SOLARWINDS TECH TIPS

How to Configure Alerts on SolarWinds IP Address Manager 4.3

Share:

solarwinds
Unexpected Simplicity™

Why is IP address alerting important?

A typical network comprises multiple network devices, servers, and user devices, which all need an IP address to function. With the number of devices increasing from tens to hundreds to thousands, administrators need to adopt a more proactive approach to monitoring and fixing network issues. Alerting plays a key role in reducing network downtime caused by IP-related issues. Administrators use alerts to proactively manage their IP address space. They do this by creating alerts triggered by specific conditions that can be sent via email or text message, saved as log files, and more. Quick-view dashboards that display relevant and real-time information also help admins quickly identify and troubleshoot IP issues.

Key benefits of using alerts

Alerts help reduce network downtime by notifying you of issues before they become real problems. Sometimes easily identifiable IP-related problems can cause network issues. Having access to timely alerts and relevant real-time information helps you avoid issues caused by:

- Duplicate IP addresses.
- IP address status changes not updated to DHCP and DNS servers.
- DHCP scope overlaps.
- Over- or under-provisioning IP addresses and DHCP scope and split scope address depletion.
- Errors created during DNS record creation.

The complexity of today's networks requires tools that help spot IP-related problems. SolarWinds® IP Address Manager (IPAM) provides you with the flexibility to monitor the following:

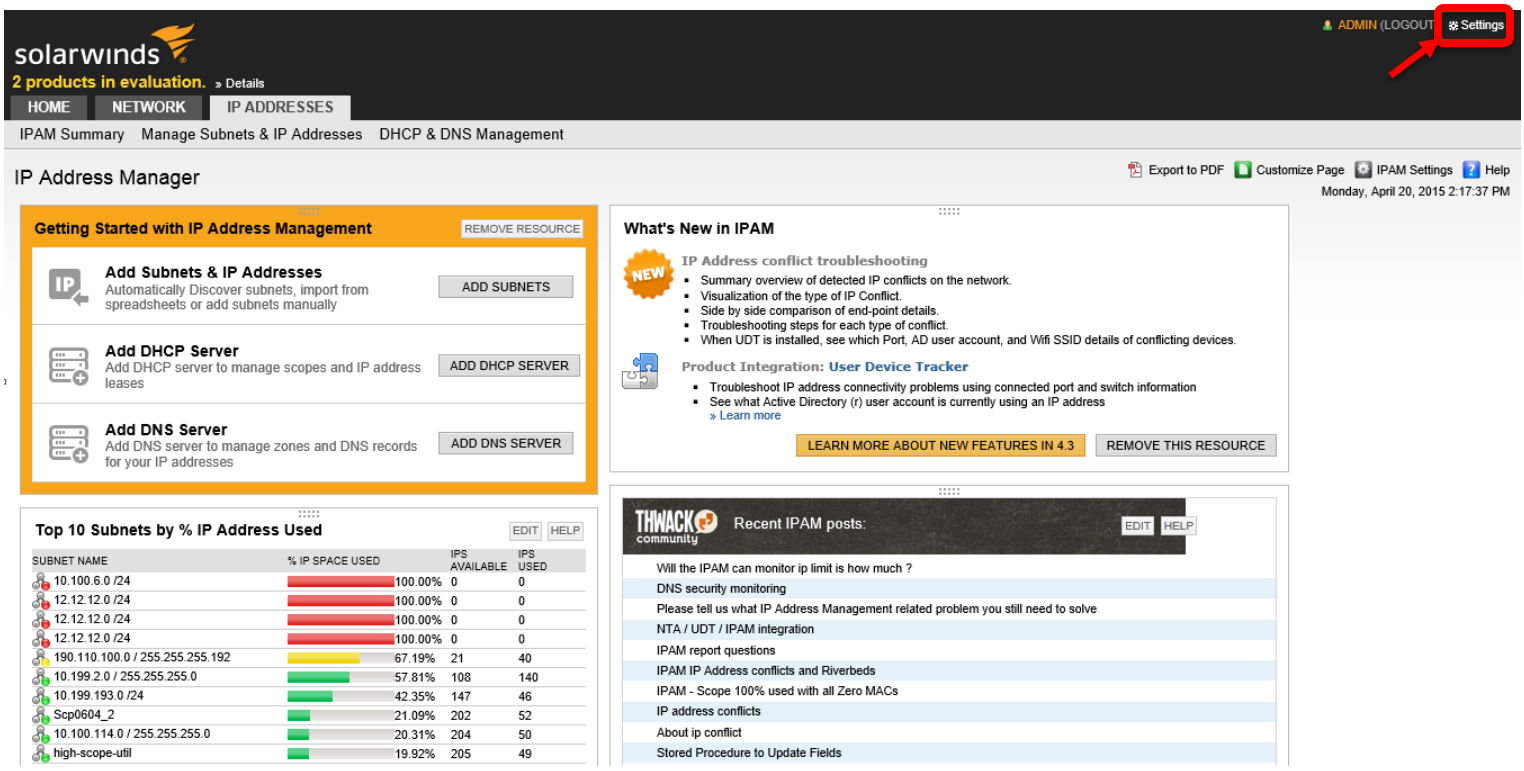
1. IP conflicts.
2. DHCP subnets and scopes for IP address pool depletion.
3. DNS forward and reverse record mismatches.
4. IPAM configuration change events.

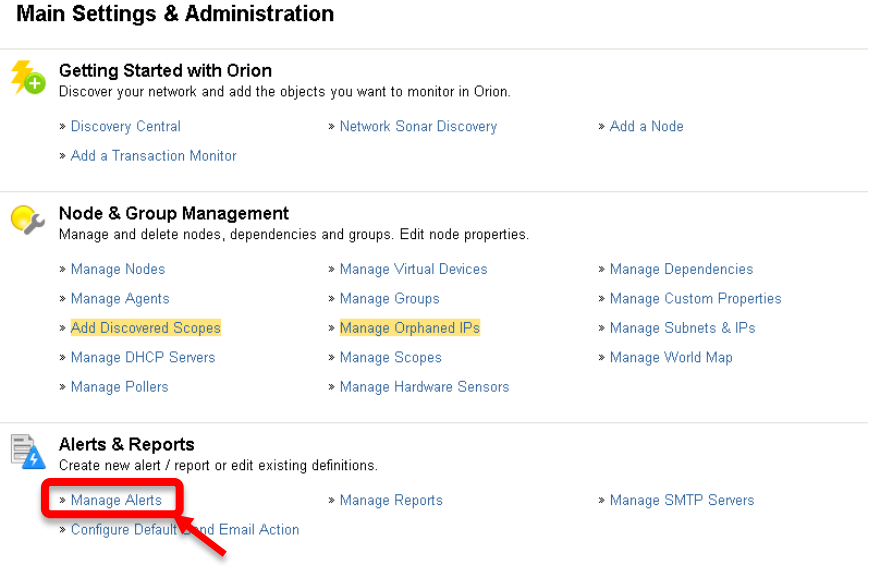
The following steps help you quickly configure and set alerts in IPAM.

Configuring alerts in IPAM

IPAM provides you with the flexibility to create alerts through an easy-to-use Web interface. The following sections provide step-by-step instructions for configuring alerts.

To begin the configuration process, click the Settings link at the top right corner of the IPAM Web interface. This opens the Settings page. Under the Alerts and Reports section, click Manage Alerts.

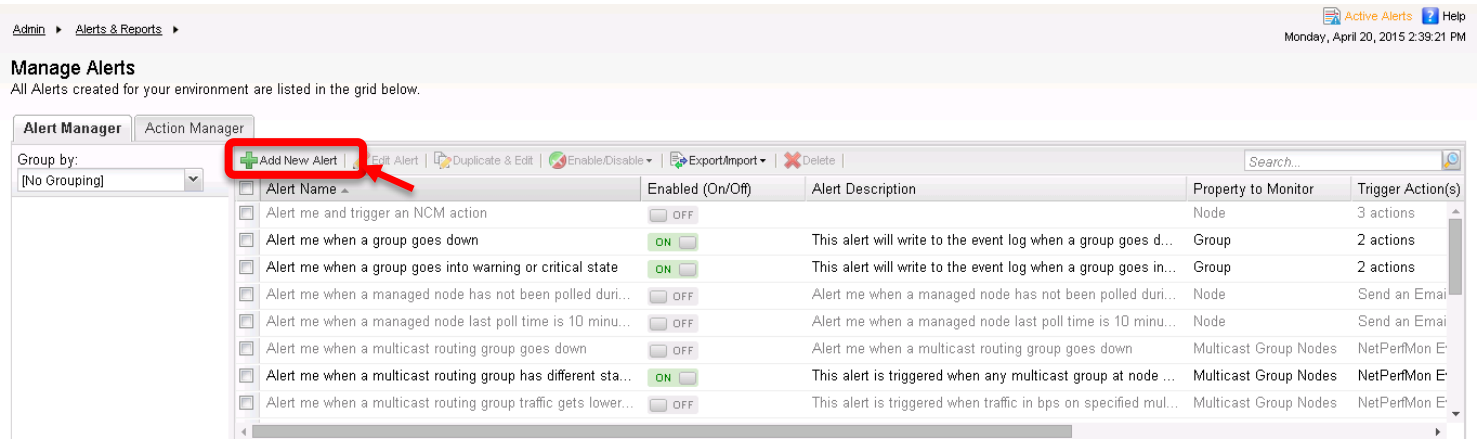




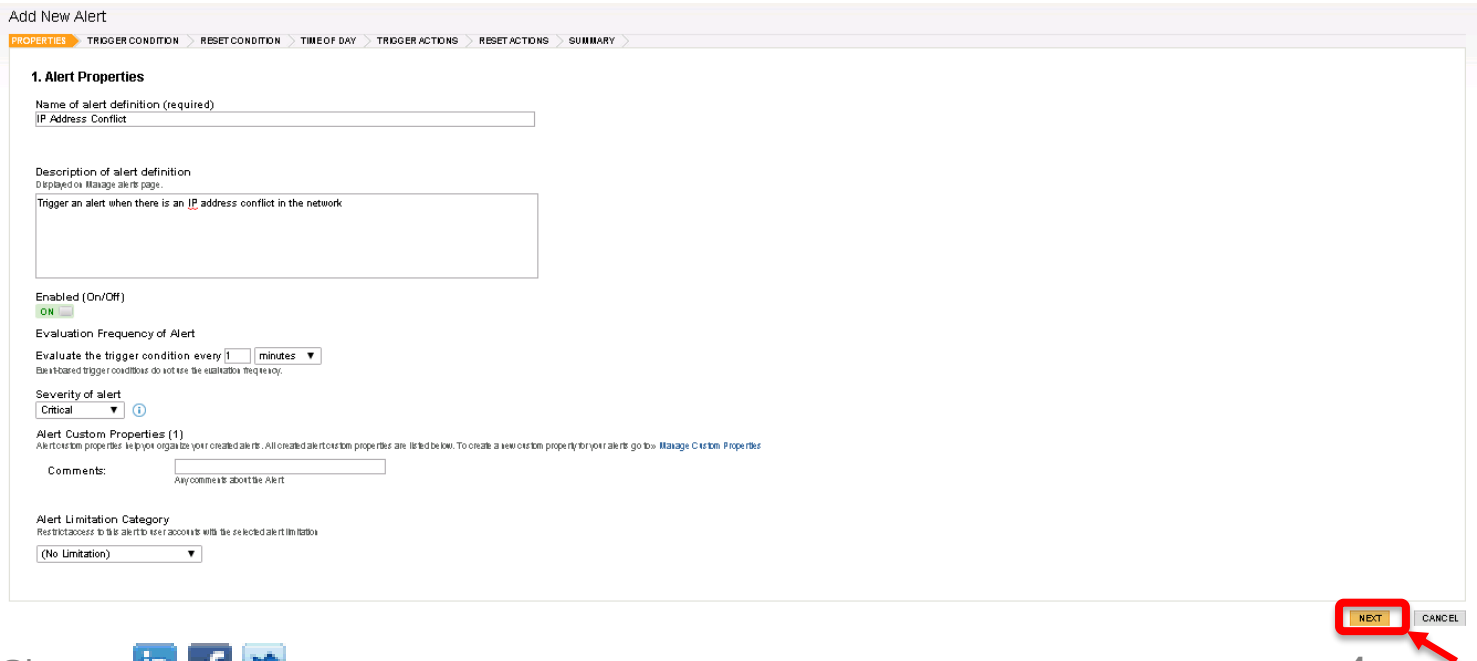
To create an alert

The Add New Alert wizard in IPAM walks you through the process of setting up your choice of customized alerts.

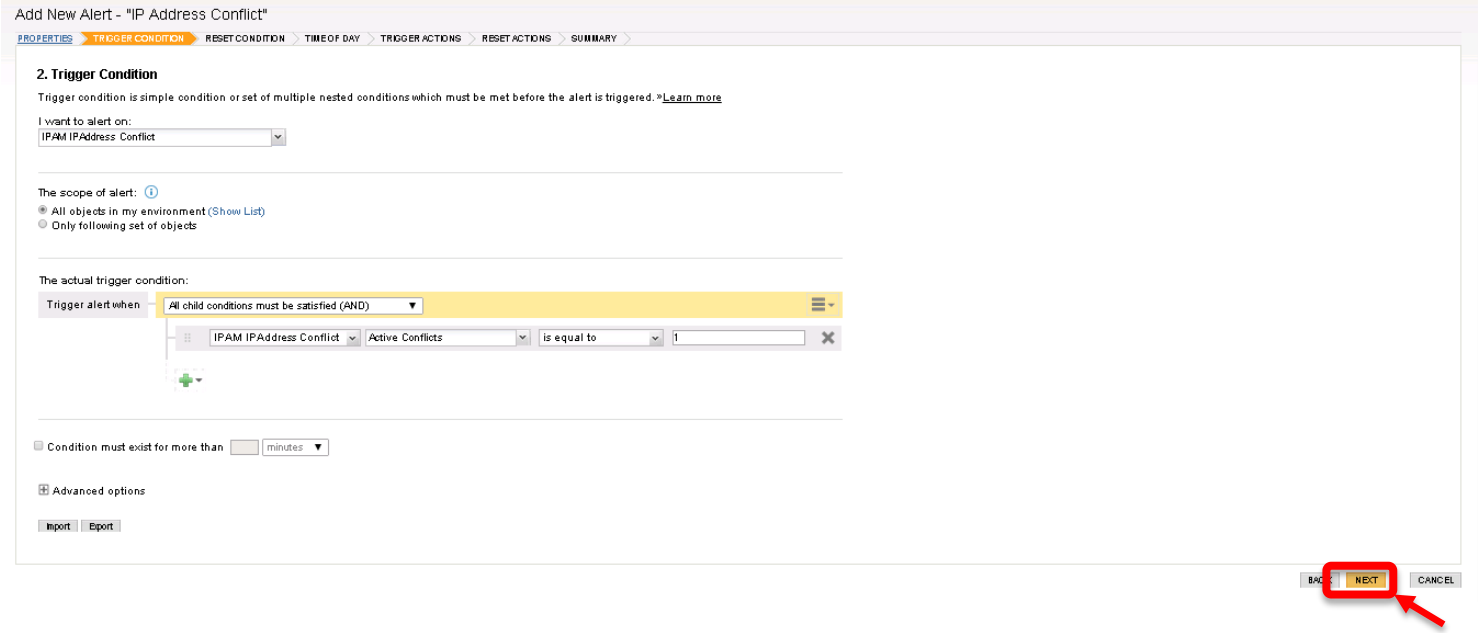
Step 1: Click Add New Alert.



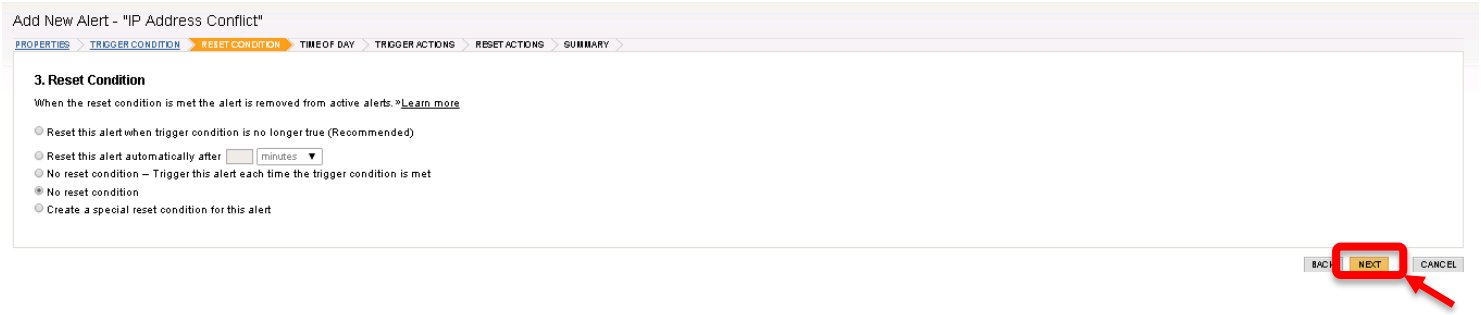
Step 2: Enter alert properties, such as alert name, description, severity, etc. Click Next.



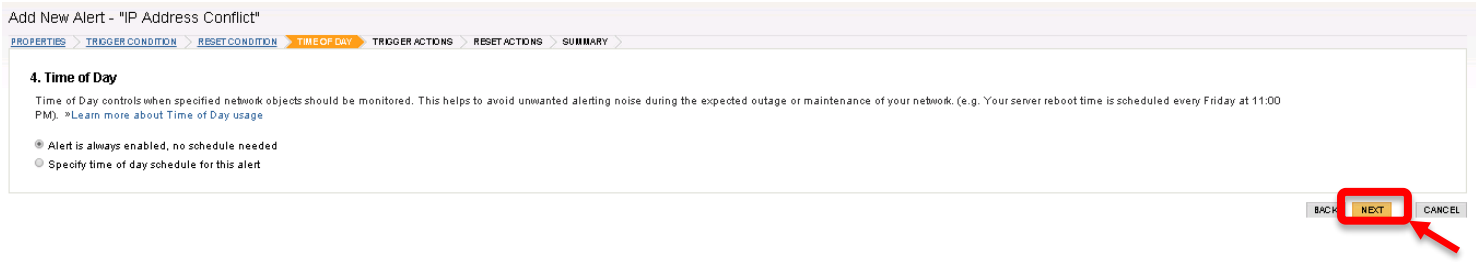
Step 3: List any nested conditions that must be met before the alert is triggered.



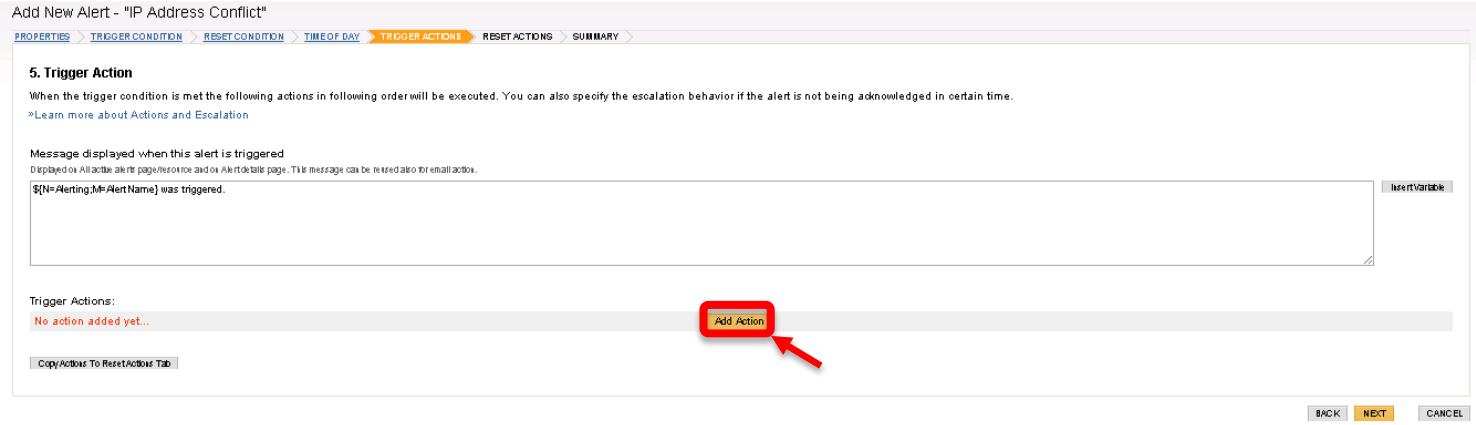
Step 4: You can set a reset condition for the alert. Otherwise, choose the option to trigger the alert every time the condition is met.



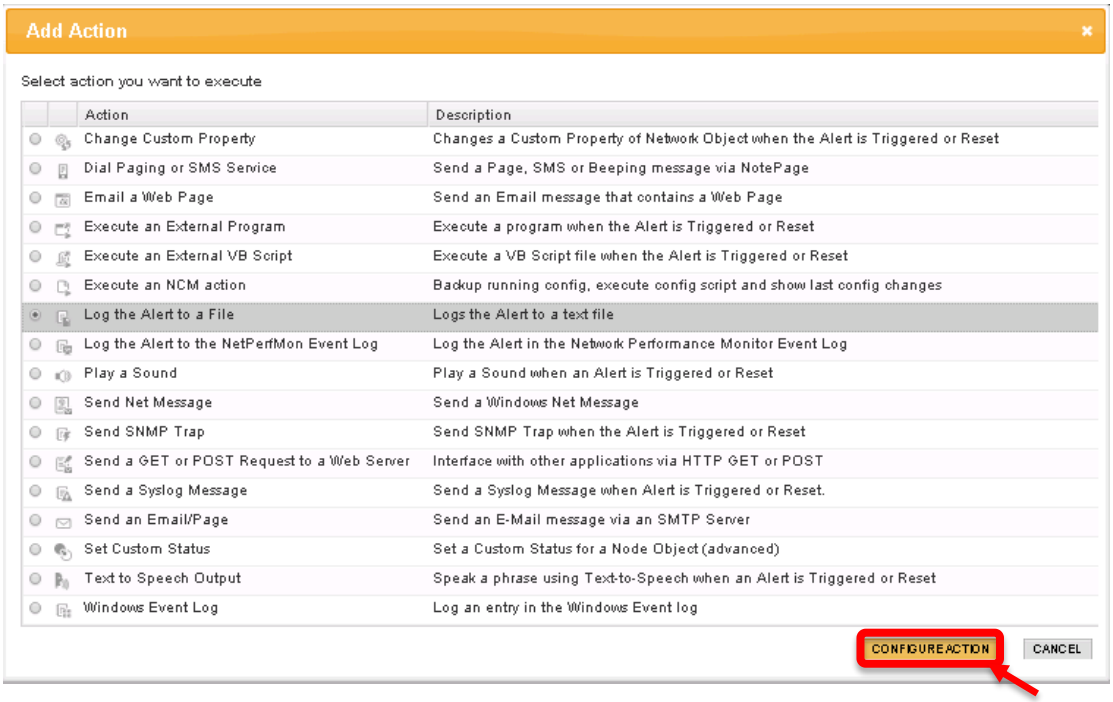
Step 5: Set the time for the alerts to be active.



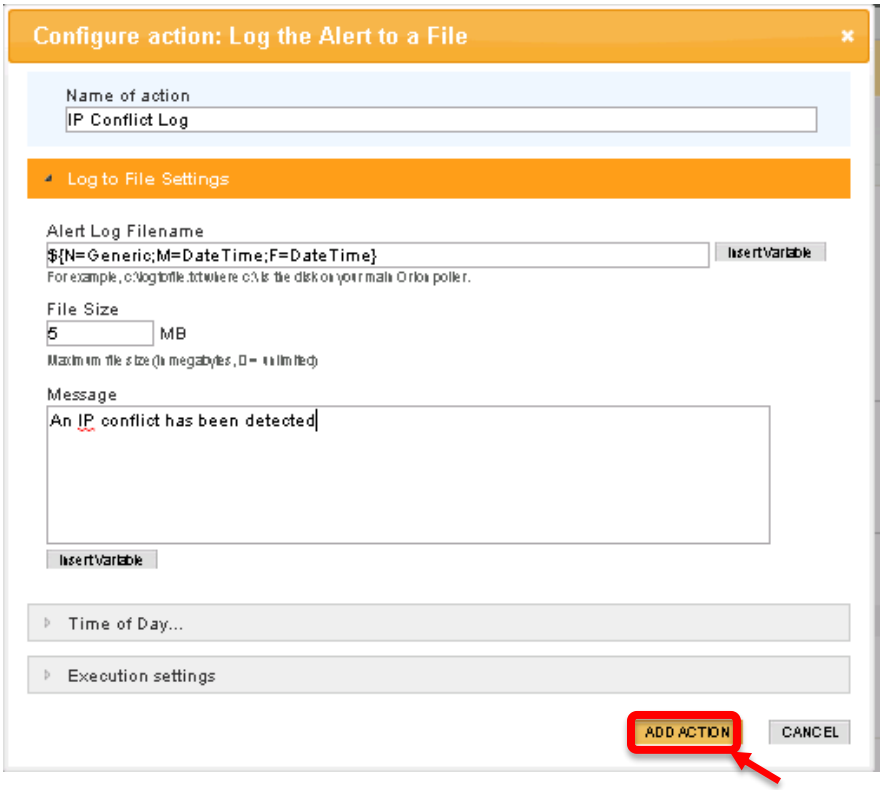
Trigger actions are executed when the trigger conditions are satisfied. For example, the trigger action for an IP conflict alert would be to send out an email alert when the trigger condition of detecting duplicate IP addresses is 'True'.



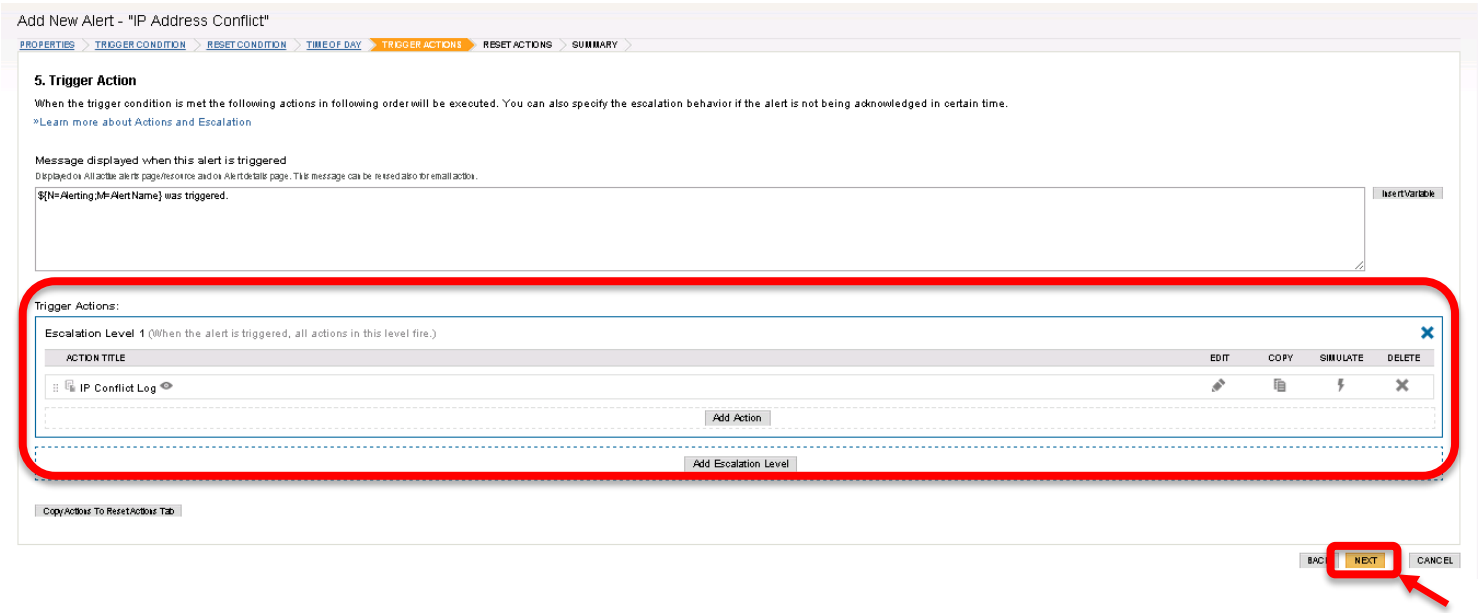
Step 6: Choose the required action to be executed when the alert is triggered, and click Configuration.



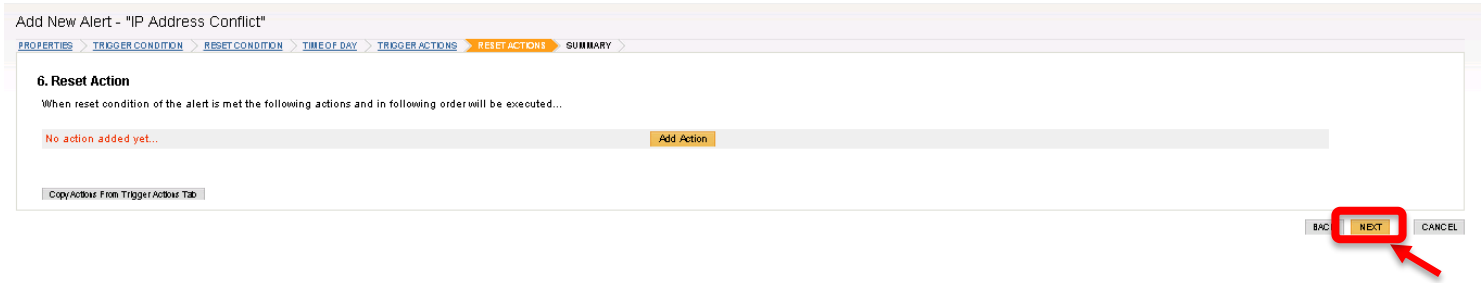
Step 7: Configure the alert action and include other execution settings as mentioned below, and click Add Action.



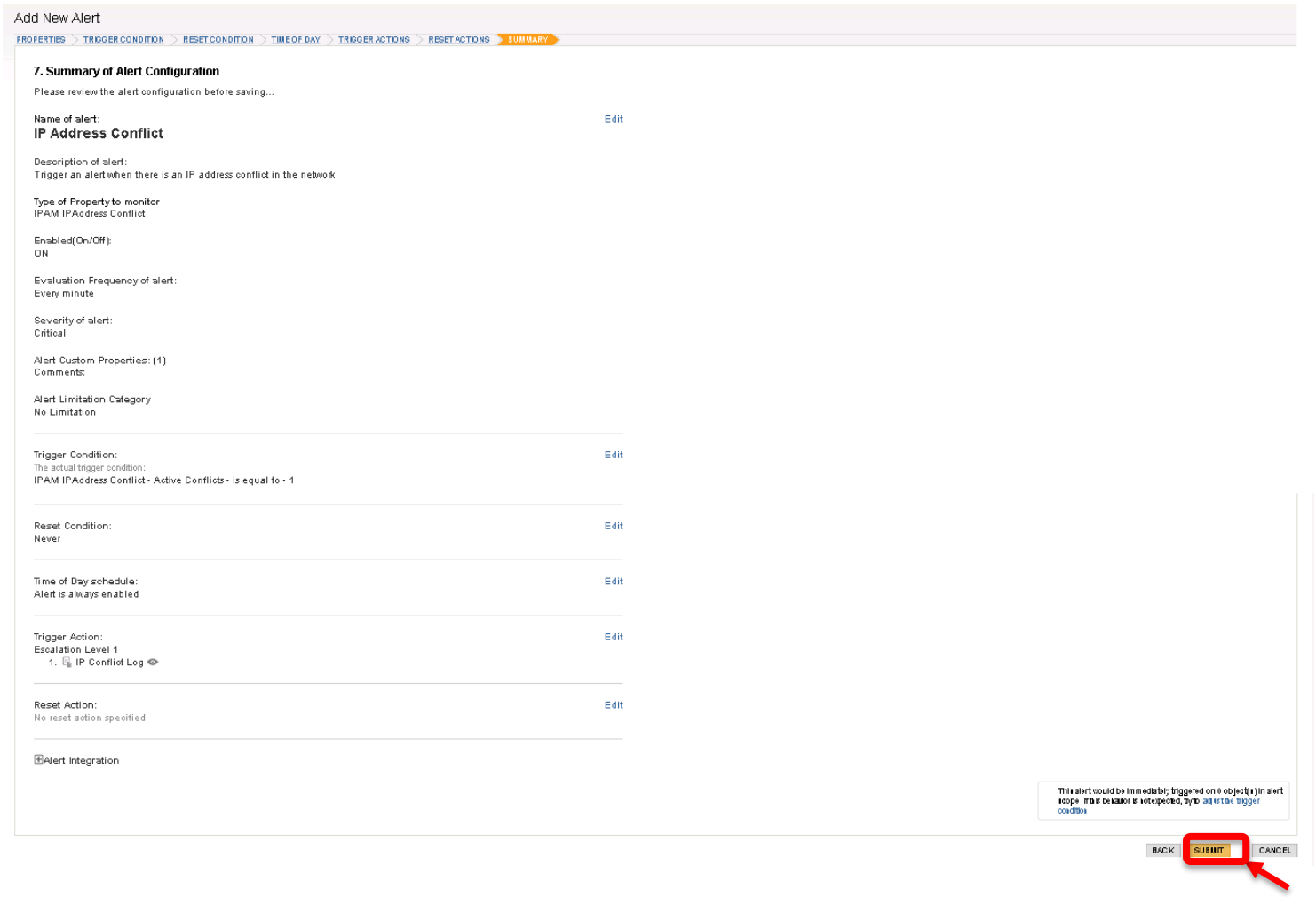
This completes the Trigger Actions step in the Add New Alerts Wizard.



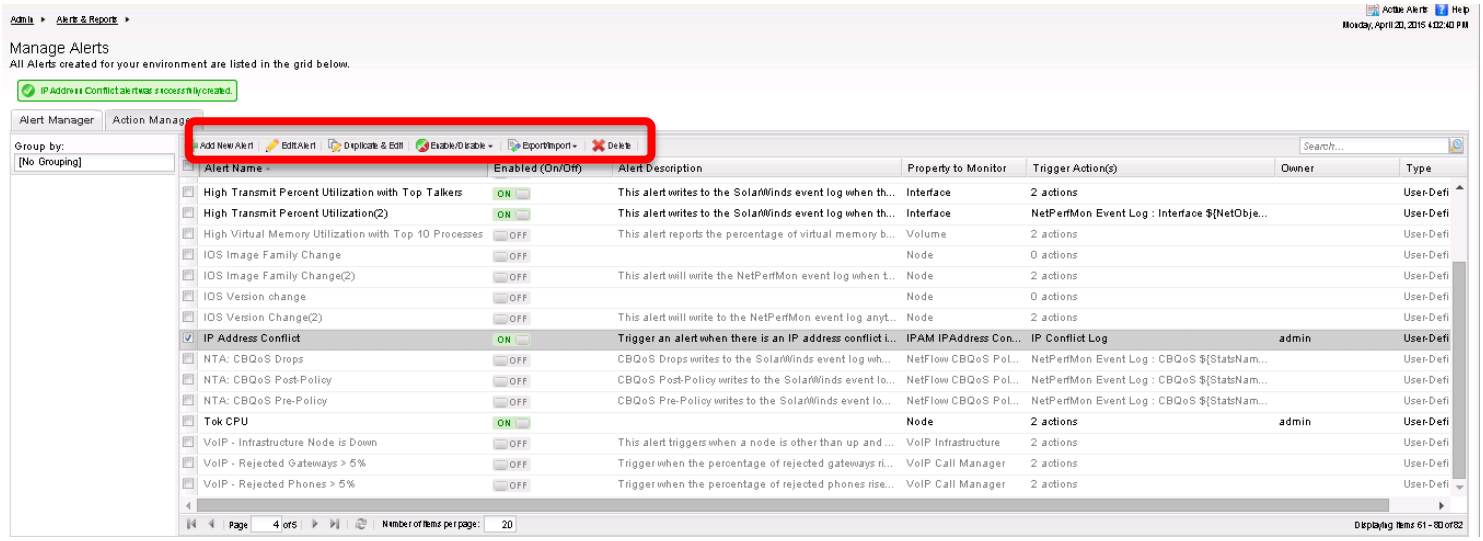
If there is a reset condition specified earlier, the reset actions are specified here.



Finally, review the specified details in the Summary view, and click Submit.

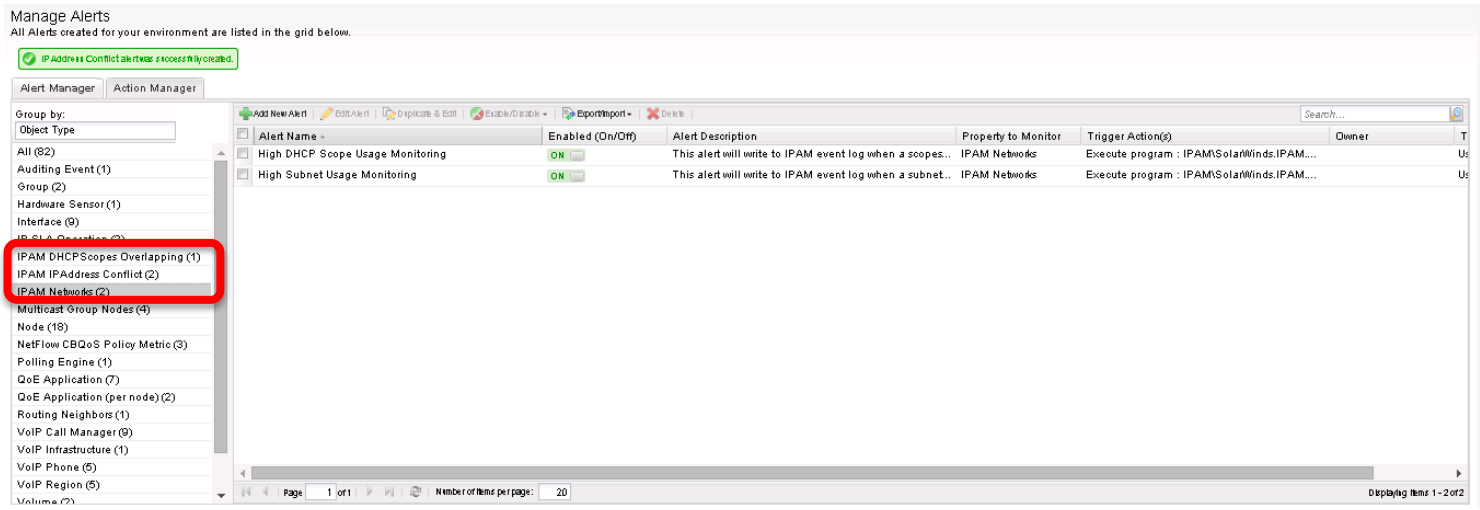


You have successfully created your network's sample alert for IP conflict notification. You can easily create, edit, duplicate, enable, disable, export, import, and delete alerts from the Manage Alerts view.

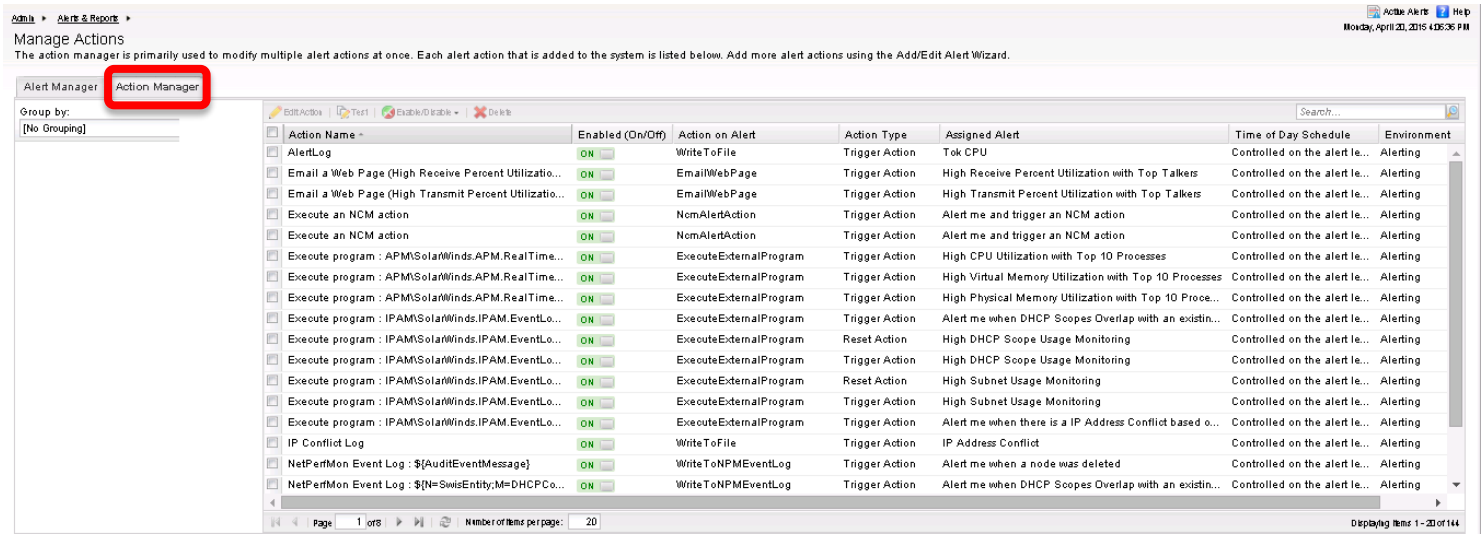


For easy viewing and manageability, group alerts by object type, trigger actions, owner, etc. Some of the default alerts available for IP address management are:

- DHCP scopes overlapping with existing IP addresses.
- IP conflicts in the network.
- High DHCP scope utilization monitoring.
- High subnet utilization monitoring.

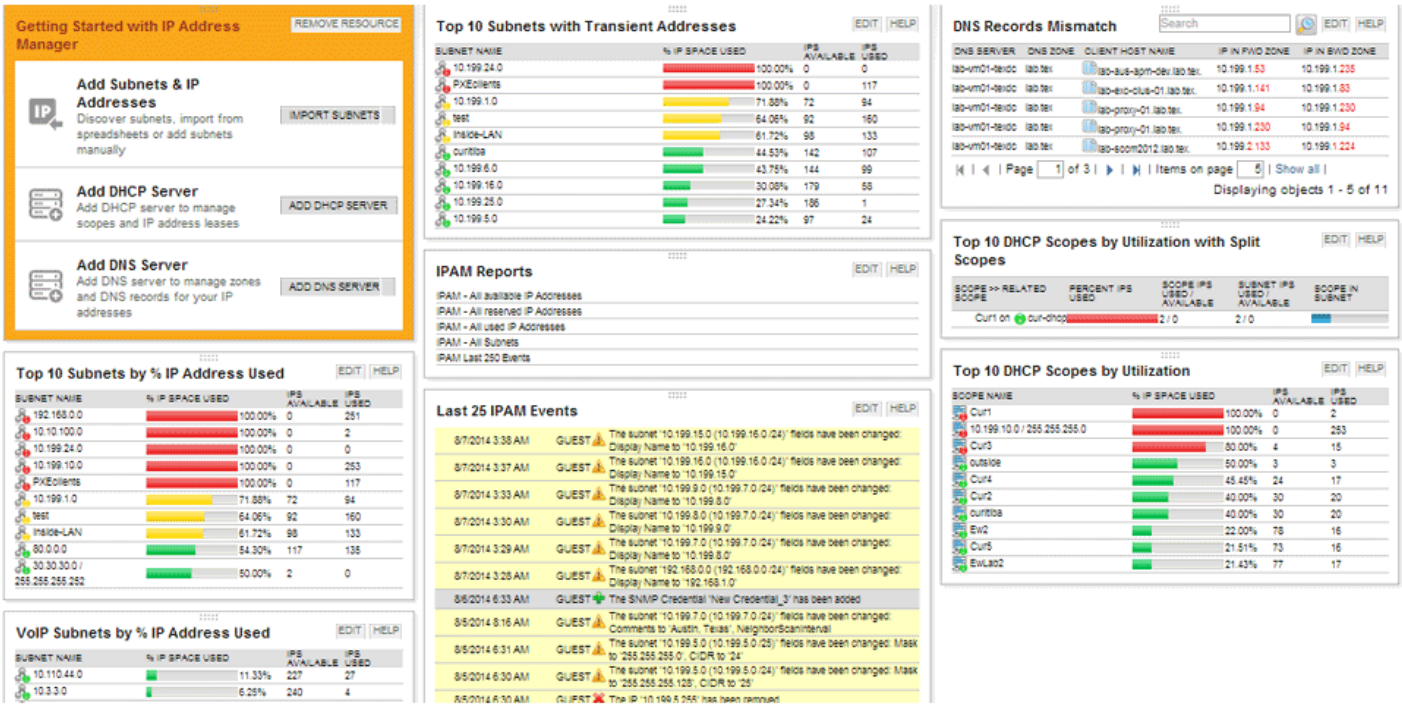


The Action Manager tab allows you to manage the actions that have been created for various alerts.



Specify custom SQL and SWQL alerts in the trigger condition for creating advanced alerts. Use IPAM to create alerts and be notified before things go wrong. Integration with SolarWinds® User Device Tracker (UDT) gives you even more options to set alerts on users and devices on the network.

The Summary page displays all alerts and events.



Top 5 reasons to use SolarWinds IPAM

- **Efficiently manage IPv4 and IPv6** address spaces together.
- **Ability to automatic propagate all DHCP and DNS changes** made via IPAM to the ISC DHCP and BIND servers.
- **Integrated monitoring and management of** your Microsoft®, Cisco®, and ISC DHCP as well as Microsoft and BIND DNS servers.
- **Active monitoring and preventive alerting** when a subnet nears full utilization, or if there are IP conflicts in the network.
- **Ability to delegate IP management tasks** with team and role-based permissioned access.

Seamlessly integrate SolarWinds IPAM into your existing DHCP and DNS environments quickly and easily in about an hour.