain:

- **No** group policies related to remote access are applied
- **None** of the RDS role components (RDCB, RDG, RDL, RDSH, RDVH, RDWA) are deployed

Deploying the Remote Desktop Services Role on a Single Server

1. Start **Server Manager**, click **Manage** menu, click **Add Roles and Features**
2. In the **Installation Type** step, select **Remote Desktop Services installation**
3. In the **Deployment type** step, select **Standard deployment**
4. In the **Deployment scenario** step, select **Session-based desktop deployment**
5. In **RD Connection Broker**, **RD Web Access**, **RD Session Host** steps, select the current server
6. In the **Confirmation** step, check **Restart the destination server automatically if required**, click **Deploy** and wait for the server to restart

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).

  <details>
  <summary>Read more</summary>

  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.
  </details>

- 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.

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 master 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.

> ⚠ **CAUTION**
>
> The wizard must be launched on the host on which management server or access server of the PAM will be installed, otherwise an error for the wizard will occur.

1. Download and unpack the Web Wizard distribution on your Linux machine.
2. Place the CA certificate in **..PAM_3.0\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. Run 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 **New PAM Installation**.
2. Click **Next** to proceed to the next step of the wizard.

▼ 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.

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 Management Server, RDS Access Server, SSH Access Server, PostgreSQL Access Server. Please note that you cannot add multiple hosts with the same address.

   ▼ 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**.
7. If you selected **by password** in the previous step, then enter **Login** and **Password**. If you selected **by SSH key** in the previous step, then enter **Login**, **sudo password**, **SSH key** and

Passphrase.
8. 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**.
7. If you selected **by password** in the previous step, then enter **Login** and **Password**. If you selected **by SSH key** in the previous step, then enter **Login**, **sudo password**, **SSH key** and **Passphrase**.
8. Click **Add**.

> ⓘ **INFO**
>
> Management Server and RDS Access Server can be located on the same host.
> RDP Access Server, SSH Access Server, PostgreSQL Access Server 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
MC/UC HTTP	80
MC/UC HTTPS	443
Gateway Service	8443

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

Certificates

In this step you need to download 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.

<details>
<summary>Selecting PostgreSQL</summary>

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.
</details>

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.

<details>
<summary>Other storage types</summary>

If you select SMB, fill in the following fields:
</details>

- 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

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

1. Click **Add User Directory**.
2. In the **Directory Service** field, select **Active Directory**.
3. Enter a value in the **Directory ID** field. Create this value yourself. It can consist of Latin letters and numbers, the maximum length is 32 characters. If you plan to use several user directories, their IDs must be different.
4. Enter a value in the **Domain DNS** field.
5. Enter a value in the **DN of user container** field.
6. Enter the username and password for the account.
7. Enable the **Use LDAPS** checkbox.
8. If necessary, change the mapping of user attributes and/or user group attributes.
9. Click **Add**.
10. Click **Next** to proceed to the next step of the wizard.

▼ Selecting FreeIPA or OpenLDAP

1. Click **Add User Directory**.
2. In the **Directory Service** field, select one of the values: **FreeIPA**, **OpenLDAP**.
3. Enter a value in the **Directory ID** field. Create this value yourself. It can consist of Latin letters and numbers, the maximum length is 32 characters. If you plan to use several user directories, their IDs must be different.
4. Enter a value in the **Domain DNS** field.
5. Enter a value in the **DN of user container** field.
6. Enter the username in DN format (example: 'uid=pamadmin,cn=users,cn=accounts,dc=my,dc=company') and password for the account.
7. Enable the **Use LDAPS** checkbox.
8. If you selected FreeIPA, specify **User and Group Identifier Format**: SID or GUID.
9. If necessary, change the mapping of user attributes and/or user group attributes.
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 | **Internal user**

1. Select an account from the directory.
2. 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 Windows.

> ⚠ **CAUTION**
>
> If you selected an internal user in the previous **Role Administrators** step, the Windows mechanism selection is not available. This combination of settings is an incorrect PAM configuration, as the administrator cannot authenticate to the system.
>
> If a user from the directory is selected as the first administrator, then the Windows mechanism can be selected. However, with this configuration, working with internal users is not supported.

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

1. If necessary, add a Syslog server.

> ▼ Syslog server
>
> Syslog server is used for integration with SIEM system. Events and text logs are written to the Syslog server in real time, during the active session, not after it is terminated. This allows incidents and anomalies associated with the actions of privileged users to be identified as quickly as possible.
>
> 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_3.2/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 master 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.

> ⚠ **CAUTION**
>
> The wizard must be launched on the host on which management server or access server of the PAM will be installed, otherwise an error for the wizard will occur.

1. Download and unpack the Web Wizard distribution on your Linux machine.
2. Place the CA certificate in **..PAM_3.0\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. Run 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 **New PAM Installation**.
2. Click **Next** to proceed to the next step of the wizard.

▼ 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.

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 Management Server, RDP Access Server, SSH Access Server, PostgreSQL Access Server. Please note that you cannot add multiple hosts with the same address.

   ▼ 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**.
7. If you selected **by password** in the previous step, then enter **Login** and **Password**. If you selected **by SSH key** in the previous step, then enter **Login**, **sudo password**, **SSH key** and **Passphrase**.
8. 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**.
7. If you selected **by password** in the previous step, then enter **Login** and **Password**. If you selected **by SSH key** in the previous step, then enter **Login**, **sudo password**, **SSH key** and **Passphrase**.
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**.

7. If you selected **by password** in the previous step, then enter **Login** and **Password**. If you selected **by SSH key** in the previous step, then enter **Login**, **sudo password**, **SSH key** and **Passphrase**.
8. 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**.
7. If you selected **by password** in the previous step, then enter **Login** and **Password**. If you selected **by SSH key** in the previous step, then enter **Login**, **sudo password**, **SSH key** and **Passphrase**.
8. Click **Add**.

> ⓘ **INFO**
>
> Management Server, RDP Access Server, SSH Access Server, PostgreSQL Access Server 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
MC/UC HTTP	80
MC/UC HTTPS	443
Gateway Service	8443

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

Certificates

In this step you need to download 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.

<details>
<summary>Selecting Microsoft SQL</summary>

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.
</details>

Data Storage

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

<details>
<summary>Other storage types</summary>

If you select SMB, fill in the following fields:

- Network path
</details>

- 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

1. Click **Add User Directory**.
2. In the **Directory Service** field, select one of the values: **FreeIPA**, **OpenLDAP**.
3. Enter a value in the **Directory ID** field. Create this value yourself. It can consist of Latin letters and numbers, the maximum length is 32 characters. If you plan to use several user directories, their IDs must be different.
4. Enter a value in the **Domain DNS** field.
5. Enter a value in the **DN of user container** field.
6. Enter the username in DN format (example: 'uid=pamadmin,cn=users,cn=accounts,dc=my,dc=company') and password for the account.
7. Enable the **Use LDAPS** checkbox.
8. If you selected FreeIPA, specify **User and Group Identifier Format**: SID or GUID.
9. If necessary, change the mapping of user attributes and/or user group attributes.
10. Click **Add**.
11. 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. Enter a value in the **Directory ID** field. Create this value yourself. It can consist of Latin letters and numbers, the maximum length is 32 characters. If you plan to use several user directories, their IDs must be different.
4. Enter a value in the **Domain DNS** field.
5. Enter a value in the **DN of user container** field.
6. Enter the username and password for the account.
7. Enable the **Use LDAPS** checkbox.
8. If necessary, change the mapping of user attributes and/or user group attributes.
9. Click **Add**.
10. 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 | **Internal user**

1. Select an account from the directory.
2. 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 or RADIUS.
2. If you selected RADIUS, add a RADIUS server and enter the required information.

<details>
<summary>RADIUS authentication</summary>

> ⚠ **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.
</details>

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

1. If necessary, add a Syslog server.

   ▼ Syslog server

   Syslog server is used for integration with SIEM system. Events and text logs are written to the Syslog server in real time, during the active session, not after it is terminated. This allows incidents and anomalies associated with the actions of privileged users to be identified as quickly as possible.

   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_3.2/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 master 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.

> ⚠ **CAUTION**
>
> The wizard must be launched on the host on which management server or access server of the PAM will be installed, otherwise an error for the wizard will occur.

1. Download and unpack the Web Wizard distribution on your Linux machine.
2. Place the CA certificate in **..PAM_3.0\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. Run 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 **New PAM Installation**.
2. Click **Next** to proceed to the next step of the wizard.

▼ 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.

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 Management Server, RDS Access Server, SSH Access Server, PostgreSQL Access Server. Please note that you cannot add multiple hosts with the same address.

   ▼ 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**.
7. If you selected **by password** in the previous step, then enter **Login** and **Password**. If you selected **by SSH key** in the previous step, then enter **Login**, **sudo password**, **SSH key** and

Passphrase.
8. 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**.
7. If you selected **by password** in the previous step, then enter **Login** and **Password**. If you selected **by SSH key** in the previous step, then enter **Login**, **sudo password**, **SSH key** and **Passphrase**.
8. Click **Add**.

> ⓘ **INFO**
>
> Management Server and RDS Access Server can be located on the same host.
> RDP Access Server, SSH Access Server, PostgreSQL Access Server 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**.
> 4. Enter the IP address or DNS in the **Balancer Address** field.
> 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**.
> 7. If you selected **by password** in the previous step, then enter **Login** and **Password**. If you selected **by SSH key** in the previous step, then enter **Login**, **sudo password**, **SSH key** and **Passphrase**.
> 8. 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
MC/UC HTTP	80
MC/UC HTTPS	443
Gateway Service	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 download 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.

<details>
<summary>Selecting PostgreSQL</summary>

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.

</details>

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.

<details>
<summary>Other storage types</summary>

If you select SMB, fill in the following fields:

- Network path
- Domain
- Username
- Password

</details>

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

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

1. Click **Add User Directory**.
2. In the **Directory Service** field, select **Active Directory**.
3. Enter a value in the **Directory ID** field. Create this value yourself. It can consist of Latin letters and numbers, the maximum length is 32 characters. If you plan to use several user directories, their IDs must be different.
4. Enter a value in the **Domain DNS** field.
5. Enter a value in the **DN of user container** field.
6. Enter the username and password for the account.
7. Enable the **Use LDAPS** checkbox.
8. If necessary, change the mapping of user attributes and/or user group attributes.
9. Click **Add**.
10. Click **Next** to proceed to the next step of the wizard.

▼ Selecting FreeIPA or OpenLDAP

1. Click **Add User Directory**.
2. In the **Directory Service** field, select one of the values: **FreeIPA**, **OpenLDAP**.

3. Enter a value in the **Directory ID** field. Create this value yourself. It can consist of Latin letters and numbers, the maximum length is 32 characters. If you plan to use several user directories, their IDs must be different.
4. Enter a value in the **Domain DNS** field.
5. Enter a value in the **DN of user container** field.
6. Enter the username in DN format (example: 'uid=pamadmin,cn=users,cn=accounts,dc=my,dc=company') and password for the account.
7. Enable the **Use LDAPS** checkbox.
8. If you selected FreeIPA, specify **User and Group Identifier Format**: SID or GUID.
9. If necessary, change the mapping of user attributes and/or user group attributes.
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 | **Internal user**

1. Select an account from the directory.
2. 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 Windows.

> ⚠ **CAUTION**
>
> If you selected an internal user in the previous **Role Administrators** step, the Windows mechanism selection is not available. This combination of settings is an incorrect PAM configuration, as the administrator cannot authenticate to the system.
>
> If a user from the directory is selected as the first administrator, then the Windows mechanism can be selected. However, with this configuration, working with internal users is not supported.

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

<details>
<summary>RADIUS authentication</summary>

> ⚠ **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.
</details>

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

1. If necessary, add a Syslog server.

   ▼ Syslog server

   Syslog server is used for integration with SIEM system. Events and text logs are written to the Syslog server in real time, during the active session, not after it is terminated. This allows incidents and anomalies associated with the actions of privileged users to be identified as quickly as possible.

   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_3.2/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 master 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.

> ⚠ **CAUTION**
>
> The wizard must be launched on the host on which management server or access server of the PAM will be installed, otherwise an error for the wizard will occur.

1. Download and unpack the Web Wizard distribution on your Linux machine.
2. Place the CA certificate in **..PAM_3.0\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. Run 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 **New PAM Installation**.
2. Click **Next** to proceed to the next step of the wizard.

▼ 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.

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 Management Server, RDP Access Server, SSH Access Server, PostgreSQL Access Server. Please note that you cannot add multiple hosts with the same address.

   ▼ 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**.
7. If you selected **by password** in the previous step, then enter **Login** and **Password**. If you selected **by SSH key** in the previous step, then enter **Login**, **sudo password**, **SSH key** and **Passphrase**.
8. 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**.
7. If you selected **by password** in the previous step, then enter **Login** and **Password**. If you selected **by SSH key** in the previous step, then enter **Login**, **sudo password**, **SSH key** and **Passphrase**.
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**.

7. If you selected **by password** in the previous step, then enter **Login** and **Password**. If you selected **by SSH key** in the previous step, then enter **Login**, **sudo password**, **SSH key** and **Passphrase**.
8. 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**.
7. If you selected **by password** in the previous step, then enter **Login** and **Password**. If you selected **by SSH key** in the previous step, then enter **Login**, **sudo password**, **SSH key** and **Passphrase**.
8. Click **Add**.

> ⓘ **INFO**
>
> Management Server, RDP Access Server, SSH Access Server, PostgreSQL Access Server 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**.
> 4. Enter the IP address or DNS in the **Balancer Address** field.
> 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**.
> 7. If you selected **by password** in the previous step, then enter **Login** and **Password**. If you selected **by SSH key** in the previous step, then enter **Login**, **sudo password**, **SSH key** and **Passphrase**.
> 8. 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
MC/UC HTTP	80
MC/UC HTTPS	443
Gateway Service	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 download 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.

<details>
<summary>Selecting Microsoft SQL</summary>

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.

</details>

Data Storage

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

<details>
<summary>Other storage types</summary>

If you select SMB, fill in the following fields:

- Network path
- Domain
- Username
- Password

</details>

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

1. Click **Add User Directory**.
2. In the **Directory Service** field, select one of the values: **FreeIPA**, **OpenLDAP**.
3. Enter a value in the **Directory ID** field. Create this value yourself. It can consist of Latin letters and numbers, the maximum length is 32 characters. If you plan to use several directories, their IDs must be different.
4. Enter a value in the **Domain DNS** field.
5. Enter a value in the **DN of user container** field.
6. Enter the username in DN format (example: 'uid=pamadmin,cn=users,cn=accounts,dc=my,dc=company') and password for the account.
7. Enable the **Use LDAPS** checkbox.
8. If you selected FreeIPA, specify **User and Group Identifier Format**: SID or GUID.
9. If necessary, change the mapping of user attributes and/or user group attributes.
10. Click **Add**.
11. 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. Enter a value in the **Directory ID** field. Create this value yourself. It can consist of Latin letters and numbers, the maximum length is 32 characters. If you plan to use several user directories, their IDs must be different.
4. Enter a value in the **Domain DNS** field.

5. Enter a value in the **DN of user container** field.
6. Enter the username and password for the account.
7. Enable the **Use LDAPS** checkbox.
8. If necessary, change the mapping of user attributes and/or user group attributes.
9. Click **Add**.
10. 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 | **Internal user**

1. Select an account from the directory.
2. 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 or RADIUS.
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

1. If necessary, add a Syslog server.

> ▼ Syslog server
>
> Syslog server is used for integration with SIEM system. Events and text logs are written to the Syslog server in real time, during the active session, not after it is terminated. This allows incidents and anomalies associated with the actions of privileged users to be identified as quickly as possible.
>
> 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_3.2/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
```

IIS Setup

Add a registry entry and configure IIS (for Windows)

Additional Components Setup

Install and configure PamSu, Axidian Privilege Agent and Axidian Privilege Desktop Console

RADIUS Configuring

Edit the appsettings.json configuration file

RDP File Signature Configuring

Edit the appsettings.json configuration file

TOTP Second Factor via Email Setup

Edit the appsettings.json configuration file (optional)

Enabling Restart of Proxy Service Containers

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

Integration with User Directories

Configure integration with FreeIPA or OpenLDAP user directories (optional)

Configuring PAM for use with NFS

2 items

IIS Setup

When deploying Management server on Windows Server and IIS please 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. Run **IIS** snap-in, go to **Default Web Site** section.
3. Open **Configuration Editor** in **Manage** section.
4. Expand the dropdown list **Section:**, select **system.webServer\security\requestFiltering**.
5. Expand the **requestLimits** item, set **maxQueryString** to **8192**.
6. Click **Apply** in the **Actions** section.
7. Go to **Default Web Site\core** section.
8. Open **Configuration Editor** in **Manage** section.
9. Expand the dropdown list **Section:**, select **system.webServer\serverRuntime**.
10. Set **uploadReadAheadSize** to **1048576**.
11. Click **Apply** in the **Actions** section.
12. Restart the server.

Additional Components Setup

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

Components are placed in the *..PAM_3.2\axidian-pam-tools\pamsu* folder.

Choose the **ossl** build to use static OpenSSL libs from the pamsu package:

- ..PAM_3.2\axidian-pam-tools\pamsu\axidian-privilege.pamsu-ossl*.x64.deb
- ..PAM_3.2\axidian-pam-tools\pamsu\axidian-privilege.pamsu-ossl*.x64.rpm

Choose the **no-ossl** build if pamsu cannot work with static OpenSSL libs and needs to use OpenSSL from the Operating System.

- ..PAM_3.2\axidian-pam-tools\pamsu\axidian-privilege.pamsu-no-ossl*.x64.deb
- ..PAM_3.2\axidian-pam-tools\pamsu\axidian-privilege.pamsu-no-ossl*.x64.rpm

Copy the pamsu installation package to the resource and run the command:

Installation on Debian-based distros

```
$ sudo dpkg -i axidian-privilege.pamsu*.deb
```

Installation on RedHat-based distros

```
$ sudo rpm -i axidian-privilege.pamsu*.rpm
```

Configuration

On the Resource, you must configure the trust to the Core and Idp web server certificate. You can check if the certificate is OK by running the command:

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

Open the **/etc/pamsu.conf** file in any editor with root privileges, specify the idp_url, api_url, log_path and log_level settings:

- **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

```
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_*
```

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

Axidian Privilege Agent

Axidian Privilege Agent should be installed directly to the resources to enable the RDP text logging capabilities.

> ⚠ **CAUTION**
>
> If the agent on the Resource is not installed and Save text logs option is enabled in the policy, **the user session will be aborted automatically** in a minute.

> ⚠ **CAUTION**
>
> Please make sure that no third-party software is blocking the Agent's work. **Axidian Privilege Windows Agent** (Pam.Proxy.WindowsAgent.exe) process will start automatically when new session starts on the resource.

After Axidian Privilege Agent is installed, reboot the computer or log out and log in again. No additional configuration is required.

Axidian Privilege 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.

Writing Events to Syslog

Windows **Linux**

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

```
1  <Application Id="pam" SchemaId="Pam.Schema">
2    <ReadTargetId>Pam.TargetDb</ReadTargetId>
3    <WriteTargets>
4      <TargetId>Pam.TargetDb</TargetId>
5      <TargetId>Pam.Syslog</TargetId>
6    </WriteTargets>
7    <AccessControl>
```

```
8       <!--<CertificateAccessControl CertificateThumbprint="001122...AA11"
    Rights="Read" />-->
9     </AccessControl>
10  </Application>
```

3. In 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

```
1  <Targets>
2    ...
3    <Target Id="Pam.TargetDb" Type="mssql"/>
4    <Target Id="Pam.Syslog" Type="syslog"/>
5  </Targets>
```

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

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 orthe 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 o

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
      }
    ]
  },
```

RDP File Signature Configuring

Enabling RDP File Signing

To do so you need to edit the Rdp section of the Core configuration file located along the path listed below:

C:\inetpub\wwwroot\core — for Windows

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

/etc/axidian/axidian-privilege/core — for Linux

```
"Rdp": {
   "UseRemoteApp": false,
   "SignRdpFile": true,
   "Certificate": "/etc/",
   "Password": "1234"
 },
```

Description of the Parameters of the Rdp Section of Configuration File

- **SignRdpFile** — enable RDP file signature
- **Certificate** — certificate thumbprint or path to the certificate itself
- **Password** — certificate password. Should be specified if **Certificate** is a path to the certificate itself

After editing the configuration file restart the **Core** component.

Windows

Restart IIS.

Linux

Go to the folder **/etc/axidian/axidian-privilege**:

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

Restart the Axidian Privilege Core component:

```
sudo docker compose -f docker-compose.management-server.yml up -d core --force-recreate
```

or

```
sudo docker-compose -f docker-compose.management-server.yml up -d core --force-recreate
```

Certificate Setup

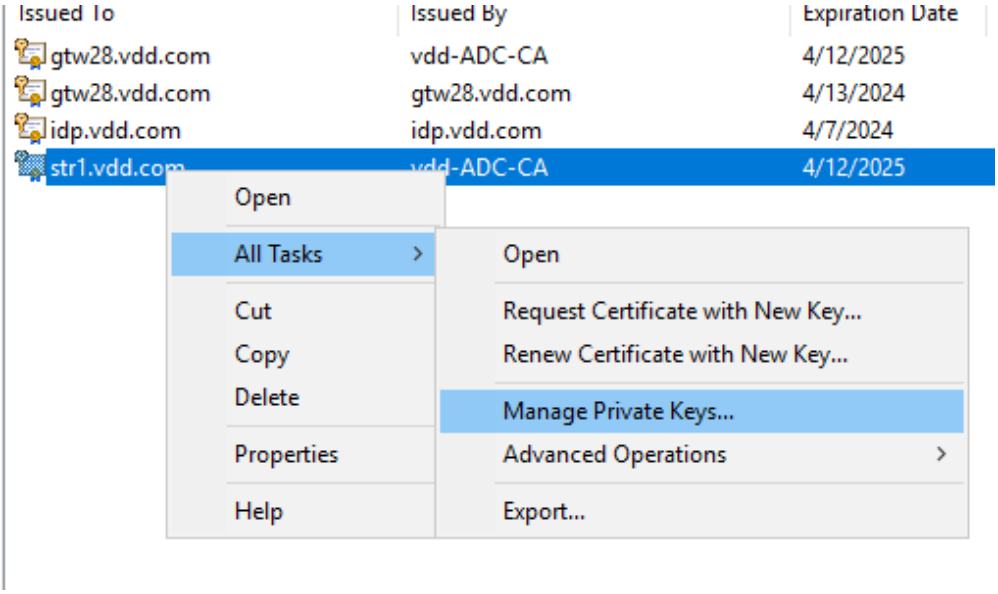
To enable RDP file signing, you need a certificate issued by a certification authority.

> **NOTE**
>
> All actions described below take place on a management server with the Core component installed.

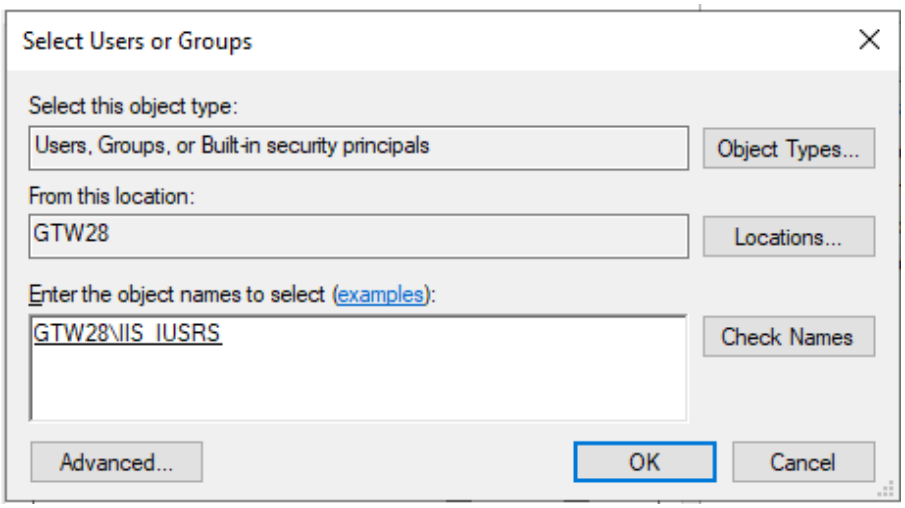
Windows with Fingerprint

1. Add the certificate to your computer's personal storage.

2. Open certificate menu, select **All Tasks** → **Manage Private Keys...**.



3. Click **Add...**, in the window that opens, click **Locations...**, select local computer → **OK**.
4. In the **Enter the object names to select** field enter **IIS_IUSRS** → **OK**.



5. Edit the configuration file by specifying the certificate thumbprint without a password.

Linux with Key Importing in PFX Format

Import a certificate in PFX format with a private key and password in the folder: **/etc/axidian/axidian-privilege/keys/rdp-sign.pfx**.

Edit the configuration file, specifying the path to the certificate and the password.

To the following file **/etc/axidian/axidian-privilege/docker-compose.management-server.yml** in the **core - volumes** section add the following line to organize certificate forwarding to the container:

```
1  volumes:
```

```
      - ./core/events:/var/lib/axidian/axidian-privilege/events
      - ./core/appsettings.json:/app/appsettings.json:ro
      - ./keys/shared/protector:/etc/axidian/axidian-
privilege/keys/shared/protector:ro
      - ./keys/core:/etc/axidian/axidian-privilege/keys/core:ro
      - ./ca-certificates:/usr/local/share/ca-certificates:ro
      - ./logs/core:/app/logs
      - ./keys/rdp-sign.pfx:/etc/axidian/axidian-privilege/keys/rdp-sign.pfx
```

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.

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
```

Integration with User Directories

This page describes how to set up Axidian Privilege integration with Active Directory, FreeIPA and OpenLDAP user directories.

To change the user catalog reading parameters, you need to edit the `UserCatalog` section in the Core and Idp configuration files.

Path to the Core configuration file:

Windows	C:\inetpub\wwwroot\core\appsettings.json
Linux	/etc/axidian/axidian-pam/core/appsettings.json

Path to the IdP configuration file:

Windows	C:\inetpub\wwwroot\idp\appsettings.json
Linux	/etc/axidian/axidian-pam/idp/appsettings.json

Setting up Integration with Active Directory

The configuration files initially contain settings for integration with Active Directory, no additional changes are required.

Setting Up a Search for Users Belonging to a Security Group

To set up a search for users belonging to a specified security group you need to configure the `CatalogFilter` parameter.

Example of setting the parameter for one security group

```
"CatalogFilter": "memberOf=cn=Admins,CN=Builtin,DC=vdd,DC=com"
```

Example of setting the parameter for multiple security groups

```
"CatalogFilter": "(|(memberOf=cn=Admins,CN=Builtin,DC=vdd,DC=com)
(memberOf=cn=PrivelledgeAccounts,OU=Groups,DC=vdd,DC=com)
(memberOf=cn=Admins1,OU=PAMUsers,DC=vdd,DC=com))"
```

Example of setting the parameter for multiple security groups when Management Server is on Linux

```
"CatalogFilter": "CatalogFilter":"|
(memberof=CN=PAM_USERS,CN=Builtin,DC=mii,DC=local,DC=com)
(memberof=CN=Test,CN=Builtin,DC=mii,DC=local,DC=com)"
```

The **ContainerPath** parameter must also be filled in, because only those users who are members of the OU that you specified in the value of the **CatalogFilter** parameter will be read.

▼ Example of a UserCatalog section with security group filled in

```
"UserCatalog": {
    "RootProvider": "ad",
    "Providers": {
      "ActiveDirectory": [
        {
          "Id": "ad",
          "ConnectorType": "Ldap",
          "Domain": "axidian.test",
          "Port": "636",
          "AuthType": "Basic",
          "SecureSocketLayer": true,
          "ContainerPath": "DC=axidian,DC=test",
          "CatalogFilter":
  "memberOf=cn=SecurityGroup,OU=PAMUsers,DC=axidian,DC=test"
          "UserName": "IPAMADReadOps@axidian.test",
          "Password": "qwe123",
          "UserMapRules": {
            "Settings": [
              {
                "Category": "person",
                "Class": "user"
              }
            ]
```

```
            }
          }
        ]
      }
}
```

For more information on configuring the CatalogFilter parameter, see the Microsoft documentation.

Setting Up Integration with FreeIpa or AldPro

To set up an integration with the FreeIPA or AldPro user directory, users of the directory must have the following attributes:

- `entryUUID` or `ipaUniqueID`
- `cn`
- `entryDn`
- `ipaNTSecurityIdentifier`
- `krbPrincipalName`
- `uid`

▼ Example of the UserCatalog section for FreeIPA or AldPro user directory

```
{
  "Id": "ad",
  "ConnectorType": "Ldap",
  "LdapServerType": "FreeIpa", // Replace with AldPro when setting to AldPro
  "Domain": "ald.sup", // Name of the domain or specific controller
  "Port": 389, // 389 for connecting via LDAP, 636 for connecting via LDAPS
  "AuthType": "Basic",
  "SecureSocketLayer": false,// false for connecting via LDAP, true for connecting via LDAPS
  "ContainerPath": "dc=ald,dc=sup",
  "UserName": "uid=pamread,cn=users,cn=accounts,dc=ald,dc=sup", // Domain access credentials. Must be in distiguishedName format, the account must have read permissions for the required attributes
  "Password": "Q1w2e3r4", // Account password to access the domain
  "GroupMapRules": {
    "Settings": [
```

```
      {
       "Category": "",
       "Class": "ipantgroupattrs"
       }
     ],
     "Attributes": {
       "Id": "ipaUniqueID",
       "Name": "cn",
       "SamAccountName": "cn",
       "CanonicalName": "cn",
       "DistinguishedName": "entryDn",
       "SidBytes": "ipaNTSecurityIdentifier"
      }
     },
     "UserMapRules": {
       "Settings": [
        {
         "Category": "",
         "Class": "person"
        }
       ],
       "Attributes": {
         "Id": "ipaUniqueID",
         "Name": "cn",
         "PrincipalName": "krbPrincipalName",
         "SamAccountName": "uid",
         "DistinguishedName": "entryDn",
         "SidBytes": "ipaNTSecurityIdentifier",
         "ThumbnailPhoto": "jpegPhoto",
         "JpegPhoto": "jpegPhoto"
        }
     }
}
```

If directory users have an `entryUUID` attribute and have no `ipaUniqueID` attribute, then in the `GroupMapRules` and `UserMapRules` sections in the `Attributes` section, you need to remove the `"Id": "ipaUniqueID"` parameter.

Setting Up Integration with OpenLDAP

To set up an integration with the OpenLDAP user directory, users of the directory must have the following attributes:

- `cn`
- `entryDn`
- `uid`

<details>
<summary>Example of the UserCatalog section for OpenLDAP user directory</summary>

```
{
  "Id": "oldap",
  "ConnectorType": "Ldap",
  "LdapServerType": "OpenLdap",
  "Domain": "oldap.local", // Name of the domain or specific controller
  "Port": 389, // 389 for connecting via LDAP, 636 for connecting via LDAPS
  "AuthType": "Basic",
  "SecureSocketLayer": false, // false for connecting via LDAP, true for connecting via LDAPS
  "ContainerPath": "DC=oldap,DC=local",
  "UserName": "cn=IPAMADReadOps,dc=oldap,dc=local", // Domain access credentials. Must be in distiguishedName format, the account must have read permissions for the required attributes
  "Password": "QWEqwe123", // Account password to access the domain
  "GroupMapRules": {
    "Settings": [
      {
        "Category": "",
        "Class": "groupOfUniqueNames"
      }
    ],
    "Attributes": {
      "Name": "cn",
      "SamAccountName": "cn",
      "CanonicalName": "cn",
      "DistinguishedName": "entryDn",
      "Members": "uniqueMember"
    }
  },
  "UserMapRules": {
    "Settings": [
      {
        "Category": "",
        "Class": "inetOrgPerson"
      }
    ],
```
</details>

```
    "Attributes": {
      "Name": "cn",
      "SamAccountName": "uid",
      "DistinguishedName": "entryDn",
      "ThumbnailPhoto": "photo",
      "JpegPhoto": "photo"
    }
  }
}
```

Setting Up an Integration with Multiple User Directories

To set up an integration with multiple user directories, please follow these steps:

1. Change the `RootProvider` parameter value to "orUCP".
2. In the `Ldap` section, list the user directories with which integration is required, separated by commas. Provider IDs must not match. The IDs of the providers that PAM previously worked with should not change.
3. Add the `Or` section from the example below, in which write the Ids of the providers sections.

▼ Example of the UserCatalog section for two user directories

```
"UserCatalog": {
    "RootProvider": "orUCP",
    "Providers": {
      "Ldap": [
        {
          "Id": "ad",
          "ConnectorType": "Ldap",
          "LdapServerType": "ActiveDirectory",
          "Domain": "axidian.test",
          "Port": 636,
          "AuthType": "Basic",
          "SecureSocketLayer": true,
          "ContainerPath": "OU=UsersPAM,DC=axidian,DC=test",
          "UserName": "IPAMADReadOps@axidian.test",
          "Password": "qwe123",
```

```
      "UserMapRules": {
        "Settings": [
          {
            "Category": "person",
            "Class": "user"
          }
        ]
      }
    },
    {
      "Id": "ipa",
      "ConnectorType": "Ldap",
      "LdapServerType": "FreeIpa",
      "Domain": "ipa.redos",
      "Port": 389,
      "AuthType": "Basic",
      "SecureSocketLayer": false,
      "ContainerPath": "DC=ipa,DC=redos",
      "UserName": "uid=IPAMADReadOps,cn=users,cn=accounts,dc=ipa,dc=redos",
      "Password": "qwe123",
      "GroupMapRules": {
        "Settings": [
          {
            "Category": "",
            "Class": "ipantgroupattrs"
          }
        ],
        "Attributes": {
          "Name": "cn",
          "SamAccountName": "cn",
          "CanonicalName": "cn",
          "DistinguishedName": "entryDn",
          "SidBytes": "ipaNTSecurityIdentifier"
        }
      },
      "UserMapRules": {
          "Settings": [
            {
              "Category": "",
              "Class": "person"
            }
          ],
          "Attributes": {
              "Name": "cn",
              "PrincipalName": "krbPrincipalName",
              "SamAccountName": "uid",
```

```
                    "DistinguishedName": "entryDn",
                    "SidBytes": "ipaNTSecurityIdentifier",
                    "ThumbnailPhoto": "jpegPhoto",
                    "JpegPhoto": "jpegPhoto"
                }
            }
          }
        ],
        "Or": [
          {
            "Id": "orUCP",
            "Providers": {
              "ad": {"IgnoreExceptions": true},
              "ipa": {"IgnoreExceptions": true}
            }
          }
        ]
      }
    }
```

▼ Example of the UserCatalog section for three user directories

```
"UserCatalog": {
    "RootProvider": "orUCP",
    "Providers": {
      "Ldap": [
        {
          "Id": "ad",
          "ConnectorType": "Ldap",
          "LdapServerType": "ActiveDirectory",
          "Domain": "axidian.test",
          "Port": 636,
          "AuthType": "Basic",
          "SecureSocketLayer": true,
          "ContainerPath": "OU=UsersPAM,DC=axidian,DC=test",
          "UserName": "IPAMADReadOps@axidian.test",
          "Password": "qwe123",
          "UserMapRules": {
            "Settings": [
              {
                "Category": "person",
                "Class": "user"
```

```
            }
          ]
        }
      },
      {
        "Id": "ad2",
        "ConnectorType": "Ldap",
        "LdapServerType": "ActiveDirectory",
        "Domain": "axidian2.test",
        "Port": 636,
        "AuthType": "Basic",
        "SecureSocketLayer": true,
        "ContainerPath": "OU=PAMUsers,DC=axidian2,DC=test",
        "UserName": "IPAMADReadOps@axidian2.test",
        "Password": "qwe123",
        "UserMapRules": {
          "Settings": [
            {
              "Category": "person",
              "Class": "user"
            }
          ]
        }
      },
      {
        "Id": "ipa",
        "ConnectorType": "Ldap",
        "LdapServerType": "FreeIpa",
        "Domain": "ipa.redos",
        "Port": 389,
        "AuthType": "Basic",
        "SecureSocketLayer": false,
        "ContainerPath": "DC=ipa,DC=redos",
        "UserName": "uid=IPAMADReadOps,cn=users,cn=accounts,dc=ipa,dc=redos",
        "Password": "qwe123",
        "GroupMapRules": {
          "Settings": [
            {
              "Category": "",
              "Class": "ipantgroupattrs"
            }
          ],
          "Attributes": {
            "Name": "cn",
            "SamAccountName": "cn",
            "CanonicalName": "cn",
```

```
                "DistinguishedName": "entryDn",
                "SidBytes": "ipaNTSecurityIdentifier"
              }
            },
            "UserMapRules": {
                "Settings": [
                  {
                    "Category": "",
                    "Class": "person"
                  }
                ],
                "Attributes": {
                    "Name": "cn",
                    "PrincipalName": "krbPrincipalName",
                    "SamAccountName": "uid",
                    "DistinguishedName": "entryDn",
                    "SidBytes": "ipaNTSecurityIdentifier",
                    "ThumbnailPhoto": "jpegPhoto",
                    "JpegPhoto": "jpegPhoto"
                }
            }
          }
        ],
        "Or": [
          {
            "Id": "orUCP",
            "Providers": {
              "ad": {"IgnoreExceptions": true},
              "ad2": {"IgnoreExceptions": true},
              "ipa": {"IgnoreExceptions": true}
            }
          }
        ]
      }
    }
```

Preparing NFS media storage

Follow the steps below on the NFS server

Configuring PAM for work with NFS

Follow the steps below on the NFS server

Preparing NFS media storage

RPM DEB

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
```

Configuring PAM for work with NFS

Before configuring PAM to work with NFS, you must install and configure NFS media storage.

Linux **Windows**

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-temp.

```
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**:

```
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:

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

7. **Restart containers using the following command:**

```
```

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

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 master 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.

> ⚠ **CAUTION**
>
> The wizard must be launched on the host on which management server or access server of the PAM will be installed, otherwise an error for the wizard will occur.

1. Download and unpack the Web Wizard distribution on your Linux machine.
2. Place the CA certificate in **..PAM_3.0\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. Run 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**.

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

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.
</details>

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.

<details>
<summary>Read more</summary>

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
```

</details>

- 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_3.2/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
```

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, for additional system protection, automatic encryption of configuration files occurs during component installation.

While working with the system, you may need to edit configuration files. To do this, you will need to remove encryption, edit the files, and then encrypt the files again.

This can be done using a utility on Windows or a script on Linux.

Configuration files of the Core, IdP, ProxyApp and Log Server components are subject to encryption.

Windows Utility

Unencryption

1. Go to the *..PAM_3.2\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_3.2\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:

- OC Windows Server — %ProgramData%\Axidian\Keys
- OC Linux — /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.e
      ],
      "ApplicationPaths": [
```

```
        "C:\\Program Files\\Axidian\\Axidian
Privilege\\Gateway\\ProxyApp\\Microsoft.WebView2.FixedVersionRuntime\\msedgewebview2.e
      ]
    },
    {
      "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 is 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.

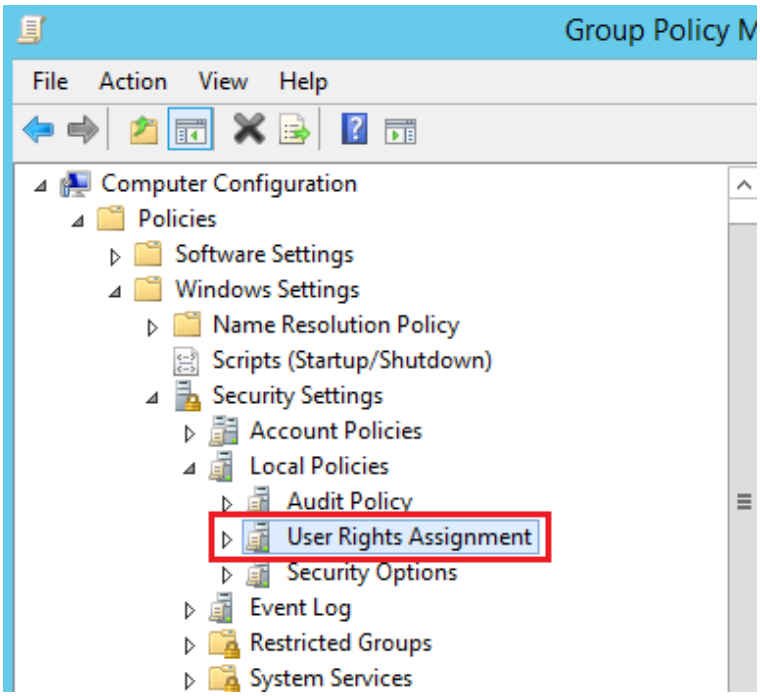
To ensure the security of footage, Axidian Privilege implements an encryption mechanism that allows you to safely store and use it within the solution. Encryption is performed using the AES256 algorithm, the key itself is unique for each Axidian Privilege session.

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
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	NT AUTHORITY\NETWORK SERVICE, NT AUTHORITY\LOCAL SERVICE, BUILTIN\Administrators

Policy	Description	Values
	a system, but its use can be harmful in such cases like attacks of type service denial.	
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
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

Policy	Description	Values
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
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
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.	Undefined

Policy	Description	Values
	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.	
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
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.	BUILTIN\Administrators

Policy	Description	Values
	Attention! Assign it only to trusted users. Symbolic links can expose vulnerabilities in applications that are not designed to handle them.	
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
Deny log on as a service	This security setting determines which service accounts are denied to execute registration of	BUILTIN\Guests

Policy	Description	Values
	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.	
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
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 privelege 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	BUILTIN\Administrators

Policy	Description	Values
	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.	
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.	NT AUTHORITY\LOCAL SERVICE, NT AUTHORITY\NETWORK SERVICE

Policy	Description	Values
	For more information, see "Audit: Shut down system immediately if security audit logging cannot be logged".	
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	BUILTIN\Administrators, NT AUTHORITY\SERVICE

Policy	Description	Values
	providing login credentials.The requested level is lower 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
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	BUILTIN\Administrators

Policy	Description	Values
	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.	
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
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	BUILTIN\Administrators

Policy	Description	Values
	Viewer security log. A user with this privilege can also view and clear the security log.	
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
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	BUILTIN\Administrators

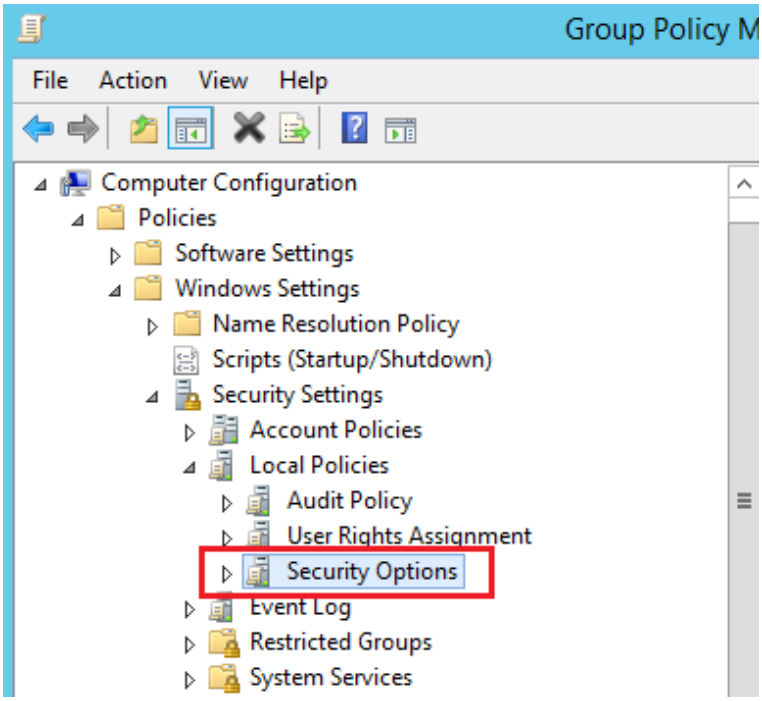
Policy	Description	Values
	users who can change the system and user environment variables that appear on the Advanced tab of the System Properties dialog box. For information about how to change these variables, see Add or change the value of environment variables.	
Perform volume maintenance tasks	This 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
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!	BUILTIN\Administrators

Policy	Description	Values
	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.	

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
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!	Enabled

Policy	Description	Values
	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.	

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	Enabled

Policy	Description	Values
	Windows. Enabling this setting can cause a very large number of events (sometimes several hundred per second) during archiving.	

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	Enabled

Policy	Description	Values
	logged on interactively, the CD drive will be accessible over the network.	
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
Network access: Do not allow anonymous	This security setting determines what additional permissions are given to anonymous connections to this computer.	Enabled

Policy	Description	Values
enumeration of SAM accounts	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.	
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
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	Enabled

Policy	Description	Values
	computer (for future use during domain authentication). Note. Changes to the configuration of this security setting will take effect only after you restart Windows.	
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

Policy	Description	Values
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
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
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.	Classic - local users authenticate as themselves

Policy	Description	Values
	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.	

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
Network security: Force logoff when	This security setting determines whether users are logged out when they connect to the local computer outside of the	Enabled

Policy	Description	Values
logon hours expire	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.	
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	Send NTLMv2 response only. Refuse LM & NTLM

Policy	Description	Values
	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 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 NTLMv2 session security: Enabled Require 128-bit encryption: Enabled

Policy	Description	Values
	Require 128-bit encryption. If 128-bit encryption is not negotiated, the connection will not be established.	
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	This security setting determines whether the virtual memory page file is cleaned up when the system shuts down.	Enabled

Policy	Description	Values
memory pagefile	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.	

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 type of rules of politics of restricted software using). With these policies, you can create a certificate rule that allows or denies launch of a programs signed with Authenticode, depending on digital certificate. To apply certificate rules, you must enable this security setting.	Enabled

Policy	Description	Values
	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.	

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	This policy setting controls whether UIAccess applications (UIA programs) can automatically disable the secure desktop for promotion requests used by a standard user.	Disabled

Policy	Description	Values
using the secure desktop	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.	
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	Prompt for consent for non-Windows binaries

Policy	Description	Values
	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. EIf 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 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.	Prompt for credentials on the secure desktop

Policy	Description	Values
	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.	
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	Enabled

Policy	Description	Values
	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.	
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
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	Enabled

Policy	Description	Values
	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.	
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 can't add Microsoft accounts

Policy	Description	Values
	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.	
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
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	Disabled

Policy	Description	Values
	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.	
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
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:	Enabled

Policy	Description	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.	
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:	User display name only

Policy	Description	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 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	

Policy	Description	Values
	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. 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. EIf 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."	
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	5 invalid logon attempts

Policy	Description	Values
	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.	
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
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	Disabled

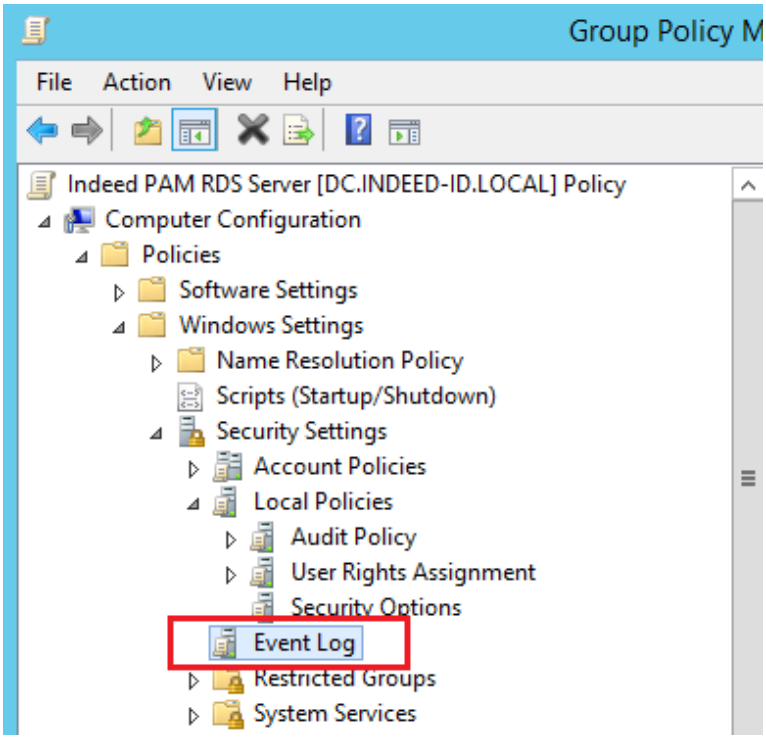
Policy	Description	Values
	whose accounts are in a domain with client computers and domain controllers running an operating system that was released before Windows 8. This setting should be set to Automatic (the default) so that the file server can automatically determine whether a user is required to 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.	
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
Microsoft network server: Server	This policy setting controls the level of verification that the folder or printer shares computer (server) performs on the	Off

Policy	Description	Values
SPN target name validation level	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.	
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

Policy	Description	Values
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



▼ Description of policies

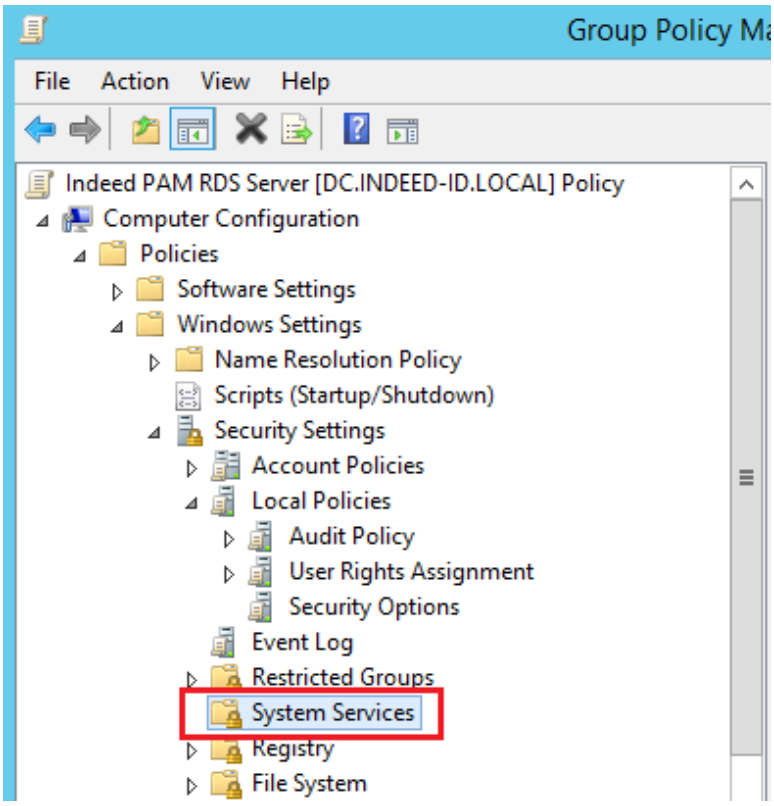
Policy	Description	Values
Maximum application log size	This security setting determines the maximum size of the application event log (max. 4 GB). In practice, a lower limit is used (approximately 300 MB). Notes. PLog file sizes must be multiples of 64 KB. If you enter a value that is not a multiple 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

Policy	Description	Values
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 to access to the application event log. Notes. This setting is not included in the local computer policy object.	Enabled
Prevent local guests group from accessing security log	This security setting determines whether guests are denied to 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 to access to the security event log. Notes. This setting is not included in the local computer policy object.	Enabled
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.	As needed

Policy	Description	Values
	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.	
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 privelege.	As needed
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

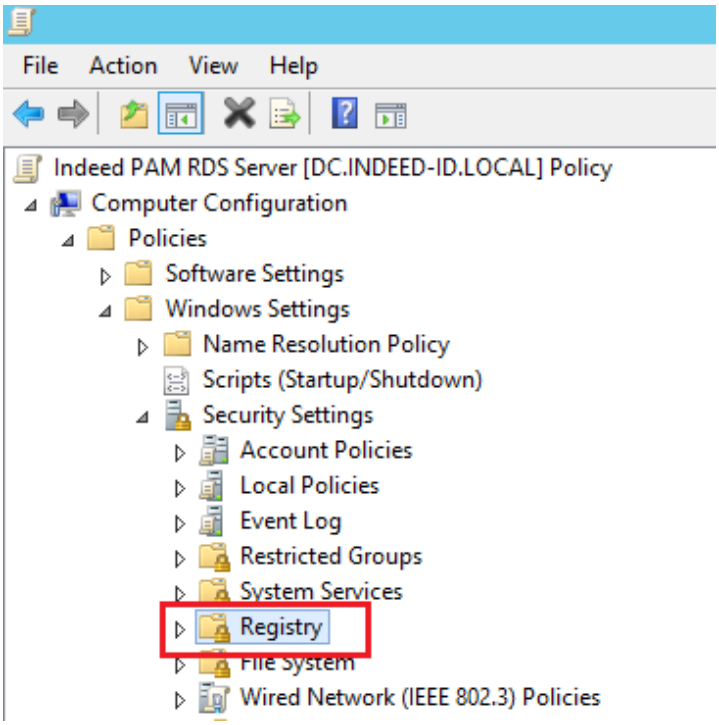
Auditing

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

Type	Principal	Access	Applies To
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

Type	Principal	Access	Applies To
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

Type	Principal	Access	Applies To
Allow	ALL APPLICATION PACKAGES	Read	This key and subkeys

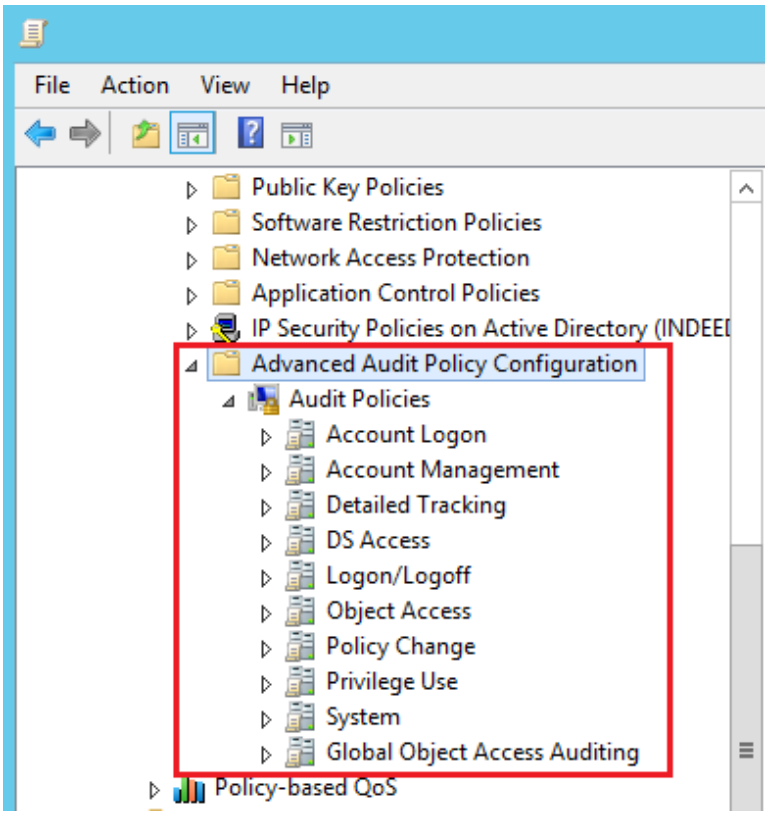
Inheritance disabled

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

Policy	Description	Values
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
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	Success, Failure

Policy	Description	Values
	is applied. No events are logged while parameters are changed.	
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
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
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.	Success, Failure

Policy	Description	Values
	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.	
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
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.	Success, Failure

Policy	Description	Values
	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.	
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	Success, Failure

Policy	Description	Values
	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.	
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
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	Failure

Policy	Description	Values
	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. AThe 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.	
Audit File Share	This policy setting allows you to audit attempts to access public folders. EWhen 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
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

Policy	Description	Values
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
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
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 priveleges: Access to a computer from the network.	Success, Failure

Policy	Description	Values
	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.	
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 priveleges) 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.	Success, Failure

Policy	Description	Values
	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.	
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.	Failure

Policy	Description	Values
	Changing the value of hardware environment parameters. Process-level token replacement. Recovering files and directories. Changing the owner of a file or other object.	

System

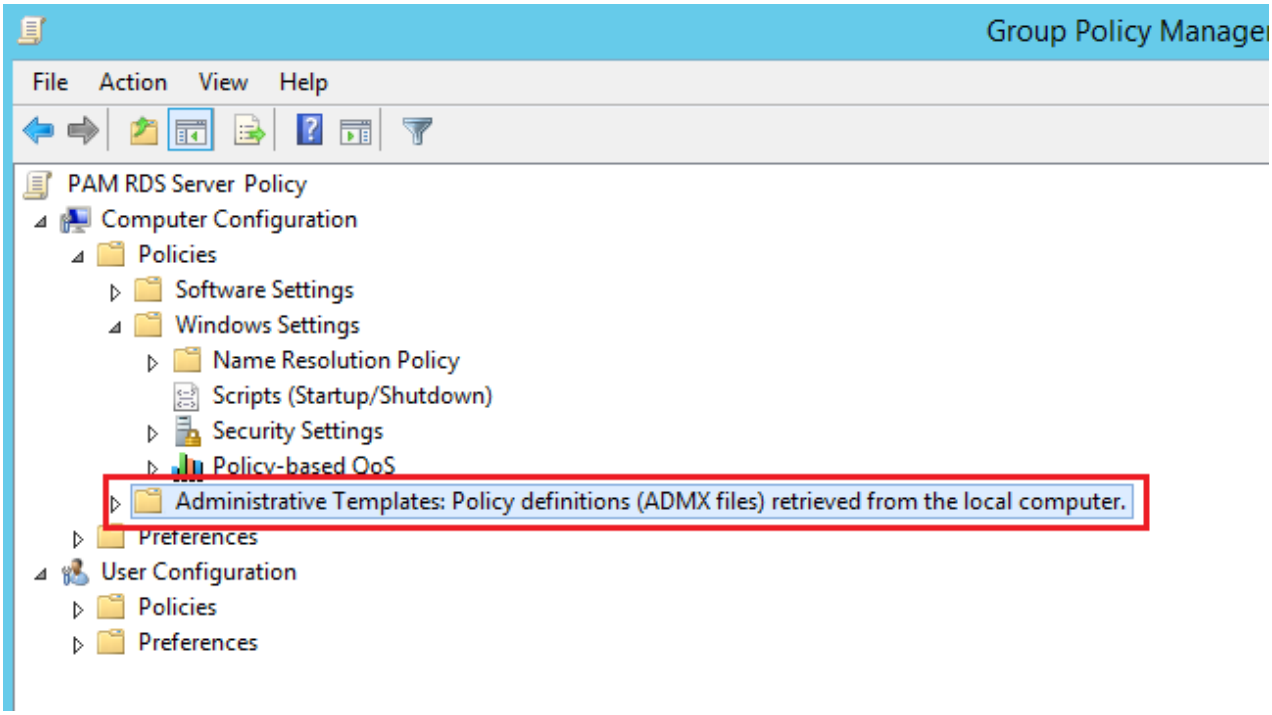
▼ Description of policies

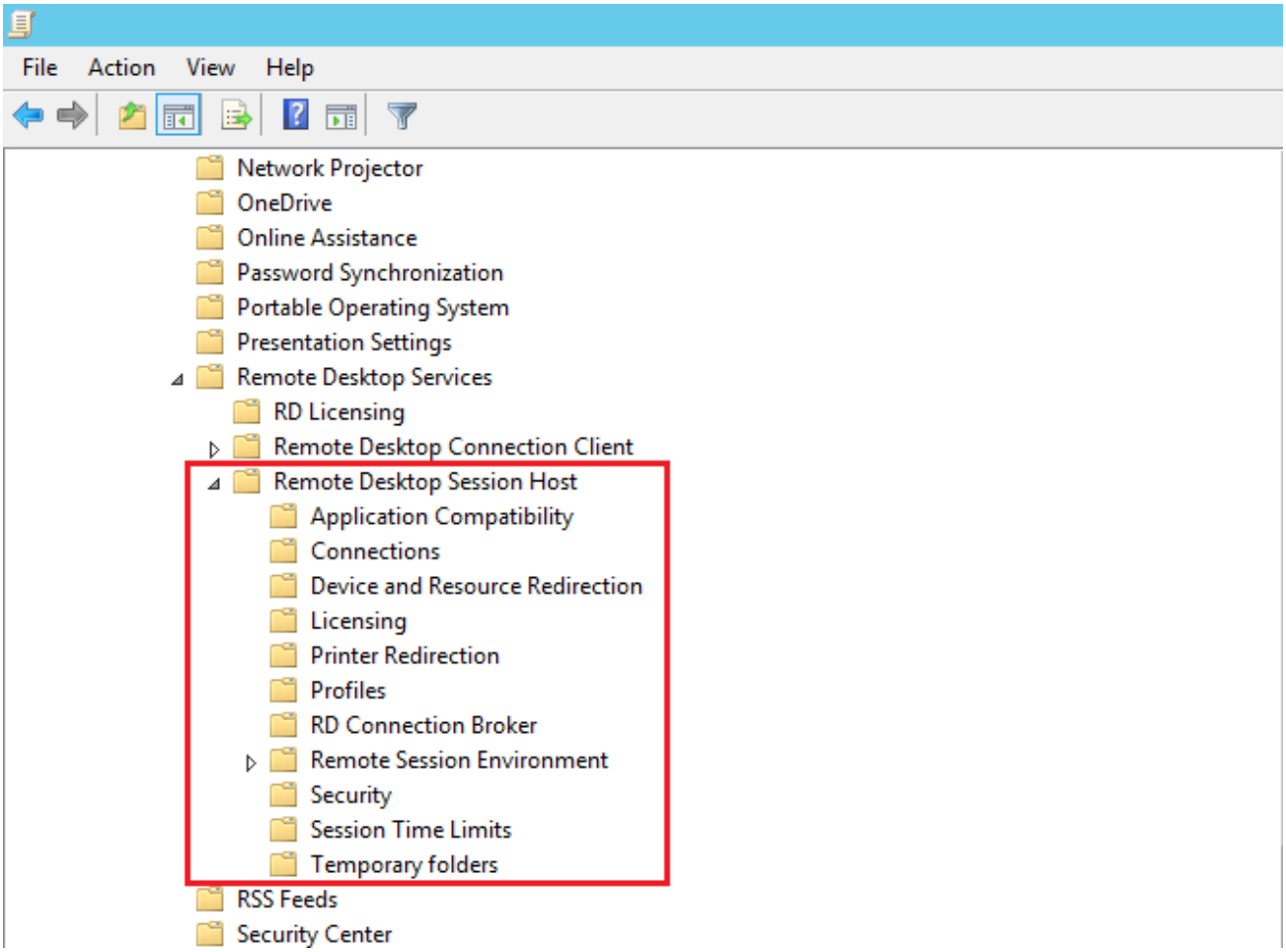
Policy	Description	Values
Audit Other System Events	This policy setting allows you to audit the following events: Starting and stopping the Windows Firewall service and driver. Security policy processing by the Windows Firewall service. Operations with encryption key files and migration operations.	Success, 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	Success, Failure

Policy	Description	Values
	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.	
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
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	Enabled Keep-Alive interval: 1

Policy	Description	Values
	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.	
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	Enabled Options: Full Control without user's permission

Policy	Description	Values
	with a user's Remote Desktop Services session if the user consents.	

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
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.	Enabled

Policy	Description	Values
	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.	
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	Enabled

Policy	Description	Values
	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.	
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.	Enabled Encryption Level: High Level

Policy	Description	Values
	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! 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	This policy setting determines whether a Remote Desktop Services session is timed out instead of disconnected.	Enabled

Policy	Description	Values
are reached	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 both settings are configured, the setting in the Computer Configuration folder takes priority.	
Set time limit for disconnected	This policy setting allows you to configure a time limit for disconnected Remote Desktop Services sessions.	Enabled End a disconnected

Policy	Description	Values
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.	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
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	Disabled

Policy	Description	Values
	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.	

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_3.2\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_3.2\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:

   i. Via Group Policy.
   ii. 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:

i. Enable **Define these policy settings** option.

ii. 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

If the encryption key is compromised, it is possible to rotate the database master key without stopping PAM.

To do so, use the Key Rotator utility.

Windows	..PAM_3.2\axidian-pam-tools\key-rotator\Pam.Tools.KeyRotator.exe
Linux	/etc/axidian/axidian-pam/tools/key-rotator.sh

Before you run the utility, you need to edit the **Encryption** section in the configuration file of the Core component.

By default, this section contains only the **Primary** subsection which specifies the current encryption key and other database settings.

To rotate the database encryption key, follow these steps:

1. Create a **Secondary** subsection in the **Encryption** section.
2. Move settings from **Primary** to **Secondary**.
3. Enter the new encryption key in the **Primary** section.
4. Save your configuration file.
5. Run the Key Rotator utility.
6. Wait for the utility to complete and remove the **Secondary** section from the configuration file.

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 **Ок**
8. Run **Windows registry editor** (RegEdit)
9. Expand
   the **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System** br
   anch
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 Active Directory

> ⚠ **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.

Administrator console

Gain access to the administrator console

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

Section Reference

17 items

Dumping Passwords

Read about dumping passwords in an emergency

Usage of PostgreSQL Proxy

Explore Axidian Privilege PostgreSQL Proxy

Administrator 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.

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.

<details>
<summary>Check users presence</summary>

1. Go to the **Users** section.
2. Click  .
3. Make sure that all users from the specified organizational unit are displayed correctly.
</details>

<details>
<summary>License the installation</summary>

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_гггг.мм.дд.lic* format.
5. In the **Configuration** → **Licenses** section, click **Add** and attach the received license file.
</details>

<details>
<summary>Fill in the component addresses</summary>

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.
</details>

<details>
<summary>Check events</summary>
</details>

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** and/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

The section contains a list of policies, sorted by priority.

The following data is displayed for policies:

- **Priority** — a number indicating the order in which a particular policy is applied. Zero priority is the default policy that is applied last. The higher the policy, the higher its priority, and vice versa.
- **Name** — policy name.
- **Description** — policy description.
- — number of users with policy.
- — number of user groups with policy.
- — number of accounts with policy.
- — number of resources with policy.
- — number of domains with policy.

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

Show Credentials 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).

Option	Description
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 credentials viewed by user it must be confirmed by 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.
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	Automatic search for resource data and privileged accounts will be

Option	Description
accounts once in X days	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.
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.

Option	Description
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.
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.

Option	Description
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 Entry

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.
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

Option	Description
	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.

Option	Description
	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 ends automatically.
Enforce exclusive usage of account	If the option is enabled, then the only one active session can be opened for 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
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

Option	Description
	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 text	If the option is enabled, then after the session will be available for viewing and downloading a text log.
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.
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. The range

Option	Description
	of values from 1 to 10.
Video resolution	The setting allows you to set the resolution for video recording.
Video log rotation	If this option is enabled, then video recordings will be automatically deleted.
Remove video older than X days	Automatically delete video recordings older than the specified number of days. Minimum is 1 day.
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.
Screenshots log rotation	If this option is enabled, screenshots will be automatically deleted.
Remove screenshots older that X days	Automatically delete screenshots older than the specified number of days.
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 will be automatically deleted.
Remove transferred files older than X days	Automatically delete transferred files older than the specified number of days.

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.

Gateway and SSH Proxy

Option	Description
Override Gateway settings	If this option is enabled, the following settings will be used instead of those specified in the Configuration section.
RDCB address	Remote Desktop Connection Broker IP address/DNS name
RDCB collection name	Remote Desktop Connection Broker collection name for Axidian Privilege Gateway
Use RDGW	Connect to Axidian Privilege Gateway with Remote Desktop Gateway
RDGW address	Remote Desktop Gateway address for Axidian Privilege Gateway
Gateway RDP file parameters	The parameters will be added to the Axidian Privilege gateway RDP settings and will override the default settings.
Override SSH Proxy settings	If this option is enabled, the following settings will be used instead of those specified in the Configuration section.
SSH Proxy address	IP address or DNS name and port (optional)

RDP

> **NOTE**
>
> The settings are applied only when connecting to servers via RDP.

Option	Description
Printers	If the option is enabled, then the user will be able to forward the printer from his workplace to the final resource.
Clipboard	If the option is enabled, the user will be able to use the clipboard between his workstation and the end resource.
Smart cards	If the option is enabled, the user will be able to forward the smart card from his workplace to the resource.
Ports	If the option is enabled, then the user will be able to forward COM ports from his workstation to the final resource.
Local drives	If the option is enabled, then the user will be able to forward local disks from his workplace to the resource.
RDP file parameters	Parameters that will be added to RDP connection settings, also they will override the default settings.
Require a trusted resource certificate to open an RDP session	If the option is enabled and the resource certificate is invalid, the user will not be able to open a session. If the option is disabled and the resource certificate is invalid, the user will be able to open a session.

SSH

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 `[`. More information on Boost regular expression syntax is available here.
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 `[`.

   More information on Boost regular expression syntax is available here.
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 option.
SFTP	SFTP file transfer option.
Maximum file size, MB	A file larger than this value cannot be transferred.

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 | **X.509 Certificate**

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.

Users

3 items

User Groups

User Groups

Resources

5 items

Services

Services

Resource Groups

Resource Groups

Accounts

2 items

Domains

4 items

Structure

Structure

Permissions

3 items

Action Requests

Action Requests

Active Sessions

Active Sessions

All Sessions

1 items

Events

Events

Notifications

Notifications

Configuration

2 items

Roles

Roles

Applications

Applications

Users

There are two types of users in Axidian Privilege 3.2:

- users from the directory service;
- internal users.

For users from the directory service, the *Directory* value is specified in the **Source** field. For internal users, the *PAM* value is specified in the **Source** field.

By default, the page displays 15 users. At the bottom of the page there is a paginator to view the remaining users. If there are fewer than 15 users, they are placed on one page and paginator is not displayed.

You can change the default number of users on a page in the configuration file.

Windows	C:\inetpub\wwwroot\pam\mc\assets\config\config.prod.json
Linux	/etc/axidian/axidian-pam/mc/config.prod.json

A maximum number of users that can be viewed is 1000. On the page with the 1000th user, you will see a message saying that more users cannot be loaded.

Search

Search is located in the **Users** section

Quick Search

Enter your **First Name**, **Last Name**, **Phone Number** or **Email** in whole or in part in the search bar.

Extended Search

Click **Extended Search** and enter one or more criteria: **First Name**, **Last Name**, **Phone Number** or **Email** in whole or in part.

> **INFO**

> There is no search by login.

Removed Users Search

1. Open the **Users** section and click **Extended Search**.
2. Select **Deleted** for the **State** parameter.
3. Click **Search**.

User Profile

The profile displays the data of an Active Directory user:

- **Username** — the name used to login to the system.
- **Path** — LDAP.
- **Email** — email address.
- **Phone** — user phone number.
- **Policy** — user-specific session policy.
- **Photo** — user photo from Active Directory (thumbnailPhoto attribute).

Permissions

The user permissions are displayed in the **Permissions** tab.

The following data is displayed for every permission:

- **#** — permission number.
- **Users** — the Active Directory user, the permission is given to.
- **Resources** — the resources that RDP, SSH or web session can be started at under the account specified in the permission. Next to the resource name there is the privileged account that is used to access the resource.
- **Permission status icons** — A status tooltip will be displayed on mouse hover.

Sessions

All active and finished sessions of the user are available in the **Sessions** tab.

The following data is displayed for every session:

- **User** — An Active Directory directory user, which initiated the session.
- **Account** — Privileged account, which is used to open the RDP, SSH or Web session.
- **Resource** — The resource on which the RDP, SSH or Web session was opened on behalf of the privileged account.
- **Connection address** — The actual address used to open the session.
- **Duration** — The duration of the session.
- **Connection** — Remote Connection Type (RDP, SSH, User connection types)
- **Connected to Axidian Privilege** — Date and time when the session was opened.
- **Finished** — Date and time when the session was finished.
- **State** — Displays the current state of the session (active, finished or aborted).

To view detailed information about the session, you must click on it. To show all sessions for this user, click **Show all**.

Authenticators

This tab displays information about password and second factor, as well as SSH keys that allow users to connect to SSH Proxy without a password.

Password

- Last password change is the date and time the password was changed in the Axidian PAM database. The field is only displayed for internal users.
- Password expiration is the number of days, hours, or minutes remaining until the next password change. The field is only displayed for internal users.

2FA

- Require the second factor: when *Enabled* or *Default* value is selected, the second factor is required for authentication in the system. If you select *Disabled* , the user will not be prompted for the second factor.
- Authenticator State: indicates, whether the authenticator factor is registered or not. *Not enrolled* value indicates an unregistered authenticator. When a user logs in to the Administrator Console or User Console for the first time, a page opens with authenticator registering instructions. After registration, the *Enrolled* value is displayed.

Supported key encryption algorithms:

- rsa-sha2-256
- rsa-sha2-512
- ecdsa-sha2-nistp256
- ecdsa-sha2-nistp384
- ecdsa-sha2-nistp521
- ssh-ed25519

SSH keys

SSH keys allow users to connect to SSH Proxy without a password. A maximum of 10 SSH keys can be added per user. The keys must be unique within the user. The same key can be used by several users.

Enable or disable the use of keys:
Configuration → User Authentication → SSH Key Authentication.

> ⚠ **CAUTION**
>
> To add a key to a user, the administrator must have the *User.ManageSshAuthorizedKeys* privilege.

You can add an SSH key in two ways:

- manually: paste the copied string containing the encryption algorithm and the key;
- attach the X.509 certificate file.

Key in text format | **X.509 Certificate**

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**.

To remove an SSH key:

> ⚠ **CAUTION**
>
> SSH key cannot be restored once removed.

1. Open the user's profile.
2. Go to the **Authenticators** tab.
3. Select one or more keys.
4. Click **Remove**.

When you remove an SSH key, the session opened with this key is not terminated.

> ⓘ **INFO**
>
> If the same key is added to more than one user, keep in mind that removing a key from one user will not remove the same key from other users.

Events

The user 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** — is the account that initiated the event generation.

To view detailed information about the event, you must click on it. To show all events for this user, click **Show all**.

Creating an Internal User

> ⚠ **CAUTION**
>
> Connection via RDS is not available for internal users.

1. Open the **Users** section.
2. Click **Create**.
3. Set the **Login**. Only Latin letters, numbers, periods, underscores and hyphens are allowed. This value is used to log in to the Administrator Console and User Console.
4. Set or generate a password.
5. Copy the password and pass it to the user.

   > ⚠ **CAUTION**
   >
   > Do not close the window until you have passed the password to the user.

6. Enter the user email.
7. Optionally fill in the fields: **Name**, **Surname**, **Phone**, **Description**.
8. Click **Create** to stay in the **Users** section, or click **Create and Open** to navigate to the new user profile.

Operations on Users

This section describes the operations that can be performed on users.

Editing

1. Open the user's profile.
2. Click ✎ to the right of the parameter to set or edit it.

Selecting a Policy

1. Open the user's profile.
2. Click ✎ to the right of the **Policy** parameter to add or change a policy.

Creating a Permission

1. Open the user's profile.
2. Click **Add permission**.
3. Select one or several resources, a group of resources or an ad hoc resource. Click **Next**.
4. Select an Account. Click **Next**.
5. Optionally set time restrictions. Click **Next**.
6. Optionally set permission parameters. Click **Next**.
7. Optionally enter a **Description**. Click **Next**.
8. Check the selected data for permission and click **Create**.

Adding to a Group

1. Open the user's profile and go to the **User Groups** tab.
2. Click **Add User Groups**.
3. Select one or several groups.
4. Click **OK** and then click **Add**.

Removing from a Group

1. Open the user's profile and go to the **User Groups** tab.
2. Select one or several groups.
3. Click **Remove**.
4. In the pop-up window, click **Remove**.

Password Reset

> ⚠ **CAUTION**
>
> This operation is only applicable for internal users.

1. Open the internal user's profile.
2. Click **Reset password**.
3. Select one of the options: **Set a password manually** or **Generate**.
4. If you selected **Set a password manually**, set the password.
5. Pass the password to the user. After closing the form, it will be impossible to find out the password.
6. Optionally disable the **Require password change on first login** option.
7. Optionally disable the **Abort all active sessions and log out** option.
8. Click **Save**.

Password Change Request

> ⚠ **CAUTION**
>
> This operation is only applicable for internal users.

1. Open the internal user's profile.
2. Click **Reset password**.
3. Select **Request Password Change**.
4. Optionally disable the **Abort all active sessions and log out option**.
5. Click **Save**.

Resetting an Authenticator

1. Open the user profile and go to the **Authenticators** tab.
2. Click ✕ to the right of the required authenticator.

Disabling an Authenticator

1. Open the user profile and go to the **Authenticators** tab.
2. Click ✎ to the right of the **Require second factor** and select the appropriate option:
   - **Default** — second factor is required;
   - **Enabled** — second factor is required;
   - **Disabled** — second factor is not required.

Blocking

This feature helps PAM administrator to quickly close user's access to the resources. At the same time, there is no need to change resources and accounts.

A blocked user is unable to:

- open sessions;
- view, set and change account password;
- access authentication data of AAPM applications.

At the moment a user is blocked, all active sessions are terminated.

> ⚠ **CAUTION**
>
> Block a user if you notice suspicious actions from them. This allows you to quickly close user's access to the resources until the circumstances are clarified. You can unblock a user as quickly as block them.

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**.

> ⚠ **CAUTION**
>
> Do not use this feature to close access to former employees. They will still be able to authenticate to the user console and the administrator console. When employees leave, remove users from directory service.

Unblocking a User

To unblock a user:

1. Go to the **Users** section.
2. Open the user's profile.
3. Click **Unblock**.
4. In the pop-up window, click **Unblock**.

Removing

> ⚠ **CAUTION**
>
> This operation is only applicable for internal users.
>
> The user cannot be restored after deletion.
>
> It is not possible to remove yourself and the first role administrator.

1. Open the internal user's profile.
2. Click **Remove**.
3. Read the information in the pop-up window and click **Remove**.

Consequences of user deletion:

- The user loses access to the PAM and cannot authenticate.
- All active sessions end.
- All granted permissions are revoked.

- The user is excluded from all user groups in which the user is a member.
- The user is excluded from the scope of the policy in which the user is a member.
- The login of the deleted user changes: the suffix `_deleted` and a randomly generated string are added to the login. This allows to avoid errors when creating new users whose username matches the username of the previously deleted user.

Removed users no longer appear in the **Users** section, but they can be viewed using extended search.

Bulk Operations on Users

This section describes the operations that can be performed on multiple users at once.

Adding to a Group

1. In the **Users** section, select one or several users.
2. Click **Add to a group**.
3. Select one or several groups.
4. Click **Add**.

Blocking

1. In the **Users** section, select one or several users.
2. Click **Block**. If there is no such button, make sure that only active users are selected.
3. Click **Block** in the pop-up window.

Unblocking

1. In the Users section, select one or several blocked users.
2. Click **Unblock**. If there is no such button, make sure that only blocked users are selected.
3. In the pop-up window, click **Unblock**.

Password Change Request

> ⚠ **CAUTION**
>
> This operation is only applicable for internal users.

1. In the **Users** section, select one or several internal users.
2. Click **Request Password Change**. If there is no such button, make sure that only internal users are selected.

3. Optionally enable the **Abort all active sessions and log out** option.
4. Click **Save**.

Removing

> ⚠ **CAUTION**
>
> This operation is only applicable for internal users.
>
> The user cannot be restored after deletion.
>
> It is not possible to remove yourself and the first role administrator.

1. In the **Users** section, select one or several users.
2. Click **Remove**. If there is no such button, make sure that only internal users are selected.
3. Read the information in the pop-up window and click **Remove**.

Consequences of user deletion:

- The user loses access to the PAM and cannot authenticate.
- All active sessions end.
- All granted permissions are revoked.
- The user is excluded from all user groups in which the user is a member.
- The user is excluded from the scope of the policy in which the user is a member.
- The login of the deleted user changes: the suffix `_deleted` and a randomly generated string are added to the login. This allows to avoid errors when creating new users whose username matches the username of the previously deleted user.

Removed 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.

Creating a User Group in the Axidian Privilege

To add a user group you need to:

- Go to **User groups** section.
- In the **Users** section click **Add,** enter the name of the new group and click **Save**.

Adding a User Group from Active Directory

To add a user group from Active Directory you need to:

- Go to **User groups** section.
- In the **Users** section click **Add** and select the group and click **Save**.

Managing a User Group

Adding Users to a Group

> **NOTE**
>
> For groups created in Axidian Privilege only.

- Go to the user group you created.
- In the **Users** section click **Add** and select the required users.

Adding Permission to a User Group

- Go to the user group you created.
- Click **Add permission** and finish the adding.

Viewing Permissions You Create

- Open **Permission** section.
- View the permissions granted for the selected user group.

Viewing Information about the Current Sessions within the User Group and Events of the Axidian Privilege

- **Sessions** section displays active sessions.
- **Events** section displays all events that occurred in the Axidian Privilege

Synchronizing a User Group with a Directory

> **NOTE**
>
> For groups imported form Active Directory only.

- Go to the user group you created.
- Click **Synchronize**.

Setting a Policy for a User Group

1. Go to the existing user group.
2. Click to add or change a policy.

Resources

The section is intended to work with servers, workstations and network equipment.

Resource Search

Search is located in the **Resources** section.

Quick Search

Enter the **Resource Name** or **Address (DNS address/IP address)** in whole or in part in the search bar.

Extended Search

Click **Extended search** and enter one or more criteria, **Resource name** or **Address** (**DNS** or **IP**) in whole or in part. Select **Resource State**, **Service Connection**, **User Connection**, **SSH Key Fingerprint**.

Resource Page

The page displays the data of the resource specified while adding it:

- **Resource name** — is the computer name.
- **Description** — this can be an arbitrary text.
- **DNS name** — DNS name of the resource.
- **IP address** — IP address of the resource.
- **Operating system** — the name and version of the operating system (populated after synchronization).
- **Policy** — is the set of rules applied to local accounts added to Axidian Privilege.
- **Organizational unit** — organizational unit's name the resource belongs to.
- **Synchronization date** — date and time of the last data synchronization.
- **Accounts synchronization date** — dates and time of the last Accounts synchronization.
- **Service connection** — the type of connection to the resource that will be used by the local or domain service account.
- **Template** — The name of the template used for service operations (for SSH connector).
- **Service account** — Account name used for Service Connection.

User Connection

Connections are displayed and configured here for opening privileged sessions.

For each resource, you can create multiple user connections if several applications are installed on the server where privileged access is required.

Permissions

All permissions where the resource is used are displayed in the **Permissions** tab.

The following data is displayed for every permission:

- **#** — permission number.
- **Users** — the Active Directory user, the permission is given to.
- **Organizational unit** — organizational unit's name the specified resource belongs to.
- **Resources** — resources on which an RDP, SSH, or web session can be opened on behalf of the account specified in the permission.
- **Permissions status icons** — Status Tip will be displayed when you hover the mouse cursor.

Local Accounts

The added local accounts are displayed in the **Local accounts tab**.

The following data is displayed for every account:

- **Name** — is the local account's name.
- **Location** — the name of the resource or domain, where the account resides.
- **State** — displays the current status of the account (Pending, Ignored, Managed, Blocked or Removed).
- **Organizational unit** — organizational unit's name the specified resource belongs to.
- **Description** — account description.

Resource Groups

Resource groups in which this resource consists, are displayed on the **Resource groups** tab.

Sessions

All active and finished sessions at the resource 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** — organizational unit's name the resource belongs to.
- **Resource** — resource on which the session was opened.
- **Connection address** — The actual address of the connection to the target resource
- **Duration** — is the session duration.
- **Connection** — the connection type.
- **Connected to Axidian Privilege** — date and time when the session was started.
- **Finished** — date and time when the session was finished.
- **State** — 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 this resource, click **Show all**.

Events

The resource 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** — is the account that initiated the event generation.

To view detailed information about the event, click on it. To display all events for this resource, click **Show all**.

Services

> ⚠ **CAUTION**

> This tab is displayed only if the selected resource has a service connection for Windows 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 resource, to do this click **Add**.

Setting a Policy for a Resource

1. Open the resource profile.
2. Click  to add or change a policy.

Adding a Resource

Manual Add

To provide access to the resource to the directory users, you must add a new resource to the Axidian Privilege.

1. Switch to **Resources** section and click **Add**.
2. Select organizational unit.
3. Fill in the **Resource name**, **DNS name** and/or **IP Address** and **Description** fields.
   For Windows resources, you must specify the real computer name.
   When specifying an IP address make sure it is static.

Add from File

1. Prepare CSV-file.
2. Click **Add from file**.
3. Choose CSV-file.
4. Check **Adding with policy** option if a policy needs to be defined for resources.
5. Click **Save**.

Line format in CSV

```
Name; Description; DNS name; IP address; User Connection (UC) type; UC address; US port; UC matching url; UC matching url is regex; ServiceConnection account name; Service Connection type; Service Connection SSH template; Service connection address; Service Connection port; Cisco's privilege mode password
```

Example

```
Computer1;Typical Computer 1;res.test.com;;RDP;;;;;;;;;;

Computer2;Typical Computer 2;;192.168.0.102;SSH;;;;;;;;;;
```

User Connection Setup

For each resource, you need to configure a user connection that will be used to open a session on the resource.

RDP Connection Setup

- Select **RDP** Connection type.
- 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.
- If you need to open a session with the `mstsc /admin` parameter, enable the **Run as administrator** option.

> **INFO**
>
> When opening a session, you can select local drives to use in the remote session. It is also possible to connect without redirecting local drive.

SSH Connection Setup

- Select **SSH** Connection type
- 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

User Connection Setup

In Axidian Privilege, RDP and SSH connections are standard. Other connection types, for example, a web session or connection to a DBMS, are configured separately for each target application. Below we will consider examples of configuring a connection to the web console Citrix NetScaler and MS SQL Management Studio. After Axidian Privilege installation, these types of connections will not be in the list of connections. To create a new connection type, you may need to contact Technical Support.

Web Session Setup

- Select **Citrix NetScaler** Connection type
- Fill in **URL** of web application
- Fill in **Sign-in page URL** of web application if different

> ⓘ **NOTE**
>
> If the **Sign-in page URL** may not match the specified value after accessing it, then enable the **Regular expression** option, the option allows you to specify an expression that will match any address value.

DBMS Connection Setup

- Select **MS SQL Management Studio** connection type
- If the MS SQL Server instance connection address is different from the DNS name/IP address, specify it by selecting the appropriate checkbox
- Enter the **Port** if necessary

Service Connection Setup

This article will not consider setting up a service connection, a detailed description of the configuration process is available in the article Setting Up a Service Connection for Resources.

- Disable the **Use connector for service connection** option
- Complete the adding resource

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 / PostgreSQL Pro

- 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 **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.

> ⚠ **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.

Resource Operations

Resource Editing

The function allows you to change the following parameters of the resource:

- **Resource Name**
- **Description**
- **Organizational Unit**
- **Policy**
- **User Connection**
- **Service Connection**

To edit a resource, click  in the resource page to the right of the desired parameter.

Adding and Removing Tags

> **INFO**
>
> If you don't have any tags yet, create them in the **Configuration** section.

To add tags to a resource:

1. Open the resource's profile.
2. Click plus-icon next to the **Tags** field.
3. Select tags.
4. Click **Next**.
5. Check the selected tags.
6. Click **Add** to finish the operation.

> **INFO**
>
> Each resource can have a maximum of 50 tags.

To remove the tag from the resource:

1. Open the resource's profile.
2. Click cross-icon next to the tag you need to remove.
3. In the confirmation window, click **Remove**.

Removing Connected Entities

It is possible to remove values of the following fields of the resource:

- **Policy**;
- **Service Connection**.

> ⚠ **CAUTION**
>
> When a service connection is removed from a resource, 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 remove a **Policy** or a **Service Connection** from a resource, click the trash can icon on the resource page to the right of the desired parameter.

Adding User Connection

The function allows you to add one or more user connections available for a given resource.

1. Click **Add** on the **User connections** tab.
2. Select the type of connection.
3. Specify the address, connection port and other parameters of user connection.

Adding an Account

The function allows adding local resource accounts to Axidian Privilege, which can be used to provide access to the resource.

- Click **Add account** in Resource Profile
- Enter an Account **Name** and **Description**

Password and SSH Key

If a service connection of the SSH type is configured for the resource, then when adding an account, 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 adding *nix account. When adding Windows OS and DBMS accounts, the **Not set** item will be missing when setting up a password, and there will be no page for generating or manually installing an SSH key.

Password Settings

- Select **Not set**, **Generate random password**, or **Set password manually**
- Enter a password or continue by selecting **Not set** or **Generate random password**

SSH Key Settings

- Select **Not set**, **Generate new SSH key**, or **Set SSH key manually**
- Select the SSH key file and enter its password, or continue by selecting **Not set** or **Generate new SSH key**
- Finish adding your account

Checking the Connection to the Resource

The function allows you to check the network availability of the resource, the correctness of the address, name and password of the service account.

- Click **Check connection** in the resource page

Synchronization

The function allows you to get the correct resource name, OS or DBMS version, local resource accounts and security groups they belong to. **Synchronization** is available only for resources with a configured service connection, otherwise the **Synchronization** function will not be present in the resource.

- Click **Sync** on the resource page

> **NOTE**
>
> Accounts that have been added to Axidian Privilege using the Synchronize function will be marked with a symbol. To continue working with them, you must set or reset their password. A detailed description of the account verification process is described in the article.

Block

The function allows you to suspend all permissions that use the resource.

- Click **Block** in the resource profile

> **NOTE**
>
> The resource will be marked with a symbol. All permissions in which the resource is a contributor will be marked with a symbol.

Remove / Rollback a Resource

Removing a Resource

Before removing a resource, you must remove all accounts that were added from this resource.

> **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.

1. Open the resource page.
2. Click **Remove**.

Rolling Back Resources

> **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.

1. Click **Extended search** in the **Resources** section.
2. Enter the **Resource name** or **Address (DNS name/IP address)** in whole or in part.
3. Select **Removed** for the **State** field and click **Search**.
4. Open the resource page and click **Rollback**.
5. Enter the reason for the recovery and click **Rollback**.

Bulk Operations for Resources

Setting up a Service Connection

- Switch to the **Resources** section, check one or more resources and click **Setup service connection**

> **NOTE**
>
> For the selected resources, the same types of service connections will be configured and one service account will be selected. It is recommended to use a domain account as a service account, which has local administrator rights on all selected resources.

Checking the Connection to the Resource

- Switch to the **Resources** section, check one or more resources and click **Check connection**

Deleting Resources

- Switch to the **Resources** section, check one or more resources and click **Remove**

> **NOTE**
>
> Before deleting resources, you must delete all accounts that were added from the deleted resources.

Set Policy

- In the **Resources** section, select one or more resources and click **Set policy**
- Choose the policy for the selected resources and click **Select**
- In the confirmation window, click **Set**

Set Organizational Unit

- In the **Resources** section, select one or more resources and click **Set organizational unit**
- Choose the OU for the selected resources and click **OK**
- In the confirmation window, click **Set**

Adding tags

> **INFO**
>
> If you don't have any tags yet, create them in the **Configuration** section.

1. In the **Resources** section, select one or more resources and click **Add tags**.
2. Select one or more tags.
3. Click **Next**.
4. Check the selected resources and the selected tags.
5. Click **Add** to finish the operation.

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 | **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 **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**.

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, 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 and/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. Optional 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 | **Removing from service page**

1. Open the **Services** section.
2. Select one or more services.
3. 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

Quick Search

Enter the Resource group **Name** or **Description** in whole or in part in the search bar.

Extended Search

Enter the Resource group **Name** in whole or in part.

Choose group **State**:

- Enabled
- Removed

Select **Organizational unit**.

Resource Groups Functions

Editing a Resource Group

The function allows you to change the Name and Description of the group.

- Click in the resource profile to the right of the required parameter

Adding 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:
    i. If you check this option, then when adding each individual resource, you will need to specify a privileged **Account** to access the **Resource**.
    ii. 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.

Adding Permissions

A detailed description of working with permissions is described below, in the Permissions section.

To create a new permission, click **Add permission**, select a user from the AD directory or User group, Time restrictions, options for credentials, Description and click **Create**.

If the **Add resources with account** option was checked, the connection to the resource will be performed with the account specified when adding the resource to this group. If this parameter has not been checked, then you will be able to select Domain account or chose **using the user account** option in the **permission**. In the case of Domain account please make sure that account has remote access to all resources in this group.

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.

The list of created permissions can be viewed in the **Permissions** tab. Clicking on a permission will open its page.

Viewing Sessions

The Sessions tab displays a list of the latest sessions with each of the group's resources. Clicking the **Show all** link will open the search result for all sessions for this resource group in the All sessions section.

Viewing Events

The **Events** tab displays the latest events about this resource group. Clicking the **Show all** link will open the search result for all events for this resource group in the Events section.

Removing Resource Groups

In the **Resource groups** section, check one or more groups and click **Remove**.

Accounts

The section allows 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.

Account Search

The search is performed in the **Accounts** section.

Quick Search

Enter **Account name** in whole or in part in the search bar.

Extended Search

Click **Extended search** and enter one or more criteria, **Account name** in whole or in part.
Select account state:

- Pending
- Ignored
- Managed
- Blocked
- Removed

Select account location:

1. **Local account** To search, enter the **Resource name** or **DNS name/IP address** in whole or in part.
2. **Domain account** To search, enter **NetBIOS name** or **DNS name** in whole or in part.

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 at 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 is the account that initiated the event generation
- **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

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

- Select **Not set**, **Generate random password**, or **Set password manually**
- Enter a password or continue by selecting **Not set** or **Generate random password**

SSH Key Settings

- Select **Not set**, **Generate new SSH key**, or **Set SSH keymanually**.

To specify the SSH key manually, you need a key file in PEM format. If the key has already been created, make sure that it starts with the specified string, otherwise the key must be converted to RSA format:

```
-----BEGIN RSA PRIVATE KEY-----
```

To create a new key, use the puttygen utility, or one of the commands:

```
ssh-keygen -t rsa -m PEM
```

```
openssl genrsa -des3 -out privatekey.pem
```

- Select the SSH key file and enter its password, or continue by selecting **Not set** or **Generate new SSH key**.

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

The function allows you to check whether the account password or SSH key is valid.

- Click **Check** in the account page

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

The search is performed in the **Domains** section.

Quick Search

Enter **NetBIOS name** or **DNS name** in whole or in part in the search bar.

Extended Search

Click **Extended search** and enter one or more criteria, **NetBIOS name** or **DNS name** in whole or in part. Select domain state:

- Enabled
- Removed

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 the **Domain accounts** tab.

Resource Containers

All containers selected for synchronization of domain computers are displayed in the the **Domain accounts** tab.

Privileged Groups

All security groups selected for synchronization of domain accounts are displayed in the the **Domain accounts** tab.

Events

All events on the resource 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.

Permission Search

The search allows you to display only those permissions 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

You can enter one or several words into the search bar. Words can be written in whole or in part (3 or more letters).

Example

To find a permission with the description **Test permission for chief administrator** you need to enter any of the words: **test**, **permis**, **chief**, **adm**.

> ⚠ **CAUTION**
>
> You can't enter the trailing substring of the word to the search bar. If you enter the **mission** (the trailing substring of the word **permission**), this permission will not be found.

You can search for a permission using two words, e.g. **test permis**, **permis chief**, **chief adm**.

> ⚠ **CAUTION**
>
> The words in the search query must be in the same order as in the description of the permission. If you enter the **permis test**, the permission will not be found, because these words follow in the opposite direction in the description of the permission.

> The words in the search query must match the words that were next to each other in the reason for opening the session. You cannot enter words that have other words between them in the description. If you enter the **test adm**, the permission will not be found, because there are some other words between these words in the description.

Extended Search

You can search by one or several criteria. If you select several criteria, permissions that meet all of the listed criteria will be displayed.

Example

If you select **john.smith@company.demo** in the **User** field and **Revoked** in the **State** field, then only permissions of this user with this connection type will be displayed.

> ⚠ **CAUTION**
>
> Only one value can be selected in each field. You will not be able to display the permissions of the users **john.smith@company.demo** and **james.smith@company.demo** by one extended search query. You can do this using a text search for the query **smith**.

Permission Page

The permission page displays the following data:

- **Description** — custom text
- **Organizational unit** — the name of organizational unit in which the resource belongs
- **Users** — Active Directory users for which permission is granted
- **Created by** — Axidian Privilege administrator account who created the permission
- **Created at** — date and time the permission was created
- **Validity period** — the dates during which the permission is active
- **Access schedule** — the time period during which the permission is active
- **View account credentials** — permission to view the password or SSH key of the access account in the user console
- **Resource** — the name of the resource on which an RDP, SSH or web session can be opened on behalf of the account specified in the permission

- **Connection type** — remote connection type (RDP, SSH, custom types)
- **Connection address** — DNS name or IP address of the resource
- **Account** — an account that is used to open an RDP, SSH or web session on the resources specified in the permission

Creating a Permission

Permissions allow AD users to open sessions.

To create a permission:

1. Go to **Permissions** section.
2. Click **Create**.
3. In the opened wizard select Organizational Unit, Users, Resources, Account, Time Restrictions and Additional Permission Options.

> ⚠ **CAUTION**
>
> To be able to manage permissions you need the **PERMISSIONS MANAGEMENT** privileges (Permission.Create, Permission.Read, Permission.Revoke, Permission.Suspend).

Organizational Unit

Select organizational unit the resource is located in.

> ⓘ **NOTE**
>
> This wizard section will not be displayed when a permission is created by the local administrator of this organizational unit.

User

Select a user or user group.

To select a user:

1. On the **User** tab, in the search bar enter **Name**, **Surname**, **Phone number** or **Email** (whole words or partially). Press ENTER or  .
2. Select one or more users.

To select a user group:

1. On the **User Groups** tab, in the search bar enter **Name** or **Description** (whole words or partially). Press ENTER or  .
2. Select a user group.

Resource

Permissions can be issued for:

- PAM resources.
- Resource groups.
- Ad hoc resources.

To select a resource:

1. On the **Resources** tab, in the search bar enter **Resource name**, **DNS** or **IP** (whole words or partially). Press ENTER or  .
2. Select one or more resources.

To select a resource group:

1. On the **Resources groups** tab, in the search bar enter **Resource group name** (whole words or partially). Press ENTER or  .
2. Select a resource group.

> ⚠ **CAUTION**
>
> A special license is required to grant permissions to PostgreSQL resources or to groups containing such resources.

To select an ad hoc resource, on the **Ad hoc resources** tab select connection types that will be available to users to connect to ad hoc resources. Available connection types: RDP, SSH, Telnet.

> ⚠ **CAUTION**
>
> A special license is required to grant permissions to ad hoc resources.

Account

To access the resource, you can use a local, domain or personal user account.

> **INFO**
>
> If you have selected more than one resource, then for each of them you need to sequentially select an access account.

To select a local or domain account:

1. In the search bar enter **Account name** (whole words or partially). Press ENTER or  .
2. Select account.

To select a personal user account click **Continue using user account**.

> **CAUTION**
>
> Selecting a local account is not available for ad hoc resources.
>
> You can select only one account for all connection types for ad hoc resources.

Time Restrictions

The settings in this section are optional.

You can set the **validity period** for the permission — start date and time, end date and time. To do so:

1. Check **Begin** and **End** options.
2. Select date and time.

> **INFO**
>
> If the **Begin** and **End** options are not set, then the permission will be considered infinite.

> **CAUTION**

> Once the permission period expires, the session will be terminated.

You can also set access schedule for the permission. Connection will be available only during the specified hours. It is not possible to use the permission outside the schedule.

1. Check the **Allow access only** option.
2. Set **From** and **To** time.

> ⓘ **INFO**
>
> If options **From** and **To** are not set, then the permission will be valid 24 hours a day.

> ⚠ **CAUTION**
>
> When the time set in the access schedule expires, the session will be terminated.

Additional Permission Options

The settings in this section are optional.

Credentials

Axidian Privilege allows the administrator to set whether the user is allowed to view the password of privileged accounts that are used in their permissions. To allow, check the **Allow user to view account credentials** option.

Axidian Privilege allows the administrator to set whether the user is allowed to change the passwords of privileged accounts that are used in their permissions. To allow, check the **Allow change account credentials** option.

Connection Source

Axidian Privilege allows the administrator to set a specific network from which the user can connect to the resource. To do so, select the network in the **Network location sources for incoming connections** drop-down menu.

> ⓘ **INFO**

> If no Network Locations have been added, the only option in the drop-down menu will be **No Restrictions**.
>
> This means that this permission can be used from any device on the network.

Raising Privileges in SSH Sessions

Axidian Privilege allows the administrator to specify for each permission whether that permission will have access to pamsu or not.

Possible options:

- **Managed by policies** — access to pamsu will be provided in accordance with the policy selected for the resource for which permission is created.
- **Allowed** — regardless of the policy settings, this permission will provide the access to pamsu.
- **Denied** — regardless of the policy settings, in this permission, access to pamsu will be disabled.

Permission Operations

Permission Copying

This feature allows you to create a permission based on a previously created one. You can copy permissions regardless of their state, including revoked and suspended ones.

Copying is similar to the process of creating a permission. When copying, administrators are asked to edit the selected objects from the original permission—add missing objects or remove unnecessary ones.

> **INFO**
>
> This feature is only available in a permission profile.

1. Open the permission profile.
2. Click **Copy**.
3. If necessary, make changes to the list of selected objects on the pages of the wizard that opens.

   To view the list of selected objects, click  .

   > **INFO**
   >
   > If any user, resource, or account specified in the original permission is deleted or blocked, they will not be selected for new permission.

4. If necessary, set **Time Limits** and **Permission settings**.
5. Select **Action on original permission**—**Keep**, **Suspend**, or **Revoke**.

Permission Revocation

This feature allows you to revoke permissions that are no longer required.

> **CAUTION**
>
> Revoked permissions cannot be returned to an active state.

If you need to temporarily disable the use of a permission, suspend it.

When revoking a permission, remember that users will lose access immediately, not after they disconnect from the resource themselves.

> ⚠ **CAUTION**
>
> If the permission is revoked, the session will be terminated.

Revocation from the permission list | **Revocation from the permission profile**

1. Open the **Permissions** section.
2. Select the desired permission.
3. Click **Revoke**.

Revoked permissions no longer appear in the **Permissions** section, but you can view them via search. To do this, open the extended search in the **Permissions** section and select **Revoked** for the **State** parameter.

Permission Suspending

This feature allows you to temporarily disable the use of a permission.

When suspending a permission, remember that users will lose access immediately, not after they disconnect from the resource themselves.

> ⚠ **CAUTION**
>
> If the permission is suspended, the session will be terminated.

Suspending from the permission list | **Suspending from the permission profile**

1. Open the **Permissions** section.
2. Select the desired permission.
3. Click **Suspend**.

Permission Reactivating

This feature allows you to return a permission to an active state.

Reactivating from the permission list | **Reactivating from the permission profile**

1. Open the **Permissions** section.
2. Select the desired permission.
3. Click **Reactivate**.

Bulk Operations for Permissions

Permission Revocation

This feature allows you to revoke permissions that are no longer required.

> ⚠ **CAUTION**
>
> Revoked permissions cannot be returned to an active state.
>
> If you need to temporarily disable the use of a permission, suspend it.

When revoking a permission, remember that users will lose access immediately, not after they disconnect from the resource themselves.

> ⚠ **CAUTION**
>
> If the permission is revoked, the session will be terminated.

1. Open the **Permissions** section.
2. Select one or more permissions.
3. Click **Revoke**.

Revoked permissions no longer appear in the **Permissions** section, but you can view them via search. To do this, open the extended search in the **Permissions** section and select **Revoked** for the **State** parameter.

Permission Suspending

This feature allows you to temporarily disable the use of a permission.

When suspending a permission, remember that users will lose access immediately, not after they disconnect from the resource themselves.

> ⚠ **CAUTION**
>
> If the permission is revoked, the session will be terminated.

1. Open the **Permissions** section.
2. Select one or more permissions.
3. Click **Suspend**.

Permission Reactivating

This feature allows you to return a permission to an active state.

1. Open the **Permissions** section.
2. Select one or more permissions.
3. Click **Reactivate**.

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

The section is intended to search and view active and finished sessions.

By default, the page displays 15 sessions.

> **INFO**
>
> You can change the default number of sessions on a page in the configuration file.

At the bottom of the page there is a paginator to view the remaining sessions.

Next to the paginator there is a switch **Show by: 15 30 60 100** to see more sessions on a page and not switch between pages too often.

If there are fewer than 15 sessions, they are placed on one page and **Show by** switch with paginator are not displayed.

Session Search

The search allows you to display only those sessions 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

You can enter one or several words into the search bar. Words can be written in whole or in part (3 or more letters).

Example

To find a session with the reason **Program update approved by the manager** you need to enter any of the words: **Prog**, **upd**, **appr**, **manag**.

> ⚠ **CAUTION**
>
> You can't enter the trailing substring of the word to the search bar. If you enter the **date** (the trailing substring of the word **update**), this session will not be found.

You can search for a session using two words, e.g. **Prog upd**, **upd appr**, **appr manag**.

> ⚠ **CAUTION**
>
> The words in the search query must be in the same order as in the reason for opening the session. If you enter the **upd prog**, the session will not be found, because these words follow in the opposite direction in the reason for opening the session.
>
> The words in the search query must match the words that were next to each other in the reason for opening the session. You cannot enter words that have other words between them in the reason for opening the session. If you enter the **prog manag**, the session will not be found, because there are some other words between these words in the reason for opening the session.

▼ States and reasons of session termination

State	Reason
Terminated due to error	• Lost connection with PAM Gateway • An error occurred during the session • SSH key fingerprint mismatch detected
Terminated according to PAM rules	• Maximum session duration reached • Permission has been revoked • Permission has been suspended • Access Schedule or Permission Period Limit reached • User has been blocked • User has been removed • User has terminated the session • Absence of user activity • Session request timeout has expired

State	Reason
	• The session has not been opened by PAM Gateway • Session text log change detected
Terminated by administrator	• Administrator has terminated the session • Administrator rejected the session request
Terminated by user	User has terminated the session
Interrupting	—
Active	—
Not initialized	—

Extended Search

You can search by one or several criteria. If you select several criteria, sessions that meet all of the listed criteria will be displayed.

Example

If you select **john.smith@company.demo** in the **User** field and **SSH** in the **Connection Type** field, then only sessions of this user with this connection type will be displayed.

> ⚠ **CAUTION**
>
> Only one value can be selected in each field. You will not be able to display the sessions of the users **john.smith@company.demo** and **james.smith@company.demo** by one extended search query. You can do this using a text search for the query **smith**.

Dumping the Session Log to a File

Session log can be unloaded into two types of files: CSV and XSLX. To download the log, click on the corresponding button.

The report is generated in the form of a table with columns: "User", "Account name", "Resource", "Duration", "Connection type", "Started at", "Finished at", "Status".

Only the last 10,000 records are dumped.

Session Page

The following data is displayed for each session:

- **User** — the user of the Active Directory that initiated the session.
- **Account** — an account that is used to open an RDP, SSH, or web session.
- **Resource** — a resource on which RDP, SSH or web-session was opened on behalf of the account.
- **Connection address** — resource IP address.
- **Reason** — is the reason for connecting to the resource.
- **Duration** — the duration of the session in hours, minutes, and seconds.
- **Connection type** — the type of connection to the resource that is used by local or domain accounts to open a session.
- **User's IP** — The IP address from which the user connects to PAM Gateway, SSH proxy or RDP Proxy.
- **Connected to PAM** — the date and time the user connected to Axidian Privilege.
- **Opened on resource** — date and time of session opening on the resource.
- **Finished** — the date and time of closing the session.
- **State** — the current state of the session.
- **Description** — the description of the permission specified at the stage of creation.
- **Created at** — the date and time the permission was created.
- **Created by** — Axidian Privilege Administrator Account.
- **Confirmation time** — the date and time the session request was confirmed.
- **Confirmed by** — Axidian Privilege administrator who confirmed the session request.

Session Operations

Aborting a Session

The function allows you to forcibly terminate the session.

- Click **Abort** on the active session profile

Session Refresh

The function allows you to manually refresh the text log, screenshots and files transferred to the server.

- Click **Refresh** in the profile of the active session

Video

Video logging is available for RDP sessions, SSH sessions that are opened through the Axidian Privilege Gateway and for sessions of client applications.

Viewing Streaming Video

- Open the **Videos** section in the active session profile

View / Download Final Video

- Open the **Videos** section in the profile of the finished or aborted session
- Play the video or click **Download all**

Text Log

For RDP sessions and SSH sessions that are opened via Axidian Privilege Gateway or Axidian Privilege SSHProxy, a text log is available.

View / Search / Download Text Log

- Open the **Text Log** section in the finished or aborted session profile

> **NOTE**
>
> 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. Complete I/O is logged in SSH sessions.

- Enter a value in the search fields or click **Download**

Screenshots

For RDP sessions, SSH sessions that are opened through the Axidian Privilege Gateway and for client application sessions.

View / Download Screenshots

- Open the **Screenshots** section of the profile for an active, ended or interrupted session
- Open the screenshot or click **Download all**

Transferred to the Server Files

In RDP sessions, interception and shadow copying are available for files transferred from mapped drives to a resource.

Also here you will find files that were transferred using SCP/SFTP protocols.

View / Download Transferred Files

- Open the **Transferred to the server files** section in the profile of an active, completed or interrupted session
- Follow the link to download the transferred files

Events

The section contains all Axidian Privilege events.

Event Search

Quick Search **Extended Search**

Enter the **Event code**, **Component** or **Initiator name** in whole or in part.

Dumping the Event Log to a File

Events can be unloaded into two types of files: CSV and XSLX. To download the log, click on the corresponding button.

The report is generated in the form of a table with columns: "Level", "Time Created", "Code", "Event", "Description", "Component", "Initiator".

Only the last 10,000 records are dumped.

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.
    i. Open the **Distribution groups** section, click the **Add** button, enter a name and description for the recipient group, click **Save**
    ii. 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 log rotation start time	At this time Axidian Privilege will start session log 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:

Option	Description
	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.
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

Option	Description
RDCB address	IP address or DNS name of Remote Desktop Connection Broker
RDCB collection name	Remote Desktop Connection Broker collection name for Axidian Privilege Gateway
Use RDGW	Check it for connecting to Axidian Privilege Gateway with Remote Desktop Gateway
RDGW address	Remote Desktop Gateway address for Axidian Privilege Gateway
Gateway RDP file parameters	These parameters will be added to RDP connection settings for Axidian Privilege Gateway. They will replace old ones

RDP Proxy

The **RDP Proxy address** parameter specifies an IP address or DNS, and optionally a port.

PostgreSQLProxy

The **PostgreSQLProxy address** parameter specifies an IP address or DNS, and optionally a port.

SSH connection settings

Option	Description
SSH Proxy address	IP or DNS, port (required) Default port: 2222
Authentication of resources using SSH server keys	Selected SSH server key fingerprint adding type. For more information, see the **Types of Adding Fingerprints** section.

Syslog

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 standart 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.

Password Requirements for Internal Users

Option	Description
Password Validity Period	Minimum value: 0—no restrictions. Default value: 45 days. Maximum value: 999 days.
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: ~!@#$%^&*()_-+={}|[] \:;"'<>,.?/

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.

User Connection

> ⚠ **CAUTION**
>
> **Manage User Connections** privileges are required to work with user connections. The following privileges are required:
>
> - UserConnectionType.Create
> - UserConnectionType.Read
> - UserConnectionType.Update

- UserConnectionType.Delete

Axidian Privilege has the following built-in user connection types:

- RDP
- SSH
- Telnet
- PostgreSQL

Built-in types cannot be changed or deleted.

It is also possible to add custom user connection types.

Adding Custom User Connection Types

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.

Service Connection

> ⚠ **CAUTION**
>
> **Manage Service Connection Types** privileges are required to work with service connections. The following privileges are required:
>
> - 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 | **Edit name or description**

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** and/or **Description**.
6. 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_3.2\axidian-pam-tools\ssh-templates*.

▼ SSH connector templates included in Axidian Privilege distribution

- Alt
- Astra
- CentOS
- Debian
- FreeBSD
- Gentoo

- Oracle
- RedOS
- 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_3.2\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 magnifying-glass-search-icon.

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

Getting

1. Copy the value from the **Installation ID** field.
2. Send this value to technical support and ask them to generate a license file.
3. Wait for a response from technical support with a license file in the *PAM_yyyy.mm.dd.lic* format.

Adding

Click **Add** and select a license file.

Removing

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 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 **Linux**

   Adding the path to CCT to the environment variable

   ```
   "New-Alias cct <path to CCT>\Pam.Tools.ConnectorCreationTool.exe" | Add-Content $PROFILE
   ```

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 **Linux**

Example

```
<path to CCT>\Pam.Tools.ConnectorCreationTool.exe new -t ps1 -p
C:\Users\user\documents\folder1\
```

Parameters of the command new

Parameter	Required	Description
-v, --verbose	—	Enable display of additional logs.
-p, --path `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 `type`	—	Script type. Possible values: sh, ps1. • 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 **Linux**

Example

```
<path to CCT>\Pam.Tools.ConnectorCreationTool.exe pack -p
C:\Users\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`	—	Path to the connector.

Parameter	Required	Description
-n, --name `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 **Linux**

Example

```
<path to CCT>\Pam.Tools.ConnectorCreationTool.exe hash -p
C:\Users\user\documents\folder1\
```

Parameters of the command hash

Parameter	Required	Description
-v, --verbose	—	Enable display of additional logs.
-p, --path `path`	Yes	Path to the connector (ZIP archive).
-h, --help	—	Usage information and help.

run

Launches the connector, executes the connector script in the specified directory.

Windows **Linux**

Example
`<path to CCT>\Pam.Tools.ConnectorCreationTool.exe run test_connection -p C:\Users\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 `address`	Yes	DNS or IP of the connector.
--port `port`	—	Connector port.
-sa, --service-account `account`	—	Service account name.
-sp, --service-account-password `password`	—	Service account password.
-skp, --service-account-key-path `key-path`	—	service account key path.
-slt, --service-account-location-type `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.

Command	Description
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

AAPM is a set of methods and tools for automating getting passwords and SSH keys (credentials) of accounts by applications.

> ⚠ **CAUTION**
>
> You must have AAPM licenses for using Applications

To add an Applications to Axidian Privilege follow the next steps:

1. Open the **Applications** section in **MC**.
2. Click the button **Add**.

Applications Setting:

In the **Applications** section you can:

- Set the application name, description, and configure the authentication type.
- Add application administrators. Administrators can view the application password in UC.
- Add **permissions**. To do so, do the following steps:
  - Click the button **Add permissions.**
  - Select organizational unit
  - Select the account you want to receive a password from.
  - Configure the remaining settings
  - Click the button **Create**.
- Reset password. To do this, click on the button **Reset password**.
- Remove application. To do this, click on the button **Remove**.
- View granted permissions and the events that occurred in the Axidian Privilege system for this application.

Applications Authentication:

Application authenticate to the IDP and receive a token.

Possibilities to authenticate applications:

1. Static password — set automatically when you create the application. Axidian Privilege administrator can **reset password** using **MC**, but cannot see the password. The Axidian Privilege user who is an administrator of the specific application, can view the password of this application in **UC**.
2. IP address — optional parameter. The IDP verifies that the token request came from the specified IP address. Set by the Axidian Privilege administrator in **MC**.

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: *..PAM_3.2\axidian-pam-tools\dump\Pam.Tools.Dump.exe*.

Editing the Configuration File

At first, Open the utility config file *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, PostgreSQL Pro
- `ConnectionStrings`—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

```
"ConnectionString": "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 insta
- `Database`—database name
- `Username`—database connection account
- `Password`—account's password
- other options available, see documentation for Npgsql connection string

```
"ConnectionString": "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 choosen 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 Proxy

In Axidian Privilege 3.0, a new component has appeared—PostgreSQL Proxy. Now all SQL sessions are initiated via this component. This feature allows administrators to read text logs, which contain all SQL queries executed by a user. This provides greater control over sessions and simplifies incident investigation.

DBMS Client Configuration

DBMS clients often have a specific behavior of their work: after connecting to the DB server, a separate session is opened to execute SQL queries. In this case, several sessions are also created in PAM, which can cause inconvenience when viewing text logs.

To run SQL queries in the same session as the connection to the DB server, you need to configure the DBMS client. Here is the information of how to perform such configuration using the DBeaver client as an example.

1. Open DBeaver.
2. On the left side of the screen, in the **Database Navigator** window, find the required server in the list of available connections, left-click on it and press F4 on the keyboard.
3. In the window that opens, go to the **Metadata** tab, check the **Datasource <servername> settings** flag.
4. For the **Open separate connection for metadata read** option, select the **Never** value from the drop-down list.
5. Go to the **SQL Editor** tab.
6. For the **Open separate connection for each editor** option, select the **Never** value from the drop-down list.
7. Save changes by clicking **OK**.
8. Repeat all the listed steps for all of your database servers.

Specifying the PostgreSQL Proxy Address in PAM

1. Open Axidian Privilege Management Console.
2. Go to **Configuration** → **System settings**.
3. In the **PostgreSQL Proxy** section, fill in the **PostgreSQL Proxy Address** field.

Opening a Session via PostgreSQL Proxy

This information is proposed in the user manual, in the section Connecting to a Resource via PostgreSQL Proxy.

Viewing Text Logs of SQL Sessions

To view text logs of a session opened via PostgreSQL Proxy:

1. Open Axidian Privilege Management Console.
2. Open the **Active sessions** section.
3. Select the desired session.
4. Click **Text Log**.

> ⓘ **INFO**
>
> Please note that different SQL clients may save the text of SQL queries differently. For example, psql doesn't include comments of SQL queries, while pgAdmin includes them.

The text log displayed in the session profile is not updated automatically. To get an up-to-date text log, you need to periodically click **Refresh**.

Text logs does not save SQL query results.

The text log contains only outgoing SQL queries (client → server). Incoming SQL queries (server → client) are not included.

Limitations

- Two-factor authentication is supported only for installations with RADIUS authentication, where the second factor is the confirmation of the request in the application. For installations with authentication via PAM, the **Use two-factor authentication** parameter will be ignored, i.e. the second factor will not be requested, the connection will open without it.
- Administrator confirmation of session opening is not supported. Disable the **Start of the session must be confirmed by Axidian Privilege administrator** option in the **Policies** → **Sessions** section, otherwise it will be impossible to open a SQL session.

- Specifying the reason for opening a session is partially supported. If the **User must specify the connection reason** setting is enabled in the session policy, users will be required to enter a reason in the same field as the account name. For more information, see Connecting to a Resource via PostgreSQL Proxy.

User Console

2 items

Connection to the Resource

2 items

Additional Utilities

3 items

Authentication in SSH Proxy via SSH key

Authentication in SSH Proxy via SSH key

User Console

Access to resources is performed via the user console. Available at the following URL:

- **Windows:** https://pam.domain.local/uc
- **Linux:** https://pam.domain.local/uc

> ⓘ **INFO**
>
> The monitor screen resolution must be at least 1280 pixels wide, otherwise the elements of the user console interface will not be displayed correctly.

Register Authenticator

To work with the user console, you must register the authenticator. Log in to the console, if the user does not have an authenticator, then he will be redirected to IDP to register him.

After successful registration, you will be redirected to the user console.

> ⚠ **CAUTION**
>
> After exceeding the number of failed OTP access attempts allowed the user will be temporarily blocked (10 minutes by default).
>
> Number of failed OTP access attempts allowed and Lockout duration are determined by the PAM administrator in the system settings section.
>
> For urgent unblocking, the PAM Administrator needs to reset the authenticator to the blocked user.

Login

1. Open the user console.
2. Enter login. Examples of login in different formats:
    - 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 factor of authentication.

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 user 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 user console.
2. In the upper right corner, click on login.
3. In the drop-down list, click **Exit** and confirm the action.

Operations on Resources

This section is intended for working with resources.

Personal Resource Folder

To create a personal folder:

1. Go to the **Resources** section, click  .
2. Enter a new folder name.
3. Click **Save**.

To edit a folder name:

1. Go to the **Resources** section.
2. Select a folder and click  .
3. Enter a new folder name.
4. Click **Save**.

To remove a folder:

1. Go to the **Resources** section.
2. Select a folder and click  .
3. Confirm removing of the folder.

To add resources to a folder:

1. Open the **Resources** section and click **All Resources** or **Resources without a folder**.
2. Select the resources to be moved to the folder.
3. Click **Move**.
4. Select a folder.
5. Click **Save**.

> **INFO**

Adding ad hoc resources to the folders is not supported.

Search

To search resources:

1. Open the **Resources** section.
2. Select a folder or click **All Resources** or **Resources without a folder**.
3. In the search bar, enter the value of one of the parameters in whole or in part:
    - resource name;
    - resource type;
    - connection address (DNS or IP);
    - account;
    - tag.

INFO

Ad hoc resources can be found by searching for "adhoc".

Operations on accounts

This section is intended for working with accounts.

Search

The search allows you to display only those accounts that meet the specified criteria.

To find an account, in the **Accounts** section, enter an account name in whole or in part.

Viewing Password and SSH Key

If the user has permission with the **Allow viewing credentials** option enabled, the credentials will be available in the **Accounts** section. To view, click **Show credentials**, enter the reason for viewing and confirm your actions.

Changing Password and SSH Key

If the user has permission with the **Allow changing credentials** enabled, then changing the account password will be available in the **Accounts** section.

To change the password, click **Change password**, enter a new password, enter a reason, and confirm your actions.

RDP, SSH and SQL Connection

Learn about ways to connect to resources

SCP/SFTP Connection to the Resource

3 items

RDP, SSH and SQL Connection

Available permissions to access resources are displayed in the user console.

Sorting is available for each column except the **Tags** column. When entering characters in the search field, matches will be displayed for all columns.

If the user has access to ad hoc resources, they will be displayed at the top of the list.

Connection to a Resource via RDP

1. In the user console, click **Download RDP file** to the right of the permission.

   By default, resources that support RDP and SSH connectivity have the **Copy SSH command** button displayed. To download RDP file, click  , and then **Download RDP file**.

2. Run the RDP file to access the resource.
3. Authenticate.
4. Optionally specify local drives to use in the remote session.

> **INFO**
>
> The downloaded RDP file can be reused for further connections.

Connection to the Access 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.

Connection to the SSH Proxy

You can connect to the SSH Proxy from the command line or by using any SSH client.

Command line | PuTTY | MobaXterm | SecureCRT

1. Open the console utility.

2. Enter the connection string of the SSH Proxy or the load balancer. Можно использовать IP-адрес или 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.

Template of SSH Proxy Connection Command

```
ssh <IP address or DNS>
```

Example of SSH Proxy Connection Command

```
ssh axidianproxy
```

Optionally specify the user login and port.

Template of SSH Proxy Connection Command

```
ssh <login>@<IP address or DNS> -p <port>
```

Example of SSH Proxy Connection Command

```
ssh user@axidianproxy -p 2222
```

Optionally specify the path to the private key.

Template of SSH Proxy Connection Command

```
ssh <login>@<IP address or DNS> -p <port> -i <path to the private key>
```

Example of SSH Proxy Connection Command

```
ssh user@axidianproxy -p 2222 -i "C:\Users\user\.ssh\id_ed25519"
```

3. Enter the password. If SSH key authentication is configured, skip this step.
4. Enter OTP.
5. Select a resource and connect.

Connection to a Resource via SSH

Command Line | **PuTTY** | **MobaXterm** | **SecureCRT**

Connection by command from the user console

1. In the user console, to the right of the permission to the SSH resource, click **Copy SSH command**.
2. Run the copied command in the terminal.
3. Enter your password and OTP.

Connection by command with additional parameters

You can write an SSH command manually using the template below.

1. Write an SSH command using the template below.
2. Run the command in the terminal.
3. Enter your password and OTP.

Template of SSH command

```
ssh [user-name]#[resource]#[account-name]#[reason]@[proxy-address]
```

- `user-name` — user name.
- `resource` — IP address or DNS.
- `account-name` — name of the privileged account.
- `reason` — text of the connection reason. If the reason contains spaces, specify it in quotation marks.
- `proxy-address` — IP address or DNS of the SSH Proxy server.

You can omit any parameter except `proxy-address`. In this case, SSH Proxy will request these parameters separately.

Example of SSH command

```
ssh ivan.ivanov#ubuntu#webmaster#"system configuration"@pam
```

Connection to a Resource via the PostgreSQL Proxy

> ⚠ **CAUTION**
>
> A special license is required to connect to the PostgreSQL resource.

GUI DBMS Client | **Console client of DBMS Psql**

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 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.

Command Line

Connection via SCP, SFTP, PSCP, PSFTP

WinSCP

Connection via WinSCP

FileZilla

Connection via FileZilla

Command Line

SCP

> **NOTE**
>
> Devices running on 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:

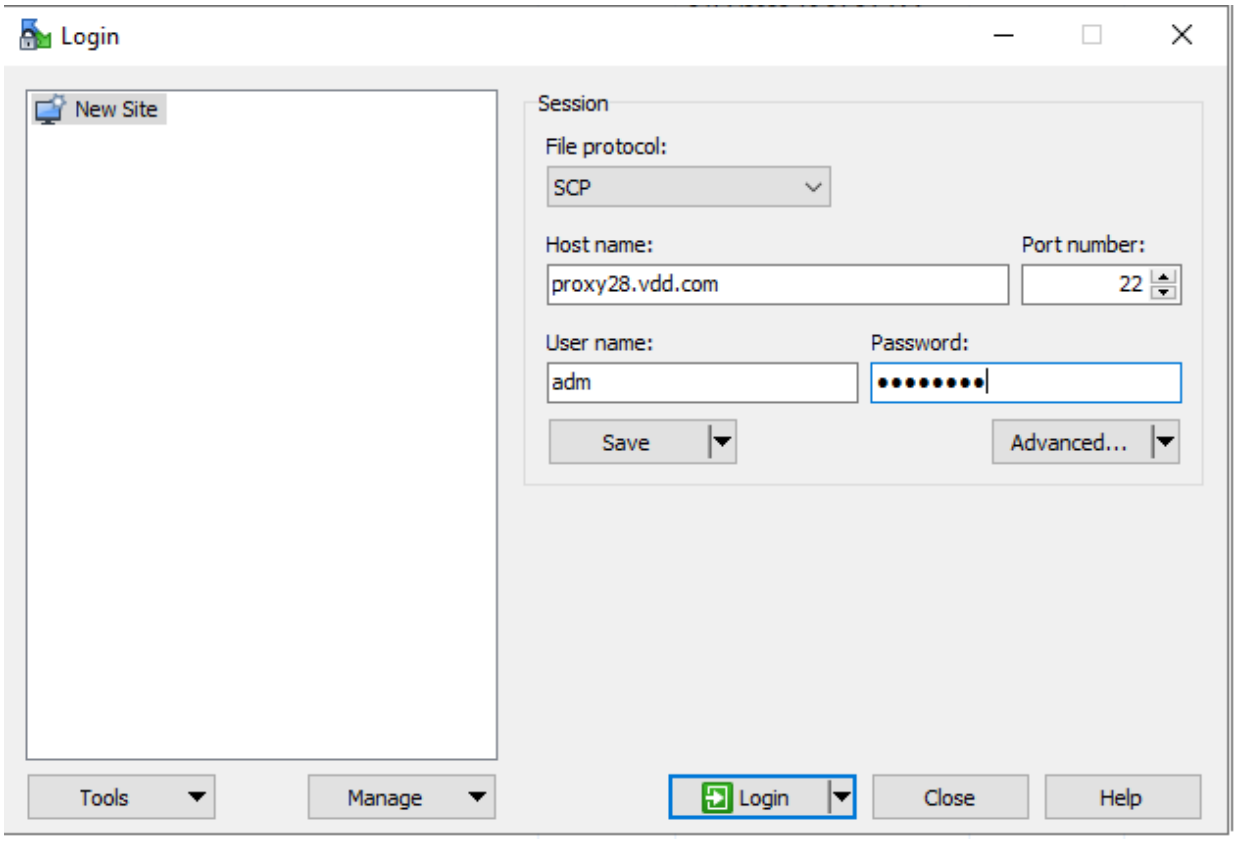
```
put -r C:\temp\configs\ /tmp/configs
put -r path_to_local_files path_to_files_on_resource
```

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.

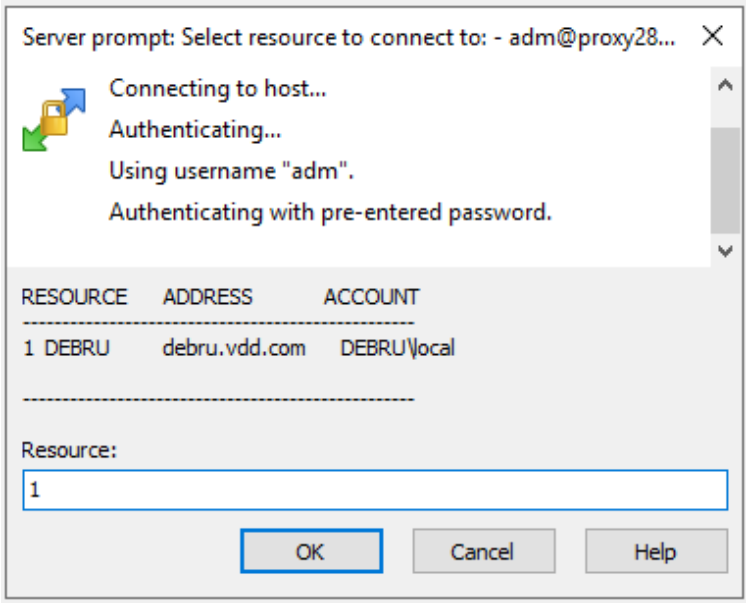
WinSCP

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 resource to connection.

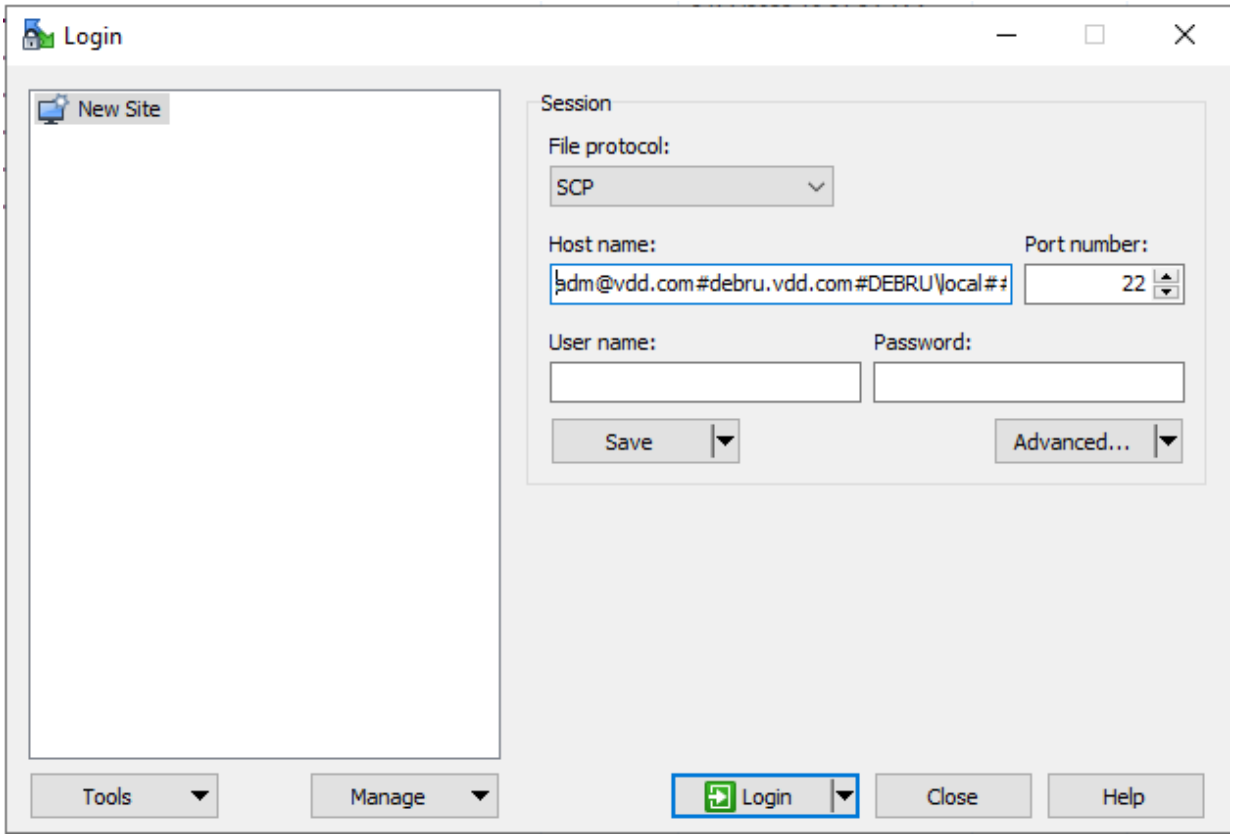


Direct Connection to the Resource

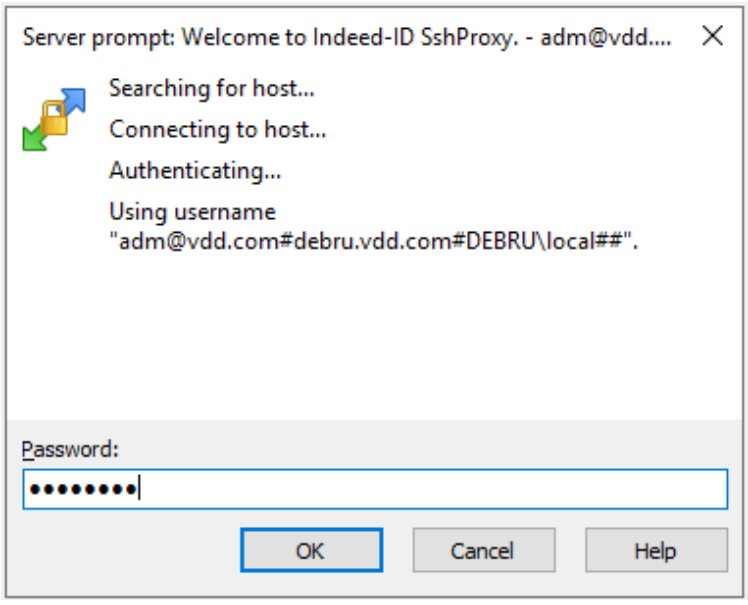
1. Open **User Console** and copy connection string to the resource.

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 to next 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 to **Connect** button.

> ⓘ **NOTE**
>
> FileZilla does not support TCP connection.

Usage of PamSu

Learn how to run a command if sudo is needed

Usage of AAPM Console Tool

Edit the appsettings.json configuration file to work with AAPM Console Tool

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 AAPM Console Tool

Pam.Tools.Aapm—console utility for retrieval a password or SSH Key accounts by Applications.

Path: *..PAM_3.2\axidian-pam-tools\aapm*

Console Utility Configuration

To configure the console utility, you need to configure **appsettings.json** file:

Section `Auth`:

- `Auth.Username`—application name
- `Auth.Password`—application password. For getting the password go to **UC → Applications → View credentials**.

Section `Endpoints`:

- **CoreUrl** — Core address.
- **IdpUrl** — Idp address.

Configuration Example

```
{
  "Auth": {
    "Username": "MyApplication",
    "Password": "M3YTy;[j;q&*DrZQSl(?B1agm$7uS+",
  },
  "Endpoints": {
    "CoreUrl": "https://debmng.axidian.test/core",
    "IdpUrl": "https://debmng.axidian.test/idp"
  }
```

Usage of Console Utility

Windows

To run the console utility, open the terminal, go to the folder with the utility and execute the command **.\Pam.Tools.Aapm.exe**

Possible Parameters:

```
get-accounts    Get accounts for which the application can view credentials.
get-ssh-key     Gets SSH key for specified account. Passphrase for the key will be written in stdout stream, the key will be saved in the output path
get-password    Gets password for specified account
help            Display more information on a specific command.
version         Display version information.
```

Usage Example:

Input:

```
./Pam.Tools.Aapm.exe get-accounts
./Pam.Tools.Aapm.exe get-password --name AXIDIAN\IPAMADServiceOps
```

Linux

> **NOTE**
>
> Make sure you have dotnet-runtime-8.0 installed.

To run the console utility, open the terminal, go to the folder with the utility:

```
cd PAM_3.2\axidian-pam-tools\aapm\
```

and run the command **dotnet Pam.Tools.Aapm.dll** with chosen argument.

```
dotnet Pam.Tools.Aapm.dll get-accounts
```

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 chose **Connect** menu item) and complete the authentication. You can open multiple connections at the same time.

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

   i. Open the Manage user certificates snap-in, and then open Personal → Certificates.
   ii. Right-click the Certificates folder. Select All Tasks → Request a new certificate.
   iii. Click Next.
   iv. Select a certificate enrollment policy and click Next.
   v. Select a certificate.
   vi. Click Request.

2. Export the certificate.

   ▼ Export Instructions

   i. Open the Manage user certificates snap-in, and then open Personal → Certificates.
   ii. Right-click on the certificate that was generated in the previous step. Select All Tasks → Export.
   iii. In the window that opens, click Next.
   iv. Select the X.509 Files option (.CER) encoded DER.
   v. Select the file location and fill in File Name. Click Next.

vi. 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.

Configuring and Collecting Logs

Learn about logging

Technical Support

Learn how to create a technical support request

Configuring and Collecting Logs

Log Files Location

Log files of all .Net components and utilities are written to text files located in the `logs` folders:

- `/etc/axidian/axidian-privilege/logs/Component_name/`
- `C:\inetpub\wwwroot\Component_name\logs\`
- `C:\Program Files\Axidian\Axidian Privilege\Gateway\ProxyApp\logs\`
- `[axidian-pam-windows\MISC]\utilities folder\logs\`

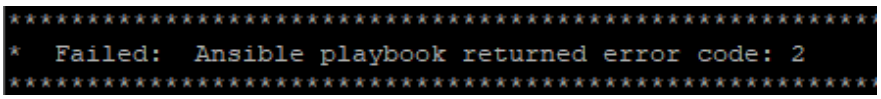
Description of the log files of the components: Core, IDP, LS

File	core	idp	LS	log content
commands.log	+	+		all logs of the commands
queries.log	+	+		all logs of the queries
errors.log	+	+	+	all errors of the Axidian Privilege/LS
jobs.log	+			all logs of the jobs
events.log	+			all logs related to Events
connections.log	+			all logs of service connections
db.log	+	+	+	all logs related to DB access
hangfire.log	+	+	+	all logs from Hangfire
ils.log	+			all logs from LogServer client
full-yyyy-MM-dd.log	+	+	+	all logs of Axidian Privilege/LS with logger name and traceId

File	core	idp	LS	log content
stdout_yyyyMMddHHmmss_xxxx.log	+	+	+	logs with errors from IIS

Installation Script Logging

The installation script run-deploy.sh may fail with an error. In this case, you need to send log files to technical support. Example of a script error:



Log files location: *..PAM_3.2/axidian-pam/logs/*.

By default, the log file contains brief information. To get detailed log output you need to run the script with the `-vvv` option:

```
run-deploy.sh -vvv
```

ProxyApp

Logs are written to the folder: `C:\Program Files\Axidian\Axidian Privilege\Gateway\ProxyApp\logs\shortDate\processId` to separate logs from multiple runs on the same day. It is possible that there are two log files in the folder:

- `ffmpeg.log` — debugging information from ffmpeg
- `Pam.Proxy.App.log` — all other logs

Utilities

All logs are written to the one file. Log file name doesn't contain a date. Log file name contains the name of the utility. For example: `Pam.Tools.Migrator.log`

Native Components Logging

The list of the native components is following:

- MstscAddin
- WindowsAgent
- Pam.Service
- Pam.Putty
- ProcessCreateHook

To enable or to get logs, you can use the Axidian Privilege GetLog utility. Logs are saved to a directory `C:\Windows\System32\LogFiles\Axidian`. Each process has its own separate directory.

nix Components Logging

SSH Proxy

All logs are written to the one file — `${ISODate}.log`.

File location: `/etc/axidian/axidian-privilege/logs/ssh/`

PAMSU

All logs generated by our code are written to the one file — `${ISODate}.log`.
File location: `/opt/Axidian Privilege/pamsu/logs/`.

In addition, it is possible to enable logging of code provided by sudo. This is done via changes to the file `/etc/pamsu.conf.` The rules for setting up and managing are the same as for `sudo`. See `man sudo.conf`.

Configuring Logging

A json file is used for logging configuration (appsettings.json).

Configuration Appsettings.json

File appsettings.json locates at:

- **C:\inetpub\wwwroot\component_name\appsettings.json** — management server Windows.
- **C:\Program Files\Axidian\Axidian Privilege\Gateway\ProxyApp\appsettings.json** — access server Windows.
- **/etc/axidian/axidian-privilege/component_name/appsettings.json** — management or access server Linux.

Section NLog

The **variables** parameter is a section where you can set variables to further configure logging. The number of variables is unlimited. This parameter is optional.

```
"variables":  {
               "minLevel":  "Trace",
               "dbMinLevel":  "Info"
               }
```

> **NOTE**
>
> The value of a variable can be inserted into an attribute value via the `${varname}` syntax.

Each log entry has a level. And each logger is configured to include or ignore certain levels. A common configuration is to specify the minimum level where that level and higher levels are included. For example, if the minimum level is Info, then Info, Warn, Error and Fatal are logged, but Debug and Trace are ignored.

The log levels ordered by severity:

LogLevel	Ordinal	Severity
Trace	0	Most verbose level. Used for development and seldom enabled in production.
Debug	1	Debugging the application behavior from internal events of interest.
Info	2	Information that highlights progress or application lifetime events.
Warn	3	Warnings about validation issues or temporary failures that can be recovered.
Error	4	Errors where functionality has failed or Exception have been caught.
Fatal	5	Most critical level. Application is about to abort.

The common configuration is to specify a minimum level in which this level and higher levels are included. For example, if the minimum level is Info, then Info, Warn, Error and Fatal are registered, but Debug and Trace are ignored.

Section **rules** — controls how LogEvents from the Logger-objects are redirected to output targets. Each type of log has its own name, which is not recommended to edit.

```
"Rules": {
"03_Hangfire": {
        "logger": "Hangfire.*",
        "minLevel": "Info",
        "writeTo": "hangfireFile",
        "final": true
      },
"20_Errors":  {
        "logger":  "*",
        "minLevel":  "Error",
        "writeTo":  "errorsFile"
              },
"40_Commands": {
        "logger": "Idp.Application.*Command",
        "minLevel": "${minLevel}",
        "writeTo": "commandsFile",
        "Enabled": false
      },
}
```

For each type of log, you can specify the following tags:

logger — logger name — this is usually the name of the element associated with the log line in the code (class name). May contain wildcard characters (* and ?). Thus, the rule name '*' corresponds to any logger name, and 'Common*' corresponds to all loggers whose names begin with 'Common'. It is not recommended to edit this parameter.

LogLevel — logging levels, it is possible to specify several levels at once:

- **minlevel** — minimum level to log.
- **maxlevel** — maximum level to log.
- **level** — single level to log.
- **levels** — comma separated list of levels to log.

writeTo — comma separated list of targets to write to.

final — no rules are processed after a final rule matches.

enabled — set to false to disable the rule without deleting it.

- parameter **targets** – defines log targets/outputs (optional parameter)
- parameter **extensions** – loads NLog extensions from the *.dll file (optional parameter)
- parameter **include** – includes external configuration file (optional parameter)

Configuring NLog.json file

Each component that records logs has a file NLog.json, which specifies where and how logs will be recorded. For Windows NLog.json file locates in the same path as the appsettings file.json and is configured for each component separately.

Section NLog

Parameter **variables** — sets the value of a configuration variable. The number of variables is unlimited. (optional parameter).

Section Targets

Each type of log has its own name, which is not recommended to edit.

- **type** — The type of the saved log. Editing is not recommended.
- **layout** — The text to be displayed. Editing is not recommended.
- **fileName** — Recording logs directory.
- **archiveFileName** — Storing directory for filled logs.
- **archiveAboveSize** — Maximum size of log file, specified in bytes.
- **archiveNumbering** — Method of numbering file archives.
- **maxArchiveFiles** — The number of stored filled logs . Old filled logs are deleted when new ones appear.

> ⓘ **NOTE**
>
> The directory for recording and storing logs is specified in one of two formats "**C:\Logs\logs.log**" or "**C:\\LogsArch\\logs.{#####}.log**".
> The **{#####}** is specified only in **archiveFileName** parameter. This is necessary for numbering filled logs.

> ⓘ **NOTE**

> If log rotation is enabled, then the directory of the recorded log and the directory of the filled logs must be different.

Example of configuration for errors log:

```
"targets":{
    "errorsFile":  {
        "type": "File",
        "layout": "${loggerLayout}",
        "fileName": "C:\Logs\errors.log",
        "archiveFileName": "C:\\LogsArch\\errors.{#####}.log",
        "archiveAboveSize": 1000000,
        "archiveNumbering": "Sequence",
        "maxArchiveFiles": 2
                    }
}
```

Log rotation is not enabled by default.

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:

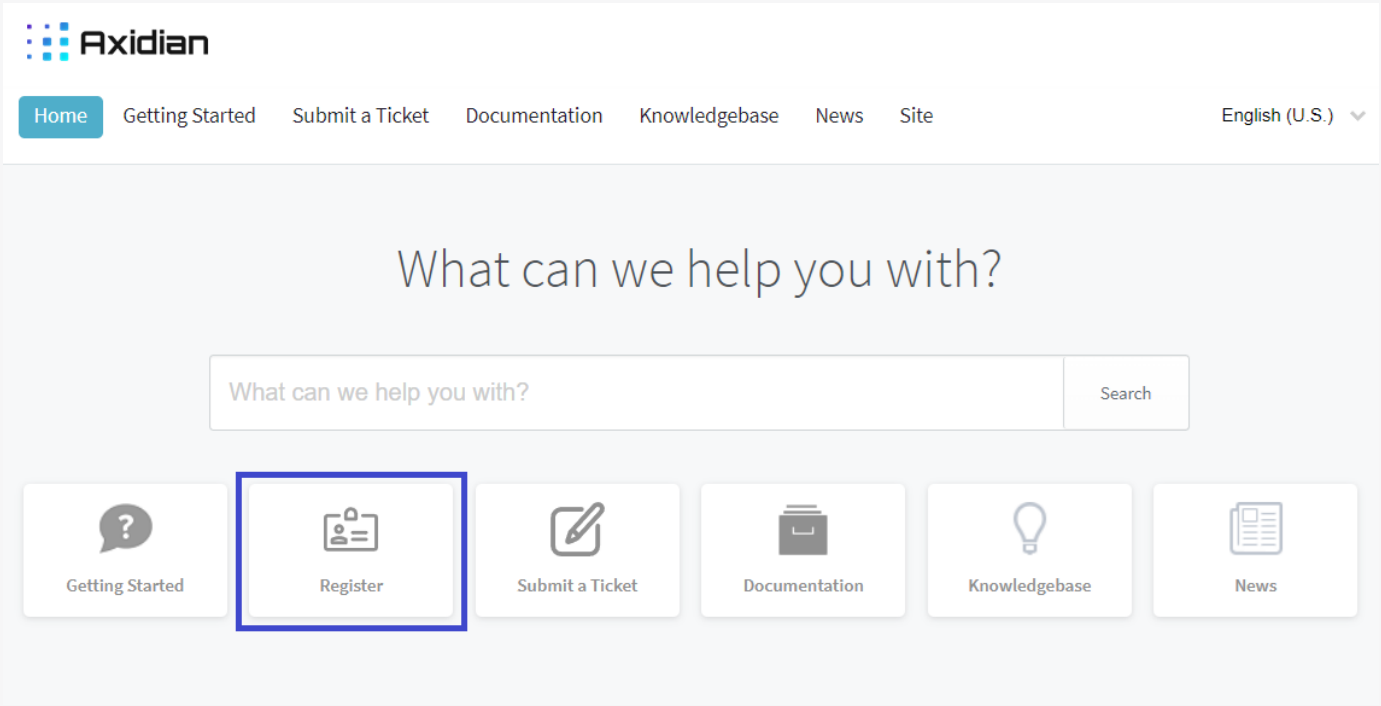
1. Open Technical Support Portal.
2. Enter your email address and password and click **Login**.

▼ 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:

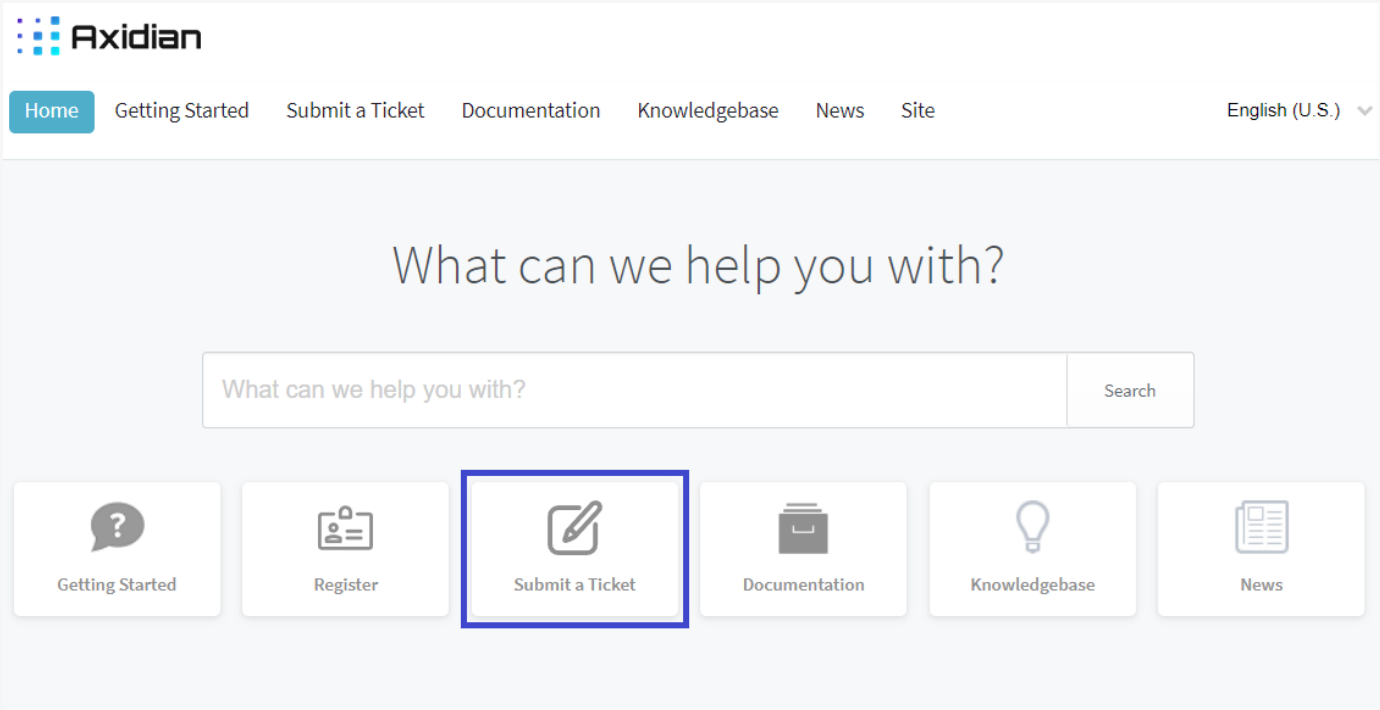
1. Click **Register**.



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**.

Release notes

This section provides a brief description of changes and improvements in the Axidian Privilege by version.

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.