# Release Notes

## Basic information

| Product Model | NTA NX3-2000E/1000E/HD2100/HD2200  NTA VM |
| --- | --- |
| Software Version | V4.5R90F02SP05 |
| Upgrade File | [update\_nta\_V4.5R90F02SP05.210224build42860.bin](http://update.intra.nsfocus.com/upgrade/getAttachment/id/69115)  3445bf96dd17fe2caa92d515a79d7104 |
| Release Date | 2021-02-24 |
| How to Obtain | Obtain the upgrade file from the upgrade system or contact NSFOCUS technical support. |

## Version Mapping

| Hardware Model | NTA NX3-2000E/1000E (NSF-2800)  NTA NX3-HD2100/HD2200 (C236) |
| --- | --- |
| ADS | V4.5R90F02SP05 |
| ADS M | V4.5R90F02SP07 |
| NTA-ATM | V4.5R89F03 |
| MagicFlow | V4.5R90F01SP01 |
| Threat Analysis and Traceback System (TAT) | V2.0.0 |
| Client Browser | Chrome  Firefox |
| Documentation | None |

## New Requirements

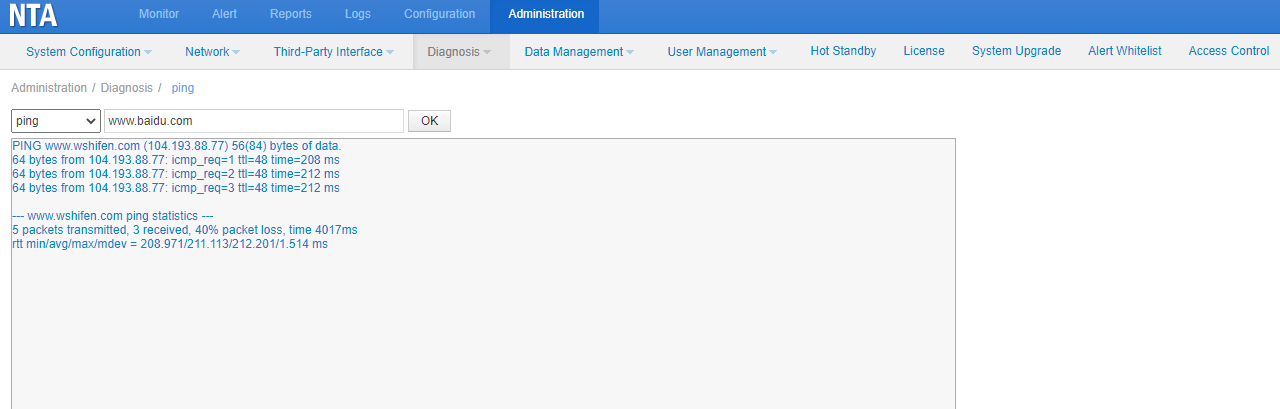
| No. | Requirement Description |
| --- | --- |
| 1 | The diagnostic tool Ping needs to support domain name pinging. |
| 2 | The A Interface needs to be upgraded to the latest version V3.0.7SP. |
| 3 | Auto-learning needs to be conducted for multiple IP groups at one go. |
| 4 | The status display of manual diversion rules needs to be optimized. |
| 5 | The cloud-side authentication mechanism needs to be optimized. |
| 6 | The flow processing performance needs to be optimized. |
| 7 | A switch is required for top N statistics of routers. |
| 8 | The HTTP host verification vulnerability needs to be fixed. |
| 9 | The collaboration with the cloud cleaning platform needs to be optimized. |

## New Functions

### Domain Name Pinging by Diagnostic Tool Ping

Description

The diagnostic tool ping supports the pinging of domain names for greater ease of use.



### Upgrade of A Interface to Latest Version V3.0.7SP

Description

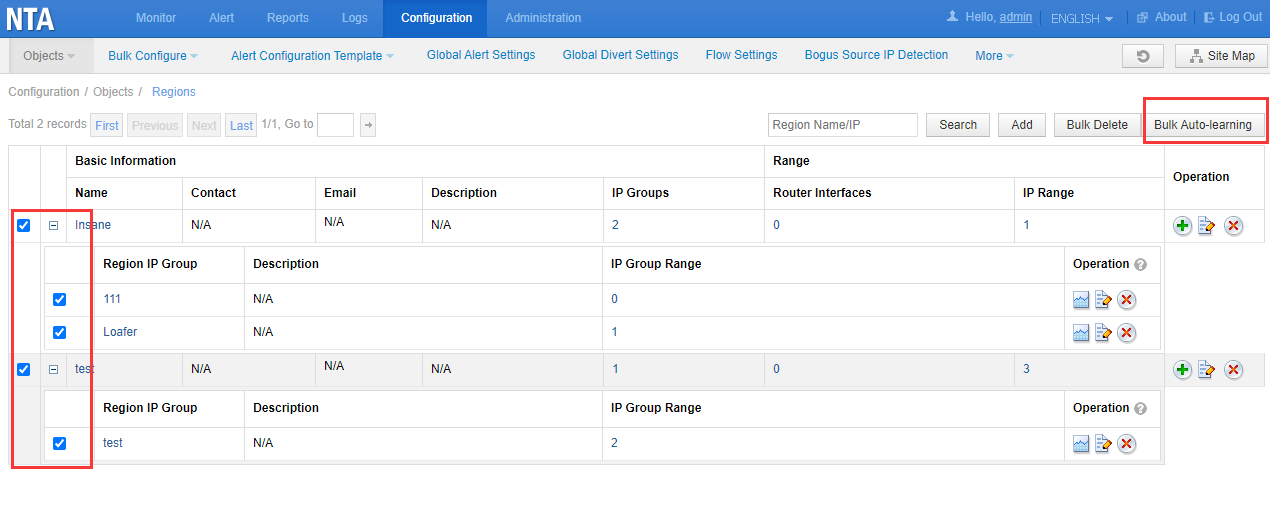
The A interface of the latest version has better security. In this version, the A interface is updated to the latest version to increase security and adapt to other products.

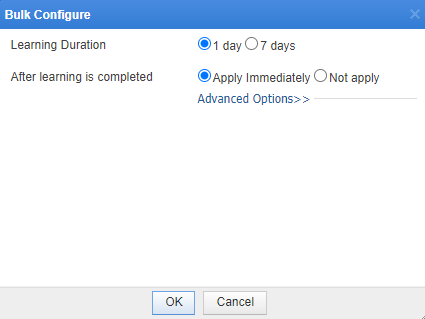
### Bulk Auto-Learning of IP Groups

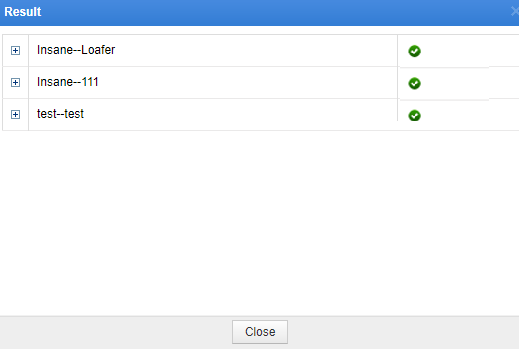
**Description**

In earlier versions, when it comes to diversion delivery or withdrawal, users need to dispatch or disable diversion rules one by one. They find the operations troublesome and expect them to be done in bulk.

**Configuration and Use**







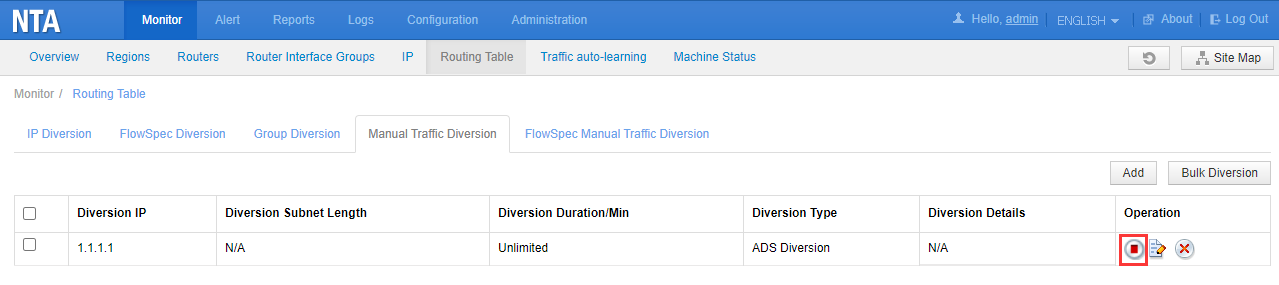
### Optimization of Status Display of Manual Diversion Rules

**Description**

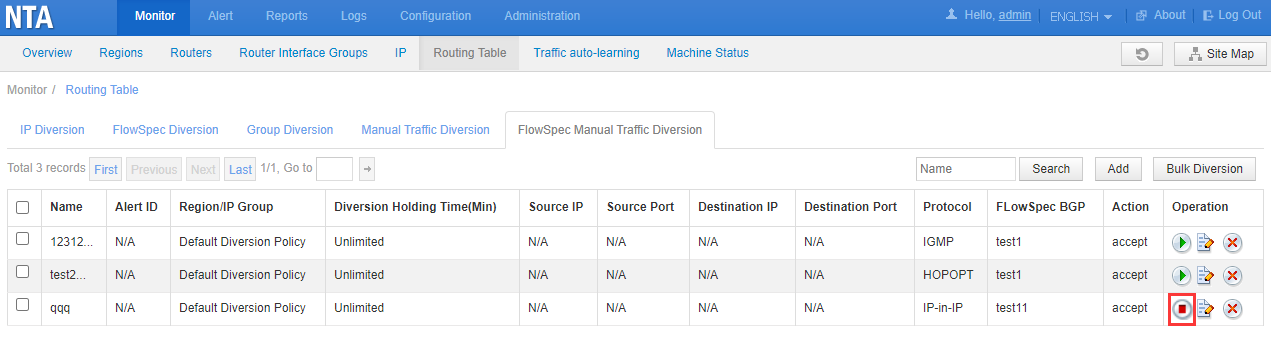
On the page for manual diversion, a button is added to show the current diversion status and allows users to withdraw diversion.

**Configuration and Use**

Choose **Monitor > Routing Table > Manual Traffic Diversion**, and click  in the **Operation** column of a manual traffic diversion to start diversion. Then the button turns to , indicating ongoing diversion. You can click this button to withdraw diversion.



Choose **Monitor > Routing Table > FlowSpec Manual Traffic Diversion**, and click  in the **Operation** column of a manual traffic diversion to start diversion. Then the button turns to , indicating ongoing diversion. You can click this button to withdraw diversion.



### Optimization of Cloud-Side Authentication

**Description**

Immediately upon the return of a cloud authentication failure message, NTA stops all its engines, leading to a service disruption. To avoid this issue, a grace period is introduced to allow the NTA to stop its engines if the cloud authentication failure persists for 30 days.

### Optimization of Flow Processing Performance

**Description**

After optimization, NTA-HD2200 powered by Caswell's C236 platform has a flow processing capacity of 250,000 flows per second.

Also, NTA-2000E based on the Gemotech 2800 platform is optimized to have a higher processing capability of 200,000 flows per second.

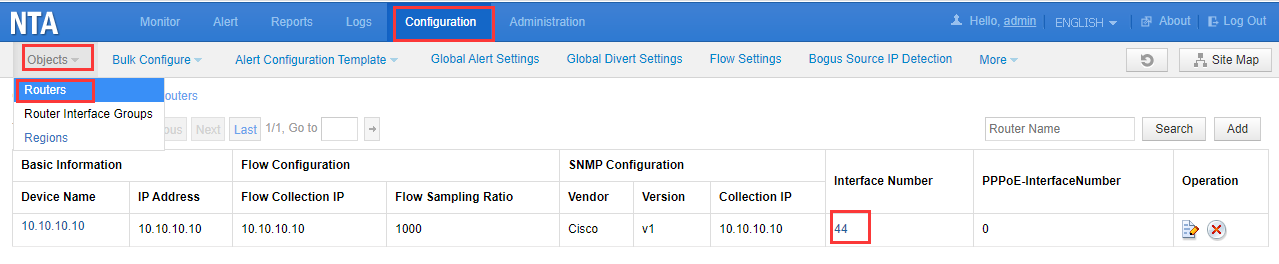
### Addition of Switches for Top N Statistics of Routers

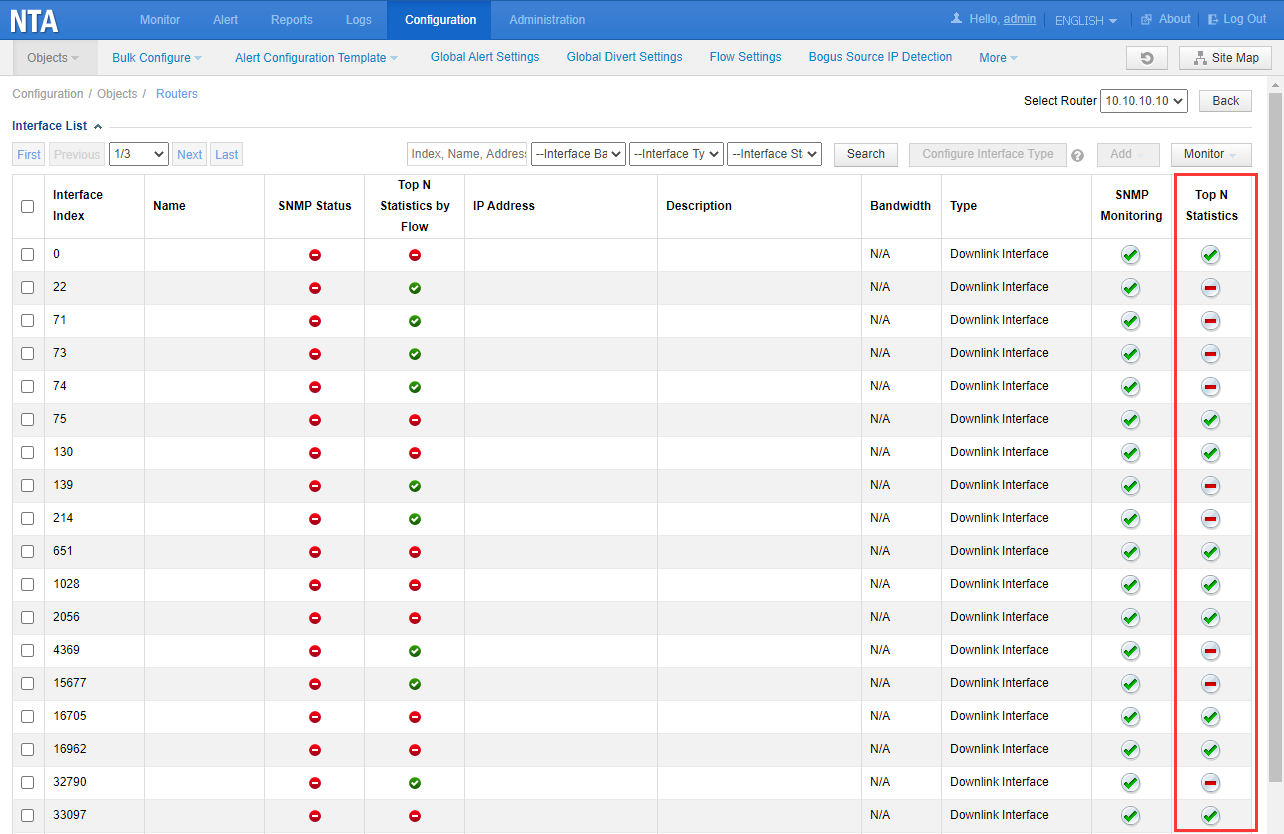
**Description**

Collecting top N statistics for each interface of routers greatly degrades device performance. Most customers focus only on top N Flow statistics on borders. For them, switches are required for top N Flow statistics for uplink interface groups. However, a small number of customers show interests in such statistics of downlink interfaces. To address requirements of all customers, a switch is added for top N flow statistics of each interface.

**Configuration and Use**

Choose **Configuration > Objects > Routers**, click the value in the **Interface Number** column of the router information table. On the **Interface List** page, the **Top N Statistics** column is added to allow users to enable or disable top N Flow statistics for one or all interfaces.





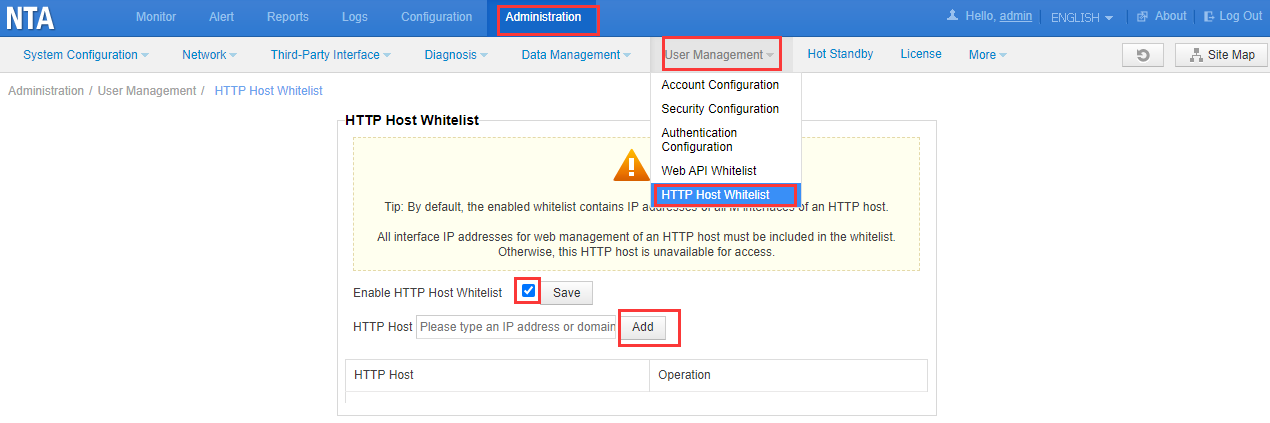
### Fix of the HTTP Host Verification Vulnerability

**Description**

The HTTP host whitelist function is added and disabled by default upon upgrade. After this function is enabled, NTA verifies the IP addresses or domain names of HTTP hosts according to the whitelist and blocks access to those IP addresses or domain names that are outside of the whitelist.

In the whitelist, an HTTP host can have up to 10 IP addresses and domain names.

**Configuration and Use**



### Optimization of Collaboration with a Cloud Cleaning Platform

**Description**

The data collection and sending logic is optimized for scenarios of collaboration with a cloud cleaning platform to prevent a data loss in the case of a program getting stuck, flipping (too low network), or data sending timeout.

## Fixed Bugs

* 193624 After the device boots up, a sock of flow\_route\_system fails to start properly, leading to a diversion dispatch failure.
* 193618 In double diversion mode, if the two diversion policies have the same next-hop IP address (next-hop IP address of BGP null route diversion or IP address of a third-party protection device)
* 193987 When regions or IP groups are dispatched via an API, no traffic statistics are collected due to the lack of a statistics notification.
* 194715 Occasionally, bsa\_repeater\_deamon fails to be started when ATM switches from the scheduled mode to the real-time mode.
* 194777 Diversion notifications for regions or IP groups cannot be sent by email.
* 192262 Bulk FlowSpec diversion fails during diversion holding time.
* 192320 Code of all earlier versions is backed up and takes up a lot of space. In this version, the upgrade script only backs up the code of the source version, while clearing code of other versions.
* 192321 The directory for saving logs of the updated A interface is changed to /usr/local/data/log.
* 191649 Some security vulnerabilities and issues are fixed.
* 191958 The option of enabling HTTP host header defense does not work. When you select this option and save the setting, it is still unselected.
* 193021 An IP group has IP addresses organized in a tree-like structure. Modifying region information will lead to an IPv6 address loading failure for this IP group.
* 193755 During a web scanning for websites under monitoring of NTA, RSAS finds a JavaScript framework vulnerability in websites.
* 167752 When the system time zone is daylight saving time (DST), the system time is inconsistent with the database time.
* 195840 If the V4.5R90F02SP01 update is not applied, attack source reports are retrieved from t\_event\_traffic\_ip rather than its corresponding child table.

## Upgrade Procedure

**Note: You must upgrade in strict accordance with the upgrade path.**

**The upgrade procedure is as follows:**

Log in to the web-based manager of NTA and choose **Administration** > **System Upgrade**.

Browse to **update\_nta\_V4.5R90F02SP05.210224build42860.bin** and click **Upload**.

Read upgrade notes and click **Confirm Upgrade** to continue the upgrade.

Wait 5 minutes for the installation to complete before refreshing the current page. Click About in the upper-right corner of the web-based manager to check the current system version. If **Product Version** is **V4.5R90F02SP05.210224build42860**, the upgrade succeeded. If not, the upgrade failed and you need to contact NSFOCUS technical support.

----End

**It is normal that the following situations arise in the upgrade process:**

1. The web-based manager displays an error message "502 Bad Gateway" for or directly denies your access request.

2. All services will stop running.

3. The upgrade takes about 5 minutes. If the page remains unresponsive after 5 minutes, you need to manually refresh the page.

**Note that the system will automatically restart after the upgrade is complete.**

## Upgrade Path

