1 Basic Information

Product Model	• ADS NX3-800E • ADS NX3-2020E • ADS NX5-4020E • ADS NX5-6025E • ADS NX5-HD1000 • ADS NX5-HD5000 • ADS NXT-HD6000 • ADS NX3-HD2500 • ADS NX5-HD4500 • ADS NX5-HD6500 • ADS NX5-HD8500 • ADS NX5-8000 • ADS NX5-10000 • ADS NX5-12000 • ADS NX1-VN01
Software Version	V4.5R90F04
Upgrade File	update_ADS_x86_V4.5R90F04_20220930.zip
MD5	b6cf8ef722cf6981b569886942fba077
SHA256SUM	499c75516331950fee7a6240e2d46086026c551c09dc4e521862aabcc04ca04c
How to Obtain	Contact NSFOCUS technical support.

2 Version Mapping

Source Software Version	V4.5R90F04
Product Model	• NSF1100-1 • NSF1100-3 • NSF2800-2 • NSF2800-6 • NSF3600-4 • NSP-7224B • NSP-7124A • NSP-71C2A • NSP-72C2A • HTCA-6U • NX1-VN
Network Traffic Analyzer Platform	NTA V4.5R90F04
Management Platform Version	ADS M V4.5R90F04
Client Software	None
Other System or Tool	None
Documentation	*NSFOCUS ADS User Guide* (V4.5R90F04)

3 Function Changes

Applicable device models:

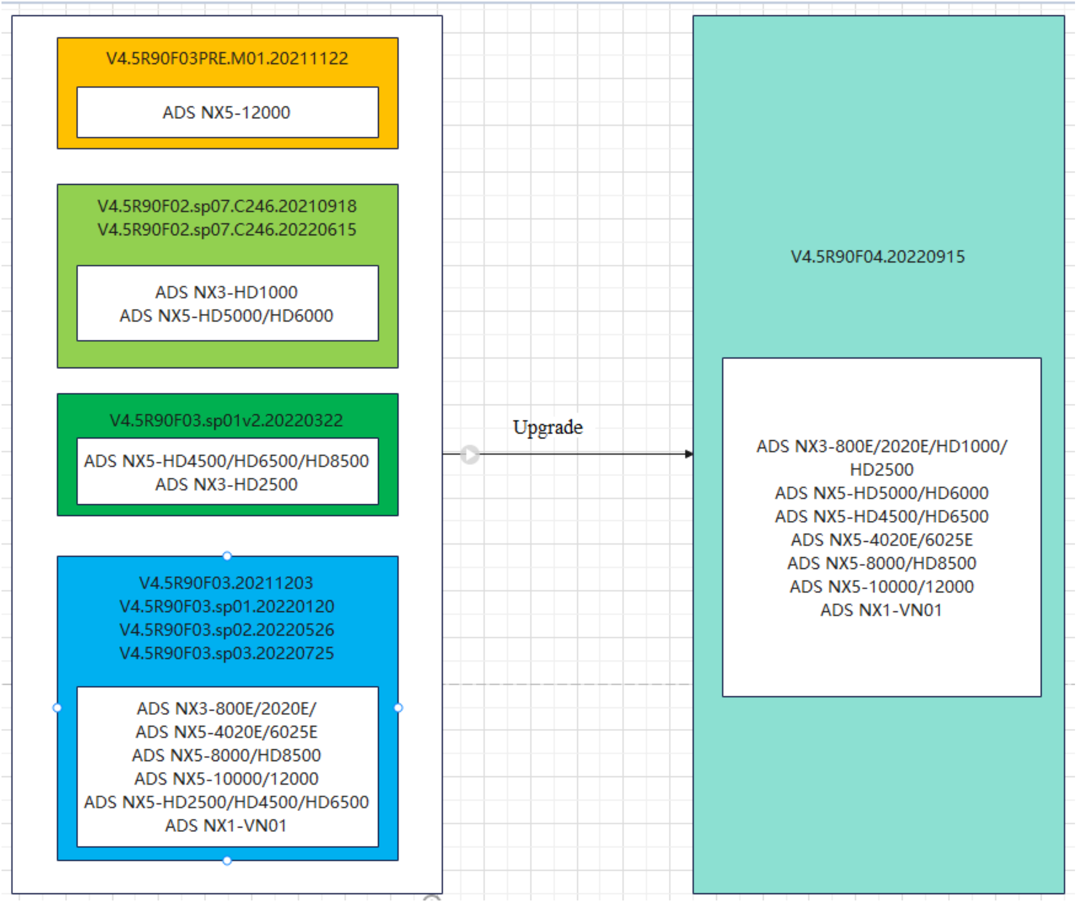
- ADS NX3-800E/2020E/HD1000/HD2500
- ADS NX5-4020E/6025E/HD4500/HD6500/HD8500/HD5000/HD6000
- ADS NX5-8000
- ADS NX5-10000/12000
- ADS NX1-VN01

3.1 Support for Hardware Platforms

V4.5R90F04 inherits the uniform platform support feature from V4.5R90F03. In other words, a software version supports all hardware platforms.

For ADS NX3-800E/2020E, NX5-4020E/6025E, NX3-HD2500/NX5-HD4500/NX5-HD6500/NX5-HD8500, NX5-8000/10000/12000, and NX1-VN0, you need to first upgrade them to V4.5R90F03 or one of its SP versions (V4.5R90F03.20211203, V4.5R90F03.sp01.20220120, V4.5R90F03.sp02.20220526, or V4.5R90F02.sp03.20220725) before upgrading to V4.5R90F04.

For ADS NX3-HD1000/NX5-HD5000/NX5-HD6000, you can directly upgrade them from the current version (V4.5R90F02.sp07.C246) to V4.5R90F04.



3.2 Function Changes

3.2.1 New Functions

Function	Description
Common UDP watermark algorithm	The common UDP watermark algorithm is added for protection groups under **Policy** > **Anti-DDoS** > **Protection Groups**.
Group-specific ACL rule	The ACL rule can be configured specific to a protection group under **Policy** > **Anti-DDoS** > **Protection Groups**.
Group-specific NTI policy	The NTI policy can be configured specific to a protection group under **Policy** > **Anti-DDoS** > **Protection Groups**.
Chassis system resources	For a rack-mounted device, its chassis system resources and service board resources are now displayed under **Real-Time Monitoring** > **System Resources**.
Web API logs	Web API logs are provided to display logs generated by other devices calling ADS's web API under **Logs** > **System Logs**.
License expiration warning	A popup window is displayed when the license is about to expire or has expired.

Function	Description
Undeletable system logs	System logs cannot be deleted to ensure data security.
MAC address configuration optimization	The static and valid MAC addresses are displayed separately under **Diversion & Injection** > **Traffic Injection** > **MAC Address Table.** The MAC addresses can be dynamically learned or statically configured, as shown in the **Status** column.
Optimized protection algorithm for ACL rules	The underlying implementation of the global ACL is refactored with optimized ACL algorithms to improve the performance.
Global NTI policy optimization	The global NTI policy is optimized by upgrading threat intelligence CBB to provide richer threat intelligence data.
Default ACK algorithm	The default ACK algorithm for the **_default** and **__web_server** protection group policy templates and the default protection group is changed to ACK check algorithm.
HA implementation between 800E and HD1000 models	The HA configuration can be implemented between the 800E and HD1000 devices.

3.2.2 Optimized Functions in V4.5R90F04 After Upgrade from V4.5R90F03

The following table lists functions optimized in V4.5R90F04 compared with V4.5R90F03.

Function	V4.5R90F03	V4.5R90F04	Impact
Log management	System logs can be directly cleared on the web-based manager.	The **Clear** button is removed, and system logs cannot be deleted.	None.
Global ACL rule	--	The underlying layer of ACL rules is refactored.	The ACL rules can be configured specific to a protection group. Also, the earlier implementation is refactored to improve the processing performance.
Global NTI policy	--	The NTI CBB is upgraded to separate download from query and provide more information.	Through global NTI, you can obtain and search for more information. You can also configure IP exceptions that will not be checked against the intelligence database.
New ACK algorithm for the **_default** and **_web_server** protection group policy templates	By default, the ACK protection algorithm is **Disable**.	The default ACK protection algorithm is changed to ACK check.	After the ACK protection algorithm is changed to ACK check, the impact of using the default ACK algorithm on ACK packets can be reduced.

3.3 Description of Major Function

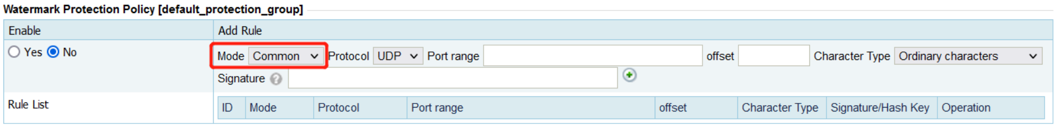
3.3.1 Common UDP Watermak Algorithm

Function Description

A UDP protection policy mostly limits the number of UDP fragments to each destination IP address that can pass through ADS per second. For UDP packets with identifiable attack signatures, configuring a patten matching rule is complex. Besides, this global rule will somewhat impact the performance. To protect these UDP packets, this version supports a common UDP watermark algorithm that allows fast configuration of a rule to match a string of ordinary or hexadecimal signature characters. The algorithm only works on the current protection group, and provides better performance than pattern matching rules.

Related Pages

Choose **Policy** > **Anti-DDoS** > **Protection Groups** and click ✎ in the **Protection Policy** column to configure a watermark protection policy.



Watermark Protection Policy [default_protection_group]

Enable: ○ Yes ● No

Add Rule: Mode Common Protocol UDP Port range offset Character Type Ordinary characters

Signature ? ⊕

Rule List

ID	Mode	Protocol	Port range	offset	Character Type	Signature/Hash Key	Operation

- Choose **Common** for **Mode** to configure a common watermark algorithm rule.
- Click the icon ⊕ to add a rule.

Notes

Click the icon ? next to **Signature** to check the requirements of signatures.

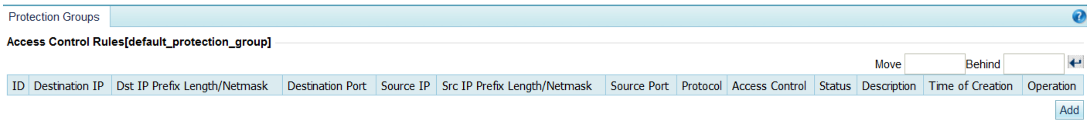
3.3.2 Group-Specific ACL Rule

Function Description

As the global ACL rules are not particularly applicable to some scenarios, an access control role can be configured specific to protection groups for more refined control. In addition, the underlying implementation of the ACL rules has been refactored, thus significantly improving its performance. A group-specific access control rule supports port ranges and re-sorting. However, the **Invert** operation does not work here.

Related Pages

Choose **Policy** > **Anti-DDoS** > **Protection Groups** and click ✎ in the **Protection Policy**. Click **Next** to configure an access control rule.



Protection Groups

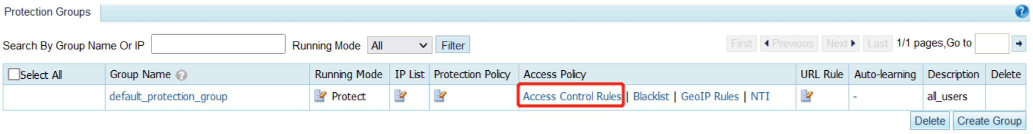
Access Control Rules[default_protection_group]

Move Behind

ID	Destination IP	Dst IP Prefix Length/Netmask	Destination Port	Source IP	Src IP Prefix Length/Netmask	Source Port	Protocol	Access Control	Status	Description	Time of Creation	Operation

Add

Or, choose **Policy** > **Anti-DDoS** > **Protection Groups** and click **Access Control Rules** under **Access Policy**.


Protection Groups

Search By Group Name Or IP [ ] Running Mode All Filter First Previous Next Last 1/1 pages,Go to

☐Select All	Group Name	Running Mode	IP List	Protection Policy	Access Policy	URL Rule	Auto-learning	Description	Delete
	default_protection_group	Protect	✎	✎	Access Control Rules | Blacklist | GeoIP Rules | NTI	✎	-	all_users	

Delete Create Group

Notes

- One protection group supports a maximum of 20 group-specific access control rules.
- The destination IP of 0.0.0.0 matches all IP addresses in the group.

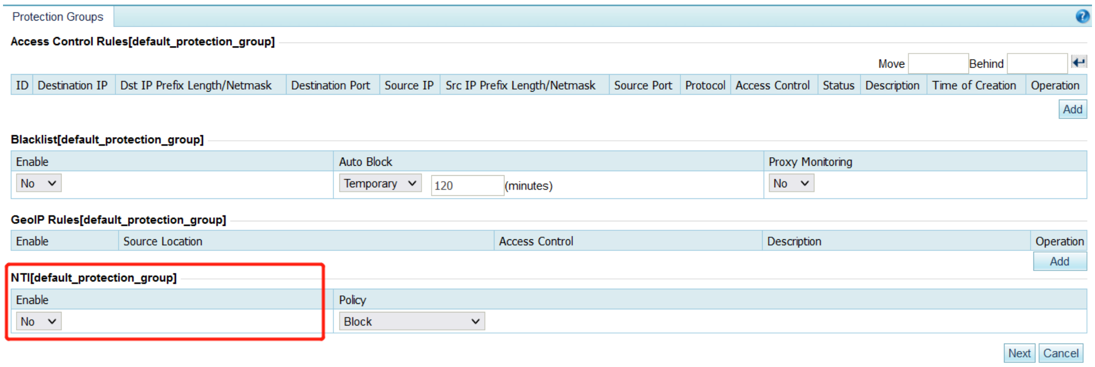
3.3.3 Group-specific NTI

Function Description

After the group blocklist ("blacklist" on the UI) is added in V4.5R90F03, the group-specific NTI is supported in this version. To use this feature, set **Protection Scope** to **Group** under **Advanced** > **NTI** > **NTI Configuration**, and then control whether to enable it in the group. The group-specific NTI policy supports **Traffic Control by Dst IP** and **Block** to minimize the impact. The group-specific NTI can better defend attacks that are insusceptible to algorithm protections.

Related Pages

Choose **Policy** > **Anti-DDoS** > **Protection Groups** and click ✎ in the **Protection Policy**. Click **Next** to set group-specific NTI.


Protection Groups

Access Control Rules[default_protection_group]

Move [ ] Behind [ ]

ID	Destination IP	Dst IP Prefix Length/Netmask	Destination Port	Source IP	Src IP Prefix Length/Netmask	Source Port	Protocol	Access Control	Status	Description	Time of Creation	Operation

Add

Blacklist[default_protection_group]

Enable	Auto Block	Proxy Monitoring
No	Temporary 120 (minutes)	No

GeoIP Rules[default_protection_group]

Enable	Source Location	Access Control	Description	Operation

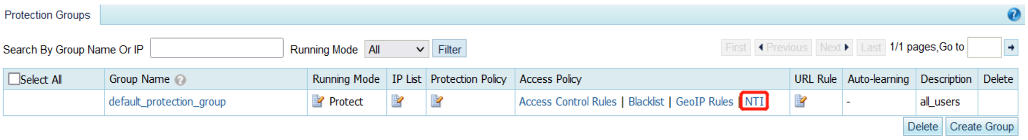
Add

NTI[default_protection_group]

Enable	Policy
No	Block

Next Cancel

Or, choose **Policy** > **Anti-DDoS** > **Protection Groups** and click **NTI** under **Access Policy**.


Protection Groups

Search By Group Name Or IP [ ] Running Mode All Filter First Previous Next Last 1/1 pages,Go to

☐Select All	Group Name	Running Mode	IP List	Protection Policy	Access Policy	URL Rule	Auto-learning	Description	Delete
	default_protection_group	Protect	✎	✎	Access Control Rules | Blacklist | GeoIP Rules | NTI	✎	-	all_users	

Delete Create Group

Notes

The NTI settings work for this group only when global NTI is enabled and the **Protection Scope** is set to **Group** under **Advanced** > **NTI** > **NTI Configuration**.

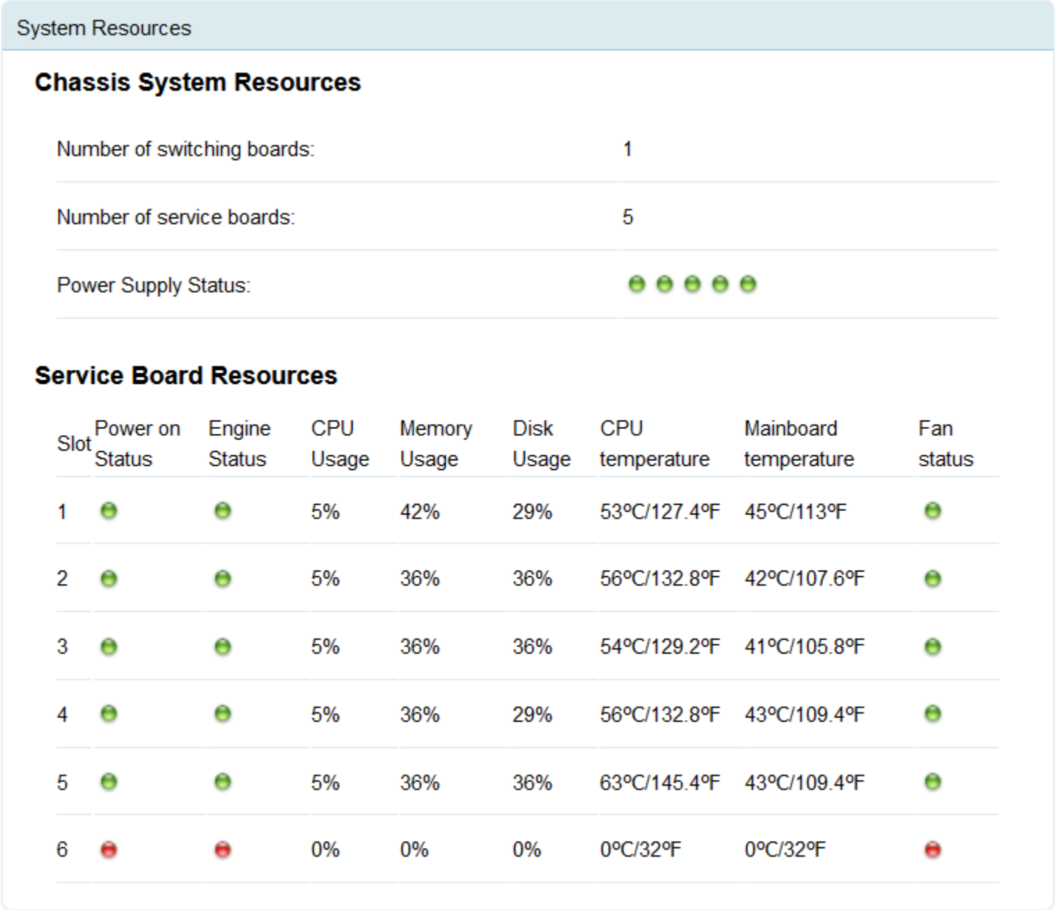
3.3.4 Chassis Health Check

Function Description

For a rack-mounted device, its overall chassis information, including its service board resources usage, is invisible on the web-based manager. Now, the chassis health check visually displays the overall information of rack-mounted devices, including the service board resource usage and engine status, to effectively help troubleshooting. Currently, ADS-1000 and ADS-12000 are rack-mounted devices.

Related Pages

Choose **Real-time Monitoring** > **System Resources**.



System Resources

Chassis System Resources

Number of switching boards:	1
Number of service boards:	5
Power Supply Status:	🟢 🟢 🟢 🟢 🟢

Service Board Resources

Slot	Power on Status	Engine Status	CPU Usage	Memory Usage	Disk Usage	CPU temperature	Mainboard temperature	Fan status
1	🟢	🟢	5%	42%	29%	53ºC/127.4ºF	45ºC/113ºF	🟢
2	🟢	🟢	5%	36%	36%	56ºC/132.8ºF	42ºC/107.6ºF	🟢
3	🟢	🟢	5%	36%	36%	54ºC/129.2ºF	41ºC/105.8ºF	🟢
4	🟢	🟢	5%	36%	29%	56ºC/132.8ºF	43ºC/109.4ºF	🟢
5	🟢	🟢	5%	36%	36%	63ºC/145.4ºF	43ºC/109.4ºF	🟢
6	🔴	🔴	0%	0%	0%	0ºC/32ºF	0ºC/32ºF	🔴

Notes

None.

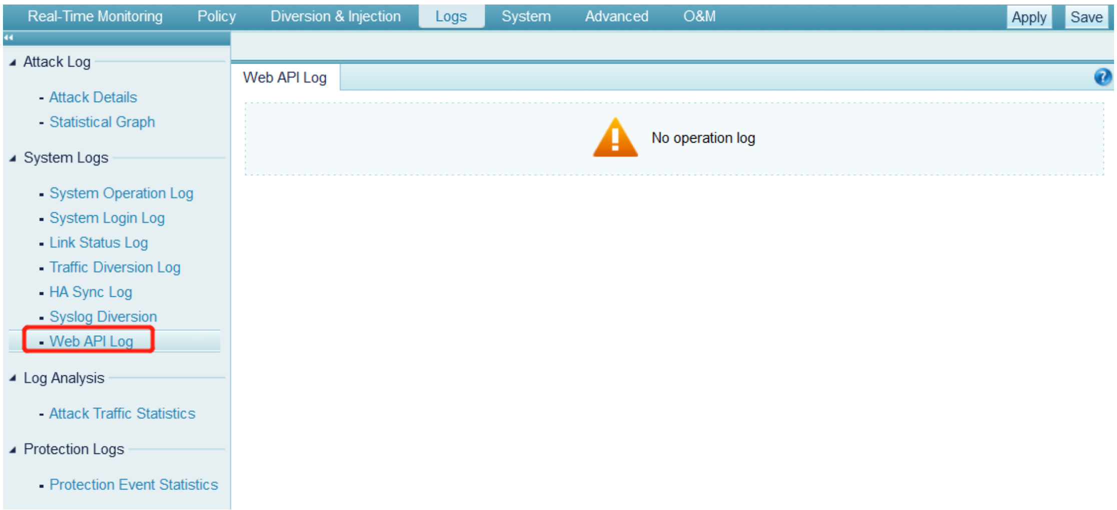
3.3.5 WEB API Logs

Function Description

ADS provides web APIs that third-party devices and ADS M can call to obtain device information and perform configurations. However, these configuration operations are untraceable because no logs are recorded. In this version, web API logs generated by calling ADS's web APIs to configure devices are displayed to enhance security and effectively help troubleshooting. If ADS M is configured, web API logs are also uploaded to ADS M for saving.

Related Pages

Choose **Logs** > **System Logs** > **Web API Log**.



No operation log

Notes

None.

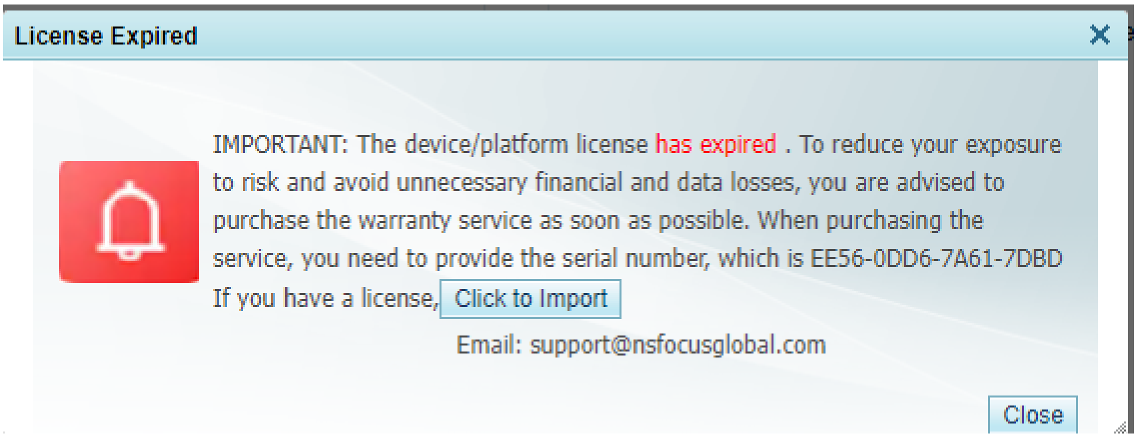
3.3.6 License Expiration Warning

Function Description

The anti-DDoS and software update services of ADS are subject to a license. After expiration, these functions will stop working, affecting DDoS protection and system upgrades. After login to ADS, users will see a popup window prompting when the license is about to expire or has expired. You can set a period during which you will not be reminded again. Click **Buy Now** to renew your license.

Related Pages

None. The popup window is automatically displayed based on the validity period of the license. The popup window is shown as follows:



IMPORTANT: The device/platform license has expired . To reduce your exposure to risk and avoid unnecessary financial and data losses, you are advised to purchase the warranty service as soon as possible. When purchasing the service, you need to provide the serial number, which is EE56-0DD6-7A61-7DBD If you have a license,

Email: support@nsfocusglobal.com

Notes

None.

3.3.7 Undeletable System Logs

Function Description

In previous versions, system logs can be cleared on the web-based manager. This may cause security risks and difficulties in troubleshooting. In this version, the **Clear** button is removed, and system logs cannot be deleted for security reasons.

Related Pages

None.

Notes

None.

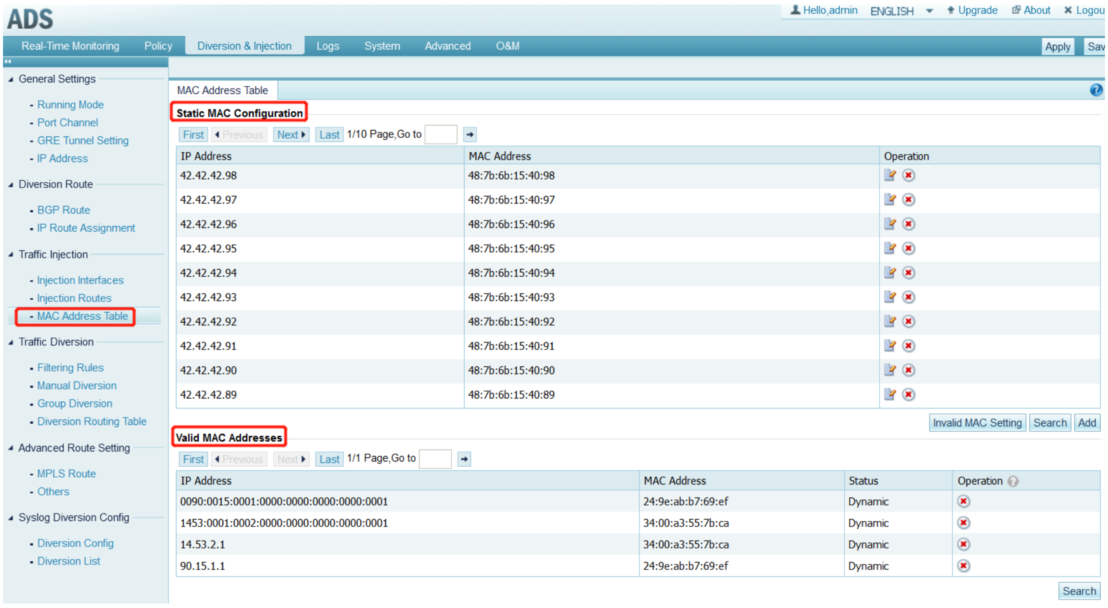
3.3.8 MAC Address Configuration Optimization

Function Description

In V4.5R90F04, the static and valid MAC address lists are separately displayed. Valid MAC addresses can be dynamically learned or statically configured, as shown in the **Status** column.

Related Pages

Choose **Diversion & Injection** > **Traffic Injection** > **MAC Address Table**.



Static MAC Configuration

1/10 Page,Go to

IP Address	MAC Address	Operation
42.42.42.98	48:7b:6b:15:40:98	
42.42.42.97	48:7b:6b:15:40:97	
42.42.42.96	48:7b:6b:15:40:96	
42.42.42.95	48:7b:6b:15:40:95	
42.42.42.94	48:7b:6b:15:40:94	
42.42.42.93	48:7b:6b:15:40:93	
42.42.42.92	48:7b:6b:15:40:92	
42.42.42.91	48:7b:6b:15:40:91	
42.42.42.90	48:7b:6b:15:40:90	
42.42.42.89	48:7b:6b:15:40:89	

Valid MAC Addresses

1/1 Page,Go to

IP Address	MAC Address	Status	Operation
0090:0015:0001:0000:0000:0000:0000:0001	24:9e:ab:b7:69:ef	Dynamic	
1453:0001:0002:0000:0000:0000:0000:0001	34:00:a3:55:7b:ca	Dynamic	
14.53.2.1	34:00:a3:55:7b:ca	Dynamic	
90.15.1.1	24:9e:ab:b7:69:ef	Dynamic	

Notes

None.

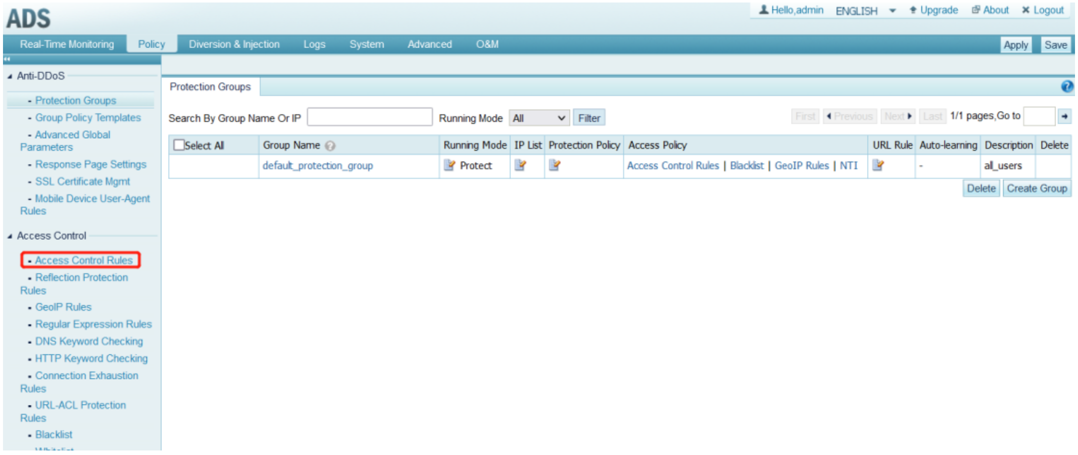
3.3.9 Global Access Control Rules Optization

Function Description

The global access control rule remains the same on the web-based manager, but its underlying implementation is refactored to improve the performance. Since V4.5R90F04, the maximum number of access control rules allowed is 1000.

Related Pages

Choose **Policy** > **Access Control** > **Access Control Rules**.



Search By Group Name Or IP
Running Mode All

1/1 pages,Go to

□Select All	Group Name	Running Mode	IP List	Protection Policy	Access Policy	URL Rule	Auto-learning	Description	Delete
	default_protection_group	Protect			Access Control Rules | Blacklist | GeoIP Rules | NTI		-	all_users	

Notes

Upgrading to V4.5R90F04 may fail if the total number of access control rules exceed 1,000. Delete some rules, and maintain the total number within 1,000 to ensure a successful upgrade.

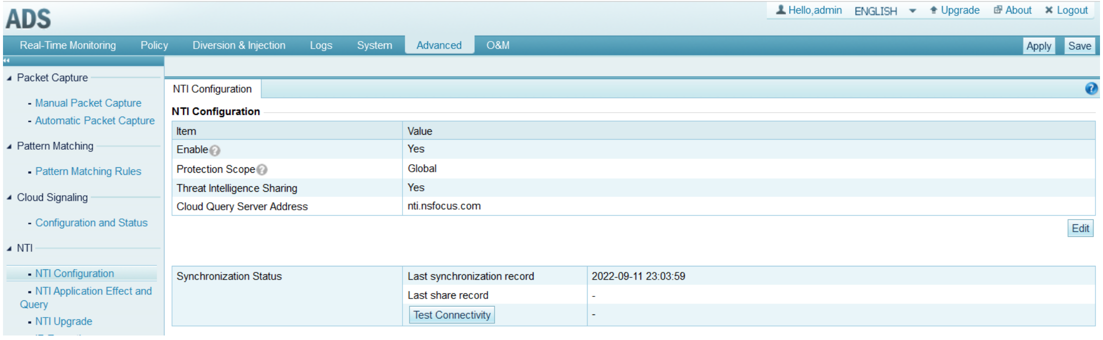
3.3.10 Global NTI Optimization

Function Description

ADS can collaborate with NTI to block high-risk IP addresses. To ensure data reliability, ADS supports daily NTI upgrades and optional upgrade periods. In the case of false blocks, you can configure an IP exception list that will not be subject to checks by ADS's NTI-based protection algorithms, but still filtered by other protection policies. Additionally, users can query the local or cloud-side database for the intelligence of an IP address, and import an offline threat intelligence upgrade package. Currently, only B-Package Indicator from NSFOCUS upgrade site can be downloaded for offline import. For refined control of destination IP addresses, you can set the **Protection Scope** to **Group**. NTI can be configured to be valid globally or for specific groups.

Related Pages

Choose **Advanced** > **NTI** > **NTI**.

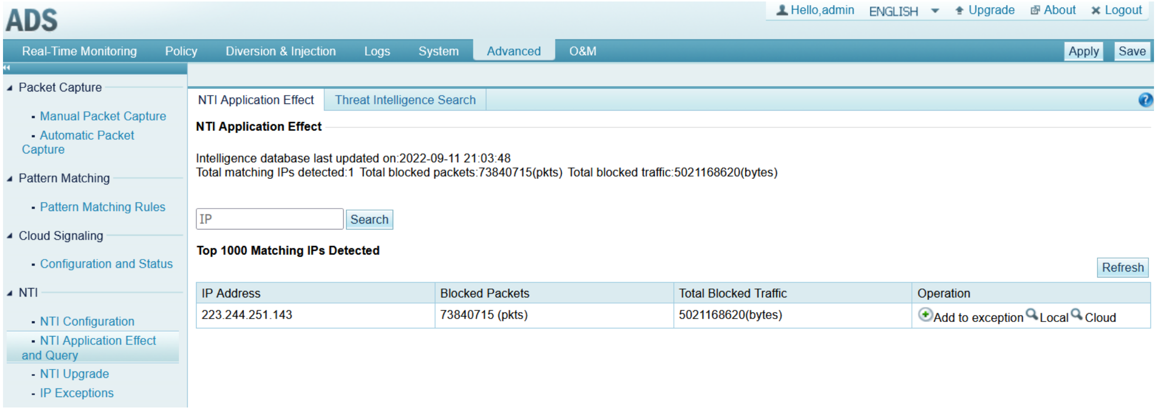


NTI Configuration

Item	Value
Enable	Yes
Protection Scope	Global
Threat Intelligence Sharing	Yes
Cloud Query Server Address	nti.nsfocus.com

Synchronization Status	Last synchronization record	2022-09-11 23:03:59
	Last share record	-
	Test Connectivity	-

- **Enable**: controls whether to enable the NTI function. The NIT function is available only after it is enabled.
- **Protection Scope**: specifies whether the function is valid globally or for specific groups.
- **Threat Intelligence Sharing**: controls whether to enable the intelligence sharing function to share the local threat intelligence to the cloud.
- **Cloud Query Server Address**: specifies a domain in China (nti.nsfocus.com) or outside of China (nti.nsfocusglobal.com) for query of intelligence data of an IP address.



NTI Application Effect

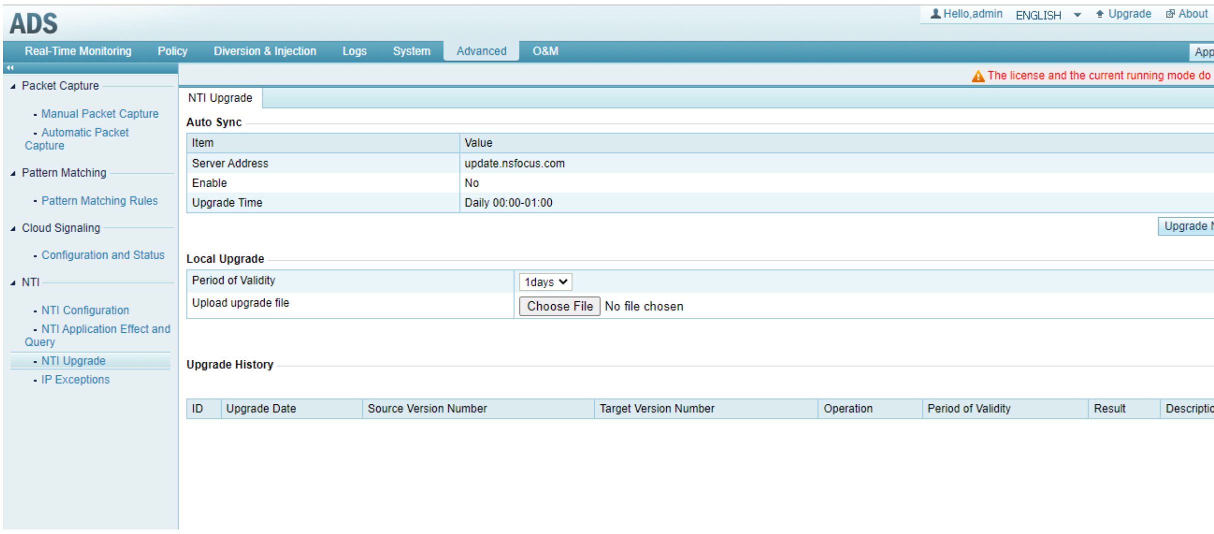
Intelligence database last updated on:2022-09-11 21:03:48
Total matching IPs detected:1 Total blocked packets:73840715(pkts) Total blocked traffic:5021168620(bytes)

IP

Top 1000 Matching IPs Detected

IP Address	Blocked Packets	Total Blocked Traffic	Operation
223.244.251.143	73840715 (pkts)	5021168620(bytes)	Add to exception Local Cloud

The **NTI Application Effect** page displays information about IP addresses that have been blocked because of having a match in the intelligence database. You can query the intelligence data of an IP address on the **Threat Intelligence Search** page.



The license and the current running mode do

Auto Sync

Item	Value
Server Address	update.nsfocus.com
Enable	No
Upgrade Time	Daily 00:00-01:00

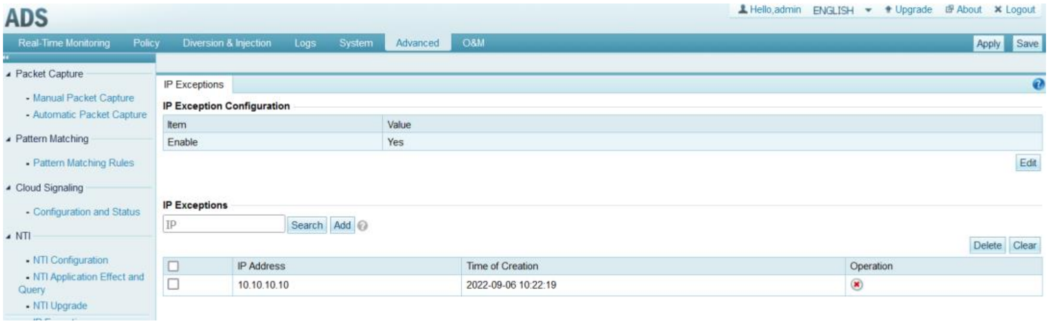
Local Upgrade

Period of Validity	1days
Upload upgrade file	Choose File No file chosen

Upgrade History

ID	Upgrade Date	Source Version Number	Target Version Number	Operation	Period of Validity	Result	Descriptio

On the **NTI Upgrade** page, you can enable or disable automatic synchronization, and import an offline intelligence package.



IP Exception Configuration

Item	Value
Enable	Yes

IP Exceptions

IP

□	IP Address	Time of Creation	Operation
□	10.10.10.10	2022-09-06 10:22:19	☒

After this is enabled, IP addresses or IP segments included in the IP exception list will not be subject to checks by ADS's NTI-based protection algorithms.

Notes

- After the NTI function is enabled on the **NTI Configuration** page, you need to enable automatic synchronization on the **NTI Upgrade** page to automatically download intelligence data. If not, import an offline intelligence package when necessary.
- Both the automatically downloaded and locally upgraded intelligence databases have an effective duration. By default, the former remains effective for 24 hours, while that of the latter is configurable.
- The NTI function is available for use only after being purchased.

3.3.11 Update of Default ACK Algorithm

Function Description

By default, the ACK protection algorithm for the **_default** and **_web_server** protection group policy templates is **Disable**, which directly drops ACK packets that match the algorithm. This may affect business traffic when the default setting is not modified. In this version, the default ACK algorithm for these protection group policy templates and for the **default_protection_group** protection group is changed to ACK check algorithm.

Related Pages

None.

Notes

None.

3.3.12 HA Implementation Between 800E and HD1000 Devices

Function Description

This version is applicable to three new product models, including HD1000, HD5000, and HD6000. These modules can be directly upgraded to V4.5R90F04. Because of their similar protection ability, the in-path HA deployment can be implemented between 800E and HD1000 devices.

Related Pages

None.

Notes

None.

3.3.13 WebAPIs are Updated

Function Description

Web APIs are updated, involving the defenderGroup module (load, add, setup, sync, and sync_url actions), the defenderGroupTemplate module (load, add, setup, and sync actions), and the NTI module (all actions)..

Related Pages

None.

Notes

None.

3.3.14 An expired license cannot be imported to V4.5R90F04

Function Description

An expired license cannot be imported to V4.5R90F04. When importing an expired license, you will be prompted that the import fails due to expiration of the license.

Related Pages

None.

Notes

None.

4 Compatiable NTA Versions

ADS can collaborate with NTA 4.5R90F04 for IPv4 and IPv6.

5 Supported Broswer Versions

You are advised to use an Edge, Chrome, or Firefox browser.

6 Upgrade

Target Version

V4.5R90F04

Source Versio

- V4.5R90F02.sp07.C246.20210918
- V4.5R90F02.sp07.C246.20220615
- V4.5R90F03.20211203
- V4.5R90F03PRE.M01.20211122
- V4.5R90F03.sp01.20220120
- V4.5R90F03.sp01v2.20220322
- V4.5R90F03.sp02.20220526
- V4.5R90F03.sp03.20220725

Applicable Device Modes

- ADS NX3-800E
- ADS NX3-2020E
- ADS NX5-4020E
- ADS NX5-6025E
- ADS NX3-HD1000
- ADS NX5-HD5000
- ADS NX5-HD6000
- ADS NX3-HD2500
- ADS NX5-HD4500
- ADS NX5-HD6500
- ADS NX5-HD8500
- ADS NX5-8000
- ADS NX5-10000
- ADS NX5-12000
- ADS NX1-VN01

Upgrade Procedure

The upgrade to V4.5R90F04 must be performed in strict accordance with the following procedure:

Step 1 Choose **System > Local Settings > Configuration File Management**. In the **Configuration File** area, click **Export** to save the exported configuration file to a local disk drive.

Step 2 Install the patch package, **update_ADS_x86_V4.5R90F04_20220930.zip** (MD5: b6cf8ef722cf6981b569886942fba077) on ADS V4.5R90F03.

When the system displays a message, prompting an upgrade success, restart the device.

Step 3 Verify that the system version turns to **V4.5R90F4** in the status bar of the web-based manager.

----End

Note: If the upgrade fails, please contact NSFOCUS technical support.

7 Rollback

Source Version

V4.5R90F04

Target Version

- V4.5R90F03
- V4.5R90F03.sp0x

Applicable Device Modes

- ADS NX3-800E
- ADS NX3-2020E
- ADS NX5-4020E
- ADS NX5-6025E
- ADS NX3-HD1000
- ADS NX5-HD5000
- ADS NX5-HD6000
- ADS NX3-HD2500
- ADS NX5-HD4500
- ADS NX5-HD6500
- ADS NX5-HD8500
- ADS NX5-8000
- ADS NX5-10000
- ADS NX5-12000
- ADS NX1-VN01

Rollback Method

To roll back the version, run the **update rollback** command in the CLI window. If the rollback succeeds, the device automatically restarts. After the restart, the device rolls back to the previous version.