Saviynt

SAVIGA-C01 Exam

Saviynt Certified IGA Professional Exam (L100)

Questions & Answers
Demo

Version: 4.0

Question: 1

Which of the following options support Authentication Mechanisms in Saviynt?

A. None of the below
B. REST
C. LDAP
D. SAML 2.0
E. Database

Answer: D

Explanation:

Saviynt primarily leverages SAML 2.0 as its core authentication mechanism. SAML (Security Assertion Markup Language) is an open standard for exchanging authentication and authorization data between parties, in this case, between users and Saviynt. It allows for secure, single sign-on experiences.
While Saviynt can interact with databases, REST APIs, and LDAP directories for various purposes like identity data aggregation or provisioning, these are not its primary authentication methods.
Databases: Saviynt can connect to databases to pull identity information, but the platform itself doesn't authenticate users directly against a database.
REST: REST APIs are used for programmatic interaction with Saviynt, not typically for initial user authentication.
LDAP: While LDAP can be a source of identity data, Saviynt's core authentication relies on SAML for its standardized and secure approach.
Key Saviynt IGA references supporting this:
Saviynt Documentation: The official Saviynt documentation consistently refers to SAML as the primary authentication mechanism.
Saviynt Connectors: Saviynt provides pre-built connectors for various identity providers (IdPs) that support SAML, further emphasizing its reliance on this standard.
Saviynt Training Materials: Saviynt's training courses and certifications highlight SAML's role in the platform's authentication framework.

Question: 2

In the process of setting up Single Sign-On using SAML 2.0, the "SP Entity ID" acts as a unique identifier for the Saviynt SP. If "SP Entity ID" is set to the value of SaviyntSP, which of the following will be the correct Single Sign-On URL to log in to EIC?

A. https://myorg.saviyntcloud.com/ECM/saml/SSO/SaviyntSP
B. https://myorg.saviyntcloud.com/SaviyntSP
C. https://myorg.saviyntcloud.com/ECM/saml/SSO/alias/SaviyntSP

Answer: C

Explanation:

In Saviynt's SAML 2.0 based Single Sign-On (SSO) configuration, the "SP Entity ID" uniquely identifies Saviynt as the Service Provider (SP) to the Identity Provider (IdP). The correct SSO URL structure incorporates this "SP Entity ID" within a specific path.
Saviynt's URL Structure: Saviynt's SSO URLs follow a pattern to ensure proper routing and authentication. The /ECM/saml/SSO/alias/ portion is crucial for directing SAML-based login attempts.

Why the other options are incorrect:
A . https://myorg.saviyntcloud.com/ECM/saml/SSO/SaviyntSP: This URL is missing the crucial "alias" segment in the path, making it invalid for SAML SSO.
B . https://myorg.saviyntcloud.com/SaviyntSP: This URL doesn't include the necessary components for SAML-based authentication within Saviynt.
Saviynt IGA Reference:
Saviynt Documentation: Saviynt's official documentation on configuring SAML SSO provides details on the correct URL structure and the significance of the "SP Entity ID."
Saviynt Support: Saviynt's support resources and knowledge base articles often address issues related to SSO configuration, reinforcing the correct URL format

Question: 3

The Max Authentication Session parameter in Single Sign-On settings specifies the maximum duration, in seconds, for which an SSO session will remain valid. The default value is 3600 seconds. If the session logout value defined in IDP is 10,000 seconds and Max Authentication Session in Saviynt SSO is 5000 seconds, how long will the session last?

A. 5000 seconds
B. 10,000 seconds
C. 3600 seconds
D. None of the above

Answer: A

Explanation:

In Saviynt's SSO setup, the "Max Authentication Session" parameter determines the maximum duration of an SSO session within Saviynt, overriding any longer durations set by the Identity Provider (IdP).
Session Duration Logic: Saviynt's internal session timeout setting takes precedence over the IdP's session timeout. This ensures that Saviynt can enforce its own security policies regarding session lifetimes.
Why other options are incorrect:
B . 10,000 seconds: This is the IdP's session logout value, but Saviynt's "Max Authentication Session" setting overrides it.
C . 3600 seconds: This is the default value, but the question specifies a configured value of 5000 seconds.
Saviynt IGA Reference:
Saviynt Documentation: The documentation for configuring SSO settings within Saviynt explains the "Max Authentication Session" parameter and its impact on session duration.
Saviynt Best Practices: Saviynt's best practices for SSO often recommend aligning session timeouts between the IdP and Saviynt to avoid confusion and potential security gaps.

Question: 4

Single Sign-On is enabled in EIC using Azure Identity Provider. In this scenario, can the user log in using Azure and EIC native authentication?

A. True
B. False

Answer: B

Explanation:

When Single Sign-On (SSO) is enabled in Saviynt EIC using an external Identity Provider (IdP) like Azure AD, it generally becomes the exclusive authentication method. This means users cannot use Saviynt's native authentication (i.e., logging in with a username/password stored directly within Saviynt).
Reasons for this:
Security and Centralized Control: SSO with an IdP enhances security by centralizing authentication and enforcing stronger password policies. Allowing native logins would create a potential bypass of these security measures.
User Experience: SSO provides a seamless login experience, eliminating the need for users to remember multiple credentials. Offering both SSO and native logins could lead to confusion and a less streamlined process.
Administrative Efficiency: SSO simplifies user management by delegating authentication to the IdP. Administrators don't need to manage separate user accounts and passwords within Saviynt.
Saviynt IGA Reference:
Saviynt Documentation: Saviynt's documentation on SSO configurations emphasizes that enabling SSO typically disables native authentication methods.
Saviynt Best Practices: Saviynt's best practices for SSO recommend enforcing SSO as the sole

authentication method for improved security and user experience.
Saviynt Implementation Guides: Implementation guides for setting up SSO with various IdPs, including Azure AD, often highlight the exclusive nature of SSO authentication.

Question: 5

Which of the following Role types should be selected for a Role containing Entitlements that span across multiple applications?

A. Application Role
B. Transactional Role
C. Enabler Role
D. Enterprise Role

Answer: D

Explanation:
In Saviynt, Enterprise Roles are specifically designed to encompass entitlements that span multiple applications. This is in contrast to Application Roles, which are limited to entitlements within a single application.
Enterprise Roles: Provide a way to group entitlements across different applications, reflecting a user's overall job function or responsibilities within the organization. This is essential for managing access for users who need permissions in various systems to perform their duties.
Other Role Types:
Application Role: Grants permissions specific to a single application.
Transactional Role: Focuses on granting permissions for specific tasks or transactions within an application.
Enabler Role: Provides supplementary permissions that enhance or support other roles.
Saviynt IGA Reference:
Saviynt Documentation: The section on Role Management within Saviynt's documentation clearly defines the different role types and their purposes.
Saviynt Training Materials: Saviynt's training courses emphasize the importance of Enterprise Roles in managing cross-application access.