Release Notes

Basic Information

Product Name	ADS NX3-M1600E
Software Version	V4.5R90F00
Upgrade File	update_adsm_V4.5R90F00build20171218.zip (MD5: 047d0ac4475b3922234cfbc86a225deb)
Image File	2018-01-10
Release Date	Contact NSFOCUS technical support.

Version Mapping

Source Software Version	• V4.5R89F03 • V4.5R89F03SP01 • V4.5R89F03SP02
Product Model	ADS NX3-M1600E
Managed Device Version	• ADS: V4.5.88.15.sp13 V4.5.88.15.sp14 V4.5R89F03 through V4.5R89F03SP03 V4.5R90F00 • NTA: V4.5.61.2.BF19 through V4.5.61.2.BF21 V4.5R89F03 through V4.5R89F03SP02 V4.5R90F00
Client	Internet Explorer 11, Chrome, or Firefox browser
Other System or Tool	None
Documentation	NSFOCUS ADS M User Guide (V4.5R90F00)

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.

Requirement List

No.	Requirement Description
1	Statistics of NTA-reported data are collected and displayed.
2	The report module is optimized.
3	The device management mode is optimized.
4	An option of login authentication via verification codes is added.
5	IP addresses that are locked due to too many login failures can be manually unlocked.
6	Upgrade notes are recorded for viewing after upgrade.
7	An SSL certificate can be imported on ADS M for login to ADS Portal.
8	Regions can be dispatched to multiple NTA devices simultaneously.

Upgrade and Rollback Paths

ADS M can be upgraded to V4.5R90F00 from V4.5R89F03, V4.5R89F03SP01, or V4.5R89F03SP02.

Note:

After being upgraded to V4.5R890F00, ADS M cannot be rolled back to the source version.

Upgrade Procedure

Make sure that the current ADS M version is V4.5R89F03, V4.5R89F03SP01, or V4.5R89F03SP02. If the current version is an earlier version, ask technical support personnel of NSFOCUS to upgrade it to V4.5R89F03, V4.5R89F03SP01, or V4.5R89F03SP02.

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_V4.5R90F00build20171218.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 installation is complete, click **OK** to restart the system service.

If no message is displayed indicating that the installation is complete, please wait 3 minutes. Then the system service 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.

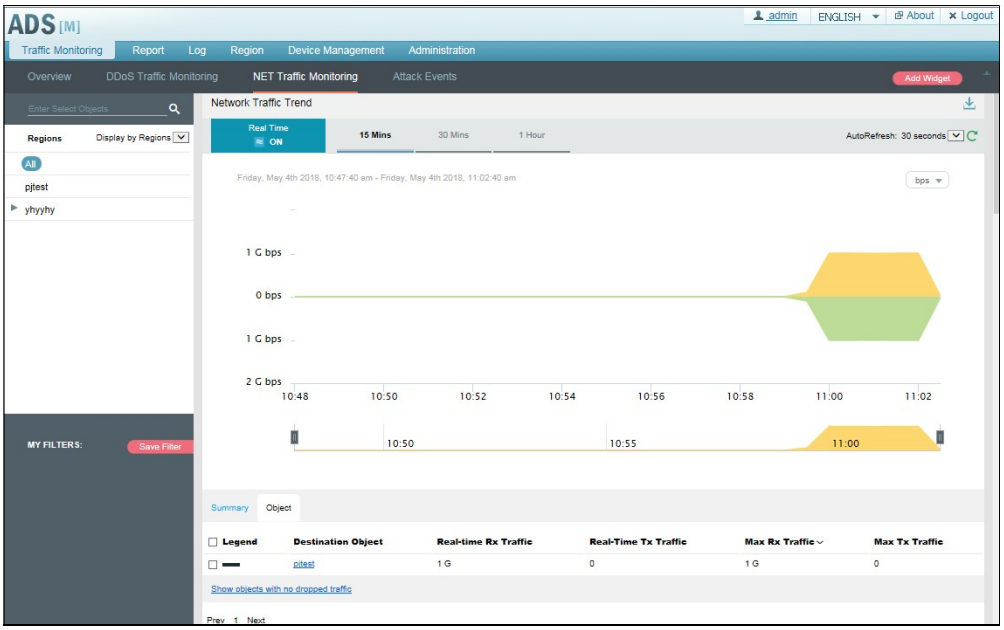
- If **Product Version** is **V4.5R90F00** and **Build Date** is **20171218**, the upgrade succeeded.
- If **Product Version** is not **V4.5R90F00** or **Build Date** is not **20171218**, the upgrade failed. In this case, contact NSFOCUS technical support.

----End

Function Changes

1 Statistics of NTA-Reported Data Are Collected and Displayed

The **NET Traffic Monitoring** tab page is added under **Traffic Monitoring**. All data on this tab page, whether current or historical, is reported by NTA in dimensions of device, region, and IP group.



2 The Report Module Is Optimized

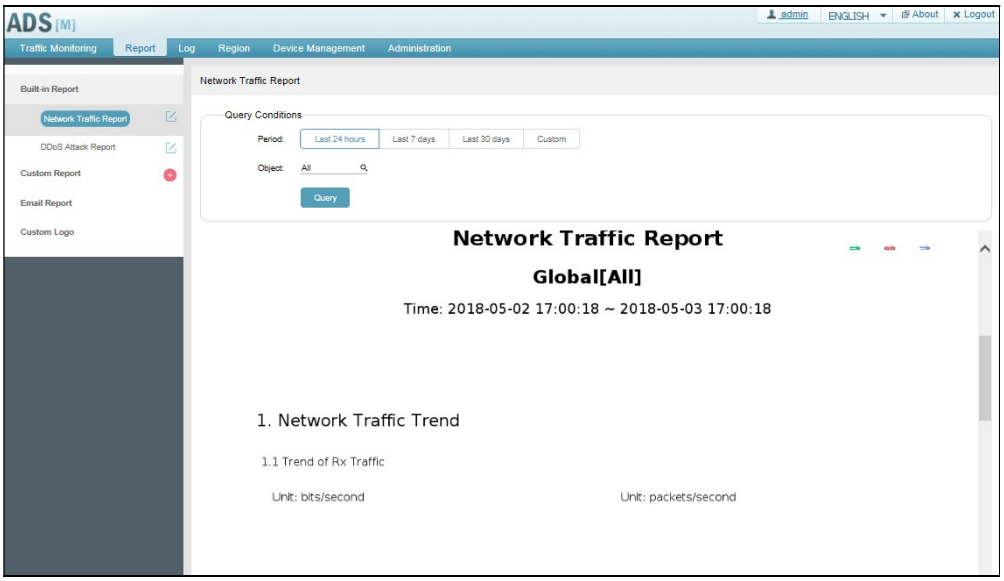
In the previous version, it is inconvenient to export and view reports and report contents cannot be customized. In V4.5R90F00, the Report module is added, covering the following:

(1) Built-in network traffic reports and DDoS attack reports

For customers' convenience, we provide the following built-in reports:

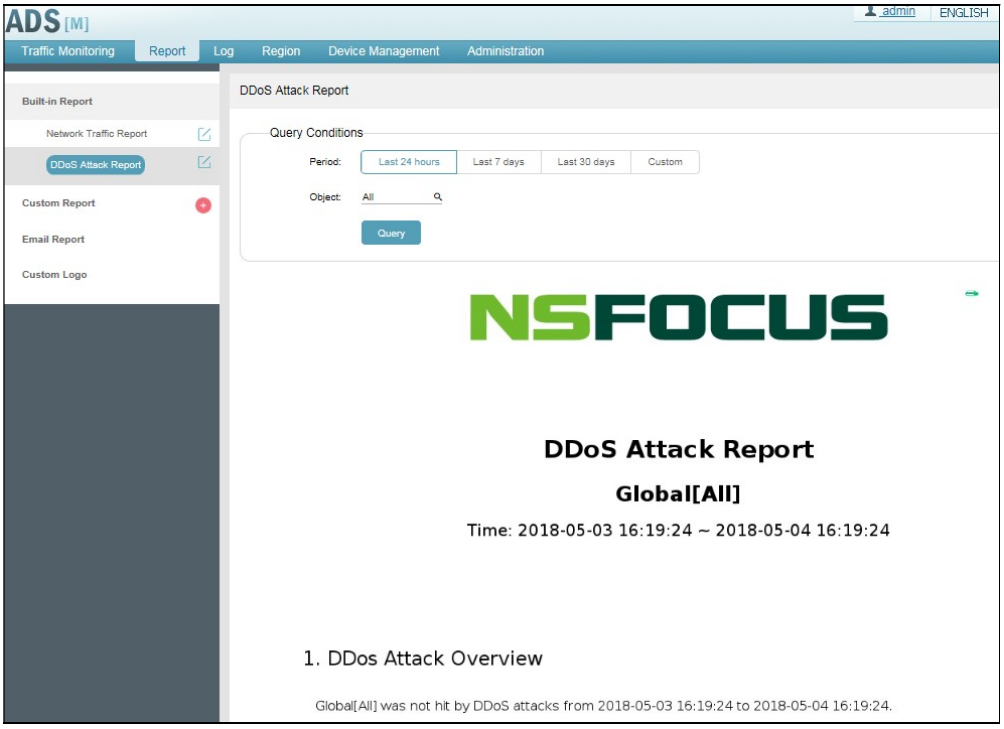
- Network traffic report

This report presents inbound and outbound traffic of the specified object generated in the specified period.



- DDoS attack report

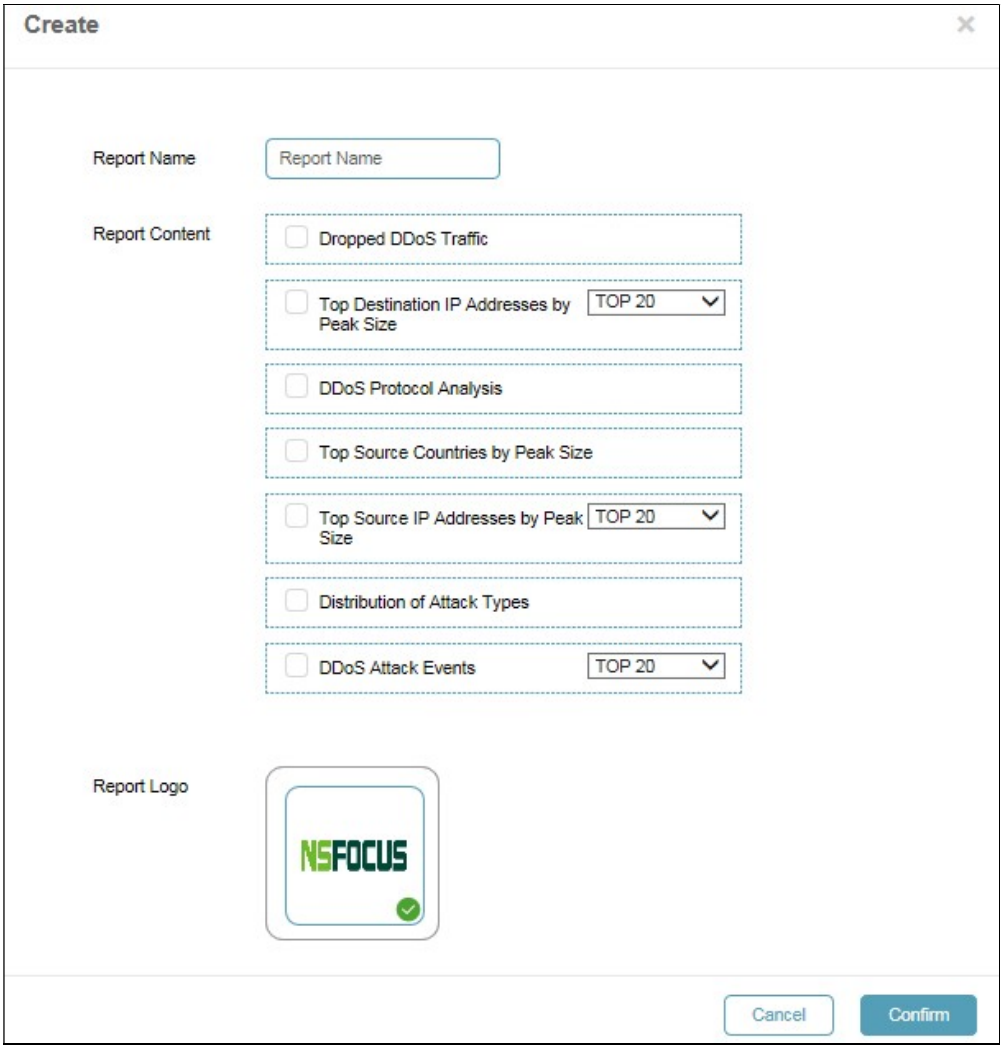
This report presents DDoS attacks of the specified object in the specified period. The report covers the attack traffic trend, attacked IP addresses, attack source IP addresses, attack events, attack types, and attack summary.



(2) Custom report

The content of the preceding types of reports is designed based on typical application scenarios and may not be applicable to all application scenarios. Therefore, we add a new design in this version to allow users to customize reports. For DDoS attack reports, customization can revolve around the following elements.

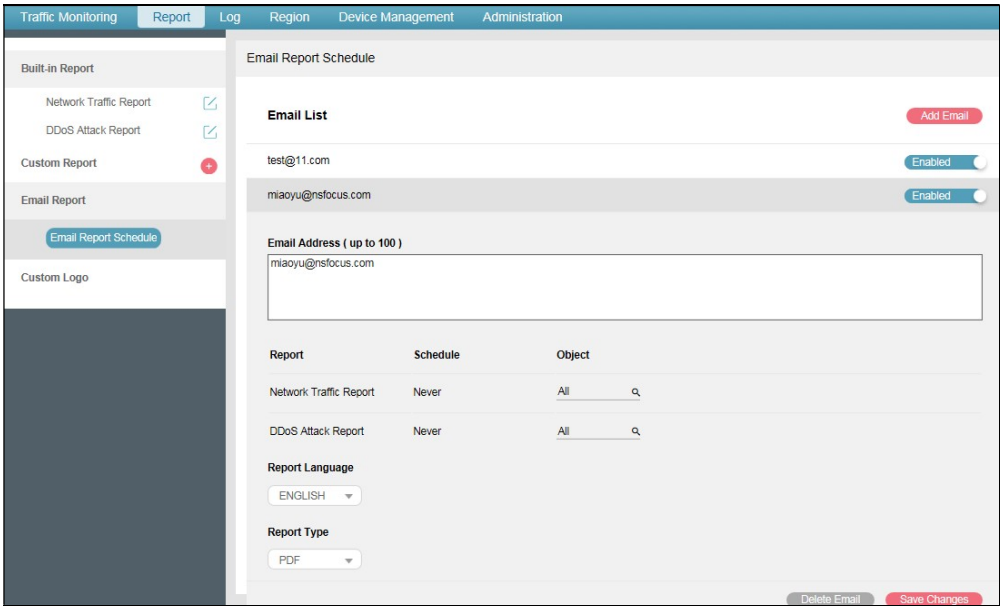
- Report name
- Report content
- Report logo



(3) Incorporating the email report function of the previous version

In the previous version, the email report function is available in the upper-right corner of the **Traffic Monitoring** page, which is used for sending scheduled reports via email. In V4.5R90F00, this function is put under **Report > Email Report** and is adjusted as follows:

- Built-in reports and custom reports can now be sent.
- Reports in the format of PDF, HTML, or Word can be sent.

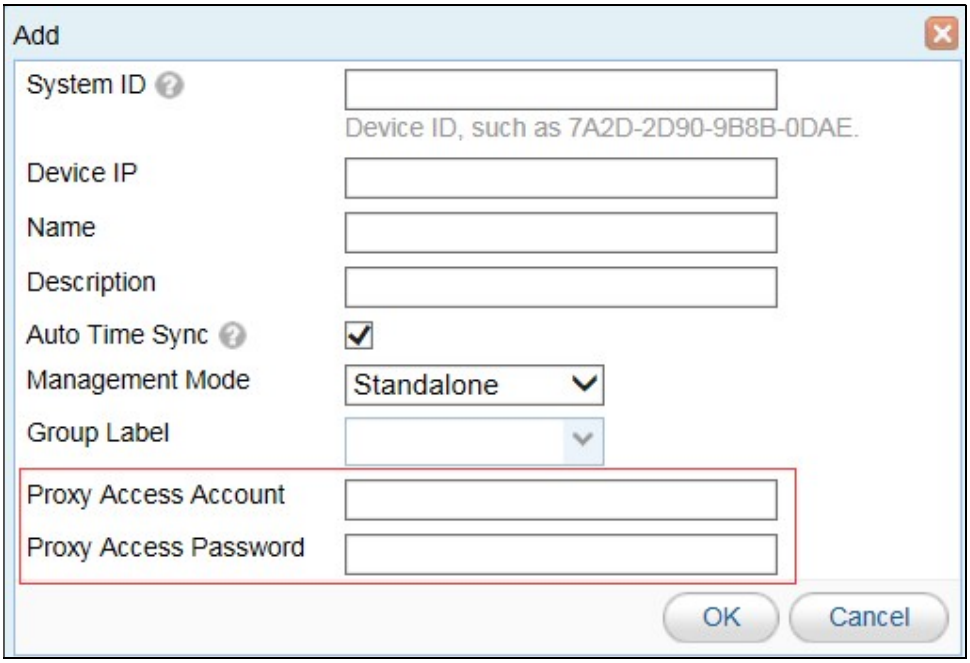


3 The Device Management Mode Is Optimized

The original device management mode requires that device versions be strongly consistent, which is not friendly for the management of devices of different versions. Therefore, the new version optimizes the device management mode by adopting the proxy method to manage devices.

The change of the device management mode brings the following changes to device configuration and management pages:

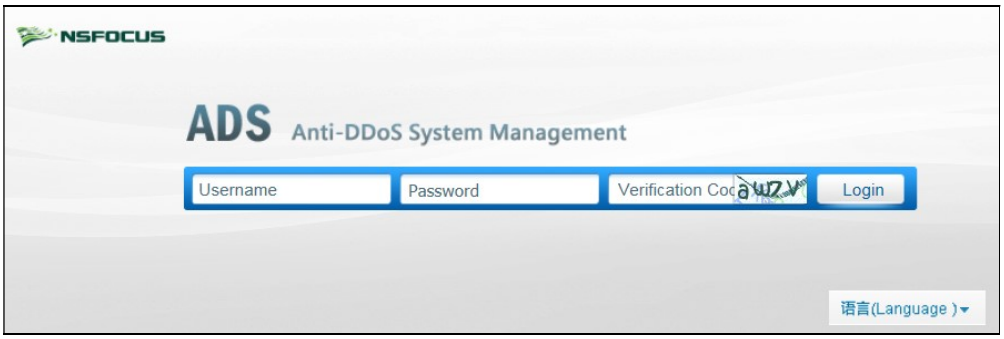
- **Proxy Access Account** and **Proxy Access Password** are added in the dialog box for adding or editing a device.



- The original management page is deleted and managed devices can now be directly operated on.

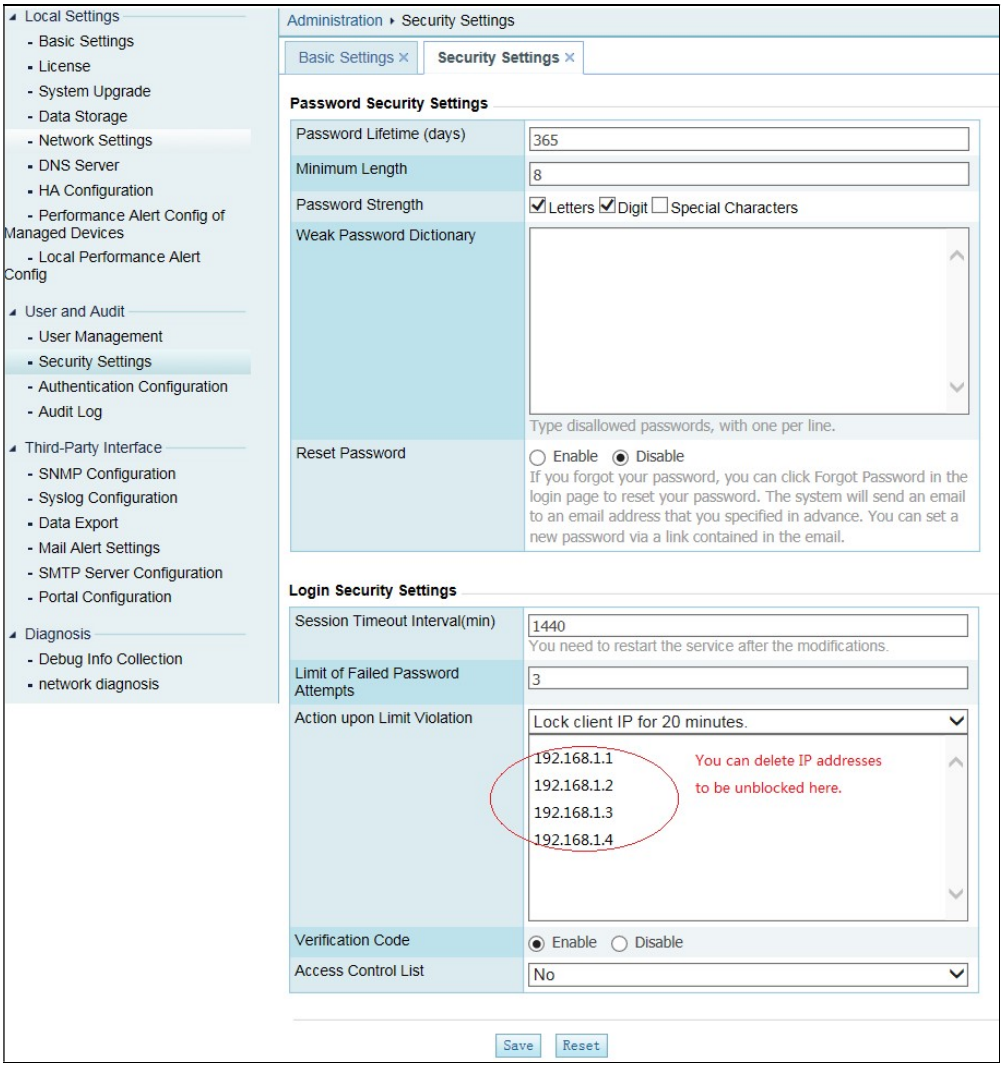
4 An Option of Login Authentication via Verification Codes Is Added

To enhance device security, login authentication via verification codes is added. This function can be enabled or disabled under **Administration > User and Audit > Security Settings**.



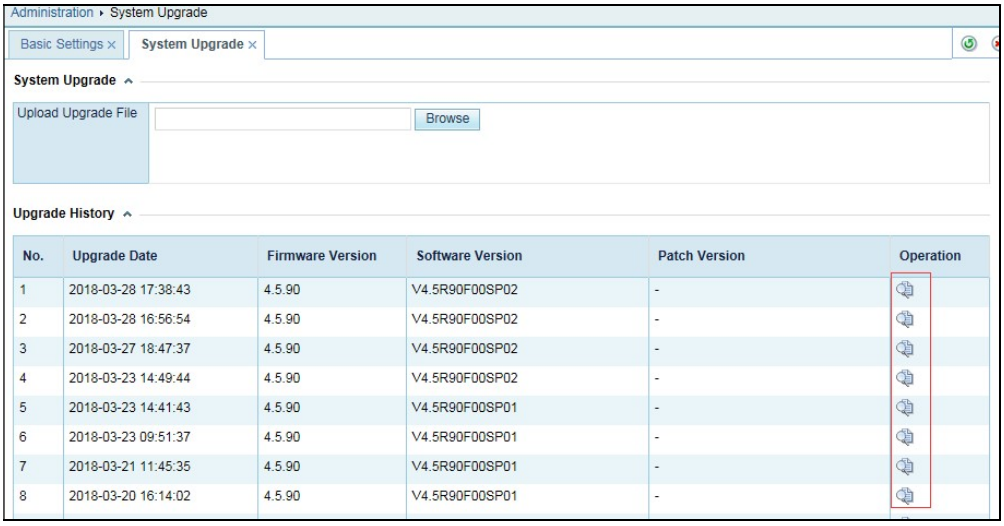
5 IP Addresses that Are Locked Due to Too Many Login Failures Can Be Manually Unlocked

If the number of a user's failed login attempts exceeds the specified threshold, his/her IP address will be locked and can be automatically unlocked only after a specified period. For the convenience of management, the function of unlocking IP addresses is added. The administrator can unlock an IP address by locating it under **Administration > User and Audit > Security Settings** and delete it, and then click **Save** to make the setting take effect.



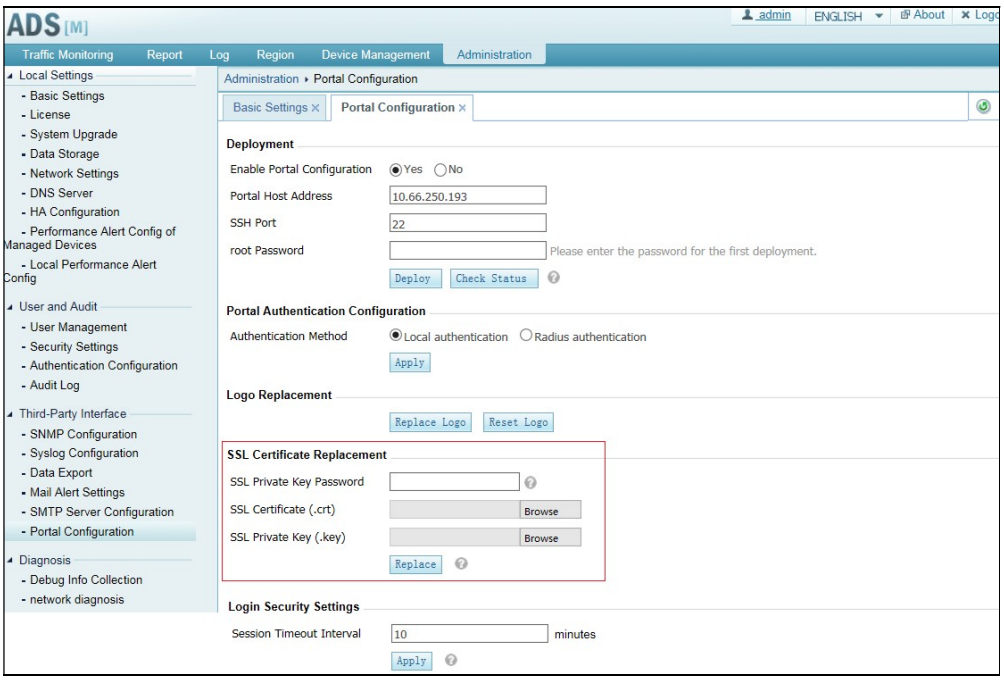
6 Upgrade Notes Are Recorded for view After Upgrade

In earlier versions, no upgrade log is recorded after system upgrade, which makes it impossible for users to have a knowledge of the upgrade. In V4.5R90F00, upgrade records are available under **Administration > Local Settings > System Upgrade** by clicking in the **Operation** column.



7 An SSL Certificate Can Be Imported on ADS M for Login to ADS Portal

In V4.5R90F00, an SSL certificate can be uploaded for login to ADS Portal under **Administration > Third-Party Interface > Portal Configuration**.



8 Regions Can Be Dispatched to Multiple NTA Devices Simultaneously

In earlier versions, regions can be dispatched to only one NTA device. In V4.5R90F00, regions can be dispatched to multiple selected NTA devices at the same time.