

SCIM Integration Instructions

SCIM integration in Creatio: setup and administration guide

This guide explains how to configure and manage SCIM 2.0 provisioning in Creatio by using the SCIM Administration page. It covers compatibility, installation, initial setup, authentication, user provisioning, group-to-role provisioning, monitoring, and troubleshooting.

Prerequisites

Before configuring SCIM, make sure that you have:

- System administrator permissions in Creatio
- Administrator permissions in your identity provider (IdP)
- Single Sign-On (SSO) is configured for user authentication [▶ Set up Single Sign-On | Creatio Academy](#)
- A clear understanding of which IdP users and groups should be provisioned to this Creatio environment

If your Creatio environment contains custom business processes that involve users, contacts, or roles, those processes can affect SCIM provisioning in unexpected ways. If such customizations are in place, test all provisioning and deprovisioning flows carefully before rolling out SCIM in production.

Compatibility and installation

The SCIM composable app is supported starting from **Creatio 8.3.1**.

You can install the app from the **Creatio App Hub** without additional setup in the following environments:

- **Creatio .NET** version **8.3.1 and later**
- **Creatio .NET Framework** version **8.3.3 and later**

For **Creatio .NET Framework 8.3.1 and 8.3.2**, additional configuration changes are required after installation.

Update `Terrasoft.WebApp\web.config`

Add the following section to `Terrasoft.WebApp\web.config`.

It is recommended to place it after the last `<location>` section and before the `xssFilterConfig` section.

```

1 <location path="rest/scim/v2/Schemas">
2   <system.web>
3     <httpRuntime
4     requestPathInvalidCharacters="&lt;,&gt;,*,%,&amp;,\,?" />
5   </system.web>
6   <system.webServer>
7     <handlers>
8       <remove name="ExtensionlessUrlHandler-Integrated-4.0" />
9       <add name="ExtensionlessUrlHandler-Integrated-4.0"
10      type="System.Web.Handlers.TransferRequestHandler"
11      precondition="integratedMode" path="*" verb="*" />
12     </handlers>
13   </system.webServer>
14 </location>

```

Update WebAppRoot\Web.config

In `WebAppRoot\Web.config`, find this line:

```

1 <add name="PutDeleteUrlHandler" path="rest/*" verb="DELETE,PUT"
2   type="System.Web.Handlers.TransferRequestHandler"
3   precondition="integratedMode, runtimeVersionv4.0"
4   responseBufferLimit="0" />

```

Replace it with:

```

1 <add name="PutDeleteUrlHandler" path="rest/*" verb="DELETE,PUT,PATCH"
2   type="System.Web.Handlers.TransferRequestHandler"
3   precondition="integratedMode, runtimeVersionv4.0"
4   responseBufferLimit="0" />

```

If you use Creatio .NET Framework 8.3.1 or 8.3.2, complete these `web.config` updates after installing the app from App Hub. These changes are not required for Creatio .NET or for Creatio .NET Framework 8.3.3 and later.

Create a SCIM profile

A SCIM profile stores the configuration of a specific SCIM integration. Use a separate profile for each independent provisioning setup, for example for different environments, tenants, or identity providers.

Open the SCIM Administration page and create a new profile. Enter a meaningful name that helps identify the integration. The profile name is used only to identify the configuration in Creatio and does not affect provisioning behavior.

After the profile is created, Creatio opens an authorization modal window for the initial setup. In this modal, you can review and change the SCIM profile name, copy the credentials and endpoints required to configure the IdP connection, and continue to the main SCIM Administration page by clicking **Proceed to settings**.

If you change the SCIM profile name in the modal, the updated name is saved when you click **Proceed to settings**.

Initial authorization setup

Creatio uses OAuth 2.0 to authorize SCIM requests from the IdP.

When a new SCIM profile is created, the authorization modal displays the values required to configure the IdP provisioning application:

- Token endpoint
- SCIM base URL
- OAuth client credentials

Copy these values to the provisioning settings of your IdP application. After you save the IdP configuration, test the connection in the IdP if that option is available.

Once the connection is configured and tested, return to Creatio and click **Proceed to settings** to open the SCIM Administration page.

SCIM Administration page layout

The SCIM Administration page contains three tabs.

Provisioning settings

This tab contains the provisioning-related settings and the group provisioning sections, including groups awaiting provisioning, provisioned groups, and failed users.

Provisioning logs

This tab is dedicated to provisioning logs and troubleshooting information.

Authorization

This tab contains the SCIM profile name, the **Profile is active** setting, and information about the associated technical user.

Authorization

Each SCIM profile is linked to a technical user. Creatio uses the active OAuth integration associated with that technical user to authorize SCIM requests.

The **Authorization** tab contains:

- SCIM profile name

- **Profile is active** switch
- Associated technical user

The **Profile is active** switch enables or disables the SCIM profile from the SCIM Administration page.

Creatio does not display whether the associated technical user itself is active in this tab. Administrators manage SCIM processing at the profile level by using the **Profile is active** switch.

If the technical user linked to the SCIM profile is removed, select another technical user in the SCIM Administration page to continue using the integration.

If the technical user or its OAuth integration becomes inactive, SCIM requests cannot be processed until the issue is resolved.

Configure the IdP application

In your identity provider:

- Create or select the SCIM provisioning application
- Configure OAuth client credentials by using the values from the Creatio authorization modal
- Enter the Token endpoint and SCIM base URL from Creatio
- Save the configuration and run a connection test if your IdP provides that option

After the setup is complete, return to Creatio and continue with provisioning settings.

User provisioning and contact mapping

Creatio receives IdP user objects and stores them internally after they are sent by the IdP. A user is provisioned to Creatio only when that user becomes eligible for provisioning.

A user is provisioned to Creatio in either of these cases:

- The user belongs to at least one IdP group that has already been provisioned to a Creatio role
- The user has no group membership and the **Provision to default role automatically** setting is enabled
- The user has no group membership and an administrator runs the manual provisioning action for such users

If your Creatio environment contains custom business processes that involve users, contacts, or roles, those processes can affect SCIM provisioning in unexpected ways. If such

customizations are in place, test all provisioning and deprovisioning flows carefully before rolling out SCIM in production.

How Creatio matches IdP users to existing users

When provisioning a user to Creatio, the application matches the IdP user to an existing SysAdminUnit by using both of these identifiers:

- SCIM `userName` → Creatio SysAdminUnit `Name`
- SCIM work email → Creatio SysAdminUnit `Email`

The matching rules are as follows:

- If `userName` and email match the same SysAdminUnit, Creatio reuses that user
- If `userName` matches a SysAdminUnit and that SysAdminUnit has an empty email, Creatio reuses it and fills the email from the IdP
- If `userName` matches one SysAdminUnit but the email matches another, provisioning fails because of a conflict
- If no suitable match is found, Creatio creates a new SysAdminUnit

Creatio stores SCIM `externalId` on the SysAdminUnit record.

Contact linking for new users

When Creatio creates a new SysAdminUnit, it also links that user to a Contact.

The **Match new users to contacts by email** setting controls this behavior.

If the setting is enabled, Creatio tries to find an existing Contact by primary email only. If several eligible Contacts are found, Creatio links one of them. If the selected Contact is already linked to another user, Creatio creates a new Contact instead.

If the setting is disabled, Creatio always creates a new Contact for the new user.

If Creatio reuses an existing SysAdminUnit and its email differs from the primary email of the linked Contact, Creatio updates the Contact primary email to match the SysAdminUnit email.

Supported SCIM user and group attributes

Creatio supports the following SCIM attributes and maps them to Creatio objects as shown below. Only currently supported mappings are included here.

User attributes

SCIM attribute	Creatio object and field
----------------	--------------------------

<code>userName</code>	<code>SysAdminUnit.Name</code>
<code>externalId</code>	Stored as SCIM identity tracking on the SCIM projection user
<code>emails[type eq "work"].value</code>	<code>SysAdminUnit.Email</code> , <code>Contact.Email</code>
<code>displayName</code>	<code>Contact.Name</code>
<code>name.formatted</code>	<code>Contact.Name</code> when <code>displayName</code> is not provided
<code>name.givenName</code>	<code>Contact.GivenName</code>
<code>name.familyName</code>	<code>Contact.Surname</code>
<code>name.middleName</code>	<code>Contact.MiddleName</code>
<code>title</code>	<code>Contact.JobTitle</code>
<code>phoneNumbers[type eq "work"].value</code>	<code>Contact.Phone</code> , <code>SysAdminUnit.Phone</code>
<code>phoneNumbers[type eq "mobile"].value</code>	<code>Contact.MobilePhone</code>
<code>addresses[type eq "work"].formatted</code>	<code>Contact.Address</code>
<code>preferredLanguage</code>	<code>Contact.LanguageId</code> , <code>SysAdminUnit.SysCultureId</code>
<code>active</code>	<code>SysAdminUnit.Active</code>
<code>id</code>	Stored as SCIM resource identity
<code>meta.created</code>	Used in SCIM metadata and filtering
<code>meta.lastModified</code>	Used in SCIM metadata and filtering
<code>groups</code>	Used for group membership handling and role assignment

Group attributes

SCIM attribute	Creatio object and field
displayName	Stored on the SCIM projection group and used in Creatio role mapping logic
externalId	Stored as SCIM identity tracking on the SCIM projection group
members	Used for membership processing and role assignment behavior
id	Stored as SCIM group resource identity

User attribute updates

When user attributes change in the IdP, Creatio updates the corresponding Creatio user and, where applicable, the linked Contact.

The mapping is based on a predefined internal mapping and is not configured in the UI.

Users without group membership

SCIM allows users without group membership, but Creatio requires every user to belong to at least one role.

To support this, the SCIM profile includes the **Default role for users without IdP group membership** setting. This role is assigned when a group-less user is provisioned to Creatio.

The **Provision to default role automatically** setting controls whether such users are provisioned automatically.

If this setting is enabled, users without group membership are provisioned automatically and assigned to the configured default role.

If this setting is disabled, users without group membership are provisioned only when an administrator runs the manual action for them.

If the default role is **All employees** and the user later receives membership in another provisioned role, **All employees** is removed.

If a user is assigned to the default role, either automatically or manually, that membership is preserved. If the same role is later linked to an IdP group and that group is subsequently

deprovisioned, Creatio does not remove users from that default role if they were originally assigned to it as the default role.

Group-to-role provisioning

IdP groups are not applied to Creatio roles automatically. All received groups must be reviewed by an administrator and explicitly provisioned.

IdP groups are always received by Creatio as a flat structure. Even if the source identity provider organizes groups differently, Creatio processes incoming groups as independent flat group records. Administrators can still build a branched, multi-level organizational role structure in Creatio by choosing parent roles during manual provisioning.

This allows administrators to control how flat IdP group structures are translated into the Creatio role model, including multi-level role hierarchies.

Groups awaiting provisioning

The **Groups awaiting provisioning** section lists groups received from the IdP that are not yet provisioned to Creatio roles.

Each record includes:

- IdP Group Name
- Map to existing role
- New Creatio role name
- Parent of new Creatio role
- Created on
- Last updated

For each group, choose one of these options:

- Map the IdP group to an existing Creatio role
- Create a new Creatio role and define its parent role

The following rules apply:

- If exactly one Creatio role matches the IdP group name and is not already mapped to another IdP group, Creatio suggests it automatically
- If multiple roles share the same name, no automatic suggestion is shown
- One IdP group can be mapped to only one Creatio role
- One Creatio role cannot be mapped to multiple IdP groups within the same profile

The fields are mutually exclusive:

- If you select **Map to existing role**, Creatio clears the new role name and parent role fields
- If you enter a new role name or parent role, Creatio clears the existing role mapping field

If there is no matching role, the **New Creatio role name** field is prefilled with the IdP group name. You can change this value before provisioning.

Default parent role for new IdP groups

To simplify provisioning of new groups, the SCIM profile includes the **Default parent role for new IdP groups** setting.

This role is used to prefill the parent role when administrators prepare new roles for provisioning. You can override it for individual groups.

Provision groups to Creatio

After completing the required fields for one or more groups, select them and run the provisioning action.

Creatio supports bulk actions such as assigning the same parent role to multiple groups and provisioning selected groups to Creatio.

When a group is provisioned:

- If it is mapped to an existing role, Creatio saves the mapping and applies user membership
- If a new role must be created, Creatio creates the role, saves the mapping, and then applies membership

If a user from the provisioned group does not yet exist in Creatio, Creatio provisions that user if the user is eligible for provisioning.

If provisioning fails for some users, the group can still be provisioned successfully, while the failed users remain unresolved until reviewed by an administrator.

Provisioned groups

The **Provisioned groups** section lists IdP groups that are already mapped to Creatio roles.

Use this section to verify mappings, review results, and identify groups that contain users who could not be provisioned successfully.

If the mapped Creatio role is renamed, the mapping remains intact because the binding is stored by role ID.

If the mapped Creatio role is deleted while the IdP group still exists, the group returns to **Groups awaiting provisioning**.

Group rename behavior

If a group is renamed in the IdP, Creatio stores the new group name internally and returns the updated value in SCIM GET responses.

If the group is still awaiting provisioning, Creatio recalculates the role suggestion based on the new name.

If the group is already provisioned, the mapping remains linked to the same Creatio role. Creatio does not automatically rename the mapped role.

Group deprovisioning behavior

If an IdP group is deleted, Creatio removes it from the internally stored IdP data so that SCIM GET no longer returns that group.

Creatio never deletes the corresponding group or role from Creatio during SCIM deprovisioning. Instead, Creatio removes users from that group or role.

If a user loses membership in the last provisioned role because of group deprovisioning, Creatio assigns that user to the configured default role for group-less users.

Group provisioning and group deprovisioning do not change the active or inactive status of users. User status changes only through user lifecycle events.

License allocation linked to the deprovisioned group is not removed automatically. However, users who were removed from that group lose the licenses that were granted through their membership in it.

If a user was assigned to the default role manually or through the default-role logic for group-less users, that default-role membership is preserved even if the same role was later linked to an IdP group and that IdP group was deprovisioned.

Users failed to provision

The **Users failed to provision** section lists users that were received from the IdP and were eligible for provisioning to Creatio, but could not be provisioned successfully.

This section helps administrators identify and resolve provisioning issues.

Typical causes include userName and email conflicts, validation issues, or other constraints in Creatio.

After resolving the underlying problem, administrators can retry provisioning for the affected users.

Provisioning logs and troubleshooting

The **Provisioning logs** tab records key provisioning events for users and groups and helps administrators troubleshoot the integration.

The logged actions are business events rather than raw HTTP methods. Examples include:

- User received from IdP
- User attributes received from IdP
- User provisioned to Creatio
- User attributes updated
- Group received from IdP
- Group provisioned to Creatio
- Group renamed by IdP
- User deprovisioned by IdP
- User deactivated by IdP
- User deactivated in Creatio

SCIM GET requests are not logged.

Typical issues and what to check

If a user fails to provision because `userName` matches one Creatio user and email matches another, resolve the conflict in Creatio or in the IdP and then retry provisioning.

If a group cannot be provisioned, check whether:

- The parent role is missing for new role creation
- The new role name is not unique
- The selected role is already mapped to another IdP group

If some group members are not assigned, review the **Users failed to provision** section and the **Provisioning logs** tab to identify which users failed and why.

If SCIM requests are not being processed, verify that:

- The SCIM profile is enabled by using the **Profile is active** switch

- The technical user linked to the SCIM profile still exists
- The technical user has an active OAuth integration

If your environment includes custom business processes related to SysAdminUnit, Contact, or role changes, test all provisioning scenarios carefully because those processes can affect SCIM behavior.

Supported SCIM endpoints

Creatio supports these SCIM 2.0 endpoints.

Users

- GET /Users
- GET /Users/{id}
- POST /Users
- PATCH /Users/{id}

Groups

- GET /Groups
- GET /Groups/{id}
- POST /Groups
- PUT /Groups/{id}
- PATCH /Groups/{id}
- DELETE /Groups/{id}

Discovery

- GET /ServiceProviderConfig
- GET /Schemas
- GET /Schemas/{id}
- GET /ResourceTypes
- GET /ResourceTypes/{id}

Filtering

Creatio supports simplified cache-backed filtering for:

- GET /Users?filter=...
- GET /Groups?filter=...

Supported operators:

- `eq`
- `and`
- `or`
- `pr`

Supported filter attributes for users:

- `userName`
- `emails.value`
- `active`
- `externalId`
- `meta.lastModified`

Supported filter attributes for groups:

- `displayName`
- `externalId`
- `meta.lastModified`

Creatio also supports `attributes` and `excludedAttributes`.

Recommended rollout approach

For enterprise deployments, use this rollout approach:

- Configure authentication and verify IdP connectivity
- Validate user matching behavior on a small pilot group
- Review **Groups awaiting provisioning** and provision a limited set of groups first
- Confirm membership and access behavior in Creatio
- Expand the scope gradually
- If your environment includes custom business processes related to SysAdminUnit, Contact, or role changes, test all provisioning scenarios carefully because those processes can affect SCIM behavior

This reduces the risk of large-scale conflicts and makes remediation easier.

Building a multi-level Creatio role hierarchy from a flat IdP group list

Identity providers may manage groups in different ways, but Creatio always receives SCIM groups as a flat structure. Even so, Creatio supports multi-level role hierarchies, so

administrators can still build a branched role tree by provisioning groups layer by layer and assigning parent roles in the SCIM Administration page.

Start by creating and provisioning the top-level groups that should become top-level Creatio roles. After these roles exist in Creatio, create the next level of groups in the IdP.

Before provisioning each batch of child groups, set **Default parent role for new IdP groups** to the Creatio role that should become their parent. This pre-fills the parent role and makes bulk provisioning faster.

If you need to create groups under different parent branches, provision them in separate batches by switching the default parent role between batches.

This approach lets administrators translate a flat IdP group structure into a role hierarchy that matches the organization's access model in Creatio.