PassQueen
a.k.a dumpsqueen.com

JumpCloud Core Certification Exam

JumpCloud JumpCloud-Core

Version Demo

Total Demo Questions: 10

Total Premium Questions: 103

Buy Premium PDF

https://passqueen.com

support@passqueen.com

QUESTION NO: 1

A wireless access point is configured with an incorrect shared secret for a JumpCloud RADIUS server. What is the expected result? Select the correct answer.

A. The access point will be unable to authenticate users through the RADIUS server.

B. The access point will automatically retrieve the correct shared secret.

C. Users will be prompted to create a new JumpCloud password.

D. The RADIUS server will use the Organization ID instead of the shared secret.

ANSWER: A

Explanation:

The wireless access point will be unable to authenticate successfully with the JumpCloud RADIUS service. The shared secret is configured on both the RADIUS client, such as an access point or VPN appliance, and the JumpCloud RADIUS configuration. It is used to validate and protect communication between the RADIUS client and server. If the values do not match, JumpCloud cannot validate the RADIUS client request, and authentication attempts through that client will fail.

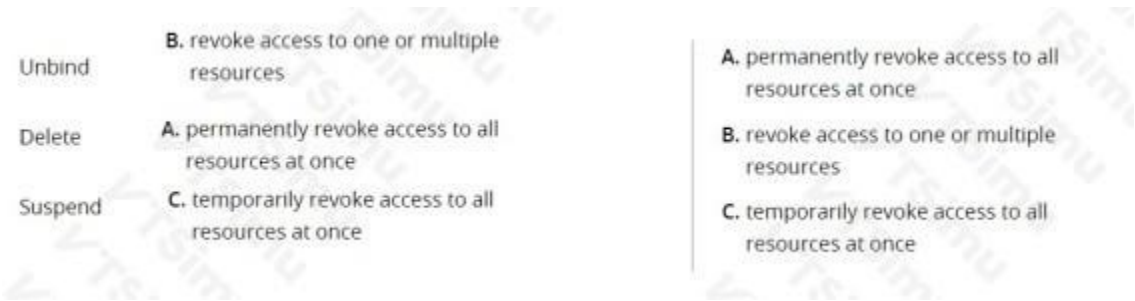
The shared secret is separate from a user's JumpCloud username and password. Users provide their individual credentials during authentication, while the shared secret establishes the trusted RADIUS-client connection. See JumpCloud's Configure RADIUS documentation for configuration guidance.

QUESTION NO: 2 - (DRAG DROP)

DRAG DROP

There are multiple options to de-provision a user's access to JumpCloud resources. Match the following options to their suggested use case.

ANSWER:



Explanation:

JumpCloud provides different de-provisioning actions so administrators can apply the least disruptive action that meets the access-control need. Unbinding a user removes that user's association with selected JumpCloud resources, such as a

particular user group, system, application, directory, or other assigned resource. The user remains active in JumpCloud and retains any other assignments that were not removed. This makes unbinding the appropriate action when access must be revoked from one resource or from a selected set of resources without ending the user's broader access.

Deleting a user is the permanent lifecycle action. It removes the user record from the organization and revokes the user's access across assigned JumpCloud resources. This is the suitable outcome when the identity should no longer exist in the organization, such as after an employee's final offboarding has been completed. JumpCloud's guidance for deleting users is available in the Delete Users support article.

Suspending a user is designed for a temporary access interruption. A suspended user cannot access their JumpCloud-assigned resources while the user object and its resource relationships are preserved. Because the assignments remain in place, an administrator can later restore access by unsuspending the account rather than rebuilding assignments. This supports situations such as a leave of absence, an investigation, or a temporary security hold. See JumpCloud's Suspend Users documentation for the suspension workflow and restoration behavior. Together, these actions let administrators selectively remove access, permanently offboard an identity, or pause all access while retaining the account for later reactivation.

QUESTION NO: 3 - (DRAG DROP)

DRAG DROP

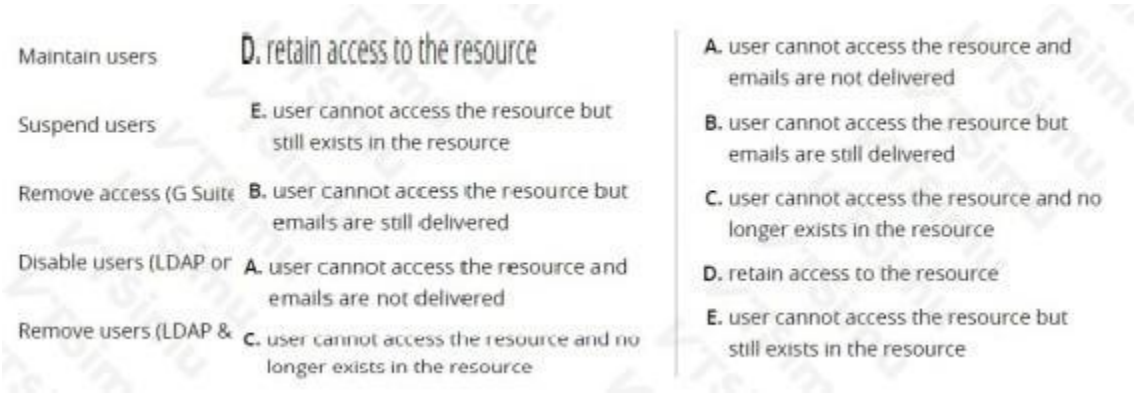
Upon user lockout in JumpCloud, administrators can customize the resulting behavior for user access to

other resources. For example, when a user gets locked out of JumpCloud, I want to

"suspend users" in G

Suite. Match the behavior to its definition.

ANSWER:



Explanation:

These mappings correctly distinguish the lifecycle and access outcomes JumpCloud can apply to downstream resources when a JumpCloud user is locked out. "Maintain users" preserves the account's existing access to the connected resource, so the user continues to retain access. "Suspend users" keeps the user record in the target resource while preventing the

user from accessing it. This is appropriate where the external account and its associated data should remain in place, but active sign-in must stop.

For Google Workspace, “Remove access (G Suite only)” blocks the user’s access while preserving mail delivery. This supports a lockout workflow in which the person should no longer use the resource but messages can still arrive at their mailbox or be handled according to the organization’s Google Workspace policies. “Disable users (LDAP only)” prevents access and stops email delivery, reflecting the disabled-account state defined for that integration behavior.

“Remove users (LDAP & RADIUS only)” is the fullest removal action in this set: the user cannot access the resource and the account no longer exists in that resource. The completed matching therefore accurately reflects whether the account remains, whether access is retained or blocked, and whether email delivery continues. JumpCloud’s documentation on locking user accounts and its identity management capabilities provides context for centrally managing user access and account state across connected resources.

QUESTION NO: 4 - (SIMULATION)

There are multiple options to de-provision a user’s access to JumpCloud resources. Match the following options to their suggested use case.

ANSWER: Check the explanation for the answer

Explanation:

Correct matches:

Unbinding removes the user from selected resource associations, while deleting removes the user permanently. Suspending disables the user’s access without deleting the account, allowing access to be restored later.

QUESTION NO: 5

When configuring a custom SAML 2.0 application in JumpCloud, which values are commonly provided by the service provider? Select all that apply.

A. Assertion Consumer Service (ACS) URL

B. Service Provider Entity ID

C. Required NameID format or user identifier

D. JumpCloud administrator password

ANSWER: A B C

Explanation:

The service provider provides information that identifies its SAML service and determines where it receives SAML authentication responses. The **ACS URL**, also known as the Assertion Consumer Service URL, is the endpoint where the service provider receives the SAML response after authentication. The **Service Provider Entity ID** uniquely identifies the service provider in the SAML trust relationship.

The service provider also specifies the identifier and attribute requirements it expects, including the required NameID format or user identifier. JumpCloud acts as the identity provider and uses its configured signing certificate and private key to sign assertions. See JumpCloud's SAML 2.0 SSO documentation for SSO configuration concepts.

QUESTION NO: 6

Within a single JumpCloud org, users are unique by _____? Select all that apply.

A. Last name

B. Email address

C. Username

D. First name

ANSWER: B C

Explanation:

Within a single JumpCloud organization, users are uniquely identified by both their email address and their username. The email address is a core identity attribute used for user records, communications, account-related workflows, and integrations that map a person to their JumpCloud identity. Administrators should therefore enter an email address that is not already associated with another user in the same organization.

The username is also an organization-level unique identifier. It is the account name used by systems associated with JumpCloud, including directory and device access workflows, so no two users in the organization can use the same username. This distinction is important when an administrator is provisioning users in bulk or connecting identity sources: a user may have a display-oriented first or last name that overlaps with another person, but the email address and username must remain unique to reliably identify the account.

When creating, importing, or managing users, validate both fields before provisioning to avoid identity conflicts and failed synchronization. JumpCloud's user-management documentation and API reference describe the user object and the identity attributes administrators manage: JumpCloud Documentation and JumpCloud API Reference.

QUESTION NO: 7

What status will a user be in if they have been added or imported to JumpCloud but their password has not been set? Select the correct answer.

A. Active (Green)

B. Pending (Orange)

C. Locked (Red)

D. Suspended (Grey)

ANSWER: B

Explanation:

A newly added or imported JumpCloud user whose password has not yet been set is in the **Pending (Orange)** status. This status indicates that the user account exists in the JumpCloud organization but has not completed the activation process required to establish credentials. A user may reach this state after an administrator creates the account manually, imports users from a directory or file, or otherwise provisions the identity without supplying an initial password. The user must set a password—typically through the activation email or an administrator-driven password process—before the account can become active and be used for normal authentication workflows. Administrators can use the Users area of the JumpCloud Admin Portal to identify pending accounts and take appropriate action, such as resending an activation email where applicable. This lifecycle status helps distinguish accounts awaiting initial credential setup from accounts that are ready for

use. JumpCloud documents user account status and activation behavior in its User States guide and describes user onboarding and account activation in the Add Users documentation.

QUESTION NO: 8

Active users with local administrative privileges can install the JumpCloud agent on their own machine

via the JumpCloud user portal.

A. True

B. False

ANSWER: A

Explanation:

True is correct. JumpCloud supports user-initiated agent installation through the User Portal. An active JumpCloud user can sign in to the portal and obtain the appropriate JumpCloud agent installer for their device. Installing endpoint-management software requires elevated privileges at the operating-system level, so the user must have local administrator rights on the computer to complete the installation. After installation, the agent connects the device to the organization's JumpCloud tenant and allows the administrator to manage the system according to assigned policies, commands, and associations.

This workflow is useful when administrators want users to enroll personally assigned devices without requiring an administrator to manually install the agent on every endpoint. The device must be able to reach JumpCloud services during installation and enrollment, and the user must be active so they can authenticate to the User Portal. JumpCloud documents the User Portal as a location where users can download the agent, while its agent-installation guidance identifies the administrative permissions required to install it. See JumpCloud: Using the User Portal and JumpCloud: Install the JumpCloud Agent.

QUESTION NO: 9

You must enable at least 1 LDAP bind DN to configure LDAP.

A. True

B. False

ANSWER: A

Explanation:

True is correct. A JumpCloud LDAP Bind DN is the service-account identity that an LDAP client uses to authenticate to JumpCloud's LDAP service before it can perform directory searches or other permitted LDAP operations. Consequently, enabling a Bind DN is a required part of making an LDAP integration operational: the application needs both the JumpCloud LDAP endpoint and valid Bind DN credentials to establish its authenticated connection. In the JumpCloud Admin Portal, administrators create and enable Bind DN entries, assign the appropriate user groups to those entries, and use the generated Bind DN and password in the LDAP client's configuration. This design provides a controlled, auditable credential for an application or service rather than requiring the application to bind as an individual end user. The Bind DN's assigned groups also determine the directory data that is available to the connected application, supporting least-privilege access. Therefore, at least one enabled LDAP Bind DN is necessary when configuring a functioning JumpCloud LDAP integration. See JumpCloud's LDAP service overview and its LDAP support resources for configuration guidance.

QUESTION NO: 10

What SSH key actions can an end user perform from the JumpCloud User Portal? Select all that apply.

A. Add a public SSH key

B. Remove a public SSH key

C. Upload a private SSH key for storage in JumpCloud

D. View another user's private SSH key

ANSWER: A B

Explanation:

The JumpCloud User Portal allows users to manage public SSH keys associated with their JumpCloud identity. A user can add a public SSH key so that it can be provisioned to systems where the user has appropriate access. A user can also remove a public SSH key that is no longer trusted or needed.

Private SSH keys are not uploaded to JumpCloud for management through the User Portal. A private key must remain under the control of its owner because it is the secret portion of the SSH key pair. See JumpCloud's User Portal documentation for supported end-user self-service functions.