DUMPSARENA

Atlassian Cloud Organization Admin Certification

Atlassian ACP-520

Version Demo

Total Demo Questions: 8

Total Premium Questions: 82

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

Topic Break Down

Topic	No. of Questions
Topic 1, User management	36
Topic 2, Product administration	13
Topic 3, Security	3
Topic 4, Organization administration	29
Topic 5, Mix Questions	1
Total	82

QUESTION NO: 1

You are viewing a list of names under Directory > Users.

The status for Rolf shows as "Active".

Which statement is definitely true?

A. Rolf belongs to at least one group.

B. Rolf's access has not been suspended.

C. Rolf has a managed account.

D. Rolf accessed your site within the past 24 hours.

E. Rolf has access to at least one product.

ANSWER: B

Explanation:

Rolf's access has not been suspended is definitely true. In Atlassian Administration, the user status shown in the organization directory reflects whether the person's account is currently able to use Atlassian services available to them. An *Active* status means the account is enabled rather than suspended. Therefore, an organization administrator has not applied a suspension that prevents Rolf from accessing the organization's Atlassian products and services.

This status is specifically about the account's current enabled state. It is useful to distinguish this from permissions and activity data: account status tells an administrator whether the account is active or suspended, while product roles, group membership, and recent usage are managed and reported separately. An active account can remain active even when its product access or group assignments change over time. Atlassian's user-management documentation describes suspending a user as preventing that user from accessing Atlassian products, making the active directory status the appropriate confirmation that suspension is not in effect. See Atlassian's guidance for suspending users and its documentation for managing organization users.

QUESTION NO: 2

Contractor Priya has access to Jira Software and Confluence through separate groups.

Her contract ends, but she must retain Confluence access for two weeks to complete documentation. Her Jira Software access comes only from the group "jira-contractors".

What is the most appropriate action?

A. Remove Priya from the "jira-contractors" group.

B. Suspend Priya's account.

C. Delete Priya's Atlassian account.

D. Remove Priya from every group in the organization.

E. Remove the Confluence User role from Priya.

ANSWER: A

Explanation:

Remove Priya from **jira-contractors**. Since that group is her only source of Jira Software access, removing her from it removes Jira Software access while leaving her separate Confluence access intact.

Suspending Priya would prevent access to Atlassian products more broadly. Deleting her Atlassian account or removing her from all groups would also remove access that she still needs.

QUESTION NO: 3

Your organization has multiple sites and Ann is a user.

The domain of Ann's email address is not verified.

What is possibly true about Ann's account?

A. She has a managed account in another organization.

B. You can enforce two-step verification on her account.

C. You can deactivate her account.

D. She has a managed account in one of your sites.

E. You can delete her account.

ANSWER: A

Explanation:

She has a managed account in another organization. Atlassian account management is based on verified email domains at the organization level, not on which individual Atlassian site a person can access. When your organization has not verified the domain in Ann’s email address, it does not have ownership of that domain and therefore does not manage Ann’s Atlassian account through its organization. This does not mean the account cannot be managed at all: another Atlassian organization may have verified that same domain and, as a result, may manage accounts whose email addresses use it. Domain verification establishes the organization’s ability to claim and manage the related user accounts, including applying centralized account controls. The fact pattern specifically says only that the domain is not verified by *your* organization, so management by a different organization remains possible. Atlassian documents that verifying a domain allows an organization to manage the accounts associated with that domain, and that managed accounts belong to the organization that verified and claimed them. See Verify a domain to manage accounts and What are managed accounts?.

QUESTION NO: 4

Your Cloud organization has multiple products on multiple sites.

Currently, Edmund is a brand new user with no product access.

You selected Edmund from Directory > Users, clicked "Add products", and set the User product role from the Product roles dropdown for a single product on

a single site. For all other products, the Product roles dropdown was None.

Which is NOT a possible outcome for Edmund?

A. He gains access to different products on multiple sites.

B. He is granted product admin privileges.

C. He gains access to the same product on multiple sites.

D. He gains access to a single product on a single site.

E. He gains access to multiple products on a single site.

F. He is granted org admin privileges.

ANSWER: F

Explanation:

He is granted org admin privileges is the outcome that is not possible through this action. The *Add products* workflow controls a user's access to specific Atlassian cloud products and sites by assigning product roles. Selecting the User product role for a product on one site can grant that product access, and product-access configuration, such as group-based access, can affect the resulting access pattern. However, an organization administrator role is separate from product access and from product-level roles. Organization admins manage organization-wide settings such as managed accounts, domains, security policies, user provisioning, and product administration across the organization. That authority must be assigned explicitly in the organization's administrator settings; it is not inherited or automatically granted when a user receives a product role. Therefore, assigning Edmund the User role in the product-access flow cannot make him an organization admin. Atlassian distinguishes organization administration from site and product administration in its administration model. See Atlassian's guidance on giving users access to products and managing organization admins.

QUESTION NO: 5

The group `legacy-contractors` currently grants Confluence and Jira Software product access. It is also referenced in a Jira permission configuration.

The organization is replacing the group with separate groups for current contractors and former contractors.

Which two actions should be completed before deleting `legacy-contractors` to avoid unintended loss of access? (Choose two.)

A. Grant the replacement groups the required Confluence and Jira Software product roles.

B. Replace the group in the Jira permission configuration.

C. Delete the group and recreate it after the replacement groups are populated.

D. Remove the organization's verified email domain.

E. Suspend the group before deleting it.

ANSWER: A B

Explanation:

Grant the replacement groups the required Confluence and Jira Software product roles and **replace the group in the Jira permission configuration** are correct. The original group currently has both product-access and Jira-permission uses. Each dependency must be replaced before the original group is deleted.

Deleting the group first can immediately remove product access and project permissions for its members. Recreating a group later with the same name is not an appropriate access-transition strategy, and changes to a verified domain do not replace group-based product or Jira permissions.

QUESTION NO: 6

Your organization has Jira Software Standard on the site `acme.atlassian.net`.

All the following people have active accounts:

• Rosa has the Jira Software User role on `acme.atlassian.net` and also has Confluence access.

• Dylan has the Jira Software User role on `acme.atlassian.net` only.

• Mina has Confluence access only.

• Omar is a portal-only customer for Jira Service Management.

Which two people are definitely included in the Jira Software billable-user count for `acme.atlassian.net`? (Choose two.)

A. Rosa

B. Dylan

C. Mina

D. Omar

ANSWER: A B

Explanation:

Rosa and Dylan are correct. Jira Software billing is based on users who have Jira Software product access for the relevant site. Rosa is counted once for Jira Software even though she also has Confluence access, while Dylan is counted because he has the Jira Software User role.

Mina has no Jira Software access, so she is not included in the Jira Software subscription count. Portal-only Jira Service Management customers do not require Jira Software product access and are not Jira Software billable users.

QUESTION NO: 7

A group named "support-agents" is the only group that grants its members Jira Service Management product access. The same group is also used in a Jira project permission configuration.

An organization admin deletes the group without replacing it.

Which two outcomes are possible? (Choose two.)

A. Members can lose Jira Service Management product access.

B. Members can lose permissions granted through the group in the Jira project.

C. Members' Atlassian accounts are automatically suspended.

D. Members automatically become unmanaged accounts.

E. Members automatically lose the organization-admin role.

ANSWER: A B

Explanation:

Deleting a group can remove product access when the group is the user's only source of the required product role. It can also affect Jira permissions where the deleted group was referenced, such as permissions in a project configuration.

Deleting a group does not suspend users, remove their managed-account status, or change organization-admin assignments. Those are separate account and role controls.

QUESTION NO: 8

Which two tasks are organization-admin tasks rather than Jira project-administration tasks? (Choose two.)

A. Verify an email domain.

B. Revoke an organization API key.

C. Configure an issue security scheme for a Jira project.

D. Edit a Jira notification scheme.

E. Create a Confluence space.

ANSWER: A B

Explanation:

Verifying an email domain and **revoking an organization API key** are organization-level tasks. Domain verification establishes the organization's authority to manage accounts associated with that domain. Organization API keys are credentials for organization administration APIs and are managed centrally in Atlassian Administration.

Configuring an issue security scheme and editing a notification scheme are Jira administration tasks. Creating a Confluence space is a Confluence content or space-administration task, not an organization-admin task.