Release Notes

Basic Information

Product Model	ADS NX3-M1600E
Software Version	V4.5R90F01
Upgrade File	update_adsm_V4.5R90F01build20180904.zip (MD5: c818752417685d365d435b9afb4e664d)
Release Date	2018-09-15
How to Obtain	Contact NSFOCUS technical support.

Version Mapping

Source Software Version	• V4.5R90F00 • V4.5R90F00SP01 • V4.5R90F00SP02 • V4.5R90F00SP03
Product Model	ADS NX3-M1600E
Managed Device Version	ADS: • V4.5.88.15.sp13–v4.5.88.15.sp15 • V4.5R89F03–V4.5R89F03SP03 • V4.5R90F00–V4.5R90F00SP05 • V4.5R90F01 NTA: • V4.5.61.2.BF19–V4.5.61.2.BF21 • V4.5R89F03–V4.5R89F03SP02 • V4.5R90F00–V4.5R90F00SP05 • V4.5R90F01
Client	• Internet Explorer 11 • Chrome • Firefox
Other System or Tool	None
Documentation	NSFOCUS ADS M User Guide (V4.5R90F01)

Note:

Make sure that this version is used together with an ADS or NTA version listed in the Managed Device Version row. Otherwise, the collaboration function will be unable to work properly.

New and Optimized Functions

No.	Function Description
1	Presentation of data of more attack types, to adapt to ADS
2	Addition of ports in attack event reports
3	New support for export of HTML reports
4	Addition of the sending interval field for syslog configuration and SNMP configuration under **Administration > Third-Party Interface**
5	Addition of the management interface access control function
6	Local performance alert thresholds valid also for the system status bar
7	Optimization of the user management function by further dividing user privileges

No.	Function Description
8	Addition of traffic-related information to syslog messages

Upgrade and Rollback Paths

ADS M can be upgraded to V4.5R90F01 from V4.5R90F00, V4.5R90F00SP01, V4.5R90F00SP02, or V4.5R90F00SP03.

Note:

After being upgraded to V4.5R90F01, ADS M cannot be rolled back to the source version.

Upgrade Procedure

Make sure that the current ADS M version is **V4.5R90F00**, **V4.5R90F00SP01**, **V4.5R90F00SP02**, or **V4.5R90F00SP03**. If the current version is earlier than any of the preceding ones, ask NSFOCUS technical support to upgrade it to one of them.

To perform the upgrade, follow these steps:

Step 1 Log in to the web-based manager of ADS M.

Step 2 Choose **Administration > Local Settings > System Upgrade**.

The **System Upgrade** page appears.

Step 3 Browse to the upgrade file **update_adsm_V4.5R90F01build20180904.zip**. Then click **Upload**.

Step 4 After the upgrade package is successfully uploaded and the version number is confirmed to be correct, click **OK** to start the installation.

Step 5 After the system informs you that the upgrade is complete, click **OK** to restart the system.

If no message is displayed to indicate installation completion, please wait 3 minutes. Then the system will automatically restart.

Step 6 Refresh the web-based manager. Click **About** in the upper-right corner of the manager to check the current system version.

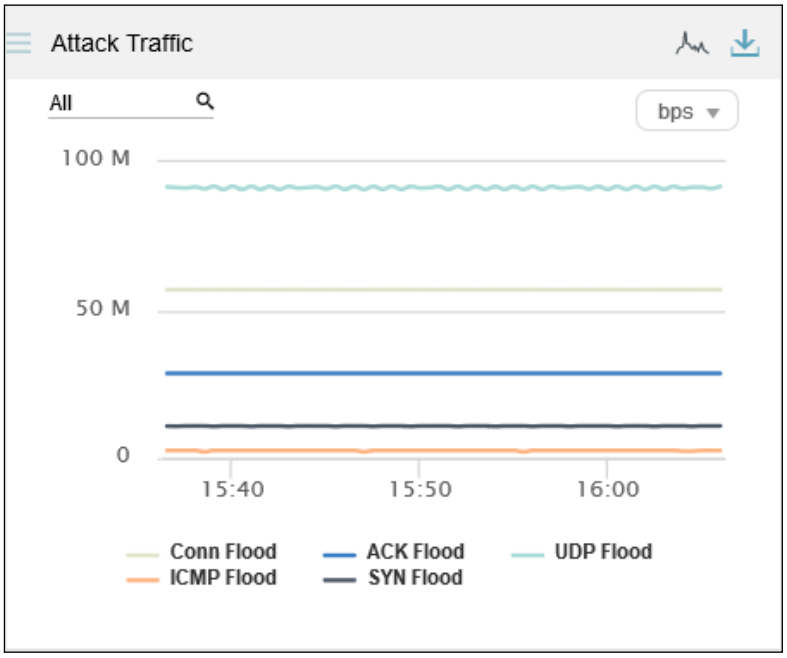
- If Product Version is V4.5R90F01 and Build Date is 20180904, the upgrade succeeded.
- If **Product Version** is not **V4.5R90F01** or **Build Date** is not **20180904**, the upgrade failed. In this case, contact NSFOCUS technical support.

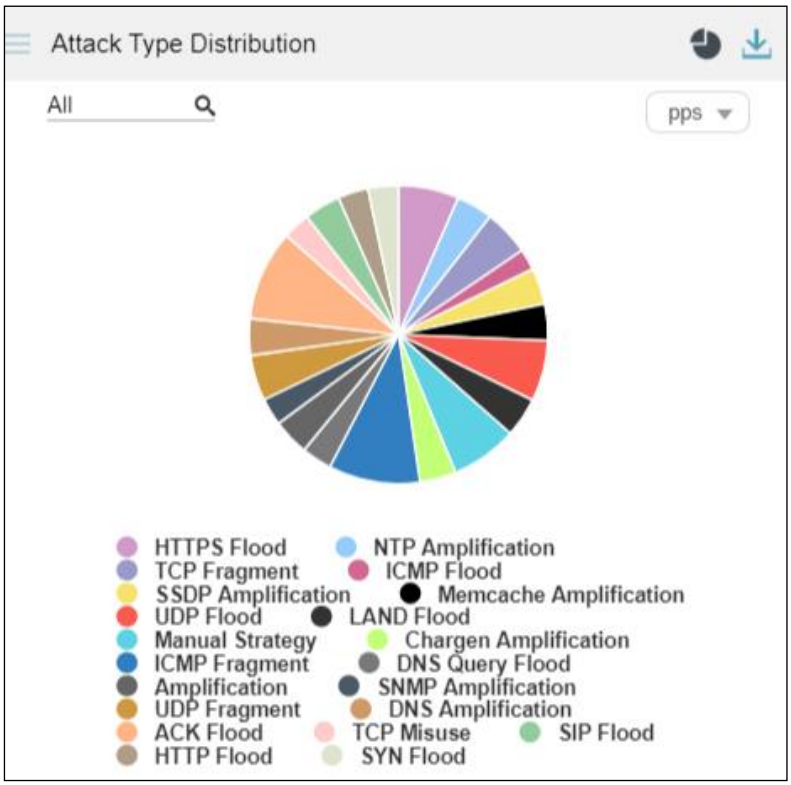
----End

Function Changes

1 Presentation of Data of More Attack Types to Adapt to ADS

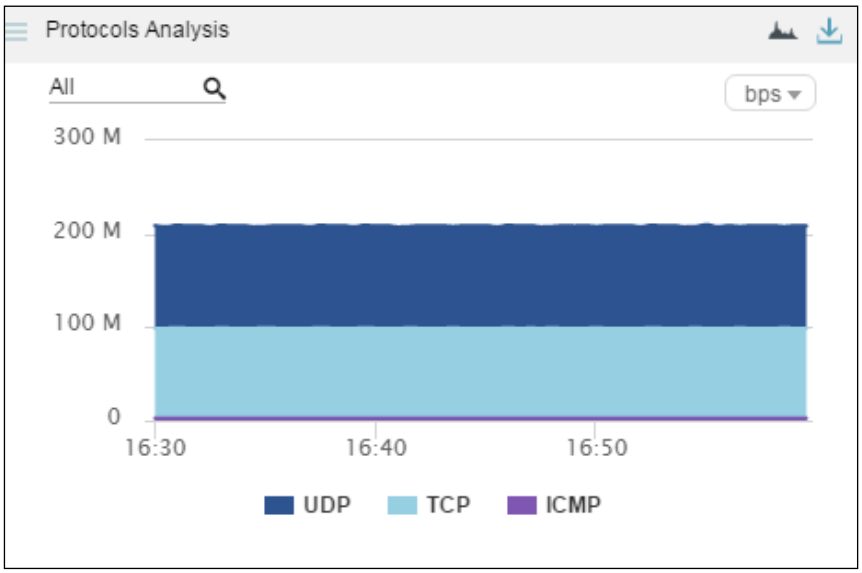
Traffic Monitoring, Reports, Log, and Administration modules are modified to support 25 attack types from the previous six types, to adapt to the new version of ADS. Following are screenshots of two panels from the Traffic Monitoring module.





2 New Support for Export of HTML Reports

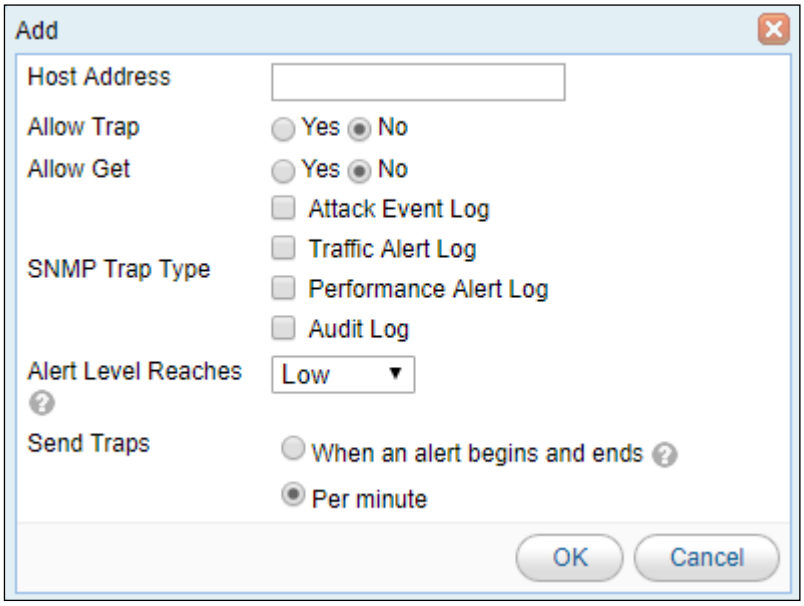
Among earlier versions, some support the export of traffic monitoring data as only an HTML report, and others support export of only PDF reports. In V4.5R90F01, such data can be exported as either a PDF or HTML report. You can point to the download icon in the upper-right corner of a panel and select **PDF** or **HTML** to export a report of the selected format.



3 Addition of the Sending Interval Field for Syslog Configuration and SNMP Configuration Under Administration > Third-Party Interface

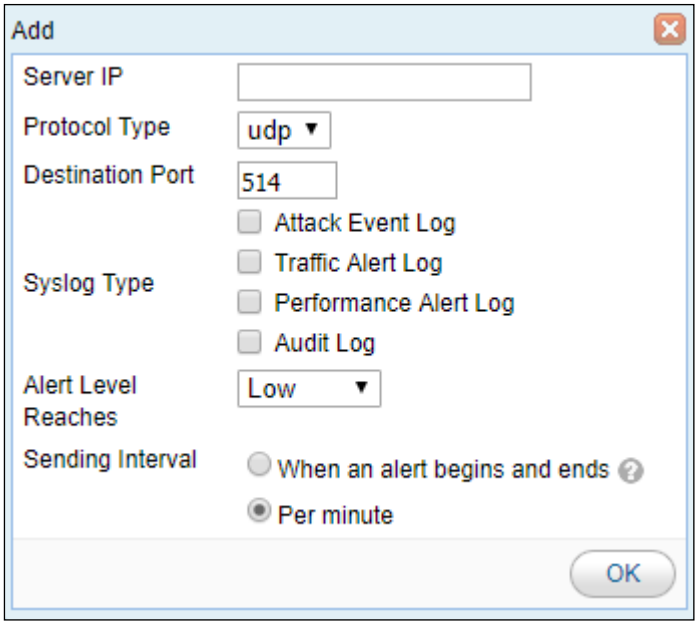
SNMP Configuration

In the SNMP configuration dialog box, **Send Traps** is added to control the interval for sending SNMP traps. The setting of this field works only for attack event logs and traffic alert logs. If **When an alert begins and ends** is selected, an alert is sent via SNMP only when an attack on the same IP address begins and ends. Following is the dialog box for configuring SNMP parameters.



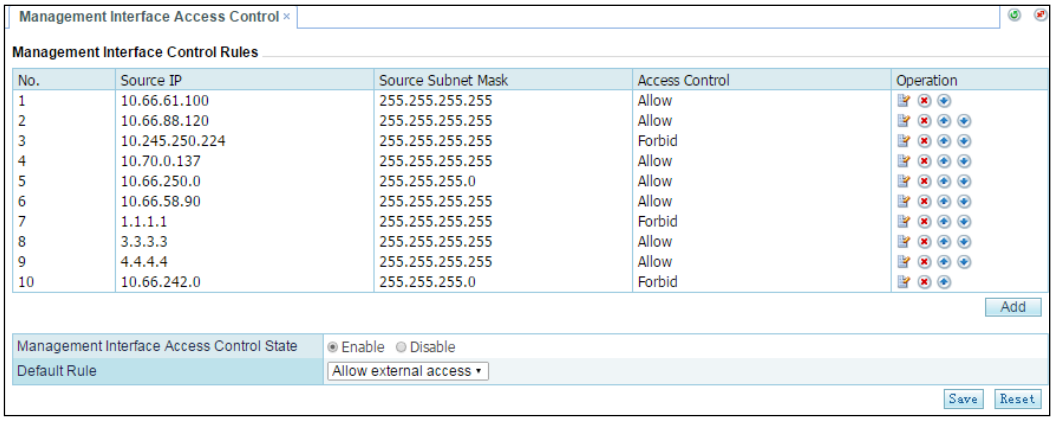
Syslog Configuration

In the syslog configuration dialog box, **Sending Interval** is added to control the interval for sending syslog messages. The setting of this field works only for attack event logs. If **When an alert begins and ends** is selected, an alert is sent via syslog only when an attack on the same IP address begins and ends. Following is the dialog box for configuring syslog parameters.



4 Addition of the Management Interface Access Control Function

This function allows users to specify which IP addresses are to be allowed or denied access to ADS M, whether via web, Telnet, SSH, or ping. The following figure shows the page for configuring this function.



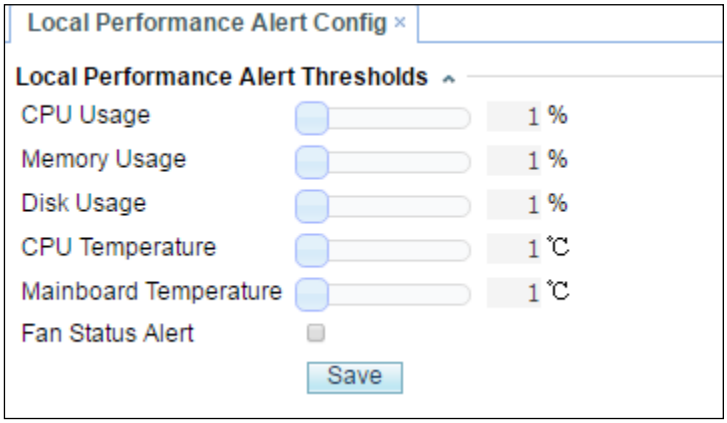
5 Local Performance Alert Thresholds Valid Also for the System Status Bar

This function is enhanced as follows from the previous version:

- The range of the CPU usage threshold, memory usage threshold, disk usage threshold, CPU temperature threshold, and mainboard temperature threshold is changed to 1% to 100%.
- The fan status alert switch is added.

In addition, settings configured (except the fan status alert setting) under **Administration > Local Settings > Local Performance Alert Config** work also for the system status bar in the lower-right corner of the window.

The following figure shows the **Local Performance Alert Thresholds** page.



6 Optimization of the User Management Function by Further Dividing User Privileges

The user management page remains unchanged.

Currently, users are divided into four types: system administrator, device configuration administrator, region administrator, and auditor. The following table lists privileges of each user role.

User Role	Privilege
Region administrator	Has access to the region module.
Device configuration administrator	Has access to the device management module.
Auditor	Has access to the device log module.
System administrator	Has access to the region, device management, traffic monitoring, system management, device log, and report modules.

Whether the device configuration administrator, region administrator, and auditor can view traffic monitoring data and reports depends on the system administrator's configuration (by enabling the access key or not) under **Administration > User and Audit > User Management**.