Saviynt University

Saviynt Certified PAM Professional (SCPP) Exam Preparation Guide

Authored by: Saviynt University

Introduction

The Saviynt Certified PAM Professional (SCPP) examination is the beginning level certification for the Saviynt Privileged Access Management platform. It is intended for individuals with the knowledge, skills, and ability to deploy primary and medium complexity use cases involving Saviynt PAM. The candidate will demonstrate an understanding of Saviynt PAM capabilities, including Setting up PAM, Configurations for PAM, Privileged Access Methods, Discovery and Bootstrapping, Password Management, KPIs and Controls related to PAM, Managing PAM Sessions, also covering best practices and troubleshooting scenarios. Job roles associated with this certification include PAM consultants, engineers, developers, and administrators with 1-3 months of experience on Saviynt PAM.

Saviynt Certified PAM Professional (SCPP) certification validates the candidate's ability to:

- Explain the value of Saviynt PAM offerings and features.
- Explore the architecture of Saviynt along with deployment models.
- Discover the supported feature matrix of PAM.
- Understand essential configurations for PAM use cases.
- Explain the process of Setting up PAM, including Vault connection, Master connections, and creating various connections.
- Describe the different PAM methods to request privileged access.
- Understand and explain the discovery and bootstrapping process.
- Understand about the KPIs and controls related to PAM.

- Explain the concepts of Periodic Password Rotation and Password Reconciliation.
- Describe the process of managing and monitoring PAM sessions.

Minimally Qualified Candidate

We recommend that candidates have at least 1-3 months of hands-on experience with the Saviynt Privilege Access Management platform in any role, including PAM consultants, engineers, managers, decision-makers, and those working in PAM sales and pre-sales departments. The minimally qualified candidate (MQC) possesses skills in deploying, configuring, and managing the Saviynt PAM solution.

Recommended General IT Knowledge

Candidates should have a basic understanding of Cloud Computing and PAM concepts.

Exam Pre-requisite

It is mandatory to complete the ***Saviynt PAM Level 100*** classroom or self-paced training before scheduling the exam.

Exam Delivery

This is an online proctored exam delivered through Examity. For more information, visit the Examity Website.

Exam Content

Question Types

There are two types of questions on the examination:

- **Scenario Based Multiple choice:** Has one correct response and three incorrect responses (distractors).
- **Multiple response:** Has two or more correct responses out of four options.
- **True/False:** Choose between true or false

Select one or more responses that best complete the statement or answer the question. Distractors, or incorrect answers, are response options that an examinee with incomplete knowledge or skill would likely choose. However, they are generally plausible responses that fit in the content area defined by the test objective. Unanswered questions are scored as incorrect; there is no negative marking.

Survey Questions

Your examination may include a few survey questions placed on the test to gather statistical information.

Exam Duration

The Saviynt Certified PAM Professional (SCPP) examination has 50 multiple-choice questions and lasts 90 minutes.

Exam Results

The Saviynt Certified PAM Professional (SCPP) examination is a pass-or-fail exam. It is scored against a minimum standard established by Saviynt professionals, guided by certification industry best practices and guidelines. Your results for the examination are reported as a score from 0 to 100, with a minimum passing score of 70. Your score shows how you performed on the examination and whether you passed.

Your score report contains a table of classifications of your performance at each section level. This information is designed to provide general feedback concerning your examination performance. The examination uses a compensatory scoring model, meaning you do not need to “pass” the individual sections, only the overall examination. Each section of the examination has a specific weighting, so some sections have more questions than others.

Content Outline

The table below lists the main exam topics and their weightings. It is not a comprehensive listing of the content of this examination.

Section	Topic	# of questions
1	Saviynt PAM Overview	3
2	Saviynt PAM Architecture	2
3	Saviynt PAM Support Matrix	4
4	Configurations for Saviynt PAM	8
5	Saviynt PAM Methods	9
6	Setting up Saviynt PAM	8
7	Manage Accounts and Workloads	8
8	End User – Privileged Access and Monitoring	3
9	Manage Saviynt PAM Sessions	2
10	New Features and Improvements	3
Total		**50**

Section 1 – Saviynt PAM Overview

Objective 1:1 – Introduction to PAM

1.1.1- Saviynt Enterprise Identity Cloud
1.1.2- Privileged Access Management
1.1.3- Highlights of Saviynt PAM

Objective 1:2- Business Challenges and PAM Solutions

1.2.1- Challenges of traditional PAM
1.2.2- Addressing PAM Needs with PAM Solutions for various challenges.

Objective 1:3 – PAM Features

1.3.1- Saviynt PAM Platform Value Proposition
1.3.2- PAM Key Features

Section 2 – Saviynt PAM Architecture

Objective 2:1 – High-level Architecture

- 2.1.1- Solution architecture
- 2.1.2- Architecture of PAM

Objective 2:2 – Deployment Architecture

- 2.2.1- Microservices-based Architecture
- 2.2.2- Different Layers of Architecture
- 2.2.3- PAM Microservices and Terminologies
- 2.2.4- High-Availability Considerations
- 2.2.5- Different Deployment Architecture Models

Objective 2:3 – Saviynt Connect 2.0

- 2.3.1 – Various Connectivity Options
- 2.3.2- Saviynt Connect 2.0

Section 3 - Saviynt PAM Support Matrix

Objective 3:1 – PAM Supported Features

- 3.1.1- PAM Features

Objective 3:2 – Supported Access Methods of PAM

- 3.2.1- Support Matrix for AWS, GCP, Azure, On-Premises, Active Directory, and Applications

Section 4 - Configurations for Saviynt PAM

Objective 4:1 – Global Configurations

4.1.1- Password Checkout
4.1.2- Privileged Sessions (Clipboard and Credential Preferences)
4.1.3- Just-in-Time (JIT) Configuration and Enable Quick Launch
4.1.4- Bootstrap Configuration
4.1.5- Server Configuration, User Interface Configuration and Unix Scan Log Locations

Objective 4:2 – Task Execution Hierarchy

4.2.1 – Understand Task Execution Hierarchy
4.2.2- PAM-related Firefighter Tasks

Objective 4:3 – Auto and Instant Provisioning

4.3.1- Enable Auto and Instant Provisioning at the Security System level
4.3.2- PAM tasks for which Instant Provisioning needs to be enabled.

Objective 4:4 – SAV Roles

4.4.1- Define SAV Roles
4.4.2- Understand PAM-related OOTB SAV Roles
4.4.3- Assigning SAV Roles
4.4.4- Feature Access of ROLE_SAV_PAMENDUSER, ROLE_SAV_PAMADMIN and ROLE_SAV_PAMOWNER

Objective 4:5 – Workflows

4.5.1- Define Workflows
4.5.2- Types of Workflows
4.5.3- Configure One-level Manager Approval Workflow
4.5.4- Configure Auto-Approval Workflow

Objective 4:6 – Creating and Managing Email Templates for PAM

4.6.1- Configuring Email History Job
4.6.2- Binding Variables for PAM Email Templates
4.6.3- Configuring Privileged Access Request Creation, Approval and Rejection Email.
4.6.4- Configuring Email Templates for Privileged Access Tasks

Objective 4:7 – Application Logs

4.7.1- Explain Application Logs
4.7.2- Understand Log Viewer
4.7.3- Log Viewer Features
4.7.4- Understand parameters in Search Results
4.7.5- Commonly Used Search Queries

Section 5 – Saviynt PAM Methods

Objective 5:1 – Role-based PAM

5.1.1- Define Role-based PAM Access Method
5.1.2- Understand Role-based Access Workflow

Objective 5:2 - Credentials and Credential-less PAM

5.2.1- Define Credential PAM Access Method
5.2.2- Understand Credential Access Workflow
5.2.3- Define Break Glass Feature
5.2.4- Understand Break Glass Workflow and Initializing Break Glass Session
5.2.5- Define Credential-less PAM Access Method
5.2.6- Understand Credential-less Access Workflow

Objective 5:3 - Just-in-Time PAM

5.3.1- Define Just-in-Time PAM Access Method
5.3.2- Understand Just-in-Time Access Workflow

Objective 5:4 – Provisioning and De-provisioning

5.4.1- Understand WSRETRY Job
5.4.2- Understand Enterprise Role Management Job

Objective 5:5 – Quick Access

5.5.1- Define Quick Access
5.5.2- Understand the pre-requisites for the Quick Access Feature

Section 6 – Setting up Saviynt PAM

Objective 6:1 – Create Vault Connection

- 6.1.1- Why is Vaulting required
- 6.1.2- HashiCorp Vault
- 6.1.3- Understand the process to set up a Vault
- 6.1.4- Create Vault Connection and Understand Parameters of Vault Connection

Objective 6:2 – Preparing Target Workloads for PAM Integration

- 6.2.1- Preparing Linux, Windows, and Database Target Workloads

Objective 6:3 – Create Master Connections

- 6.3.1- Define Master Connection
- 6.3.2- Define Master Account
- 6.3.3- Create Windows Master Connection
- 6.3.4- Create Unix/Linux Master Connection
- 6.3.5- Create Database Master Connection

Objective 6:4 – Create Active Directory Connection

- 6.4.1- Preparing for Integration
- 6.4.2- Create Active Directory Connection

Objective 6:5 – Create AWS Connection

- 6.5.1- Set up a Cross-Account Role
- 6.5.2- Understand Options for Establishing Trust
- 6.5.3- Understand PAM-related CloudFormation (CF) templates
- 6.5.4- Create an AWS connection

Objective 6:6 – Create GCP Connection

- 6.6.1- Configure Connection using the Service Account Key method
- 6.6.2- Configure Connection using OAuth Client ID method
- 6.6.3- Create GCP Connection

Objective 6:7 – Create On-Premises Connection

- 6.7.1- Create On-Premises Connection

Objective 6:8 – Create a Security system

- 6.8.1- Define a Security System
- 6.8.2- Create a Security System
- 6.8.3- Create an Endpoint

Objective 6:9 – Import Accounts and Access

6.9.1- Understand Import Type Options such as Accounts and Access
6.9.2- Create and execute Import Job

Objective 6:10 – AWS Emergency roles

6.10.1- Define AWS Emergency Role
6.10.2- Understand how to Map Entitlements to the AWS Emergency Role

Section 7 – Manage Accounts and Workloads

Objective 7:1 – Overview

7.1.1- Understand what can be managed in Saviynt PAM
7.1.2- Understand the process of onboarding Application Targets
7.1.3- Understand the process of onboarding Cloud Workloads and On-Premises Workloads
7.1.4- PAM_Config
7.1.5- Checklist for setting up PAM
7.1.6- Pre-configurations required for bootstrapping targets
7.1.7- Sync jobs to be run after bootstrapping process

Objective 7:2 – Discovery & Bootstrapping of Active Directory

7.2.1- Understand the process of Bootstrapping
7.2.2- Understand Active Directory Use cases for PAM
7.2.3- Execute PAM bootstrap job for Active Directory
7.2.4- Understand how the shareable accounts become FirefighterID
7.2.5- Validate PAM Bootstrapping at Endpoint and Account level

Objective 7:3 – Discovery & Bootstrapping of Cloud Workloads

7.3.1- Periodic discovery for Cloud – AWS and GCP
7.3.2- Understand Real-time discovery and onboarding of cloud workloads for AWS and GCP
7.3.3- Steps to enable PAM protection for onboarding cloud workloads
7.3.4- Understand AWS Use cases for PAM
7.3.5- Execute PAM bootstrap job for AWS and GCP
7.3.6- Validate PAM Bootstrapping at Endpoint and Account level

Objective 7:4 – Discovery & Bootstrapping of On-Premises Workloads

7.4.1- Discover On-Premises workloads
7.4.2- Onboard On-Premises Workloads using Scanning Tool
7.4.3- Onboarding On-Premises Workloads using CSV
7.4.4- Automated Onboarding of On-Premises Workloads

Objective 7:5 – KPIs and Controls

7.5.1- Saviynt's Control Center
7.5.2- Understand Control center components
7.5.3- Understand how to analyze KPIs and relevant records

Objective 7:6 – Password Management

7.6.1- Define the Periodic password rotation process
7.6.2- Create and execute Periodic password rotation job
7.6.3- Define the Password reconciliation process
7.6.4- Create and execute Password reconciliation job

Section 8 – End User – Privileged Access and Monitoring

Objective 8:1 – Credential-less - Overview

8.1.1- Understand Privileged access request
8.1.2- Understand Credential-less access process
8.1.3- Steps to submit a request for a Credential-less session
8.1.4- Understand how Credential-less sessions are initiated for Windows, Unix, and Database

Objective 8:2 – Credentials - Overview

8.2.1- Understand Credential access process
8.2.2- Steps to submit a request for a Credential session
8.2.3- Define Generic Vault use case
8.2.4- Execute steps to vault privileged account
8.2.5- Execute steps to create generic vault PAM requests
8.2.6- Define Application to Application Password Management (AAPM) use case
8.2.6- Execute steps for AAPM process

Objective 8:3 – Remote Apps

8.3.1- Understand Remote applications process
8.3.2- Steps to submit requests for remote access session for AWS and GCP Console access
8.3.3- Understand how the AWS and GCP Console are launched

Objective 8:4 – MFA for Privileged Access

8.4.1- Understand MFA
8.4.2- Steps to configure MFA

Section 9 – Manage Saviynt PAM Sessions

Objective 9:1 – Monitor Privileged Sessions

9.1.1- Over-the-shoulder monitoring
9.1.2- Understand how to view live and recorded privileged sessions
9.1.3- Understand different modes of view, such as Standard view and Detailed view
9.1.4- Understand about PAM Audit Viewer

Objective 9:2 – Session Actions

9.2.1- Understand Session actions – Terminate the session and Remove Access options
9.2.2- Understand steps to terminate the session and remove access

Objective 9:3 – Restricted and Risky commands

9.3.1- Understand categories of risk activity
9.3.2- Search options such as filter by risk type and event type
9.3.3- Understand how to configure restricted and risky commands
9.3.4- Understand how the restricted commands are blocked from being executed.

Section 10 – New Features and Improvements

Objective 10:1 – Simplified Endpoint Access Control Capability Using Policies

10.1.1- Key Highlights of the Feature
10.1.2- Pre-requisite 1: Endpoint Access Groups
10.1.3- Pre-requisite 2: Enable Policy Rules
10.1.4- Managing Endpoint Visibility
10.1.5- Managing Tags for Endpoints
10.1.6- Managing Endpoint Group Policies

Objective 10:2 – Endpoint Access Policies for Linux

10.2.1- Key Highlights of the Feature
10.2.2- PAM Endpoint Group Policies
10.2.3- Entitlements Selection to Specify Access
10.2.4- Endpoint Group Policy Conditions
10.2.5- Endpoint Count

Objective 10:3 – Virus and Malware Scanning

10.3.1- Key Highlights of the Feature

Objective 10:4 – Simplified User Experience with Neo (Beta)

10.4.1- Key Highlights of the Feature
10.4.2- Enable NEO UI - Global Configuration
10.4.3- Using the Privileged Access Page (Neo Experience)
10.4.4- Requesting and Accessing Privileged Sessions
10.4.5- Privileged Access Assets & Sessions

Objective 10:5 – Privileged Access to Windows Target Using AD Endpoint (Neo)

10.5.1- Key Highlights of the Feature
10.5.2- Privileged Access for Active Directory endpoint
10.5.3- Connect to Session
10.5.4- Launch Session

Objective 10:6 – Privileged Access Management to Azure Workloads

10.6.1- Key Highlights of the Feature
10.6.2- Azure Pam Template
10.6.3- PAM_Config in Azure
10.6.4- Import Job for Azure
10.6.5- Bootstrapping job for Azure
10.6.6- Firefighter IDs
10.6.7- Privileged Access Assets & Sessions

Objective 10:7 – Granular Password Policies

10.7.1- Key Highlights of the Feature
10.7.2- Granular Password Policies – Configuration
10.7.3- Granular Policy Options
10.7.4- Manually Rotating Password using Policies
10.7.5- On-demand Password Change different Scenarios
10.7.6- Vault New Passwords for Disconnected Applications

Sample Questions

Sample questions presented here are examples of the types of questions candidates may encounter and should not be used as a resource for exam preparation.

Sample Question 1

An Admin in Saviynt can enable/disable the Privileged Session recording feature through Global Configuration.

Options

A: True
B: False

Sample Question 2

Which of the following are the out-of-the-box (OOTB) SAV roles that allow users to request privileged access in Saviynt Identity Cloud? (Multi-Select)

Options

A: ROLE_SAV_PAMENDUSER
B: ROLE_SAV_PAMOWNER
C: ROLE_SAV_PAMADMIN
D: ROLE_ADMIN

Recertification Policy

Saviynt certification is valid for 24 months from the date of issue. To maintain the certification, the learner must complete minimum CPE training hours, including attending the Time-to-Value (TTV) workshop and completing new release summary videos. The recertification period opens 60 days before the expiry date of the certification. During the 60-day recertification period, you must submit proof of completing the minimum CPE training hours.

Also, passing a higher-level certification exam automatically renews the expiration date of the lower-level exam. The new expiry date of the lower-level exam will match the expiry date of the higher-level exam. For example, passing the Saviynt Certified Advanced Professional exam automatically renews the expiration date of the Saviynt Certified Professional Exam if you took that earlier.

Exam Fee

The exam cost will be USD 300. The cost is valid for only 1 attempt.

Exam Content Contributors

1. Anitha Swapna Paradesi - Lead Technical Training Consultant
2. Nagesh Kunchakarra – Director, Field Engineering
3. Gulshan Vaswani – Senior Director, Product Management

For more information, visit: https://saviynt.com/university
certification@saviynt.com: Certification Exams related queries
training.support@saviynt.com: Training-related queries