Release Notes

1. Basic Information

Device Model	• NTA NX3-2000E/1000E/D1100/D1200/D2100/D2200 • vNTA
Software Version	V4.5R90F01SP03
Upgrade File	update_nta_V4.5R90F01SP03.190617build31166.bin MD5: EC4350D2CE90D85B38F0CA9A2AEC499E
Release Date	2019-06-19
How to Obtain	Obtain the upgrade file from the upgrade system or contact NSFOCUS technical support.

2. Version Mapping

Product Model	• NTA NX3-2000E/1000E (NSF-2800) • NTA NX3-D1100/D1200/D2100/D2200 (C236)
ADS	• V4.5.88.15 • V4.5R90F01 • V4.5R90F01SP01 • V4.5R90F01SP02 • V4.5R90F01SP03 • V4.5R90F01SP04 • V4.5R90F01SP05
ADS M	V4.5R90F01SP04
NTA-ATM	V4.5R89F03
Threat Analysis and Traceback System (TAT)	V2.0.0
Client Browser	• Chrome • Firefox • Internet Explorer 10
Documentation	NSFOCUS NTA Installation Guide/User Guide (V4.5R90F01)

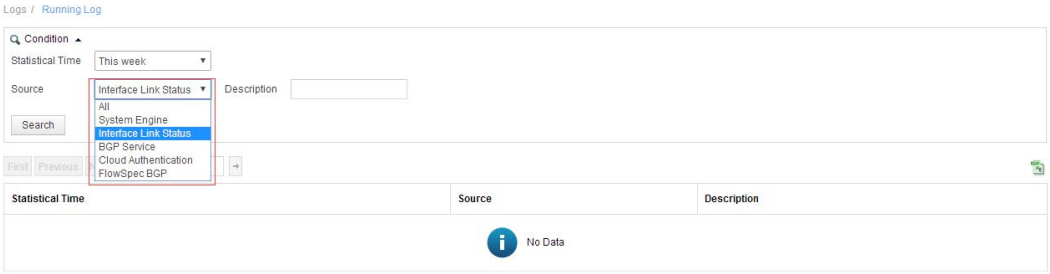
3. Satisfied Requirements

No.	Requirement Description
1	Interface link status changes should be recorded in running logs.
2	A new A interface should be used for cloud-based authentication.
3	The cloud-based authentication timeout period should be modified.
4	The longest allowed holding time of BGP diversion should be extended to 10,080 minutes (7 days).
5	Interim and subscription licenses should be added.
6	A port number should be configured for collaboration with the cloud-based cleaning platform.
7	The address family of FlowSpec BGP should be changed to include only IPv4 and IPv6 flows.
8	The time zone configuration file should be changed to separate Araguaina and Sao Paulo.
9	Beijing should be displayed in the GMT+8:00 time zone.
10	The historical CPU usage, memory usage, and number of flows should be displayed.

4. New Functions

4.1 Interface Link Status Changes Provided in Running Logs

When the physical network is disconnected or connected, resulting interface link status changes are recorded in running logs under **Logs > Running Log**. You can select **Interface Link Status** from the **Source** drop-down list to search for logs of this type.



4.2 New A Interface Added for Cloud-Based Authentication

The communication interface for cloud-based authentication is changed to a new A interface, so the authentication program is updated as well.

4.3 Cloud-based Authentication Timeout Period Changed

The cloud-based authentication timeout period is changed from 7 days to 15 days. That is, if the cloud-based authentication has failed for 15 consecutive days, the status will be displayed as **Unauthorized** and all services will become unavailable.

4.4 Longest Allowed Holding Time of BGP Diversion Extended to 10,080 Minutes (7 Days)

To guarantee the collaboration between NTA and other platforms, the longest allowed holding time of BGP diversion is extended to 10,080 minutes. Details are as follows:

- For global diversion configuration, the longest diversion holding time of ADS diversion, BGP diversion, null-route diversion, and FlowSpec diversion can be set to 10,080 minutes.
- For region-specific traffic diversion configuration, the longest diversion holding time of null-route diversion can be set to 10,080 minutes.
- For region-specific diversion policy configuration, the longest diversion holding time of ADS diversion, BGP diversion, null-route diversion, and FlowSpec diversion can be set to 10,080 minutes.
- For IP group-specific traffic diversion configuration, the longest diversion holding time of null-route diversion can be set to 10,080 minutes.
- For IP group-specific diversion policy configuration, the longest diversion holding time of ADS diversion, BGP diversion, null-route diversion, and FlowSpec diversion can be set to 10,080 minutes.
- For diversion routing table configuration, when manual traffic diversion is enabled, the longest diversion holding time of ADS diversion, BGP diversion, and null-route diversion can be set to 10,080 minutes.

- For diversion routing table configuration, when FlowSpec manual traffic diversion is enabled, the longest diversion holding time can be set to 10,080 minutes.

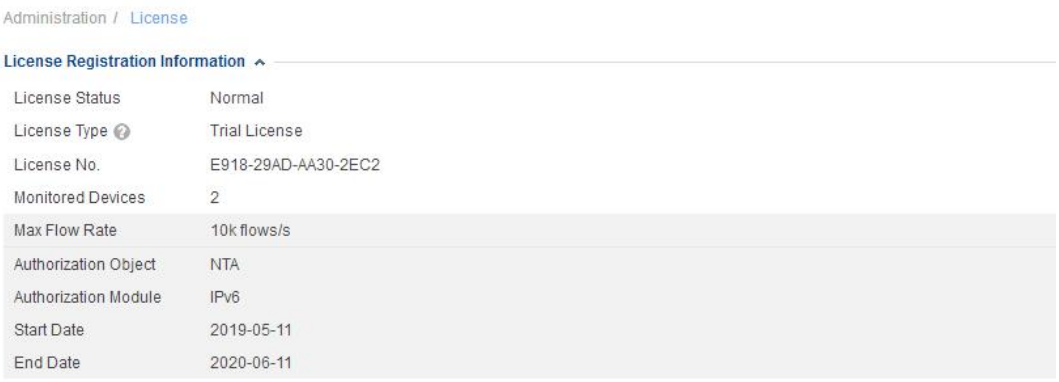
4.5 Interim and Subscription Licenses Are Added

The type of interim license is added for both NTA and vNTA, indicating the purchasement agreement has been signed without full payment. The type of subscription license is added for vNTA, indicating completion of sales and full payment.

After a license expires, results are as follows:

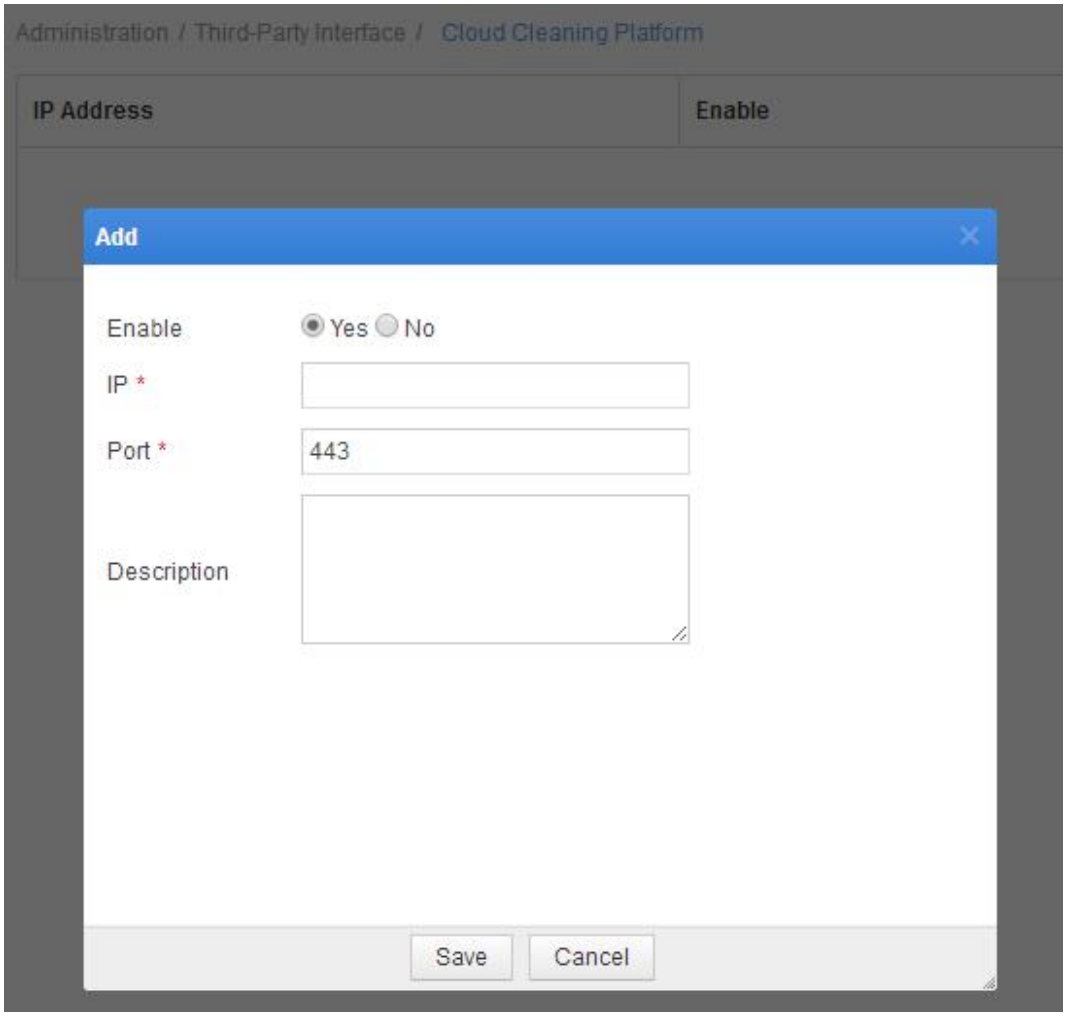
- After the trial license expires, the device can neither be used nor updated.
- After the interim license expires, the device can neither be used nor updated.
- After the paid license expires, the device can still be used, but cannot be updated.
- After the subscription license expires, the device can neither be used nor updated.

A prompt message is added on the **License** page. Pointing at  after **License Type** displays the prompt message.



4.6 A Port Number Can Be Configured for Collaboration with the Cloud Cleaning Platform

Under **Administration > Third-Party Interface > Cloud Cleaning Platform**, after clicking **Add** in the upper-right corner of the page, you can set a port number in the range of 1–65535 in the dialog box that appears.



For an NTA device whose port number is configured by modifying the configuration file in the background, the port number is set to 443 after the device is upgraded to V4.5R90F01SP03.

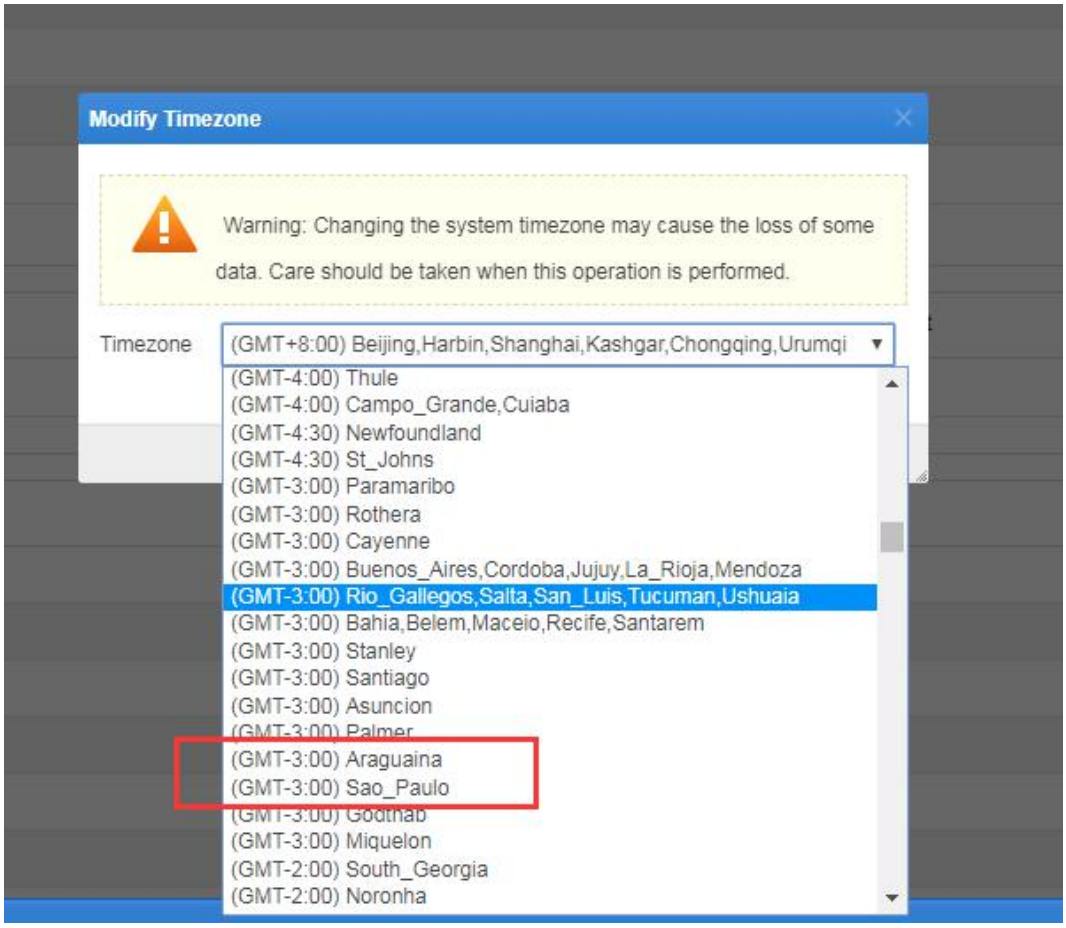
4.7 The Address Family of FlowSpec BGP Is Set to IPv4 and IPv6 Flows

Originally, the default setting of address family was used for NTA to establish BGP neighborship, with too many BGP protocols supported. However, in actual environments, FlowSpec only requires IPv4 and IPv6 flow configuration.

4.8 The Time Zone Configuration File Is Split by Separating Araguaina and Sao Paulo

Both Araguaina and Sao Paulo belong to the GMT-3 time zone and are included in the same time zone entry. However, Sao Paulo adopts the daylight saving time (DST), but Araguaina does not. When the time zone is set to GMT-3, the system time zone is set to that of Araguaina, causing a problem.

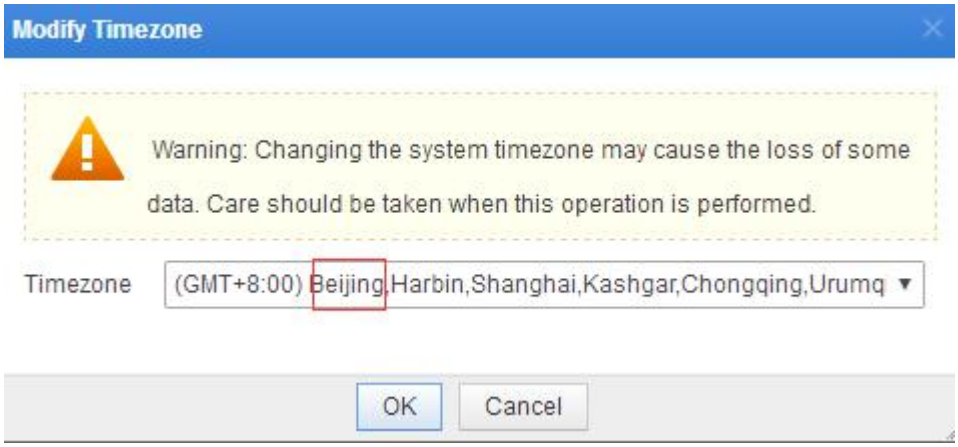
Araguaina and Sao Paulo are now separated and you can select either as required.



If the time zone is set to **Araguaina and Sao_Paulo**, after the device is upgraded to V4.5R90F01SP03, the time zone is set to **Sao_Paulo** by default.

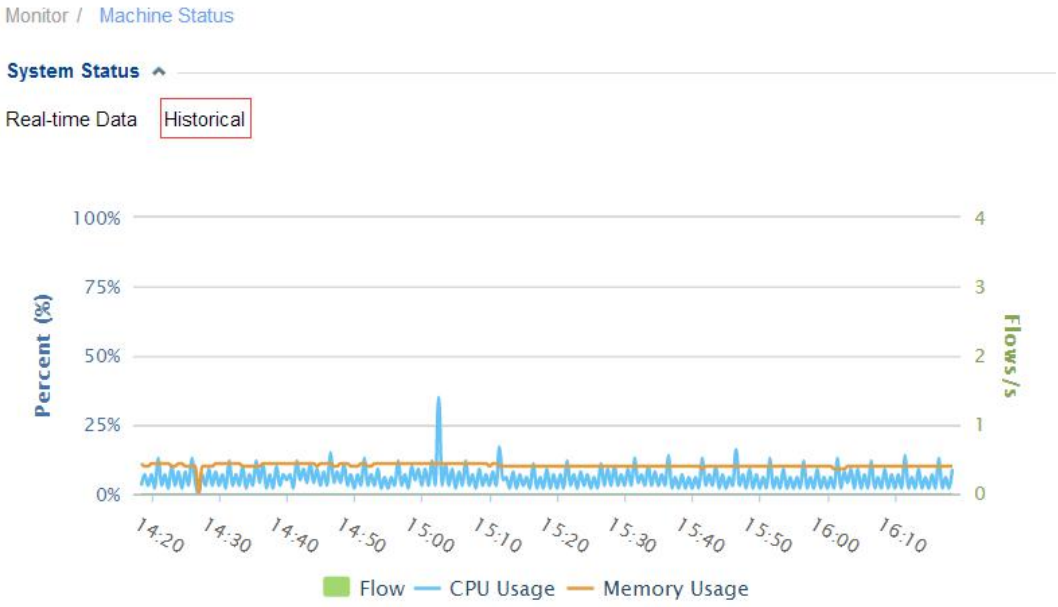
4.9 Beijing Is Displayed in the GMT+8:00 Time Zone

Beijing is now displayed when the time zone is set to GMT+8:00.



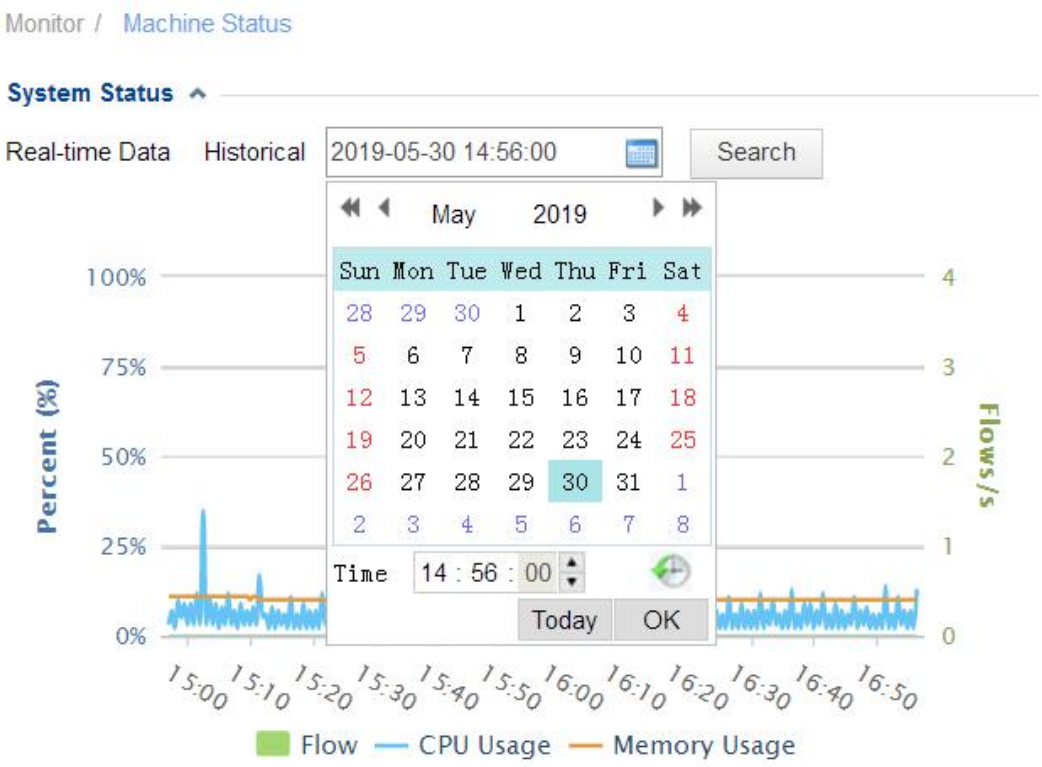
4.10 The Historical CPU Usage, Memory Usage, and Number of Flows Are Displayed

The **Historical** tab page is added under **Monitor > Machine Status**.



On the **Historical** tab page, you can set a historical time to view data of 2 hours after the specified time.

The 1-minute automatic refresh mechanism is removed from this page.



Historical data will be saved for one year and cleared once a month.

5. Fixed Bugs

Bug ID	Description
108349	In stable environments, database connections run out.
146772	After an interface status changes from down to up, the configured IPv6 addresses for this interface is missing.
146774	Link-local IPv6 addresses cannot be configured as the default gateway of an IPv6 route.
148044	After an interface is configured during region range configuration, the traffic direction is incorrectly detected.
152992	Chinese fields are included in alert email messages.
153237	In particular circumstances, the alert time cannot be updated.
152554	IPv6 addresses whose prefix length is 127 are unidirectionally unreachable.
111098	When the two-node cluster hot backup function is enabled, NTA cannot collaborate with ADS via a virtual IP address.
147623	The cloud-based authentication of vNTA fails repeatedly.
153755	For 1000E/D2100/D1100 models, flow restriction is not stable.
155682	During system running, an error occurs because the system memory runs out.

Bug ID	Description
155752	During region configuration, when router interfaces are selected as the protection scope, uplink interfaces are displayed as interconnection interfaces.
155728	When Alert Status is set to All, querying historical alerts always displays ongoing alerts.
155230	The maximum traffic of a region displayed under Monitor > Regions is not the same as that in that region's traffic report.
158248	Once configured, manual BGP FlowSpec diversions cannot be edited under Monitor > Routing Table > FlowSpec Manual Traffic Diversion page.

6. Notes

It is important to note that many customers who have configured the HA environment use an actual IP address rather than a virtual one for NTA to collaborate with ADS, which may cause a collaboration failure after system upgrade. In this case, they need to change the IP address to a virtual one for collaboration with ADS. In the HA environment, a virtual IP address is required for NTA to collaborate with other devices, such as ADS M and BSA.

7. Upgrade Procedure

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

The upgrade procedure is as follows:

Step 1 Log in to the web-based manager of NTA and choose **Administration** > **System Upgrade**.

Step 2 Browse to update_nta_V4.5R90F01SP03.190617build31166.bin and click Upload.

Step 3 Read upgrade notes and click **Confirm Upgrade** to start the upgrade.

Step 4 The upgrade takes about 5 minutes. After the upgrade is complete, refresh the current page.

Step 5 Click **About** in the upper-right corner of the web-based manager to check the current system version.

If **Product Version** is **V4.5R90F01SP03.190617build31166**, the upgrade succeeded. If not, the upgrade failed and you need to contact NSFOCUS technical support.

It is normal that the following situations arise during the upgrade:

- The web-based manager displays an error message "502 Bad Gateway" for or directly denies your access request.
- All services will stop running.
- The upgrade takes about 5 minutes. Later, you need to manually refresh the page.

Note that the system will automatically restart after the installation is complete.

8. Upgrade Path