

Saviynt Certified Advanced PAM Professional (SCAPP)

Exam Preparation Guide

Authored by: Saviynt University

Introduction

The Saviynt Certified Advanced PAM Professional (SCAPP) certification exam validates a candidate's ability to implement, configure, and manage advanced Privileged Access Management (PAM) capabilities using the Saviynt platform. Aligned with the Saviynt PAM Level 200 training, this certification is intended for PAM Implementation Specialists, Solution Architects, and security consultants who are responsible for deploying and supporting privileged access solutions in enterprise environments. Candidates are recommended to have 3 to 6 months of hands-on experience with the Saviynt PAM solution. This certification is available exclusively to affiliated partners and customers.

The Saviynt Certified Advanced PAM Professional (SCAPP) certification validates an individual's ability to:

- Explain core PAM functionalities and features.
- Describe Just-in-Time (JIT) account naming, workflow customizations, and privileged role elevation.
- Utilize bulk update APIs across various PAM use cases.
- Apply granular password controls and review the password history of privileged accounts.
- Manage Windows service accounts and IIS application pools.
- Explain native SSH capabilities, Integration support for FIPS and ESXi servers.
- Configure and onboard systems such as on-premises environments, Active Directory, SAP, Okta, and Azure into PAM solutions.
- Implement advanced PAM controls, including SIEM integrations with tools like Splunk.
- Troubleshoot issues and effectively analyze root causes and logs.

Minimally Qualified Candidate

We recommend that candidates have at least 3-6 months of hands-on experience with the Saviynt PAM platform in any role, including PAM architects, consultants, engineers, managers, decision-makers, and those working in PAM sales and pre-sales departments. The minimally qualified candidate (MQC) possesses the skills to deploy, configure, and manage Saviynt PAM solutions.

Recommended General IT Knowledge

Candidates should have a basic understanding of cloud computing concepts and Cybersecurity.

Exam Pre-requisite

It is mandatory to complete the **Saviynt PAM Level 200** classroom or self-paced training before scheduling the exam.

Exam Delivery

This is an online proctored exam delivered through ProctorU. Go to [ProctorU Test-Taker Library](#) to learn more about the certification exam requirements.

Exam Content

Question Types

There are various types of questions on the examination:

- **Multiple choice:** One correct response and three incorrect responses (distractors).
- **Multiple response:** Has two or more correct responses out of four options.
- **Scenario-Based:** Based on a given scenario/use case, it will have one or more correct responses out of four options.

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 Advanced PAM Professional (SCAPP) examination contains 50 multiple-choice questions and lasts 2 hours.

Exam Results

The Saviynt Certified Advanced PAM Professional 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 examination results are reported as a score from 0 to 100, with a minimum passing score of 65%. 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.

Saviynt Certified Advanced PAM Professional (SCAPP) – FAQs

What is SCAPP?

The **Saviynt Certified Advanced PAM Professional (SCAPP)** examination is an advanced-level certification for the Saviynt Privileged Access Management platform.

Who should earn the SCAPP certification?

This certification is exclusively available to affiliated partners and customers. It is designed for individuals with the skills to implement and manage use cases ranging from basic to medium complexity. Candidates should have 3-6 months of hands-on experience with identity security solutions using Saviynt PAM.

What is the best way to prepare for the SCAPP exam?

The preparation is generally a 2-step process:

- Complete the mandatory Saviynt PAM Level 200 training.
- Practice the training labs and gain hands-on experience as a PAM professional.

How long is this certification valid for?

The certification is valid for two years from the date of passing the exam.

Do I need to pass the Saviynt PAM Professional certification exam before taking the Advanced PAM Professional exam?

While obtaining a professional-level certification is beneficial for PAM professionals, passing the Saviynt Certified PAM Professional exam is not a prerequisite for the Saviynt Certified Advanced PAM Professional exam.

Additionally, earning a higher-level certification automatically extends the validity of lower-level certifications to match the higher-level certification's expiration date. For example, if you pass the Saviynt Certified Advanced Professional exam after completing the Professional exam, the Professional certification's expiration date will align with that of the Advanced certification.

Content Outline

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

Section	Topic	# of questions
01	Advanced PAM Onboarding	10
02	Advanced Access Controls	5
03	Advanced Privileged Access Methods	10
04	Password Management	5
05	Privileged Access to Connected Applications	5
06	Privileged Access Across Workloads	5
07	Advanced PAM Controls	5
08	Troubleshooting Issues	5
Total		50

Section 1 – Advanced PAM Onboarding

Objective 1:1 – Bootstrap Using EVQuery

- 1.1.1- Bootstrapping
- 1.1.2- EV Query using Custom Property
- 1.1.3- EV Query using Tags

Objective 1:2- Onboarding On-Premises Workloads

- 1.2.1- Onboard using Saviynt Scanning Tool
- 1.2.2- Onboard using a manually created CSV
- 1.2.3- Automated Onboarding

Objective 1:3 – Onboarding Azure

- 1.3.1- Azure Integration
- 1.3.2- Azure Connection
- 1.3.3- Azure Bootstrapping
- 1.3.4- Endpoint Mapping between Azure AD and Azure

Objective 1:4 – Onboarding Active Directory

- 1.4.1- Saviynt Identity Cloud and Active Directory Integration
- 1.4.2- AD Connection
- 1.4.3- AD Bootstrapping
- 1.4.4- Domain joined windows servers using AD Accounts
- 1.4.5- Associate Remote Apps with AD Endpoints

Objective 1:5 – Bulk Update APIs for PAM

- 1.5.1- Bulk Updating Specific PAM-Enabled Endpoints
- 1.5.2- Bulk Updating All PAM-Enabled Endpoints
- 1.5.3- Bulk Update View Password Parameter for All Credential-less Accounts
- 1.5.4- Bulk Update View Password Using Account and Endpoint Names
- 1.5.5- Bulk Update View Password Using Account Keys
- 1.5.6- Bulk Update View Password Using Account Keys, Account and Endpoint Names

Objective 1:6 – Real-Time Workload Discovery

- 1.6.1- Real-Time Discovery for AWS
- 1.6.2- Real Time Discovery for GCP

Section 2 – Advanced Access Controls

Objective 2:1 – Managing Endpoint Visibility

- 2.1.1- Endpoint Visibility
- 2.1.2- Prerequisites of Endpoint policies
- 2.1.3- Updating Existing Endpoints with Tags

Objective 2:2 – Endpoint Group Policies

- 2.2.1- Endpoint Group Policies
- 2.2.2- Entitlements Selection to Specify Access
- 2.2.3- Endpoint Group Policy Conditions
- 2.2.4- Endpoint List – Policy Access

Objective 2:3 – Managing Account Visibility

- 2.3.1– Account Visibility
- 2.3.2– Default Analytic Controls for Account Visibility
- 2.3.3- Use Case 1: Visibility of Shared Accounts and A-Accounts
- 2.3.4- Use Case 2: Visibility of Shared Accounts to Specific Users

Section 3 - Advanced Privileged Access Methods

Objective 3:1 – Privileged Role Elevation

- 3.1.1- Emergency Access Role
- 3.1.2- Check Out Role Request Details

Objective 3:2 – Emergency Roles Access Policy

- 3.2.1- Emergency Roles Access Policy
- 3.2.2- Prerequisites of Emergency Roles Access Policy

Objective 3:3 – Bulk Role Select Mode

- 3.3.1- Bulk Role Select Mode
- 3.3.2- Check Out Role Options
- 3.3.3- Enable Bulk Role Selection
- 3.3.4- Roles Filter and Manage Selections
- 3.3.5- Limitations on Roles Selection

Objective 3:4 – JIT Task Creation

- 3.4.1- Just-In-Time (JIT) Access Method
- 3.4.2- Global Configurations - JIT
- 3.4.3- JIT Request – Temporary Privileged Account

Objective 3:5 – JIT Account Name Rule Customization

- 3.5.1- Account Name Rule
- 3.5.2- Account Name Rule Attribute – Basic Config
- 3.5.3- Account Name Rule Attribute – Advanced Config

Objective 3:6 – JIT Account Workflow Customization

- 3.6.1- JIT Workflow

Section 4 - Password Management

Objective 4:1 – Break Glass

- 4.1.1- Break Glass Process
- 4.1.2- Break Glass Workflow
- 4.1.3- Initializing Break Glass Session

Objective 4:2 – Retrieving Account Password History

- 4.2.1- Steps to Retrieve the Password History of a Shared Account
- 4.2.2- Steps to Retrieve the Password History of Connection Credentials

Objective 4:3 – Granular Password Rotation Policies

- 4.3.1- Prerequisite: Enable Account Password Rotation Policies
- 4.3.2- Account Password Rotation Policies
- 4.3.3- Granular Policy Option

Objective 4:4 – Rotating Password Manually Using Policies

- 4.4.1- Manual Password Change as On and Allow Manual Entry as On
- 4.4.2- Manual Password Change as Off and Allow Manual Entry as On
- 4.4.3- Manual Password Change as On and Allow Manual Entry as Off
- 4.4.4- Manual Password Change as Off and Allow Manual Entry as Off
- 4.4.5- Managing Privileged Accounts Without Password Rotation

Objective 4:5 – Password Reconciliation

- 4.5.1- Password Reconciliation
- 4.5.2- Initial Setup
- 4.5.3- Password Reconciliation Job
- 4.5.4- PAMEnabledOutOfBandAccounts Analytical Control

Section 5 – Privileged Access to Connected Applications

Objective 5:1 – Identity Repository of Applications

- 5.1.1- Identity Repository of Applications
- 5.1.2- Integration Between Saviynt Identity Cloud and Apps
- 5.1.3- Prerequisites – Okta and SAP

Objective 5:2 - SAP Connection

- 5.2.1- SAP Connected Application
- 5.2.2- Create SAP Connection
- 5.2.3- Options to Create SAP Connection
- 5.2.4- SAP Connection Parameters
- 5.2.5- SAP Provisioning Parameters

Objective 5:3 - Privileged Access for SAP Application

- 5.3.1- Requesting and Accessing Privileged Sessions
- 5.3.2- Privileged Access for SAP Application
- 5.3.3- Check Out Credentials
- 5.3.4- Connect To Session
- 5.3.5- Launch Session
- 5.3.6- Managing Privileged Access

Objective 5:4 – Okta Connection

- 5.4.1- Creating the Okta API Token
- 5.4.2- Create Okta Connection

Objective 5:5 – Privileged Access for Okta Application

- 5.5.1- Execute PAM Bootstrap Job for Okta
- 5.5.2- Validate Bootstrapping Process

Section 6 – Privileged Access Across Workloads

Objective 6:1 – Windows Service Account Management

- 6.1.1- Windows Service Accounts
- 6.1.2- Prerequisites to Enable the Password Rotation
- 6.1.3- Password Rotation JAR File – Platform Service Accounts
- 6.1.4- Periodic Password Rotation
- 6.1.5- ServiceRestartAfterPassChange
- 6.1.6- Periodic Password Rotation – AD and Local Accounts
- 6.1.7- Task Status – After Using Password Rotation JAR File
- 6.1.8- Execute Microservices Job – Password Reconcile
- 6.1.9- Task Status – After Using Password Reconcile Job

Objective 6:2 – IIS Application Pool

- 6.2.1- IIS Application Pool
- 6.2.2- New Capabilities of this feature
- 6.2.3- IIS Pool – Technical Details
- 6.2.4- Sample ChangeCredentialJson Config

Objective 6:3 – Native SSH - Bring Your Own Tool

- 6.3.1- Bring Your Own Tool – Native SSH
- 6.3.2- Supported Authentication Methods
- 6.3.3- Managing Native SSH Sessions
- 6.3.4- Auditing & Monitoring – Native SSH
- 6.3.5- SSH Login and Authorization
- 6.3.6- Initiate Privileged Sessions using Native SSH Clients

Objective 6:4 – Integration Support with FIPS

- 6.4.1- Federal Information Processing Standards (FIPS)
- 6.4.2- New APIs Introduced for FIPS
- 6.4.3- Managing Certificates for Credential-less Access
- 6.4.4- Credential-less Session Launch

Objective 6:5 – Integration with ESXi Servers for PAM

- 6.5.1- Integration with the ESXi Servers for PAM
- 6.5.2- Key Features of VMware ESXi Infrastructure Support
- 6.5.3- ESXi Integration Enhancements
- 6.5.4- Check-Out and Check-In of ESXi Credentials

Section 7 – Advanced PAM Controls

Objective 7:1 – SIEM Integration

- 7.1.1- Prerequisites of SIEM Integration
- 7.1.2- Integration between Saviynt Identity Cloud and Splunk
- 7.1.3- Options to Generate and Obtain Data
- 7.1.4- Creating an Analytics Record
- 7.1.5- Schedule a Job

Section 8 – Troubleshooting Issues

Objective 8:1 – Log Viewer Features and Search Queries

- 8.1.1- Log Viewer Page
- 8.1.2- Log Viewer Features
- 8.1.3- Log Search Results
- 8.1.4- Commonly Used Log Search Queries
- 8.1.5- Commonly Used Log Search Keywords

Objective 8:2 - Log Analysis

- 8.2.1- Troubleshooting – Connection Failure

Objective 8:3 – Implementation Methodology

- 8.3.1- Prerequisites for PAM Implementation
- 8.3.2- Checklist for Saviynt Identity Cloud for PAM Use Cases

Objective 8:4 – Best Practices and Troubleshooting

- 8.4.1- Troubleshooting Real-time Use Case:1
- 8.4.2- Troubleshooting Real-time Use Case:2
- 8.4.3- Troubleshooting Real-time Use Case:3
- 8.4.4- Root Cause Analysis - Session Connectivity and Launch Failures (SSH, RDP and Remote Apps)
- 8.4.5- Root Cause Analysis - Credential Check out and Password Issues (Vault)
- 8.4.6- Root Cause Analysis - Task Provisioning and Job Failures
- 8.4.7- Root Cause Analysis - Endpoint Visibility and Account Visibility Control
- 8.4.8- Root Cause Analysis - Bootstrap Failures
- 8.4.9- Root Cause Analysis - Session Recording and Playback Issues

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

Is it possible to make an application requestable only for certain users?

Options

- A: True
- B: False

Sample Question 2

Which role types can be created in Saviynt? Select all correct options.

Options

- A: Enterprise
- B: Firefighter
- C: Entitlement
- D: Application

Recertification Policy

Saviynt certification is valid for 24 months from the date of issue. To maintain the certification, the learner must complete a minimum of CPE training hours, including attending the Time-to-Value (TTV) workshop or 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 one attempt.

Exam Content Contributors

1. Anitha Swapna Paradesi – Manager, Training
2. Nirav Dedhia – Principal Technical Solutions Engineer, Solutions Engineering
3. Krishna Chander G – Sr. Technical Training Consultant, Training
4. Nagesh Kunchakarra – Director, Product Management
5. Eyal Koren – Director, Professional Services
6. Matt Smith – VP, Solutions Engineering
7. Ragul G – Consultant, Professional Services
8. Rajashekar P – Technical Architect, Professional Services

For more information, visit: <https://saviynt.com/university>

Visit the [ProctorU Test-Taker Library](#) for certification exam requirements

Reach out to certification@saviynt.com for certification exam-related questions

Reach out to training.support@saviynt.com for training-related questions