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.

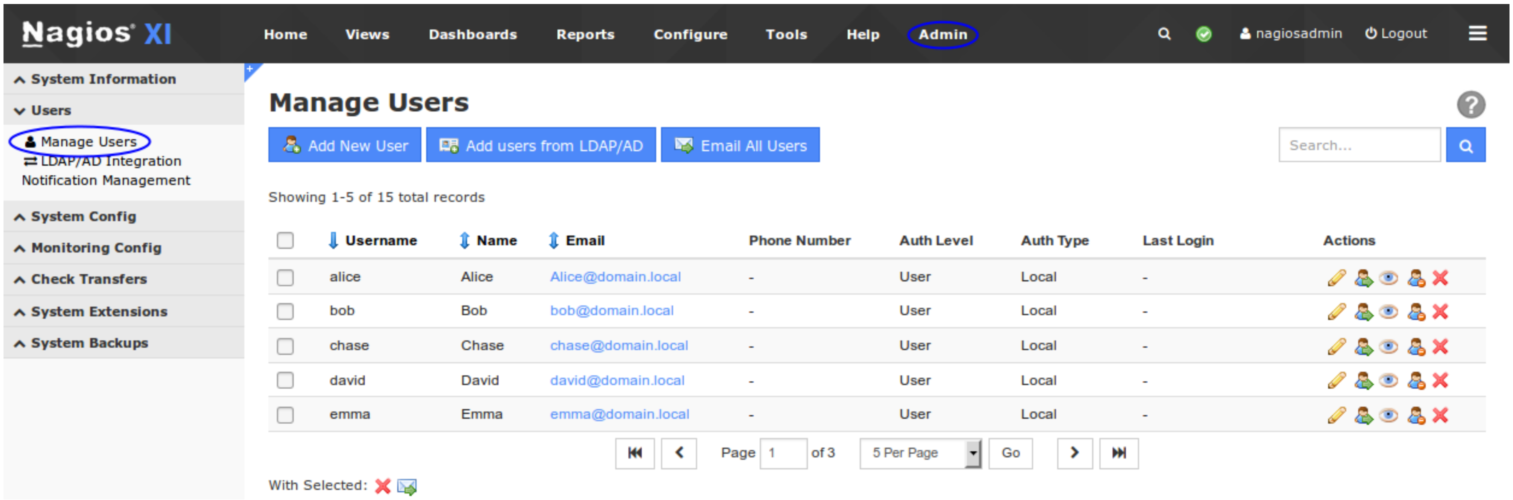
Additional Resources

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 may be helpful in understanding default user rights and permissions in Nagios XI.

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

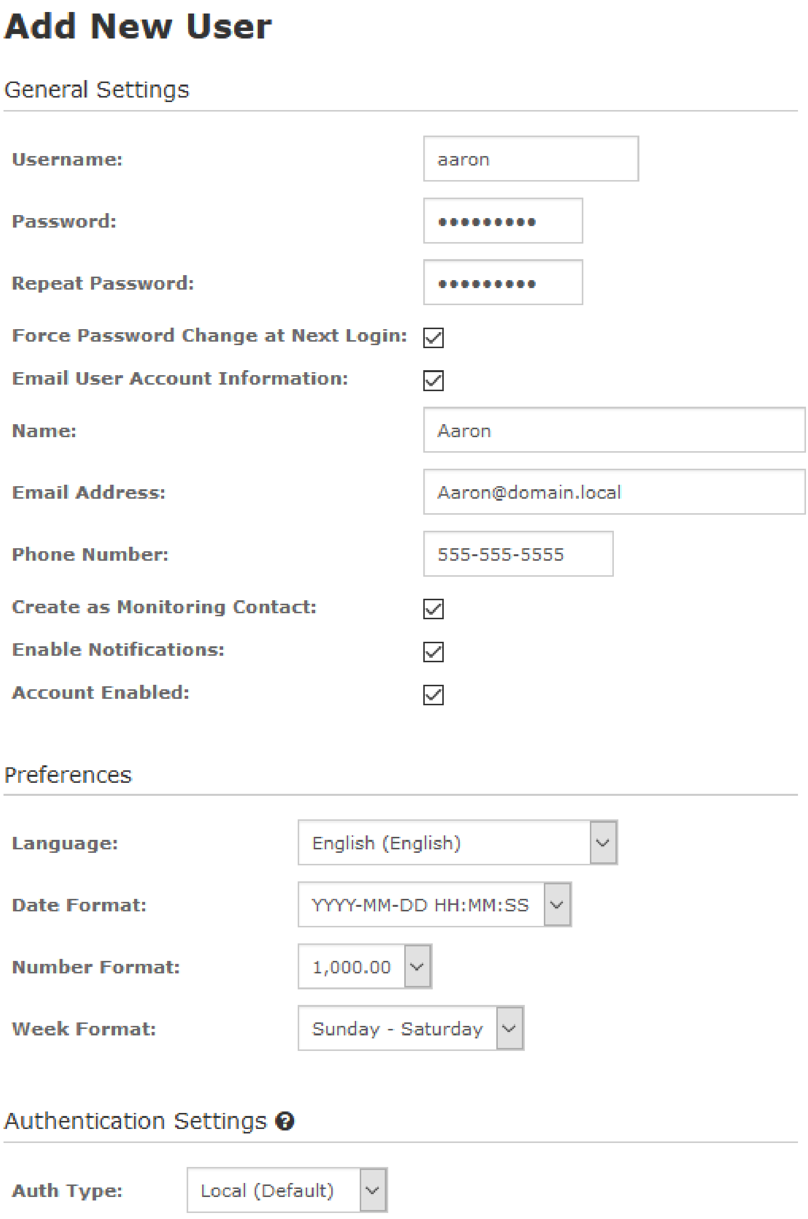


Showing 1-5 of 15 total records

	Username	Name	Email	Phone Number	Auth Level	Auth Type	Last Login	Actions
□	alice	Alice	Alice@domain.local	-	User	Local	-	
□	bob	Bob	bob@domain.local	-	User	Local	-	
□	chase	Chase	chase@domain.local	-	User	Local	-	
□	david	David	david@domain.local	-	User	Local	-	
□	emma	Emma	emma@domain.local	-	User	Local	-	

To create a new user click the **Add New User** button. To edit an existing user click the edit ✎ icon for the user you want to edit.

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.



Add New User

General Settings

Username:	aaron
Password:	•••••••••
Repeat Password:	•••••••••
Force Password Change at Next Login:	☑
Email User Account Information:	☑
Name:	Aaron
Email Address:	Aaron@domain.local
Phone Number:	555-555-5555
Create as Monitoring Contact:	☑
Enable Notifications:	☑
Account Enabled:	☑

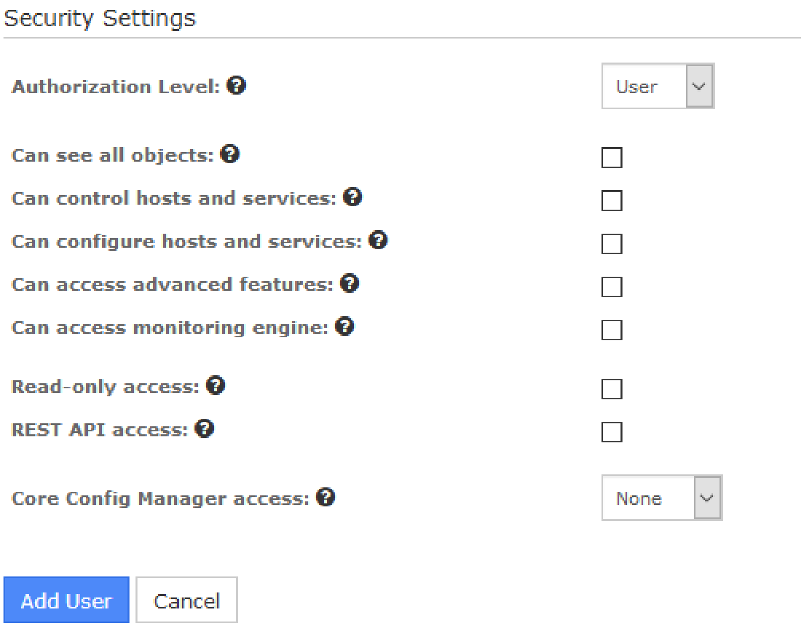
Preferences

Language:	English (English)
Date Format:	YYYY-MM-DD HH:MM:SS
Number Format:	1,000.00
Week Format:	Sunday - Saturday

Authentication Settings ?

Auth Type:	Local (Default)

Permissions are determined by the options selected in the **Security Settings** section of the Add/Edit User screen.



Security Settings

Authorization Level: User

Can see all objects: □

Can control hosts and services: □

Can configure hosts and services: □

Can access advanced features: □

Can access monitoring engine: □

Read-only access: □

REST API access: □

Core Config Manager access: None

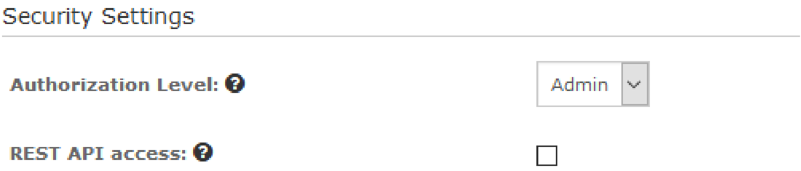
The default selection under **Authorization Level** is **User**. This permission is the most restrictive permission in Nagios XI.

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



Security Settings

Authorization Level: Admin

REST API access: □

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.

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.

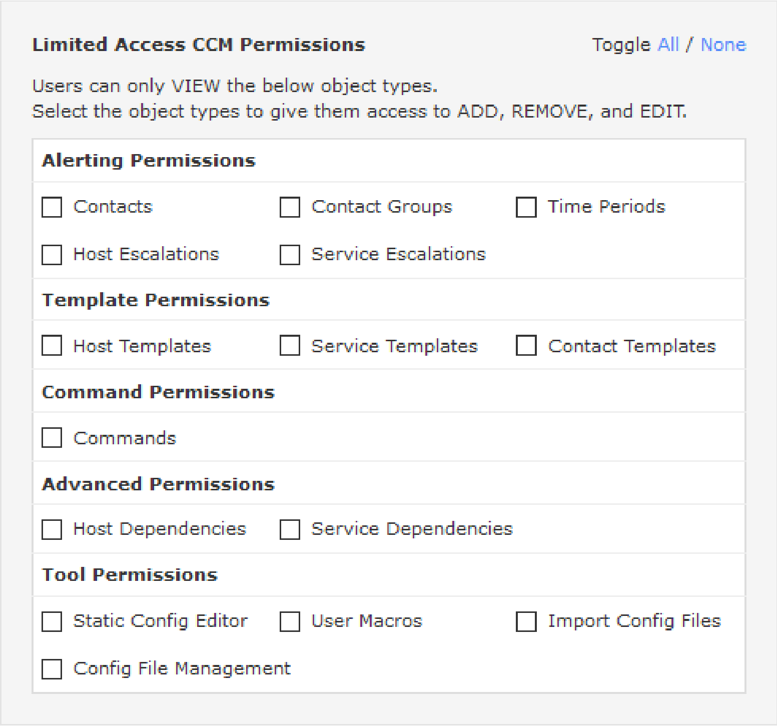
Setting	What It Means
Can see all objects	The user can see all hosts and services that are being monitored – not just the ones they are a direct or indirect notification contact.
Can control hosts and services	The user can: Acknowledge problems Schedule downtime Toggle notifications Force checks on all 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	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

Setting	What It Means
Read-only access	This option restricts the user to a read only role and overwrites other options preceding it
REST 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.
Core Config Manager access	User access to Core Config Manager (CCM) depending on: **None** = No access, CCM is not visible to the user **Login** = Can view CCM links and can login with a CCM user account **Limited** = Allows integrated CCM access, they only have access to the objects their contact has been granted to however higher permission can be granted (see below) **Full** = Full CCM access with no Admin features

The screenshot to the right shows the table that will appear the the **Limited** option is selected for Core 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.



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.

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

Tool Permissions

□ Static Config Editor □ User Macros □ Import Config Files
□ Config File Management

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, access is outlined as follows:

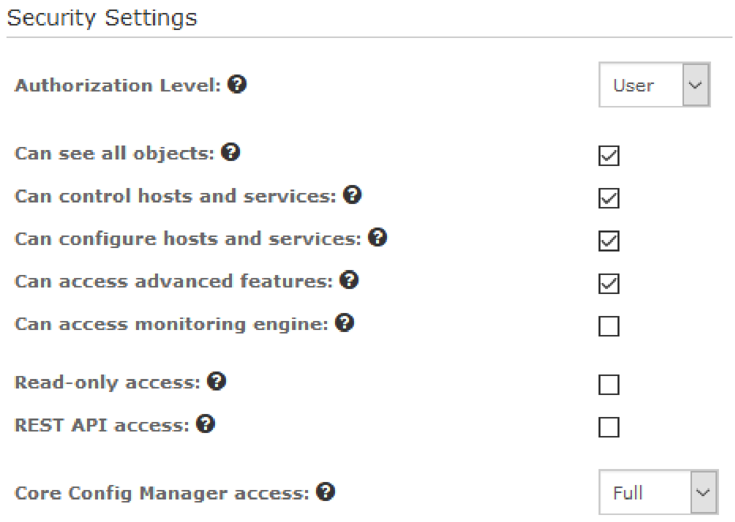
- Normal users are allowed to have **read** access if the **REST API Access** setting is selected
  - They will only have access to the **Objects** API endpoint and the relevant documentation
- Admin users have **full** access to the API if the **REST API Access** setting is selected
- Access to the documentation is restricted to users who have API access

Detailed information on how to use the API can be found under **Help** > **REST API Docs**.

Example User Privileges

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 the image to the right.



Security Settings

Authorization Level: User

Can see all objects: ☑

Can control hosts and services: ☑

Can configure hosts and services: ☑

Can access advanced features: ☑

Can access monitoring engine: □

Read-only access: □

REST API access: □

Core Config Manager access: Full

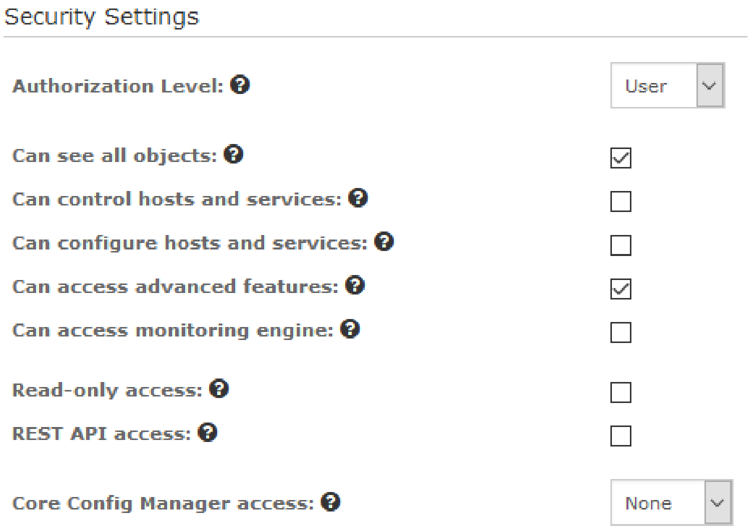
A user with these settings will have access to advanced information and commands relating to hosts and services that are being monitored, but will not have access to control (shutdown, start, etc) the monitoring engine.

This user will also have the ability to use CCM to manage object configurations.

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 in the image to the right.

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.



Security Settings

Authorization Level:	User
Can see all objects:	☑
Can control hosts and services:	□
Can configure hosts and services:	□
Can access advanced features:	☑
Can access monitoring engine:	□
Read-only access:	□
REST API access:	□
Core Config Manager access:	None

Finishing Up

This completes the documentation on understanding Nagios XI user rights.

If you have additional questions or other support related questions, please visit us at our Nagios Support Forums:

https://support.nagios.com/forum

The Nagios Support Knowledgebase is also a great support resource:

https://support.nagios.com/kb