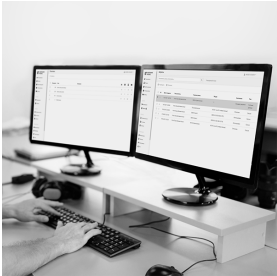


# Documentation of Axidian Privilege 2.10



# Table of contents:

- [Overview](#)
- [Terms](#)
  - [User Directory](#)
  - [Users](#)
  - [Accounts](#)
  - [Resources](#)
  - [Domains](#)
  - [Structure](#)
  - [Data Storage](#)
  - [Service Connection](#)
  - [User Connection](#)
  - [Permissions](#)
  - [Policies](#)
- [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](#)
    - [Axidian Privilege Gateway](#)
    - [Axidian Privilege SSH Proxy](#)
    - [Axidian Privilege RDP Proxy](#)
    - [Axidian Privilege ESSO Agent and Axidian Privilege Admin Pack](#)
  - [Windows Resources](#)
    - [Axidian Privilege Agent](#)
  - [Linux Resources](#)
    - [PAMSU Component](#)
  - [User's Workplace](#)
    - [Axidian Privilege Desktop Console](#)
  - [Simplified on Windows](#)
  - [Simplified on Linux](#)
  - [Basic](#)
  - [Fault Tolerant](#)

- Simplified on Windows
  - Components
    - Management Server / Access Server (RDP/RemoteApp)
    - Access Server (SSH/SCP/SFTP)
  - Work Scenarios
    - User Scenario
    - Administrator Scenario
- Simplified on Linux
  - Components
    - Management Server / Access Server (RDP/SSH/SCP/SFTP)
    - Access Server (RDP/RemoteApp)
  - Work Scenarios
    - User Scenario
    - Administrator Scenario
- Basic
  - Components
    - Management server
    - Access server (RDP/RemoteApp)
    - Access server (RDP/SSH/SCP/SFTP)
  - Work Scenarios
    - User Scenario
    - Administrator Scenario
- Fault Tolerant
  - Components
    - Management Server
    - Access Server (RDP/RemoteApp)
    - Access Server (RDP/SSH/SCP/SFTP)
  - Work Scenarios
    - User Scenario
    - Administrator Scenario
  - Windows Environment
  - Linux Environment
  - DBMS Environment
- Windows Environment
  - Management Server
    - Hardware Requirements
    - Software Requirements
    - Network Connectivity

- Access Server (RDP)
  - Hardware Requirements
  - Software Requirements
  - Network Connectivity
- Linux Environment
  - Management Server
    - Hardware Requirements
    - Software Rquirements
    - Network Connectivity
  - Access Server (SSH)
    - Hardware Requirements
    - Software Requirements
    - Network Connectivity
  - Access Server (RDP)
    - Hardware Requirements
    - Software Requirements
    - Network Connectivity
  - CIS Benchmark Security Settings
- DBMS Environment
  - Supported DBMS
  - Hardware Requirements
  - Software Requirements
  - Network Connectivity
- Licensing
  - Licensing by Users and Resources
    - Issuance of a License
      - User License
      - Resource License
    - Revocation (Release) of a License
      - User License
      - Resource License
    - License Validity Period
  - Licensing by Session
    - Issuance and Release of a License
    - License Validity Period
  - Application to Application Password Management License
    - Issuance and Release of a License
    - License Validity Period

- General Plan of Implementation
  - Preparing the Infrastructure
  - Installation and Configuration of Axidian Privilege Server Components
    - Windows
    - Linux
  - Installation and Configuration of Axidian Privilege Client Components
  - Test Run of Axidian Privilege
  - Final Step
  - Active Directory Accounts
  - Certificates
  - Databases
  - Media Storage
  - Servers
  - IIS Setup
- Active Directory Accounts
  - Account to Use with User Directory
  - Account for Service Operations in Active Directory
- Certificates
  - Preparation
    - Windows
    - Linux
  - Certificates Export
    - Windows
    - Linux
- Databases
  - Database Creation
  - Creating a Service Account to Work with Data Storage
- Media Storage
  - File Storage Account
  - Creating and Configuring File Storage
- Servers
- IIS Setup
  - Simplified Installation on Linux OS
  - Configuration Files Setup
  - Windows Server OS
  - Linux OS
  - 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](#)
- [Simplified Installation on Linux OS](#)
  - [Preparation](#)
  - [Certificates](#)
    - [Certificate of Certification Authority](#)
    - [Server Certificate](#)
  - [vars](#)
  - [Flat Configuration File](#)
  - [Installation](#)
  - [Web-Wizard Launch](#)
  - [Configuration Files Setup](#)
- [Web-Wizard Launch](#)
- [Configuration Files Setup](#)
  - [Management Server \(Windows\)](#)
  - [Access Server \(RDP\RemoteApp\)](#)
  - [Access Server \(SSH Proxy\)](#)
- [Management Server \(Windows\)](#)
- [Access Server \(RDP\RemoteApp\)](#)
- [Access Server \(SSH Proxy\)](#)
  - [Inventory](#)
  - [Configuration Files](#)
  - [Installation](#)
  - [Certification Authority Certificate](#)
  - [Installation without Balancing](#)
  - [Installation with Balancing](#)
  - [Access Server \(RDP/RemoteApp\)](#)
- [Installation without Balancing](#)
  - [Inventory](#)
  - [Configuration Files](#)
  - [Certificates](#)
    - [Certification Authority Certificate](#)
    - [Server Certificates](#)
  - [vars](#)
  - [Installation](#)
  - [Components Restarting](#)

- Management Server
- Access Server
- Installation with Balancing
  - Inventory
  - Configuration Files
  - Certificates
    - Certification Authority Certificate
    - Server Certificates
  - vars
  - Installation
  - Components Restarting
    - Management Server
    - Access Server
- Access Server (RDP/RemoteApp)
- Additional Components Setup
  - PamSu
    - Installation
    - Configuration
  - Axidian Privilege Agent
  - Axidian Privilege Desktop Console
    - Configuring for Domain Computers
    - Configuring for Computers to which Domain Policies are not Applied
  - Writing Events to Syslog
- RADIUS Configuring
  - Section IdentitySettings
  - Section Radius
- RDP File Signature Configuring
  - Enabling RDP File Signing
    - Description of the Parameters of the Rdp Section of Configuration File
  - Certificate Setup
    - Windows with Fingerprint
    - Linux with Key Importing in PFX Format
- TOTP Second Factor via Email Setup
- Enabling Restart of Proxy Service Containers
  - Enabling Restart in the Configuration File
  - Additional Settings
  - Restarting the Access Server
  - Example of Restarting the RDP Proxy Component

- Example of Restarting the SSH Proxy Component
- Integration with User Directories
  - Setting up Integration with Active Directory
    - Setting Up a Search for Users Belonging to a Security Group
  - Setting Up Integration with FreeIPA or AldPro
  - Setting Up Integration with OpenLDAP
  - Setting Up an Integration with Multiple User Directories
- Backup Accounts
- Security of Passwords and Secret Keys
- Process Filtering and File Security
- Session Logs Encryption
- Access Server Security Policy
- Access Server Security Settings
- Changing the Encryption Key of the PAM Database
- Backup Accounts
- Security of Passwords and Secret Keys
  - Axiom Privilege Components Protection
  - Encryption Mechanism Details
- Process Filtering and File Security
  - Preventing Users from Starting Unwanted Processes
  - Protecting Vulnerable Files
- Session Logs Encryption
- Access Server Security Policy
  - User Rights Assignment Section
  - Security Options Section
    - Accounts
    - Audit
    - Devices
    - Interactive Logon
    - Microsoft Network Client
    - Network Access
    - Network Security
    - Shutdown
    - System Settings
    - User Account Control
    - Other
- 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
    - Account for service operations in Active Directory
  - Service Operations for \*nix Resources

- Creating and Configuring a Service Account
- Configuring a Group of Privileged Accounts
- Administrator console
- First Launch
- Policy Setup
- Section Reference
- Dumping Passwords
- Administrator console
  - Authentication
- First Launch
  - Adding the Domain
  - Add and Take Control of Accounts
  - Adding Non-Domain Resources
- Policy Setup
  - Policies
    - Adding New Policy
      - General Information
      - Sections
      - Scope
    - Creating a Copy of the Policy
    - Removing Policy
    - Changing the Priority of a Policy
  - Policy Sections
    - Accounts
    - Sessions
    - Gateway and SSH Proxy
    - RDP
    - SSH
      - Privilege Elevation
      - Allowed and Forbidden Commands
      - Data Transfer
- Users
- User Groups
- Resources
- Resource Groups
- Accounts
- Domains
- Structure

- [Permissions](#)
- [Action Requests](#)
- [Active Sessions](#)
- [All Sessions](#)
- [Events](#)
- [Notifications](#)
- [Configuration](#)
- [Roles](#)
- [Applications](#)
- [Users](#)
  - [Search](#)
    - [Quick Search](#)
    - [Extended Search](#)
  - [User Profile](#)
    - [Permissions](#)
    - [Sessions](#)
    - [Authenticators](#)
    - [Events](#)
  - [Resetting User Authenticator](#)
  - [Disabling User Authenticator](#)
  - [Blocking a User](#)
  - [Unblocking a User](#)
  - [Setting a Policy for a User](#)
- [User Groups](#)
  - [Creating a User Group in the Axidian Privilege](#)
  - [Adding a User Group from Active Directory](#)
  - [Managing a User Group](#)
    - [Adding Users to a Group](#)
    - [Adding Permission to a User Group](#)
    - [Viewing Permissions You Create](#)
    - [Viewing Information about the Current Sessions within the User Group and Events of the Axidian Privilege](#)
    - [Synchronizing a User Group with a Directory](#)
    - [Setting a Policy for a User Group](#)
- [Resources](#)
  - [Resource Search](#)
    - [Quick Search](#)
    - [Extended Search](#)

- Resource Page
  - User Connection
  - Permissions
  - Local Accounts
  - Resource Groups
  - Sessions
  - Events
- Setting a Policy for a Resource
- Adding a Resource
  - Manual Add
  - Add from File
  - User Connection Setup
    - RDP Connection Setup
    - SSH Connection Setup
  - User Connection Setup
    - Web Session Setup
    - DBMS Connection Setup
  - Service Connection Setup
- Setting Up a Service Connection for Resources
  - Adding Accounts
  - Selecting and Setting Up a Service Connection
    - Setting Up a Service Connection for Windows
      - Selecting a Service Account
    - Setting Up a Service Connection for \*nix
      - Selecting a Service Account
    - Setting Up a Service Connection for MS SQL Server DBMS
      - Selecting a Service Account
    - Setting Up a Service Connection for OracleDB
      - Selecting a Service Account
    - Setting Up a Service Connection for PostgreSQL / PostgreSQL Pro
      - Selecting a Service Account
    - Setting Up a Service Connection for MySQL
      - Selecting a Service Account
      - Setting Up a MySQL Service Account
    - Setting Up a Service Connection for Cisco IOS
      - Selecting a Service Account
    - Setting Up a Service Connection for Inspur BMC
      - Selecting a Service Account

- Resource Operations
  - Resource Editing
  - Adding User Connection
  - Adding an Account
    - Password and SSH Key
      - Password Settings
      - SSH Key Settings
  - Checking the Connection to the Resource
  - Synchronization
  - Block
  - Remove / Rollback a Resource
    - Removing a Resource
    - Rolling Back Resources
- Bulk Operations for Resources
  - Setting up a Service Connection
  - Checking the Connection to the Resource
  - Deleting Resources
  - Set Policy
  - Set Organizational Unit
- Resource Groups
  - Resource Groups Search
    - Quick Search
    - Extended Search
  - Resource Groups Functions
    - Editing a Resource Group
    - Adding Resources
    - Adding Permissions
    - Viewing Sessions
    - Viewing Events
  - Removing Resource Groups
- Accounts
  - Adding an account
  - Account Search
    - Quick Search
    - Extended Search
  - Account Page
    - Permissions
    - Sessions

- Events
- Security Groups
- Setting a Policy for an Account
- Account Operations
  - Account Editing
  - Account Confirmation
  - Password and SSH Key
    - Password Settings
    - SSH Key Settings
    - Rollback Password or SSH Key
    - Verification of Password or SSH Key
    - Password Change
    - SSH Key Change
    - Removing Unmanaged SSH Keys
    - Synchronization
    - Blocking
    - Ignoring
    - Removing an Account
  - Rolling Back an Account
- Bulk Operations for Accounts
  - Confirmation
  - Password or SSH Key Checking
  - Blocking
  - Ignoring
  - Changing Policy
  - Removing
- Domains
  - Domain Search
    - Quick Search
    - Extended Search
  - Domain Page
  - Domain Accounts
  - Resource Containers
  - Privileged Groups
  - Events
  - Setting a Policy for a Domain
- Adding a Domain
- Configuring Service Connection for Domains

- Adding Accounts
- Setting up a Service Connection
- Domain Operations
  - Domain Editing
  - Adding an Account
    - Password Setting
  - Domain Connection Check
  - Import Resources
    - Selection of Containers
    - Import
  - Synchronizing Accounts
    - Selecting Groups of Privileged Accounts
    - Synchronization
  - Remove / Rollback a Domain
    - Removing a Domain
    - Rolling Back Domains
- Bulk Operations for Domains
  - Checking the Connection to the Domains
  - Deleting Domains
- Structure
  - Organizational Unit Types
  - Local Administrator
- Permissions
  - Permission Search
    - Quick Search
    - Extended Search
  - Permission Page
- Creating a Permission
  - Organizational Unit
  - User
  - Resource
  - Account
  - Time Restrictions
  - Additional Permission Options
- Permission Operations
  - Permission Revocation
  - Permission Suspending
  - Permission Reactivating

- Bulk Operations for Permissions
  - [Permission Revocation](#)
  - [Permission Suspending](#)
  - [Permission Reactivating](#)
- Action Requests
  - [Search Action Requests](#)
    - [Quick Search](#)
    - [Extended Search](#)
  - [Action Request Functions](#)
    - [Action Request Confirmation](#)
    - [Action Request Rejection](#)
  - [Request Page](#)
- [Active Sessions](#)
- All Sessions
  - [Session Search](#)
    - [Quick Search](#)
    - [Extended Search](#)
  - [Dumping the Session Log to a File](#)
  - [Session Page](#)
- Session Operations
  - [Aborting a Session](#)
  - [Session Refresh](#)
  - [Video](#)
    - [Viewing Streaming Video](#)
    - [View / Download Final Video](#)
  - [Text Log](#)
    - [View / Search / Download Text Log](#)
  - [Screenshots](#)
    - [View / Download Screenshots](#)
  - [Transferred to the Server Files](#)
    - [View / Download Transferred Files](#)
- [Events](#)
  - [Event Search](#)
  - [Dumping the Event Log to a File](#)
- [Notifications](#)
  - [Presetting](#)
  - [Configuring Notifications](#)
  - [Removing Distribution Groups or Notifications](#)

- Configuration
  - Licenses
    - Add License
    - Removing Licenses
  - System Settings
  - User Connection
    - Adding New Connection Types
  - Service Connection
    - Adding a Service Connection with SSH Type
  - Network Location
    - Adding the Network Location
- Specifying the Length of a Video Segment when Recording an RDP Session
- Roles
  - Presetting
  - Built-in Roles
  - Creating New Roles
  - Adding Users to a Role
  - Removing Roles
- Applications
- Dumping Passwords
  - User Console
  - Access to the Resource
  - Connection via SSH Clients
  - SCP/SFTP Connection to the Resource
  - Personal Resource Folders
  - Executing Commands with Root Privilege
  - Account Operations
  - Usage of AAPM Console Tool
  - Desktop Console
- User Console
  - Register Authenticator
- Access to the Resource
  - Direct Connection to a Resource
  - Connection to the Access Gateway
  - Connection to the SSH Proxy
  - Direct Connection via SSH
  - Connection to an Ad Hoc Resource
  - Setting a Password when Connecting

- End of Session
- Connection via SSH Clients
  - Connecting via Access Gateway
  - Connecting to a Specific Resource
  - Command Line
  - WinSCP
  - FileZilla
- Command Line
  - SCP
  - SFTP
  - PSCP
  - PSFTP
- WinSCP
  - Connecting via Access Gateway
  - Direct Connection to the Resource
- FileZilla
  - SFTP Connection to a Resource
- Personal Resource Folders
  - Creating a Personal Resource Folder
  - Editing Folder Name
  - Deleting a Folder
  - Adding Resources to a Folder
  - Resource Search
- Executing Commands with Root Privilege
- Account Operations
  - Account Search
  - Viewing an Account's Password and SSH Key
  - Changing an Account's Password and SSH Key
- Usage of AAPM Console Tool
  - Console Utility Configuration
    - Usage of Console Utility
- Desktop Console
  - Configuring and Collecting Logs
  - Technical Support
- Configuring and Collecting Logs
  - Log Files Location
    - Installation Script Logging
    - ProxyApp

- [Utilities](#)
- [Native Components Logging](#)
- [nix Components Logging](#)
  - [SSH Proxy](#)
  - [PAMSU](#)
- [Configuring Logging](#)
  - [Configuration Appsettings.json](#)
    - [Section NLog](#)
  - [Configuring NLog.json file](#)
    - [Section NLog](#)
    - [Section Targets](#)
- [Technical Support](#)
- [Release notes](#)
  - [2.10](#)

# Overview

## INFORMATION

New version of the product is available: [Axidian Privilege 3.0](#).

You are now viewing the documentation for version 2.10.

Follow the [link](#) to read the latest documentation.

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

## INFORMATION

New version of the product is available: [Axidian Privilege 3.0](#).

You are now viewing the documentation for version 2.10.

Follow the [link](#) to read the latest documentation.

## 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)
- ALD Pro (PAM 2.10 and higher)

## 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
- PostgreSQL
- MySQL
- OracleDB
- Cisco (IOS XE)
- Inspur BMC (IPMI)

## 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

A resource can have one or more 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.



**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

## INFORMATION

New version of the product is available: [Axidian Privilege 3.0](#).

You are now viewing the documentation for version 2.10.

Follow the [link](#) to read the latest documentation.

## 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 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:

- Keeping track of the names of running processes, active windows 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)

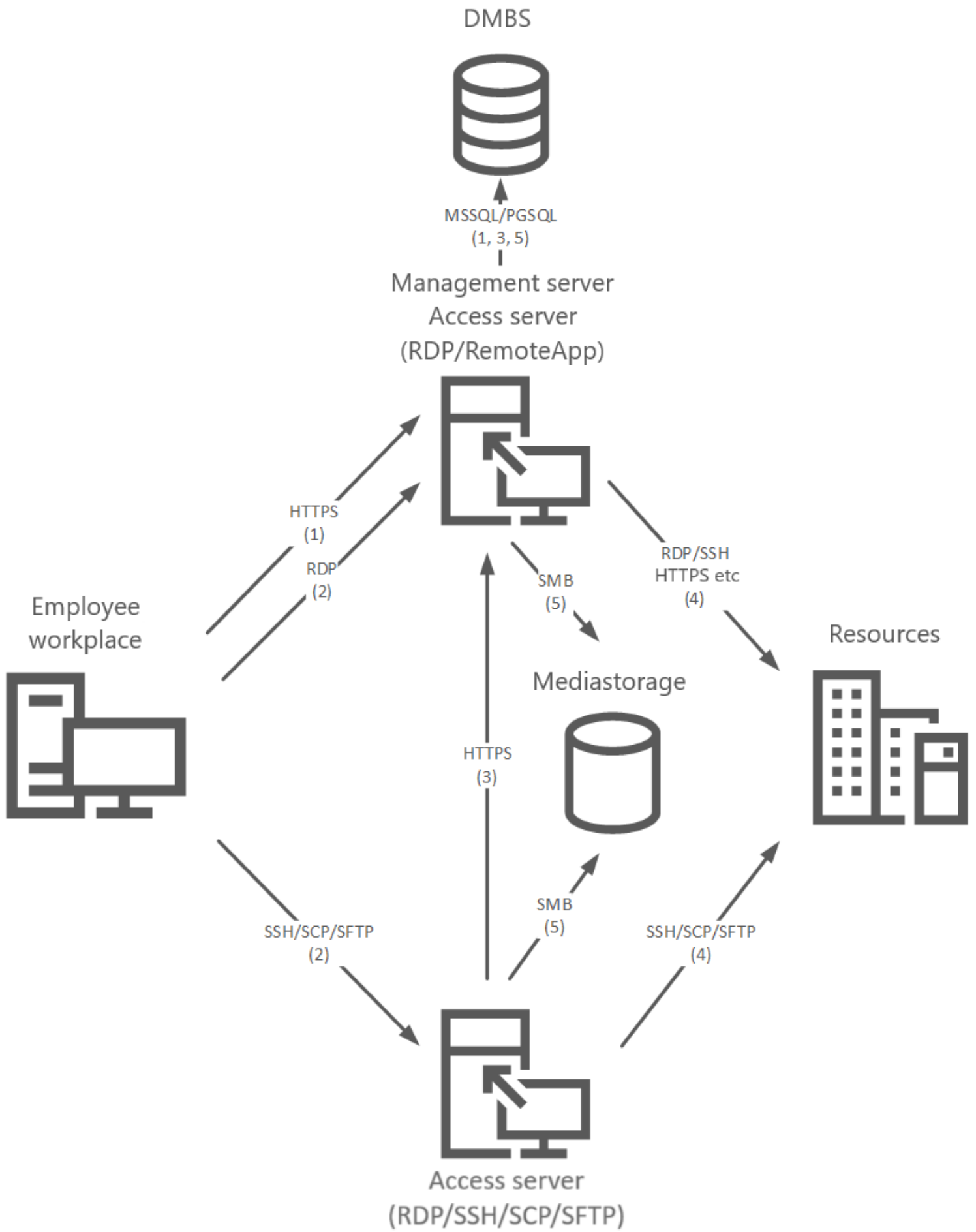
- Axidian Privilege Core
- Axidian Privilege IdP
- Axidian Privilege Management Console
- Axidian Privilege User Console
- Axidian Privilege Log Server
- Axidian Privilege EventLog
- Axidian Privilege Gateway
- Axidian Privilege ESSO Admin Pack
- Axidian Privilege ESSO Agent

### Access Server (SSH/SCP/SFTP)

- Axidian Privilege SSH Proxy
- Axidian Privilege RDP Proxy

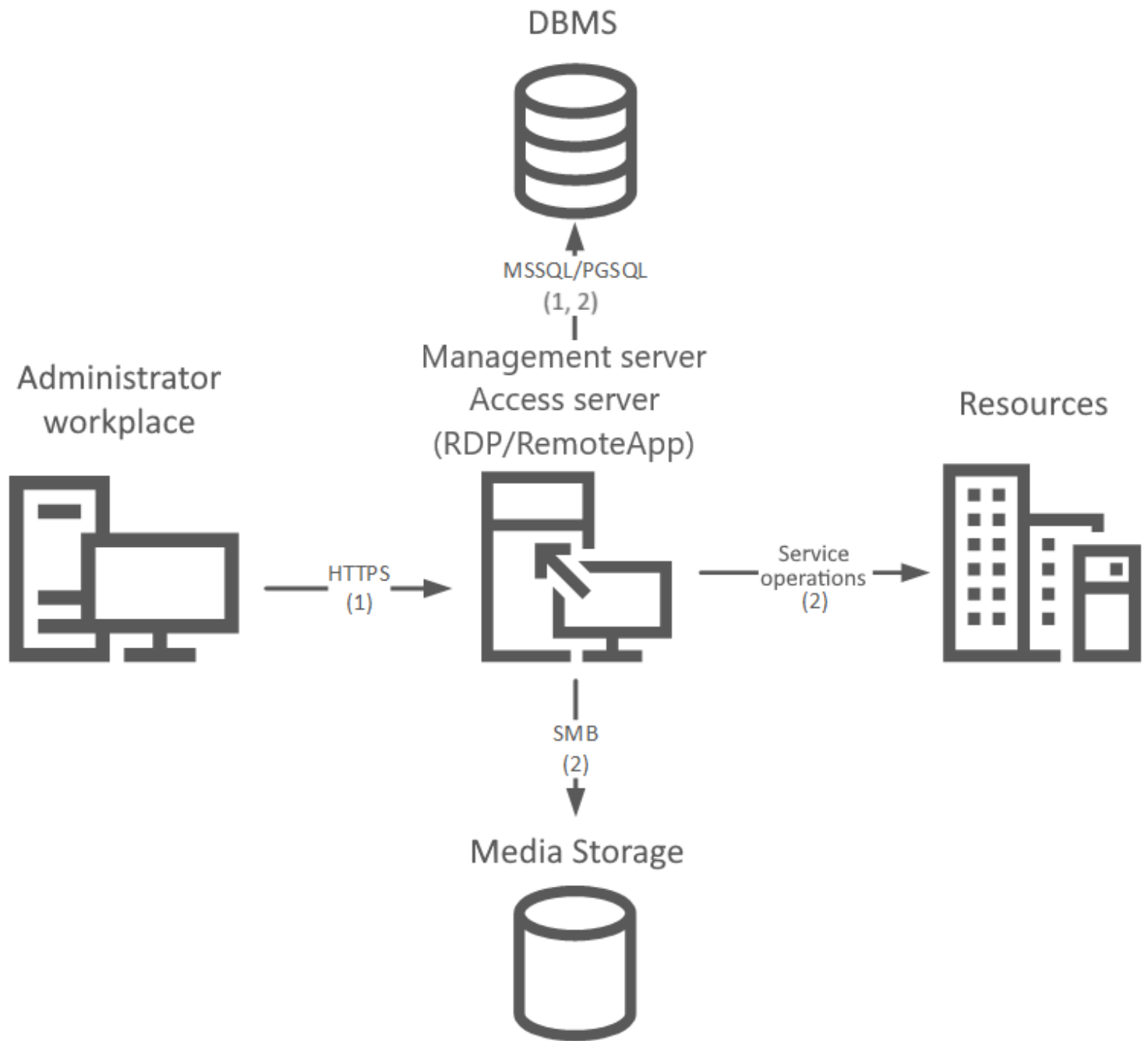
## Work Scenarios

### 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) 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)

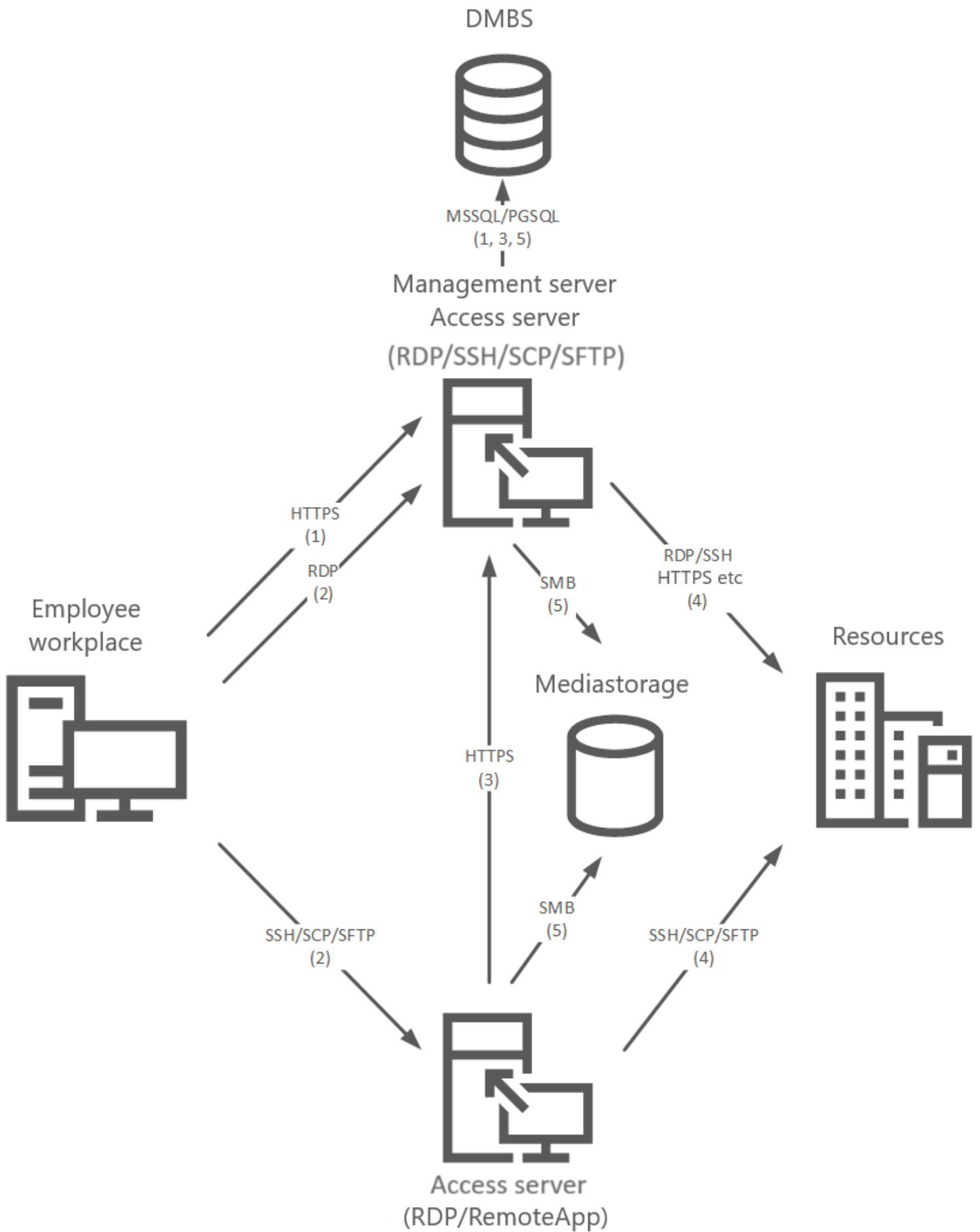
- Axidian Privilege Core
- Axidian Privilege IdP
- Axidian Privilege Management Console
- Axidian Privilege User Console
- Axidian Privilege Log Server
- Axidian Privilege SSH Proxy
- Axidian Privilege RDP Proxy

### Access Server (RDP/RemoteApp)

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

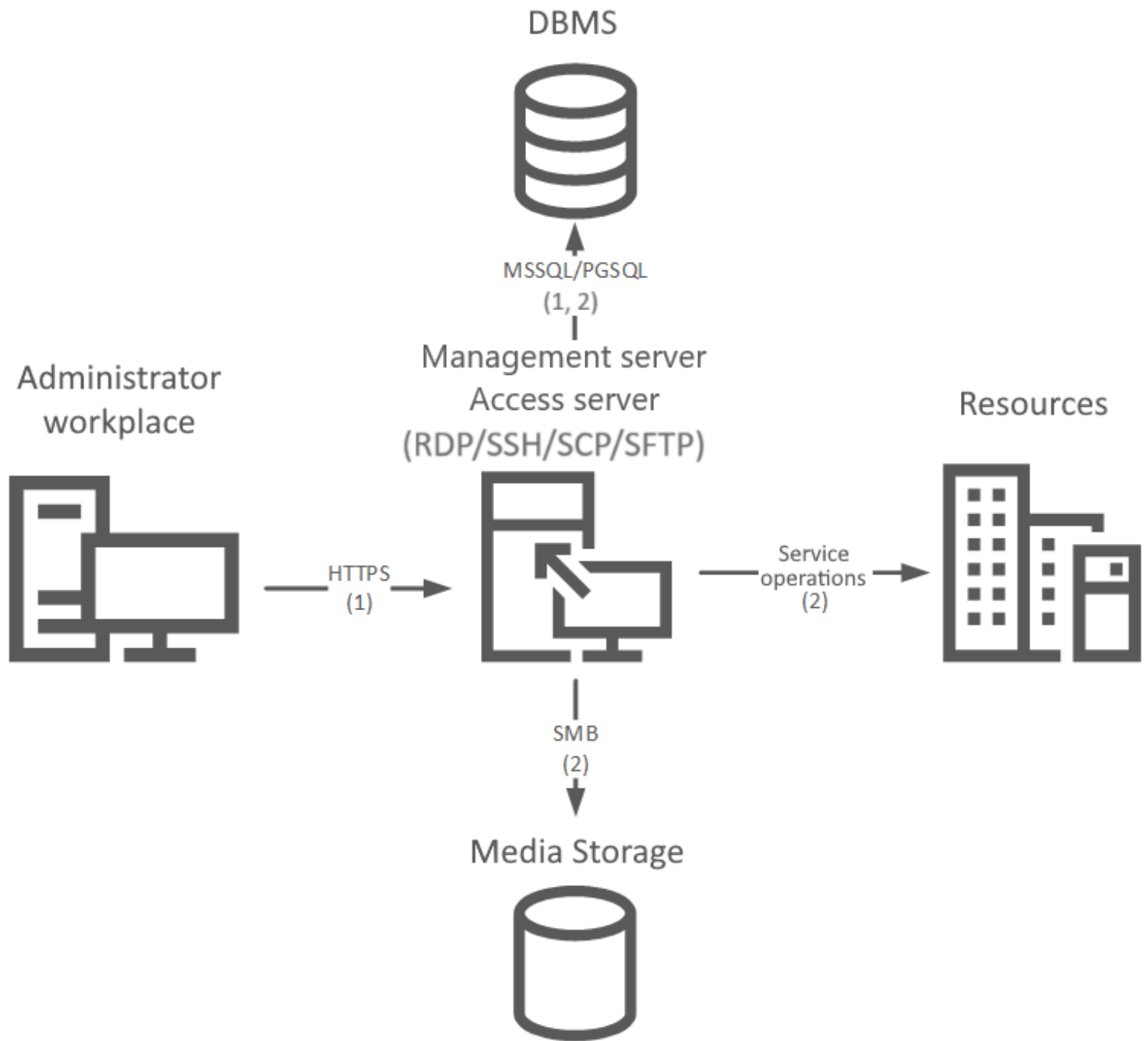
## Work Scenarios

### 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) 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)

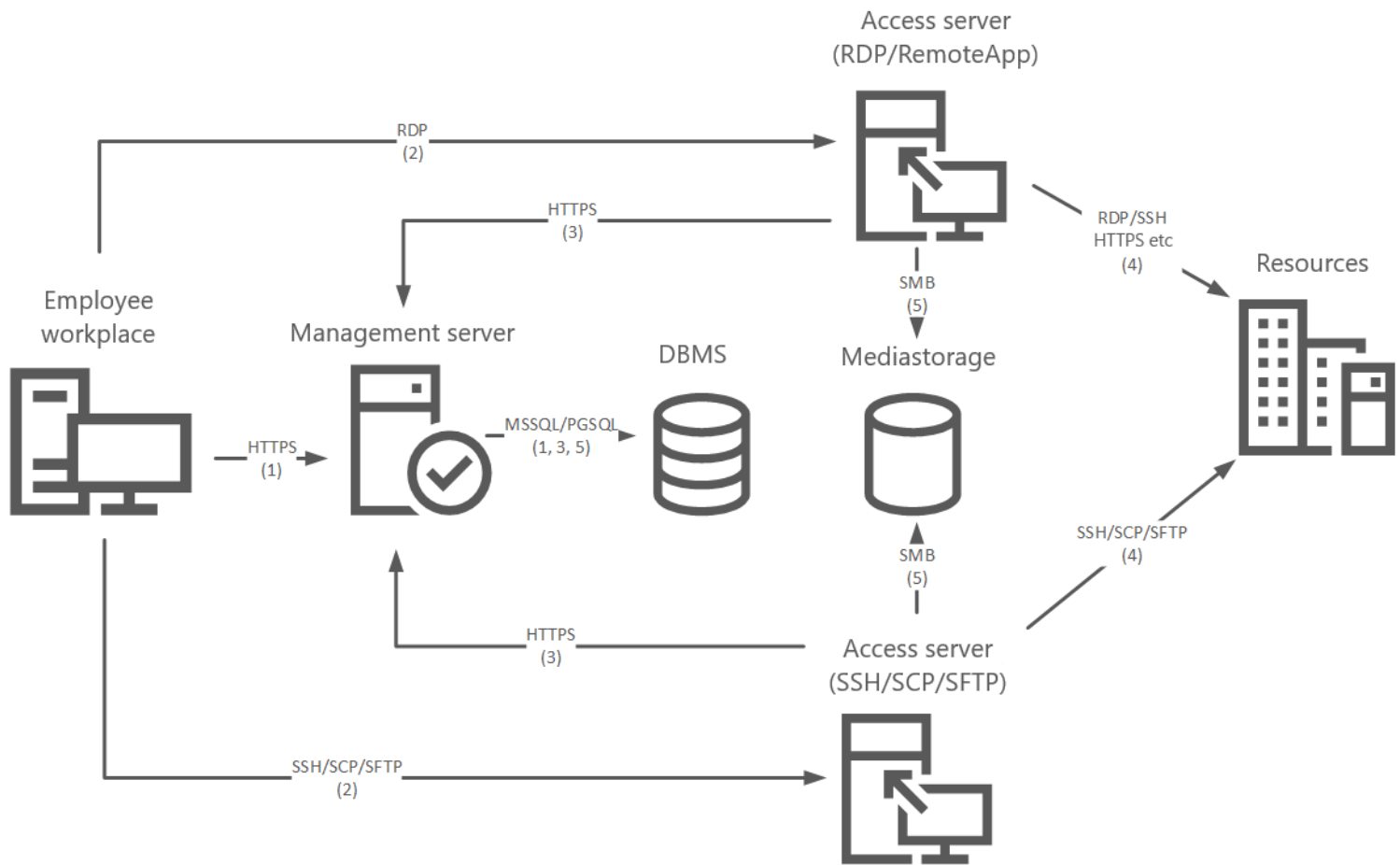
- Axidian Privilege Gateway
- Axidian Privilege ESSO Admin Pack
- Axidian Privilege ESSO Agent

### Access server (RDP/SSH/SCP/SFTP)

- Axidian Privilege SSH Proxy
- Axidian Privilege RDP Proxy

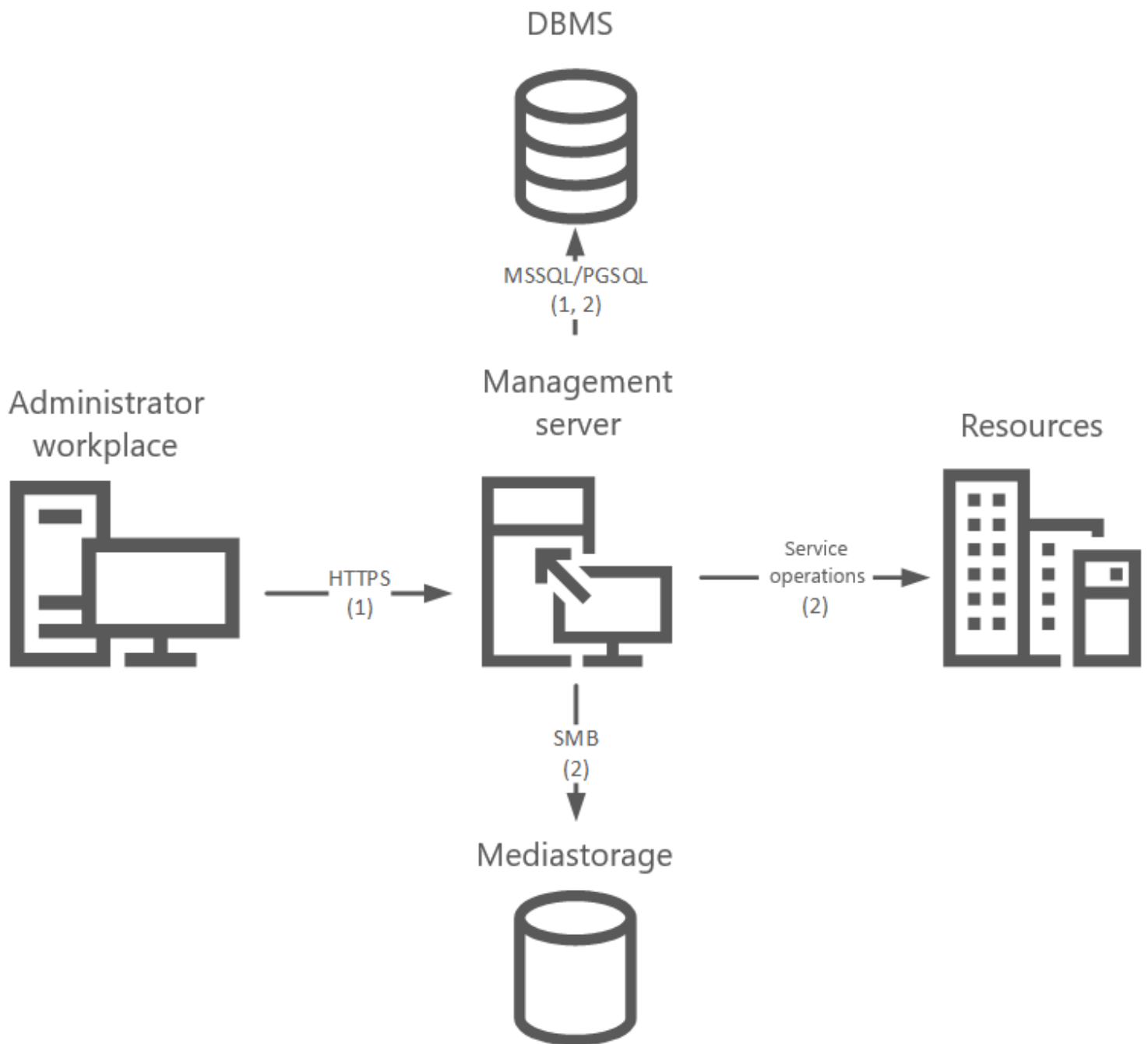
## Work Scenarios

### 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) 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)

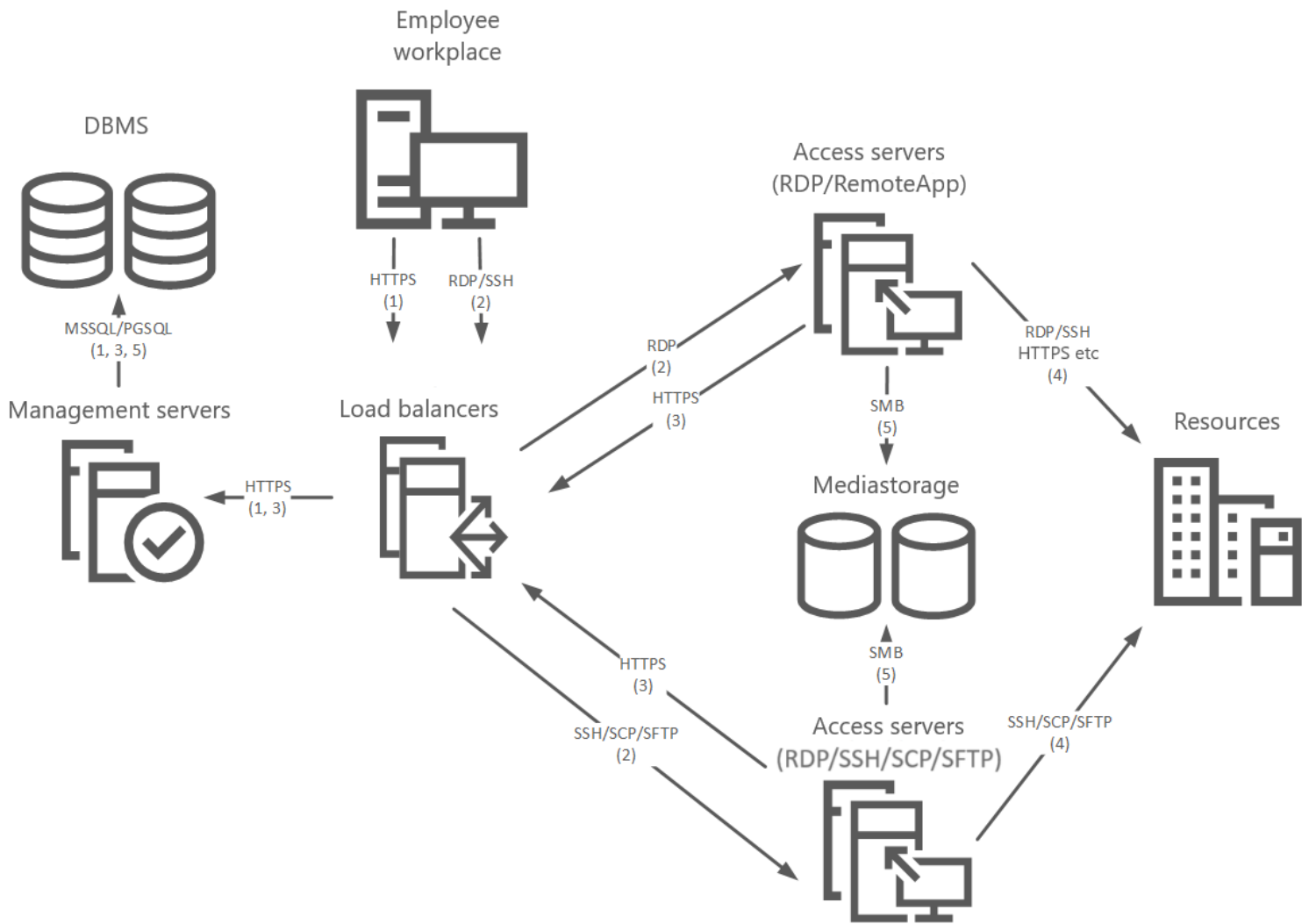
- Axidian Privilege Gateway
- Axidian Privilege ESSO Admin Pack
- Axidian Privilege ESSO Agent

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

- Axidian Privilege SSH Proxy
- Axidian Privilege RDP Proxy

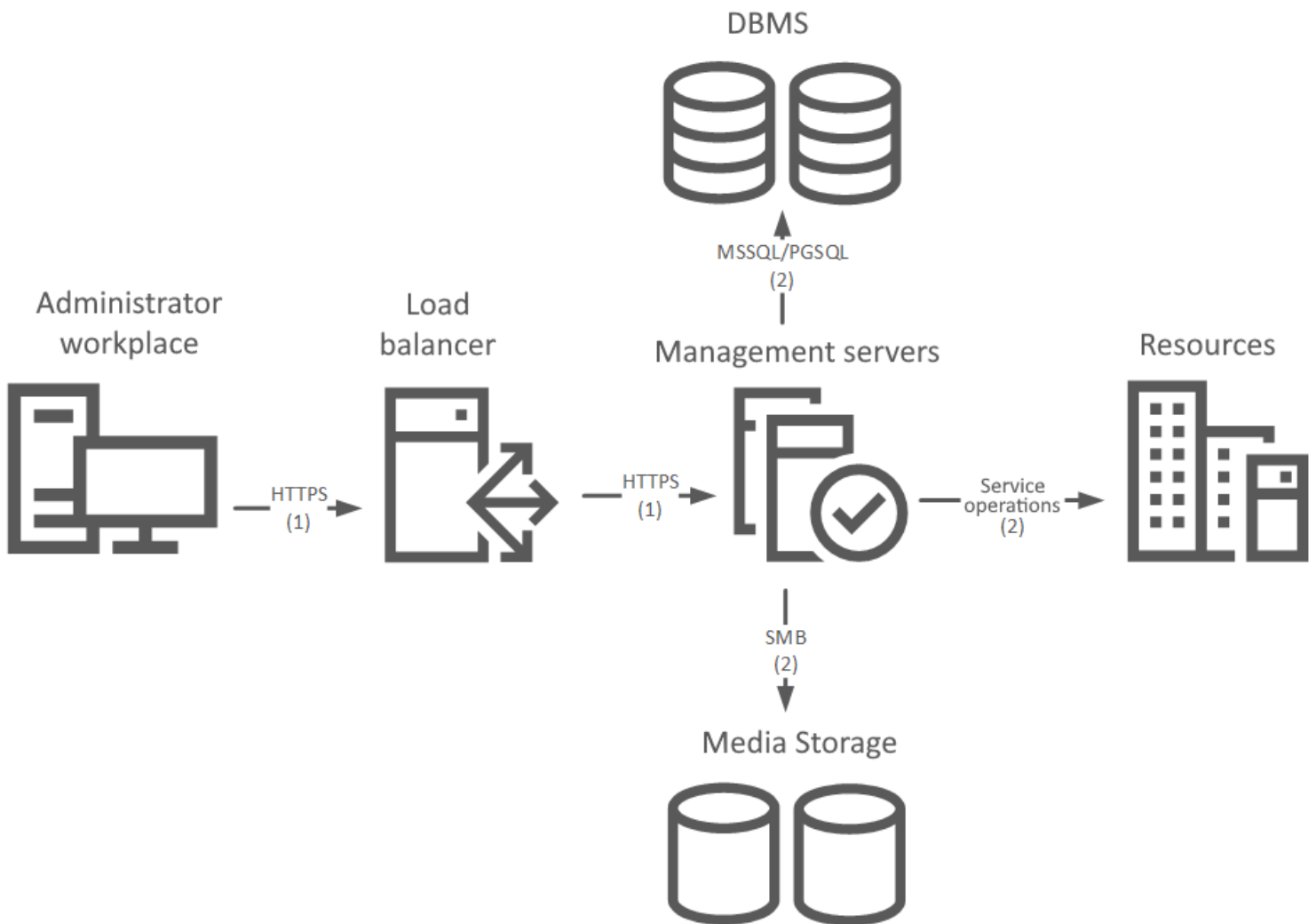
## Work Scenarios

### 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 6
- 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 6](#)
- 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

# 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 Requirements

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.

#### ▼ Alternative way to install Docker (not recommended)

---

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.

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 installed 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**.

Web server:

- Nginx 1.23.1 (docker image included)

## 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	3389	Connection to the Access server
TCP	8443	Reading a session stream

## CIS Benchmark Security Settings

PAM servers must have [CIS Benchmark security settings](#) applied.

# 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

# 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. [Installation without Balancing](#)

2. [Installation with Balancing](#)
3. [Access Server \(RDP/RemoteApp\)](#)

# 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.



## Active 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)



## IIS Setup

Add a registry entry and configure IIS (for Windows)

# Active 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

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, **IPAMManager**.
5. Fill in the required fields and complete the account creation.

Alternatively, you can use an existing account.

## Account for Service Operations in Active Directory

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

15. Save.

Alternatively, you can use an existing account.

# Certificates


## Preparation

### Windows

1. Create a management server certificate in PFX format with a private key (you need to issue a domain CA certificate) with the following attributes:
  - i. Subject: Common name — <DNS name of the management server>
  - ii. Subject Alternative name:
    - a. DNS — <DNS name of the management server>
    - b. DNS — <DNS domain name>
2. Certificate Authority certificate in CRT format (Base64)

### Linux

1. Create certificates for each server on which you plan to install Axidian Privilege components (you need to issue a domain CA certificate) with the following attributes:
  - i. Subject: Common name — <DNS name of the component server>
  - ii. Subject Alternative name:
    - a. DNS — <DNS name of the component server>
    - b. DNS — <DNS domain name>

 **CAUTION**

Certificate attributes must be specified in lowercase.

2. Certificate Authority certificate in CRT format (Base64)

## Certificates Export

## Windows

On the management server, add the management server certificate to the personal certificates.

Add the CA certificate to the trusted root certificates on all servers where Axidian Privilege components will be installed.

## Linux

Export Axidian Privilege component server certificates in PFX format with the same password for all certificates.

Export the certificate of the certification authority in CRT (Base64) format.

# 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.
- **LS** — 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**, **LS**.
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 **LS** 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 file system directories, for example **MediaData**, **ShadowCopy**, **Screencasts**.
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

# IIS Setup

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

1. Add the following registry entries:

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

2. Run **IIS** snap-in, go to **Default Web Site\pam** 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\pam\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.



## Simplified Installation on Linux OS

Explore Axidian Privilege



## Configuration Files Setup

2 items



## Windows Server OS

3 items



## Linux OS

3 items



## 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, OpenLDAP, ALD Pro user directories (optional)

# Simplified Installation on Linux OS

## CAUTION

With this type of installation you will install the components of management server and access server (SSH-Proxy or RDP-Proxy) on the one server.

## Preparation

Before you begin the installation, please read the [preparation for installation](#) section.

## Certificates

### Certificate of Certification Authority

Move the CA certificate to the distribution along the path:

```
axidian-pam-linux\state\ca-certificates
```

### Server Certificate

Move the server certificate to the distribution along the path:

```
axidian-pam-linux\state\certs
```

## vars

1. Go to the folder `axidian-pam-linux\scripts\ansible` and open the file `vars.yml`.
2. Find the line `# pfx_pass: "ENTER_HERE"` and delete the `#` symbol.
3. Instead of `ENTER_HERE`, specify the password for the server certificate and save the changes.

## Flat Configuration File

1. Go to the distribution folder.
2. Change the **config.json.template** file extension from template to json.
3. Make sure the file name is **config.json**.

Fill in the indicated fields in the configuration file:

```
1 {
2   "DefaultServer": "TARGET_SERVER_FQDN", //to be filled out
3   "DefaultDbServer": "pgsql",
4   "DefaultDbUser": "admin",
5   "DefaultDbPassword": "Q1w2e3r4",
6   "IdpAdminSids": [
7     "AD_ADMIN_SID" //to be filled out
8   ],
9   "CoreServiceStorageConfiguration": {
10    "Type": "FileSystem",
11    "Settings": {
12      "Root": "/mnt/storage"
13    }
14  },
15  "GatewayServiceStorageConfiguration": {
16    "Type": "FileSystem",
17    "Settings": {
18      "Root": "/mnt/storage"
19    }
20  },
21  "Database": "pgsql",
22  "LogServerUrl": "http://ls:5080/api",
23  "EncryptionKey": "3227cff10b834ee60ad285588c6510ea1b4ded5b24704cf644a51d2a9db3b7e5",
    //to be filled out
24  "ActiveDirectoryDomain": "AD_FQDN", //to be filled out
25  "ActiveDirectoryContainerPath": "USER_CONTAINER_DN", //to be filled out
26  "ActiveDirectoryUserName": "AD_SERVICE_USER_NAME", //to be filled out
27  "ActiveDirectoryPassword": "AD_SERVICE_USER_PASSWORD", //to be filled out
28  "ActiveDirectorySsl": false,
29  "IsLinux": true,
30  "ThreadPoolSize": 8,
31  "Enable2faByDefault": true,
32  "enableOrganizationalUnits": false
33 }
```

Parameters:

- **DefaultServer** — FQDN of the server, for example `server.domain.local.com`.
- **DefaultDbServer** — FQDN of the database server, for example `server.domain.local.com`. To install a postgresql with local docker image for simplified installation, you need to specify `postgresql`.
- **DefaultDbUser** — database user. To install a postgresql with local docker image, you need to specify `admin`.
- **DefaultDbPassword** — password of the database user. To install a postgresql with local docker image, you need to specify `Q1w2e3r4`.
- **IdpAdminSids** — Administrator SID from Active Directory.
- **CoreServiceStorageConfiguration** — path to the media storage from where the Core component will read session artifacts.
- **GatewayServiceStorageConfiguration** — path to the media storage where session artifacts will be placed.
- **Database** — database type, for simplified installation specify `postgresql`.
- **LogServerUrl** — URL address for accessing the LogServer component. Leave unchanged.
- **EncryptionKey** — encryption key. You can use the key specified above.

ⓘ **NOTE**

It is recommended to generate a new database encryption key using the **Axidian PAM.KeyGen.exe** utility, located at the path `axidian-pam-tools\key-gen`.

- **ActiveDirectoryDomain** — DNS of the domain, for example `domain.local.com`.
- **ActiveDirectoryContainerPath** — path to Active Directory users, for example `DC=axidian,DC=test`.
- **ActiveDirectoryUserName** — username for connecting to Active Directory.
- **ActiveDirectoryPassword** — user password for connecting to Active Directory.
- **ActiveDirectorySsl** — this parameter is responsible for selecting a connection via LDAPS.
- **IsLinux** — this parameter is responsible for applying default settings for Linux and Windows systems.

- **ThreadPoolSize** — total number of created threads in rdp-proxy. Leave unchanged.
- **Enable2faByDefault** — parameter responsible for requesting 2FA from users by default.
- **enableOrganizationalUnits** — parameter responsible for adding the **Structure** section to PAM.

### Example of a completed config.json

```
1 {
2   "DefaultServer": "pamserver.axidian.local", //to be filled out
3   "DefaultDbServer": "pgsql",
4   "DefaultDbUser": "admin",
5   "DefaultDbPassword": "Q1w2e3r4",
6   "IdpAdminSids": [
7     "S-1-5-21-2099084505-2851035876-2509165319-1112" //to be filled out
8   ],
9   "CoreServiceStorageConfiguration": {
10    "Type": "FileSystem",
11    "Settings": {
12      "Root": "/mnt/storage"
13    }
14  },
15  "GatewayServiceStorageConfiguration": {
16    "Type": "FileSystem",
17    "Settings": {
18      "Root": "/mnt/storage"
19    }
20  },
21  "Database": "pgsql",
22  "LogServerUrl": "http://ls:5080/api",
23  "EncryptionKey": "3227cff10b834ee60ad285588c6510ea1b4ded5b24704cf644a51d2a9db3b7e5",
  //to be filled out
24  "ActiveDirectoryDomain": "axidian.local", //to be filled out
25  "ActiveDirectoryContainerPath": "OU=PAMUsers,DC=axidian,DC=local", //to be filled
  out
26  "ActiveDirectoryUserName": "IPAMADReadOps", //to be filled out
27  "ActiveDirectoryPassword": "!Q2w3e$R", //to be filled out
28  "ActiveDirectorySsl": false,
29  "IsLinux": true,
30  "ThreadPoolSize": 8,
31  "Enable2faByDefault": true,
32  "enableOrganizationalUnits": false
33 }
```

# Installation

1. Move the **axidian-pam-linux** distribution folder to the target Linux resource
2. 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
```

3. At the **Enter target IP** step press **Enter**
4. When prompted, enter your local sudo user name (for example, root) and password
5. Wait until the installation is complete

## ⓘ INFO

If the script aborted with an error, send the [log file](#) to technical support.



## Web-Wizard Launch

Download and run Web-Wizard (for Linux)



## Configuration Files Setup

Fill in the fields in the Web-Wizard

# Web-Wizard Launch

1. Download and unpack the Web-Wizard distribution on your Linux machine and go to the distribution directory.
2. Run the command:

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

3. Wait for the script to complete.

```
admin@ubuntu16:~/indeed-pam-linux$ sudo bash run-wizard.sh
2023-11-28 19:57:40 |
*****
* Check docker
*****
2023-11-28 19:57:40 | Docker: Installed and working
2023-11-28 19:57:58 |
*****
* Run web wizard with docker-compose
*****
2023-11-28 19:58:33 |
*****
* AuthenticationCode: DTBjia0BKspCoYVCNMZtXYXfXAOFycRb
*****
2023-11-28 19:58:33 | Web wizard started successfully.
2023-11-28 19:58:33 | URL: https://ubuntu16.test.com
admin@ubuntu16:~/indeed-pam-linux$
```

4. Once the script is completed, go to the URL you see in the console.

## Logging into the PAM Configuration Wizard

Specify the code that the PAM Configuration Wizard application specified when it started in the logs

5. In the **Authentication Code** field, enter the value you see in the console after executing the script.

6. Select **New Configuration**.

PAM Configuration Wizard Exit

What PAM configuration do you want to set up?

7. Go to the next section of the documentation—[Configuration Files Setup](#).

8. After completing the setup and loading the configuration files, stop the web-wizard by running the command:

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

# Configuration Files Setup

1. Select the OS which you plan to install the Axidian Privilege on and click **Next**.
2. Enter the FQDN of the management server in the **Management server address** field.

Fill in the **IP addresses of PAM access servers** field.

IP addresses can be specified in the following formats:

- Single IP address. Example: `192.168.0.1`
- Range of IP addresses (first and last IP addresses in the range, separated by a hyphen). Example: `172.168.0.0 - 172.168.255.255`
- Subnet (in IP/mask format). Example: `10.0.0.0/8`

You can enter multiple values separated by commas or semicolons.

Example: `192.168.0.1, 192.168.0.2, 172.168.0.0 - 172.168.255.255, 10.0.0.0/8, 2001:0db8:abf2:29ea:5298:ad71:2ca0:4ff1.`

## CAUTION

Don't leave the field empty. If you need to allow all networks please enter `0.0.0.0/0; ::/0.`

Click **Next**.

3. In the next window specify the information about the database: **Server type**, **Server address**. Enter the [login and password of the account](#) in **User** and **Password** fields. Leave the **Add a new encryption key** option disabled.

## CAUTION

To use a named MSSQL instance, you will need to make changes to the configuration files of the core, idp and ls components. It is necessary to specify the instance in the **Data Source** field, in the **ConnectionString** section, for example: **Data Source=storage.axidian.local\\sqlexpress**

In the core and idp configuration files, you must specify the instance using 2 slashes: **\\sqlexpress**

In the ls configuration file, you must specify the instance using 1 slash: **\\sqlexpress**

Click **Next**.

4. Select **Storage type**.

Possible values: - **File system - SMB - S3** If you select **SMB**, fill in the following fields: **Network Path, Domain, Username** and **Password**.

If you select **S3**, fill in the following fields: **Network address of the S3 server, Path to the root directory of the storage on the S3 server, Access key id, Secret access key**. If necessary, fill in the optional fields: **Region, Location restriction**.

Click **Next**.

5. In the next window, specify the DNS domain name, DN container name of the user directory, enter the login and password of the account for reading the user directory, and check whether it is necessary to use the LDAPS protocol when reading the directory (LDAP is used by default) and click **Next**.

6. In the next window, enter the SID of the role administrator and click **Next**.

7. Download the necessary configuration files and click **Finish**.

8. Stop the web-wizard by running the command:

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



## Management Server (Windows)

Install Management Server Components (Windows)



## Access Server (RDP\RemoteApp)

Install Access Server Components (RDP/RemoteApp)



## Access Server (SSH Proxy)

Install Access Server Components (SSH Proxy)

# Management Server (Windows)

## TIP

To get the Axidian Privilege distribution, please contact Technical Support.

## CAUTION

Before you begin the installation, prepare the configuration files.

1. Download and unzip the Axidian Privilege archive to the management server.
2. Login with Active Directory account and run PowerShell as administrator.
3. Run the **axidian-pam-wizard.ps1** installation script.
4. In the **Select components** window, check **Management Server** and click **Next**.
5. In the next step, click **Install** and wait for the installation to finish.  
Click **OK** in the popup window.
6. Place the prepared configuration files along the following paths:
  - i. C:\inetpub\wwwroot\pam\core — core
  - ii. C:\inetpub\wwwroot\pam\idp — idp
  - iii. C:\inetpub\wwwroot\pam\mc\assets\config — mc
  - iv. C:\inetpub\wwwroot\pam\uc\assets\config — uc
  - v. C:\inetpub\wwwroot\ls\targetConfigs — ls
  - vi. C:\inetpub\wwwroot\ls — AxidianPAM\_2.10.0\axidian-pam-windows\LS\clientApps.config

## CAUTION

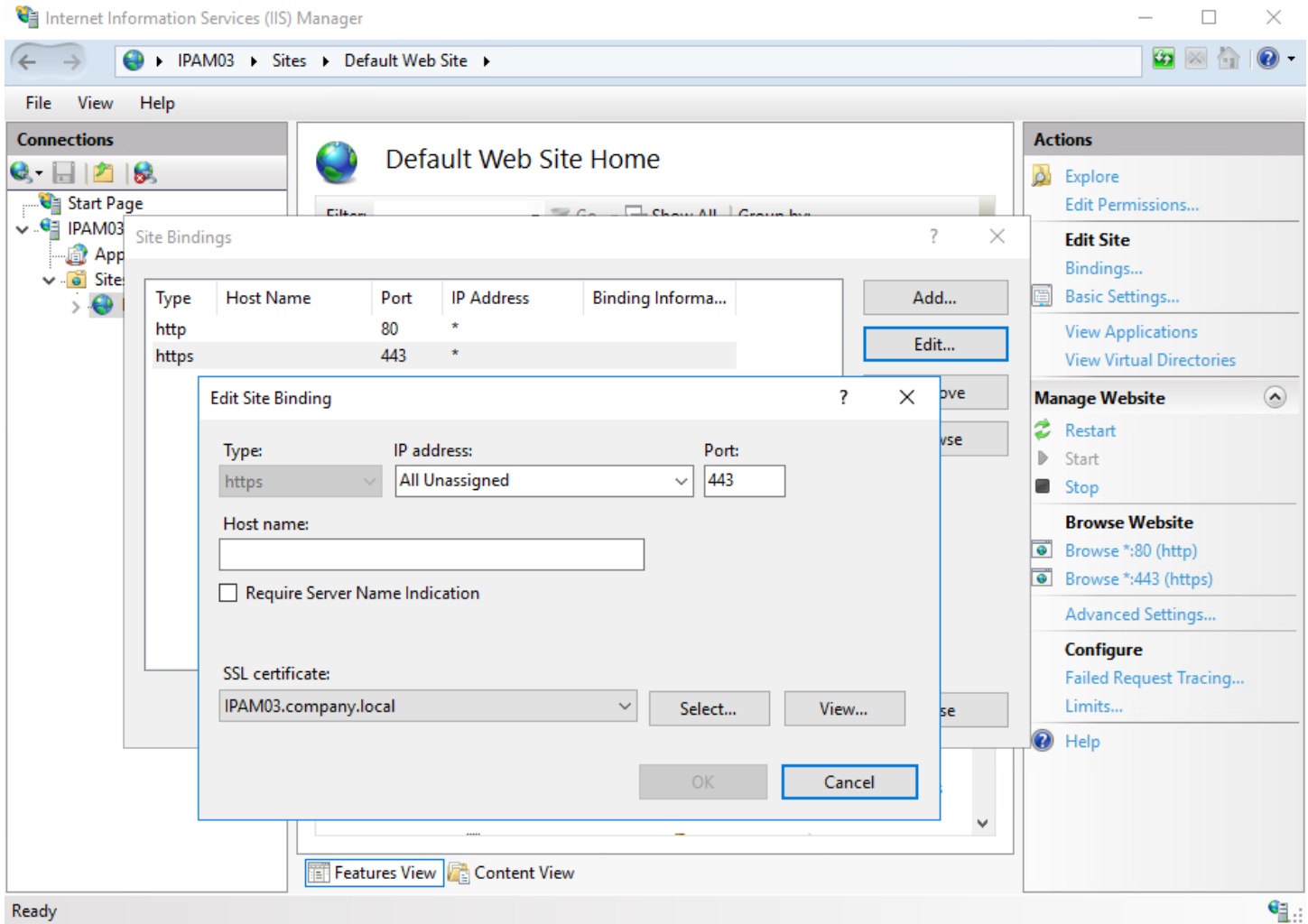
If you are using a PostgreSQL database, you need to change the **Type** value from **mssql** to **pgsql** in the **clientAppsconfig** file in the `<Target Id="Pam.DbTarget" Type="mssql"/>` line.

7. Navigate to the path: `axidian-pam-tools\scripts`, run PowerShell as administrator and run the **ils-access-list.ps1** script.
8. Add the CA certificate to your trusted root certificates.
9. Add the prepared server certificate to your personal certificate store.
10. In the Axidian Privilege distribution, navigate to the path: `axidian``-pam-windows\MISC\ConfigurationProtector` and run PowerShell as administrator.
11. Run the command:

```
.\Pam.Tools.Configuration.Protector.exe generate-signing-cert
```

12. Start **Internet Information Services (IIS) Manager**.
13. Select **Default Web Site**, click **Bindings....**
14. Click **Add...**, select **Type: http**, **Port: 80**, click **OK**.
15. Click **Add...**, select **Type: https**, **Port: 443**, click **OK**.

16. Choose prepared server certificate in **SSL certificate**, click **OK**.



17. If you are installing the management server on Windows Server version 2022, then in HTTPS bindings, enable the **Disable TLS 1.3 over TCP** option. For versions 2016 and 2019, skip this step.

18. Click to **Restart** on the **Manage Website** section in the **Default Web Site** window.

# Access Server (RDP\RemoteApp)

## TIP

To get the Axidian Privilege distribution, please contact Technical Support.

## CAUTION

Before you begin the installation of the access server components, you need to [deploy Remote Desktop Services roles](#) and [prepare configuration files](#).

## CAUTION

After installing and configuring the access server components, you need to [apply security settings](#) required for Axidian Privilege Gateway.

Otherwise, sessions will be interrupted when connecting to the Access server.

1. Unzip the Axidian Privilege archive to the management server.
2. Login with Active Directory account and run PowerShell as administrator.
3. Run the **axidian-pam-Wizard.ps1** installation script.
4. In the **Select components** window, check **Access Server** and click **Next**.
5. In the next step, click **Install** and wait for the installation to finish.  
Click **NO** in the first popup window. Click **OK** in the second popup window.
6. Place the [prepared configuration files](#) along the following path:
  - i. C:\Program Files\Axidian\Axidian Privilege\Gateway\ProxyApp — rds-proxy
7. Open the **Server Manager**.
8. Go to **Remote Desktop Services** → **Collections**.
9. Click **Tasks** and click **Create session collections**.

10. Specify the settings you need and finish the collection creation.

 **CAUTION**

The name of the RDS collection you create must contain no more than 16 characters.

11. In **RemoteApp Programs** section click **Tasks** and click **Publish RemoteApp Programs**.

12. Click **Add** and select `C:\Program Files\Axidian\Axidian  
Privilege\Gateway\ProxyApp\Pam.Proxy.App.exe` application. Click **Next** → **Publish**.

13. In **RemoteApp Programs** section open the context menu of the published application and click **Edit Properties**.

14. Go to **Parameters**, check the **Allow any command-line parameters** and click **OK**.

15. Apply the [security settings](#).

16. Restart the server.

# Access Server (SSH Proxy)

## CAUTION

Before you begin the installation, prepare the configuration files.

## Inventory

1. Go to the axidian-pam-linux distribution folder and rename the **inventory.template** file to **inventory**.
2. Edit the **inventory** file:
  - i. In the **access** section, specify the FQDN addresses of the access servers
  - ii. For all of the servers except the local one, add the following line: **remote\_user=root ansible\_password=123 ansible\_become\_password=123**
    - a. **remote\_user=root** — username for remote connection to the resource
    - b. **ansible\_password=123** — user password for remote connection to the resource
    - c. **ansible\_become\_password=123** — user password for remote connection to the resource
  - iii. Comment out all fields that have not been changed and save.

### /client-dist/inventory file contents

```
1 # NOTE: To access docker host use local.docker name instead of localhost
2
3 #[management]
4 #MANAGEMENT_SERVER_FQDN_OR_IP
5
6 [access]
7 pamgtw1.test.local
8 pamgtw2.test.local remote_user=root ansible_password=123 ansible_become_password=123
9
10 #[haproxy]
11 #HAPROXY_SERVER_FQDN_OR_IP
12
13 #[rds]
14 #RDS_SERVER_FQDN_OR_IP
15
16 # Use this section to override vars
17 #[all:vars]
```

# Configuration Files

Unzip the downloaded [configuration files](#) and move the **ssh-proxy** and **rdp-proxy** folders to **axidian-pam-linux\state**.

## Installation

1. Move the distribution to the target Linux resource.
2. Run the installation script with the command:

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

3. When prompted, enter your local sudo user name (for example, root) and password.
4. Wait for the installation to finish.

### ! INFO

If the script aborted with an error, send the [log file](#) to technical support.

## Certification Authority Certificate

1. Add the downloaded CA certificate in .crt format along the path **/etc/axidian/axidian-privilege/ca-certificates**.
2. Go to the **/etc/axidian/axidian-privilege** folder.
3. Restart Axidian Privilege access server components using 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
```



## Installation without Balancing

Install Management Server and Access Server on separate hosts



## Installation with Balancing

Install Management Server and Access Server on separate hosts with balancing



## Access Server (RDP/RemoteApp)

Install Access Server Components (RDP/RemoteApp)

# Installation without Balancing

## CAUTION

The installation without balancing includes installation of the management server and access servers (SSH-Proxy or RDP-Proxy) on different servers.

## CAUTION

Before you begin the installation, [prepare the configuration files](#).

## Inventory

1. Go to the distribution folder.
2. Change the name of the **inventory.template** file to **inventory**.

Edit the **inventory** file:

1. In the **managment** section, specify the FQDN address of the management server.
2. In the **access** section, specify the FQDN address of the SSH Proxy access server.
3. For all of the servers except the local one, add the following line: **remote\_ssh\_user=root ansible\_ssh\_password=123 ansible\_become\_password=123**.
  - i. **remote\_ssh\_user=root** — username for remote connection to the resource.
  - ii. **ansible\_ssh\_password=123** — user password for remote connection to the resource.
  - iii. **ansible\_become\_password=123** — user password for remote connection to the resource.
4. Comment out all fields that have not been changed.
5. Save.

### **/client-dist/inventory file contents**

```
1 # NOTE: To access docker host use local.docker name instead of localhost
2
3 [management]
4 pamng.test.local
5
6 [access]
```

```
7 pamgtw.test.local remote_ssh_user=root ansible_ssh_password=123
  ansible_become_password=123
8
9 #[haproxy]
10 #HAPROXY_SERVER_FQDN_OR_IP
11
12 #[rds]
13 #RDS_SERVER_FQDN_OR_IP
14
15 # Use this section to override vars
16 #[all:vars]
17 #server_fqdn=OVERRIDE_SERVER_FQDN
```

## Configuration Files

Unzip the downloaded [configuration files](#) and move the extracted folders to **axidian-pam-linux\state**.

## Certificates

### Certification Authority Certificate

Move the CA certificate along the path **axidian-pam-linux\state\ca-certificates**.

### Server Certificates

1. Go to **axidian-pam-linux\state\certs** and create a separate folder for the management server. Name it with the FQDN of the management server.
2. Move the management server certificate to the folder corresponding to the management server.
3. Go to **axidian-pam-linux\state\keys\rdp-proxy** and create a separate folder for the access server. Name it with the FQDN of the access server.
4. Move the access server certificate to the folder corresponding to the access server.

## vars

1. Go to axidian-pam-linux\scripts\ansible and open the file **vars.yml**.
2. In the **# pfx\_pass: "ENTER\_HERE"** line remove the **#** symbol.

3. Instead of **ENTER\_HERE**, specify the password for the certificates.
4. Save.

## Installation

1. Move the distribution to the target Linux resource.
2. 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
```

3. When prompted, enter your local sudo username (for example, root) and password.
4. Wait for the installation to finish.

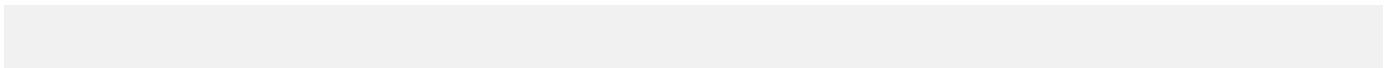
### ⓘ INFO

If the script aborted with an error, send the [log file](#) to technical support.

## Components Restarting

### Management Server

1. Go to the `/etc/axidian/axidian-privilege` folder.
2. Restart Axidian Privilege management server components using the following commands:
  - i. Restarting all of the components:



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

or

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

## ii. Restarting a specific component:

```
sudo docker compose -f docker-compose.management-server.yml up -d <component
name> --force-recreate
```

or

```
sudo docker-compose -f docker-compose.management-server.yml up -d <component
name> --force-recreate
```

## iii. Example of restarting the Axidian Privilege Core component:

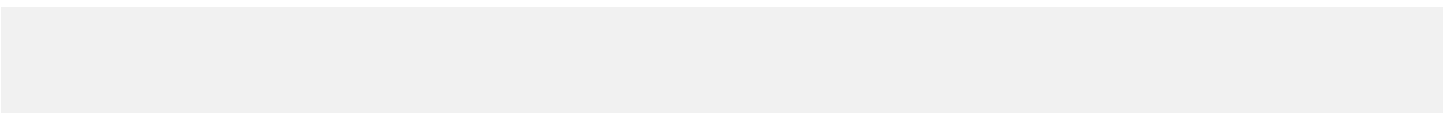
```
sudo docker compose -f docker-compose.management-server.yml up -d core --force-
recreate
```

or

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

# Access Server

1. Go to the **/etc/axidian/axidian-privilege** folder.
2. Restart Axidian Privilege access server components using 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
```

# Installation with Balancing

## CAUTION

The installation with balancing includes installation of multiple management servers and access servers (SSH-Proxy or RDP-Proxy) on different servers.

## CAUTION

Before you begin the installation, [prepare configuration files](#).

## Inventory

1. Go to the axidian-pam-linux distribution folder and rename the **inventory.template** file to **inventory**.
2. Edit the **inventory** file:
  - i. In the **managment** section, specify the FQDN address of the management server, in the **access** section, specify the FQDN address of the SSH Proxy accessserver.
  - ii. For all of the servers except the local one, add the following line: **remote\_ssh\_user=root ansible\_ssh\_password=123 ansible\_become\_password=123**
    - a. **remote\_ssh\_user=root** — username for remote connection to the resource
    - b. **ansible\_ssh\_password=123** — user password for remote connection to the resource
    - c. **ansible\_become\_password=123** — user password for remote connection to the resource
  - iii. Uncomment the last two lines of the file.
  - iv. In the **all:vars** section, set **server\_fqdn=** to the Axidian Privilege name.
  - v. Comment out all fields that have not been changed and save.

### /client-dist/inventory file contents

```
1 # NOTE: To access docker host use local.docker name instead of localhost
2
3 [management]
4 pamng1.test.local
5 pamng2.test.local remote_ssh_user=root ansible_ssh_password=123
   ansible_become_password=123
6
7 [access]
```

```
8 pamgtw1.test.local remote_ssh_user=root ansible_ssh_password=123
  ansible_become_password=123
9 pamgtw2.test.local remote_ssh_user=root ansible_ssh_password=123
  ansible_become_password=123
10
11 #[haproxy]
12 #HAPROXY_SERVER_FQDN_OR_IP
13
14 #[rds]
15 #RDS_SERVER_FQDN_OR_IP
16
17 # Use this section to override vars
18 [all:vars]
19 server_fqdn=pammng.test.local
```

## Configuration Files

Unzip the downloaded [configuration files](#) and move the extracted folders to **axidian-pam-linux\state**.

## Certificates

### Certification Authority Certificate

Move the CA certificate along the path **axidian-pam-linux\state\ca-certificates**.

### Server Certificates

1. Go to **axidian-pam-linux\state\certs** and create a separate folder for each of the management server. Name each of the folders with the FQDN name of the management server.
2. Move the management server certificates to the folders corresponding to the management servers.
3. Go to **axidian-pam-linux\state\keys\rdp-proxy** and create a separate folder for the access server. Name each of the folders with the FQDN name of the access server.
4. Move the access server certificate to the folder corresponding to the access server.

## vars

1. Go to **axidian-pam-linux\scripts\ansible** and open the file **vars.yml**.

2. In the `# pfx_pass: "ENTER_HERE"` line remove the `#` symbol.
3. Instead of `ENTER_HERE`, specify the password for the certificates.
4. Save.

## Installation

1. Move the distribution to the target Linux resource.
2. 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
```

3. When prompted, enter your local sudo username (for example, root) and password.
4. Wait for the installation to finish.

### ⓘ INFO

If the script aborted with an error, send the [log file](#) to technical support.

## Components Restarting

### Management Server

1. Go to the `/etc/axidian/axidian-pam` folder.
  2. Restart Axidian Privilege management server components using the following commands:
    - i. Restarting all of the components:
-

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

or

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

## ii. Restarting a specific component:

```
sudo docker compose -f docker-compose.management-server.yml up -d <Имя
компонента> --force-recreate
```

or

```
sudo docker-compose -f docker-compose.management-server.yml up -d <Имя
компонента> --force-recreate
```

## iii. Example of restarting the Axidian Privilege Core component:

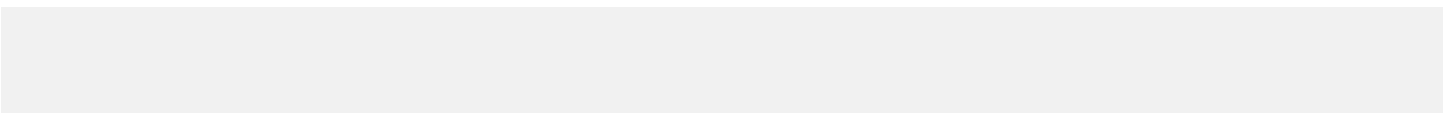
```
sudo docker compose -f docker-compose.management-server.yml up -d core --force-
recreate
```

or

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

# Access Server

1. Go to the **/etc/axidian/axidian-pam** folder.
2. Restart Axidian Privilege access server components using 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
```

# Access Server (RDP/RemoteApp)

## TIP

To get the Axidian Privilege distribution, please contact Technical Support.

## CAUTION

Before you begin the installation of the access server components, you need to [deploy Remote Desktop Services roles](#) and [prepare configuration files](#).

## CAUTION

After installing and configuring the access server components, you need to [apply security settings](#) required for Axidian Privilege Gateway.

Otherwise, sessions will be interrupted when connecting to the Access server.

1. Copy the Axidian Privilege distribution folder to the Access server.
2. Login with Active Directory account and run PowerShell as administrator.
3. Launch the **axidian-pam-wizard.ps1** installation script.
4. In the **Select components** window, check **Access Server** and click **Next** button.
5. In the next step, click **Install** button, wait for the installation to finish. Click **No** button when prompt to reboot appears.
6. Place the [prepared configuration files](#) along the following path:  
C:\Program Files\Axidian\Axidian Privilege\Gateway\ProxyApp — rds-proxy
7. Start the **Server Manager**.
8. Go to **Remote Desktop Services** → **Collections**.
9. Under **Collections**, click **Tasks** and select **Create session collections**.
10. Complete the wizard to create a collection with the settings you need.

 **CAUTION**

The name of the RDS collection you create must contain no more than 16 characters.

11. Under **RemoteApp Programs** click **Tasks** and select **Publish RemoteApp Programs**.
12. Click **Add**, select  
application `\\PAMServerName\c$\ProgramFiles\Axidian\AxidianPrivilege\Gateway\ProxyApp\Pam.  
Proxy.App.exe`, click **Next**, **Publish**.
13. In the **RemoteApp Programs** section, open the context menu of the published application and  
select **Edit Properties**.
14. Go to **Parameters**, set the **Allow any command-line parameters** option and click **OK**.
15. Apply the [security settings](#).
16. 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_2.10.0\axidian-pam-tools\pamsu\` folder.

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

- `..PAM_2.10.0\axidian-pam-tools\pamsu\axidian-privilege.pamsu-ossl*.x64.deb`
- `..PAM_2.10.0\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_2.10.0\axidian-pam-tools\pamsu\axidian-privilege.pamsu-no-ossl*.x64.deb`
- `..PAM_2.10.0\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**
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**

# 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 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\pam\idp` and edit file `appsettings.json`.

## Section IdentitySettings

- **DirectoryMechanism** — Mechanism of authentication.
- **Authentication** — Authentication provider.

### IdentitySettings section in appsettings.json configuration file

```
1 "IdentitySettings": {  
2   ...  
3   "DirectoryMechanism": "Radius",  
4   "Authentication": "Local",  
5   ...  
6 }
```

## Section Radius

- **AuthenticationScheme** — authentication scheme in RADIUS. Possible parameters: `PAP`, `CHAP`, `MSCHAPV2`. The `PAP` scheme is insecure.

## NOTE

Using CHAP authentication in Windows, it is necessary to enable **Store passwords using reversible encryption** in the user account settings and update the user's password.

- **AuthenticationUserName** — name format for authentication. Possible parameters:
  - **NameWithoutDomain** — name without domain (for authentication in FreeRadius)
  - **SamCompatibleName** — name in the format AXIDIAN\\user
  - **PrincipalName** — name in the format `user@axidian.domain`
- **Secret** — secret for the additional authentication of the component.
- **Timeout** — timeout waiting for a RADIUS server response.
- **RemoteEndpoint:**
  - **Address** — RADIUS server address for connection.
  - **Port** — RADIUS server port for connection (default port: 1812).

#### Radius section in appsettings.json configuration file (one RADIUS server)

```
1 "Radius": {
2     "AuthenticationScheme": "MSCHAPV2",
3     "AuthenticationUserName": "PrincipalName",
4
5     "Secret": "ENCRYPTED_CfDJ8MPJ7V58kqpLvtoHgdiuk5VKMK_hf3r437uZdHjdZAfve5wtVvgDZPjjDm7bgjC",
6     "Timeout": 10,
7     "RemoteEndpoint": {
8         "Address": "PAM_RADIUS_SERVER",
9         "Port": 1812
10    }
11 }
```

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

#### Radius section in appsettings.json configuration file (two RADIUS servers)

```
1 "Radius": {
2     "Timeout": 10,
3     "RemoteEndpoints": [
```

```
4      {
5        "Address": "10.11.4.28",
6        "Port": 1812,
7        "Secret": "123",
8        "AuthenticationScheme": "MSCHAPV2",
9        "AuthenticationUserName": "PrincipalName"
10     },
11     {
12       "Address": "10.11.4.128",
13       "Port": 1812,
14       "Secret": "123",
15       "AuthenticationScheme": "MSCHAPV2",
16       "AuthenticationUserName": "PrincipalName"
17     }
18   ]
19 },
```

# 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\pam\core — for Windows

```
1  "Rdp": {
2    "UseRemoteApp": false,
3    "SignRdpFile": true,
4    "Certificate": "16c214ba7dec702a7ce5e4ac727502b0c0d448e2",
5    "Password": ""
6  },
```

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

```
1  "Rdp": {
2    "UseRemoteApp": false,
3    "SignRdpFile": true,
4    "Certificate": "/etc/",
5    "Password": "1234"
6  },
```

### 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.

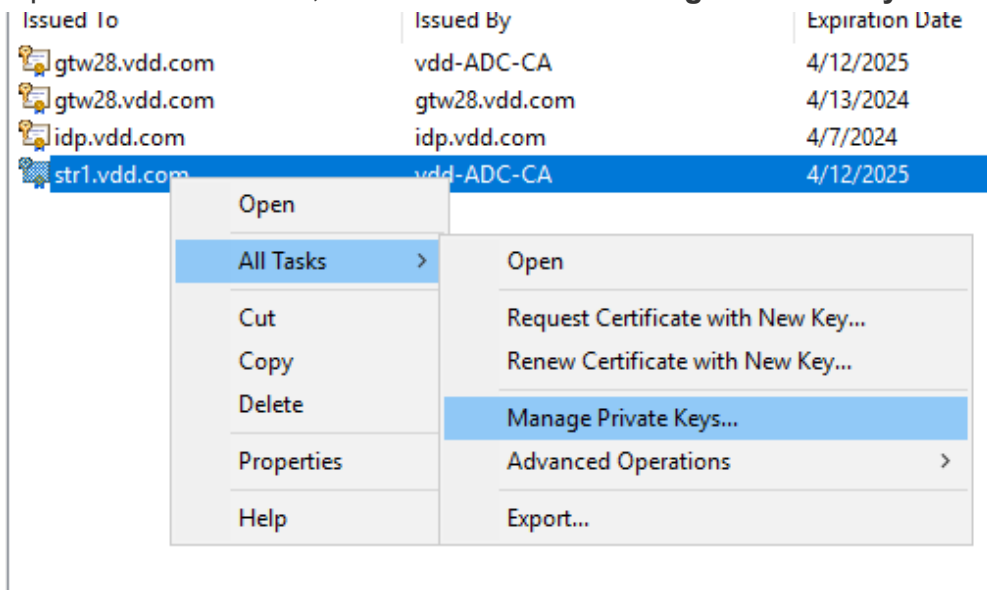
### NOTE

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

## Windows with Fingerprint

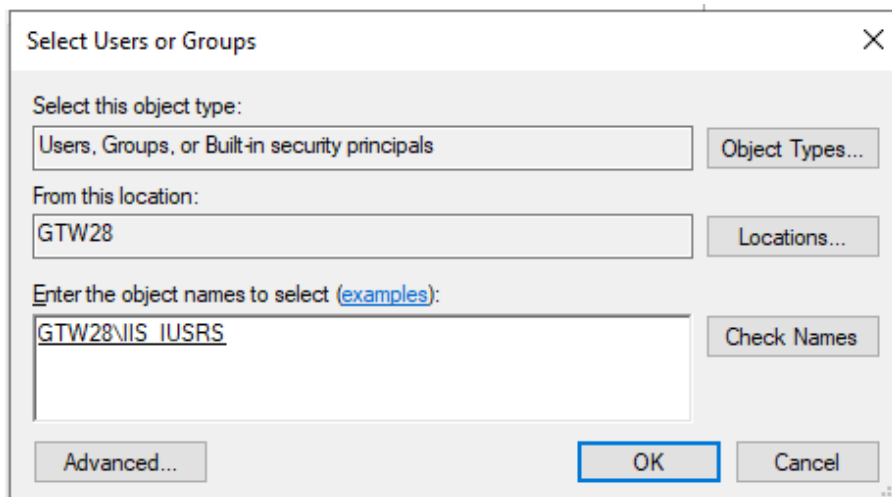
1. Add the certificate to your computer's personal storage.

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:
```

```
2     - ./core/events:/var/lib/axidian/axidian-privilege/events
3     - ./core/appsettings.json:/app/appsettings.json:ro
4     - ./keys/shared/protector:/etc/axidian/axidian-
privilege/keys/shared/protector:ro
5     - ./keys/core:/etc/axidian/axidian-privilege/keys/core:ro
6     - ./ca-certificates:/usr/local/share/ca-certificates:ro
7     - ./logs/core:/app/logs
8     - ./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\pam\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 Section

```
1 "IdentitySettings": {
2     ...
3     "SecondFaType": "TOTP",
4     ...
5 }
```

## SMTP Section

```
1 "Smtp": {
2     "Address": "PAM_SMTP_ADDRESS",
3     "Port": 587,
4     "SenderAddress": "PAM_SMTP_SENDER_ADDRESS",
5     "Username": "PAM_SMTP_USERNAME",
6     "Password": "",
7     "EncryptionMethod": "TLS"
8     "AllowedSslProtocols": "Tls12,Tls13"
9 }
```

- **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 SSH Proxy and RDP 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 [change the parameter value in the configuration file](#) and [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 — [restarting the access server](#).

### 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.

## 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 Pam.RdpProxy.Service --force-recreate
```

or

```
sudo docker-compose -f docker-compose.access-server.yml up -d Pam.RdpProxy.Service --force-recreate
```

## Example of Restarting the SSH Proxy Component

```
sudo docker compose -f docker-compose.access-server.yml up -d Pam.SshProxy.Service --force-recreate
```

or

```
sudo docker-compose -f docker-compose.access-server.yml up -d Pam.SshProxy.Service --force-recreate
```

# Integration with User Directories

This page describes how to set up Axidian Privilege integration with Active Directory, FreeIPA, OpenLDAP and ALD Pro 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:

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

## Path to the IdP configuration file:

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

## 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=PrivilegedAccounts,OU=Groups,DC=vdd,DC=com)
(memberOf=cn=Admins1,OU=PAMUsers,DC=vdd,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

```

1  "UserCatalog": {
2    "RootProvider": "ad1",
3    "Providers": {
4      "Ldap": [
5        {
6          "Id": "ad1",
7          "ConnectorType": "Ldap",
8          "LdapServerType": "ActiveDirectory",
9          "Domain": "axidian.test",
10         "Port": 636,
11         "AuthType": "Basic",
12         "SecureSocketLayer": true,
13         "ContainerPath": "OU=UsersPAM,DC=axidian,DC=test",
14         "CatalogFilter":
15         "memberOf=cn=SecurityGroup,OU=PAMUsers,DC=axidian,DC=test",
16         "UserName": "IPAMADReadOps@axidian.test",
17         "Password": "qwe123",
18         "UserMapRules": {
19           "Settings": [
20             {
21               "Category": "person",
22               "Class": "user"
23             }
24           ]
25         }
26       ]
27     }
28   }

```

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

```

1  {
2  "Id": "ad",
3  "ConnectorType": "Ldap",
4  "LdapServerType": "FreeIpa", // Replace with AldPro when setting to AldPro
5  "Domain": "ald.sup", // Name of the domain or specific controller
6  "Port": 389, // 389 for connecting via LDAP, 636 for connecting via LDAPS
7  "AuthType": "Basic",
8  "SecureSocketLayer": false, // false for connecting via LDAP, true for
   connecting via LDAPS
9  "ContainerPath": "dc=ald,dc=sup",
10 "UserName": "uid=pamread,cn=users,cn=accounts,dc=ald,dc=sup", // Domain access
   credentials. Must be in distinguishedName format, the account must have read
   permissions for the required attributes
11 "Password": "Q1w2e3r4", // Account password to access the domain
12 "GroupMapRules": {
13   "Settings": [
14     {
15       "Category": "",
16       "Class": "ipantgroupattrs"
17     }
18   ],
19   "Attributes": {
20     "Id": "ipaUniqueID",
21     "Name": "cn",
22     "SamAccountName": "cn",
23     "CanonicalName": "cn",
24     "DistinguishedName": "entryDn",
25     "SidBytes": "ipaNTSecurityIdentifier"
26   }
27 },
28 "UserMapRules": {
29   "Settings": [
30     {
31       "Category": "",
32       "Class": "person"

```

```

33     }
34 ],
35   "Attributes": {
36     "Id": "ipaUniqueID",
37     "Name": "cn",
38     "PrincipalName": "krbPrincipalName",
39     "SamAccountName": "uid",
40     "DistinguishedName": "entryDn",
41     "SidBytes": "ipaNTSecurityIdentifier",
42     "ThumbnailPhoto": "jpegPhoto",
43     "JpegPhoto": "jpegPhoto"
44   }
45 }
46 }

```

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`

### ▼ Example of the UserCatalog section for OpenLDAP user directory

```

1 {
2   "Id": "oldap",
3   "ConnectorType": "Ldap",
4   "LdapServerType": "OpenLdap",
5   "Domain": "oldap.local", // Name of the domain or specific controller
6   "Port": 389, // 389 for connecting via LDAP, 636 for connecting via LDAPS
7   "AuthType": "Basic",
8   "SecureSocketLayer": false, // false for connecting via LDAP, true for
   connecting via LDAPS

```

```

9   "ContainerPath": "DC=oldap,DC=local",
10  "UserName": "cn=IPAMADReadOps,dc=oldap,dc=local", // Domain access credentials.
    Must be in distinguishedName format, the account must have read permissions for the
    required attributes
11  "Password": "QWEqwe123", // Account password to access the domain
12  "GroupMapRules": {
13    "Settings": [
14      {
15        "Category": "",
16        "Class": "groupOfUniqueNames"
17      }
18    ],
19    "Attributes": {
20      "Name": "cn",
21      "SamAccountName": "cn",
22      "CanonicalName": "cn",
23      "DistinguishedName": "entryDn",
24      "Members": "uniqueMember"
25    }
26  },
27  "UserMapRules": {
28    "Settings": [
29      {
30        "Category": "",
31        "Class": "inetOrgPerson"
32      }
33    ],
34    "Attributes": {
35      "Name": "cn",
36      "SamAccountName": "uid",
37      "DistinguishedName": "entryDn",
38      "ThumbnailPhoto": "photo",
39      "JpegPhoto": "photo"
40    }
41  }
42 }

```

## 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 multiple user directories

```
1  "UserCatalog": {
2      "RootProvider": "orUCP",
3      "Providers": {
4          "Ldap": [
5              {
6                  "Id": "ad",
7                  "ConnectorType": "Ldap",
8                  "LdapServerType": "ActiveDirectory",
9                  "Domain": "axidian.test",
10                 "Port": 636,
11                 "AuthType": "Basic",
12                 "SecureSocketLayer": true,
13                 "ContainerPath": "OU=UsersPAM,DC=axidian,DC=test",
14                 "UserName": "IPAMADReadOps@axidian.test",
15                 "Password": "qwe123",
16                 "UserMapRules": {
17                     "Settings": [
18                         {
19                             "Category": "person",
20                             "Class": "user"
21                         }
22                     ]
23                 }
24             },
25             {
26                 "Id": "ad2",
27                 "ConnectorType": "Ldap",
28                 "LdapServerType": "ActiveDirectory",
29                 "Domain": "axidian.test",
30                 "Port": 636,
31                 "AuthType": "Basic",
32                 "SecureSocketLayer": true,
33                 "ContainerPath": "OU=UsersPAM,DC=axidian,DC=test",
34                 "UserName": "IPAMADReadOps@axidian.test",
```

```
35     "Password": "qwe123",
36     "UserMapRules": {
37         "Settings": [
38             {
39                 "Category": "person",
40                 "Class": "user"
41             }
42         ]
43     }
44 },
45 {
46     "Id": "ipa",
47     "ConnectorType": "Ldap",
48     "LdapServerType": "FreeIpa",
49     "Domain": "ipa.redos",
50     "Port": 389,
51     "AuthType": "Basic",
52     "SecureSocketLayer": false,
53     "ContainerPath": "DC=ipa,DC=redos",
54     "UserName": "uid=IPAMADReadOps,cn=users,cn=accounts,dc=ipa,dc=redos",
55     "Password": "qwe123",
56     "GroupMapRules": {
57         "Settings": [
58             {
59                 "Category": "",
60                 "Class": "ipantgroupattrs"
61             }
62         ],
63         "Attributes": {
64             "Name": "cn",
65             "SamAccountName": "cn",
66             "CanonicalName": "cn",
67             "DistinguishedName": "entryDn",
68             "SidBytes": "ipaNTSecurityIdentifier"
69         }
70     },
71     "UserMapRules": {
72         "Settings": [
73             {
74                 "Category": "",
75                 "Class": "person"
76             }
77         ],
78         "Attributes": {
79             "Name": "cn",
80             "PrincipalName": "krbPrincipalName",
```

```
81         "SamAccountName": "uid",
82         "DistinguishedName": "entryDn",
83         "SidBytes": "ipaNTSecurityIdentifier",
84         "ThumbnailPhoto": "jpegPhoto",
85         "JpegPhoto": "jpegPhoto"
86     }
87 }
88 }
89 ],
90 "Or": [
91     {
92         "Id": "orUCP",
93         "Providers": {
94             "ad": {"IgnoreExceptions": true},
95             "ad2": {"IgnoreExceptions": true},
96             "ipa": {"IgnoreExceptions": true}
97         }
98     }
99 ]
100 }
101 }
```



## 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

For additional system protection, it is recommended to encrypt the configuration files after final edits.

## Axidian Privilege Components Protection

The distribution kit includes the Configuration protector utility that located in the `..PAM_2.10.0\axidian-pam-windows\MISC\ConfigurationProtector\` folder.

The utility can encrypt the configuration files of the Core, IdP, ProxyApp and Log Server components.

Run the following commands to encrypt the corresponding configuration files:

- **Core** component:

```
Pam.Tools.Configuration.Protector protect --component Core --file  
C:\inetpub\wwwroot\pam\core\appsettings.json
```

- **IDP** component

```
Pam.Tools.Configuration.Protector protect --component Idp --file  
C:\inetpub\wwwroot\pam\idp\appsettings.json
```

- **Log Server** component

```
Pam.Tools.Configuration.Protector protect --component LogServer --file  
C:\inetpub\wwwroot\ls\targetConfigs\PamTargetDb.config
```

- **ProxyApp** component

```
Pam.Tools.Configuration.Protector protect --component ProxyApp --file "C:\Program  
Files\Axidian\Axidian Privilege\Gateway\ProxyApp\appsettings.json"
```

### ! INFO

These commands are provided for execution when deploying components on Windows.

When deploying components on Linux, the configuration files are encrypted automatically when the deployment script is executed.

To decrypt the configuration, run the command:

```
Pam.Tools.Configuration.Protector unprotect --file "c:\path\to\configuration\file"
```

## 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 in `%ProgramData%\Axidian\Axidian Privilege\Keys` folder.

Keys are encrypted using the Windows Data Protection API with binding to a computer. So, any user within a computer can encrypt or decrypt keys. If the Data Protection API encryption keys are not synchronized between the load balancer instances, then the configuration must be re-encrypted, since the instances will have different keys.

# 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 file `C:\Program Files\Axidian\Axidian Privilege\Gateway\ProcessCreateHook\processprotection.settings.json`

Example:

### `processprotection.settings.json`

```
1 {
2   "Rules": [
3     {
4       "Comment": "Common, record video",
5       "ParentProcessPaths": [
6         "C:\\Program Files\\Axidian\\Axidian
7         Privilege\\Gateway\\ProxyApp\\Pam.Proxy.App.exe"
8       ],
9       "ApplicationPaths": [
10        "C:\\Program Files\\Axidian\\Axidian
11        Privilege\\Gateway\\ProxyApp\\ffmpeg.exe",
```

```
10     "C:\\Program Files\\Axidian\\Axidian
Privilege\\Gateway\\ProxyApp\\ffprobe.exe"
11     ]
12     }
13 }
```

**Section Rules** — Rules for allowed processes.

Configuration 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 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.

Default configuration:

### filesprotection.settings.json

```
1 {
2   "VulnerableFiles": [
3     {
4       "Path": "C:\\Program Files\\Axidian\\Axidian
Privilege\\Gateway\\ProxyApp\\appsettings.json",
5       "AllowedProcesses": [
```

```

6         "C:\\Program Files\\Axidian\\Axidian
Privilege\\Gateway\\ProxyApp\\Pam.Proxy.App.exe"
7     ]
8 },
9 {
10     "Path": "C:\\ProgramData\\Axidian\\Axidian Privilege\\SessionTemp",
11     "AllowedProcesses": [
12         "C:\\Program Files\\Axidian\\Axidian
Privilege\\Gateway\\ProxyApp\\Pam.Proxy.App.exe",
13         "C:\\Program Files\\Axidian\\Axidian
Privilege\\Gateway\\SshClient\\Pam.Putty.exe",
14         "C:\\Windows\\System32\\mstsc.exe",
15         "C:\\Windows\\SysWOW64\\mstsc.exe"
16     ]
17 },
18 {
19     "Path": "C:\\ProgramData\\Axidian\\Axidian Privilege\\VideoTemp",
20     "AllowedProcesses": [
21         "C:\\Program Files\\Axidian\\Axidian
Privilege\\Gateway\\ProxyApp\\Pam.Proxy.App.exe",
22         "C:\\Program Files\\Axidian\\Axidian
Privilege\\Gateway\\ProxyApp\\ffmpeg.exe",
23         "C:\\Program Files\\Axidian\\Axidian
Privilege\\Gateway\\ProxyApp\\ffprobe.exe"
24     ]
25 }
26 ]
27 }

```

Configuration 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.

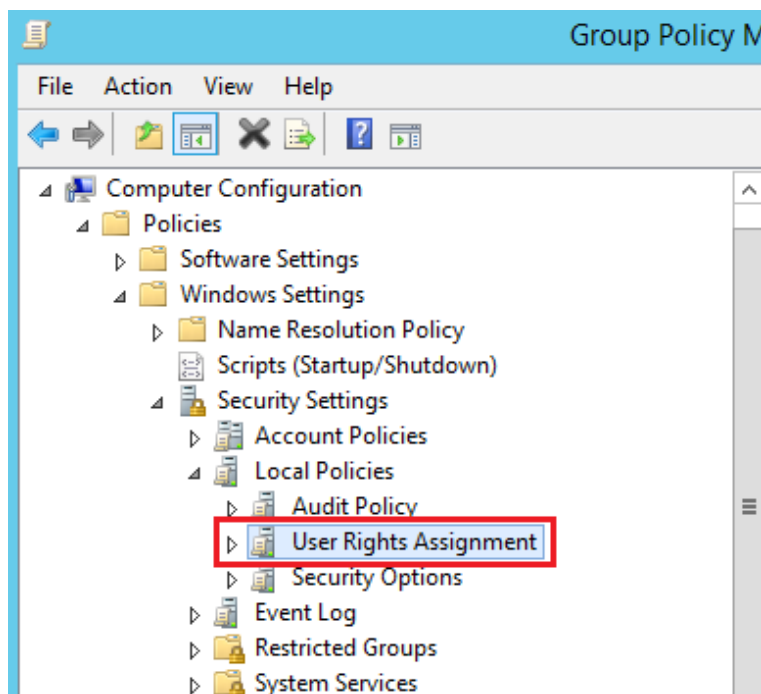
To ensure the security of footage, Axidian Privilege implements an encryption mechanism that allows you to safely store and use it within the solution. Encryption is performed using the AES256 algorithm, the key itself is unique for each Axidian Privilege session.

# 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
<p>Act as part of the operating system</p>	<p>This user right allows a process to impersonate any user without authentication. The process can thus access the same local resources as the user.</p> <p>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.</p> <p>Attention!</p> <p>Assigning this right to a user may pose a security risk. Assign such rights only to trusted users.</p>	<p>Undefined</p>
<p>Adjust memory quotas for a process</p>	<p>This privilege determines who can change the maximum amount of memory used by a process.</p> <p>This user right is defined in the default domain controller's Group Policy Object (GPO) and in the local workstation and server security policy.</p> <p>Note. This privilege is useful when configuring</p>	<p>NT AUTHORITY\NETWORK SERVICE, NT AUTHORITY\LOCAL SERVICE, BUILTIN\Administrators</p>

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	<p>This user right determines which users can override permissions on files, directories, the registry, and other persistent objects for the purpose of system backup.</p> <p>Specifically, this user right is similar to granting the following permissions to a user or group on all folders and files on the system:</p> <ul style="list-style-type: none"> <li>- Browse Folders/Execute Files</li> <li>- Folder Contents/Read Data</li> <li>- Reading attributes</li> <li>- Reading extended attributes</li> <li>- Reading Permissions</li> </ul> <p>Attention!</p> <p>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.</p>	BUILTIN\Administrators

Policy	Description	Values
Bypass traverse checking	<p>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.</p>	BUILTIN\Administrators, NT AUTHORITY\Authenticated Users, NT AUTHORITY\LOCAL SERVICE, NT AUTHORITY\NETWORK SERVICE
Change the system time	<p>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.</p>	BUILTIN\Administrators, NT AUTHORITY\LOCAL SERVICE
Change the time zone	<p>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.</p>	BUILTIN\Administrators, NT AUTHORITY\LOCAL SERVICE
Create a token object	<p>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.</p> <p>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.</p>	Undefined

Policy	Description	Values
	<p>Attention!</p> <p>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.</p>	
Create global objects	<p>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.</p> <p>Attention!</p> <p>Assigning this right to a user may pose a security risk. Assign it only to trusted users.</p>	BUILTIN\Administrators, NT AUTHORITY\SERVICE
Create permanent shared objects	<p>This user right controls which accounts can be used by processes to create a directory object using the Object Manager.</p> <p>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.</p>	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
	<p>Attention!</p> <p>Assign it only to trusted users. Symbolic links can expose vulnerabilities in applications that are not designed to handle them.</p>	
Debug programs	<p>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.</p> <p>Attention!</p> <p>Assigning this right to a user may pose a security risk. Assign it only to trusted users.</p>	BUILTIN\Administrators
Deny access to this computer from the network	<p>This security setting determines which users are denied access to the computer from the network. This setting replaces the <b>Allow access to this computer from the network</b> policy setting if both policies apply to the user account.</p>	BUILTIN\Guests
Deny log on as a batch job	<p>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.</p>	BUILTIN\Guests
Deny log on as a service	<p>This security setting determines which service accounts are denied to execute registration of</p>	BUILTIN\Guests

Policy	Description	Values
	<p>a process as a service. This policy setting replaces the "Allow logon as a service" setting if both options apply to the user account.</p> <p>Note. This security setting does not apply to the <i>System</i>, <i>Local Service</i>, or <i>Network Service</i> accounts.</p>	
Deny log on locally	<p>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.</p> <p>Attention!</p> <p>If this security setting is applied to the Everyone group, no one will be able to log on locally.</p>	BUILTIN\Guests
Deny log on through Terminal Services	<p>This security setting determines which users and groups are prohibited from logging on as a Remote Desktop Services client.</p>	BUILTIN\Guests
Enable computer and user accounts to be trusted for delegation	<p>This security setting determines which users can set the Delegation Allowed setting for a user or computer object.</p> <p>A user or object after getting this privilege will have write access to control flags of the user account or computer object. A server process running on a computer (or in a user context) that has delegation enabled can access the resources of another computer using the client's delegated credentials until the "Account cannot be delegated" control flag is</p>	BUILTIN\Administrators

Policy	Description	Values
	<p>set on the client account.</p> <p>This user right is defined in the default domain controller's Group Policy Object (GPO) and in the local workstation and server security policy.</p> <p>Attention!</p> <p>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.</p>	
Force shutdown from a remote system	<p>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.</p> <p>This user right is defined in the default domain controller's Group Policy Object (GPO) and in the local workstation and server security policy.</p>	BUILTIN\Administrators
Generate security audits	<p>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.</p>	NT AUTHORITY\LOCAL SERVICE, NT AUTHORITY\NETWORK SERVICE

Policy	Description	Values
	<p>For more information, see "Audit: Shut down system immediately if security audit logging cannot be logged".</p>	
<p>Impersonate a client after authentication</p>	<p>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.</p> <p>Attention!</p> <p>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.</p> <p>Additionally, a user can impersonate an access token if any of the following conditions are met:</p> <p>An impersonated access token is assigned to this user. In this login session, the user created an access token by explicitly</p>	<p>BUILTIN\Administrators, NT AUTHORITY\SERVICE</p>

Policy	Description	Values
	<p>providing login credentials. The requested level is lower than "Impersonate", for example: "Anonymous" or "Identify".</p> <p>Therefore, users generally do not need this user right.</p> <p>More information can be found by searching for <code>SelImpersonatePrivilege</code> in the Microsoft Platform SDK.</p> <p>Attention!</p> <p>Enabling this setting may cause programs that have this privilege to lose their Impersonate privilege and block their execution.</p>	
<p>Increase scheduling priority</p>	<p>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.</p>	<p>BUILTIN\Administrators</p>
<p>Load and unload device drivers</p>	<p>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.</p> <p>Attention!</p> <p>Assigning this right to a user may pose a</p>	<p>BUILTIN\Administrators</p>

Policy	Description	Values
	<p>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.</p>	
<p>Lock pages in memory</p>	<p>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).</p>	<p>Undefined</p>
<p>Log on as a batch job</p>	<p>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.</p> <p>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.</p>	<p>BUILTIN\Administrators</p>
<p>Manage auditing and security log</p>	<p>This security setting determines which users can specify object access audit settings for individual resources, such as files, Active Directory objects, and registry keys.</p> <p>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".</p> <p>Audit events can be viewed in the Event</p>	<p>BUILTIN\Administrators</p>

Policy	Description	Values
	<p>Viewer security log. A user with this privilege can also view and clear the security log.</p>	
<p>Modify an object label</p>	<p>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.</p>	<p>Undefined</p>
<p>Modify firmware environment values</p>	<p>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.</p> <p>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.</p> <p>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.</p> <p>On all computers, this user right is required to install and update Windows.</p> <p>Note. This security setting does not affect</p>	<p>BUILTINAdministrators</p>

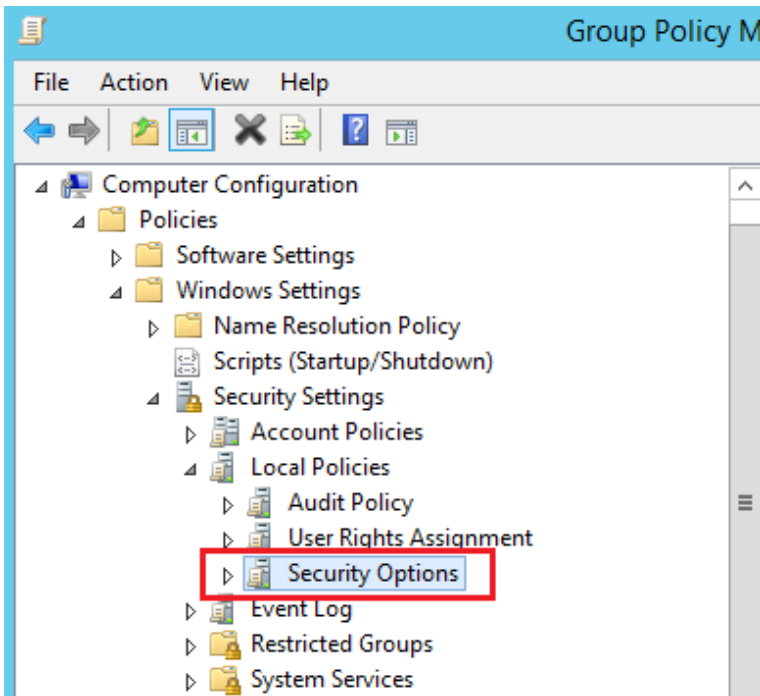
Policy	Description	Values
	<p>users who can change the system and user environment variables that appear on the Advanced tab of the System Properties dialog box. For information about how to change these variables, see Add or change the value of environment variables.</p>	
<p>Perform volume maintenance tasks</p>	<p>This security setting determines the users and groups that can perform volume maintenance tasks, such as remote defragmentation.</p> <p>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.</p>	<p>BUILTIN\Administrators</p>
<p>Profile single process</p>	<p>This security setting determines the users who can use performance monitoring tools to monitor the performance of non-system processes.</p>	<p>BUILTIN\Administrators</p>
<p>Profile system performance</p>	<p>This security setting determines the users who can use performance monitoring tools to monitor the performance of system processes.</p>	<p>BUILTIN\Administrators</p>
<p>Replace a process level token</p>	<p>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.</p>	<p>NT AUTHORITY\LOCAL SERVICE, NT AUTHORITY\NETWORK SERVICE</p>

Policy	Description	Values
Restore files and directories	<p>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.</p> <p>Specifically, this user right is similar to granting the following permissions to a user or group on all folders and files on the system:</p> <ul style="list-style-type: none"> <li>- Browse Folders/Execute Files</li> <li>-Write</li> </ul> <p>Attention!</p> <p>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.</p>	BUILTIN\Administrators
Shut down the system	<p>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.</p>	BUILTIN\Administrators
Take ownership of files or other objects	<p>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.</p> <p>Attention!</p>	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
<p>Accounts: Administrator account status</p>	<p>This security setting determines whether the local administrator account is enabled or disabled.</p> <p>Notes.</p> <p>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 <a href="#">Reset Your Password</a> overview.</p> <p>Disabling the administrator account may hinder maintenance in some circumstances.</p> <p>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.</p>	<p>Enabled</p>
<p>Accounts: Guest account status</p>	<p>This security setting determines whether the guest account is enabled or disabled.</p> <p>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.</p>	<p>Disabled</p>
<p>Accounts: Limit local account use of blank passwords to console logon only</p>	<p>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.</p> <p>Attention!</p>	<p>Enabled</p>

Policy	Description	Values
	<p>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.</p> <p>Notes.</p> <p>This setting has no effect if domain accounts are used to log in.</p> <p>Applications that use remote interactive logon can bypass this setting.</p>	

## Audit

### ▼ Description of policies

Policy	Description	Values
<p>Audit: Audit the use of Backup and Restore privilege</p>	<p>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.</p> <p>If this security setting is disabled, backup and restore privilege usage is not audited even if the "Audit privilege usage" option is enabled.</p> <p>Note. In versions of Windows earlier than Vista, changes made by configuring this security setting will not take effect until you restart</p>	<p>Enabled</p>

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	<p>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.</p> <p>Notes.</p> <p>This setting does not affect the ability to add a local printer. This setting does not affect administrators.</p>	Enabled
Devices: Restrict CD-ROM access to locally logged-on user only	<p>This security setting determines whether the CD drive is accessible to both local and remote users.</p> <p>When enabled, access to CDs is limited to users who are logged on interactively. If this option is enabled and no one is</p>	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	<p>This security setting determines whether a removable floppy drive can be accessed by both local and remote users.</p> <p>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.</p>	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	<p>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.</p> <p>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.</p> <p>If this policy is disabled, pressing CTRL+ALT+DEL is required for any user before logging on to Windows.</p>	Disabled

Policy	Description	Values
<p>Interactive logon: Number of previous logons to cache (in case domain controller is not available)</p>	<p>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".</p> <p>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.</p> <p>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.</p>	<p>0 logons</p>
<p>Interactive logon: Require Domain Controller authentication to unlock workstation</p>	<p>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.</p>	<p>Enabled</p>

## Microsoft Network Client

▼ Description of policies

Policy	Description	Values
Microsoft network client: Send unencrypted password to third-party SMB servers	<p>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.</p> <p>Sending unencrypted passwords poses a security risk.</p>	Disabled

## Network Access

### ▼ Description of policies

Policy	Description	Values
Network access: Allow anonymous SID/Name translation	<p>This policy setting determines whether an anonymous user can query another user's security identifier (SID) attributes.</p> <p>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).</p> <p>If this policy setting is disabled, an anonymous user cannot request another user's SID.</p>	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	<p>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.</p> <p>This security setting allows you to place additional restrictions on anonymous connections.</p> <p>Enabled: Do not allow enumeration of SAM accounts. This setting replaces the <b>Everyone</b> setting with the <b>Authenticated</b> in security permissions for resources.</p> <p>Disabled: No additional restrictions. Default permissions are used.</p>	
<p>Network access: Do not allow anonymous enumeration of SAM accounts and shares</p>	<p>This security setting determines whether anonymous users are allowed to enumerate SAM accounts and shares.</p> <p>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.</p>	Enabled
<p>Network access: Do not allow storage of passwords and credentials for network authentication</p>	<p>This security setting determines whether Credential Manager stores passwords and credentials during domain authentication (for later use).</p> <p>If this setting is enabled, Credential Manager does not save passwords and credentials on this computer.</p> <p>If this policy setting is disabled or not set, Credential Manager will store passwords and credentials on this</p>	Enabled

Policy	Description	Values
	<p>computer (for future use during domain authentication).</p> <p>Note. Changes to the configuration of this security setting will take effect only after you restart Windows.</p>	
<p>Network access: Let Everyone permissions apply to anonymous users</p>	<p>This security setting determines what additional permissions are given to anonymous connections to your computer.</p> <p>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.</p> <p>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.</p>	<p>Disabled</p>
<p>Network access: Named Pipes that can be accessed anonymously</p>	<p>This security setting determines which communication sessions (channels) will have attributes and permissions that allow anonymous access.</p>	<p>Undefined</p>
<p>Network access: Remotely accessible registry paths</p>	<p>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.</p>	<p>Undefined</p>

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	<p>When enabled, this security setting restricts anonymous access to shares and named pipes based on the following settings:</p> <ul style="list-style-type: none"> <li>- Network access: Allow anonymous access to named pipes</li> <li>- Network access: Allow anonymous access to shared resources</li> </ul>	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	<p>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.</p> <p>By default on domain computers: Normal.</p>	Classic - local users authenticate as themselves

Policy	Description	Values
	<p>By default on standalone computers: Guest.</p> <p>Attention!</p> <p>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.</p> <p>Note. This setting does not affect interactive logon operations that are performed remotely by using services such as Telnet or Remote Desktop Services.</p>	

## 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	<p>logon time that is configured for their account. This setting affects the Server Message Block (SMB) component.</p> <p>When this policy is enabled, client sessions with the SMB server are forced to terminate after the client logon timeout expires.</p> <p>If this policy is disabled, the client's session is retained after the client's login timeout expires.</p> <p>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.</p>	
Network security: LAN Manager authentication level	<p>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.</p> <p>Send LM and NTLM responses: Clients use LM and NTLM authentication and never use NTLMv2 session security; Domain controllers accept LM, NTLM, and NTLMv2</p>	Send NTLMv2 response only. Refuse LM & NTLM

Policy	Description	Values
	<p>authentication.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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).</p> <p>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).</p>	
<p>Network security: Minimum session security for NTLM SSP based (including secure RPC) clients</p>	<p>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:</p> <p>Require NTLMv2 session security. If the NTLMv2 protocol is not negotiated, the connection will not be established.</p>	<p>Require NTLMv2 session security: Enabled</p> <p>Require 128-bit encryption: Enabled</p>

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	<p>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:</p> <p>Require NTLMv2 session security. If message integrity is not consistent, the connection will not be established.</p> <p>Require 128-bit encryption. If 128-bit encryption is not negotiated, the connection will not be established.</p>	<p>Require NTLMv2 session security: Enabled</p> <p>Require 128-bit encryption: Enabled</p>

## Shutdown

### ▼ Description of policies

Policy	Description	Values
Shutdown: Allow system to be shut down without having to log on	<p>This security setting determines whether you can shut down your computer without logging on to Windows.</p> <p>If this policy is enabled, the Shutdown option can be selected on the Windows logon screen.</p> <p>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.</p>	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	<p>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.</p> <p>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.</p>	

## 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	<p>This policy setting determines the administrator approval behavior characteristics of the built-in administrator account.</p> <p>Possible values:</p> <p>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.</p> <p>Disabled (default). The built-in Administrator account runs all applications with full Administrator rights.</p>	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	<p>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.</p> <p>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.</p>	
User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode	<p>This policy setting controls the behavior of the privilege elevation prompt for administrators.</p> <p>Possible values:</p> <p>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.</p> <p>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.</p> <p>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</p>	Prompt for consent for non-Windows binaries

Policy	Description	Values
	<p>continues with the user's maximum available privileges.</p> <p>For any operation that requires elevation of privileges, you are prompted to enter the user name and password for the administrator account. If valid credentials are entered, the operation continues with appropriate privileges.</p> <p>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.</p> <p>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.</p>	
<p>User Account Control: Behavior of the elevation prompt for standard users</p>	<p>This policy setting determines the behavior of the privilege escalation prompt for standard users.</p> <p>Possible values:</p> <p>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.</p> <p>Automatically reject requests to escalate privileges.</p>	<p>Prompt for credentials on the secure desktop</p>

Policy	Description	Values
	<p>When an operation requires elevation of privileges, an access denied error message is displayed.</p> <p>Organizations whose desktop computers are used by standard users can select this policy setting to reduce the number of support calls.</p> <p>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.</p>	
<p>User Account Control: Only elevate UIAccess applications that are installed in secure locations</p>	<p>User Account Control: Elevate privileges only for UIAccess applications installed in a secure location.</p> <p>This policy setting determines whether applications that request execution at the UIAccess integrity level must reside in a secure folder on the file system.</p> <p>Only the following folders are considered safe:</p> <ul style="list-style-type: none"> <li>- ...\.Program Files\, including subfolders</li> <li>- ...\.Windows\system32\</li> <li>- ...\.Program Files (x86)\, including subfolders for 64-bit versions of Windows</li> </ul> <p>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.</p> <p>Possible values:</p> <p>Enabled (default). The application will only run with the UIAccess integrity level if it is located in a secure</p>	<p>Enabled</p>

Policy	Description	Values
	<p>folder on the file system.</p> <p>Disabled. The application will run with the UIAccess integrity level even if it is not in a secure file system folder.</p>	
<p>User Account Control: Run all administrators in Admin Approval Mode</p>	<p>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.</p> <p>Possible values:</p> <p>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.</p> <p>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.</p>	<p>Enabled</p>
<p>User Account Control: Switch to the secure desktop when prompting for elevation</p>	<p>This policy setting determines whether elevation prompts are displayed on the user's interactive desktop or on the secure desktop.</p> <p>Possible values:</p> <p>Enabled (default). All elevation requests are displayed on the secure desktop, regardless of the prompt behavior policy settings for administrators and</p>	<p>Enabled</p>

Policy	Description	Values
	<p>standard users.</p> <p>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.</p>	
User Account Control: Virtualize file and registry write failures to per-user locations	<p>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.</p> <p>Possible values:</p> <p>Enabled (default). Application write failures are redirected at runtime to user-defined locations in the file system and registry.</p> <p>Disabled. Applications that write data to secure locations fail with an error.</p>	Enabled

## Other

▼ Description of policies

---

Policy	Description	Values
Accounts: Block Microsoft accounts	<p>This policy setting prevents users from adding new Microsoft accounts on this computer.</p> <p>If you select the "Users can't add Microsoft accounts" option,</p>	Users can't add Microsoft accounts

Policy	Description	Values
	<p>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.</p> <p>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.</p> <p>If this policy is disabled or not configured (recommended), users will be able to use Microsoft accounts in Windows.</p>	
<p>Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings</p>	<p>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.</p> <p>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.</p>	<p>Enabled</p>
<p>Domain member: Disable machine account password changes</p>	<p>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</p>	<p>Disabled</p>

Policy	Description	Values
	<p>every 30 days.</p> <p>Default: Disabled.</p> <p>Notes.</p> <p>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.</p> <p>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.</p>	
<p>Domain member: Maximum machine account password age</p>	<p>This security setting determines how often a domain member will attempt to change the computer account password.</p>	<p>30 days</p>
<p>Domain member: Require strong (Windows 2000 or later) session key</p>	<p>This security setting determines whether secure channel encrypted data requires a 128-bit key.</p> <p>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.</p> <p>Depending on the version of Windows used on the domain controller with which the connection is made, as well as on the parameter values:</p>	<p>Enabled</p>

Policy	Description	Values
	<p>Domain Member: Digital signature or encryption of secure channel data is always required.</p> <p>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.</p> <p>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.</p>	
<p>Interactive logon: Display user information when the session is locked</p>	<p>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.</p> <p>Changes in Windows 10 version 1607</p> <p>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.</p> <p>This Group Policy setting defines this same functionality.</p> <p>Possible values:</p>	<p>User display name only</p>

Policy	Description	Values
	<p>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.</p> <p>Username Only: Displays the full name of the user who locked the session.</p> <p>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.</p> <p>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.</p> <p>Hotfix for Windows 10 version 1607</p> <p>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.</p> <p>Interaction with the "Prevent user from displaying account</p>	

Policy	Description	Values
	<p>information on login screen" command.</p> <p>In all versions of Windows 10, only the username is displayed by default.</p> <p>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.</p> <p>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.</p> <p>Recommendations.</p> <p>Whether you can enforce this policy depends on your security requirements for the login credentials displaying. If you work with computers that store sensitive information and have monitors in unsecured locations, or if your computers with sensitive information are accessed remotely, displaying the full names of logged-in users or domain account names may be against your overall security policy. Based on your security policy, it may be appropriate to set the value to "Interactive logon: Do not display last user's credentials."</p>	
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
	<p>console. Make sure the appropriate access recovery policies are enabled.</p> <p>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.</p> <p>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.</p>	
<p>Microsoft network server: Amount of idle time required before suspending session</p>	<p>This security setting determines how long an SMB session can elapse before it is suspended due to inactivity.</p> <p>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.</p> <p>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.</p> <p>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.</p>	<p>15 minutes</p>
<p>Microsoft network server: Attempt S4U2Self to obtain claim information</p>	<p>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</p>	<p>Disabled</p>

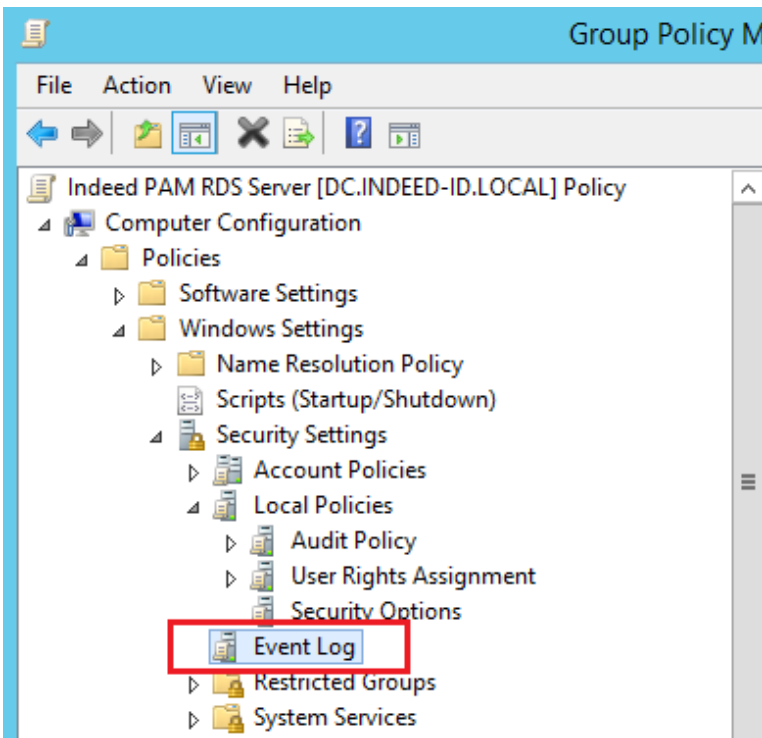
Policy	Description	Values
	<p>whose accounts are in a domain with client computers and domain controllers running an operating system that was released before Windows 8.</p> <p>This setting should be set to Automatic (the default) so that the file server can automatically determine whether a user is required to enroll. This setting should only be explicitly set to Enabled if you have local file access policies that include user access claims.</p> <p>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.</p> <p>If this setting is disabled, Windows File Server will not attempt to obtain a claims-based access token for the client principal.</p>	
<p>Microsoft network server: Disconnect clients when logon hours expire</p>	<p>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.</p> <p>When enabled, client sessions with the SMB service are forced to terminate after the client's allowed logon time has expired.</p> <p>If this setting is disabled, the client's session is saved after the client's allowed login time has expired.</p>	<p>Enabled</p>
<p>Microsoft network server: Server</p>	<p>This policy setting controls the level of verification that the folder or printer shares computer (server) performs on the</p>	<p>Off</p>

Policy	Description	Values
SPN target name validation level	<p>service principal name provided by the client computer when it establishes a session using the SMB protocol.</p> <p>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.</p> <p>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.</p> <p>Parameters:</p> <p>Disabled - The SMB client SPN is not required (not checked) by the SMB server.</p> <p>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.</p> <p>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.</p>	
Recovery console: Allow automatic administrative logon	<p>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.</p>	Disabled

Policy	Description	Values
<p>Recovery console: Allow floppy copy and access to all drives and all folders</p>	<p>When you enable this security setting, the Recovery Console SET command is available and allows you to set the following Recovery Console environment variables.</p> <p>AllowWildCards: allows wildcards to be used for some commands (such as the DEL command).</p> <p>AllowAllPaths: allows access to any files and folders on the computer.</p> <p>AllowRemovableMedia: allows you to copy files to removable media, such as floppy disks.</p> <p>NoCopyPrompt: cancels the warning when overwriting existing files.</p>	<p>Disabled</p>

## Event Log

Computer Configuration → Policies → Windows Settings → Security Settings → Event Log



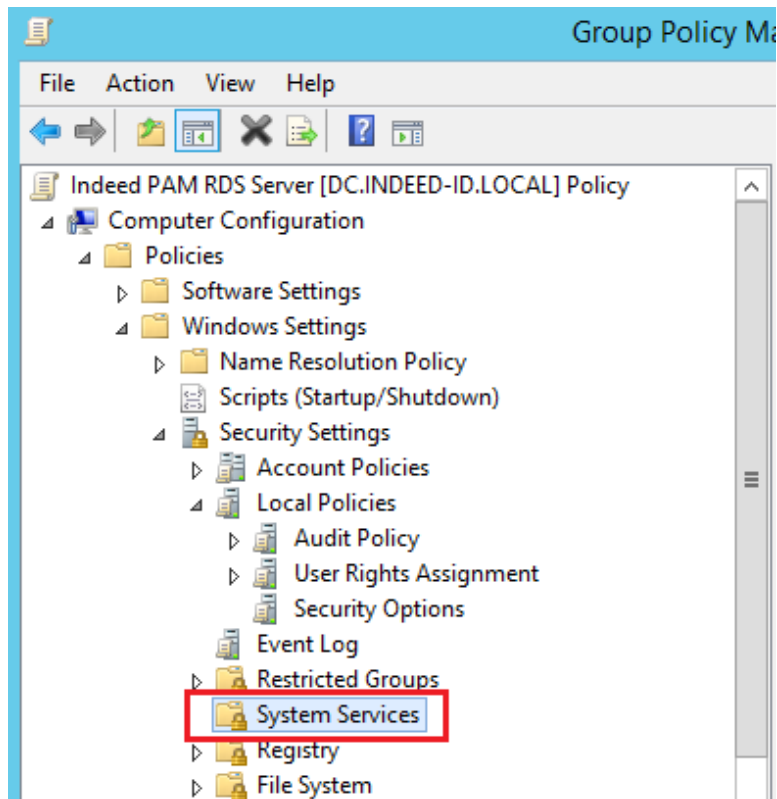
▼ Description of policies

Policy	Description	Values
Maximum application log size	<p>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).</p> <p>Notes.</p> <p>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.</p> <p>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.</p>	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	<p>This security setting determines whether guests are denied to access to the application event log.</p> <p>Notes.</p> <p>This setting is not included in the local computer policy object.</p>	Enabled
Prevent local guests group from accessing security log	<p>This security setting determines whether guests are denied to access to the security event log.</p> <p>Notes.</p> <p>This setting is not included in the local computer policy object.</p>	Enabled
Prevent local guests group from accessing system log	<p>This security setting determines whether guests are denied to access to the security event log.</p> <p>Notes.</p> <p>This setting is not included in the local computer policy object.</p>	Enabled
Retention method for application log	<p>This security setting determines how the application log is rewritten.</p> <p>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.</p>	As needed

Policy	Description	Values
	<p>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.</p> <p>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.</p> <p>Note. This setting is not included in the local computer policy object.</p>	
Retention method for security log	<p>This security setting determines how the security log is overwritten.</p> <p>Notes.</p> <p>This setting is not included in the local computer policy object.</p> <p>To access the security log, the user must have the Manage Audit and Security Log privilege.</p>	As needed
Retention method for system log	<p>This security setting determines how the system log is overwritten.</p> <p>Note. This setting is not included in the local computer policy object.</p>	As needed

## 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

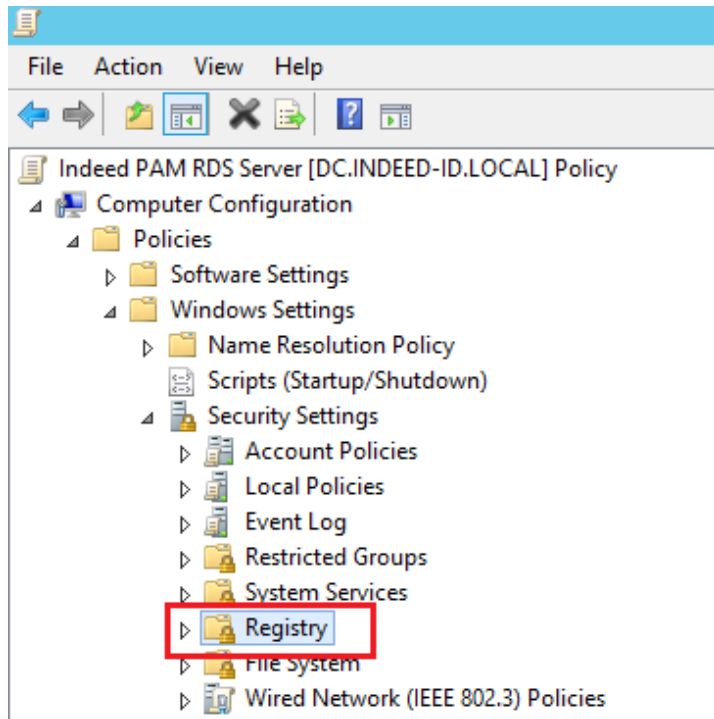
### Auditing

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

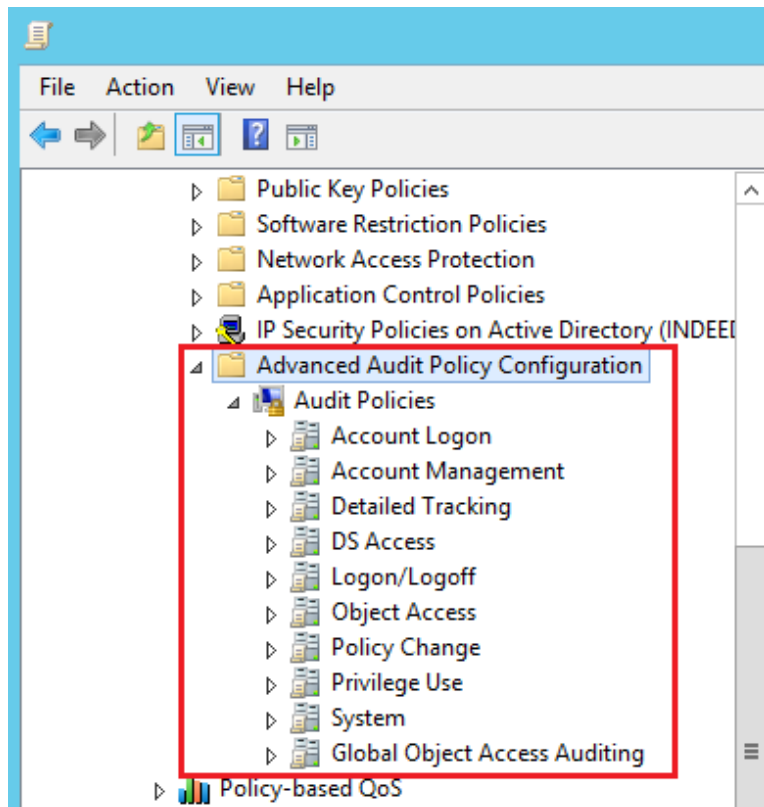
Inheritance disabled

### 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	<p>This policy setting allows you to audit events that occur when validating the login credentials of a user account.</p> <p>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.</p>	Success, Failure
Audit Other Account Logon Events	<p>Other account login events.</p> <p>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.</p>	Success, Failure

## Account Management

### ▼ Description of policies

Policy	Description	Values
Audit Application Group Management	<p>This policy setting allows you to audit events that occur when you make the following changes to application groups:</p> <p>Create, edit, or delete an application group.</p> <p>Add or remove a member to an application group.</p>	Success, Failure
Audit Computer Account Management	<p>This policy setting allows you to audit events that occur when computer accounts are modified, such as when they are created, modified, or deleted.</p>	Success, Failure

Policy	Description	Values
<p>Audit Distribution Group Management</p>	<p>This policy setting allows you to audit events that occur when you make the following changes to distribution groups:</p> <p>Create, edit, or delete a distribution group.</p> <p>Add a member to or remove a member from a distribution group.</p> <p>Change the distribution group type.</p> <p>Note. Events in this subcategory are logged only on domain controllers.</p>	<p>Success, Failure</p>
<p>Audit Other Account Management Events</p>	<p>This policy setting allows you to audit events that occur when other user account changes are made that are not listed in this category:</p> <p>Accessing the password hash for a user account. This operation is typically performed when migrating passwords using the Active Directory management tool.</p> <p>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.</p> <p>Changes the default domain group policy to the following group policy paths:</p> <p>Computer Configuration\Windows Settings\Security Options\Account Policies&gt;Password Policies</p> <p>Computer Configuration\Windows Settings\Security Options\Account Settings\Account Lockout Policy</p> <p>Note. A security audit event is logged when the policy setting</p>	<p>Success, Failure</p>

Policy	Description	Values
	is applied. No events are logged while parameters are changed.	
Audit Security Group Management	<p>This policy setting allows you to audit events that occur when the following security group changes are made:</p> <p>Create, edit, or delete a security group.</p> <p>Add a member to or remove a member from a security group.</p> <p>Changing the group type.</p>	Success, Failure
Audit User Account Management	<p>This policy setting allows you to audit changes made to user accounts. The following events are monitored:</p> <p>Create, edit, delete, rename, disable, enable, block and unblock accounts.</p> <p>Set or change the user account password.</p> <p>Adds a security identifier (SID) to the user account SID log.</p> <p>Set a password for Directory Services Restore mode.</p> <p>Change permissions for administrator accounts.</p> <p>Archive or restore Credential Manager credentials.</p>	Success, Failure

## Logon/Logoff

### ▼ Description of policies

Policy	Description	Values
Audit Account Lockout	<p>This policy setting allows you to audit events generated when a logon attempt to a locked account fails.</p> <p>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.</p> <p>Login events are important for understanding user activity and detecting possible attacks.</p>	Success, Failure
Audit Logoff	<p>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.</p> <p>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.</p> <p>If this policy setting is not configured, no audit events are raised when the logon session is closed.</p>	Success, Failure
Audit Logon	<p>This policy setting allows you to audit events that occur when you attempt to log on using a user account.</p> <p>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.</p>	Success, Failure

Policy	Description	Values
	<p>The following events are monitored:</p> <p>Successful login attempts.</p> <p>Failed login attempts.</p> <p>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.</p> <p>Denying logins as a result of security identifier (SID) filtering.</p>	
Audit Network Policy Server	<p>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.</p> <p>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.</p>	Success, Failure
Audit Other Logon/Logoff Events	<p>This policy setting allows you to audit other logon and logout events that are not covered by the Logon/Logout policy setting, for example:</p> <p>Ending Terminal Services sessions.</p> <p>Creating new Terminal Services sessions.</p> <p>Locking and unlocking a workstation.</p> <p>Calling up the screensaver.</p>	Success, Failure

Policy	Description	Values
	<p>Disabling the screensaver.</p> <p>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.</p> <p>Granting access to a wireless network to a user or computer account.</p> <p>Granting access to a wired 802.1x network to a user or computer account.</p>	
Audit Special Logon	<p>This policy setting allows you to audit events that occur when you perform special logon operations such as the following:</p> <p>Using a special login, that is, a login with rights similar to an administrator's, which can be used to elevate a process.</p> <p>Special group member login.</p> <p>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.</p>	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
	<p>the Windows audit APIs.</p> <p>The following events in this subcategory are monitored:</p> <p>Creating the application client context.</p> <p>Deleting the application client context.</p> <p>Initializing the application client context.</p> <p>Other application operations using Windows auditing APIs.</p>	
<p>Audit Certification Services</p>	<p>This policy setting provides auditing of Active Directory Certificate Services (AD CS) operations.</p> <p>AD CS operations include the following:</p> <p>Starting, shutting down, backing up, and restoring AD CS services.</p> <p>Changing the certificate revocation list (CRL).</p> <p>Requesting for new certificates.</p> <p>Issuing a certificate.</p> <p>Revocation of a certificate.</p> <p>Changing certificate manager settings for AD CS.</p> <p>Changing AD CS services configuration.</p> <p>Changing the Certificate Services template.</p> <p>Importing a certificate.</p> <p>Publishing a CA certificate to Active Directory Domain Services.</p> <p>Changing security permissions for AD CS services.</p> <p>Archiving the key.</p> <p>Importing a key.</p> <p>Removing the key.</p> <p>Starting the OCSP response service.</p> <p>Stopping the OCSP response service.</p>	<p>Success, Failure</p>
<p>Audit Detailed File Share</p>	<p>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</p>	<p>Failure</p>

Policy	Description	Values
	<p>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.</p> <p>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.</p> <p>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.</p>	
Audit File Share	<p>This policy setting allows you to audit attempts to access public folders.</p> <p>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.</p> <p>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.</p>	Success, Failure
Audit File System	<p>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.</p> <p>Note. To set a SACL for a file system object, use the Security tab of the object's Properties dialog box.</p>	Success, Failure

Policy	Description	Values
Audit Kernel Object	<p>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).</p> <p>Note. Auditing: The default SACLs for kernel objects are controlled by the Global System Objects access audit setting.</p>	Success, Failure
Audit Registry	<p>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.</p> <p>Note. To set a SACL for a registry object, use the Permissions dialog box.</p>	Success, Failure
Audit Removable Storage	<p>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.</p>	Success
Audit SAM	<p>This policy setting audits events that occur when you attempt to access Security Accounts Manager (SAM) objects. SAM objects include the following:</p> <ul style="list-style-type: none"> <li>SAM_ALIAS – local group.</li> <li>SAM_GROUP – a group that is not local.</li> <li>SAM_USER – user account.</li> <li>SAM_DOMAIN – domain.</li> <li>SAM_SERVER – computer account.</li> </ul> <p>Note. You can only change the system access control list (SACL) for the SAM_SERVER object.</p>	Success, Failure

## Policy Change

### ▼ Description of policies

Policy	Description	Values
Audit Audit Policy Change	<p>This policy setting allows you to audit changes to security audit policy settings, such as the following:</p> <ul style="list-style-type: none"><li>Set permissions and audit settings for an audit policy object.</li><li>Changes in system audit policy.</li><li>Logging security event sources.</li><li>Unregistration of security event sources.</li><li>Changes to audit settings for individual users.</li><li>Changes in the CrashOnAuditFail parameter value.</li><li>Changes to the system access control list for a file system or registry object.</li><li>Changes to the list of special groups.</li></ul> <p>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.</p>	Success, Failure
Audit Authentication Policy Change	<p>This policy setting allows you to audit events that occur when you make changes to security groups, such as the following:</p> <ul style="list-style-type: none"><li>Create trusts for a forest or domain.</li><li>Change trust relationships for a forest or domain.</li><li>Remove trusts for a forest or domain.</li><li>Changes to the Kerberos policy in the following path: Computer Configuration\Windows Settings\Security Options\Account Policies\Kerberos Policy.</li><li>Grant a user or group the following privileges:<ul style="list-style-type: none"><li>Access to a computer from the network.</li></ul></li></ul>	Success, Failure

Policy	Description	Values
	<p>Local input.</p> <p>Logging in using Terminal Services.</p> <p>Logging in using a batch job.</p> <p>Login to the service.</p> <p>There is a namespace conflict (for example, if the name of the new trust is the same as the name of an existing namespace).</p> <p>Note. A security audit event is logged when the policy setting is applied. No events are logged while parameters are changed.</p>	
<p>Audit Authorization Policy Change</p>	<p>This policy setting allows you to audit events that occur when authorization policy changes are made, such as the following:</p> <p>Assigning privileges to users, such as SeCreateTokenPrivilege, that are not audited in the "Change Authentication Policy" subcategory.</p> <p>Removing user privileges, such as SeCreateTokenPrivilege, that are not audited under the "Change Authentication Policy" subcategory.</p> <p>Encrypting File System (EFS) policy changes.</p> <p>Changes to object resource attributes.</p> <p>Changes to the centralized access policy (CAP) applied to an object.</p>	<p>Success, Failure</p>
<p>Audit Filtering Platform Policy Change</p>	<p>This policy setting allows you to audit events that occur when Windows Filtering Platform (WFP) changes are made, such as the following:</p> <p>IPsec service status.</p> <p>Changes to IPsec policy settings.</p> <p>Changes to Windows Firewall policy settings.</p> <p>Changes to suppliers and WFP module.</p>	<p>Success, Failure</p>

Policy	Description	Values
Audit MPSSVC Rule-Level Policy Change	<p>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:</p> <ul style="list-style-type: none"> <li>Messages from active policies when the Windows Firewall service starts.</li> <li>Changes to Windows Firewall rules.</li> <li>Changes to the Windows Firewall exceptions list.</li> <li>Changes to Windows Firewall settings.</li> <li>Rules are skipped or not enforced by the Windows Firewall service.</li> <li>Changes to Windows Firewall Group Policy settings.</li> </ul>	Success, Failure

## Privilege Use

### ▼ Description of policies

Policy	Description	Values
Audit Non Sensitive Privilege Use	<p>This policy setting provides auditing of events that occur when privileges that do not affect sensitive data (user privileges) are used. Using the following privileges does not affect sensitive data:</p> <ul style="list-style-type: none"> <li>Access the Credential Manager as a trusted caller.</li> <li>Access to a computer from the network.</li> <li>Adding workstations to a domain.</li> <li>Setting memory quotas for a process.</li> <li>Local login.</li> <li>Login through Terminal Services.</li> <li>Bypass cross-validation.</li> <li>Changing the system time.</li> <li>Creating a swap file.</li> </ul>	Success, Failure

Policy	Description	Values
	<p>Creating global objects.</p> <p>Creating permanent shared objects.</p> <p>Creating symbolic links.</p> <p>Access to the computer from the network is denied.</p> <p>Login as a batch job is denied.</p> <p>Login as a service is denied.</p> <p>Local login is denied.</p> <p>Login through Terminal Services is denied.</p> <p>Force remote shutdown.</p> <p>Increasing the working set of a process.</p> <p>Increasing execution priority.</p> <p>Locking pages in memory.</p> <p>Login in as a batch job.</p> <p>Login as a service.</p> <p>Changing the object's label.</p> <p>Performing volume maintenance tasks.</p> <p>Profiling a single process.</p> <p>System performance profiling.</p> <p>Disconnecting the computer from the docking station.</p> <p>Shutting down the system.</p> <p>Directory service data synchronization.</p>	
<p>Audit Sensitive Privilege Use</p>	<p>This policy setting audits events that occur when rights are used that affect sensitive data (user rights) as follows:</p> <p>Call a privileged service.</p> <p>Call one of the following privileges:</p> <p>Action on behalf of an operating system component.</p> <p>Archiving files and directories.</p> <p>Creating a token object.</p> <p>Debugging programs.</p> <p>Enable computer and user accounts that are allowed to delegate.</p> <p>Creating a security audit.</p> <p>Impersonate the client after authentication.</p> <p>Loading and unloading device drivers.</p> <p>Audit and security log management.</p>	<p>Failure</p>

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

## System

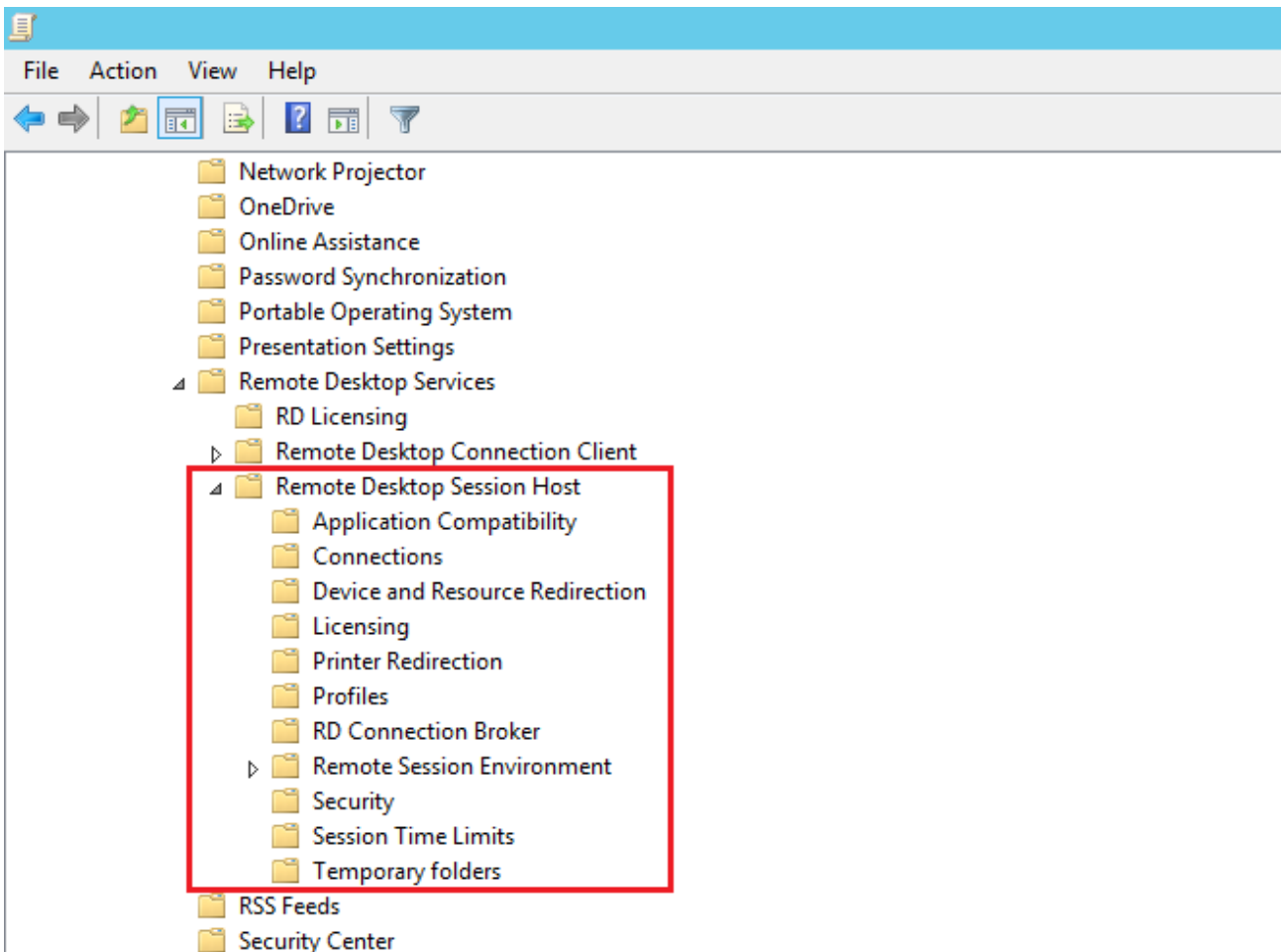
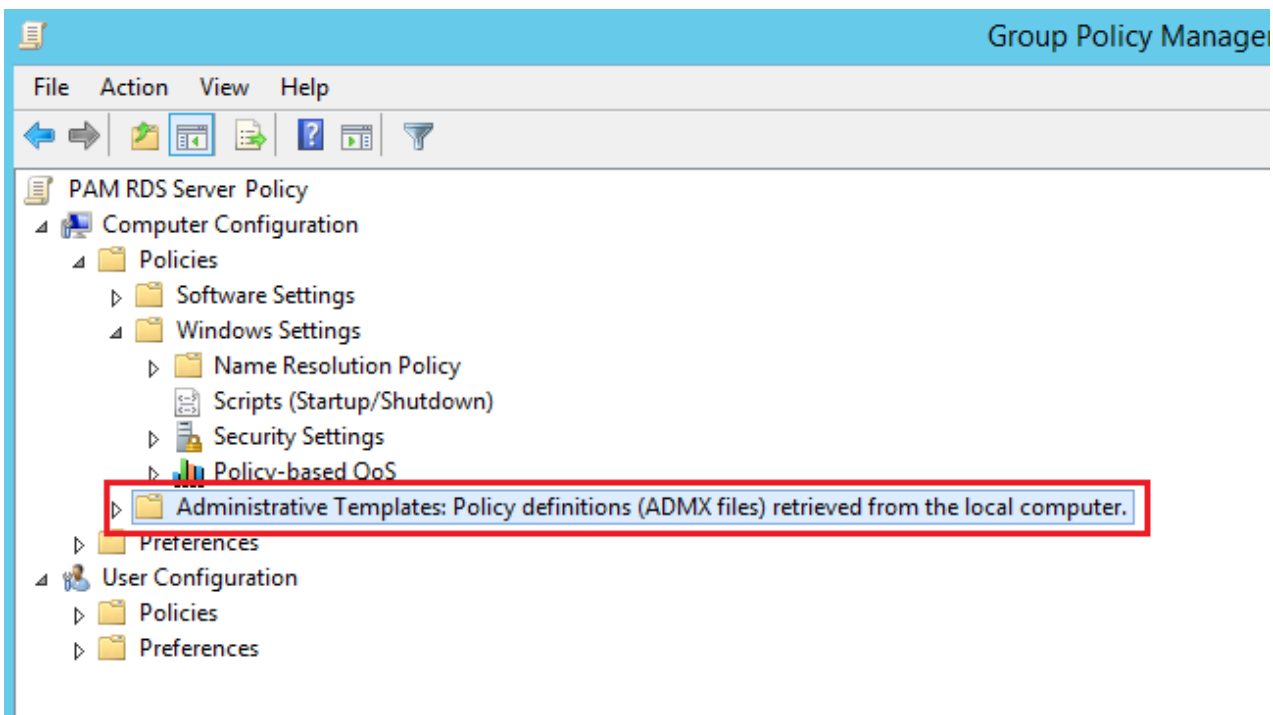
### ▼ Description of policies

Policy	Description	Values
Audit Other System Events	<p>This policy setting allows you to audit the following events:</p> <p>Starting and stopping the Windows Firewall service and driver.</p> <p>Security policy processing by the Windows Firewall service.</p> <p>Operations with encryption key files and migration operations.</p>	Success, Failure
Audit Security State Change	<p>This policy setting allows you to audit events that occur when you make changes to the computer's security state, such as the following:</p> <p>Starting and shutting down the computer.</p> <p>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.</p>	Success, Failure
Audit Security System Extension	<p>This policy setting allows you to audit events related to the security extension, such as the following:</p> <p>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</p>	Success, Failure

Policy	Description	Values
	<p>passwords. Examples of security extensions are Kerberos and NTLM.</p> <p>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.</p>	
Audit System Integrity	<p>This policy setting allows you to audit events related to security subsystem integrity violations, such as the following:</p> <ul style="list-style-type: none"> <li>Events that cannot be recorded in the event log due to errors in the auditing system.</li> <li>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.</li> <li>Detection of a remote procedure call (RPC) that compromises the integrity of the system.</li> <li>Detection of an invalid executable hash value by a code integrity checker.</li> <li>Encryption operations that violate the integrity of the system.</li> </ul>	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	<p>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.</p> <p>When set to Enabled, all clients running a Remote Desktop connection attempt to reconnect automatically when a network connection is unavailable.</p> <p>If the setting is set to Disabled, automatic client reconnections are disabled.</p> <p>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.</p>	Disabled
Configure keep-alive connection interval	<p>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.</p> <p>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</p>	Enabled Keep-Alive interval: 1

Policy	Description	Values
	<p>be active.</p> <p>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.</p> <p>If this policy setting is disabled or not configured, the keepalive interval is not set and the server does not check session state.</p>	
<p>Set rules for remote control of Remote Desktop Services user sessions</p>	<p>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:</p> <p>Remote control not allowed: Prevents the administrator from using remote control or viewing remote user sessions.</p> <p>Full control with user permission: Allows the administrator to interact with the session, subject to the user's consent.</p> <p>Full control without user permission: Allows the administrator to interact with the session even without the user's consent.</p> <p>Monitor session with user permission: Allows an administrator to view a remote user's session with the user's consent.</p> <p>Monitor session without user permission: Allows an administrator to view a remote user's session without the user's consent.</p> <p>If you disable this policy setting, administrators can interact</p>	<p>Enabled</p> <p>Options: Full Control without user's permission</p>

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	<p>Determines whether data redirection from the remote computer to client COM ports should be disabled in Remote Desktop Services sessions.</p> <p>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.</p> <p>If you enable this policy setting, users cannot forward server data to the COM ports of local computers.</p> <p>If you disable this policy setting, COM port redirection is always allowed by Remote Desktop Services.</p> <p>If you do not configure this policy setting, COM port redirection is not defined at the Group Policy level.</p>	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
	<p>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.</p> <p>If you enable this policy setting, users during a Remote Desktop Services session cannot forward server data to local LPT ports.</p> <p>If you disable this policy setting, redirection to LPT ports is always allowed.</p> <p>If you do not configure this policy setting, LPT port redirection is not defined at the Group Policy level.</p>	
<p>Do not allow supported Plug and Play device redirection</p>	<p>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.</p> <p>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.</p> <p>If you enable this policy setting, users cannot redirect supported Plug and Play devices to a remote computer.</p> <p>If you disable or do not configure this policy setting, users can redirect supported Plug and Play devices to the remote computer.</p> <p>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.</p>	<p>Enabled</p>

# 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	<p>This policy setting allows you to remove the "Disconnect Session" item from the Shut Down Windows dialog box in Remote Desktop Services sessions.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p>	Enabled

Policy	Description	Values
Remove Windows Security item from Start menu	<p>Determines whether the Windows Security item should be removed from the Options menu on Remote Desktop Services clients.</p> <p>You can use this policy setting to prevent insufficiently experienced users from being inadvertently disconnected from Remote Desktop Services.</p> <p>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).</p> <p>If the setting is set to Disabled or Not Configured, Windows Security remains in the Start menu.</p>	Enabled

## Security

Windows Components → Remote Desktop Services → Remote Desktop Session Host → Security

### ▼ Description of policies

Policy	Description	Values
Require secure RPC communication	<p>Indicates whether the Remote Desktop Session Host server requires secure RPC connections from all clients or allows insecure connections.</p> <p>This setting can be used to improve the security of client RPC connections by allowing only authenticated and encrypted requests.</p> <p>When the status is Enabled, Remote Desktop Services accepts requests only from RPC clients that support secure requests</p>	Enabled

Policy	Description	Values
	<p>and does not allow insecure connections from untrusted clients.</p> <p>When the status is Disabled, Remote Desktop Services always requests that all RPC traffic be sent securely.</p> <p>If the status is Not Configured, insecure connections are allowed.</p> <p>Note. The RPC interface is used to administer and configure Remote Desktop Services.</p>	
<p>Set client connection encryption level</p>	<p>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.</p> <p>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:</p> <p>High.</p> <p>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.</p> <p>Client compatible.</p> <p>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.</p>	<p>Enabled Encryption Level: High Level</p>

Policy	Description	Values
	<p>Low.</p> <p>When set to Low, only data sent from the client to the server is encrypted using 56-bit encryption.</p> <p>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.</p> <p>Important!</p> <p>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.</p>	

## 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	<p>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.</p> <p>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."</p> <p>If you enable this policy setting, Remote Desktop Services terminates all timed-out sessions.</p> <p>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.</p> <p>If you do not configure this policy setting, Remote Desktop Services disconnects sessions that time out, unless otherwise specified in local settings.</p> <p>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.</p>	
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	<p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p>	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	<p>This policy setting determines whether Remote Desktop Services temporary folders are saved after sessions end.</p> <p>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.</p> <p>If you enable this policy setting, temporary user session folders are not deleted when sessions end.</p> <p>If you disable this policy setting, temporary folders are deleted when the session ends, even if the server administrator has specified otherwise.</p> <p>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.</p> <p>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.</p>	Disabled
Do not use temporary folders per session	<p>This policy setting prevents Remote Desktop Services from creating temporary session folders.</p> <p>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.</p> <p>If you enable this policy setting, temporary session folders are not created. Instead, the user's temporary files for all sessions on the</p>	Disabled

Policy	Description	Values
	<p>remote computer are stored in the Temp shared folder of the user's profile folder on the remote computer.</p> <p>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.</p> <p>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.</p>	

## 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_2.10.0\axidian-pam-windows\MISC\ConfigurationProtector\` 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_2.10.0\axidian-pam-windows\MISC\ConfigurationProtector\` 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.

<b>Windows</b>	PAM\MISC\KeyRotator\Pam.Tools.KeyRotator.exe
<b>Linux</b>	/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 **Ok**
8. Run **Windows registry editor** (RegEdit)
9. Expand  
the **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System** branch
10. Open the context menu of **System** section
11. Select **Create** → **DWORD (32-bit) Value**
12. Specify the parameter name — **LocalAccountTokenFilterPolicy**
13. Open the context menu of **LocalAccountTokenFilterPolicy** parameter
14. Select **Modify** item and set the **Value data:** equal to **1**

Registry editing is required due to restrictions on remote WinRM management for all local accounts except for built-in administrator account.

## Configuring Axidian Privilege Core to Perform Service Operations on behalf of Local Resource Accounts

Service operations are performed using WinRM. To use local resource accounts as service one, you must add the resource to the **TrustedHosts** list of trusted ones on Axidian Privilege Core server.

### Configuring the TrustedHosts List

1. Log in to the server on which Axidian Privilege Core will be installed
2. Run **Command line** (CMD) as Administrator
3. Execute the following command:

```
C:\>winrm s winrm/config/client @{TrustedHosts="Resource1.domain.local,  
Resource2.domain.local"}
```

The specified resources shall be added to the TrustedHosts list.

### CAUTION

When adding new resources to the trusted list, you must specify previously added resources and new ones, since the new value overwrites the old one.

```
@{TrustedHosts="Resource1.domain.local, Resource2.domain.local,  
Resource3.domain.local"}
```

## Service Operations in 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



## Section Reference

16 items



## Dumping Passwords

Read about dumping passwords in an emergency

# 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/pam/mc>
- **Linux:** <https://pam.domain.local/mc>

## 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.

# First Launch

After the first login, go to the **Roles** section and add the current user to the Administrator role, refresh the page, then all sections should be available in the console.

Open the **Users** section, click the search icon, make sure that all users from the specified Organization Unit are read correctly.


Go to the **Configuration** → **Licenses** section. Copy the **Installation ID** and submit it to [Technical Support](#) to issue a license file. When you receive a license file **PAM\_yyyy.mm.dd.lic**, here in the section, click **Add** and select the specified file.

Go to the **Configuration** → **System settings** section. Fill in the network paths to storages of video, files transferred to the server, screencasts of sessions, as well as the domain, username and password to access these folders. In the **Gateway connection settings**, specify the **RDCB address**, **RDCB collection name**. In the **RDP Proxy settings** specify the **RDP Proxy address**. In the **SSH Proxy settings**, specify the **SSH Proxy address**. Save the changes.

Go to the **Events** section, the event of changing the configuration parameters should be displayed there.

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 accounts once in X days	Automatic search for resource data and privileged accounts will be performed once every specified number of days, from 1 to 10,000 days

Option	Description
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 requirements

Option	Description
Generated password length	Total number of characters for automatically generated and manually entered passwords.
Min. password length (manual input)	The minimum number of characters when manually changing the password.

Option	Description
Lowercase letters	If this option is enabled, then automatically generated passwords will consist of lowercase letters. When combined with other settings, the password will contain at least one lowercase letter.
Uppercase letters	If this option is enabled, then automatically generated passwords will consist of capital letters. When combined with other settings, the password will contain at least one uppercase letter.
Numbers	If this option is enabled, then automatically generated passwords will consist of numbers. When combined with other settings, the password will contain at least one number.
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.

## Sessions

### General

Option	Description
User must specify the connection reason	If the option is enabled, then when connecting to the resource, the user must indicate the reason for starting the session.
Limit session duration	If the option is enabled, after the specified duration the session will terminate automatically.
Maximum session duration	The option enables the session duration limit in hours and minutes, after which the session will end automatically.
Enforce exclusive usage of account	If the option is enabled, then the only one active session can be opened for account

Option	Description
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.
Session confirmation timeout, min.	Timeout for confirmation by the Axidian Privilege administrator, in the range from 1 to 180 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	<p>When option is enabled:</p> <p>If connection with the PAM agent is lost, the session is not terminated, users can continue working in this session.</p> <p>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.</p> <p>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.</p> <p>When option is disabled (by default):</p> <p>If connection with the PAM agent is lost, the session is terminated.</p>

Option	Description
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 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 than 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 <a href="#">Configuration</a> 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 <a href="#">Configuration</a> 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	<a href="#">Parameters</a> 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	<p>If the option is enabled and the resource certificate is invalid, the user will not be able to open a session.</p> <p>If the option is disabled and the resource certificate is invalid, the user will be able to open a session.</p>

## SSH

### Privilege Elevation

- **Allow run pamsu** — support for executing commands with root privileges on resources with the PamSu component installed.

#### NOTE

Allowing to use PamSu while creating the permission takes priority over the setting in the policy.

### Allowed and Forbidden Commands

- **Prompt** — regular expression to correctly recognize command input.
- **Reaction to forbidden command** — terminal behavior in response to a forbidden command: CTRL + C (cancel execution) or Abort the session.

Creating a list of controlled commands:

1. Click the **Add** button.
2. Enter the command or regular expression.
3. Select the status **Allowed** or **Forbidden**.

 **NOTE**

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.



## Users

Users



## User Groups

User Groups



## Resources

4 items



## 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

1 items



## Roles

Roles



# Applications

Applications

# Users

The section is intended to work with user directory of Active Directory.

By default, the page displays 15 users.

## ! INFO

You can change the default number of users on a page in the [configuration file](#).

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.

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.

## 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

The user authenticators and corresponding settings are displayed in the **Authenticators** tab. You can change the 2fa requirement setting here to enable, disable or use defaults. To change requirement setting:

- Open the user profile and go to the **Authenticators** tab.
- Click the pen  icon and select the appropriate option.

## 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**.

## Resetting User Authenticator

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

## Disabling User Authenticator

1. Open the user profile and go to the **Authenticators** tab.
2. Click the pen  icon 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 a User

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 closed.

## RECOMMENDATION

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**.

## ATTENTION

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](#) (if access was available). When employees leave, remove users from Active Directory.

# 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**.

## Setting a Policy for a User

1. Open the user's profile.

2. Click  to add or change a policy.

# 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 from 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 address / IP address)** in whole or in part.

Select resource **State**:

- Enabled
- Blocked
- Removed

Select service connection

- Not set
- Windows
- SSH
- Microsoft SQL Server
- MySQL
- PostgreSQL
- Oracle Database
- Cisco IOS
- Inspur BMC

# 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**.

## 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.

### **NOTE**

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**.

### **NOTE**

Line format:

'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 port; Cisco's privilege mode password **At least either DNS name or IP address should be filled.**

Examples:

```
Computer;Typical Computer 1;;192.168.0.101;RDP;;;;;DEV\root;Windows;;;Computer;Typical Computer 2;;192.168.0.101;RDP;;3390;;;;;;Website;Typical Website3;dev.local;WebTemplate;http://dc.dev.local/;;http://dc.dev.local/login;FALSE;DEV\root;Windows;;;Server;Typical Server 4;;192.168.0.3;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.

#### ⓘ NOTE

If you need to open a session with the `mstsc /admin` parameter, enable the **Run as administrator** option

### 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 **Resource Name**, **Description**, **Policy**, **User** or **Service Connection**.

- Click  in the resource page to the right of the required parameter.

## Adding User Connection

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

- Click **Add** on the User connections tab
- Select the type of connection: RDP, SSH, Telnet or another user connection, specify the address, connection port and other parameters of user connections

## 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

- Click **Remove** on the resource profile

#### ⓘ NOTE

Before removing a resource, you must delete all accounts that were added from the removed resource

### Rolling Back Resources

- Click **Extended search** in the **Resources** section
- Enter the **Resource name** or **Address (DNS name/IP address)** in whole or in part
- Select **Removed** for the **State** field and click **Search**
- Open the resource profile and click **Rollback**
- 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**

# 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.

## 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 key manually**.

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

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**

# 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

## 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**

# 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.

# 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.

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.


## Account

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



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 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.

## 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

## Licenses

The section contains Axidian Privilege licensing information.

The section displays the following data:

- **Installation ID** — a unique installation code is required to generate a license.
- **User licenses available** — total number of user licenses.
- **User licenses used** — total number of licenses used.
- **Resource licenses available** — total number of resource licenses.
- **Resource licenses used** — number of licenses used.

The following data is displayed for each license:

- **Start date** — license start date.
- **End date** — license expiration date.
- **User licenses** — total number of user licenses.
- **Resource licenses** — total number of licenses used.
- **Issue date** — license release date.

## Add License

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

## Removing Licenses

Mark the required license and click **Delete**.

## System Settings

Option	Description
Number of failed OTP access attempts allowed	<p>After exceeding this value the user will be temporarily blocked, i.e. will not be able to enter OTP.</p> <p>Min value: 0 Default value: 10 Max Value: 99</p> <p>0 means that no blocking is applied, i.e. the number of input attempts is not limited.</p>
Lockout duration	<p>Defines the period of time after which the user will be unblocked and will be able to enter OTP again.</p> <p>Min value: 1 Default value: 10 Max Value: 9999</p>

## User Connection

The section contains data about user connections. **RDP**, **SSH**, **Telnet** connections are built-in and cannot be changed or deleted.

### Adding New 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

The section contains data on service connections. All the service connections except SSH is built-in and cannot be changed or deleted.

## Adding a Service Connection with SSH Type

The service operations template is unique for each \*nix distribution. The distribution includes templates for SUSE Linux Enterprise Server, FreeBSD, CentOS, and Ubuntu in the `..PAM_2.10.0\axidian-pam-tools\ssh-templates\` folder.

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.

## Adding the Network Location

Click **Add**.

Enter a **Name** and add the **Network addresses** of the resources to which you want to issue a limited connection.

# 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**

# 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 **axidian-pam-tools\Dump\Pam.Tools.Dump.exe**

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**

## ▼ 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 instance
- **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

The utility can be executed with the following arguments:

- **decrypt-ssh-key** — decrypting encrypted exported ssh key of the account
- **decrypt-password** — decrypting encrypted exported password of the account
- **decrypt-secrets** — decrypting credentials of accounts from specified or chosen folder
- **ssh-key** — dumping the SSH key of the account, you must specify the account, for example:  

```
Pam.Tools.Dump.exe ssh-key --name res2\administrator
```
- **password** — dumping the password of a privileged account, you must specify an account, for example:  

```
Pam.Tools.Dump.exe password --name res2\administrator
```
- **all-secrets** — dumping all credentials to the **.\Results** folder, or to the specified one. Passwords will be dumped to **accounts.csv** file, keys will be dumped to **sshKeys** folder in separate files. Example

command:

```
Pam.Tools.Dump.exe all-secrets --output c:\temp
```

- **help** — displaying more information of a specific command
- **version** — displaying version information



## User Console

Gain access to the User Console



## Access to the Resource

Learn about ways to connect to resources



## Connection via SSH Clients

Learn how to connect to resources via third-party SSH clients



## SCP/SFTP Connection to the Resource

3 items



## Personal Resource Folders

Learn how to group resources into folders



## Executing Commands with Root Privilege

Learn how to run a command if sudo is needed



## Account Operations

Learn about searching accounts, viewing and changing passwords and SSH keys



## Usage of AAPM Console Tool

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



## Desktop Console

Learn about Axidian Privilege Desktop Console

# User Console

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

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

## 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.

### NOTE

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.

# Access to the Resource

The user console displays permissions to access the resources. For each permission the following fields are displayed:

- **Resource**.
- **Type** — connection protocol.
- Address (**IP** or **DNS**).
- **Account** — privileged account on whose behalf the session will be opened.

It is possible to sort any column and use the search. As you enter characters in the search box, matches will be displayed across all columns.

If the user has access to [ad hoc resources](#), they will be displayed at the top of the list.

To connect to a resource you need to download the RDP file of this resource. You can download it once and save this file to use for future connections. You can use this file as long as the permission is valid.

Another way to connect to a resource is to use RDP file of PAM Access Gateway. This file can be used to connect to resources regardless of available permissions because each time you connect to the gateway, an up-to-date list of resources will be displayed.


Clicking on a permission line displays additional information about the permission:

- Validity period.
- Access schedule.
- Permission ID — unique number which identifies the permission.

## Direct Connection to a Resource

1. Click **Connect** to the right of the desired permission. This will make the RDP file started to download.
2. Run the downloaded RDP file to access the resource.
3. Authenticate and set up your connection.



For resources that can be connected via both types of connections (RDP and SSH), the **Copy SSH command** button is displayed by default. In this case, if you need to download RDP file, click  first and then click **Download RDP file for connection**.

## Connection to the Access Gateway

1. Click **Connect to access gateway**. This will make the RDP file started to download.
2. Run the downloaded RDP file to connect to the gateway.
3. Authenticate and set up your connection.

## Connection to the SSH Proxy

You can use [any SSH client](#) to connect to the SSH Proxy gateway.

- Launch a SSH client.
- Enter the SSH Proxy address and connect.
- Authenticate.
- Select a resource to connect.

## Direct Connection via SSH

To the right of the desired permission to the SSH resource, click the **Copy SSH Command**. The SSH command for connecting to this resource will be copied to the clipboard.

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

### SSH Command Template

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

- `user-name` — username
- `resource` — IP address or DNS of the target resource
- `account-name` — name of the privileged account
- `reason` — text of the reason for the connection. If it contains spaces, put it in quotation marks.

- `proxy-address` — IP address or DNS of the SSH Proxy

You can omit any parameter except the `proxy-address`. In this case, the terminal will request these parameters one by one.

After executing the command, the terminal will ask for the user's password and TOTP.

### SSH command Example

```
ssh james.miller#ubuntu#webmaster#"system configuration"@pam
```

## Connection to an Ad Hoc Resource

Ad hoc resources are those resources that are not registered in the Axidian Privilege system. This type of connection allows to connect to any resources using connection types predefined by the PAM administrator.

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 defined 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** for connection.

#### ⓘ 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 when Connecting

When connecting to a resource, you may be asked for a password.

This means that the account on behalf of which 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 about connecting to this resource, as only the administrator can set the account password.

## End of Session

To end the session, end the user's session on the resource, or right-click on resource in the **Connections** pane or on connection tab and select **Disconnect** menu item, or close the Remote Desktop window.

# Connection via SSH Clients

This section describes how to connect SSH through third-party clients.

## Connecting via Access Gateway

[Command Line](#)   [PuTTY](#)   [MobaXterm](#)   [SecureCRT](#)

---

1. Open the terminal.
2. Enter the connection string for SSH Proxy or Balancer. You can use IP address or DNS.

```
ssh axidianproxy
```

If necessary, specify the user and port.

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

3. Enter password and TOTP.
4. Select the resource you want to connect to.

## Connecting to a Specific Resource

[Command Line](#)   [PuTTY](#)   [MobaXterm](#)   [SecureCRT](#)

---

1. In the user console, next to the SSH resource, click **Copy**. This will copy to the clipboard the SSH connecting command to this resource.
2. Paste the copied line into the terminal.
3. Enter password and TOTP.



## 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:

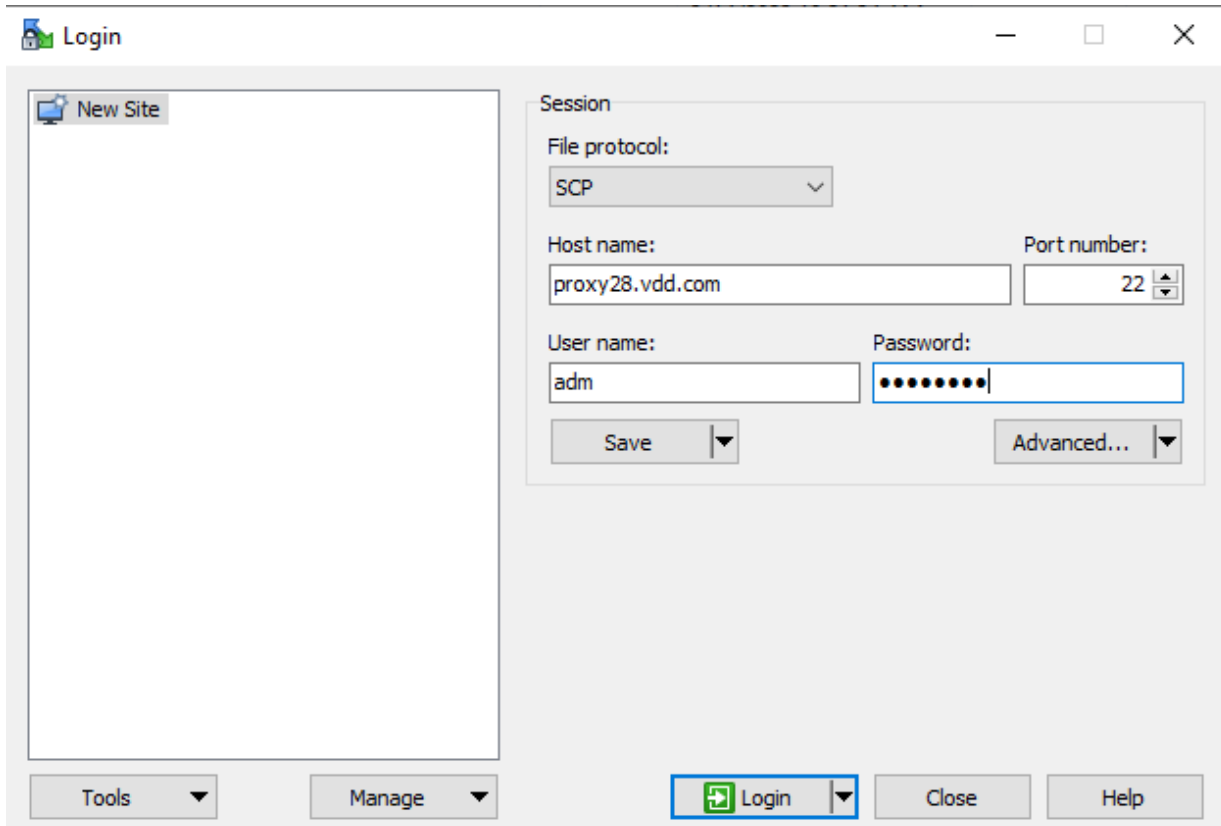
```
put -r C:\temp\configs\ /tmp/configs  
put -r path_to_local_files path_to_files_on_resource
```

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.

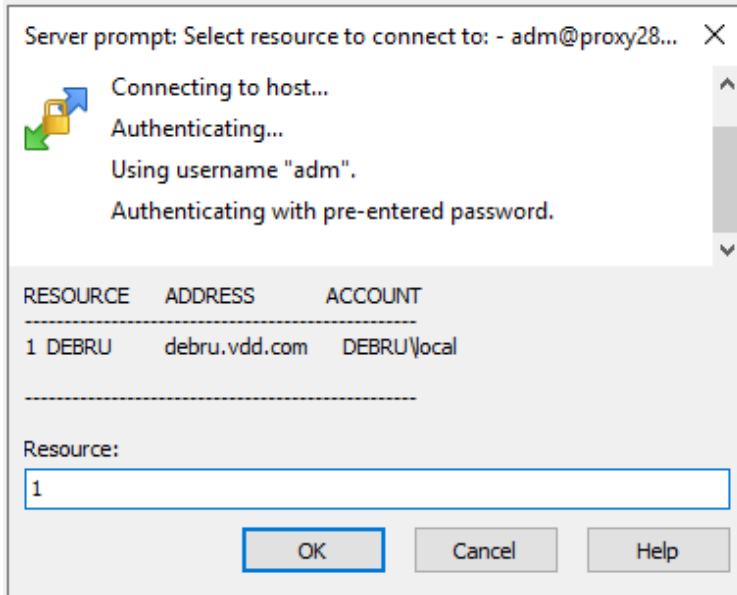
# WinSCP

## 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".



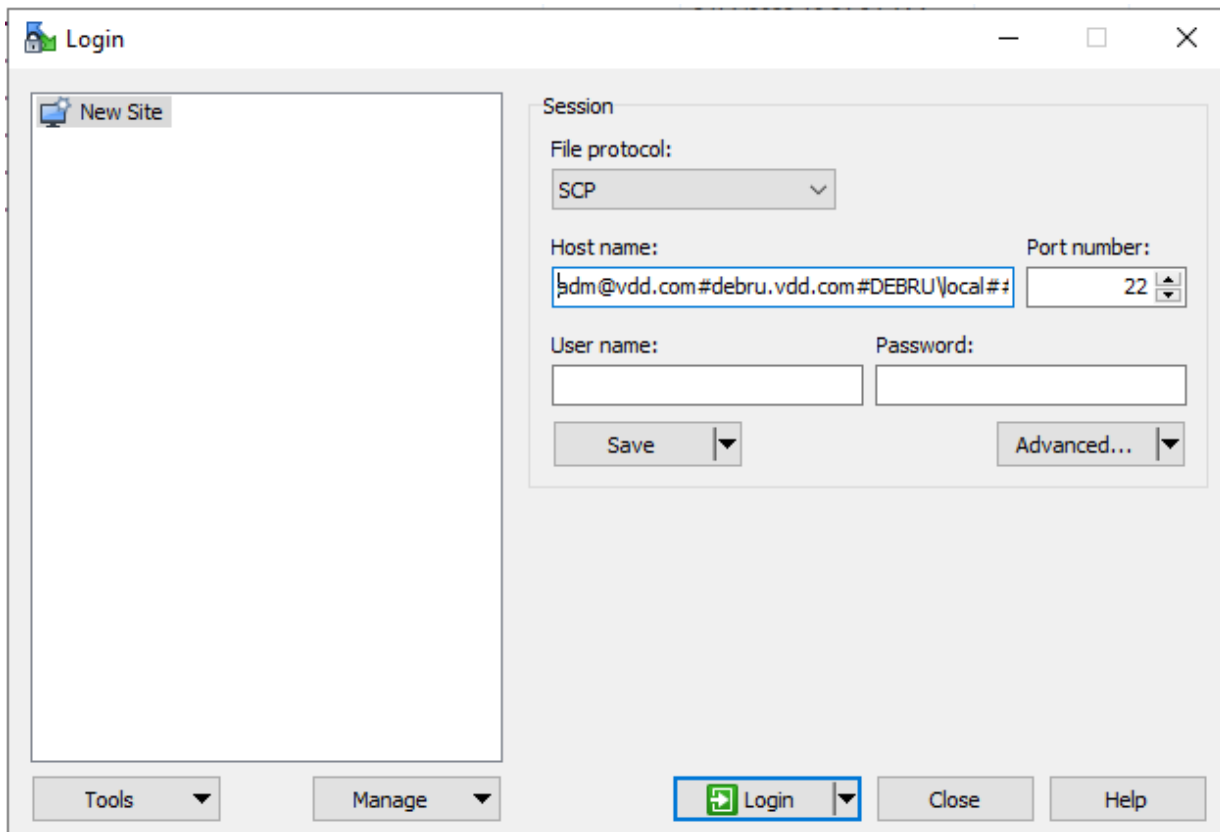
3. Click **Login** button and select resource to connection.



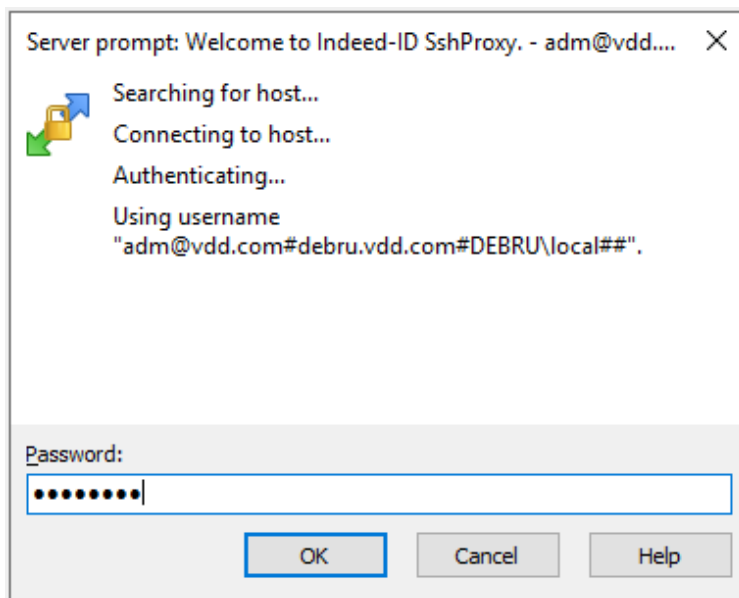
## Direct Connection to the Resource

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.


# Personal Resource Folders

This section describes working with personal resource folders.


## Creating a Personal Resource Folder

- In the **Resources** section click the folder icon .
- Enter a new folder name and click **Save**.

## Editing Folder Name

- Open the **Resources** section.
- Select a folder and click the pencil icon .
- Enter a new folder name and click **Save**.

## Deleting a Folder

- Open the **Resources** section.
- Select a folder and click the bin icon .
- Confirm deleting the folder.

## Adding Resources to a Folder

- Open the **Resources** section and click **All Resources/Resources without a folder**.
- Select the resources that need to be moved to the folder.
- Click the button **Move**
- Choose a folder and click **Save**.

Adding [ad hoc resources](#) to folders is not supported.

## Resource Search

- Open the **Resources** section.
- Select a folder or click **All Resources/Resources without a folder**.
- Enter the resource name in search string.

### INFO

[Ad hoc resources](#) can be found by searching for "adhoc".

# Executing Commands with Root Privilege

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
```

# Account Operations

## Account Search

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

Searching for accounts works similarly to searching for resources.

## Viewing an Account's Password and SSH Key

If the user has permission, in which the option **Allow user to view account credentials** is enabled, then the **Accounts** section will become available in the personal account. The section displays all accounts for which the password and SSH key can be viewed. To view, click **View credentials**, enter the reason for viewing and confirm your actions.

The Axidian Privilege administrator can configure confirmation to view the password of a privileged account, in which case the user will wait for confirmation.

## Changing an Account's Password and SSH Key

If the user has a permission to editing the account password, then the user can do it in the **Accounts** section.

To change the password, click **Change Password**, set a new password, write the reason and click **Save**.

# Usage of AAPM Console Tool

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

Path: `..PAM_2.10.0\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

```
1 {
2   "Auth": {
3     "Username": "MyApplication",
4     "Password": "M3YTy;[j;q&*DrZQSl(?B1agm$7uS+",
5   },
6   "Endpoints": {
7     "CoreUrl": "https://debmng.axidian.test/core",
8     "IdpUrl": "https://debmng.axidian.test/idp"
9   }
}
```

## 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-6.0](#) installed.

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

```
cd PAM_2.10.0\axidian-pam-tools\aapm\
```

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

### Usage Example

Input

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

# 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.



## 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\pam\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 the log file to technical support. Example of a script error:

```
*****
* Failed: Ansible playbook returned error code: 2
*****
```

Location of the log file: `axidian-pam-linux/logs/deploy.log`.

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/receive 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\\pam\\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.

```
1  "variables": {
2    "minLevel": "Trace",
3    "dbMinLevel": "Info"
4  }
```

### ⚠ 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.

```
1  "Rules": {
2  "03_Hangfire": {
3      "logger": "Hangfire.*",
4      "minLevel": "Info",
5      "writeTo": "hangfireFile",
6      "final": true
7  },
8  "20_Errors": {
9      "logger": "*",
10     "minLevel": "Error",
11     "writeTo": "errorsFile"
12 },
13 "40_Commands": {
14     "logger": "Idp.Application.*Command",
15     "minLevel": "${minLevel}",
16     "writeTo": "commandsFile",
17     "Enabled": false
18 },
19 }
```

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:

```
1  "targets":{
2      "errorsFile": {
3          "type": "File",
4          "layout": "${loggerLayout}",
5          "fileName": "C:\\Logs\\errors.log",
6          "archiveFileName": "C:\\\\LogsArch\\errors.{#####}.log",
7          "archiveAboveSize": 1000000,
8          "archiveNumbering": "Sequence",
9          "maxArchiveFiles": 2
10         }
11 }
```

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:**

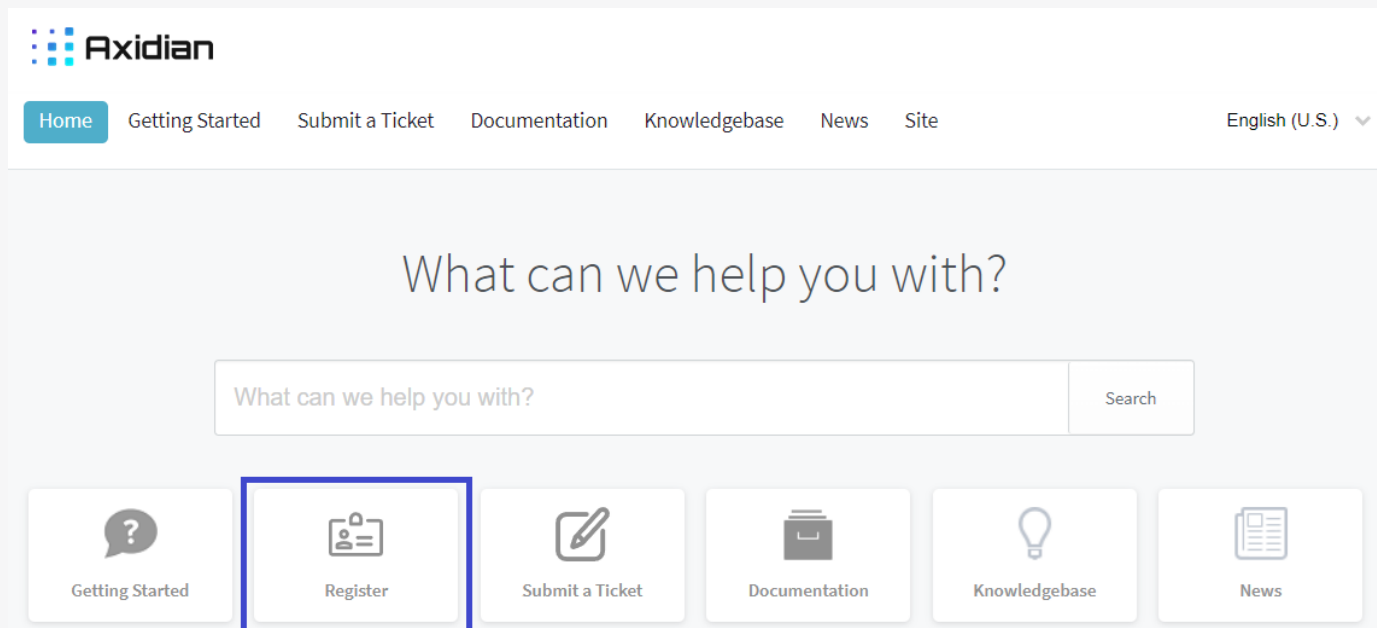
1. Open [Technical Support Portal](#).
2. Enter your email address and password and click **Login**.

▼ 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**.

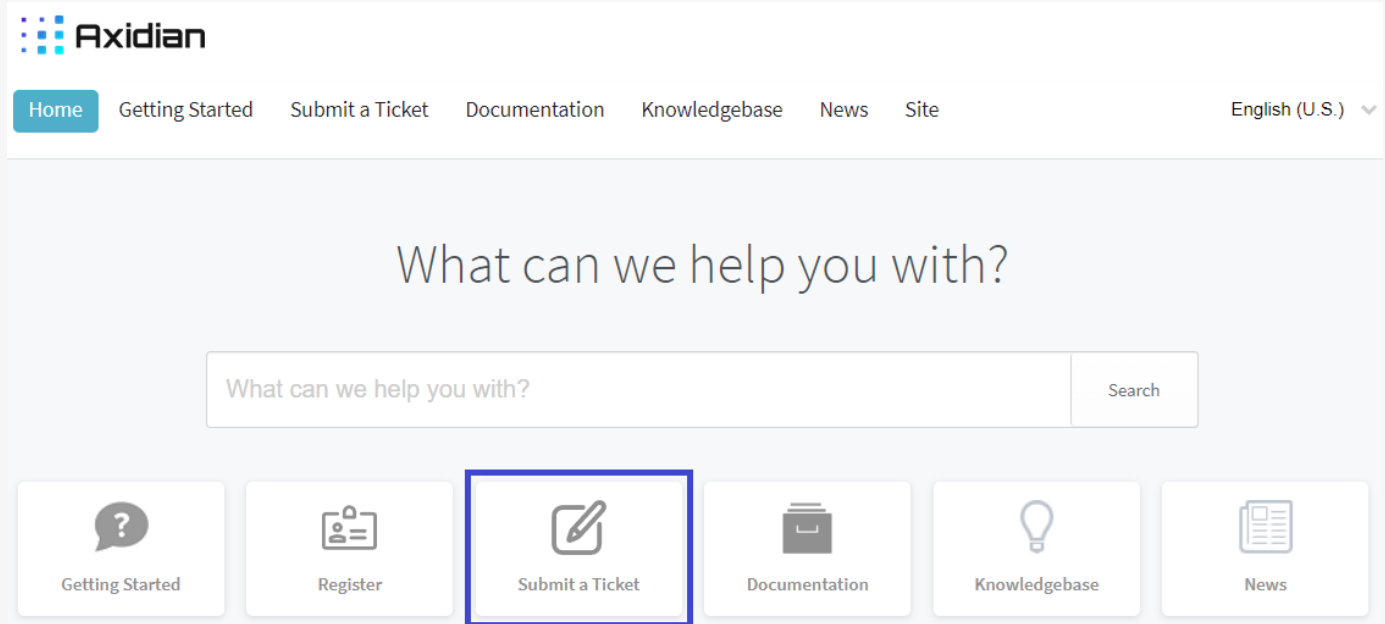


The screenshot shows the Axidian Technical Support Portal. At the top left is the Axidian logo. A navigation menu includes 'Home', 'Getting Started', 'Submit a Ticket', 'Documentation', 'Knowledgebase', 'News', and 'Site'. On the right, there is a language selector set to 'English (U.S.)'. The main heading is 'What can we help you with?'. Below this is a search bar with the placeholder text 'What can we help you with?' and a 'Search' button. A row of six icons is displayed: a question mark for 'Getting Started', a person with a plus sign for 'Register' (which is highlighted with a blue border), a pencil for 'Submit a Ticket', a folder for 'Documentation', a lightbulb for 'Knowledgebase', and a document for 'News'.

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.

## 2.10

- [OpenLDAP and ALD PRO 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.](#)