Chainformation Admin User Guide
(Roles Administration)

Last Updated: October 26, 2024

Welcome to the **Chainformation** user guide. In this manual, we will learn how to manage the **Roles** section on the **System setup** page.

The role-based access system on a **Chainformation** platform ensures that every individual user in your organisation has quick access to the information that is relevant to their job. **Chainformation** allows you to create roles with different access levels for each function and module of your organisation's platform. In this way, the users associated with these roles can perform only those actions that have been assigned to their roles. They cannot access and/or change the information that is beyond the access level of their role in your organisation.

Furthermore, the internal substructures within a **Chainformation** platform, defined by Areas (geo), Business areas, Units (stores) and Unit Clusters, allow the roles with the same access levels to work in their local or regional isolated online work spaces. In this way, local and regional managers can effortlessly manage staff in their respective units, areas and clusters and no irrelevant individual could breach the privacy of their work space.

On the other hand, you can also create roles with global rights to share content and manage users in all areas. In this way, the global tasks that affect your entire network could be performed effortlessly.

By default, users with sharing and editing access on different modules can share content and manage staff from their business area only. Extended rights allow users to use certain features or modules in any business areas from the organisation based on their rights (local, central, global).

Here is a list of all the features of the **Roles** module that we will discuss in this manual.
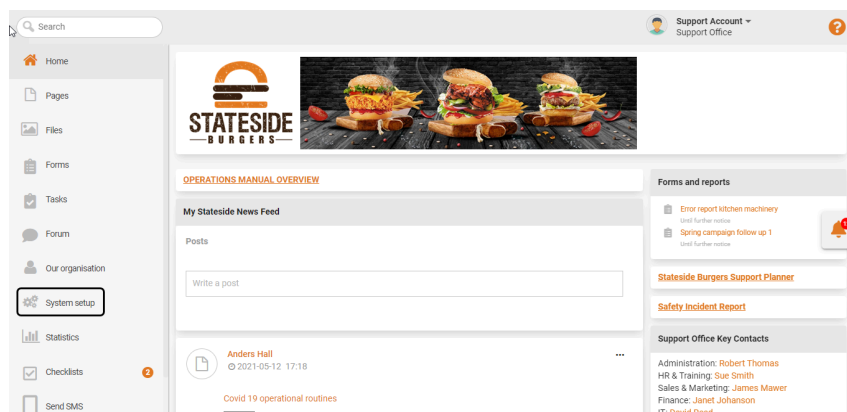
Create a New Role

Once you have logged in to the **Chainformation** platform, follow these navigation steps to **create** a **new role**.
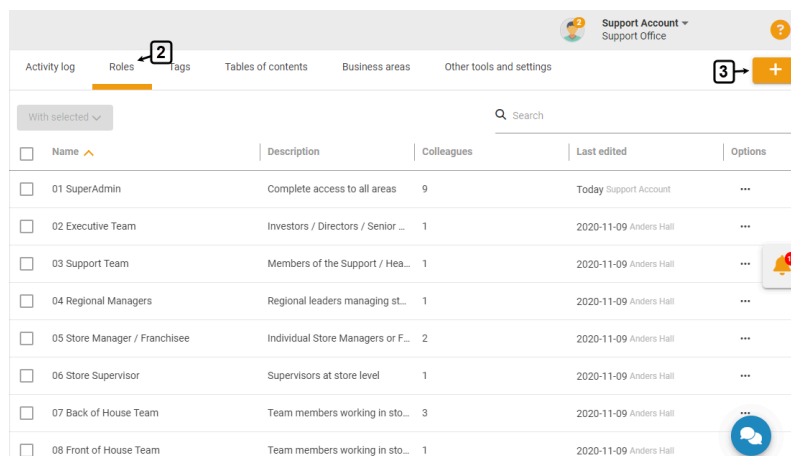
1. Click the **System setup** button in the left-side menu to open the **System setup** page.

By default, you will be redirected to the **Activity log** tab.

2. Click the **Roles** button from the header menu of the **System setup** page to open the **Roles** tab.

3. Click the **(+)** icon in the top-right corner of the **Roles** page to create a new role

https://chainformation.com/userguides

This will open the **New role** page.
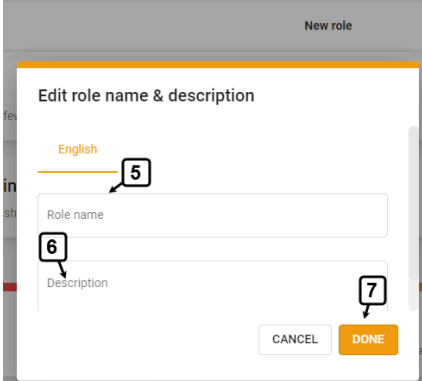

4. On the **New role** page, click the **pencil** (✎) icon next to the **Role name** heading to edit the role presentation.

This will open the **Edit role name and description** dialogue where you can enter the role name and description in different languages (if available).

5. On this pop-up tab, enter the **Name** of the new role.

The name of a role should be clear, descriptive and reflect the responsibilities and access level of the users associated with it in your organisation. E.g Franchisee, Store Manager, Chef, Runner, Area Manager etc.

Arranging names of all roles in a numeric order might be a good option for you to keep things in order. To do so, you can add numbers such as 01, 02, 03, … at the start of each name. These numbers should be assigned to the roles according to their access level in your organisation.

6. Enter a brief **Description** (if applicable) of the new role to further explain the mandate of the users who will be associated with it.

7. Click the **Done** button once you have entered the role name and description.

This will redirect you back to the **New role** page where you can proceed to define its access level for different modules of the **Chainformation** platform.

Manage Rights of the New Rule for Each Module

Note: Every **Chainformation** platform has pre-defined, restricted rights assigned to the new role for each module. These default settings will grant users read access to content shared, but no admin or edit rights.

You will find some modules disabled altogether for the new role. When a particular module is disabled for a role, the system will not show this module and its relevant tabs on the profile page of the users who are associated with the selected role.

However, you can **enable/disable** these modules and also change rights of the new role for each module manually depending on the access level you want to assign the users associated with it in your organisation.

https://chainformation.com/userguides

Remember, be very careful with the rights you are assigning to the new role because not every user in your organisation can be associated with a role that has unrestricted access to all the modules of the **Chainformation** platform.

In fact, associating a user with an inappropriate role or assigning unsuitable rights to a role may really mess up the management set up of your organisation.

Now, we will discuss all the available rights for each module of the **Chainformation** platform that you can assign to a role on the **New role** page and what could be the appropriate rights for some typical roles in an organisation.

By default, the enabled modules are shown at the top of the list and the disabled modules could be found at the bottom.

Let's discuss the options available for all of these modules one by one.

8. On the **New role page**, hover your mouse over the **module widget** you want to edit and **click** anywhere on it to **adjust rights** of the selected role for this module.

System will open a **pop-up tab** when you click a module widget where you can manage the **rights** of the **new role** for the **selected module**.
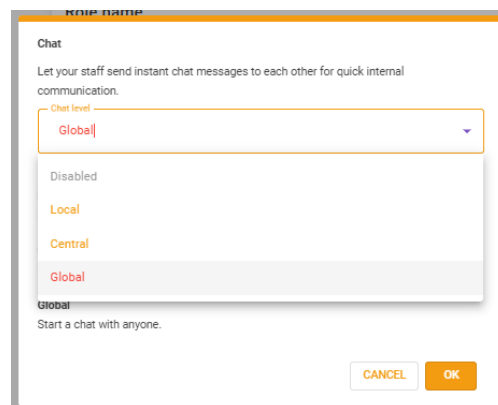
9. Select an appropriate right of the new role for the "**Chat**" module.

Note: You should keep the **Messaging** i.e. **Chat** module enabled for all the roles in your organisation as the instant messages allow the users in your organisation to remain in touch with each other.

9(a). Selecting the **Local** option will allow the users associated with the selected role to start conversation via the **Messaging** module with their colleagues from their own units and other units in their cluster (within their business area).

Important Tip: Local workers, support and marketing teams are some typical roles that could be assigned the **Local** right for the **Chat** function.

9(b). Selecting the **Central** option will allow the users associated with the selected role to start conversation via the **Messaging** module with their colleagues from all units in their area and cluster (within their business area).

Important Tip: Local unit manager or franchisee, regional or country manager, central support and marketing teams are some typical roles that could be assigned the **Central** right for the **Chat** function.

9(c). Selecting the **Global** option will allow the users associated with the selected role to start conversation via the **Messaging** module with their colleagues from all units (within their business area) of Our organisation.

Important Tip: The super admin, global support and marketing teams are some typical roles that should be assigned the **Global** right for the **Chat** function.

Remember, a user with any level of access on the "**Chat**" module can chat with colleagues from other business areas only if they have been allowed to do so in the extended rights of the selected role. See the User Guide for **Extended Rights**

Otherwise, they can send messages only to those colleagues who are associated with their business area.

10. Select appropriate rights of the new role for the "**Checklists**" module.

11(a). Selecting the **Read** option for the "**Checklists- Local**" function will allow the users associated with the new role to complete and submit checklists shared with them but they cannot make any changes to these checklists. They will not be allowed to create new checklists as well.

Important Tip: You should restrict local workers and other roles with a limited access level in your organisation to the **Read** option for "**Checklists- Local**" function.

11(b) Selecting the **Share** option will allow the users associated with the selected role to create new local checklists for their respective units and other units in their cluster (within their business area). Moreover, they can complete and submit the checklists shared with them and edit the selected local checklists as well.

Remember, users with the **Share** right for the "**Checklists- Local**" function cannot create new checklist templates or save settings of a checklist as a new template. However, they can use checklist templates shared with them by other users.

Important Tip: Local support and marketing teams are some typical roles that may be assigned the **Share** right for the "**Checklists- Local**" function.

11(c). Selecting the **Administrate** option will allow the users associated with the selected role to create new local checklists for their respective units and other units in their cluster (within

their business area). They can also create checklist templates or save settings of a checklist as a new template.

Moreover, they can complete and submit the checklists shared with them, use checklist templates shared with them by other users, edit the selected local checklists and templates as well.

Important Tip: You may assign the **Administrate** right for the "**Checklists- Local**" function to the role of local unit manager or franchisee in your organisation.

12(a). Selecting the **Read** option for the "**Checklists- Central**" function will allow the users associated with the new role to complete and submit checklists shared with them but they cannot make any changes to any central checklists. They will not be allowed to create new central checklists or templates as well.

However, they can still create new local checklists and edit the selected local checklists shared with them if you have assigned them the **Share** right for the "**Checklists- Local**" function. Likewise, they can manage local checklists templates as well if you have assigned them the **Administrate** right for the "**Checklists - Local**" function.

12(b) Selecting the **Share** option will allow the users associated with the selected role to create new central checklists for all units in their area and cluster (within their business area).

Moreover, they can complete and submit the checklists shared with them and edit the selected central checklists as well.

Remember, users with the **Share** right for the "**Checklists- Central**" function cannot create new central checklist templates. However, they can still save settings of a checklist as a new template for themselves, create new local templates and use checklist templates shared with them by other users if you have assigned them the **Administrate** right for the "**Checklists - Local**" function.

Important Tip: Central support and marketing teams are some typical roles that may be assigned the **Share** right for the "**Checklists- Central**" function.

12(c). Selecting the **Administrate** option will allow the users associated with the selected role to create central checklists for all units in their area and cluster (within their business area).

They can also create central checklist templates or save settings of a checklist as a new template.

Moreover, they can complete and submit the checklists shared with them, use checklist templates shared with them by other users, edit the selected central checklists and templates as well.

Important Tip: You may assign the **Administrate** right for the "**Checklists- Central**" function to the role of country/area manager in your organisation.

13(a). Selecting the **Read** option for the "**Checklists- Global**" function will allow the users associated with the new role to complete and submit checklists shared with them but they cannot make any changes to any global checklists. They will not be allowed to create new central checklists or templates as well.

However, they can still create new local/central checklists and edit the selected local/central checklists shared with them if you have assigned them the **Share** right for the "**Checklists- Local/Central**" function. Likewise, they can manage local/central checklists templates as well if you have assigned them the **Administrate** right for the "**Checklists - Local/Central**" function.

13(b) Selecting the **Share** option will allow the users associated with the selected role to create new global checklists for all units from any area (within their business area).

Moreover, they can complete and submit the checklists shared with them and edit the selected global checklists as well.

Remember, users with the **Share** right for the "**Checklists- Global**" function cannot create new global checklist templates. However, they can still save settings of a checklist as a new template for themselves, create new local/central templates and use checklist templates shared with them by other users if you have assigned them the **Administrate** right for the "**Checklists - Local/Central**" function.

Important Tip: Global support and marketing teams are some typical roles that may be assigned the **Share** right for the "**Checklists- Global**" function.

13(c). Selecting the **Administrate** option will allow the users associated with the selected role to create central checklists for all units from any area (within their business area).

They can also create global checklist templates or save settings of a checklist as a new template.

Moreover, they can complete and submit checklists shared with them, use checklist templates shared with them by other users, edit the selected central checklists and templates as well.

Important Tip: Only the **super admin** role should be assigned the **Administrate** right for the "**Checklists- Global**" function because not many users in an organisation could be given access to every checklist template.

14. Users associated with the selected role cannot see checklist reports for checklists created by themselves or shared with them unless you enable the "**Checklist Reports**" function for the selected role and assign an appropriate right to this role for this function.

When you enable the "**Checklist Reports**" function for the selected role, they can view reports of selected checklists on the **Reports** tab of the **Checklists** page.

14(a). You should keep the "**Checklists Reports**" function disabled for local workers and other roles with a limited access level in your organisation.

14(b). Selecting the **Local** option for the "**Checklists Reports**" function will allow the users associated with the selected role to view reports for local checklists created by themselves and other users in their respective unit/cluster (within their business area).

Important Tip: The **Local** right for the "**Checklists Reports**" function should be assigned to the role of the local unit manager or franchisee in an organisation.

14(c). Selecting the **Central** option will allow the users associated with the selected role to view reports for central checklists created by themselves and other users from their respective main area (within their business area).

Important Tip: The **Central** right for the "**Checklists Reports**" function should be assigned to the role of the regional or country manager in an organisation.

14(d). Selecting the **Global** option will allow the users associated with the selected role to view reports for global checklists created by themselves and other users from any area (within their business area).

Important Tip: Only the **super admin** role should be assigned the **Global** right for the "**Checklists Reports**" function because not many users in an organisation should be allowed to view reports of all the checklists.

Note: Users associated with the selected role can view reports for the checklists created by their colleagues only if the checklist creator has allowed the other users to see the report for these checklists.

15. Select appropriate rights of the new role for the "**Checklists 2.0**" module.

Note: Checklists 2.0 is an updated version of our existing Checklists module with various new settings and powerful advanced features. User access for Share and Administrate rights on Checklists 2.0 also work differently as compared to Checklists 1.0. So, you need to carefully understand these rights before assigning them to different roles in your organisation.

16(a). Selecting the **Read** option for the "**Checklists 2.0- Local**" function will allow users associated with the new role to complete checkpoints on available checklist schedules for their unit. They cannot make a checklist or its checkpoints "Not applicable" or "Applicable" for their unit.

Users with **Local Read** right for **Checklists 2.0** are not allowed to create new checklists and schedules. They cannot edit available checklists and their connected schedules.

Important Tip: You should restrict local workers and other roles with a limited access level in your organisation to the **Read** option for "**Checklists 2.0- Local**" function.

16(b) Selecting the **Share** option will allow the users associated with the selected role to create new recurring, one-time and on-demand schedules, connect them to available checklists and share them to their unit and other units in their cluster (within their business area). They can also edit local schedules shared only to their unit/cluster if they have sharing rights for all roles and business areas involved in sharing selection of schedule.

They can complete checkpoints on available checklist schedules, make a checklist or its checkpoints "Not applicable" or "Applicable" for their unit.

Remember, users with the **Share** right for the "**Checklists 2.0- Local**" function cannot create new checklists. They can only use checklists shared with them by other users to create new schedules.

Important Tip: Local support and marketing teams are some typical roles that may be assigned the **Share** right for the "**Checklists 2.0- Local**" function.

16(c). Selecting the **Administrate** option will allow the users associated with the selected role to create new schedules, checklists, templates and share them to their unit and other units in their cluster (within their business area). They can also edit local schedules, checklists, templates shared only to their unit/cluster if they have sharing rights for all roles and business areas involved in sharing selection of schedule/checklist/template.

They can complete checkpoints on available checklist schedules, make a checklist or its checkpoints "Not applicable" or "Applicable" for their unit.

Important Tip: You may assign the **Administrate** right for the "**Checklists 2.0- Local**" function to the role of local unit manager or franchisee in your organisation.

17(a). Selecting the **Read** option for the "**Checklists 2.0- Central**" function will allow users associated with the new role to complete checkpoints on available checklist schedules for their unit. They cannot edit any central checklists and their connected schedules. They will not be allowed to create new central schedules, checklists or templates.

Remember, users with the **Read** right for the "**Checklists 2.0- Central**" function can make a checklist or its checkpoints "Not applicable" or "Applicable" for their unit only if they are assigned at least the **Share** right on the local level of **Checklists 2.0** module. If a role is assigned **Read** right on both local and central levels of **Checklists 2.0** module, users associated with this role cannot make a checklist or its checkpoints "Not applicable" or "Applicable" for their unit.

Users with the **Read** right for the "**Checklists 2.0- Central**" function can create new local schedules and edit the selected local schedules shared with them if you have assigned them the **Share** right for the "**Checklists 2.0- Local**" function. Likewise, they can manage local

checklists and templates as well if you have assigned them the **Administrate** right for the "**Checklists 2.0- Local**" function.

17(b) Selecting the **Share** option will allow the users associated with the selected role to create new central schedules for all units in their area and cluster (within their business area). They can also edit central schedules shared only to their area if they have sharing rights for all roles and business areas involved in sharing selection of schedule.

They can complete checkpoints on available checklist schedules, make a checklist or its checkpoints "Not applicable" or "Applicable" for their unit.

Remember, users with the **Share** right for the "**Checklists 2.0- Central**" function cannot create new central checklists and templates. But, they can still create local checklists and templates if you have assigned them the **Administrate** right for the "**Checklists 2.0- Local**" function. If a role is assigned **Share** right on both local and central levels of **Checklists 2.0** module, users associated with this role can only use checklists shared with them by other users to create new schedules.

Important Tip: Central support and marketing teams are some typical roles that may be assigned the **Share** right for the "**Checklists 2.0- Central**" function.

17(c). Selecting the **Administrate** option will allow the users associated with the selected role to create new central schedules, checklists and templates for all units in their area and cluster (within their business area). They can also edit central schedules, checklists, templates shared only to their area if they have sharing rights for all roles and business areas involved in sharing selection of schedule/checklist/template.

They can complete checkpoints on available checklist schedules, make a checklist or its checkpoints "Not applicable" or "Applicable" for their unit.

Important Tip: You may assign the **Administrate** right for the "**Checklists 2.0- Central**" function to the role of country/area manager in your organisation.

18(a). Selecting the **Read** option for the "**Checklists 2.0- Global**" function will allow users associated with the new role to complete checkpoints on available checklist schedules for their unit. They cannot edit any global checklists and their connected schedules. They will not be allowed to create new global schedules, checklists or templates.

Remember, users with the **Read** right for the "**Checklists 2.0- Global**" function can make a checklist or its checkpoints "Not applicable" or "Applicable" for their unit only if they are assigned the **Share** right on at least local level of **Checklists 2.0** module. If a role is assigned **Read** right on all three levels of **Checklists 2.0** module, users associated with this role cannot make a checklist or its checkpoints "Not applicable" or "Applicable" for their unit.

Users with the **Read** right for the "**Checklists 2.0- Global**" function can create new local/central schedules and edit the selected local schedules shared with them if you have assigned them the **Share** right for the "**Checklists 2.0- Local/Central**" function. Likewise, they can manage local/central checklists and templates as well if you have assigned them the **Administrate** right for the "**Checklists 2.0- Local/Central**" function.

18(b) Selecting the **Share** option will allow the users associated with the selected role to create new global schedules for all areas and their business area. They can also edit available schedules if they have sharing rights for all roles and business areas involved in sharing selection of a schedule.

They can complete checkpoints on available checklist schedules, make a checklist or its checkpoints "Not applicable" or "Applicable" for their unit.

Remember, users with the **Share** right for the "**Checklists 2.0- Global**" function cannot create new global checklists and templates. But, they can still create local/central checklists and templates if you have assigned them the **Administrate** right for the "**Checklists 2.0- Local/Central**" function. If a role is assigned **Share** right on all three levels of **Checklists 2.0** module, users associated with this role can only use checklists shared with them by other users to create new schedules.

Important Tip: Global support and marketing teams are some typical roles that may be assigned the **Share** right for the "**Checklists 2.0- Global**" function.

18(c). Selecting the **Administrate** option will allow the users associated with the selected role to create new global schedules, checklists and templates for all areas and their business area. They can also edit available schedules, checklists, templates if they have sharing rights for all roles and business areas involved in sharing selection of schedule/checklist/template.

They can complete checkpoints on available checklist schedules, make a checklist or its checkpoints "Not applicable" or "Applicable" for their unit.

Important Tip: Only the **super admin** role should be assigned the **Administrate** right for the "**Checklists 2.0- Global**" function because not many users in an organisation could be allowed to manage all checklists and templates.

19. Users associated with the selected role cannot see checklist reports for schedules created by themselves or shared with them unless you enable the "**Checklists 2.0 Reports**" function for the selected role and assign an appropriate right to this role for this function.

When you enable the "**Checklists 2.0 Reports**" function for the selected role, they can view reports of selected checklist schedules on the **Reports** dashboard of the **Checklists 2.0** module.

19(a). You should keep the "**Checklists 2.0 Reports**" function disabled for local workers and other roles with a limited access level in your organisation.

19(b). Selecting the **Local** option for the "**Checklists 2.0 Reports**" function will allow the users associated with the selected role to view reports for local checklist schedules created by themselves and other users in their respective unit/cluster (within their business area).

Important Tip: The **Local** right for the "**Checklists 2.0 Reports**" function should be assigned to the role of the local unit manager or franchisee in an organisation.

19(c). Selecting the **Central** option will allow the users associated with the selected role to view reports for central checklist schedules created by themselves and other users from their respective main area (within their business area).

Important Tip: The **Central** right for the "**Checklists 2.0 Reports**" function should be assigned to the role of the regional or country manager in an organisation.

19(d). Selecting the **Global** option will allow the users associated with the selected role to view reports for global checklist schedules created by themselves and other users from any area (within their business area).

Important Tip: Only the **super admin** role should be assigned the **Global** right for the "**Checklists Reports**" function because not many users in an organisation should be allowed to view reports of all checklist schedules.

Note: Users associated with the selected role can view reports for the checklist schedules created by their colleagues only if the schedule creator has allowed the other users to see the report for these schedules.

20. Select appropriate rights of the new role for the "**Files**" module.

21(a). Selecting the **Read** option for the "**Files- Local**" function will allow the users associated with the new role to view, and download files shared with them but they cannot make any changes to these files. They will not be allowed to upload new files as well.

21(b) Selecting the **Share** option will allow the users associated with the selected role to upload files and share them with their selected colleagues in their respective units and other units in their cluster (within their business area).

Moreover, they can view and download the files shared with them and edit the selected local files as well.

Important Tip: Local unit manager or franchisee, local support and marketing teams are some typical roles that should be assigned the **Share** right for the "**Files- Local**" function.

22(a). Selecting the **Read** option for the "**Files- Central**" function will allow the users associated with the new role to view and download files shared with them but they cannot make any changes to any central files. They will not be allowed to upload new central files as well.

However, they can still add new local files and edit the selected local files shared with them if you have assigned them the **Share** right for the "**Files- Local**" function.

22(b). Selecting the **Share** option will allow the users associated with the selected role to upload files and share them to all units in their area and cluster (within their business area).

Moreover, they can read, download the files shared with them and edit the selected central files as well.

Important Tip: Country/area manager, central support and marketing teams are some typical roles that should be assigned the **Share** right for the "**Files- Central**" function.

23(a). Selecting the **Read** option for the "**Files- Global**" function will allow the users associated with the new role to view and download files shared with them but they cannot make any changes to any global files. They will not be allowed to upload new global files as well.

However, they can still add new local/central files and edit the selected local/central files shared with them if you have assigned them the **Share** right for the "**Files- Local/Central**" function.

23(b). Selecting the **Share** option will allow the users associated with the selected role to upload files and share them to all units from any area (within their business area).

Moreover, they can read, download the files shared with them and edit the selected global files as well.

Important Tip: Global support and marketing teams are some typical roles that should be assigned the **Share** right for the "**Files- Global**" function.

23(c). Selecting the **Super Admin** option will allow the users associated with the new role to view and manage all the files uploaded by their colleagues. They can access even those files which have not been shared with them.

Important Tip: The **Super Admin** right for the "**Files- Global**" function should be assigned to the super admin role only because not many users in an organisation should be allowed to manage all the files shared across the organisation.

24. Select appropriate rights of the new role for the "**Forms- Local**" module.

25(a). Selecting the **Read** option for the "**Forms- Local**" function will allow the users associated with the new role to view, answer, download and print forms shared with them but they cannot make any changes to these forms. They will not be allowed to create new forms as well.

Important Tip: You should restrict local workers and other roles with a limited access level in your organisation to the **Read** right for "**Forms- Local**" function.

25(b) Selecting the **Share** option will allow the users associated with the selected role to create new local forms and share them with their selected colleagues in their respective units and other units from their cluster (within their business area).

Moreover, they can answer, download, print the forms shared with them, make new copies and edit the selected local forms as well.

Important Tip: Local unit manager or franchisee, local support and marketing teams are some typical roles that may be assigned the **Share** right for the "**Forms- Local**" function.

26(a). Selecting the **Read** option for the "**Forms- Central**" function will allow the users associated with the new role to view, answer, download and print forms shared with them but they cannot make any changes to any central forms. They will not be allowed to create new central forms as well.

However, they can still create new local forms, make local copies of the forms shared with them and edit the selected local forms if you have assigned them the **Share** right for the "**Forms- Local**" function.

26(b) Selecting the **Share** option will allow the users associated with the selected role to create new central forms and share them to all units from their area and cluster (within their business area).

Moreover, they can answer, download, print the forms shared with them, make copies of these forms and edit the selected central forms as well.

Important Tip: Country/area manager, central support and marketing teams are some typical roles that could be assigned the **Share** right for the "**Forms- Central**" function.

27(a). Selecting the **Read** option for the "**Forms- Global**" function will allow the users associated with the new role to view, answer, download and print forms shared with them but they cannot make any changes to any global forms. They will not be allowed to create new global forms as well.

However, they can still create new local/central forms, make local/central copies of the forms shared with them and edit the selected local/central forms if you have assigned them the **Share** right for the "**Forms- Local/Central**" function.

27(b) Selecting the **Share** option will allow the users associated with the selected role to create new global forms and share them to all units from any area (within their business area).

Moreover, they can answer, download, print the forms shared with them, make copies of these forms and edit the selected global forms as well.

Important Tip: Other than the super admin, global support and marketing teams are some typical roles that could be assigned the **Share** right for the "**Forms- Global**" function.

28. When you enable the "**Forms- Reports**" function for the selected role, they can view reports and answers submitted by other users to the selected forms on the **Reports** tab of the **Forms** page.

28(a). You should keep the "**Forms- Reports**" function disabled for local workers and other roles with a limited access level in your organisation.

28(b). Selecting the **Local** option for the "**Forms- Reports**" function will allow the users associated with the selected role to view and download the reports and answers submitted by their local colleagues to available forms.

When you assign the **Share** right for the "**Forms- Reports**" function to a particular role, the system automatically assigns the **Local** right for the "**Forms- Reports**" function to that role so that the users associated with it can keep track of the forms created by them.

Important Tip: You should keep this selection as it is for the roles of local unit manager or franchisee, local support and marketing teams in your organisation.

28(c). Selecting the **Central** option will allow the users associated with the selected role to view and download the reports and answers submitted to available forms by their central colleagues.

Important Tip: Country/area manager, central support and marketing teams are some typical roles that could be assigned the **Central** right for the "**Checklists Reports**" function.

28(d). Selecting the **Global** option will allow the users associated with the selected role to view and download the reports and answers submitted to available forms by their colleagues from all areas (within their business area).

Important Tip: Only the **super admin** role should be assigned the **Global** right for the "**Checklists Reports**" function because not many users in an organisation should be allowed to view reports of all the forms.

Note: Users associated with the selected role can view reports of the forms created by their colleagues only if the form creator has allowed the other users to see the report of this form.

29. Select appropriate rights of the new role for the "**Our organisation**" module.

30(a). Selecting the **Read** option for the "**Our organisation- Local**" function will allow the users associated with the selected role to access the **Colleagues** and **Units** tabs on the **Our organisation** page.

On the **Colleagues** page, they can see all the users who belong to their local unit and other units in their cluster (within their business area).

On the **Units** page, they can see details of their local unit and other units in their cluster (within their business area). Moreover, they can also see names and other corresponding details of their colleagues associated with a specific unit.

Remember, a user with the **Read** right for the "**Our organisation- Local**" function cannot edit any user or unit on the **Our organisation** page.

30(b). Selecting the **Write** option will allow the users associated with the selected role to edit their respective local units, other available units in their clusters and selected colleagues associated with these units. They can also add new local users to their organisation i.e. the users associated with their respective local units and other available units in their cluster.

Important Tip: The **Write** option for the "**Our organisation- Local**" function should be assigned to the role of the local unit manager or franchisee in an organisation.

31(a). Selecting the **Read** option for the "**Our organisation- Central**" function will allow the users associated with the selected role to see all users and units in their cluster and all the sub areas in their main geographic area (within their business area).

Moreover, they can edit their respective local units, other available units in their cluster and their selected colleagues in those units as well if you have selected the **Write** option for the "**Organisation manager- Local**" function.

31(b). Selecting the **Write** option for the "**Our organisation- Central**" function will allow the users associated with the new role to edit all available units in their cluster and area. They can also edit their selected colleagues associated with these units.

Moreover, they can add new users and create new units within their geographical area and business area.

Important Tip: The **Write** option for the "**Organisation manager- Central**" function should be assigned to the role of the regional or country manager in an organisation.

32(a). Selecting the **Read** option for the "**Our organisation- Global**" function will allow the users associated with the selected role to see all users and units from all areas (within their business area).

Moreover, they can edit their respective local units, other available units in their clusters/areas and their selected colleagues in those units as well if you have selected the **Write** option for the "**Organisation manager- Local/Central**" function.

32(b). Selecting the **Write** option for the "**Organisation manager- Global**" function will allow the users associated with the new role to edit all available units within their business area and any geographical area of your organisation. They can also edit their selected colleagues associated with these units.

Moreover, they can add new users and create new units in all geographical areas and their business area.

32(c). Selecting the **Administrate** option for the "**Organisation manager- Global**" function will give the users associated with the new role full access to the **Our organisation** module.

They can view and manage all the relevant information on the **Colleagues**, **Areas**, **Units, Clusters, User Requests** pages of the **Our organisation** module and **Roles, Extended Rights, Business areas** pages of the **System Setup** module.

They can also manage request access, support contact, data fields and other system setup settings on the **Other settings** page of the **System setup** module. Moreover, they can see all the user activity on their organisation's internet in the **Activity log** on the **System setup** page.

Important Tip: The **Administrate** right for the "**Our organisation- Global**" function should be assigned only to the highest role in the hierarchy of an organisation.

You may name this role the super admin and only a limited number of users of your organisation should be assigned this role.

Remember, a user with **Read/Write** access on any level of "**Our organisation**" module can view and manage colleagues and units from other business areas only if they have been allowed to do so in the extended rights of the selected role. See the User Guide for **Extended Rights**

Otherwise, they can view and manage colleagues and units from their business area only.

Similarly, users with the **Write** access on "**Our organisation**" module can manage only those colleagues who are associated with the roles that the selected role is allowed to manage. See the User Guide for **Role Relation Settings**

33. Select an appropriate right of the new role for the "**Pages**" module.

34(a). Selecting the **Read** option for the "**Pages- Local**" function will allow the users associated with the new role to read, download, and print pages shared with them but they cannot make any changes to these pages. They will not be allowed to create new pages as well.

34(b) Selecting the **Share** option will allow the users associated with the selected role to create local pages and share them to their respective units and other units in their cluster (within their business area).

However, they cannot create page templates on their own. Therefore, they must have access to at least one template to create a new page. If they do not have access to any page template, then they can ask one of their superior colleagues to provide them with a template before they can create a page.

Moreover, they can read, download, print the pages shared with them, make local copies of these pages and edit the selected local pages as well.

Important Tip: Local support and marketing teams are some typical roles that should be assigned the **Share** right for the "**Pages- Local**" function.

34(c). Selecting the **Administrate** option will allow the users associated with the new role to create local pages, page templates and share them to their respective units and other units in their cluster (within their business area).

They can also use templates shared with them by other users, read and manage pages shared with them. Moreover, they can edit the selected local pages and templates as well.

Important Tip: The **Administrate** right for the "**Pages- Local**" function should be assigned to the role of the local unit manager or franchisee in an organisation.

35(a). Selecting the **Read** option for the "**Pages- Central**" function will allow the users associated with the new role to read, download and print pages shared with them but they cannot make any changes to any central pages. They will not be allowed to create new central pages as well.

However, they can still create new local pages, edit the selected local pages shared with them and make local copies of those pages if you have assigned them the **Share** right for the "**Page manager- Local**" function.

Likewise, they can manage the local page templates as well if you have assigned them the **Administrate** right for the "**Pages- Local**" function.

35(b). Selecting the **Share** option will allow the users associated with the selected role to create central pages and share them to all units in their area and cluster (within their business area).

Remember, assigning the **Share** right for the "**Pages- Central**" function automatically assigns them the same right for the "**Pages- Local**" function.

However, they can create templates for their pages only if you have assigned them the **Administrate** right for the "**Pages- Local**" function. Otherwise, they can use the page templates shared with them by other users in the organisation.

Moreover, they can read, download, print the pages shared with them, make copies of these pages and edit the selected central pages as well.

Important Tip: Central support and marketing teams are some typical roles that should be assigned the **Share** right for the "**Page manager- Central**" function.

35(c). Selecting the **Administrate** option will allow the users associated with the new role to create central pages, page templates and share them to all units in their area and cluster (within their business area).

They can also use templates shared with them by other users, read and manage pages shared with them. Moreover, they can edit the selected central pages and templates as well.

Important Tip: The **Administrate** right for the "**Pages- Central**" function should be assigned to the role of the country/area manager in an organisation.

36(a). Selecting the **Read** option for the "**Pages- Global**" function will allow the users associated with the new role to read, download and print pages shared with them but they cannot make any changes to any global pages. They will not be allowed to create new global pages as well.

However, they can still create new local/central pages, edit the selected local/central pages shared with them and make local/central copies of those pages if you have assigned them the **Share** right for the "**Page manager- Local/Central**" function.

Likewise, they can manage the local/central page templates as well if you have assigned them the **Administrate** right for the "**Pages- Local/Central**" function.

36(b). Selecting the **Share** option will allow the users associated with the selected role to create central pages and share them to all units from any area (within their business area).

Remember, assigning the **Share** right for the "**Pages- Global**" function automatically assigns them the same right for the "**Pages- Local/Central**" function.

However, they can create templates for their pages only if you have assigned them the **Administrate** right for at least the "**Pages- Local**" function. Otherwise, they can use the page templates shared with them by other users in the organisation.

Moreover, they can read, download, print the pages shared with them, make copies of these pages and edit the selected global pages as well.

Important Tip: Global support and marketing teams are some typical roles that should be assigned the **Share** right for the "**Page manager- Global**" function.

36(c). Selecting the **Administrate** option will allow the users associated with the new role to create global pages, page templates and share them to all units from any area (within their business area).

They can also use templates shared with them by other users, read and manage pages shared with them. Moreover, they can edit the selected central pages and templates as well.

36(d). Selecting the **Super Admin** option for the "**Pages- Global**" function will allow the users associated with the new role to read and manage all the pages and templates created by their colleagues.

They can access even those pages and templates which have not been shared with them.

Important Tip: The **Super Admin** right for the "**Pages- Global**" function should be assigned to the super admin role only because not many users in an organisation should be allowed to manage all the pages and templates shared across the organisation.

37. Select appropriate rights of the new role for the "**Posts**" module.

38(a). Selecting the **Read** option for the "**Posts- Local**" function will allow the users associated with the new role to read the posts shared with them and comment on these posts.

However, they will not be allowed to create new posts and manage posts shared with them.

38(b) Selecting the **Share** option will allow the users associated with the selected role to share new posts to their respective units and other units in their cluster (within their business area).

Moreover, they can read the posts shared with them and comment on these posts. However, they will not be allowed to manage the posts shared by other users.

Important Tip: Local support, marketing teams and other staff are some typical roles that should be assigned the **Share** right for the "**Posts- Local**" function.

38(c) Selecting the **Administrate** option will allow the users associated with the selected role to share new local posts to their respective units and other units in their cluster (within their business area). They can read the posts shared with them and comment on these posts as well.

Moreover, they can remove selected local posts and other news items e.g. pages, files shared by their colleagues on the News feed.

Important Tip: The **Administrate** right for the "**Posts- Local**" function could be assigned to the role of the local unit manager or franchisee in an organisation.

39(a). Selecting the **Read** option for the "**Posts- Central**" function will allow the users associated with the new role to read the posts shared with them and comment on these posts. However, they will not be allowed to create new central posts and manage any central posts shared with them.

They can still share new local posts if you have assigned them the **Share** right for the **Posts- Local** function. Moreover, they can manage the selected local posts and other news items shared by their colleagues as well if you have assigned them the **Administrate** right for the **Posts- Local** function.

39(b) Selecting the **Share** option will allow the users associated with the selected role to share new posts to all units in their area and cluster (within their business area).

Moreover, they can read the posts shared with them and comment on these posts. They will not be allowed to manage any central posts shared by other users. However, they can still manage the selected local posts and other news items shared by their colleagues if you have assigned them the **Administrate** right for the **Posts- Local** function.

Important Tip: Central support, marketing and executive teams are some typical roles that should be assigned the **Share** right for the "**Posts- Central**" function.

39(c) Selecting the **Administrate** option will allow the users associated with the selected role to share new posts to all units in their area and cluster (within their business area). They can read the posts shared with them and comment on these posts as well.

Moreover, they can pin a post or any other available item on top of the news feed. They can also remove selected central posts and other news items e.g. pages, files shared by their colleagues on the News feed.

Important Tip: The **Administrate** right for the "**Posts- Central**" function should be assigned to the role of the country/area manager.

40(a). Selecting the **Read** option for the "**Posts- Global**" function will allow the users associated with the new role to read the posts shared with them and comment on these posts. However, they will not be allowed to create new global posts and manage global posts shared with them.

They can still share new local/central posts if you have assigned them the **Share** right for the **Posts- Local/Central** function. Moreover, they can manage the selected local/central posts and other news items shared by their colleagues as well if you have assigned them the **Administrate** right for the **Posts- Local/Central** function.

40(b) Selecting the **Share** option will allow the users associated with the selected role to share new posts to all units from any area (within their business area).

Moreover, they can read the posts shared with them and comment on these posts. They will not be allowed to manage any global posts shared by other users. However, they can still manage the selected local/central posts and other news items shared by their colleagues if you have assigned them the **Administrate** right for the **Posts- Local/Central** function.

Important Tip: Global support, marketing and executive teams are some typical roles that should be assigned the **Share** right for the "**Posts- Central**" function.

40(c) Selecting the **Administrate** option will allow the users associated with the selected role to share new posts to all units from any (within their business area). They can read the posts shared with them and comment on these posts as well.

Moreover, they can pin a post or any other available item on top of the news feed. They can also remove selected global posts and other news items e.g. pages, files shared by their colleagues on the News feed.

Important Tip: The **Administrate** right for the "**Posts- Global**" function should be assigned only to the super admin.

41. Select an appropriate right of the new role for the "**Tasks**" module.

Note: You should keep the **Tasks** module enabled for all the roles in your organisation as the **Tasks** module helps users to keep track of all the important to-do things for themselves and their colleagues.

41(a). Selecting the **Local** option will allow the users associated with the selected role to create tasks for themselves, assign tasks to colleagues from their respective local units and other units in their cluster (within their business area).

Important Tip: Local unit manager or franchisee and other roles related to local staff should be assigned the **Local** right for the **Tasks** function.

41(b). Selecting the **Central** option will allow the users associated with the selected role to create tasks for themselves, assign tasks to their colleagues from all units in their area and cluster (within their business area).

Important Tip: Regional or country manager, central support and marketing teams are some typical roles that should be assigned the **Central** right for the **Tasks** function.

41(c). Selecting the **Global** option will allow the users associated with the selected role to create tasks for themselves, assign tasks to their colleagues from all units in any area (within their business area).

Important Tip: The super admin, global support and marketing teams are some typical roles that should be assigned the **Global** right for the **Tasks** function.

42. Select appropriate rights of the new role for the "**Forums**" module.

43. Selecting the **Share** option will allow the users associated with the new role to read and share posts in the forums shared with them. However, they cannot create a new forum.

Note: It's better to **enable** the **Forum** module for all roles of an organisation as a forum can be used to share information and start a discussion with almost every type of users from global marketing team to local unit staff.

44(a). You should keep the "**Forum admin**" function disabled for local workers and other roles with a limited access level in your organisation.

44(b). Selecting the **Local** option for the "**Forum admin**" function will allow the users associated with the selected role to create new forums and share them to their respective units and other units in their cluster (within their business area). They can also manage selected local forums shared by their colleagues.

Important Tip: The **Local** right for the "**Forum admin**" function should be assigned to the role of the local unit manager or franchisee in an organisation.

44(c). Selecting the **Central** option will allow the users associated with the selected role to create new forums and share them to all units in their area and cluster (within their business area). They can also manage selected central forums shared by their colleagues.

Important Tip: The **Central** right for the "**Forum admin**" function should be assigned to the role of the regional or country manager in an organisation.

44(d). Selecting the **Global** option will allow the users associated with the selected role to create new forums and share them to all units from any area (within their business area). They can also manage selected global forums shared by their colleagues.

Global forum admins can view and participate in all forums shared to their business area even if a forum is not shared with their role and/or area. If they are allowed to share content to all business areas, they can access all forums shared to any area and business area.

Important Tip: Other than the super admin, global support, marketing and executive teams are some typical roles that should be assigned the **Global** right for the "**Forum admin**" function.

Note: Whatever right you choose for the "**Forum admin**" function, users with the selected role can always add new posts in the forums shared with them, read posts in these forums, manage these posts and comment on them.

Remember, users with any level of access on the "**Forum admin**" function can share forums to other business areas only if they have been allowed to do so in the extended sharing rights of the selected role. Otherwise, they can share forums to only those units and colleagues who are associated with their business area.

Forum admins can share forums with only those colleagues who are associated with the roles that have been listed in the sharing rights of the selected role. <u>See the User Guide for</u> **<u>Role Relation Settings and Extended Rights</u>**

Now, we will discuss modules that are disabled by default.

45. Select appropriate rights of the new role for the "**Audit checklists**" module.

Note: Audits are distinct from standard checklists, which is why we added them as a separate "module." Access rights of a role for the **Audit checklists** module are completely independent of this role's rights for the **Checklists 2.0** module. A user's access on different levels of the Audit checklists module is not affected by their access level on Checklists 2.0 module.

Audit checklist creation and scheduling is similar to Checklists 2.0. So, Share, Administrate rights on local, central and global levels of Audit checklists work on the logic identical to Checklists 2.0. But, audit checklist submission is different from regular checklist completion. So, Read right on Audit checklists module works on a completely different logic as compared to Read right on Checklists 2.0 module. Read access on the two modules work as follows:

Regular checklists completion: User can submit a regular checklist for their current unit only. They can submit a regular checklist for multiple units only if they have access to two or more units from their profile. Also, they need to change their current unit before they can complete a checklist for a different unit (if available).

Audit checklist submission: User can submit an audit checklist for multiple units (depending on their role right for Audit checklists module) even if they have access to only one unit from their profile. So, users don't need to switch their current unit before submitting an audit for a specific unit. Also, they may not belong to a unit but can still conduct an audit for this unit.

46(a). Selecting the **Read** option for the "**Audit checklists- Local**" function will allow users associated with the new role to conduct audits for their unit and other units in their cluster (within their business area) using available audit schedules.

Users with **Local Read** right for **Audit checklists** are not allowed to create new audit checklists and schedules. They cannot edit available audit checklists and their connected schedules.

46(b) Selecting the **Share** option will allow the users associated with the selected role to create new audit schedules, connect them to available audit checklists and share them to their unit and other units in their cluster (within their business area). They can also edit local audit schedules shared only to their unit/cluster if they have sharing rights for all roles and business areas involved in sharing selection of schedule.

They can conduct audits for their unit and other units in their cluster (within their business area) using available audit schedules.

Remember, users with the **Share** right for the "**Audit checklists**" function cannot create new audit checklists. They can only use audit checklists shared with them by other users to create new audit schedules.

46(c). Selecting the **Administrate** option will allow the users associated with the selected role to create new audit schedules, checklists, templates and share them to their unit and other units in their cluster (within their business area). They can also edit local audit schedules, checklists, templates shared only to their unit/cluster if they have sharing rights for all roles and business areas involved in sharing selection of schedule/checklist/template.

They can conduct audits for their unit and other units in their cluster (within their business area) using available audit schedules.

Important Tip: Country/area managers in an organisation could be assigned local level of rights to conduct audits in different units from their area and manage local audit schedules, checklists, templates.

47(a). Selecting the **Read** option for the "**Audit checklists- Central**" function will allow users associated with the new role to conduct audits for their unit and other units in their area, cluster (within their business area) using available audit schedules.

They cannot edit any central audit checklists and their connected schedules. They will not be allowed to create new central audit schedules, checklists or templates.

Users with the **Read** right for the "**Audit checklists- Central**" function can create new local audit schedules and edit the selected local audit schedules shared with them if you have assigned them the **Share** right for the "**Audit checklists- Local**" function. Likewise, they can manage local audit checklists and templates as well if you have assigned them the **Administrate** right for the "**Audit checklists- Local**" function.

47(b) Selecting the **Share** option will allow the users associated with the selected role to create new central audit schedules for all units in their area and cluster (within their business area). They can also edit central audit schedules shared only to their area if they have sharing rights for all roles and business areas involved in sharing selection of schedule.

They can conduct audits for their unit and other units in their area, cluster (within their business area) using available audit schedules.

Remember, users with the **Share** right for the "**Audit checklists- Central**" function cannot create new central audit checklists and templates. But, they can still create local audit checklists and templates if you have assigned them the **Administrate** right for the "**Audit checklists- Local**" function. If a role is assigned **Share** right on both local and central levels of **Audit checklists** module, users associated with this role can only use audit checklists shared with them by other users to create new audit schedules.

47(c). Selecting the **Administrate** option will allow the users associated with the selected role to create new central audit schedules, checklists and templates for all units in their area and cluster (within their business area). They can also edit central audit schedules, checklists, templates shared only to their area if they have sharing rights for all roles and business areas involved in sharing selection of schedule/checklist/template.

They can conduct audits for their unit and other units in their area, cluster (within their business area) using available audit schedules.

48(a). Selecting the **Read** option for the "**Audit checklists- Global**" function will allow users associated with the new role to conduct audits for any unit in any area (within their business area). They cannot edit any global audit checklists and their connected schedules. They will not be allowed to create new global audit schedules, checklists or templates.

Users with the **Read** right for the "**Audit checklists- Global**" function can create new local/central audit schedules and edit the selected local schedules shared with them if you have assigned them the **Share** right for the "**Checklists 2.0- Local/Central**" function. Likewise, they can manage local/central audit checklists and templates as well if you have assigned them the **Administrate** right for the "**Audit checklists- Local/Central**" function.

48(b) Selecting the **Share** option will allow the users associated with the selected role to create new global audit schedules for all areas and their business area. They can also edit available audit schedules if they have sharing rights for all roles and business areas involved in sharing selection of a schedule.

They can conduct audits for any unit in any area (within their business area).

Remember, users with the **Share** right for the "**Audit checklists- Global**" function cannot create new global checklists and templates. But, they can still create local/central audit checklists and templates if you have assigned them the **Administrate** right for the "**Audit checklists- Local/Central**" function. If a role is assigned **Share** right on all three levels of **Audit checklists** module, users associated with this role can only use audit checklists shared with them by other users to create new audit schedules.

48(c). Selecting the **Administrate** option will allow the users associated with the selected role to create new global audit schedules, checklists and templates for all areas and their business area. They can also edit available audit schedules, checklists, templates if they have sharing rights for all roles and business areas involved in sharing selection of schedule, checklist, template.

They can conduct audits for any unit in any area (within their business area).

Important Tip: Mostly, super admins are responsible for conducting audits on all units from all areas in an organisation. So, you should keep central, global levels of the Audit checklists module disabled for all other roles.

If you have dedicated teams to conduct audits on central or global level, you can assign appropriate rights to their role on local and central levels of the Audit checklists module.

Remember, only the **super admin** role should be assigned the **Administrate** right for the "**Audit checklists- Global**" function because not many users in an organisation could be allowed to manage all audit checklists and templates.

49. Users associated with the selected role cannot see reports for audit schedules created by themselves or shared with them unless you enable the "**Audit checklist Reports**" function for the selected role and assign an appropriate right to this role for this function.

When you enable the "**Audit checklists Reports**" function for the selected role, they can view reports of selected audit schedules on the **Audit reports** dashboard of the **Audit Checklists** module.

49(a). Selecting the **Local** option for the "**Audit checklists Reports**" function will allow the users associated with the selected role to view reports for local audit schedules created by themselves and other users in their respective unit/cluster (within their business area).

49(b). Selecting the **Central** option will allow the users associated with the selected role to view reports for central audit schedules created by themselves and other users from their respective main area (within their business area).

49(c). Selecting the **Global** option will allow the users associated with the selected role to view reports for global audit schedules created by themselves and other users from any area (within their business area).

Note: Users associated with the selected role can view reports for the audit schedules created by their colleagues only if the schedule creator has allowed the other users to see the report for these schedules.

Important Tip: Audit Reports function could be enabled for a role even if the **Audit checklists** module itself is disabled for this role on all three levels.

For example, you might enable **Audit Checklists Reports- Local** function for local manager/franchisee to share reports of audits conducted on their unit by higher management.

50. Select whether the new role will be allowed to **Administrate** the **Appearance** of your organisation intranet or not.

When you enable the **Appearance** function for the selected role, then the users associated with it can **manage** the layout and graphical appearance of different pages of your organisation's internet.

As these are usually one-time settings and not many people should be allowed to manage them, therefore, you should keep the **Appearance** function **disabled** for all other roles except the **Super Admin**.

51. Select an appropriate right of the new role for the "**SMS**" module.

51(a). You should keep the "**SMS**" module disabled for local workers and other roles with a limited access level in your organisation.

51(b). Selecting the **Share** option will allow the users associated with the selected role to **send SMS** to their selected colleagues or other people from their respective local unit using your brand name.

Important Tip: The country or regional manager, local unit manager or franchisee, support and marketing teams are some typical roles that should be assigned the **Share** right for the "**SMS manager**" function.

51(c). Selecting the **Administrate** option will allow the users associated with the selected role to send SMS as well as see the cost of SMS sent by other users from all the units and areas in the past 12 months.

Important Tip: Only the **super admin** should be assigned the **Administrate** right for the **SMS manager** function.

Remember, users with the **Share** access on the **SMS** module can send SMS to only those colleagues whose phone numbers are listed in their contact information on the **Our organisation** page. See the User Guide for **Colleagues**

52. Select an appropriate right of the new role for the "**Statistics**" module.

52(a). You should keep the "**Statistics**" module disabled for local staff of a unit, support, marketing teams and other roles with a limited access level in your organisation.

52(b). Selecting the **Local** option will allow the users associated with the selected role to see statistics for their own unit and other units in their cluster (within their business area).

Important Tip: The **Local** right for the "**Statistics**" function should be assigned to the role of the local unit manager or franchisee in an organisation.

52(c). Selecting the **Central** option will allow the users associated with the selected role to see statistics for all units in their area and cluster (within their business area).

Important Tip: The **Central** right for the "**Statistics**" function should be assigned to the role of the regional or country manager in an organisation.

52(d). Selecting the **Global** option will allow the users associated with the selected role to see statistics for all units from any area (within their business area).

Important Tip: Only the **super admin** role should be assigned the **Global** right for the "**Statistics**" function because not many users in an organisation should be allowed to see statistics for all the users and areas.

Remember, a user with any level of access to the "**Statistics**" module can see data of units and colleagues from other business areas only if they have been allowed to do so in the extended rights of the selected role. See the User Guide for **Extended Rights**

Otherwise, they can see data of only those units and colleagues who are associated with their business area.

53. Select Appropriate right of the new role for the "**Tag**" module.

Selecting the **Administrate** option for the **"Tag administration"** function will allow the users associated with the selected role to access the **Tags** and **Table of contents** tabs on the **System setup** page.

They can view and manage all the tags and tables available on the **Tags** and **Table of contents** pages. Moreover, they can create new tags, tables of contents and share them with their selected colleagues.

Important Tip: You should keep the **Tag administration** function **disabled** for all other roles except the **Super Admin**.

54. Now, scroll to the **Role relation settings and extended rights** widget and click it to open the **Role relation and extended rights** tab of the **New role**.

Manage Role Relations Settings and Extended Rights of the New Role

Remember, users with the **Share** rights on different content sharing modules can share content items e.g. pages, posts, forms, etc. to only those roles that are listed in the sharing relations of their role.

55. Select the required roles under the "**May share content with**" menu to allow the current role to share content with these roles.

Now, users associated with the current role will be allowed to share content to the selected roles in the modules where the current role has been assigned the sharing access right on the **Rights** tab.

Remember, users with the **Share** rights on content sharing modules can share content items e.g. pages, posts, forms, etc. to all business areas only if they have been allowed to do so in the extended sharing rights of the selected role. Similarly, users with access to Checklist and Form reports can view reports data for other business areas only if allowed from extended rights settings.

Otherwise, they can share content and view reports data for only those units and colleagues who are associated with their business area.

56. You can **allow** the users associated with the current role to **share content to any business area** by **switching** to the **Yes** option for the respective button under the **Extended rights** heading.

Remember, users with the **Share/Administer** rights on content sharing modules can edit or delete a content item only if they have sharing access to all roles, business areas, areas, units, clusters and users involved in the sharing selection of this item.

Note: "May share content with" (55) and extended sharing rights (56) settings are only valid for the modules where a particular role has been assigned the sharing access on the **Rights** tab.

These settings may apply to:

- Posts
- Pages
- Files
- Forms
- Tasks
- Checklists
- Checklists 2.0
- Audit checklists
- Forum admin
- Tag administration

Now, customise the staff management rights for the current role (if required) under the **May manage staff in** menu.

57. Select the required roles under the " **May manage staff in**" menu to allow the current role to manage users with these roles.

Note: " **May manage staff in**" settings are valid only if a role is assigned **"Write"** access on at least local level of **Our organisation** module.

These settings are irrelevant for roles for which Our organisation module is disabled or the role is assigned the **Read** right on its each level i.e. **Local**, **Central**, and **Global**.

When you are setting staff management relation of a particular role with other roles, make sure you don't allow users associated with it to manage any role that has a higher access level in your organisation than them.

In fact, only the **super admin** should be allowed to manage users associated with every role in your organisation.

57(a). You could allow the role of local unit manager or franchisee to manage local workers and other staff working under them.

57(b). You could allow the role of country/area manager to manage the roles of local unit manager or franchisee and other central staff working under them in their respective main areas.

By default, users associated with a role cannot view and manage users and units from other business areas.

58. You can allow users associated with the current role to **manage users and units in any business area** by **switching** to the **Yes** option for the respective button under the **Extended rights** heading.

This option (58) may apply to

- Our organisation
- Chat
- Statistics

So, when a role is allowed to manage users and units in any business area. Depending on their access levels on these three modules, users associated with this role can

- view/manage staff from other business areas in clusters and areas they have access to
- send messages to their colleagues from other business areas via the Chat module
- view data for units and colleagues from other business areas on the User activity module

59. Click the **Done** button in the bottom-right corner of the **Role relations and extended rights** page to save the selections you've made on this page for the new role.

Once you have made all the required and optional selections for the new role, carefully review all the information on both tabs of the **New role** page.

60. Click the **Save** button in the top-right corner of the page to add the new role to the **System setup** of your organisation.

After you save the new role, a pop-up message will show up suggesting you to adjust the relation between the newly created role and your existing roles and share some of your existing content with this role.
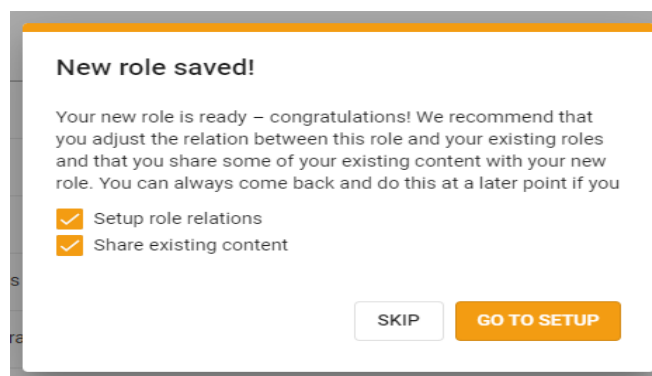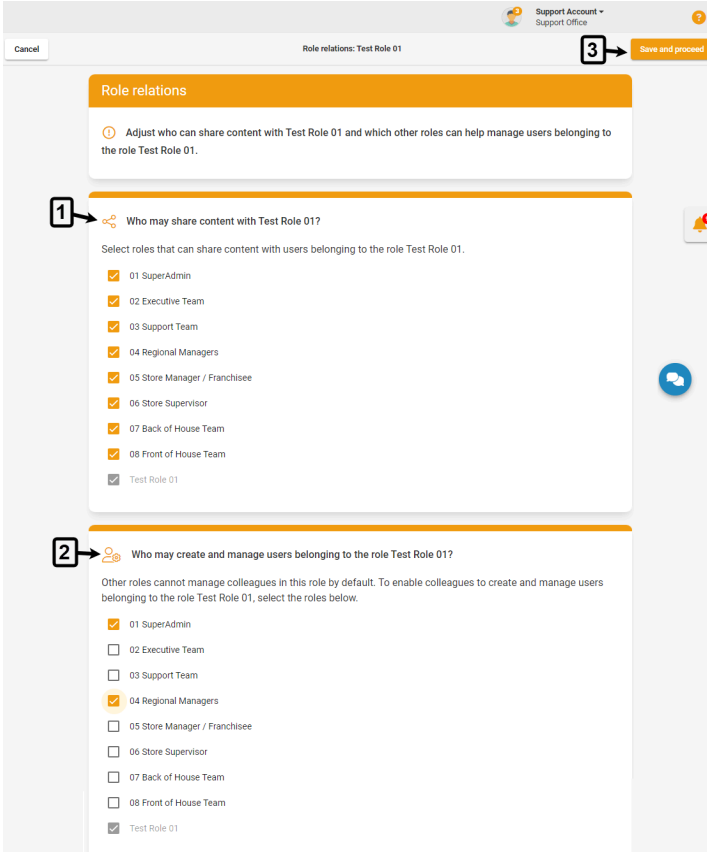
If this is the very first role you have created in your organisation and you do not have any content to share with it for now or want to adjust the role relation and share the content with it at a later point, you can simply **skip** this message.

61. However, if you have already created some other roles before this one and there is some existing relevant content that could be valuable for the current role, then you should click the **GO TO SETUP** button.

Set up Relation of the New Role with Other Roles

When you click the **GO TO SETUP** button, you will be redirected to the **Role relations** page for the selected role where you can set up the relation between this role and other roles in your organisation.

On the **Role relations** page for the selected role, you can decide who may share content with the role you have recently created and which other roles may administrate users associated with the selected role.

1. Under the **Who may share content with this role?** list, select the roles who will be allowed to share content with the current role from now on.
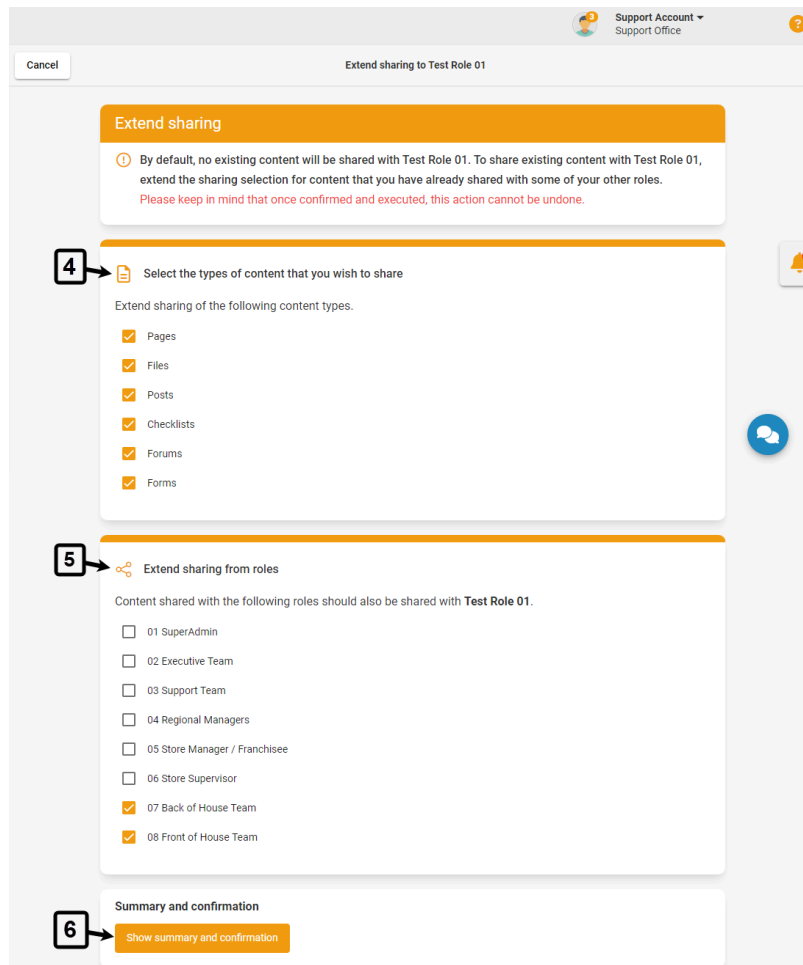
2. Under the **Who may create and manage users with this role?** list, select the roles who will be allowed to create and manage users associated with the current role.

Note: Keep the guidelines for the sharing and colleague management rights of a role in mind when you are making selections for the **Who may share content with this role?** list. See the User Guide for **Role Relation Settings and Extended Rights**

3. Click the **Save and proceed** button in the top-corner of the page to apply the selections you have made on the **Role relations** page for the selected role.

Extend Sharing of the Existing Content to the New Role

Now, you will be redirected to the **Extend sharing** page for the selected role where you can share existing pages, files, feed posts, checklists, forums, and forms with the recently created role.

You can share this content with the current role by extending the sharing selection for the content already shared with some other roles in your organisation.

https://chainformation.com/userguides

4. **Select the types of content that you wish to share** with the current role.

5. Under the **Extend sharing from roles** list, select the roles content shared with them you also want to share with the current role.

6. Now click the **Show summary and confirmation** button to review the number of each content type that will be shared with the current role once you confirm this action.

Note: Once you have confirmed the selections made on the **Extend sharing** page for the current role, the system will automatically share the selected content items shared with the selected roles, with the current role as well.

However, these selections will be valid only for the existing content and will not apply to any new page, file, post, checklist, forum, or form shared with the selected roles in the future.

Remember, you cannot undo this action from this page once it has been executed if you decide to stop sharing the content shared with the current role in the future.

Instead, you will have to stop sharing this content with the current role one by one by changing the **sharing selection** of each page, file, post, checklist, forum, and form shared directly from the **Extend sharing** page. See the User Guide for **Sharing Selection**

Therefore, carefully review the content types and roles you have selected on the **Extend sharing** page.
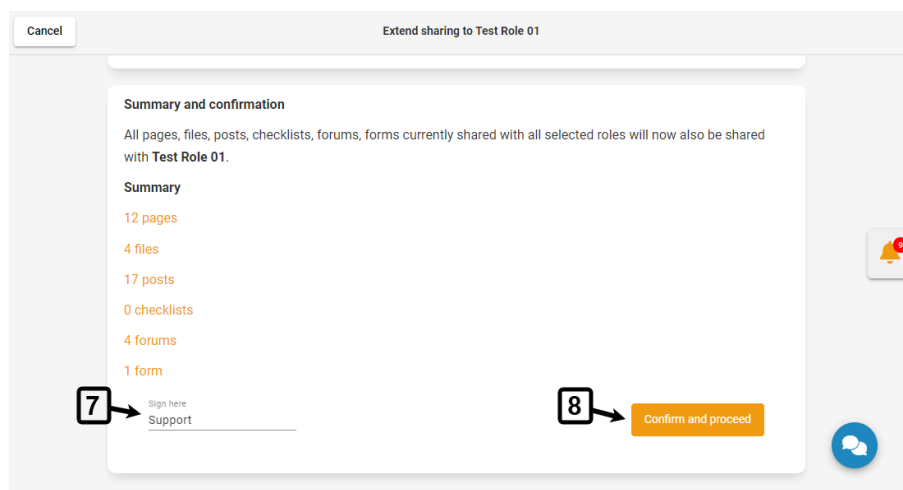
7. Once you have reviewed your selections, enter your digital signature in the **Sign here** field in the bottom-left corner of the page.

8. Click the **Confirm and proceed** button in the bottom-right corner of the page to execute the changes you have made.

9. Type the letters "**CONFIRM**" in the warning field shown on the screen and click the **CONFIRM** button to to extend sharing of the selected content items to the current role.
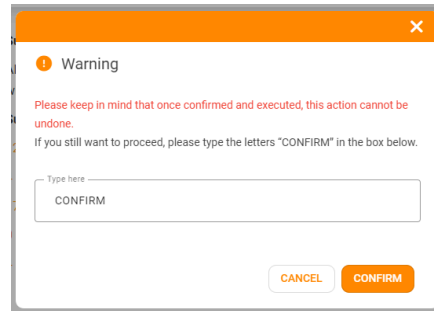
You have set up the new role and its relation with the existing roles in your organisation completely.

Now, you and other users associated with the roles that have been allowed to create and manage users with this role can associate the existing or new users with it. See the User Guide for **Colleagues**

Review the Existing Roles in Your Organisation

On the **Roles** tab of the **System setup** page, you can review and manage all the roles created by you and your colleagues.
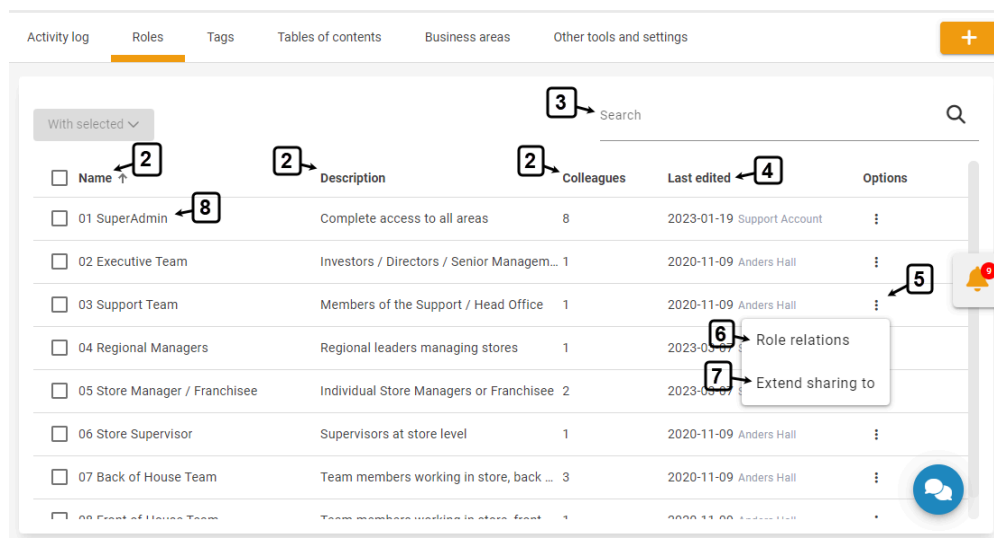
2. On the **Roles** page, you can view all the roles in your organisation, description of each role and the number of colleagues associated with it.

3. You can also use the **Search** field to find a role based on any of the available data/information. See the User Guide for **Search**

4. You can also view when and who has last edited a particular role in your organisation.

https://chainformation.com/userguides

5. You can adjust the relation of a role with other roles in your organisation and share existing content with it by clicking the **three-dots ellipsis** icon under the **Options** heading next to its name.

6. Click the **Role relations** button from the options menu of the role whose relation with other roles you want to adjust.

This will open the **Role relations** page for the selected role where you can adjust the relation between this role and other roles in your organisations. See the User Guide for **Role Relations**

7. Click the **Extend sharing to** button from the options menu of the role with which you want to share the existing content.

This will open the **Extend sharing** page for the selected role where you can share the existing content with it by extending the sharing selection for content already shared with some of your other roles. See the User Guide for **Extend Sharing to a Role**

8. Click the name of a role to view its details.

This will open the selected role page where you can view its complete description, all the functions enabled for it and the rights assigned to it for these functions.
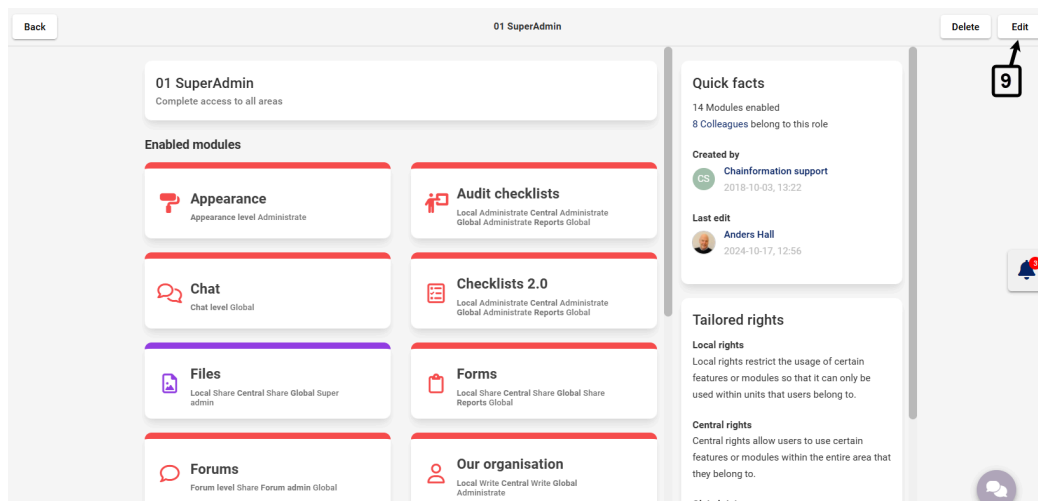
Note: Information about the extended rights of a role and its relations with other roles is not available on this page.

You can review this information on the editor page of a role only. (See the User Guide for **Edit a Role**)

9. You can edit the selected role by clicking the **Edit** button in the top-right corner of the page.

This will open the **Edit role** page where you can edit the selected role following the navigation steps demonstrated in the next section

Edit a Role
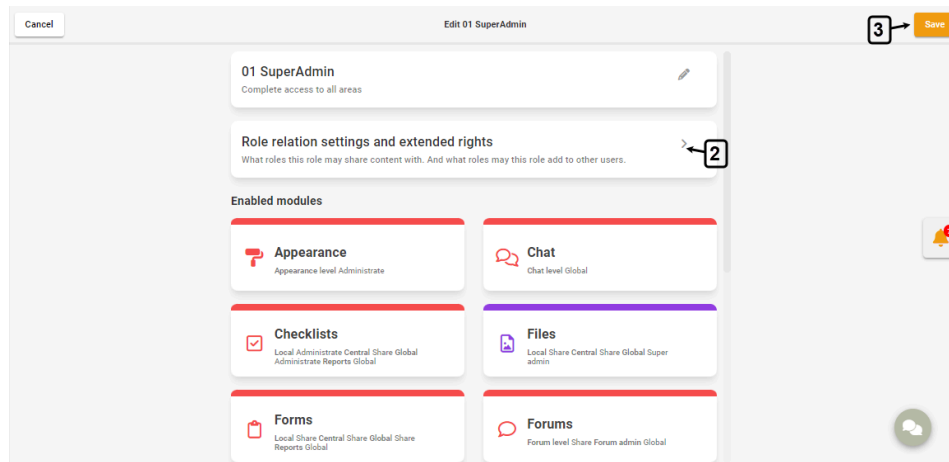
1. On the **Edit role** page, update the rights of the selected role for different modules of your organisation as required.

2. Click the **Role relation settings and extended rights** button to review and update (if required) these settings for the selected role.

Note: Keep the guidelines for the appropriate right of the selected role for each module, its relations with other roles and extended rights in mind when you are updating these settings. See the User Guide for **Create a New Role**

Once you have edited all the required details of the selected role, carefully review all the updated information on the editor page.

2. Click the **Save** button in the top-right corner of the page to apply the changes you have made for the selected role.

Visual Examples of Some Typical Roles in an Organisation

Now, we will show you visual examples of some typical roles in an organisation so that you could get a better idea about what should be the appropriate rights and extended rights for these roles.

Super Admin

These are the recommended rights of the **super admin** role for each module of an organisation.

These are the recommended extended rights of the **super admin** role of an organisation.

Regional or Country Manager

These are the recommended rights of the **regional or country manager** role for each module of an organisation.

These are the recommended extended rights of the **regional or country manager** role of an organisation.

Local Store Manager or Franchisee

These are the recommended rights of the **local store manager or franchisee** role for each module of an organisation.

These are the recommended extended rights of the **local store manager or franchisee** role of an organisation.

https://chainformation.com/userguides

Global Support / Marketing Team

These are the recommended rights of the **global support / marketing team** roles for each module of an organisation.

These are the recommended extended rights of the **global support / marketing team** role of an organisation.

https://chainformation.com/userguides

Local Staff

These are the recommended rights of the **local staff** and other roles with a limited access level for each module of an organisation.

These are the recommended extended rights of the **local staff** and other roles with a limited access level in an organisation.

https://chainformation.com/userguides

Remember, these are only a few examples and you may have some other roles in your organisation as well. Similarly, the exact names of roles in your organisation may differ from these examples. However, these visuals could help you to assign the appropriate rights and extended rights to the roles in your organisation similar to these examples.

Furthermore, the rights for each function of the roles and their extended rights shown in these examples are only recommendations and you may change them for your organisation as required.

Delete a Role

Remember, there is no Trash folder for the Roles module on the Chainformation platform from which you can restore a deleted role. Therefore, when you delete a role, the system will delete all the custom selections you have made for its rights and extended rights permanently.

Follow the navigation steps demonstrated below to delete a role from your organisation if you really want to do so.

1. Access the Roles tab on the System setup page by following the navigation steps as demonstrated in the previous section.

2. On the Roles page, navigate to the role you want to delete and check the checkbox next to its name.

3. Click the With selected button above the listed roles.

4. Click the **Delete** option from the **With selected** dropdown to delete the selected roles.

5. You can also delete a role by clicking the **Delete** button in the top-right corner of the Details page of the role you want to delete.

6. Click the **DELETE** button in the pop-up message shown on the screen to delete the selected role.
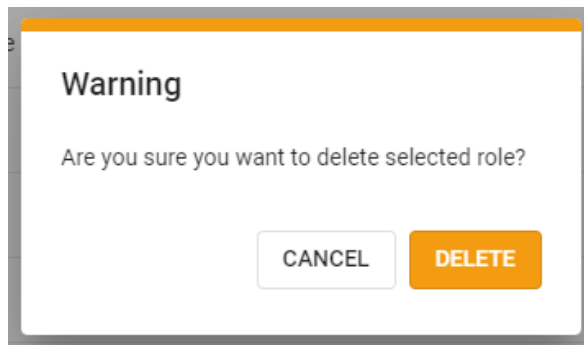
Note: You cannot delete a role until you have deleted all the users associated with it or assigned them another role. The system will show an error when you will try to delete a role that is connected to at least one user in your organisation.