Understanding User Rights And Roles In Nagios XI 2026R2

Purpose

This document describes Nagios XI user rights and permissions both individually, and through the use of Roles. Permissions enable you to to ensure security and obtain a web interface tailored to various individuals' needs.

Upgrade Considerations: if you are upgrading to 2026R2+ from a pre-2026R2 version, you can find details on how the migration of your users from the legacy per-user approach to Roles is handled by the upgrader in the special Understanding Upgrading From Pre-2026R2 Versions section.

Additional Resources

In addition to this document, Nagios XI Administrators should also familiarize themselves with this documentation that provides supporting information that will help you understand default user rights and permissions in Nagios XI:

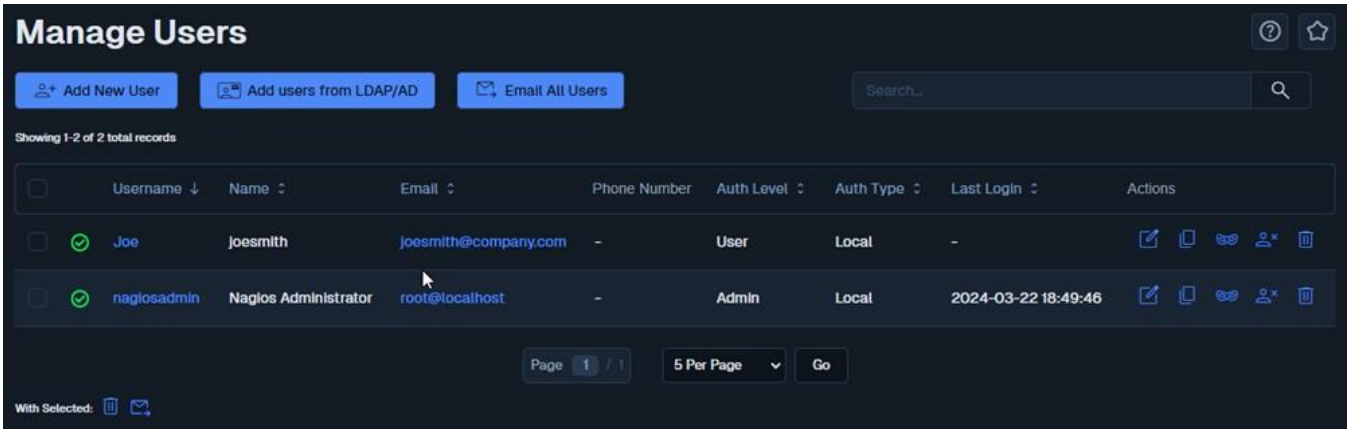
Nagios XI Multi-Tenancy

Managing Individual Users & Permissions

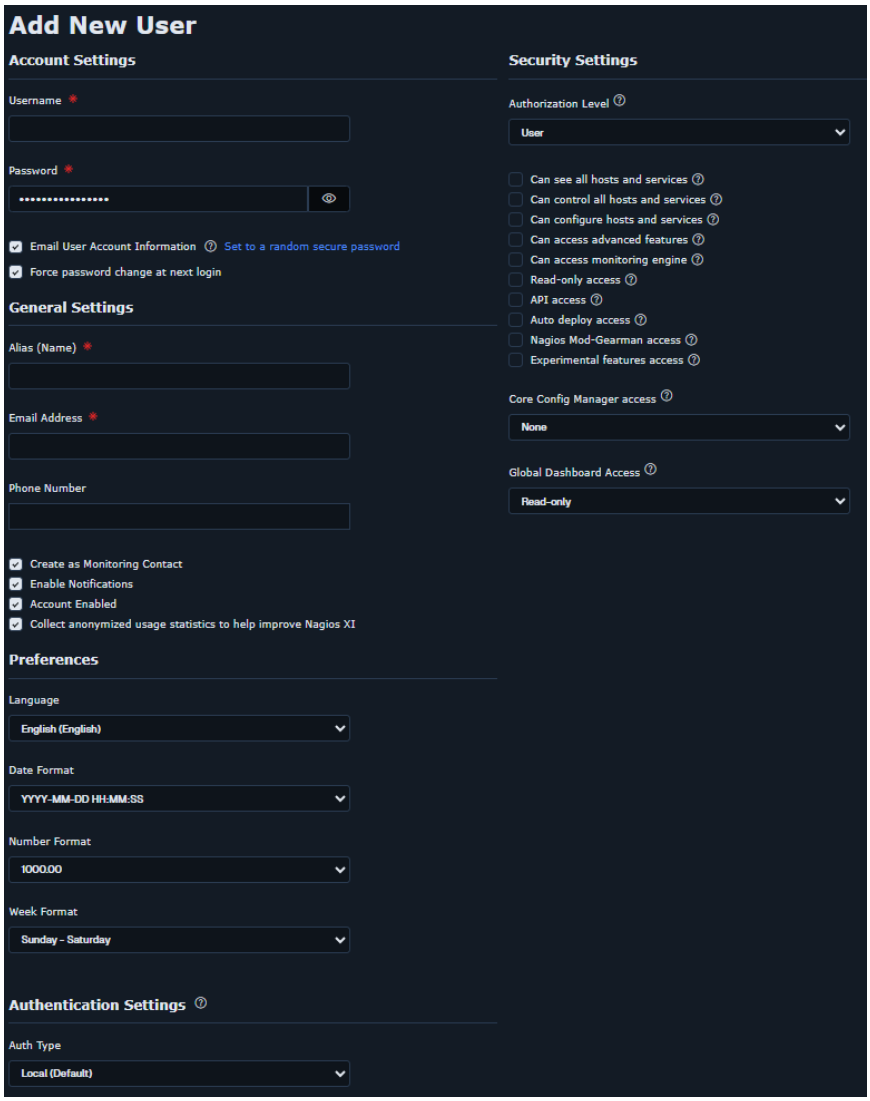
Permissions for individual users can be configured or changed when adding a new user account to Nagios XI or editing an existing user on the **Manage Users** page.

Note that permissions templates can also be created using Roles, covered later in this guide.

1. Navigate to **Admin > Users > Manage Users** to access this page.
2. To create a new user, click the **Add New User** button.
3. To edit an existing user, click the **edit** icon for the user you want to edit.



4. It is recommended that you enable the **Create as Monitoring Contact** option when creating a user. This ensures a matching contact object is created in the Nagios monitoring configuration. Most object access and visibility is validated against the contact when using Nagios XI.
5. Permissions are determined by the options selected in the **Security Settings** section of the **Add/Edit User** screen.
    a. The default selection under **Authorization Level** when a new user is created is **None**.
    b. With none of the options selected, the user will only be able to see host and services that have the user defined as a contact (in the notification preferences of the host or service object in Core Config Manager or when running a Configuration Wizard).



Authorization Level Settings

None

Select this option to either manage this user's settings individually, or to manage them with custom Roles other than User or Admin. If no Roles are applied to the user, the settings in the Edit User menu will determine their permissions. To manage settings individually, use the checkboxes and dropdowns in the Security Settings section, and do not make them a member of any Roles. To manage them with custom Roles, refer to the Managing Roles section of this guide. Permissions are granted based on a combination of individual settings and assigned Roles in an **additive** fashion.

User

This is the default Authorization Level selected when a *new* user is created.

This default Role, which can be customized in the **Manage Roles** menu, is highly restrictive and enables no permissions out of the box. So Users with this auth level will have various permissions depending on their individual settings and other Roles they are also a member of. Permissions granted by the User role settings are combined with individual permissions and other Roles they are a member of in an **additive** fasion.

Admin

Users that are configured with an **Authorization Level** of **Admin** will have the ability to access, add, and re-configure the following:

- Users
- Hosts
- Services
- Components
- Configuration Wizards
- Dashlets
- Program Settings
- Security Credentials
- Nagios XI REST API (full access)

Note that the full access Admin Role cannot be edited or deleted.

Security Setting Options

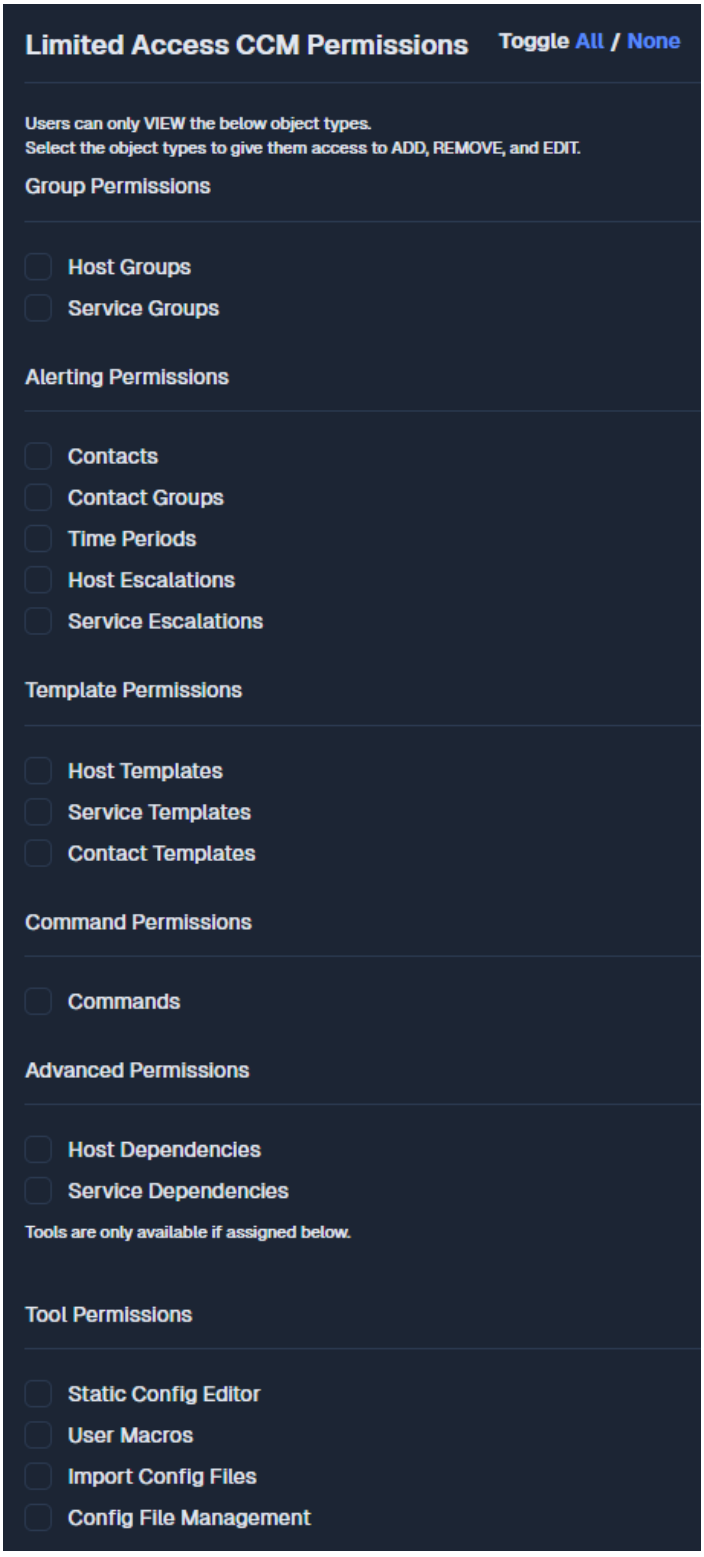
Setting	What It Means
Can see all hosts and services	The user can see all hosts and services that are being monitored – not just the ones they are a direct or indirect notification contact.
Can control all hosts and services	The user can: - Acknowledge problems - Schedule downtime - Toggle notifications - Force checks on all objects
Can configure hosts and services	The user can: - Run Configuration Wizards - Delete from detail page - Re-configure from detail page
Can access advanced features (in Roles, *Advanced User)*	The user can: - Edit check command in re-configure host/service page - Show the Advanced tab and commands on host/service page - Allows setting host parents in wizards and in re-configure host/service page
Can access monitoring engine	The user can: - See the monitoring process icon on the navigation bar - Control (e.g. shutdown or restart) the monitoring engine - Allows access to the Event Log
Read-only access	This option restricts the user to a read only role and overwrites other options preceding it
API access	The Nagios XI REST API allows users to create/query to read, write, delete, and update data in the Nagios XI system through commands that are authenticated via Nagios XI API keys. This is explained in the Nagios XI API section in this document.
Auto deploy access	Allow access to use the Auto Deployment component (**Configure > Auto Deployment**).

Setting	What It Means
Nagios Mod-Gearman access	Allow access to Nagios Mod-Gearman (**Configure > Remote Workers**).
Experimental features access	Allow access to experimental features, if they are enabled. *Note: This can be overridden by the Make accessible for all users setting in the System Settings page.*
Configuration Manager access (*see details on following page*).	Determines access to the Core Config Manager: - **None** = No access, Configuration Manager is not visible to the user - **Login** = Can view Configuration Manager links and must login with a Configuration Manager user account - **Limited** = Allows integrated Configuration Manager access, they only have access to the objects their contact has been granted to however higher permission can be granted (see below) - **Full** = Full Configuration Manager access with no Admin features
Global Dashboard Access	Determines level of access to global dashboards.

Limited Access CCM Permissions

The screenshot shows the table that will appear when the **Limited** option is selected for **Core Config Manager** access.

You can grant the ability to **ADD**, **REMOVE**, and **EDIT** specific object types. An option not selected implies they will only have the **VIEW** ability.

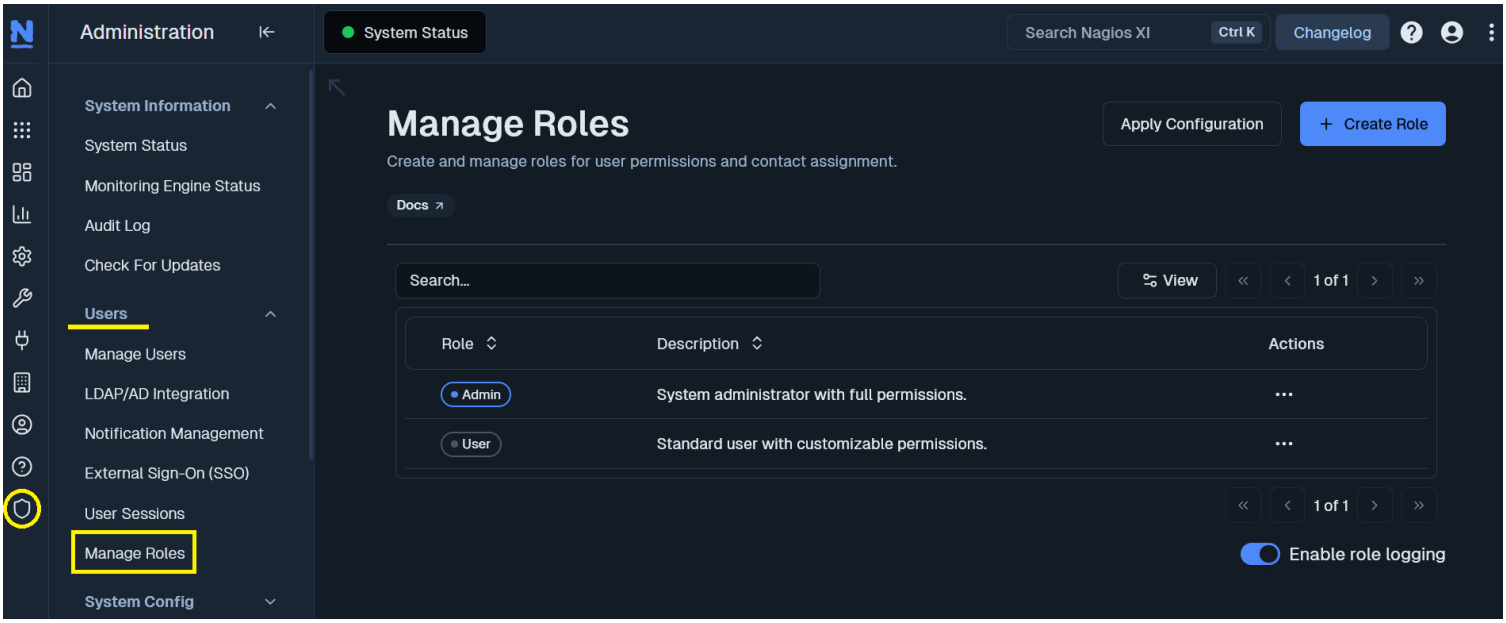


Managing Roles

Roles provide a way to template user permissions and quickly apply them to new and existing users.

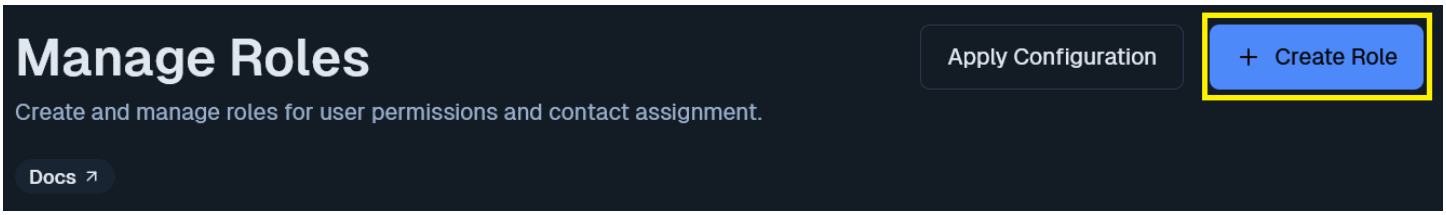
Note that when multiple Roles, or Roles and individual user settings (in the **Add/Edit User** menu) are combined, the user will be granted permissions in an **additive** fasion. For example, if one assigned Role does not allow the user to see all hosts and services, and another does, the user will be able to see all hosts and services.

Roles can be found in the **Admin > Users > Manage Roles** menu:

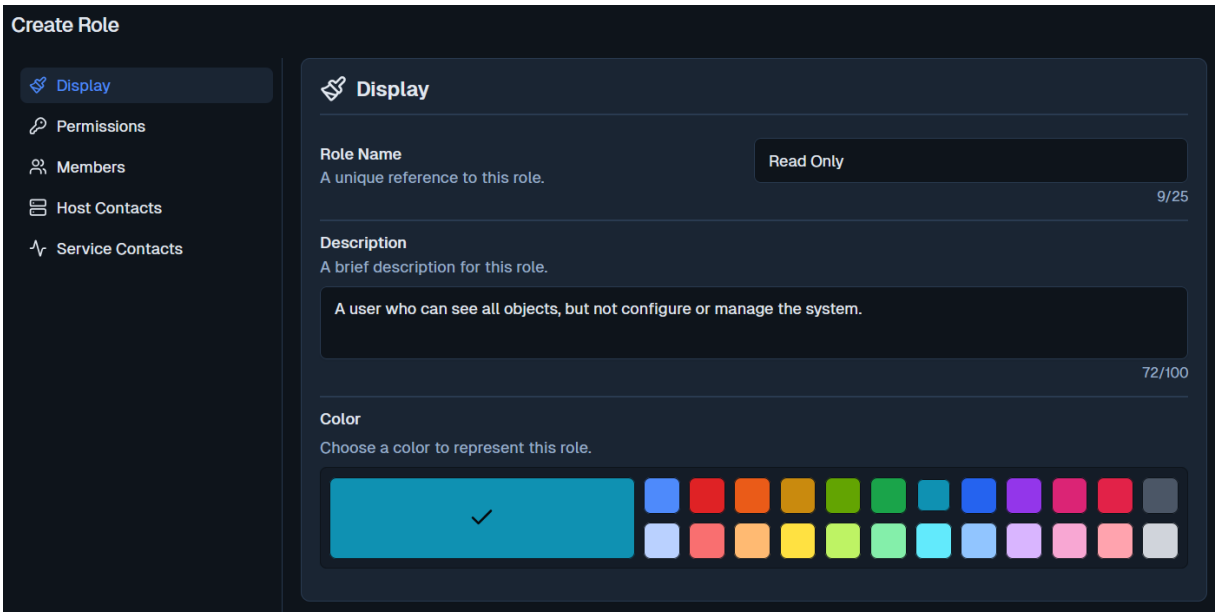


Creating a New Role

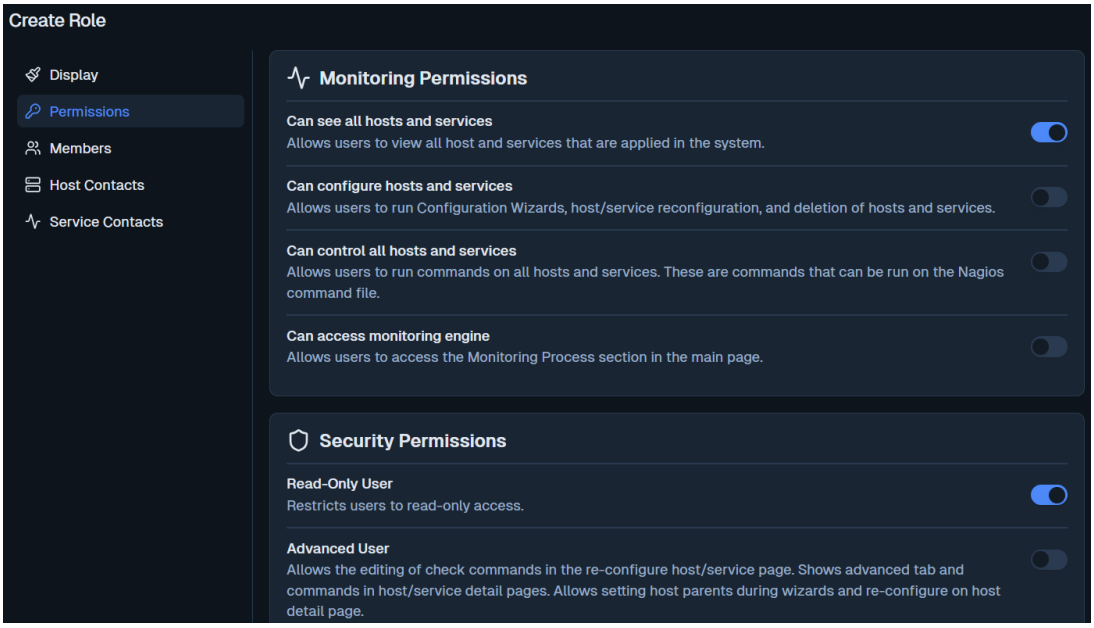
To create a new Role, click **+ Create Role** on the upper right.



In the **Display** section, enter a unique Role Name, optional Description, and choose a Color.

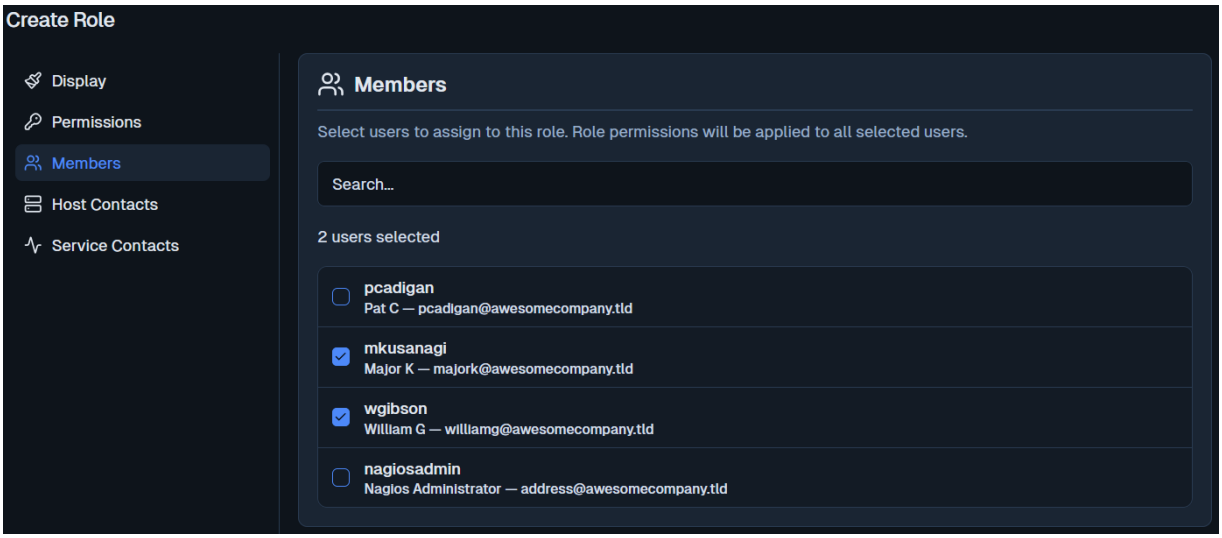


In the **Permissions** section, choose the Role permissions.

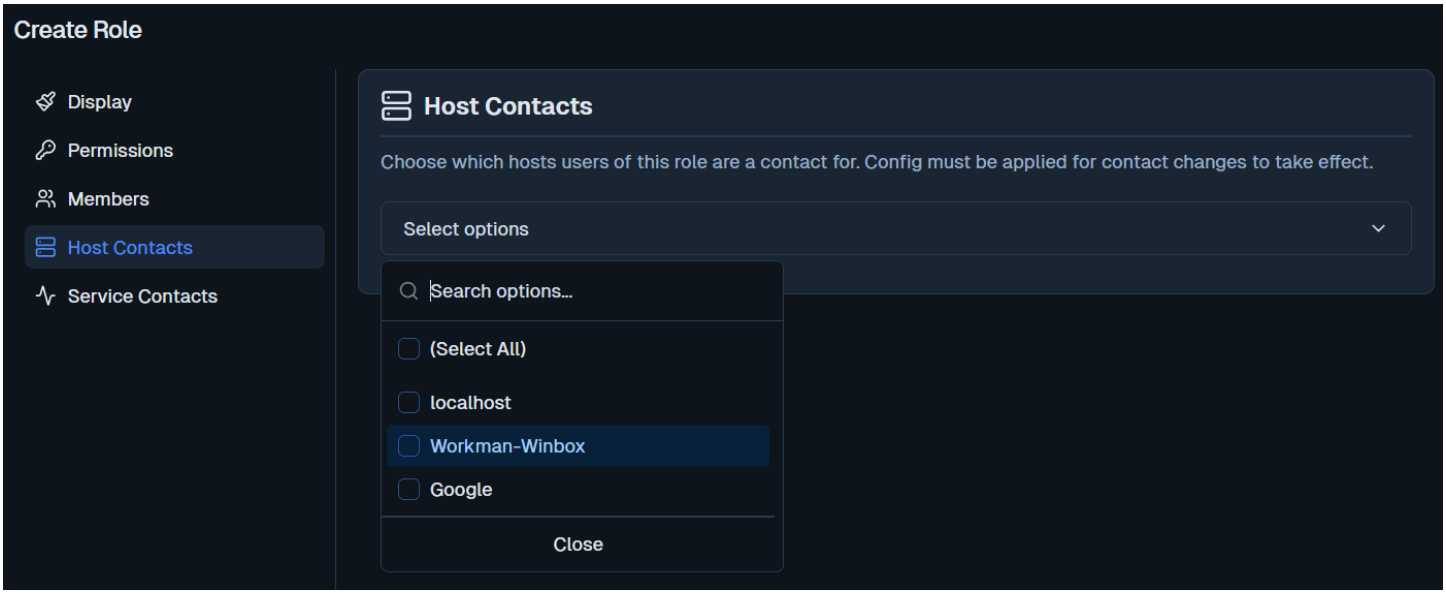


In this example, we've also chose **Read Only Global Dashboard Access** lower in the menu**.**

Next, choose the users to apply the Role to in the **Members** section.



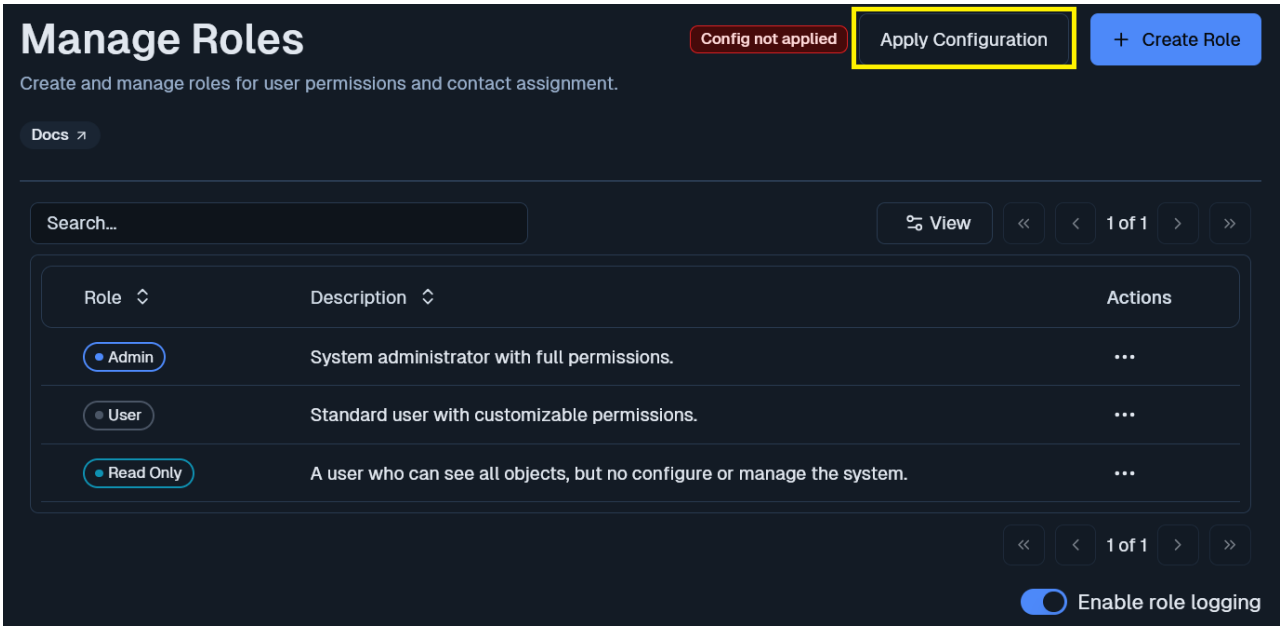
Finally, choose the hosts and services that the Role should be a contact on in the **Host Contacts** and **Service Contacts** sections.



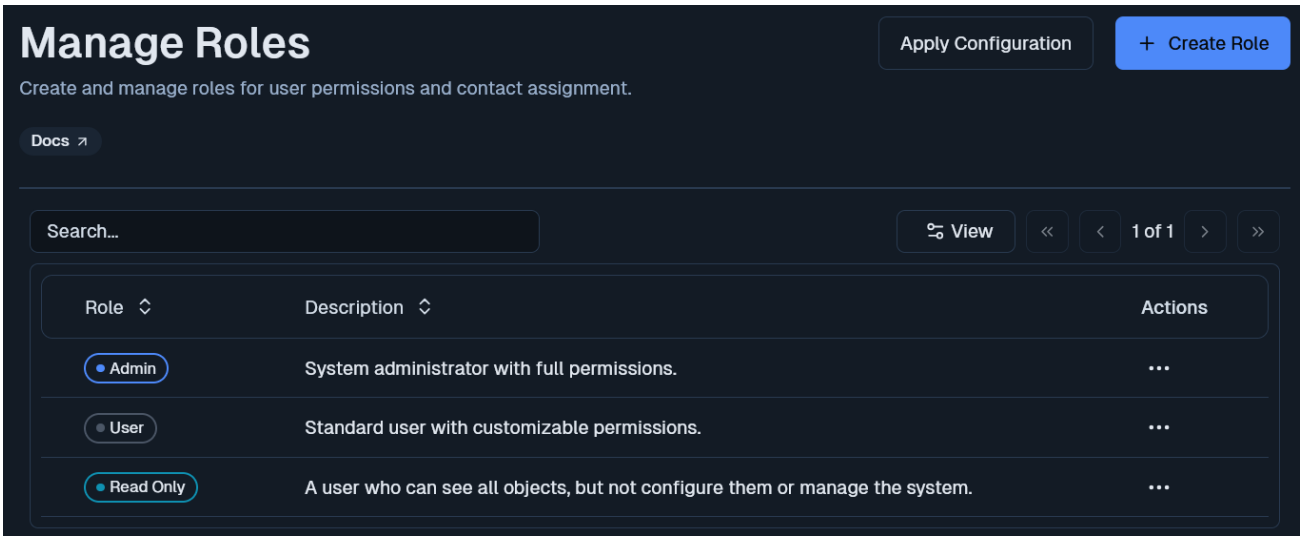
Click **Create Role** to finalize the Role creation.

When a Role is created, a corresponding contact group is also created, so that group members will have visibility of the selected host and service objects chosen in the Host Contacts and Service Contacts section.

After creating your Role or editing it later, you will need to apply the config to write the contact group changes to the Core configs. To do so, click **Apply Configuration** on the upper right.



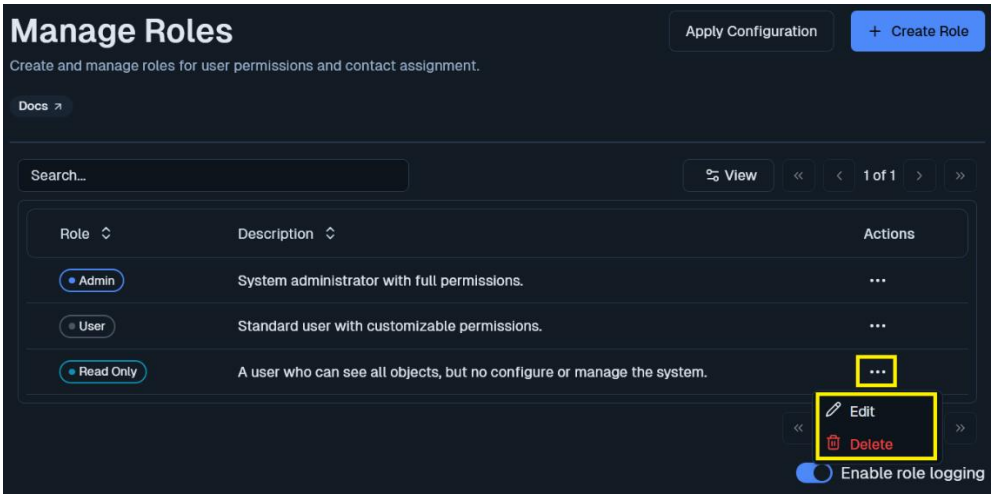
Your new Role is now fully configured and active.



Editing and Deleting Roles

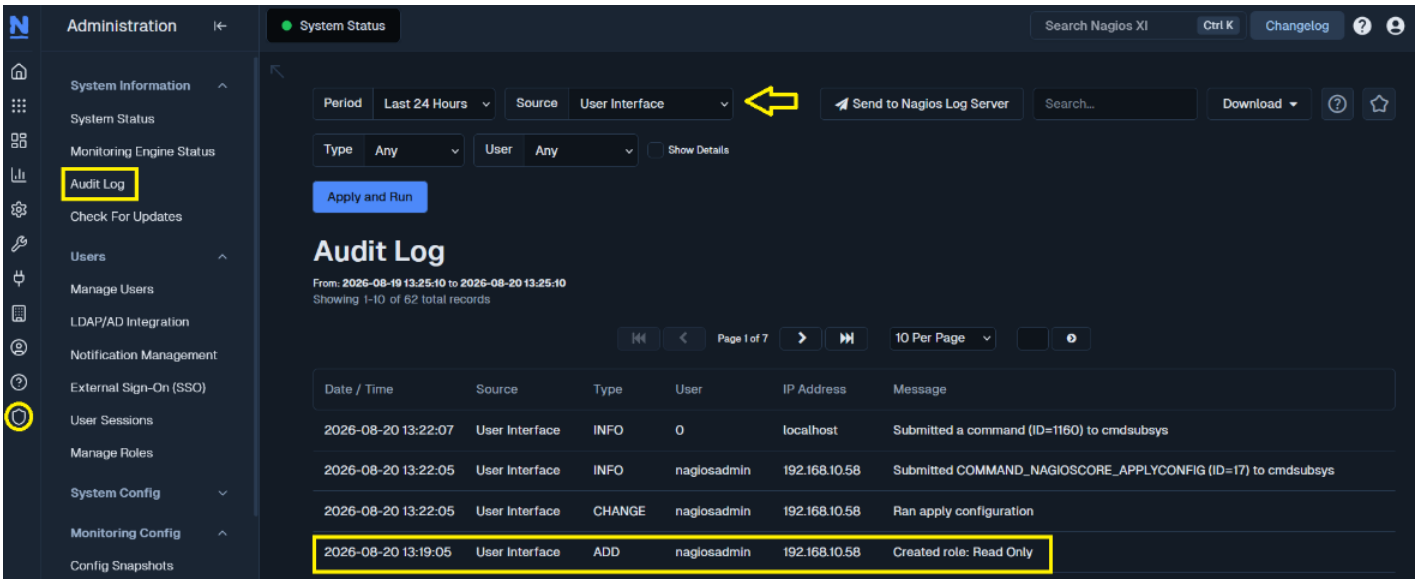
To **Edit** or **Delete** a Role, click the Actions icon to the right of the entry, then select your desired funcion from the dropdown.

Note that after editing a Role, you'll need to again Apply Configuration.



About Role Logging

The **Enable role logging** toggle on the bottom right of Manage Roles can be used to activate/deactivate Role logging. If it is enabled, Role management actions will appear as User Interface Source events in **Admin > Audit Log**.

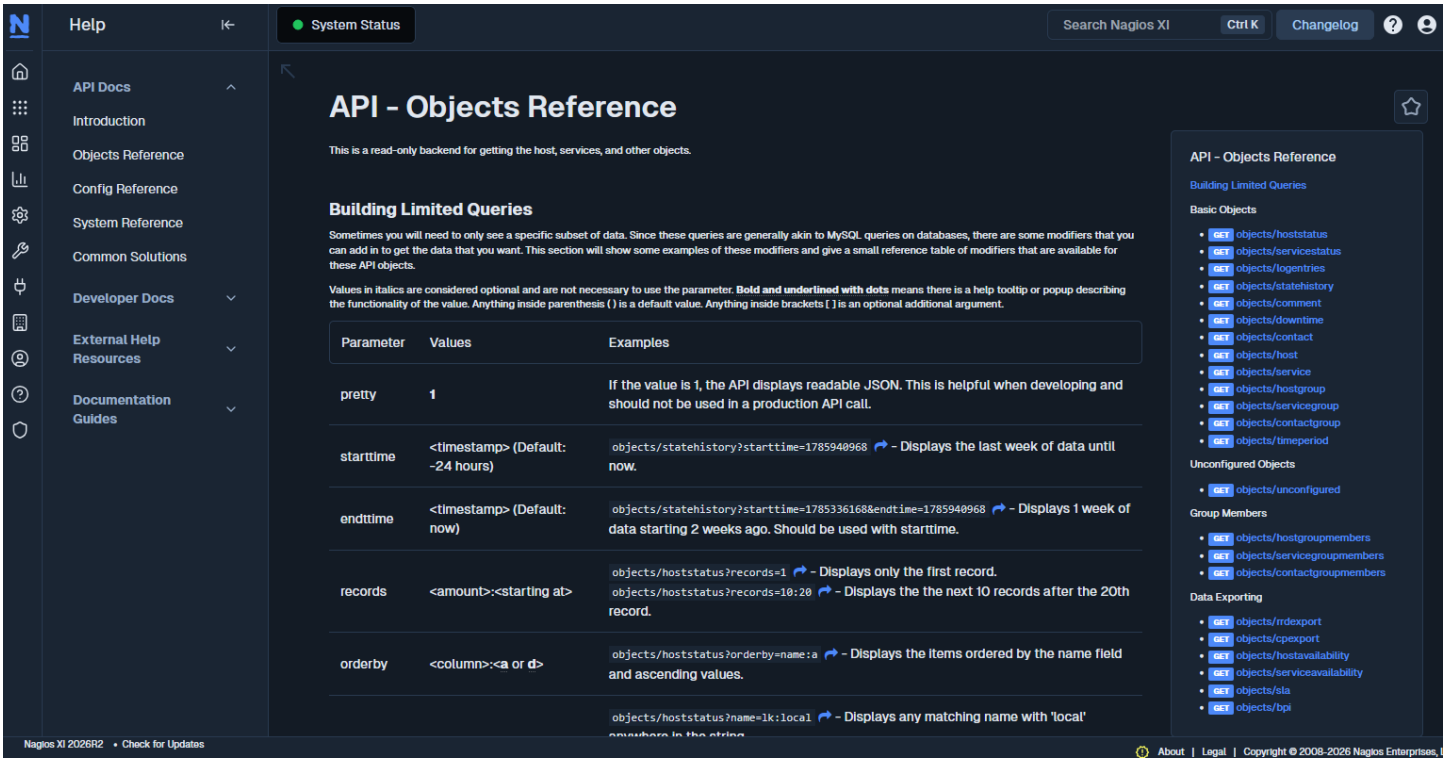


Nagios XI API

The Nagios XI REST API allows users to read, write, delete, and update data in the Nagios XI system through commands that are authenticated via Nagios XI API keys. Each user has their own API key to access the API and access is outlined as follows:

- Normal users are allowed to have read access if granted API Access via their user settings or Roles they are a member of. They will only have access to the Objects API endpoint and the related Help documentation.
- **Admin** users have full access to all sections of the API automatically.
- Access to any of the API documentation in the Help menu is restricted to users who have API access.

Detailed information on how to use the API can be found in the Nagios XI web interface under **Help > API Docs**.



You can also refer to this guide for additional details:

Accessing and Using the Nagios XI REST API

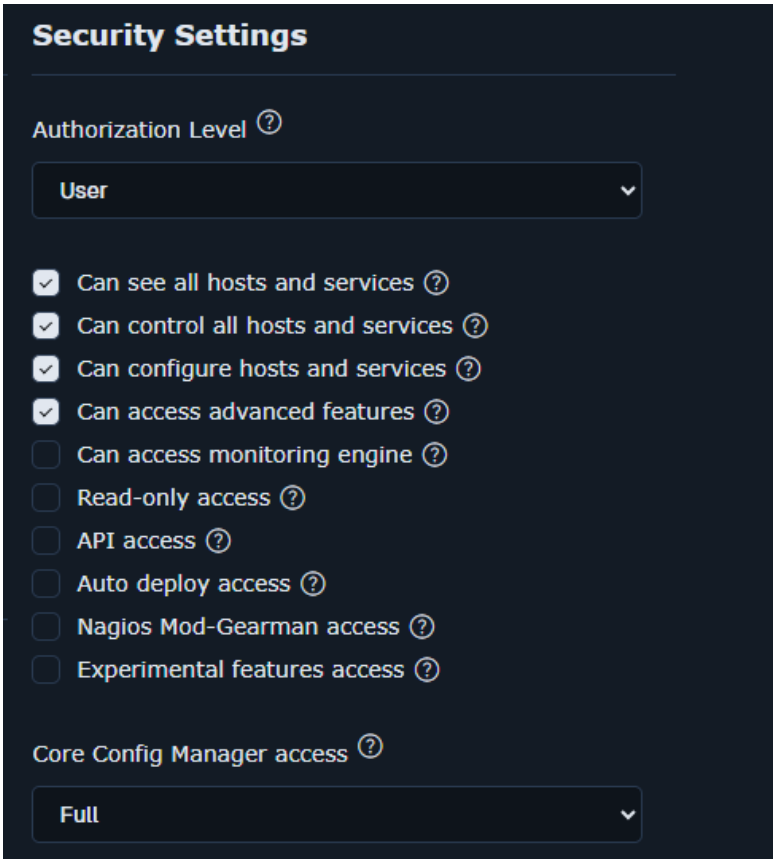
Example User/Role Permissions

Advanced User with Change Control

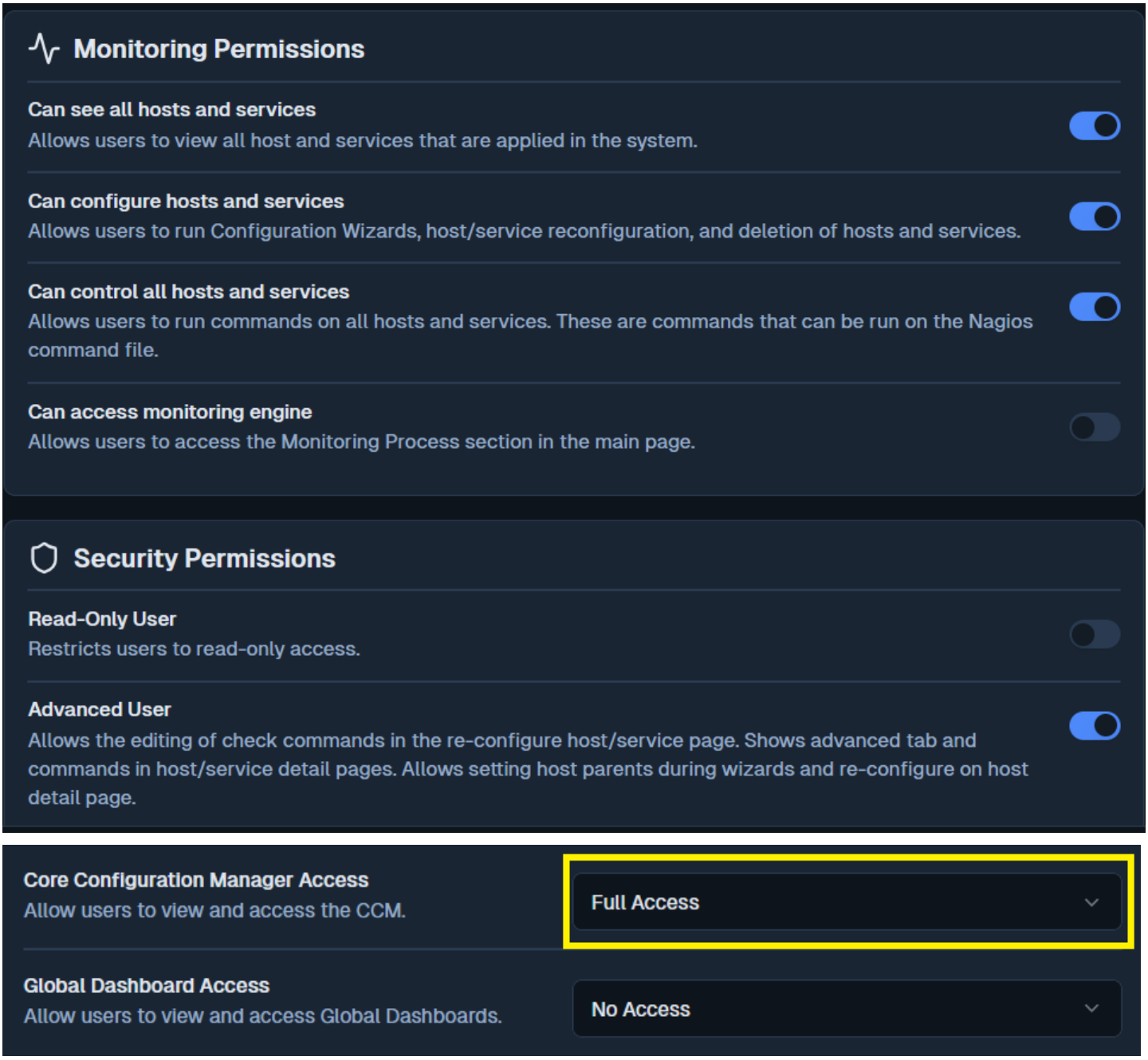
Common settings for an advanced user who should have rights to see, control, and re-configure all existing hosts and services that are being monitored, as well as add new hosts and services to the monitoring configuration is shown in this screenshot.

A user with these settings will have access to advanced information and commands relating to hosts and services that are being monitored, but will not have access to control (shutdown, start, etc.) the monitoring engine.

This user will also have the ability to use the **Core Configuration Manager** to manage object configurations. Individual user settings would look like this:



A Role reflecting the above permissions would look like this:

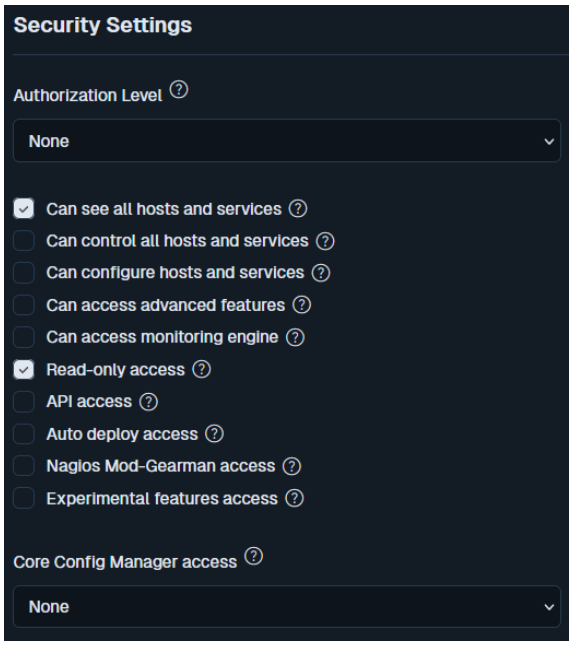


Basic Read-Only User

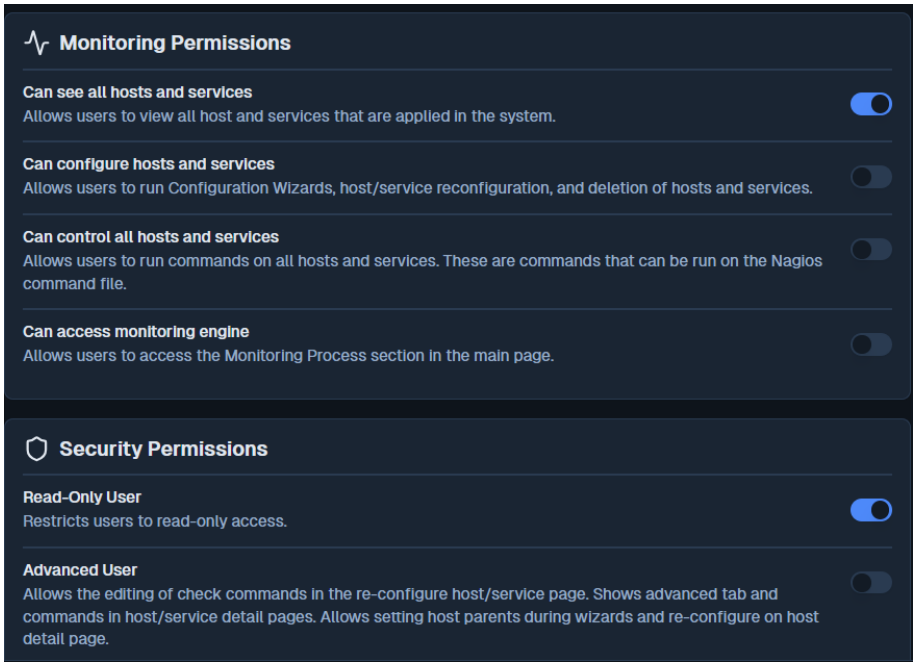
Common settings for a basic user who can see all hosts and services that are being monitored, but who cannot re-configure anything or submit commands to the monitoring engine is shown this screenshot.

These settings are often used when configuring access for IT managers or decision makers that should be granted access to view monitoring information, but do not need access to modify anything.

Invididual User Settings



Role Settings



Understanding Upgrading From Pre-2026R2 Versions

This section outlines the imlications on your existing users when upgrading to XI 2026R2+ from pre-2026R2 versions. Although your existing user permissions will persist after the upgrade, it's useful to understand specifically what happens after upgrade, and to understand the impact the migration to Roles will have going forward.

What You'll See After Upgrade

After upgrade, users will retain their previously assigned Authorization Level, either User or Admin. Permissions for those with the User auth level will be determined by their individual Security Settings, since by default the User Role has no permissions. Those with the Admin auth level will retain their full visibility and access, since the Admin Role enables all possible permissions.

Effects on Contact Groups

Since each Role has an associated Contact Group, your existing users will also be added to the new User or Admin contact groups. Adding associated users to these groups enables multi-tenant limited object visibility based on Role.

Since each Role has an associated contact group, going forward you'll see these contact groups in places like Step 4 of the monitoring wizards. To give users with a Role visibility of the objects you're creating with the wizard, simply select the associated contact group.

Effects of Modifying the User Role

Keep in mind that if you enable any permissions in the User Role, that will impact every user who has that auth level. Since all of your users who were not Admin are converted to the User Role, enabled permissions will effect all but Admin users.

For example, if you enable API access for the User Role, every User level user will be granted API access. To avoid this, one option would be to switch the Authorization Level of any users you don't want the User Role to impact to None, so that only their individual Security Settings, and other Roles will impact their permissions. Switching them between User, None, and Admin in the Edit User menu will update their Role membership, and modifying their User or Admin Role membership will update the Authorization Level shown in their individual user settings.

Finishing Up

This completes the documentation on understanding user rights. If you have additional questions or other support-related questions, please visit the Nagios Support Forum, Nagios Documentation Hub, or Nagios Library:

Visit Nagios Support Forum Visit Documentation Hub Visit Nagios Library