

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 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.

Manage Users

Showing 1-2 of 2 total records

☐	Username ↓	Name ↕	Email ↕	Phone Number	Auth Level ↕	Auth Type ↕	Last Login ↕	Actions
☐	Joe	joesmith	joesmith@company.com	-	User	Local	-	edit copy reset add delete
☐	nagiosadmin	Nagios Administrator	root@localhost	-	Admin	Local	2024-03-22 18:49:46	edit copy reset add delete

Page 1 / 1 5 Per Page Go

With Selected: [edit](#) [copy](#)

Understanding User Rights And Roles In Nagios XI 2026R2

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).

Add New User

Account Settings

Username *

Password *

☒ Email User Account Information ⓘ [Set to a random secure password](#)

☒ Force password change at next login

General Settings

Alias (Name) *

Email Address *

Phone Number

☒ Create as Monitoring Contact

☒ Enable Notifications

☒ Account Enabled

☒ Collect anonymized usage statistics to help improve Nagios XI

Security Settings

Authorization Level ⓘ

User

☐ Can see all hosts and services ⓘ

☐ Can control all hosts and services ⓘ

☐ Can configure hosts and services ⓘ

☐ Can access advanced features ⓘ

☐ Can access monitoring engine ⓘ

☐ Read-only access ⓘ

☐ API access ⓘ

☐ Auto deploy access ⓘ

☐ Nagios Mod-Gearman access ⓘ

☐ Experimental features access ⓘ

Core Config Manager access ⓘ

None

Global Dashboard Access ⓘ

Read-only

Preferences

Language

English (English)

Date Format

YYYY-MM-DD HH:MM:SS

Number Format

1000.00

Week Format

Sunday - Saturday

Authentication Settings ⓘ

Auth Type

Local (Default)

Understanding User Rights And Roles In Nagios XI 2026R2

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** fashion.

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.

Understanding User Rights And Roles In Nagios XI 2026R2

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, <i>Advanced User</i>)	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).

Understanding User Rights And Roles In Nagios XI 2026R2

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. <i>Note: This can be overridden by the Make accessible for all users setting in the System Settings page.</i>
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.

Understanding User Rights And Roles In Nagios XI 2026R2

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.

Limited Access CCM Permissions Toggle [All](#) / [None](#)

Users can only **VIEW** the below object types.
Select the object types to give them access to **ADD, REMOVE, and EDIT**.

Group Permissions

- ☐ Host Groups
- ☐ Service Groups

Alerting Permissions

- ☐ Contacts
- ☐ Contact Groups
- ☐ Time Periods
- ☐ Host Escalations
- ☐ Service Escalations

Template Permissions

- ☐ Host Templates
- ☐ Service Templates
- ☐ Contact Templates

Command Permissions

- ☐ Commands

Advanced Permissions

- ☐ Host Dependencies
- ☐ Service Dependencies

Tools are only available if assigned below.

Tool Permissions

- ☐ Static Config Editor
- ☐ User Macros
- ☐ Import Config Files
- ☐ Config File Management

Understanding User Rights And Roles In Nagios XI 2026R2

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** fashion. 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:

The screenshot shows the Nagios XI interface. In the left sidebar, the 'Users' menu is expanded, and 'Manage Roles' is highlighted. The main content area is titled 'Manage Roles' and includes a search bar, a table of roles, and a '+ Create Role' button. The table lists two roles: 'Admin' (System administrator with full permissions) and 'User' (Standard user with customizable permissions). The 'Create Role' button is highlighted in the top right corner.

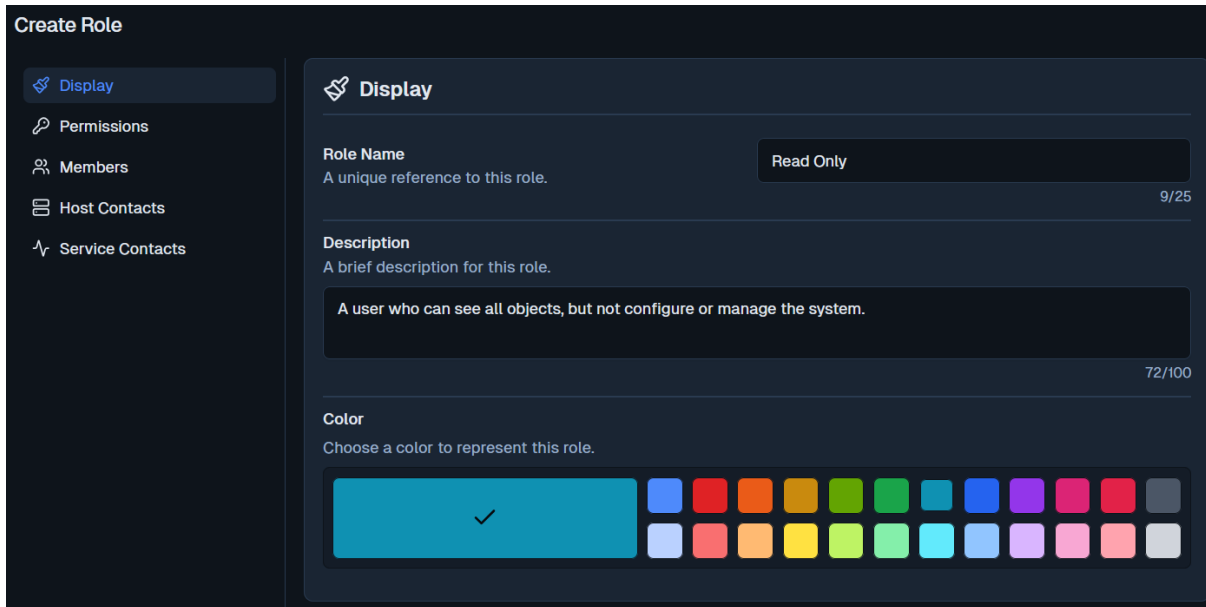
Creating a New Role

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

This is a close-up of the 'Manage Roles' page. The '+ Create Role' button is highlighted with a yellow box. The page title is 'Manage Roles' and the subtitle is 'Create and manage roles for user permissions and contact assignment.' The 'Docs' link is visible in the bottom left.

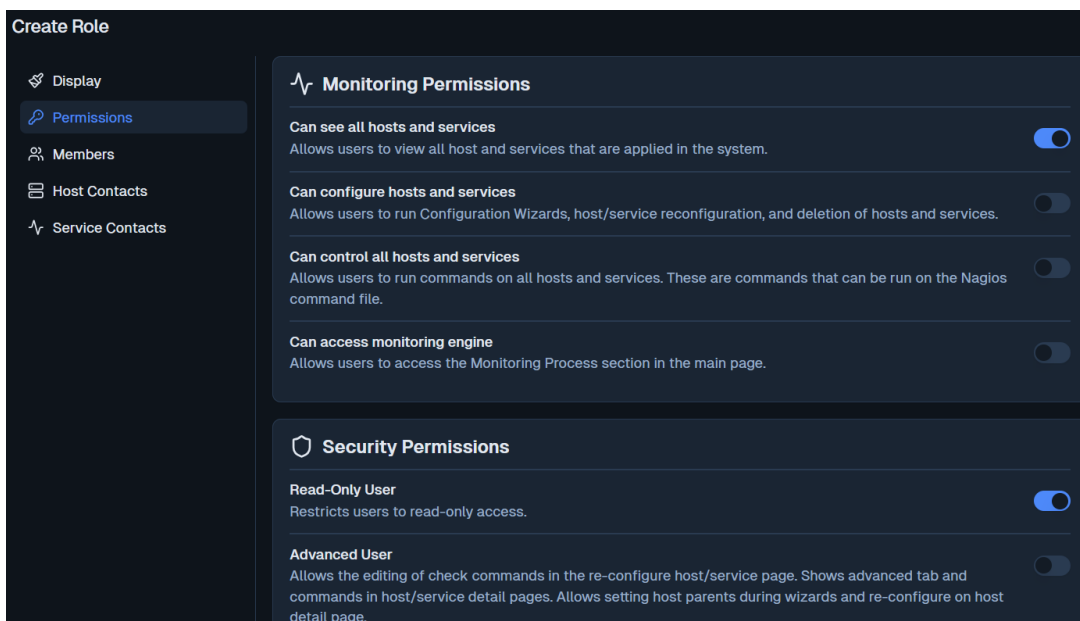
Understanding User Rights And Roles In Nagios XI 2026R2

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



The screenshot shows the 'Create Role' form in Nagios XI, specifically the 'Display' section. On the left is a sidebar with navigation links: Display (selected), Permissions, Members, Host Contacts, and Service Contacts. The main form area has a title 'Display' with a tag icon. It contains three fields: 'Role Name' with the value 'Read Only' and a character count of 9/25; 'Description' with the text 'A user who can see all objects, but not configure or manage the system.' and a character count of 72/100; and 'Color' with a color picker showing a teal color selected with a checkmark. Below the color picker is a grid of 24 color swatches.

In the **Permissions** section, choose the Role [permissions](#).



The screenshot shows the 'Create Role' form in Nagios XI, specifically the 'Permissions' section. The sidebar is the same as the previous screenshot, but 'Permissions' is now selected. The main form area has a title 'Monitoring Permissions' with a tag icon. It contains four toggle switches: 'Can see all hosts and services' (checked), 'Can configure hosts and services' (unchecked), 'Can control all hosts and services' (unchecked), and 'Can access monitoring engine' (unchecked). Below these is a section titled 'Security Permissions' with a shield icon. It contains two toggle switches: 'Read-Only User' (checked) and 'Advanced User' (unchecked).

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

Understanding User Rights And Roles In Nagios XI 2026R2

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

The screenshot shows the 'Create Role' interface in Nagios XI. On the left is a sidebar with navigation links: 'Display', 'Permissions', 'Members' (highlighted), 'Host Contacts', and 'Service Contacts'. The main panel is titled 'Members' and contains the text 'Select users to assign to this role. Role permissions will be applied to all selected users.' Below this is a search bar labeled 'Search...'. A status line indicates '2 users selected'. A list of users follows, each with a checkbox, a name, and an email address: 'pcadigan' (Pat C — pcadigan@awesomecompany.tld), 'mkusanagi' (Major K — majork@awesomecompany.tld), 'wglbson' (William G — williamg@awesomecompany.tld), and 'nagiosadmin' (Nagios Administrator — address@awesomecompany.tld). The checkboxes for 'mkusanagi' and 'wglbson' are checked.

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

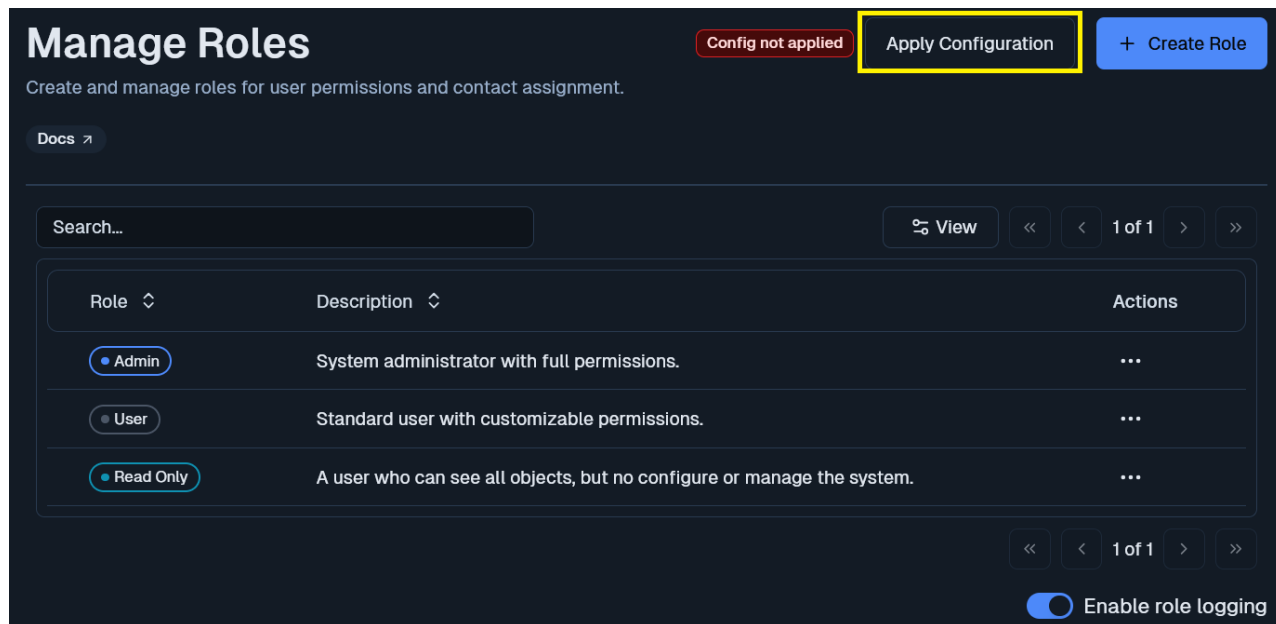
The screenshot shows the 'Create Role' interface in Nagios XI, specifically the 'Host Contacts' section. The sidebar on the left has 'Host Contacts' highlighted. The main panel is titled 'Host Contacts' and contains the text 'Choose which hosts users of this role are a contact for. Config must be applied for contact changes to take effect.' Below this is a dropdown menu labeled 'Select options'. A search modal is open, showing a search bar 'Search options...' and a list of options: '(Select All)', 'localhost', 'Workman-Winbox' (highlighted), and 'Google'. A 'Close' button is at the bottom of the modal.

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

Understanding User Rights And Roles In Nagios XI 2026R2

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.

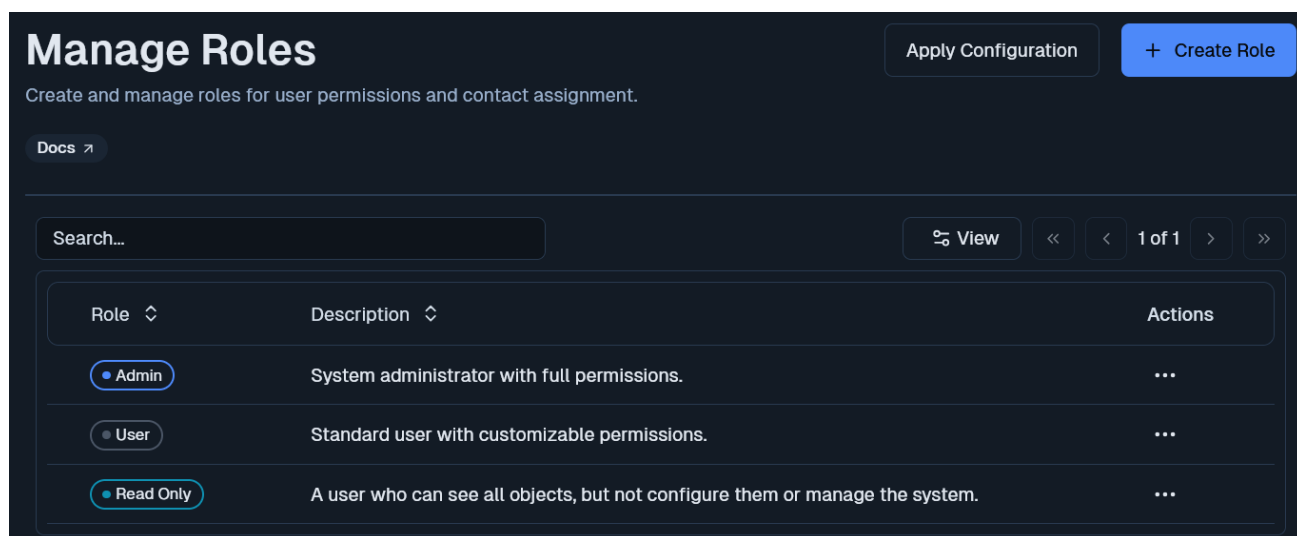
After creating your Role or editing it later, you will need to apply the config to write the contact group changes to the Core configs. To do so, click **Apply Configuration** on the upper right.



The screenshot shows the 'Manage Roles' interface in Nagios XI. At the top right, there is a red button labeled 'Config not applied' and a blue button labeled 'Apply Configuration', which is highlighted with a yellow box. To the right of the 'Apply Configuration' button is a blue button labeled '+ Create Role'. Below these buttons is a subtitle: 'Create and manage roles for user permissions and contact assignment.' On the left, there is a 'Docs' link. Below the subtitle is a search bar labeled 'Search...'. To the right of the search bar is a 'View' button and pagination controls showing '1 of 1'. Below this is a table with three columns: 'Role', 'Description', and 'Actions'. The table contains three rows: 'Admin' (System administrator with full permissions), 'User' (Standard user with customizable permissions), and 'Read Only' (A user who can see all objects, but no configure or manage the system). At the bottom right, there is a toggle switch labeled 'Enable role logging' which is currently turned on.

Role	Description	Actions
Admin	System administrator with full permissions.	...
User	Standard user with customizable permissions.	...
Read Only	A user who can see all objects, but no configure or manage the system.	...

Your new Role is now fully configured and active.



This screenshot is similar to the previous one, showing the 'Manage Roles' interface. The 'Apply Configuration' button is now visible without the 'Config not applied' warning. The table and other elements remain the same.

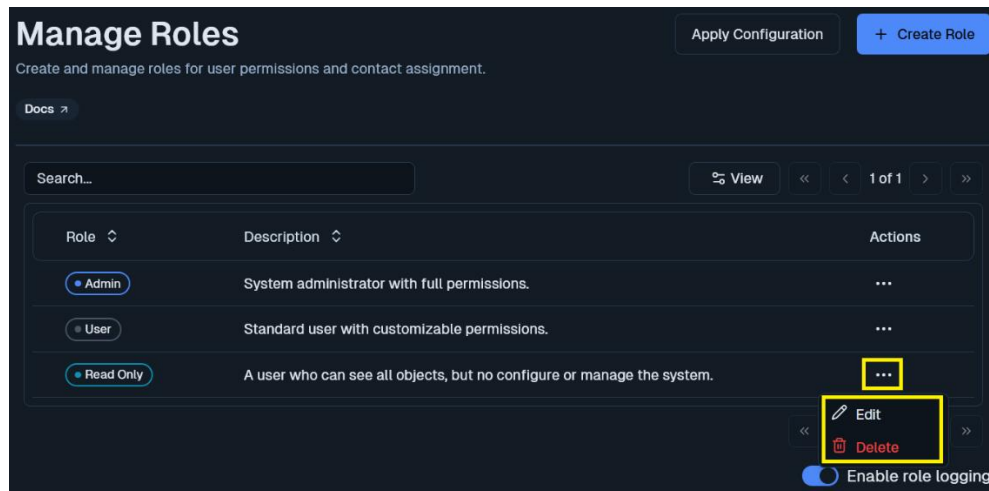
Role	Description	Actions
Admin	System administrator with full permissions.	...
User	Standard user with customizable permissions.	...
Read Only	A user who can see all objects, but not configure them or manage the system.	...

Understanding User Rights And Roles In Nagios XI 2026R2

Editing and Deleting Roles

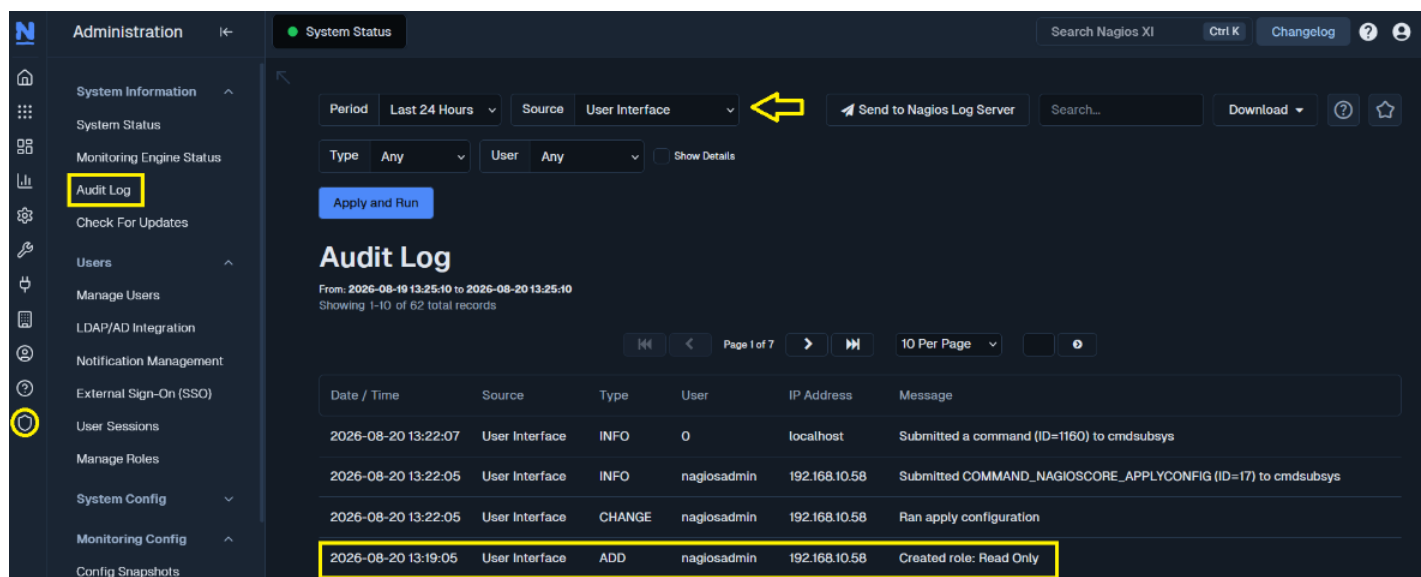
To **Edit** or **Delete** a Role, click the Actions icon to the right of the entry, then select your desired function from the dropdown.

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**.



Understanding User Rights And Roles In Nagios XI 2026R2

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**.

The screenshot displays the Nagios XI web interface's API documentation. The left sidebar contains a 'Help' menu with links to 'API Docs', 'Introduction', 'Objects Reference', 'Config Reference', 'System Reference', 'Common Solutions', 'Developer Docs', 'External Help Resources', and 'Documentation Guides'. The main content area is titled 'API - Objects Reference' and includes a section 'Building Limited Queries' which explains that the API is a read-only backend for getting host, service, and object data. Below this, a table lists various query parameters and their values. The table has three columns: 'Parameter', 'Values', and 'Examples'. The parameters listed are 'pretty', 'starttime', 'endtime', 'records', and 'orderby'. The 'pretty' parameter has a value of '1' and an example showing readable JSON. The 'starttime' and 'endtime' parameters have values like '<timestamp> (Default: -24 hours)' and examples showing how to filter data by time. The 'records' parameter has a value of '<amount>:<starting at>' and an example showing how to filter data by record number. The 'orderby' parameter has a value of '<column>:<a or d>' and an example showing how to sort data by name field and ascending values. The right sidebar lists 'API - Objects Reference' with links to various API endpoints like 'objects/hoststatus', 'objects/servicestatus', 'objects/logentries', 'objects/statehistory', 'objects/comment', 'objects/downtime', 'objects/contact', 'objects/host', 'objects/service', 'objects/hostgroup', 'objects/servicegroup', 'objects/contactgroup', 'objects/timeperiod', 'objects/unconfigured', 'objects/hostgroupmembers', 'objects/servicegroupmembers', 'objects/contactgroupmembers', 'objects/rndexport', 'objects/cpxport', 'objects/hostavailability', 'objects/serviceavailability', 'objects/sla', and 'objects/bpi'.

Parameter	Values	Examples
pretty	1	If the value is 1, the API displays readable JSON. This is helpful when developing and should not be used in a production API call.
starttime	<timestamp> (Default: -24 hours)	objects/statehistory?starttime=1785940968 - Displays the last week of data until now.
endtime	<timestamp> (Default: now)	objects/statehistory?starttime=1785336168&endtime=1785940968 - Displays 1 week of data starting 2 weeks ago. Should be used with starttime.
records	<amount>:<starting at>	objects/hoststatus?records=1 - Displays only the first record. objects/hoststatus?records=10:20 - Displays the next 10 records after the 20th record.
orderby	<column>:<a or d>	objects/hoststatus?orderby=name:a - Displays the items ordered by the name field and ascending values. objects/hoststatus?name=1k:local - Displays any matching name with 'local' anywhere in the string.

You can also refer to this guide for additional details:

[Accessing and Using the Nagios XI REST API](#)

Understanding User Rights And Roles In Nagios XI 2026R2

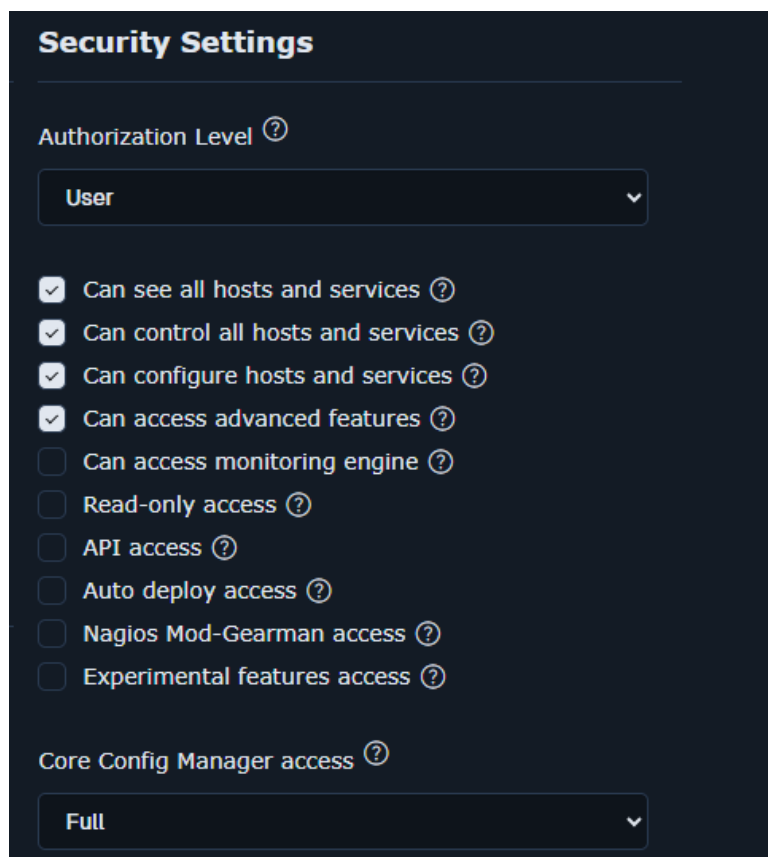
Example User/Role Permissions

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:



The screenshot shows the 'Security Settings' interface for a user role. It features a dark theme with white text. At the top, the title 'Security Settings' is followed by a horizontal line. Below this, the 'Authorization Level' is set to 'User' in a dropdown menu. A list of permissions follows, each with a checkbox and a help icon. The first four permissions are checked: 'Can see all hosts and services', 'Can control all hosts and services', 'Can configure hosts and services', and 'Can access advanced features'. The remaining five are unchecked: 'Can access monitoring engine', 'Read-only access', 'API access', 'Auto deploy access', and 'Nagios Mod-Gearman access'. Below the list, 'Core Config Manager access' is set to 'Full' in a dropdown menu.

Security Settings

Authorization Level [?]

User [?]

- ☒ Can see all hosts and services [?]
- ☒ Can control all hosts and services [?]
- ☒ Can configure hosts and services [?]
- ☒ Can access advanced features [?]
- ☐ Can access monitoring engine [?]
- ☐ Read-only access [?]
- ☐ API access [?]
- ☐ Auto deploy access [?]
- ☐ Nagios Mod-Gearman access [?]
- ☐ Experimental features access [?]

Core Config Manager access [?]

Full [?]

Understanding User Rights And Roles In Nagios XI 2026R2

A Role reflecting the above permissions would look like this:

Monitoring Permissions

Can see all hosts and services
Allows users to view all host and services that are applied in the system.

☒

Can configure hosts and services
Allows users to run Configuration Wizards, host/service reconfiguration, and deletion of hosts and services.

☒

Can control all hosts and services
Allows users to run commands on all hosts and services. These are commands that can be run on the Nagios command file.

☒

Can access monitoring engine
Allows users to access the Monitoring Process section in the main page.

☐

Security Permissions

Read-Only User
Restricts users to read-only access.

☐

Advanced User
Allows the editing of check commands in the re-configure host/service page. Shows advanced tab and commands in host/service detail pages. Allows setting host parents during wizards and re-configure on host detail page.

☒

Core Configuration Manager Access
Allow users to view and access the CCM.

Full Access

Global Dashboard Access
Allow users to view and access Global Dashboards.

No Access

Understanding User Rights And Roles In Nagios XI 2026R2

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.

Individual User Settings

Security Settings

Authorization Level [?](#)

None

☒ Can see all hosts and services [?](#)

☐ Can control all hosts and services [?](#)

☐ Can configure hosts and services [?](#)

☐ Can access advanced features [?](#)

☐ Can access monitoring engine [?](#)

☒ Read-only access [?](#)

☐ API access [?](#)

☐ Auto deploy access [?](#)

☐ Nagios Mod-Gearman access [?](#)

☐ Experimental features access [?](#)

Core Config Manager access [?](#)

None

Role Settings

Monitoring Permissions

Can see all hosts and services
Allows users to view all host and services that are applied in the system. ☒

Can configure hosts and services
Allows users to run Configuration Wizards, host/service reconfiguration, and deletion of hosts and services. ☐

Can control all hosts and services
Allows users to run commands on all hosts and services. These are commands that can be run on the Nagios command file. ☐

Can access monitoring engine
Allows users to access the Monitoring Process section in the main page. ☐

Security Permissions

Read-Only User
Restricts users to read-only access. ☒

Advanced User
Allows the editing of check commands in the re-configure host/service page. Shows advanced tab and commands in host/service detail pages. Allows setting host parents during wizards and re-configure on host detail page. ☐

Understanding Upgrading From Pre-2026R2 Versions

This section outlines the implications 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.

Understanding User Rights And Roles In Nagios XI 2026R2

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](#)