

# How To Understand User Rights in Nagios XI 2024

## Purpose

This document describes Nagios XI user rights or permissions and how to effectively manage permissions to ensure security and obtain a web interface tailored to various individuals' needs.

## Target Audience

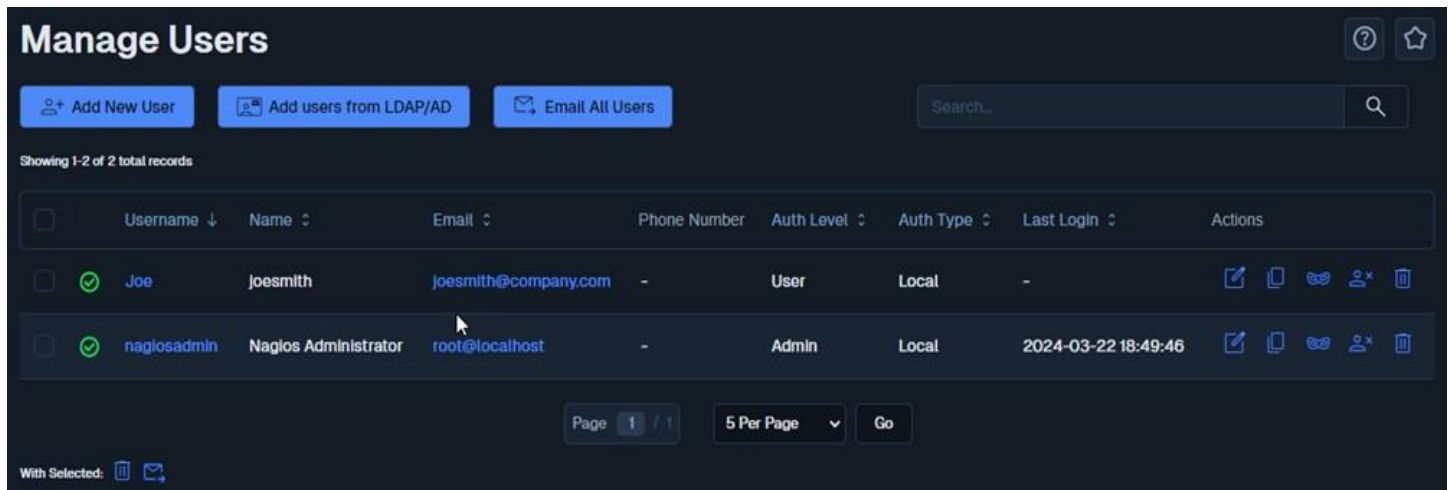
This document is intended for use by Nagios XI administrators.

## Additional Resources

In addition to this document, Nagios XI administrators should also familiarize themselves with the [Nagios XI Multi-Tenancy](#) documentation.

This document provides supporting information that will help you understand default user rights and permissions in Nagios XI.

## Managing Permissions



The screenshot displays the 'Manage Users' interface in Nagios XI. At the top, there are three buttons: 'Add New User', 'Add users from LDAP/AD', and 'Email All Users'. A search bar is located on the right. Below the buttons, it indicates 'Showing 1-2 of 2 total records'. The main content is a table with the following columns: Username, Name, Email, Phone Number, Auth Level, Auth Type, Last Login, and Actions. The table contains two rows of user data:

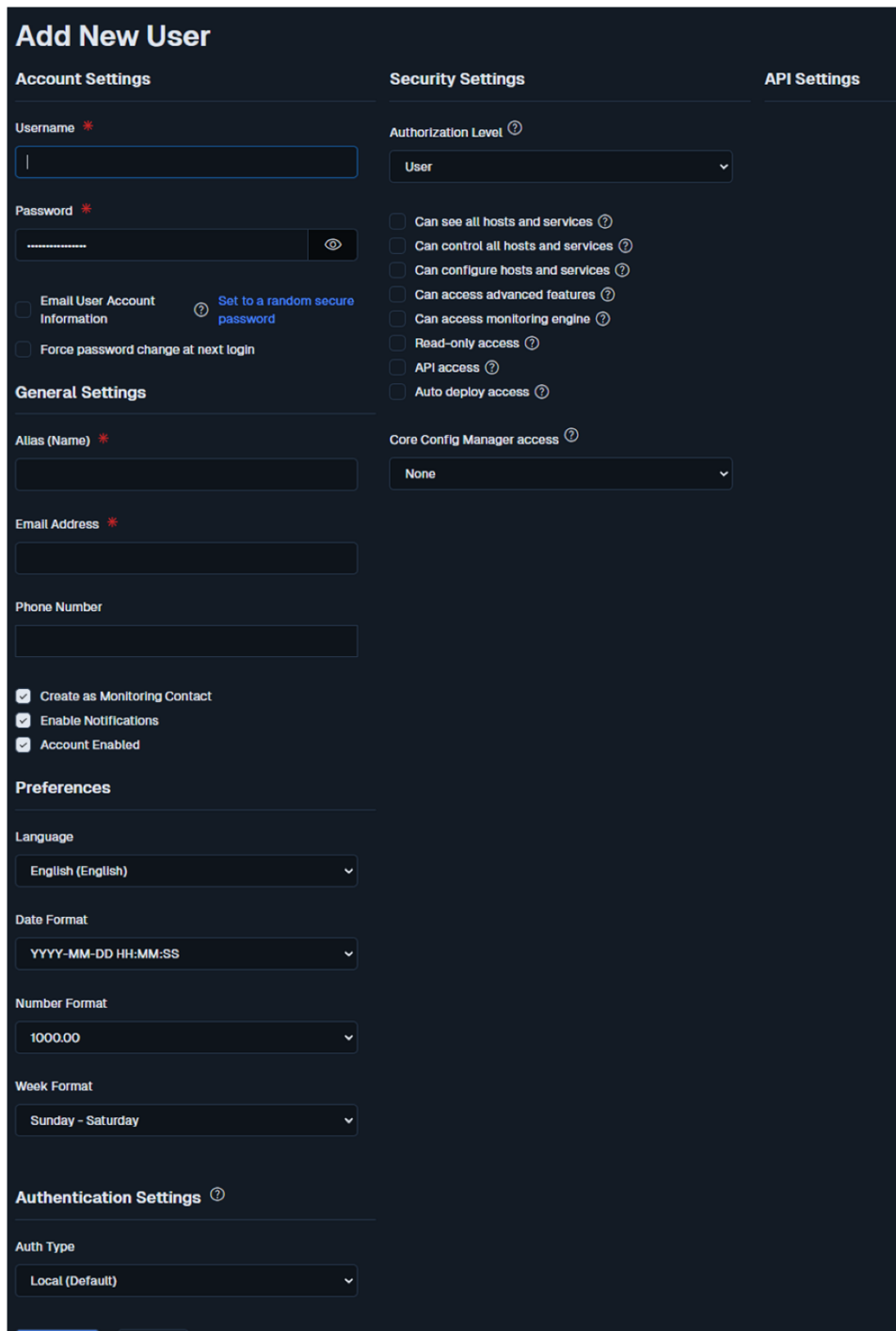
Username	Name	Email	Phone Number	Auth Level	Auth Type	Last Login	Actions
Joe	joesmith	joesmith@company.com	-	User	Local	-	[Edit] [Copy] [Refresh] [Add] [Delete]
nagiosadmin	Nagios Administrator	root@localhost	-	Admin	Local	2024-03-22 18:49:46	[Edit] [Copy] [Refresh] [Add] [Delete]

At the bottom of the table, there are pagination controls: 'Page 1 / 1', '5 Per Page', and 'Go'. Below the table, there is a section for 'With Selected:' with icons for deleting and emailing.

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.

# How To Understand User Rights in Nagios XI 2024

1. Navigate to **Admin > Users > Manage Users** to access this page.



## Add New User

**Account Settings**

Username \*

Password \*

Email User Account Information Set to a random secure password

Force password change at next login

**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 ⓘ

**API Settings**

Core Config Manager access ⓘ  
None

**General Settings**

Alias (Name) \*

Email Address \*

Phone Number

Create as Monitoring Contact

Enable Notifications

Account Enabled

**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)

# How To Understand User Rights in Nagios XI 2024

2. To create a new user, click the **Add New User** button.
  - a. To edit an existing user, click the **edit**  icon for the user you want to edit.
3. 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 access is validated against the contact when using Nagios XI.
4. Permissions are determined by the options selected in the **Security Settings** section of the **Add/Edit User** screen.
5. The default selection under **Authorization Level** is User. This permission is the most restrictive permission in Nagios XI.
6. 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).

## Administrator Privileges

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**

By default, the Rest API access option is not enabled when selecting Admin, this is explained in the [Nagios XI API section](#) of this documentation.

# How To Understand User Rights in Nagios XI 2024

## User Security Settings

There are various levels of security settings available to grant to users depending on what their requirements are. A description of each individual security setting option is given in the table below.

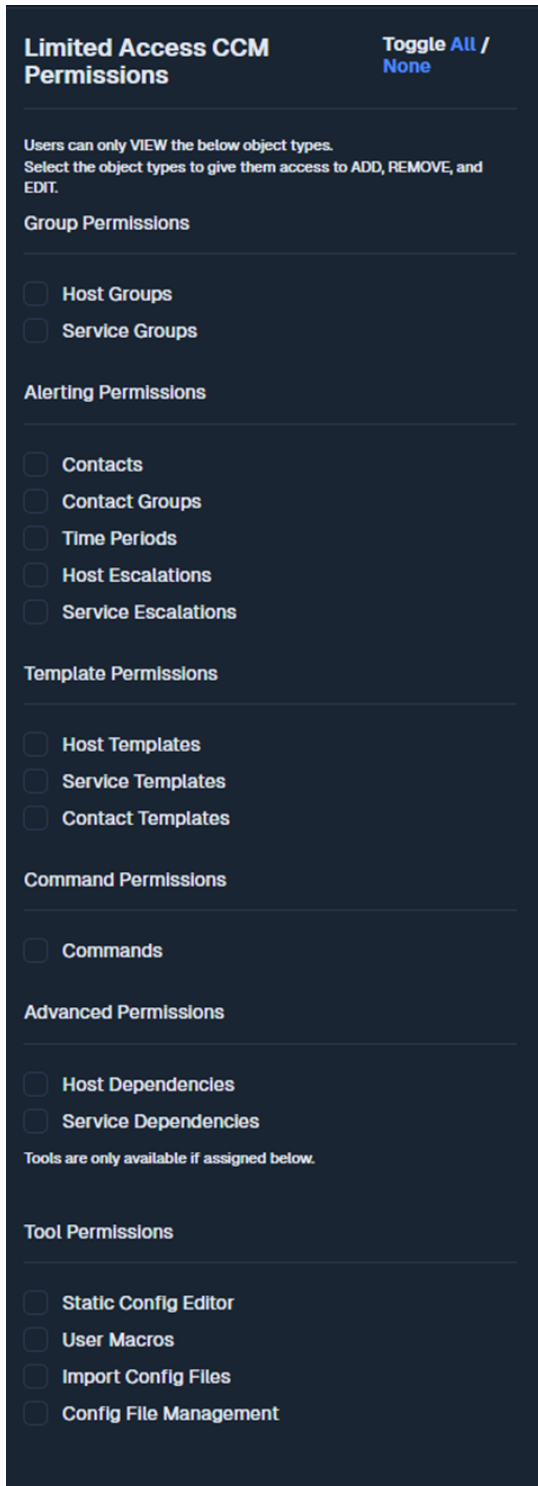
Setting	What It Means
<b>Can see all objects</b>	The user can see all hosts and services that are being monitored – not just the ones they are a direct or indirect notification contact.
<b>Can control hosts and services</b>	The user can: Acknowledge problems Schedule downtime Toggle notifications Force checks on all objects
<b>Can configure hosts and services</b>	The user can: Run Configuration Wizards Delete from detail page Re-configure from detail page
<b>Can access advanced features</b>	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

# How To Understand User Rights in Nagios XI 2024

<b>Can access monitoring engine</b>	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
-------------------------------------	--

Setting	What It Means
<b>Read-only access</b>	This option restricts the user to a read only role and overwrites other options preceding it
<b>REST API access</b>	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 <a href="#">Nagios XI API</a> section in this document.
<b>Configuration Manager access</b>	User access to Configuration Manager depending on:  None = No access, Configuration Manager is not visible to the user  Login = Can view Configuration Manager links and can 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

# How To Understand User Rights in Nagios XI 2024



**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

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

You can see that 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.

# How To Understand User Rights in Nagios XI 2024

## Nagios XI API

The Nagios XI API was introduced in XI 5. It is a REST API that includes far more features and control over the Nagios XI system. The 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 the REST API Access setting is selected. They will only have access to the Objects API endpoint and the relevant documentation
- Admin users have full access to the API if the REST API Access setting is selected
- Access to the documentation 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 > REST API Docs**.

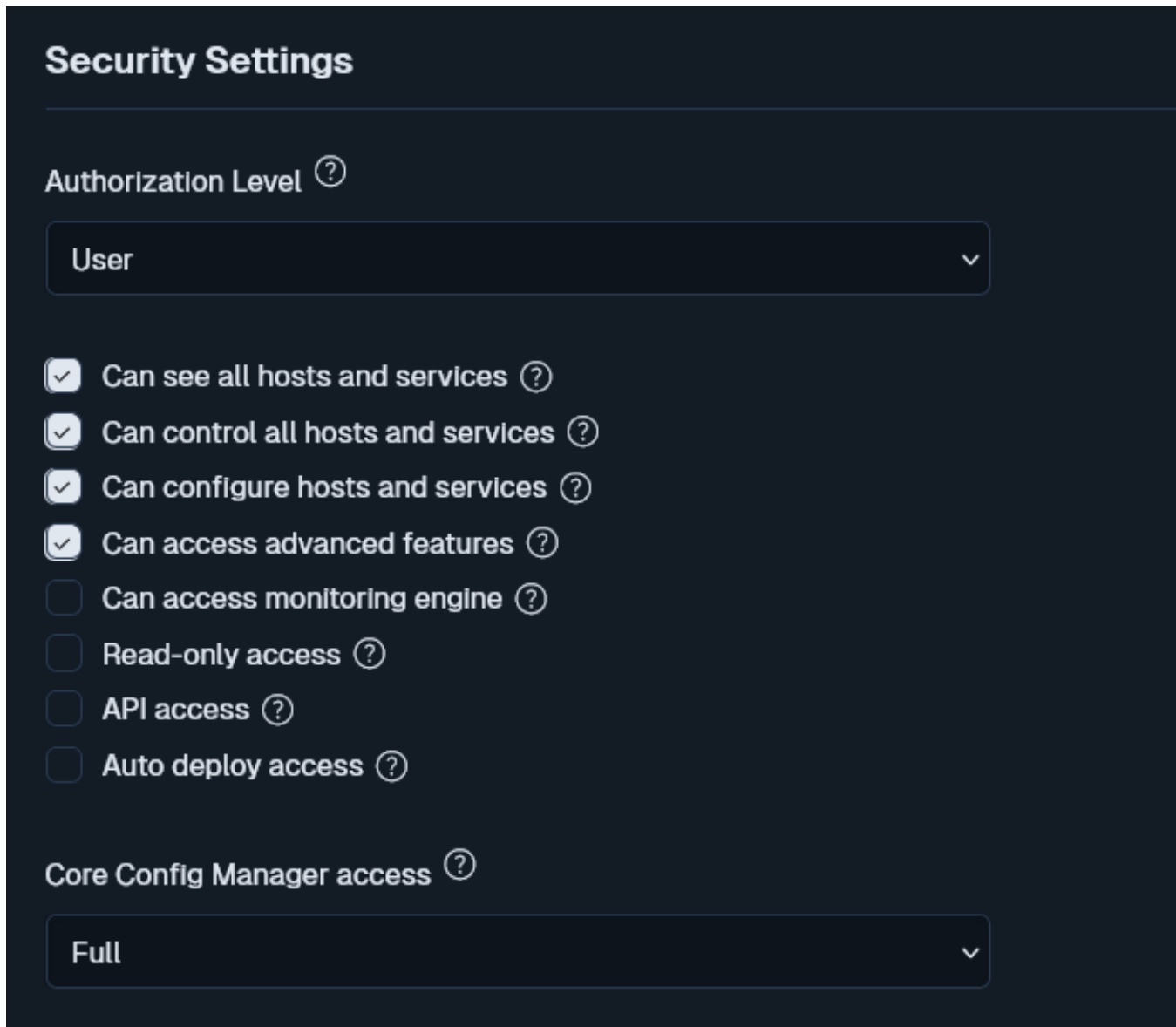
The screenshot shows the 'API - Objects Reference' page in the Nagios XI web interface. The page title is 'API - Objects Reference' and it includes a sub-section 'Building Limited Queries'. Below this, there is a table with columns 'Parameter', 'Values', and 'Examples'. The table lists parameters like 'pretty', 'starttime', 'endtime', 'records', and 'orderby' with their respective values and example API calls. A sidebar on the right contains a list of API endpoints under 'Basic Objects', 'Unconfigured Objects', 'Group Members', and 'Data Exporting'.

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=1740088334 - Displays the last week of data until now.
endtime	<timestamp> (Default: now)	objects/statehistory?starttime=1739483534&endtime=1740088334 - 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.

# How To Understand User Rights in Nagios XI 2024

## Example User Privileges

### Advanced User with Change Control



The screenshot shows the 'Security Settings' interface for a user. It features a dark blue background with white text. At the top, the title 'Security Settings' is displayed. Below it, the 'Authorization Level' is set to 'User'. A list of permissions follows, with checkboxes indicating which are enabled. The 'Core Config Manager access' is set to 'Full'.

**Security Settings**

Authorization Level <sup>?</sup>

User ▼

- Can see all hosts and services <sup>?</sup>
- Can control all hosts and services <sup>?</sup>
- Can configure hosts and services <sup>?</sup>
- Can access advanced features <sup>?</sup>
- Can access monitoring engine <sup>?</sup>
- Read-only access <sup>?</sup>
- API access <sup>?</sup>
- Auto deploy access <sup>?</sup>

Core Config Manager access <sup>?</sup>

Full ▼

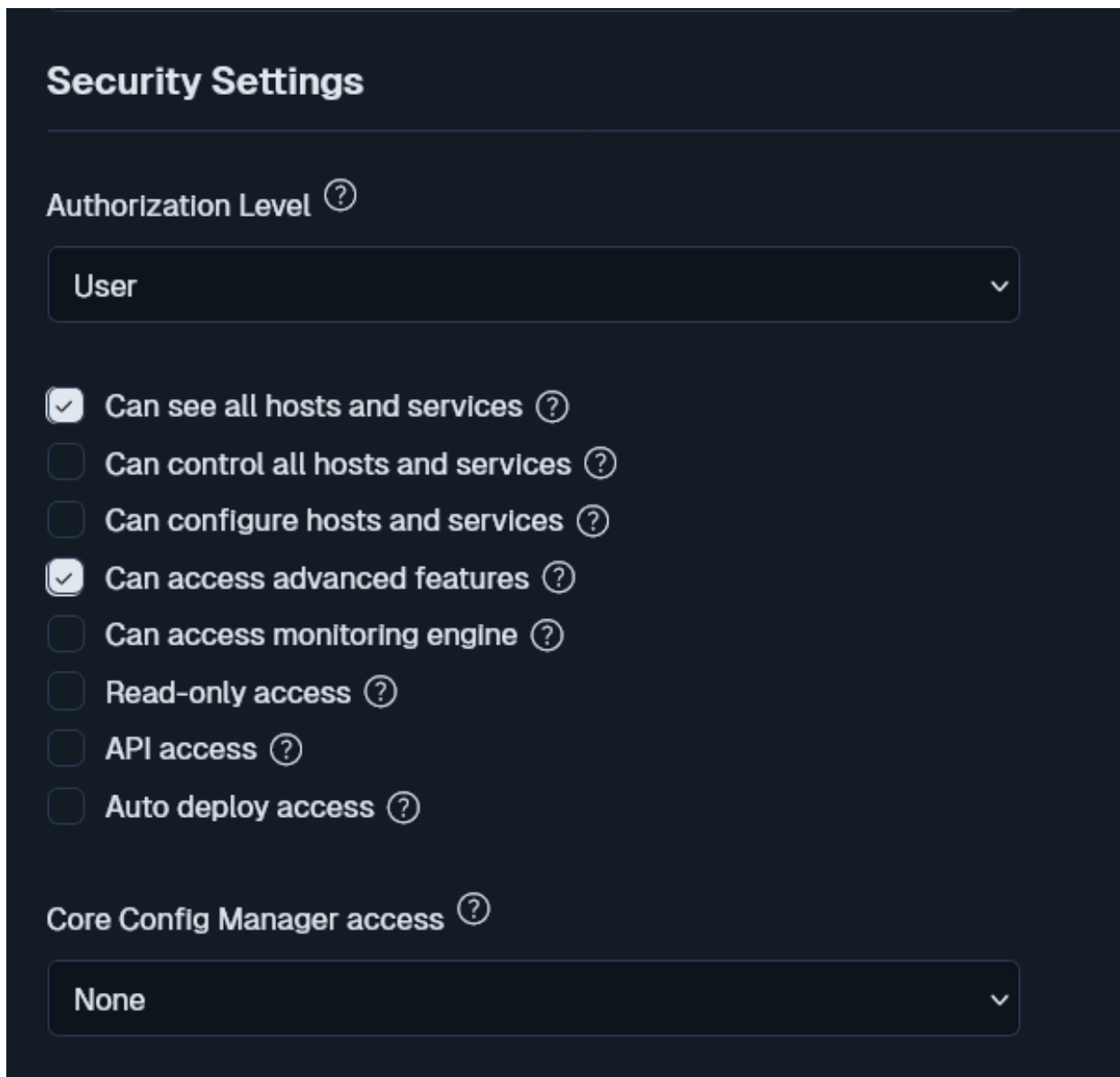
Common settings for an advanced user who should have rights to see, control, and re-configure all existing hosts and services that are being monitored, as well as add new hosts and services to the monitoring configuration is shown in the image to the right.



# How To Understand User Rights in Nagios XI 2024

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 **Configuration Manager** to manage object configurations.

## Basic Read-Only User



The screenshot shows the 'Security Settings' interface for a user. It features a dark blue background with white text. At the top, the title 'Security Settings' is displayed. Below it, the 'Authorization Level' is set to 'User'. A list of permissions follows, with checkboxes indicating which are active. The 'Core Config Manager access' is set to 'None'.

**Security Settings**

Authorization Level <sup>?</sup>

User ▼

- Can see all hosts and services <sup>?</sup>
- Can control all hosts and services <sup>?</sup>
- Can configure hosts and services <sup>?</sup>
- Can access advanced features <sup>?</sup>
- Can access monitoring engine <sup>?</sup>
- Read-only access <sup>?</sup>
- API access <sup>?</sup>
- Auto deploy access <sup>?</sup>

Core Config Manager access <sup>?</sup>

None ▼

# How To Understand User Rights in Nagios XI 2024

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 in the image above.

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.

## Finishing Up

This completes the documentation on understanding user rights. If you have additional questions or other support-related questions, please visit us at our Nagios Support Forum, Nagios Knowledge Base, or Nagios Library:

[Visit Nagios Support Forum](#)

[Visit Nagios Knowledge Base](#)

[Visit Nagios Library](#)