I want site-admin role in the site I created. But when I go to [admin.atlassian.com](http://admin.atlassian.com/) → Directory → Users the roles I see are App Admin, User, User access admin.

**Understanding Site Admin Role Visibility**

In Atlassian's current centralized user management, the "site-admin" role may not always appear as a distinct label in the Directory > Users section. Instead, admin roles are managed through group membership and role assignments. The main admin roles you’ll see are:

* **Organization admin**
* **Site admin**
* **App admin**
* **User access admin**

If you only see "App Admin," "User," and "User access admin," it’s possible that the "site admin" role hasn’t been assigned yet, or the interface is showing the new role structure. To assign yourself the "site admin" role:

**How to Assign the Site Admin Role**

1. Go to [admin.atlassian.com](http://admin.atlassian.com/) and select your organization.
2. Navigate to **Directory > Users**.
3. Click your user profile.
4. Open the more actions menu (•••).
5. Select **Assign site admin role**.
6. In the Roles column for your site, select **Site admin** and then click **Grant** **1**.

**Note:** Only an organization admin can assign the site admin role. If you created the site, you should already be an organization admin and can grant yourself this role.

**Role Names and Groups**

* The "site admin" role may be managed via group membership (e.g., site-admins or org-admins), depending on when your organization was created **1**.
* If you don’t see the option to assign the site admin role, double-check your organization admin status.

Would you like step-by-step help checking your current admin roles or assigning the site admin role?

**Sources**

1. [Give users admin permissions | Atlassian Support](https://support.atlassian.com/user-management/docs/give-users-admin-permissions)

The more actions menu (•••) only has view app details and remove access

You won't see the option to assign the "site-admin" role from the more actions menu if your organization is using group-based role management. In this setup, admin roles like "site-admin" are granted by adding users to specific groups, rather than through the user profile actions menu **1**.

**How to Assign Yourself the Site Admin Role:**

1. Go to [**admin.atlassian.com**](http://admin.atlassian.com/) and select your site.
2. Click on **Groups** in the left navigation.
3. Find the group named **site-admins** (or similar).
4. Open the group and select **Add members**.
5. Add your user account to this group.

Once you’re in the "site-admins" group, you’ll have the site admin role for your site **1**.

Would you like guidance on finding the correct group or adding yourself as a member?

**Sources**

1. [Give users admin permissions | Atlassian Support](https://support.atlassian.com/user-management/docs/give-users-admin-permissions)

There is no site-admins group. Only confluence-admins-arnavaclab, confluence-guests-arnavaclab, confluence-user0access-admins-arnavaclab, confluence-users-arnavaclab and org-admins

Based on your group list, it looks like your site is using the new default group structure for Confluence Cloud, where the traditional site-admins group may not exist. Instead, admin roles are managed through groups like org-admins and confluence-admins-[sitename] **1** **2**.

* **org-admins**: Grants organization-level admin permissions, which include the ability to manage users, groups, and admin roles across all products **2**.
* **confluence-admins-arnavaclab**: Grants Confluence admin permissions for your site, allowing you to manage global and space permissions within Confluence **3**.

If you are a member of org-admins, you already have the highest level of admin access for your organization, including the ability to assign admin roles and manage groups **2**. The absence of a site-admins group is expected in this setup.

If you need to grant someone Confluence admin rights, add them to the confluence-admins-arnavaclab group. For organization-wide admin rights, add them to org-admins **3** **2**.

Is there a specific permission or action you’re unable to perform that you believe requires the site-admin role?

**Sources**

1. [What are the different types of admin roles? | Atlassian Support](https://support.atlassian.com/user-management/docs/what-are-the-different-types-of-admin-roles)
2. [Understand default groups | Atlassian Support](https://support.atlassian.com/user-management/docs/default-groups-and-permissions)

I gues, yes, I am getting Unauthorised message for calling "[https://api.atlassian.com/admin/v1/orgs/"](https://api.atlassian.com/admin/v1/orgs/%22) + orgId + "/users/search"

The "401 Unauthorized" error when calling Atlassian Cloud APIs—such as [https://api.atlassian.com/admin/v1/orgs/{orgId}/users/search—can](https://api.atlassian.com/admin/v1/orgs/%7BorgId%7D/users/search%E2%80%94can) happen for a few reasons, even if you are an org-admin:

**Key Points to Check**

* **API Token Type & Endpoint:** If you are using a scoped API token (the new default for service accounts and enhanced security), you must use the correct API endpoint format:
  + For Confluence Cloud:  
    https://api.atlassian.com/ex/confluence/<cloudid>/<api>
  + For admin APIs, ensure you are using the correct endpoint and that your token has the required scopes **1** **2**.
* **Permissions:** Even as an org-admin, some admin APIs require specific scopes or permissions set when creating the API token. Double-check that your token includes all necessary scopes for user and org management **3** **2**.
* **Token Scope Limitations:** Scoped tokens restrict what actions you can perform. If your token does not have the right scopes, you will get a 401 or 403 error **4** **3**.

**What to Do Next**

* Review your API token and ensure it was created with the correct scopes for the actions you want to perform.
* Make sure you are using the correct API endpoint for scoped tokens.
* If you are using a service account, remember that only scoped tokens are supported, and integrations may not work with these unless specifically designed for them **1** **2**.

Would you like step-by-step instructions on creating a scoped API token with the right permissions or help finding your Cloud ID for the API endpoint?

**Sources**

1. [401 Unauthorized error when service account accesses Jira or Confluence API | Atlassian Cloud | Atlassian Support](https://support.atlassian.com/atlassian-cloud/kb/401-unauthorized-error-when-service-account-accesses-jira-or-confluence-api)
2. [Manage API tokens for service accounts | Atlassian Support](https://support.atlassian.com/user-management/docs/manage-api-tokens-for-service-accounts)
3. [Manage API tokens for your Atlassian account | Atlassian Support](https://support.atlassian.com/atlassian-account/docs/manage-api-tokens-for-your-atlassian-account)
4. [Scoped API Tokens in Confluence Cloud | Confluence | Atlassian Support](https://support.atlassian.com/confluence/kb/scoped-api-tokens-in-confluence-cloud)

Which API token should I use? The one generated from <https://id.atlassian.com/> or the one generated from <https://admin.atlassian.com/?>

For Atlassian Cloud admin APIs, you should use the API token generated from your Atlassian account at <https://id.atlassian.com/manage-profile/security/api-tokens.> This token is used for authenticating scripts and API calls to Atlassian Cloud apps, including admin endpoints **1**.

If you are using a service account, you can also generate scoped API tokens from the admin portal at <https://admin.atlassian.com/> under Directory > Service accounts. These scoped tokens are specifically for service accounts and allow you to define fine-grained permissions **2**.

**Key Points:**

* For most admin API use cases as an individual user, generate your API token from [https://id.atlassian.com/](https://id.atlassian.com/%5B%5E01%5E%5D.) **1**[.](https://id.atlassian.com/%5B%5E01%5E%5D.)
* For service accounts (not regular user accounts), generate the token from [https://admin.atlassian.com/](https://admin.atlassian.com/%5B%5E02%5E%5D.) **2**[.](https://admin.atlassian.com/%5B%5E02%5E%5D.)

Would you like guidance on creating a token or selecting the right scopes for your use case?

**Sources**

1. [Manage API tokens for your Atlassian account | Atlassian Support](https://support.atlassian.com/atlassian-account/docs/manage-api-tokens-for-your-atlassian-account)
2. [Manage API tokens for service accounts | Atlassian Support](https://support.atlassian.com/user-management/docs/manage-api-tokens-for-service-accounts)

Well in that case I am using the right API tested with '<https://'+site+'/wiki/rest/api/'> urls. It just does not get authorization to call "[https://api.atlassian.com/admin/v1/orgs/"](https://api.atlassian.com/admin/v1/orgs/%22) urls

You are encountering this issue because Atlassian Cloud now has two types of API tokens: classic (unscoped) and scoped. The key difference is that:

* **Classic tokens** work with site-specific URLs like https://<your-site>.atlassian.net/wiki/rest/api/.
* **Scoped tokens** (the new default) only work with the [https://api.atlassian.com/ex/confluence/<cloudid>/<api>](https://api.atlassian.com/ex/confluence/%3Ccloudid%3E/%3Capi%3E) or [https://api.atlassian.com/ex/jira/<cloudid>/<api>](https://api.atlassian.com/ex/jira/%3Ccloudid%3E/%3Capi%3E) endpoints, and not with the old site-specific URLs **1** **2** **3**.

If your API token works with https://<your-site>.atlassian.net/wiki/rest/api/ but not with <https://api.atlassian.com/admin/v1/orgs/,> it is likely a classic token or a token without the required scopes. The admin APIs require a scoped token with the correct permissions and must be called using the <https://api.atlassian.com/> endpoints **1** **2** **3**.

**What you should do:**

* Generate a scoped API token from <https://id.atlassian.com/manage-profile/security/api-tokens> and select the necessary scopes for admin actions.
* Use the [https://api.atlassian.com/ex/confluence/<cloudid>/<api>](https://api.atlassian.com/ex/confluence/%3Ccloudid%3E/%3Capi%3E) or <https://api.atlassian.com/admin/v1/orgs/> endpoints with this token.
* Do not use the classic site-specific URL format for admin or scoped-token API calls **1** **2** **3**.

There is an ongoing feature request to allow scoped tokens to work with the old site-specific URLs, but currently, this is not supported **4**. You can watch this ticket for updates.

Would you like step-by-step help generating a scoped token and using it with the correct endpoint?

**Sources**

1. [Scoped API Tokens in Confluence Cloud | Confluence | Atlassian Support](https://support.atlassian.com/confluence/kb/scoped-api-tokens-in-confluence-cloud)
2. [401 Unauthorized error when service account accesses Jira or Confluence API | Atlassian Cloud | Atlassian Support](https://support.atlassian.com/atlassian-cloud/kb/401-unauthorized-error-when-service-account-accesses-jira-or-confluence-api)
3. [Manage API tokens for service accounts | Atlassian Support](https://support.atlassian.com/user-management/docs/manage-api-tokens-for-service-accounts)
4. [Add support for atlassian.net when sending web requests with scoped API tokens to avoid permission errors](https://jira.atlassian.com/browse/CLOUD-12617)

Okay, what scopes do I want? I see classic and granular scope types

To call <https://api.atlassian.com/admin/v1/orgs/> endpoints, you need to use an API key (not a classic or granular user API token) generated from the admin portal, specifically under Settings > API keys in your organization’s admin settings **1** **2**.

**Scope Selection:**

* When creating the API key, you’ll be prompted to select scopes. The available scopes determine what the API key can do in your organization.
* For organization and user management endpoints, select the relevant admin scopes as described in the API documentation. You can review the available scopes here: [Cloud Admin scopes](https://developer.atlassian.com/cloud/admin/scopes/) **1**.

**Classic vs. Granular (Scoped) Tokens:**

* Classic (unscoped) tokens are being deprecated and do not provide fine-grained control.
* Granular (scoped) API keys are recommended for admin APIs, as they allow you to specify exactly what the key can do, improving security **1**.

**Important:**  
Currently, the Organization REST APIs are only accessible via API keys without scopes. There is an open feature request to enable support for scoped API keys for these endpoints **3**. You can watch this ticket for updates.

Would you like step-by-step instructions for generating an admin API key or help choosing the right scopes for your use case?

**Sources**

1. [Manage an organization with the admin APIs | Atlassian Support](https://support.atlassian.com/organization-administration/docs/manage-an-organization-with-the-admin-apis)
2. [Setting up Postman for Organization User Management | Atlassian Cloud | Atlassian Documentation](https://confluence.atlassian.com/cloudkb/setting-up-postman-for-organization-user-management-1388159381.html)
3. [Enable scoped API keys to support Organisation Rest APIs](https://jira.atlassian.com/browse/JRACLOUD-94807)

So you are telling me to generate from <https://admin.atlassian.com/> and not <https://id.atlassian.com/?>

Yes, for calling admin APIs like <https://api.atlassian.com/admin/v1/orgs/,> you should generate your API key from the admin portal at <https://admin.atlassian.com/> and not from https://id.atlassian.com/ **1**.

* **API keys generated from** <https://admin.atlassian.com/> are associated with your organization and can be created with specific scopes for admin-level actions. These are required for organization-level admin APIs **1**.
* **API tokens from** <https://id.atlassian.com/> are user-based and mainly used for app-level APIs (like Jira or Confluence REST APIs), not for organization admin endpoints **2**.

Would you like step-by-step instructions for generating an admin API key with the right scopes?

**Sources**

1. [Manage an organization with the admin APIs | Atlassian Support](https://support.atlassian.com/organization-administration/docs/manage-an-organization-with-the-admin-apis)
2. [Status of API tokens/keys when a user who generated the token/key has left the organization | Jira and Jira Service Management | Atlassian Support](https://support.atlassian.com/jira/kb/atlassian-api-token-key-status-of-api-tokens-keys-when-a-user-who-generated-the-token-key-has-left-the-organization)

And would it be more convenient to generate one with no scopes at all?

Yes, for many organization admin APIs, it is actually required to generate an API key with no scopes at all. Some admin endpoints—such as certain Organization REST APIs—do not yet support scoped API keys, and will only work with a key that has no scopes assigned **1** **2** **3**.

**Important considerations:**

* An API key without scopes grants access to all admin APIs, which can be a security risk if the key is compromised **1**.
* Atlassian is working on adding scope support to all admin APIs, but for now, using a key with no scopes is the only option for some endpoints **2** **3**.

**How to create an API key without scopes:**

1. Go to <https://admin.atlassian.com/> and select your organization.
2. Navigate to **Settings > API keys**.
3. Choose to create an API key without scopes.
4. Complete the process and securely store your new key **1**.

If you want to limit risk, monitor and rotate these keys regularly, and revoke them if they are no longer needed **4**.

Would you like a step-by-step walkthrough for creating an API key without scopes?

**Sources**

1. [Manage an organization with the admin APIs | Atlassian Support](https://support.atlassian.com/organization-administration/docs/manage-an-organization-with-the-admin-apis)
2. [Scope all Organizations APIs](https://jira.atlassian.com/browse/AX-712)
3. [Enable scoped API keys to support Organisation Rest APIs](https://jira.atlassian.com/browse/JRACLOUD-94807)
4. [Maintain your Atlassian Government organization | Atlassian Support](https://support.atlassian.com/organization-administration/docs/maintain-your-atlassian-government-organization)

Okay I have generated the API key through the [https://admin.atlassian.com/.](https://admin.atlassian.com/) How to use it? Same as token?

You can use your organization admin API key (generated from <https://admin.atlassian.com/)> as a Bearer token in the Authorization header when making API requests—this is different from the basic auth method used with user API tokens **1** **2**.

**How to use your API key:**

* Set the Authorization header in your HTTP request as follows:

Authorization: Bearer <your-api-key>

* Do not include your email address—just the API key as the Bearer token.
* Use this method for all admin API endpoints, such as [https://api.atlassian.com/admin/v1/orgs/{orgId}/users/search](https://api.atlassian.com/admin/v1/orgs/%7BorgId%7D/users/search%5B%5E01%5E%5D%5B%5E02%5E%5D.) **1****2**[.](https://api.atlassian.com/admin/v1/orgs/%7BorgId%7D/users/search%5B%5E01%5E%5D%5B%5E02%5E%5D.)

**Example with curl:**

curl -X GET "https://api.atlassian.com/admin/v1/orgs/<orgId>/users/search" \

-H "Authorization: Bearer <your-api-key>"

Let me know if you’d like a step-by-step example for a specific tool or endpoint!

**Sources**

1. [Setting up Postman for Organization User Management | Atlassian Cloud | Atlassian Documentation](https://confluence.atlassian.com/cloudkb/setting-up-postman-for-organization-user-management-1388159381.html)
2. [Manage an organization with the admin APIs | Atlassian Support](https://support.atlassian.com/organization-administration/docs/manage-an-organization-with-the-admin-apis)