How To Manage Users and Roles in Nagios Network Analyzer 2026

Purpose

This document describes how to manage users in Nagios Network Analyzer 2026. It covers both individual user management, as well as providing details on defining Roles for templated access control.
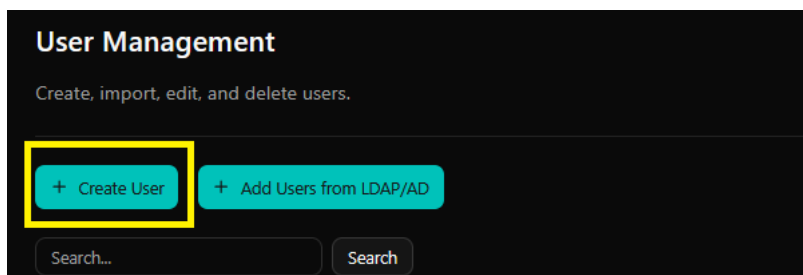
User Management

To manage users, navigate to **Administration > User Management**.

The **User Management** page allows administrators to create new users and edit or delete existing users.
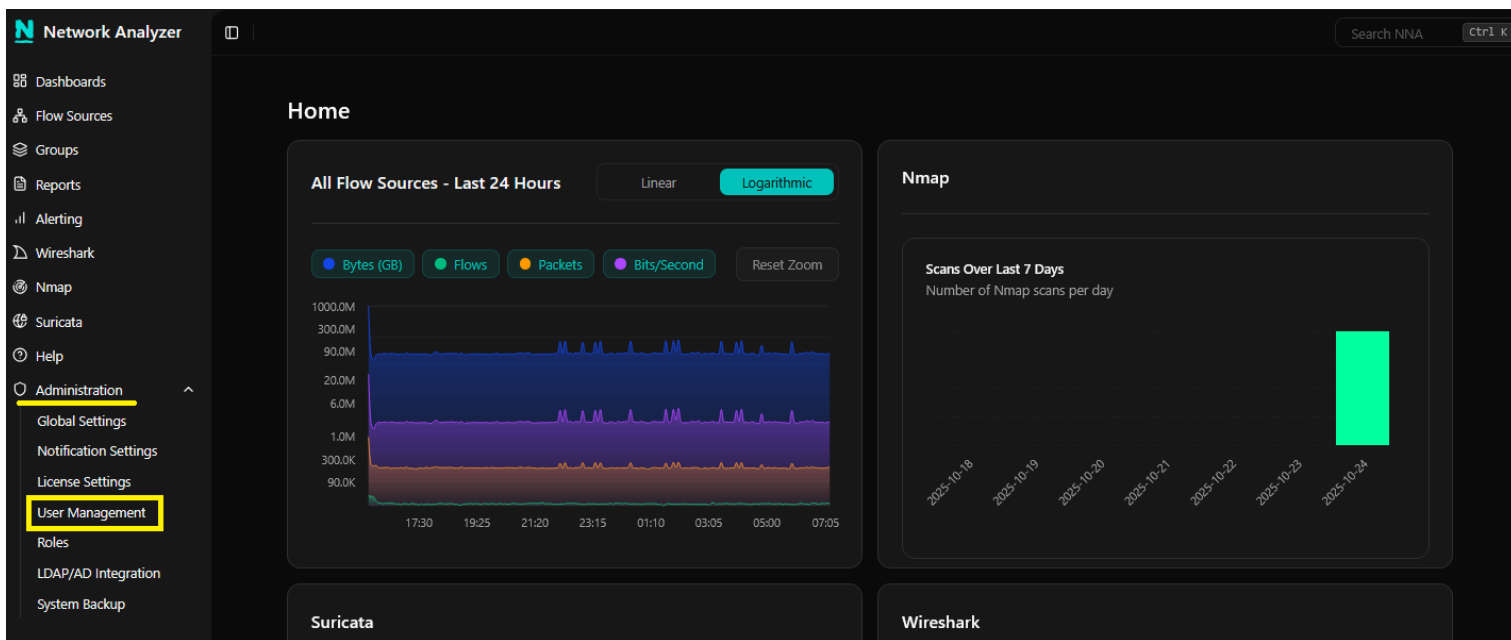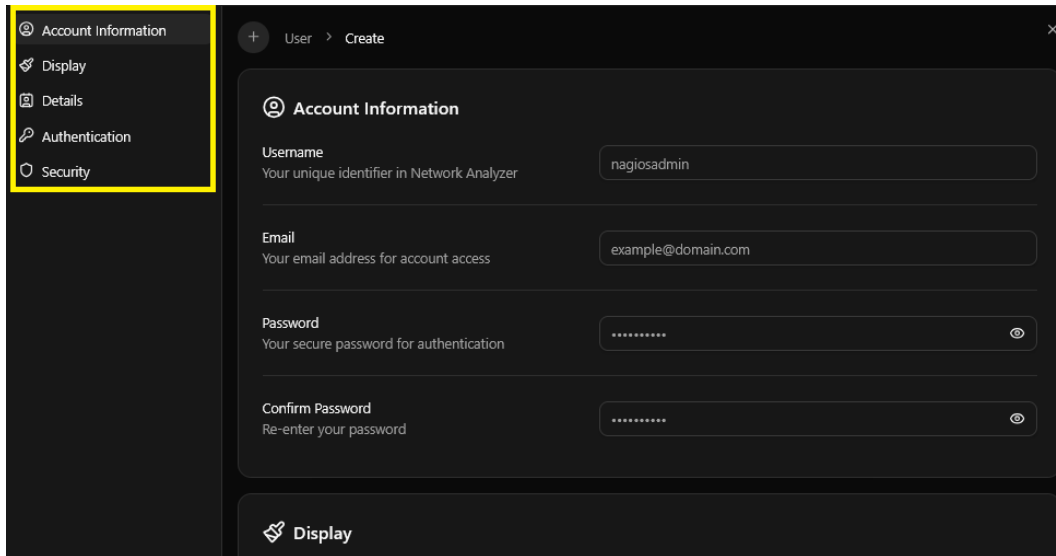

Creating a User

To create a new user from scratch, click the **+Create User** button.

Nagios®

You will be presented with a list of fields to populate for creating a new user, divided into several sections.

Account Information

In this section, you must define your user's Username, Email, and Password.

Display

Here, you can customize your user's Language and User Theme.

Details

Here, you can optionally enter a Full Name, Company, and Phone Number for your user.

Authentication

Nagios Network Analyzer allows you to use external authentication sources such as LDAP and Active Directory (AD):

- The **Local** option is selected by default
- For LDAP / AD options please refer to the External Authentication section of this document
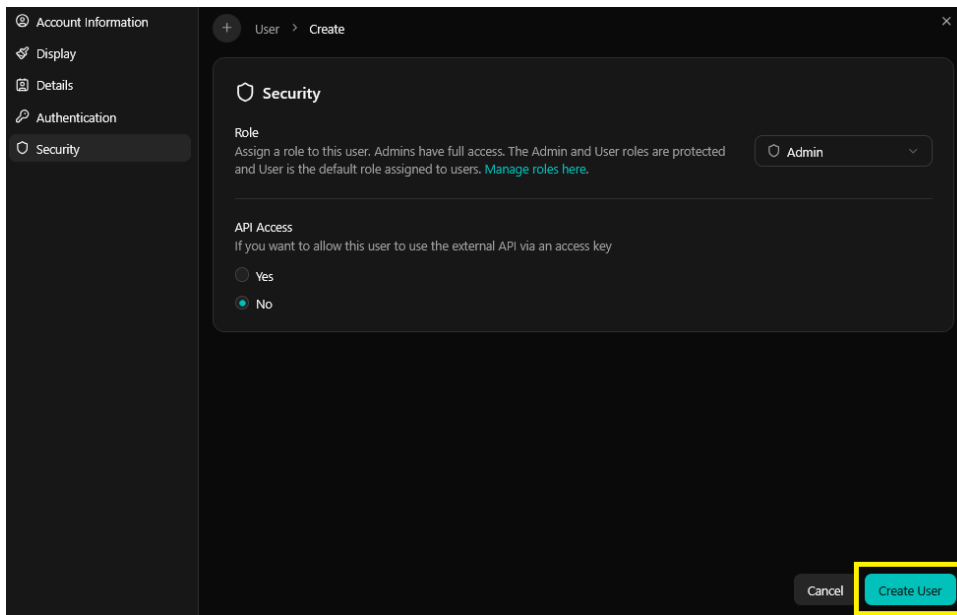
Security

In this section, you can choose a Role for your user (or keep the automatically selected User default), and decide whether they should have API access.

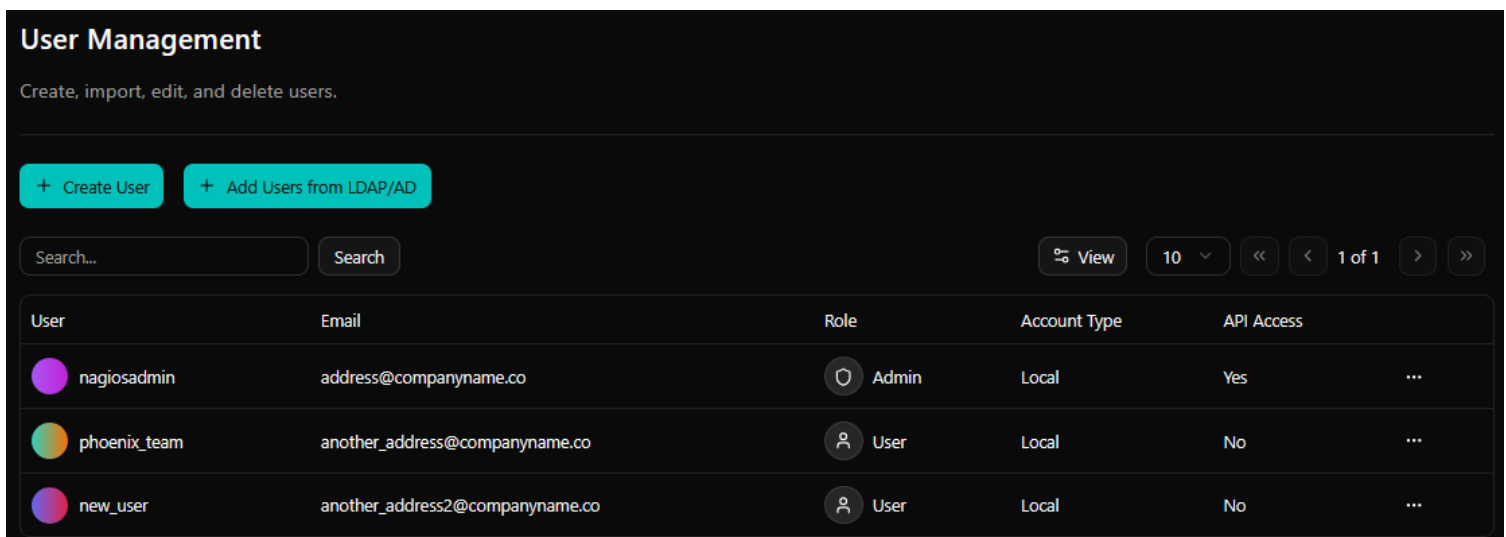You can refer to the Roles section of this document to learn more about managing this feature.

Nagios®

Click the **Create User** button once you have finished customizing the sections.

The **User Management** page will now display your newly-created user:

Editing a User

To edit an existing user, click the **Actions** icon (three dots on the right), then choose **Edit**.

This will open a menu like the **Create User** page explained in the previous section.

Click the **Update User** button to save your changes:

Deleting a User

To delete an existing user, click the **Delete** link in the **Actions** dropdown.

Managing Roles

Roles enable you to template user access settings related to flow Sources and Groups, Wireshark, Nmap, and Suricata so that they can be quickly applied to new and existing users.

To access Roles, navigate to **Administration > Roles**:

Admin and User Roles

Two key Roles are pre-defined in Network Analyzer:

Admin

This is the superadmin Role, with access to view, create, edit, and delete all feature and integration functions, as well as visibility of and control over all of the sections and functions of the **Administration** menu.

This Role cannot be edited or deleted.

NAGIOS®

User

This Role cannot be deleted, but can be edited as needed to fit your unique requirements. It serves as your default Role in several key respects:

- When new users are created, this Role is assigned by default in the Security section of the Create User dialog.
- When new Roles are created, the default form values are automatically filled based on these settings.
- In the event that the Role assigned to a user is deleted, this role will be automatically assigned to them.

The initial settings for this Role on a fresh installation of Network Analyzer provide a full visibility read-only user. The user will be able to see data from flow Sources and integrations, but cannot control Sources or do things like starting Wireshark, Nmap, and Suricata scans, or manage things like the Wireshark Ring Buffer, Nmap Profiles, or the Suricata Data Config.
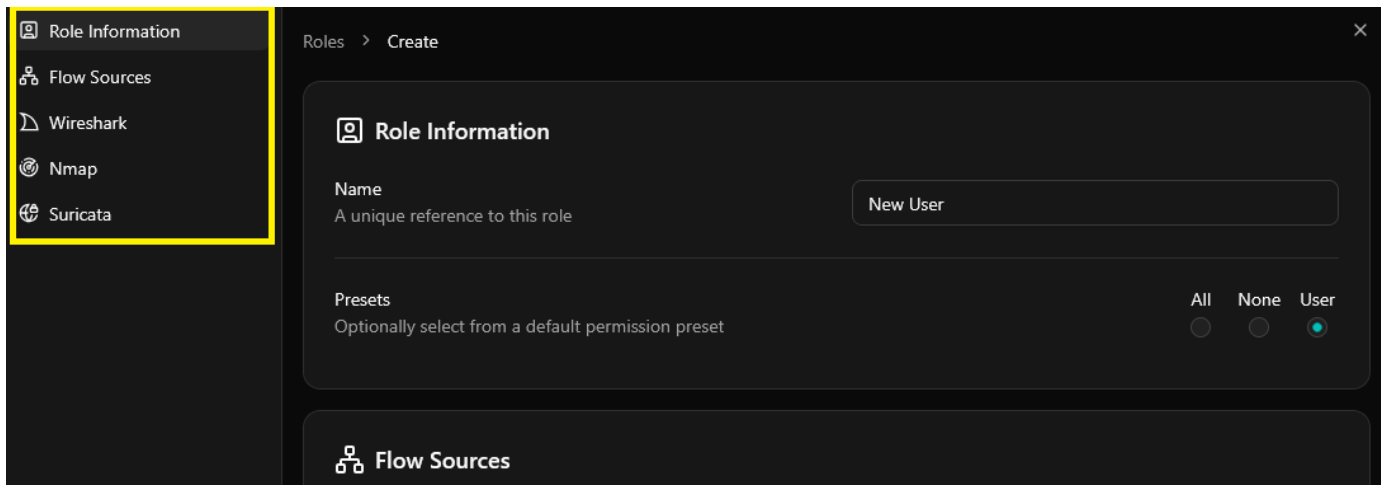
Creating a New Role

To create a new Role, click the **+New Role** button.

NAGIOS®

Here you will see several sections of options to customize:

Each option of each section includes details on the purpose of the setting, along with checkboxes which can be used to determine the Role's view, create, edit, delete, or other (depending on the specific function) privileges. For example, here are the Nmap scans options:

Role Information

In this section, define a Name for the Role, and optionally choose a Preset. The Preset you choose will either pre-select All of the section checkboxes, None of the section checkboxes, or the settings defined in the User Role. By default, **User** is automatically selected.

Flow Sources

In this section, you'll determine the level of visibility and control the Role has of flow data Sources and Groups.

Wireshark

Here, you'll determine whether the Role can access and manage Wireshark PCAP files, start and stop captures, and manage the Ring Buffer.

Nmap

In this section, you'll decide the Role's visibility and control over Nmap scans, Profiles, and Ndiffs.

Suricata

Here you'll set the Role's level of access to Suricata Rules and Rulesets, Data, Alerts, Scans, and whether the Role can scan PCAPs.

Once you've chosen your settings in each section, click the **Submit** button on the bottom right to create your Role.

Your new Role will now be present in the **Role** dropdown in the **Security** section of the Create/Edit User dialog in **Administration > User Management:**
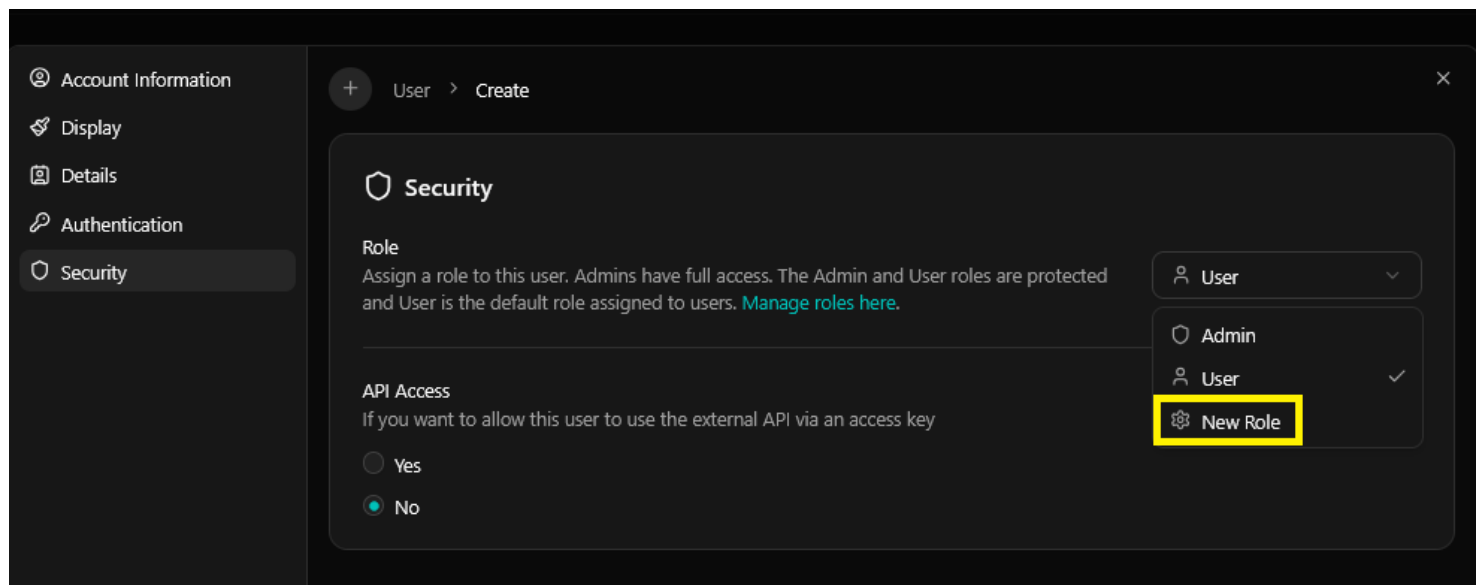
Nagios®

Editing and Deleting Roles

To edit or delete an existing role, choose the corresponding option from the **Actions** dropdown:

External Authentication

Nagios Network Analyzer allows you to use external authentication sources such as Lightweight Directory Access Protocol (LDAP) or Active Directory (AD). Please refer to the following documentation for more information:

[Authenticating and Importing Users with AD and LDAP](#)

Finishing Up

This completes the documentation on how to manage users in Nagios Network Analyzer. 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](#)