NSFOCUS RSAS
User Guide

Version: V6.0R04F04 (2024-06-30)

Confidentiality: RESTRICTED

■ Statement

The purchased products, services, or features are stipulated in the contract made between NSFOCUS and the customer. Part of products, services, and features described in this document may not be within the purchased scope or the usage scope.

All information in this document is provided "AS-IS" without guarantees of any kind, express or implied. The information in this document is subject to change without notice. It may slightly differ from the actual product due to version upgrade or other reasons.

■ Disclaimer

Please read the disclaimer carefully before using the product. Once you use the product, you acknowledge and agree to all the contents of this disclaimer. NSFOCUS shall not assume any responsibility for any loss or damage in the following circumstances:

- Data loss and system availability reduction caused by the negligence or misconduct of the system O&M or management personnel, for example, they do not handle alerts that affect system stability and availability in a timely manner.
- Data loss and system availability reduction caused by the fact that the traffic exceeds the planned hardware capacity.
- Data loss and system availability reduction or unavailability caused by natural disasters (including but not limited to floods, fires, and earthquakes) or environmental factors (including but not limited to network disconnection and power outage).

Contents

Preface

This document covers all functions of the NSFOCUS Remote Security Assessment System (RSAS) and details its main function modules and usage.

The product information involved in this document may slightly differ from your product to be installed because of version upgrades or other reasons.

Organization

Chapter	Description
1 Product Overview	Briefly introduces RSAS.
2 Getting Started	Describes the configurations for the first use of RSAS.
3 Dashboard	Describes dashboard content.
4 New Task	Describes how to quickly create a task and manage common scanning policies.
5 Scan Management	Describes how to manage scanning policies and tasks.
6 Asset Management	Describes how to manage assets.
7 Report Management	Describes how to manage reports and report templates.
8 Knowledge Base Management	Describes how to manage the knowledge base, including vulnerability database, templates, tools, and password dictionary.
9 Authentication	Describes RSAS authentication.
10 Administration	Describes system configuration.
11 Collaboration Management	Describes how to configure RSAS to collaborate with multiple devices or platforms.
12 Log Management	Describes how to manage RSAS logs.
13 Alert Management	Describes alerts.
A Console-based Management	Describes console-based management.
B Default Parameters	Provides default parameters of RSAS.
C FAQ	Provides frequently asked questions and answers about RSAS.
D MLPS	Describes security protection levels.

Change History

Version	Description
V6.0R04F04	First release.

Conventions

Convention	Description
Bold font	Keywords, names of screen elements like buttons, drop-down lists or fields, and user-entered text appear in bold font.
Italic font	Document titles, new or emphasized terms, and arguments for which you supply values are in italic font.
Note	Reminds users to take note.
Tip	Indicates a tip to make your operations easier.
Caution	Indicates a situation in which you might perform an action that could result in equipment damage or loss of data.
Warning	Indicates a situation in which you might perform an action that could result in bodily injury.
A > B	Indicates selection of menu options.

Technical Support

Hardware and Software Support

Email: support@nsfocusglobal.com

Cloud Mitigation Support

Email: cloud-support@nsfocusglobal.com

Phone:

- USA: +1-844-673-6287 or +1-844-NSFOCUS
- UK: +44 808 164 0673 or +44 808 164 0NSF
- Australia: +61 2 8599 0673 or +61 2 8599 0NSF
- Netherlands: +31 85 208 2673 or +31 85 208 2NSF
- Brazil: +55 13 4042 1673 or +55 13 4042 1NSF
- Japan: +81 3-4510-8673 or +81 3-4510-8NSF
- Singapore: +65 3158 3757

- Hong Kong: +852 5803 2673 or +852 5803 2NSF
- Middle East: +973 1619 7607

Documentation Feedback

For any query regarding the usage of the documentation, you can contact us:

Email: info-support@nsfocus.com

1 Product Overview

Based on years of practical experience in vulnerability discovery, configuration checking, and security services, NSFOCUS has developed RSAS, a next-generation vulnerability scanning and configuration management product.

This chapter provides basic information about RSAS. It contains the following sections:

Section	Description
Product Characteristics	Describes characteristics of RSAS.
Main Functions	Describes major functions of RSAS.
Typical Deployment	Describes deployment modes supported by RSAS.

1.1 Product Characteristics

As a next-generation vulnerability scanning and configuration management product, RSAS can fully detect vulnerabilities on the network, enabling users to quickly identify potential cyber risks.

All-Round Detection of Vulnerabilities

RASA can comprehensively detect vulnerabilities in IT systems. For example, it can detect security vulnerabilities in the target hosts, security configuration defects, web application vulnerabilities, weak passwords, and code defects and identify accounts, services, and ports that should not be opened in the system.

Graphic Display of Vulnerabilities

By means of NSFOCUS's proprietary security risk calculation method, RSAS analyzes various vulnerabilities on the network and evaluates the risks, provides an overall security status assessment, and comprehensively presents security risks in the information system, forming a complete security risk report. This helps the administrator to discover vulnerabilities earlier than attackers and fix the vulnerabilities timely.

The analysis result is displayed on the dashboard from perspectives of the risk area, type, and severity. As a result, you can comprehensively know the security risks, focus on critical areas and assets, and fix serious vulnerabilities first. Clicking the risk data on the dashboard helps you to locate vulnerabilities of an IP address.

Clear Asset Management

RSAS manages assets, which are uniquely identified with IP addresses, by using the risk view, in which the system and network security status is visualized in real time. When deploying RSAS, users could define a logical network structure in advance to manage risks by using either the asset view or the asset repository automatically generated from assessment tasks.

Asset management includes the following:

- When performing a scanning task, RSAS automatically detects IP addresses on the network and updates asset information to the asset repository.
- You can search the asset repository for the status of network assets.
- RSAS determines the risk level based on the risk score, which is calculated with the criticality of assets in the asset repository taken into account.
- When generating a report, RSAS locates the matched assets for each IP address. Then it reads and displays the node name and node administrator. In this manner, when a vulnerability is found in a node, the related node administrator can promptly identify the vulnerable asset and ask the asset owner to immediately fix the vulnerability.

Diversified Vulnerability and Configuration Databases

NSFOCUS boasts a professional security research team, NSFOCUS Security Team, with full-time researchers for vulnerability tracking and prospective study. The team has independently found over 40 vulnerabilities in common images, operating systems, databases, and network devices and been providing vulnerability-related rule support for world-famous network security vendors. NSFOCUS Security Team is responsible for maintaining the vulnerability database and detection rules and performing an upgrade every two weeks. In addition, for major vulnerabilities, the team can upgrade the vulnerability database and detection rules within two days after they are first detected.

Taking advantage of NSFOCUS Security Team's research accumulation, the RSAS knowledge base has over 270,000 vulnerabilities, covering all mainstream underlying systems, application systems, and network devices. It also provides the configuration checking base, professional suggestions for remediation, and security configuration checking standards for multiple industries. The configuration checking base is available for hundreds of systems, which are divided into seven categories and cover more than 30 products.

RSAS can discover security defects and noncompliant code practices by auditing mainstream code files.

Identification of Nonstandard Ports

With the advanced nonstandard port identification technology and protocol fingerprint base, RSAS can identify application service types on nonstandard ports quickly and accurately and conduct vulnerability checking, effectively avoiding false negatives and false positives during scanning.

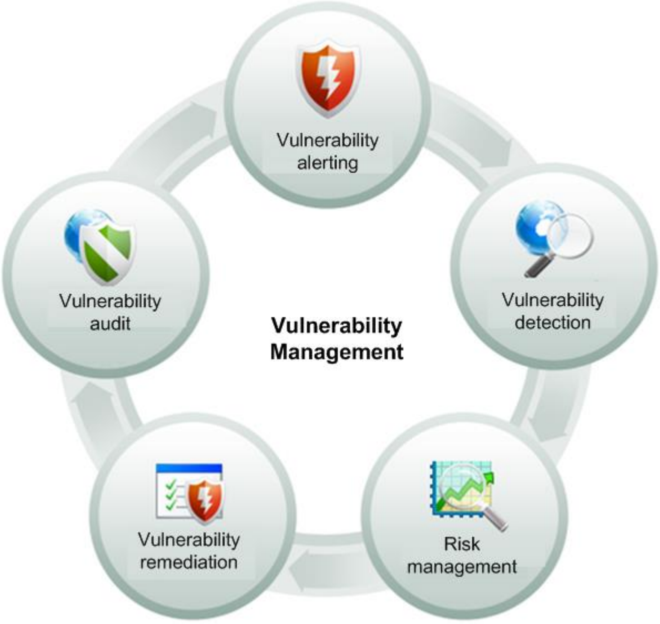
1.2 Main Functions

Baseline security requirements consist of security vulnerability and security configuration checking items. The coverage and effectiveness of such checking items are crucial to baseline security.

Vulnerability Management

According to security management regulations, RSAS provides risk alerting, checking, management, remediation, and auditing and supervises the implementation of security management regulations in each phase of the risk management process. RSAS can effectively and comprehensively detect vulnerability risks on the network, provide professional and effective analysis and remediation suggestions, and audit remediation effects throughout the risk management process, as shown in Figure 1-1. RSAS can reduce attacks to the maximum extent possible and is a "vulnerability management expert".

Figure 1-1 Security management process



Configuration Management

With a complete security configuration database, RSAS helps security configuration and remediation for IT information systems.

- By means of machine languages and the combination of remote detection and local detection, RSAS can automatically check security configurations and provide detailed detection reports. Compared with the traditional manual check, this helps reduce the check time and avoid mistakes.
- RSAS integrates leading technologies (including NSFOCUS Intelligent Profile (NSIP)) to detect security configuration issues in network assets automatically, effectively, and accurately.
- With continuous updates and improvement, RSAS is capable of supporting emerging device types. Check rules are also continuously updated to provide the most comprehensive automatic configuration checks, reducing risk costs and protecting your assets.

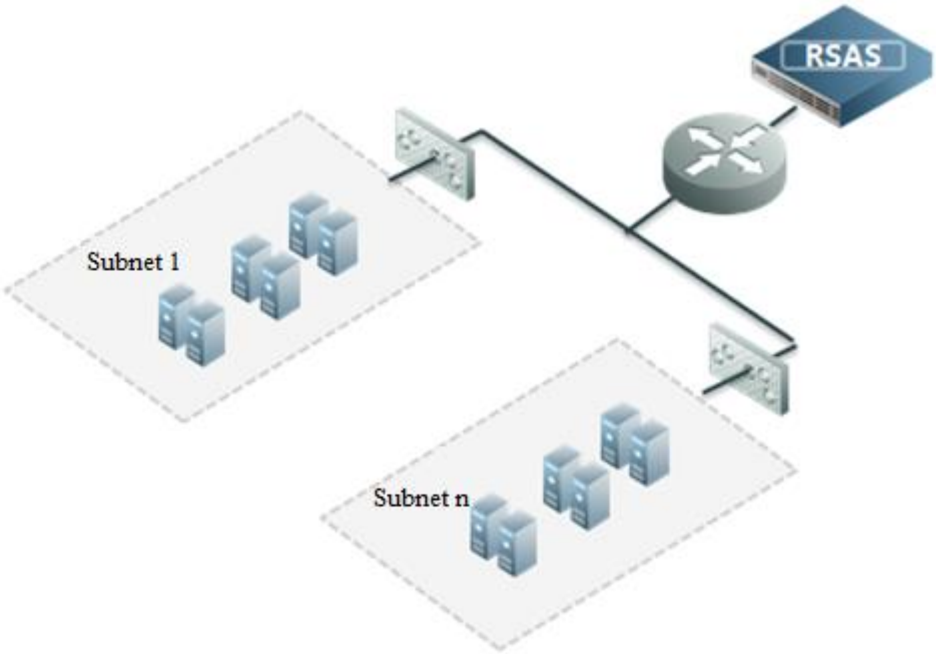
1.3 Typical Deployment

Standalone deployment is recommended for small and medium-sized enterprises, e-commerce, e-government, educational institutions, and independent Internet Data Centers (IDCs), which have more centralized data and simpler network topologies (mostly bus or star).

1.3.1 Deployment in a Small-Scale Network

RSAS can be easily deployed in the security maintenance environment of small-scale networks to detect various security vulnerabilities in business systems.

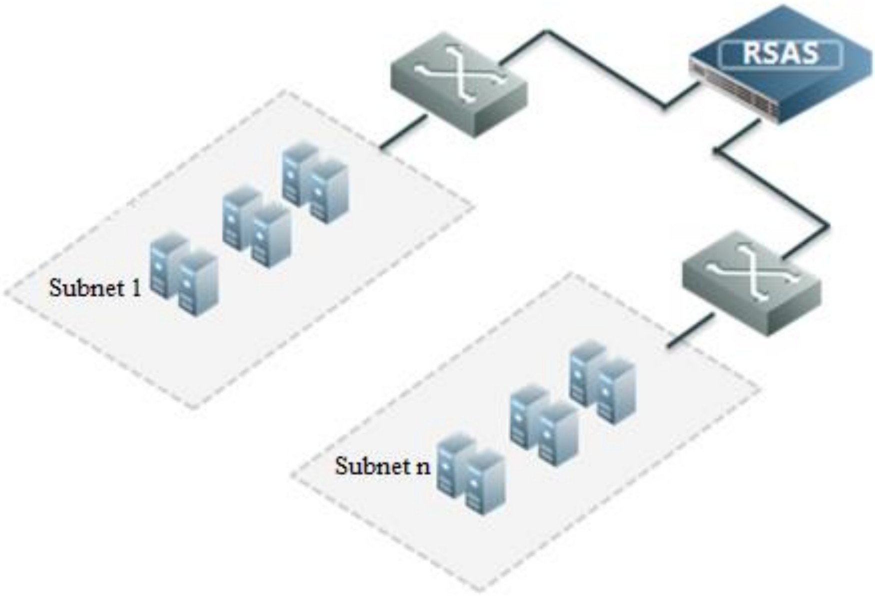
Figure 1-2 Deployment of RSAS in a small-scale network



1.3.2 Deployment in a Small and Medium-Scale Network

For small and medium-sized enterprises, their business networks may be divided into multiple subnets. It is costly to deploy a vulnerability management system on each subnet and also dangerous to open access permissions for vulnerability management on subnet firewalls. To cater to this situation, RSAS provides multiple scanning links and ports, each of which can connect to a subnet without extra firewall rule, as shown in Figure 1-3. This effectively reduces costs and avoids risks.

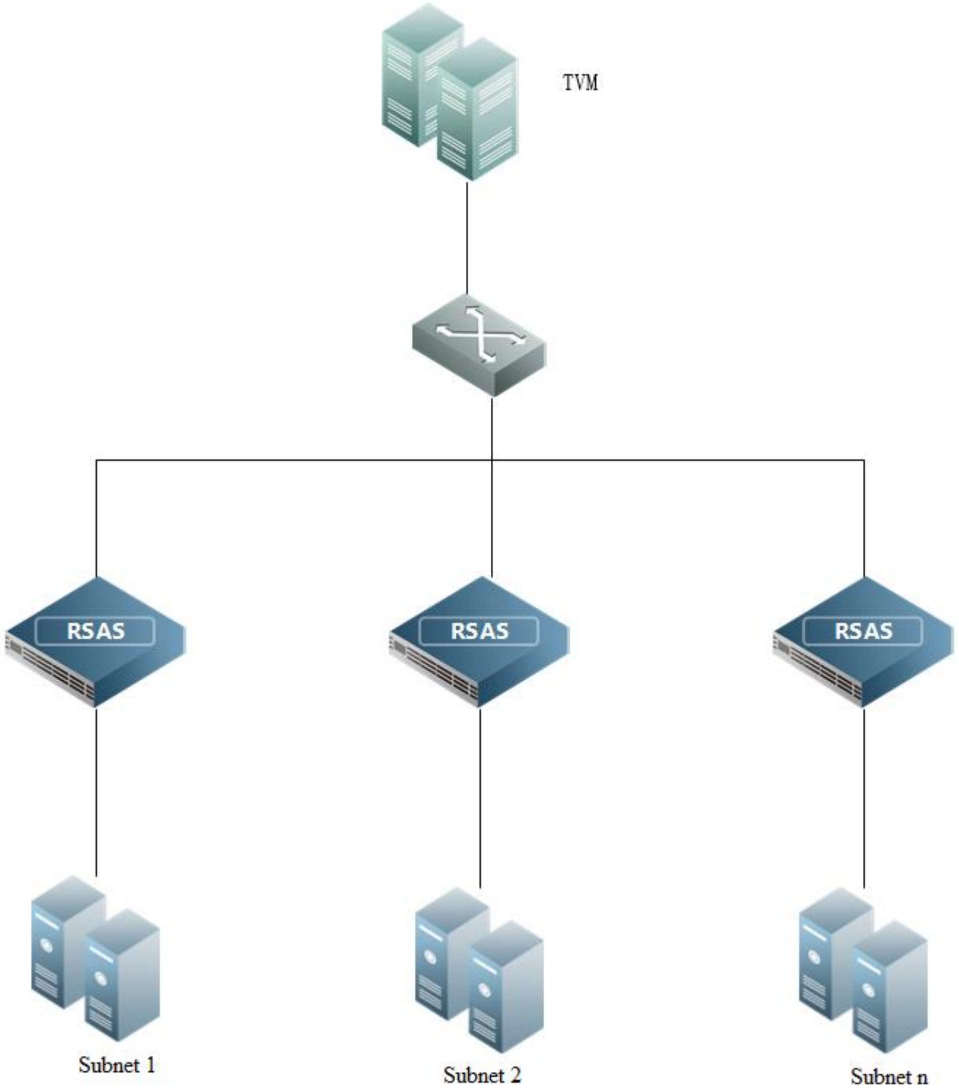
Figure 1-3 Deployment in a small and medium-scale network



1.3.3 Deployment in a Subnet with Limited Access

In certain circumstances, a business subnet may fail to RSAS, or RSAS cannot be directly deployed due to too many subnets. To cater to such situations, multiple RSAS devices can be deployed with TVM, under management of the latter. See Figure 1-4.

Figure 1-4 Deployment in a subnet with limited access



2 Getting Started

This chapter contains the following sections:

Section	Description
Initial Configuration	Provides instructions for initial configuration of RSAS.
Web-based Management	Describes the login method and page layout of the web-based manager.
Workflow	Describes the risk management procedure of RSAS.

2.1 Initial Configuration

This section describes how to configure RSAS for the first use. Initial configuration steps are different for the hardware edition and virtual edition of RSAS and are described in two separate sections.

2.1.1 Hardware Edition

The management interface can be configured only via the console, while scanning interfaces can be configured via console or web-based manager (after a license is imported). The following describes how to configure the management interface.

Prepare a computer, a serial cable, and terminal software for connecting to the console port and set default parameters listed in Default Parameters.

Step 1 Connect the RSAS device to the computer with the serial cable.

Step 2 Log in to the console.

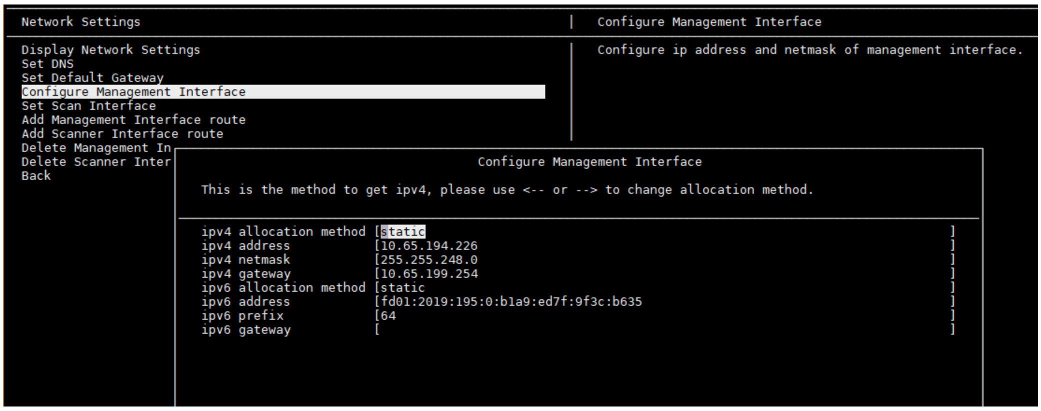
a. Use terminal software to connect to the RSAS console via a serial port.

b. Type the initial user name and password (see Default Parameters) of the console administrator to open the main menu of the console.

Step 3 Configure the management interface.

Choose **Network Settings** > **Network Settings**, set the IP address and subnet mask of the management interface, and then press **Enter** to commit the settings.

Figure 2-1 Configuring management interface parameters



```
Network Settings                                            | Configure Management Interface

Display Network Settings                                    | Configure ip address and netmask of management interface.
Set DNS                                                     |
Set Default Gateway                                         |
Configure Management Interface                              |
Set Scan Interface                                          |
Add Management Interface route                              |
Add Scanner Interface route                                 |
Delete Management In
Delete Scanner Inter                        Configure Management Interface
Back
                     This is the method to get ipv4, please use <-- or --> to change allocation method.

                     ipv4 allocation method [static                                                    ]
                     ipv4 address           [10.65.194.226                                             ]
                     ipv4 netmask           [255.255.248.0                                             ]
                     ipv4 gateway           [10.65.199.254                                             ]
                     ipv6 allocation method [static                                                    ]
                     ipv6 address           [fd01:2019:195:0:b1a9:ed7f:9f3c:b635                       ]
                     ipv6 prefix            [64                                                        ]
                     ipv6 gateway           [                                                          ]
```

----End

2.1.2 Virtual Edition

The virtual edition of RSAS (vRSAS) can be installed on different virtualization platforms. The method for logging in to the console of vRSAS varies with the virtualization platform. For details, see the *NSFOCUS RSAS V6.0R04F04 Installation Guide*.

You can log in to vRSAS after importing a valid license. You must change the initial password after the first login.

2.2 Web-based Management

The web-based manager provides an intuitive human-machine interaction interface for users to manage and configure RSAS.

In addition to the console-based management, RSAS can be remotely managed via software supporting SSH.

Supported Browsers

Browser	Version	Remarks
Firefox	Latest	• Check whether the option of blocking pop-ups or disabling JavaScript is selected in the browser. If yes, clear the check box. • Disable the enhanced protection mode.
Chrome	Latest	
Microsoft Edge	Latest	

Recommended Screen Resolution

The recommended screen resolution is 1280 x 1024 pixels or higher.

Web Login

Before login to the web-based manager, you must have completed Initial Configuration and ensure that RSAS is properly connected to the network.

Open a browser and access the IP address of the management interface via HTTPS by typing, for example, **https://192.168.1.1**, in the address bar. After accepting prompted risks, you can view the web login page. Type a correct user name, password, and verification code. Click **Log In**.

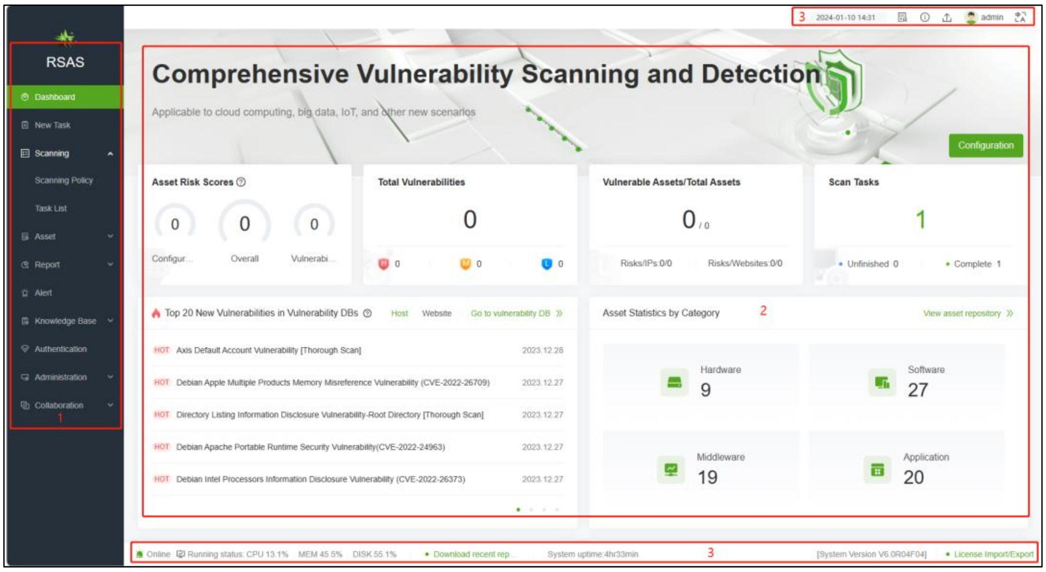
- For the default user name and password, see Default Parameters.
- When logging in for the first time, you need to change the initial password and log in again with the new password.

Page Layout

The page layout for all modules of RSAS is the same, as shown in Figure 2-2.

Note	The menus and work area vary with user roles and data permissions.

Figure 2-2 Page layout



HOT Axis Default Account Vulnerability [Thorough Scan] 2023.12.28
HOT Debian Apple Multiple Products Memory Misreference Vulnerability (CVE-2022-26709) 2023.12.27
HOT Directory Listing Information Disclosure Vulnerability-Root Directory [Thorough Scan] 2023.12.27
HOT Debian Apache Portable Runtime Security Vulnerability(CVE-2022-24963) 2023.12.27
HOT Debian Intel Processors Information Disclosure Vulnerability (CVE-2022-26373) 2023.12.27

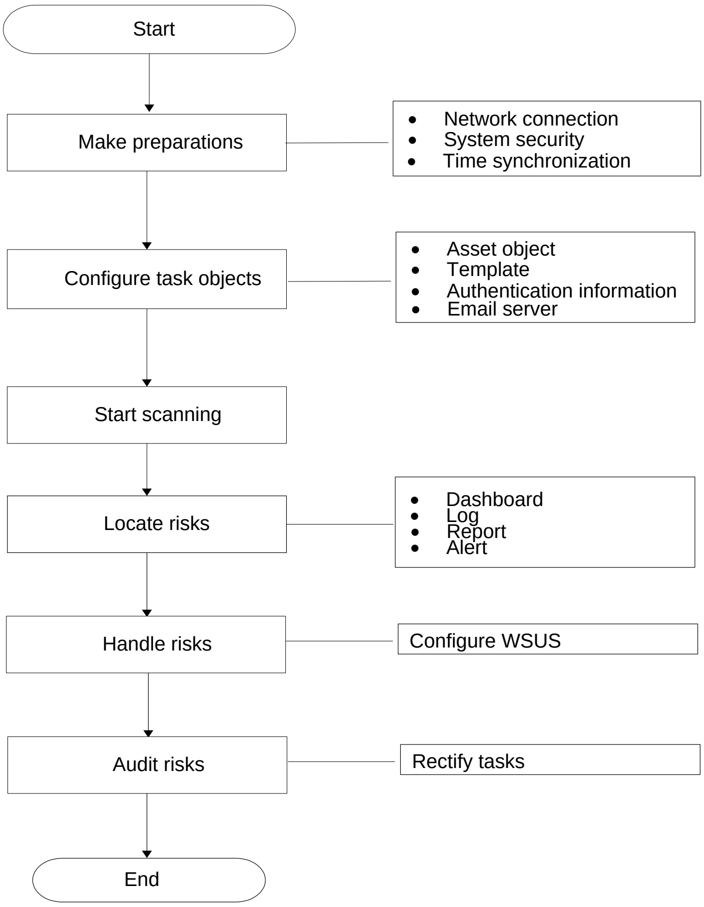
No.	Area	Description
1	Menu bar	Area of function menus from which you can perform further operations.
2	Work area	Area where you can perform configurations and operations and view data.
3	Quick access bar	Area providing the following quick access buttons of the system:

No.	Area	Description
		• 2024-03-27 13:58 : allows you to view the system time. • LIC / License Import/Export : allows you to import and export a license, as detailed in Importing and Exporting a License. • ⓘ : allows you to query system information or online help. • ⇪ : allows you to upgrade the system, as detailed in System Upgrade. • admin : allows you to manage the current login account. For details about administrators, see User. Also, you can log out of the system. • 中A : allows you to change the system language. • **Running status**: allows you to view the system running status. • **Download recent reports**: allows you to download reports from the Report Management page. • **System uptime**: allows you to view the system uptime. • **Update available**: allows you to immediately upgrade RSAS to the available version on the System Upgrade page when there is an upgrade prompt.

2.3 Workflow

Figure 2-3 shows the risk management flow of RSAS.

Figure 2-3 Risk management flow



3 Dashboard

The dashboard allows you to check general statistics of the scanned servers and hosts to learn about security risks at any time.

The dashboard data is composed of the risk analysis for all assets last scanned by RSAS. After RSAS scans servers and hosts as instructed, it refreshes data every day at 5:00 and displays all the historical data on the dashboard, where you can view risk statistics about such servers and hosts.

Dashboard Configuration

You can set the statistical period and displayed items on the dashboard. Choose **Dashboard**, click **Configuration**, and set parameters shown on the dashboard. Table 3-1 describes items to be displayed on the dashboard.

Table 3-1 Dashboard parameters

Parameter	Description
Displayed Items	Specifies the items to be displayed on the dashboard. For details, see Statistics.
Statistical Period	• **Cycle Granularity** and **Cycle Length**: specifies the length of the specified statistical cycle. • **Custom Time Frame**: specifies the start time and end time of a period. • RSAS displays scanning tasks in either period you set.
Data Source	Specifies the source of statistical data to display in the dashboard as needed. Only the system administrator **admin** can configure this parameter.

Statistics Display

RSAS refreshes data every day at 5:00 and displays all the historical scanning tasks on the dashboard.

Table 3-2 Dashboard display

Item	Description
Asset Risk Scores	Displays risk scores and security information about all hosts in the statistical

Item	Description
	period and within your privileges. • **Configuration**: It is the average configuration risk score obtained after configurations of all hosts are scanned. • **Overall**: It is the overall score obtained after all hosts are scanned. This score is calculated by assessing the configuration risks and system risks (including system vulnerabilities and web application vulnerabilities). • **Vulnerability**: It is the average vulnerability risk score obtained after vulnerabilities of all hosts are scanned, including system vulnerabilities and web application vulnerabilities.
Total Vulnerabilities	Displays vulnerabilities by risk level (high, medium, and low) that were found in scanning tasks, including system vulnerabilities and web application vulnerabilities.
Vulnerable Assets/Total Assets	Displays the number of vulnerable assets and the total number of assets. • **Risks/IPs**: displays the numbers of vulnerable and total IP addresses. • **Risks/Websites**: displays the numbers of vulnerable and total websites.
Scan Tasks	Displays the numbers of total, unfinished, and complete tasks. Tasks, except for complete ones, are unfinished. Waiting tasks are also counted as unfinished.
Top 20 New Vulnerabilities in Vulnerability DBs	Displays the top 20 new vulnerabilities with the highest risks in four rolling pages. Each page displays five vulnerabilities. • Clicking a vulnerability name displays details about this vulnerability. • You can click **Go to vulnerability DB** to query all vulnerabilities on the Vulnerability Database page.
Asset Statistics by Category	Displays the numbers of assets by category, including hardware, software, middleware, and application software. You can click **View asset repository** to query all assets on the Asset List page that appears.
Asset Distribution by Risk Level	Displays the numbers of assets by risk level.
Vulnerability Distribution by Risk	Displays the numbers of discovered high-, medium-, and low-risk vulnerabilities in a histogram.
Top 5 Risk IPs	Lists the top 5 assets with the highest risks, including hosts and websites. Assets with the same risk score will be ranked by task delivery time. You can click an IP address to view information about the scanning task on the Task List page that appears.
Top 5 Vulnerabilities	Displays the top 5 vulnerabilities that affect the most assets, including system vulnerabilities and web application vulnerabilities, in a donut chart. Vulnerabilities with the highest risks are displayed, if the number of affected assets is the same.
Risk Number Trend (Week)	Displays changing trends of high-, medium-, and low-level risks brought by system vulnerabilities, web application vulnerabilities, weak passwords, and noncompliant configurations in a histogram and line chart.
Overall Risk Score Trend (Week)	• Displays changing trend of the overall risk score in a histogram. • Displays the percent increase or decrease in the overall risk score in a line chart.

4 New Task

A scanning policy is a task template, which generates a scanning task after policy execution. This module provides a quick access to scanning tasks and policies, allowing you to quickly create and manage them.

Tasks serve as a basis for RSAS to proactively conduct vulnerability detection, configuration checks, and weak password guesses.

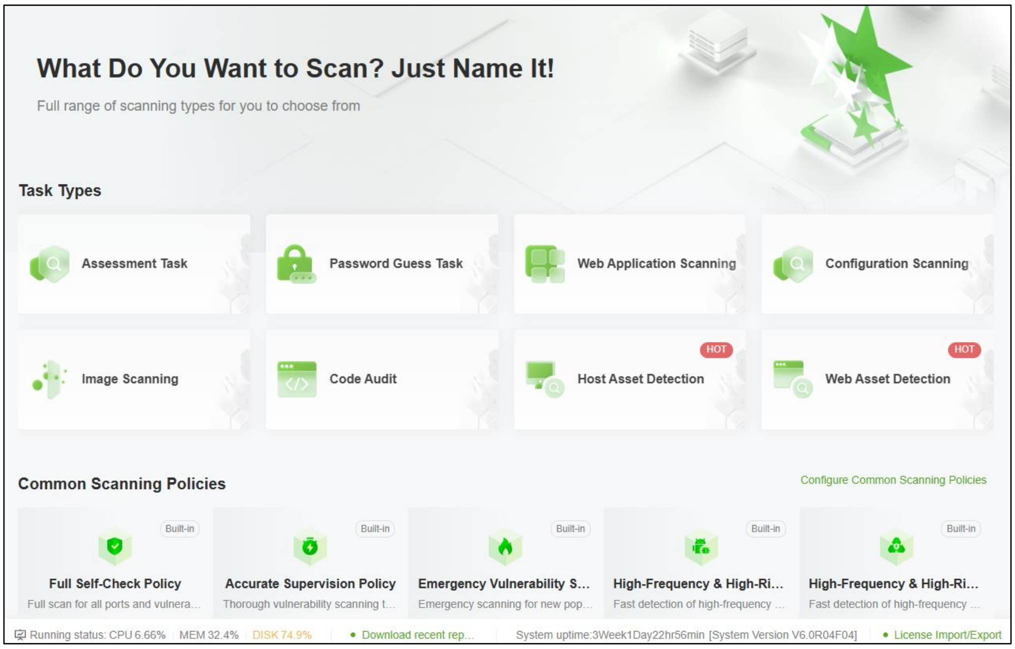
This chapter describes how to manage scanning tasks. It contains the following sections:

Section	Description
Task Type	Describes how to create a task.
Common Scanning Policies	Provides a quick access to policy management.

4.1 Task Type

Choose **New Task**, select a type under **Task Types**, and configure parameters. Click **Create** to create and dispatch a task of the specified type. A task, after being created, is displayed on the Task List page, where you can manage it.

Figure 4-1 New Task page



What Do You Want to Scan? Just Name It!

Full range of scanning types for you to choose from

Task Types
Assessment Task
Password Guess Task
Web Application Scanning
Configuration Scanning
Image Scanning
Code Audit
HOT
Host Asset Detection
HOT
Web Asset Detection
Common Scanning Policies
Configure Common Scanning Policies
Built-in
Full Self-Check Policy
Full scan for all ports and vulnera...
Built-in
Accurate Supervision Policy
Thorough vulnerability scanning t...
Built-in
Emergency Vulnerability S...
Emergency scanning for new pop...
Built-in
High-Frequency & High-Ri...
Fast detection of high-frequency ...
Built-in
High-Frequency & High-Ri...
Fast detection of high-frequency ...
Running status: CPU 6.66% | MEM 32.4% | DISK 74.9%
Download recent rep...
System uptime:3Week1Day22hr56min [System Version V6.0R04F04]
License Import/Export

4.1.1 Assessment Task

An assessment task aims to scan the target for possible vulnerabilities (system vulnerabilities) and configuration noncompliance. After task execution, RSAS sends network security assessment results to the specified email address or FTP server, notifying the administrator of remediation. Also, RSAS supports task report export for the administrator to download for asset risk analysis.

Choose **New Task > Task Types > Assessment Task** and configure parameters.

- Click **Create** to create a task.
- Click **Save** to save the task as a scanning policy.

Table 4-1 to Table 4-6 describe parameters for creating an assessment task.

Table 4-1 Basic information parameters for an assessment task

Parameter	Description
Existing Configuration (optional)	**Policy**: Creates a task based on an existing scanning policy (namely, task template). • Click **Set as Default** to set the task as the default scanning policy. Then the system can directly call this policy to create a task for another scan target. • Click **Reset** to restore default settings.
	Historical task: Creates a task based on an existing task.
Scan Target	Specifies the scan target. A maximum of 10,000 lines or 65,535 IP addresses are allowed. The scan target can be specified in any of the following ways:

Parameter	Description
	• **IP**: Multiple IP addresses or address ranges should be separated by the comma (,), semicolon (;), carriage return, or space. If an IP address or IP address range is preceded with an exclamation mark (!), it indicates that this IP address or IP address range will not be scanned. For details, hover over ❔ next to the parameter. • **Domain**: Domain names should be typed in a format like www.example.com. Multiple domain names should be separated by the comma (,), semicolon (;), carriage return, or space. If all domain names map the same IP address, you must also select **Virtual host**. For details, hover over ❔ next to the parameter. • **Import from asset repository**: You can click **Import from asset repository** and then select a scan target from the list that appears below. • **Upload target file**: You can click **Click to Upload**, browse to a file in any of the following formats, and then import the file. - TXT: lists IP addresses in separate lines, as described in the input box. - EXCEL: based on a downloaded template (click Download Template on the Authentication page and fill in relevant information as required). - DAT: file exported from the Authentication page.
Task Name	Specifies the name of the new task. After the scan target is specified, the task name will be generated automatically. Alternatively, you can specify a different name. It should be a string of 1–256 characters.
Execution Mode	• **Instant**: indicates that the task will be executed immediately after you complete the configuration. This is applicable where network security assessment should be immediately conducted. • **Scheduled**: indicates that the task will be executed as scheduled. This is applicable where network security assessment should be conducted during off hours. • **Daily, Weekly, Monthly (date)**, or **Monthly (day of the week)**: indicates that the task will be executed repeatedly as scheduled. This is applicable where network security assessment should be conducted regularly (daily, weekly, or monthly). • **Advanced configuration**: indicates that the task will be executed repeatedly as scheduled. You can set the cycle lengths and specify multiple scanning cycles by clicking **Add**.
Vuln Template	Specifies a vulnerability template for vulnerability scanning. • **Auto match scan**: RSAS calls the template matching the scan target for vulnerability scanning. • **No template**: RSAS will not perform vulnerability scanning. • **Verifiable Vulnerabilities Scan:** RSAS only scans vulnerabilities that can be verified. If such vulnerabilities are detected, you can verify them. For details, see Verifying Vulnerabilities. • If RSAS scans and detects verifiable vulnerabilities that are included in other templates, you can verify them. For details, see Verifying Vulnerabilities. • **Network Info Collection**: RSAS only collects network information without scanning configurations or vulnerabilities. • **Full Info Collection**: RSAS only collects information from target hosts with an agent installed, without scanning configurations or vulnerabilities. You can click **Vulnerability Template Management** to configure and view vulnerability templates on the Vulnerability Template page.

Parameter	Description
Auto Vuln Verification	Controls whether the vulnerabilities are verified. After it is enabled, the POC verification principle and vulnerability verification template are used to accurately verify vulnerabilities in assets.
Full Agent Scan	After an agent is installed on the scanned host, the agent reports the host information to RSAS or the platform every four hours. After this function is enabled, RSAS only scans the latest hosts reported by the agent for vulnerabilities. For details about how to manage agents, see Agent Management.
Scan Time Frame	Specifies the periods in which this scanning task will be executed. After you specify periods, RSAS will execute this task only in the specified periods regardless of the setting of **Execution Mode**.
Scheduling Priority	Specifies the priority of this task. RSAS determines the task priority based on the specified priority value and the background algorithm.

Table 4-2 Login check parameters on the Basic Information tab for an assessment task

Parameter	Description
Post-login vulnerability check	Checks for system vulnerabilities after login to the scan target. Login protocols SMB, SSH, and RDP are supported.
Post-login configuration check	Checks for noncompliant items after login to the scan target. • **Accurate check**: checks for noncompliant items in the scan target against configuration templates you selected. • **Intelligent check**: collects information and automatically checks for noncompliant items in the scan target against configuration templates you selected. You are advised to log in to the target host as an administrator for a more accurate scan result. • **Information collection**: looks into the system environment of the scan target. You are advised to log in to the target host as an administrator for a more accurate scan result. Login protocols SMB, SSH, RDP, Telnet, HTTP, HTTPS, and WinRM are supported.
Bulk Login Test	Checks for the status of hosts after login to them in bulk.

Table 4-3 Parameters for configuring host authentication in post-login check

Item	Parameter	Description
Add or import host authentication information	-	After **Login Check** is enabled, the login check module will automatically read the host authentication information. • Such information can be added manually or imported. To import a file, click **Download Template** to save the authentication information template to a local disk drive and add authentication information in the file. • The host authentication information beyond the scan scope cannot be imported.

Item	Parameter	Description
		- You can click **Export** to save the host authentication information to a local disk drive.
Authentication	Sync to authentication mgmt	If **Sync to authentication mgmt** is enabled, the authentication information of the host with the same IP address will be overwritten. For details, see Authentication.
System Login Information	IP	Specifies IP addresses or IP address ranges of the scan target. The IP addresses or IP address ranges typed here must be within the scope specified with **Scan Target**.
	- Domain Name/Domain User - Password (Domain Password)	Specifies the user name and password for login to the scan target. RSAS stores the user name and password in an encrypted way to ensure security.
	Obtain	You can click **Obtain** to obtain the host login password from NSFOCUS Operation Security Management System (OSMS) that collaborates with RSAS. For how to configure collaboration with OSMS, see Authentication Management.
	Login Protocol/Login Port	Specifies the protocol and port used for login to the scan target. Login protocols for a post-login configuration check include SMB, SSH, and RDP. Login protocols for a post-login vulnerability check include SMB, SSH, RDP, Telnet, HTTP, HTTPS, and WinRM For login via HTTP, HTTPS, and WinRM, RSAS can only do configuration checks, but cannot conduct vulnerability scanning.
	Host Jump	When RSAS can log in to multiple target hosts directly or using the same jump host, you can configure the same jump host after host jump is enabled. - If RSAS cannot directly log in to the target host, it can use the jump host for scanning. In this case, you need to configure the authentication information for the jump host in advance. - Make sure that the jump host can connect to the target host. - This parameter is available only when **Login Protocol** is set to **SSH** or **Telnet**.
	Login Path/Site Cookie	Specifies the login path and website cookies (which record login session IDs) for login to the scan target via HTTP or HTTPS. You can click **Record** to set the browser proxy as prompted. After the proxy server is set, RSAS can capture cookies.
	Login Authentication	Clicking **Login Authentication** checks whether login information is correct to make sure that RSAS can log in to the target host for local scanning.
ORACLE Scanning Policy	Oracle	Controls whether to enable deep scan of vulnerabilities in Oracle. At the same time, you need to enable **Oracle Deep Scan** on the **Advanced Settings** tab (see Table 4-5) during task creation. If this parameter on the **Advanced Settings** tab is not enabled, RSAS only calls thorough Oracle scan, rather than local scan or remote version scan of Oracle.

Item	Parameter	Description
WebLogic Scanning Policy (Enables the deep scan of vulnerabilities in WebLogic.)	System Scanning	Controls whether to allow access to WebLogic via the management background of a device on which the WebLogic service resides. • **Linux/Windows**: operating system type • **WebLogic Version**: WebLogic version • **WebLogic Install Account**: user name for access to WebLogic • **WebLogic Opatch Install Dir**: installation path of WebLogic WLS
	Page Scanning	Controls whether to allow access to WebLogic via web. • **User Name/Password**: user name and password for access to WebLogic. • **Path**: WebLogic URL.
Configuration Template	Enable MLPS	Controls whether to enable the multilevel protection function. If it is enabled, you need to select a Multilevel Protection Scheme (MLPS) level and select the corresponding MLPS template. For details about MLPS levels, see MLPS.
	Host	Indicates computers with an operating system installed. You can click a template name to add the template to the **Selected Templates** box and then configure template parameters. • **Operating system template**: configuration specifications of operating systems • **Virtual device template**: configuration specifications of virtual devices • **Application template**: configuration specifications of applications • **Database template**: configuration specifications of databases • **Big data template**: configuration specifications of big data software or platforms
	Network device	Indicates physical entities connected to the network except for hosts, such as switches and routers. • You can click a template name to add the template to the **Selected Templates** box and then configure template parameters. • Select configuration specifications of network devices.
Status Template	Template	Specifies an allowlist of items that are deemed to be compliant. You can click **Status Template Management** to open the page for configuring a status template. For how to create a status template, see Status Template.

Table 4-4 Parameters for configuring password guess in an assessment task

Parameter	Description
Password Guess	After it is enabled, click **Detailed configuration**, and then set parameters in the drawer that appears. • After login to the target host with a vulnerable account, RSAS will conduct local vulnerability scanning. • If no scanning is done via a login to the host, RSAS will guess the host password based on the content included in the password dictionary. For details about the password dictionary, see Password Dictionary. Password guess tasks can be conducted only for active hosts.
Service Type	Specifies a service subject to password guessing. • In standard mode, the same dictionary is used for both user names and passwords. • In combined mode, both the user name dictionary and the password dictionary are used. Note • You can click **Password dictionary management** to edit the default password dictionary. • The custom password dictionary comes before the default password dictionary for password guessing. Passwords are guessed in the same sequence as they are arranged in the dictionaries. • Enabling password guess may cause account locking as a result of multiple consecutive login failures during scanning. Therefore, enable this function with caution.
Timeout	Specifies the maximum duration within which a password guessing plugin can run. After the duration expires, the plugin stops running.
Frequency	Specifies the interval between two password guesses of the same protocol for the same target.
Guessing Times	Specifies the maximum number of guesses allowed for a single asset. The value **0** indicates no limit.
Max Concurrent Threads	Specifies the maximum number of concurrent threads for a single-service password guess task on a single host. A greater value ensures a faster scanning speed.

Table 4-5 Advanced parameters for an assessment task

Section	Parameter	Description
Port Scan	Port Scanning Policy	• **Standard port scan**: scans only the ports listed under Port List. • **Fast port scan**: scans ports 1 to 1024. • **Specify ports**: scans specified ports. • **Full port scan**: scans all ports. Note A full port scan involves a large number of sent packets. You are advised to verify in advance that your network environment can support such scans.

Section	Parameter	Description
	Scan Speed	Specifies how fast the scanning should be conducted. A smaller scan speed indicates more accurate information about open ports and a longer scanning time.
	TCP Port Scan Method	• **CONNECT**: determines whether a port is open by establishing a complete TCP connection. This mode ensures quick and accurate scanning. • **SYN**: determines whether a port is open based on receiving of the ACK packet sent by the port in response to the SYN packet from RSAS.
	UDP Scan	Controls whether to enable UDP scanning. Selecting this option significantly lengthens the time to complete the task. Therefore, you are advised not to enable it. UDP ports defined in the port list can be scanned only when this option is enabled. For details about the port list, see Port List.
Host Status Test	Host Status Test	Controls whether to enable the host status test. After enabling it, you also need to specify the test method and port.
	Status Detection Speed	A smaller status detection speed indicates more accurate host status information and a longer scanning time.
Scan Restrictions	Scan Depth	Scanning depth. A greater value indicates more information to be captured and a longer scanning time. The default value **3** is recommended.
	Plugin Timeout	A single plugin that does not end within specified time will be terminated by the scheduler. Value range: 1–300, in seconds.
	Socket Timeout	Specifies the longest wait time allowed for reading data from the network layer. This option greatly affects the scanning speed and accuracy. The recommended value is **5** seconds for a local area network (LAN) or **15** seconds for an asymmetric digital subscriber line (ADSL) network. You can set the value according to the network speed. Set a greater value when the network speed is slow.
Others	Dangerous Plugin Scan	Dangerous plugins may cause system crashes or service interruption. You are advised to enable it only for special purposes such as testing.
	Notify Host Before Scan	Controls whether to notify the host before scanning. After you enable it, a message is displayed on the host, prompting the to-be-performed scanning. You can customize the message content as required. Note Only hosts enabled with the messaging service can receive messages.
	Ignore Plugin Dependency	You are advised not to enable it in normal circumstances. Plugins in RSAS have different responsibilities. For example, plugin 1 is responsible for identifying the target's operating system type, and plugin 2 is responsible for scanning a certain vulnerability in Windows operating systems. If plugin 2 relies on plugin 1's scan result and plugin 1 detects that the target operating system is not Windows, plugin 2 is skipped, increasing the scanning speed and accuracy.

Section	Parameter	Description
	Remote OpenSSH Version Scan/Remote NTP Version Scan	You are advised not to enable it in normal circumstances. Controls whether to remotely check OpenSSH or NTP versions. Note The default disabled setting is recommended for a more accurate scan result. After it is enabled, you should determine whether risks discovered in the scan are false positives.
	Oracle Deep Scan	• Disable: indicates that RSAS only identifies Oracle-related services and reports vulnerabilities of the thorough scan type. • Enable: indicates that RSAS reports all vulnerabilities, including local vulnerabilities regarding the Oracle service. For this purpose, you need to enable and configure Oracle parameters for the vulnerability scanning policy, in addition to Manually Adding Authentication Information.
	Debug Mode	This parameter is useful when an error occurs during scanning. If the debug mode is enabled, task execution information is recorded. When an error occurs, the error information will be exported and sent to the technical support personnel of NSFOCUS for analysis.
Coding Language	Encoding Used by Target System	Specifies the coding language for the target system. Its values include **Simplified Chinese (GBK)** and **Unicode (UTF-8)**.

Table 4-6 Report export parameters for an assessment task

Parameter	Description
Report Format	Specifies the format of the report to be generated, which can be **HTML**, **WORD, EXCEL**, **PDF**, and/or **XML**.
Report Type	• **Summary Report**: A summary report comprehensively analyzes an assessment task, describes and presents risks, as well as presents the vulnerability-related graphs, operating system distribution, account information, and assessment criteria. • **Host Report**: A host report analyzes and details risks of a single host. A host report contains a host's scan data, various profile information, vulnerability list, and solution. To analyze problems occurring in a scanning task, you need to generate a host report.
Summery Rpt Template/Host Rpt Template	If no suitable report template is available, you can click **Report Template Management** and add a report template on the **Report Template Management** page that appears. For how to add a report template, see Report Template.
Auto Generation	• If it is enabled, an offline report of the specified type will be generated when the task is complete and this report will be sent to the given email address. In addition, the offline reports will be added to the report list. For details, see Report List. • Whether auto generation is enabled or not, an online report of the HTML format will be generated when the task is complete. For details, see Assessment Task Report.
Upload via FTP	This parameter can be configured only after **Auto Generation** is enabled. If this option is enabled, RSAS automatically uploads offline reports to the

Parameter	Description
	specified report FTP server. In this case, you must configure the report FTP server. For details, see Report FTP.
Send Report	This parameter can be configured only after **Auto Generation** is enabled. If this option is enabled, RSAS automatically sends offline reports to the specified email address. In this case, you must configure the email server. For details, see Mail Server. • **Report Format**: specifies the format of the report file. • **Email**: specifies the email address for receiving reports. A maximum of five email addresses can be configured. Multiple email addresses should be separated by the comma (,), semicolon (;), carriage return, or space.

4.1.2 Password Guess Task

Password guess tasks can be conducted on active hosts. RSAS attempts to log in to the target host using user names and passwords described in Password Dictionary. If the login succeeds, vulnerable accounts exist on the target host.

Choose **New Task > Task Types > Password Guess Task** and configure the parameters, as described in Figure 4-1, Table 4-4, and Table 4-5.

4.1.3 Web Application Scanning Task

With web application scanning, RSAS performs remote security scanning and security checks for customers' Internet websites by continuously crawling, analyzing, and matching web pages of target websites according to supervisory requirements of website administrators. In this way, RSAS can provide a complete monitoring solution to securing websites.

Choose **New Task > Task Types > Web Application Scanning** and configure parameters.

- Click **Create** to create a task.
- Click **Save** to save the task as a scanning policy.

Table 4-7 to Table 4-13 describe parameters for configuring a web application scanning task.

Table 4-7 Basic parameters for a web application scanning task

Parameter	Description
Existing Configuration (optional)	**Policy**: Creates a task based on an existing scanning policy (namely, task template). • Click **Set as Default** to set the task as the default scanning policy. Then the system can directly call this policy to create a task for another scan target. • Click **Reset** to restore default settings.
	Historical task: Creates a task based on an existing task.
Scan Target	Specifies the scan target. You can type specific scan targets in the text box or upload a target file. For details about the scan target format, hover over ? next to the parameter.
Task Name	Specifies the name of the new task. After the scan target is specified, the task name will

Parameter	Description
	be generated automatically. Alternatively, you can specify a different name. The task name should be a string of 1–256 characters.
Scan Scope	Specifies the crawling scope of crawlers, which can be one of the following: • **Scan by domain name** - **Scan whole website**: scans all URLs under the parent domain and each of its subdomains. - **Scan subdomains**: scans all URLs under the parent domain and only its subdomains specified here. - **Do not scan subdomains**: scans all URLs under the parent domain name and other subdomain names than the specified ones. • **Scan current directory and subdirectories**: scans the URLs under the directory specified with **Scan Target** and all its child directories. • **Scan target URL**: scans URLs specified with **Scan Target**.
Execution Mode	• **Instant**: indicates that the task will be executed immediately after you complete the configuration. This is applicable where network security assessment should be immediately conducted. • **Scheduled**: indicates that the task will be executed as scheduled. This is applicable where network security assessment should be conducted during off hours. • **Daily, Weekly, Monthly (date)**, or **Monthly (day of the week)**: indicates that the task will be executed repeatedly as scheduled. This is applicable where network security assessment should be conducted regularly (daily, weekly, or monthly). • **Advanced configuration**: indicates that the task will be executed repeatedly as scheduled. You can set the cycle lengths and specify multiple cycles by clicking **Add**.
Vuln Template	Specifies the vulnerability templates used for scanning. For operations on vulnerability templates, see Vulnerability Template. You can select **Auto match scan** or use default templates or custom templates that you have permissions to load. • **Auto match scan**: RSAS calls the templates matching the scan target for vulnerability scanning. • **Verifiable Vulnerabilities Scan:** RSAS only scans vulnerabilities that can be verified. If such vulnerabilities are detected, you can verify them. For details, see Verifying Vulnerabilities. • If RSAS scans and detects verifiable vulnerabilities that are included in other templates, you can verify them. For details, see Verifying Vulnerabilities.
Auto Vuln Verification	Controls whether the vulnerabilities are verified. After it is enabled, the POC verification principle and vulnerability verification template are used to accurately verify vulnerabilities in assets.
Scan Time Frame	Specifies the periods in which this scanning task will be executed. After you specify periods, RSAS will execute this task only in the specified periods regardless of the setting of **Execution Mode**.
Scheduling Priority	Specifies the priority of this task. RSAS determines the task priority based on the specified priority value and the background algorithm.
Debug Mode	This parameter is useful when an error occurs during scanning. If the debug mode is enabled, task execution information is recorded. When an error occurs, the error information will be exported and sent to the technical support personnel of NSFOCUS for analysis.

Table 4-8 Authentication configuration parameters for a web application scanning task

Parameter	Description
Scan Target	This parameter is specified in the same way as **Scan Target** described in Table 4-7.
Protocol Authentication	Specifies the authentication protocol used by the scan target, which can be **Auto recognition**, **NTLM**, **Basic** or **Digest-MD5**.
Login Scan	Controls whether to scan upon login to the target. • **Preset cookie**: You need to type cookies to record login session IDs, for example, **action=login&username=admin&password=admin88**. • **Prerecord login**: You need to click **Record** and continue as prompted in the dialog box that appears. Then, related cookies will be recorded.
User Name/Password	Specifies the user name and password for login to the scan target. RSAS stores the user name and password in an encrypted way to ensure security.
Custom Link	Specifies URLs to be scanned. External links are allowed here. Multiple links should be separated by the comma (,), semicolon (;), carriage return, or space.
Excluded Link	Specifies the URLs excluded from crawling.

Table 4-9 Proxy configuration parameters for a web application scanning task

Parameter	Description
Proxy Type	Specifies the type of the proxy server, which can be **SOCKS4**, **SOCKS5**, or **HTTP**.
Protocol Authentication	Specifies the authentication protocol used by the proxy server, which can be **NTLM**, **Basic**, or **Digest-MD5**.
Server Address/Port	Specifies the address or port of the proxy server. The server address can be an IP address and domain name.
User Name/Password	Specifies the user name and password used to log in to the proxy server. You must configure both the user name and password.
Connectivity Test	After the parameter configuration is complete, you can click **Connectivity Test** to check whether the system can properly connect to the proxy server.

Table 4-10 Web scan options and web access policy parameters for a web application scanning task

Parameter	Description
Scan Level	• **Deep scan**: The scan plugin calls all detection logic and takes a long time. • **Fast scan**: The scan plugin does not call time-consuming detection logic and thus takes a short time. • **Intelligent scan**: It takes acceptable time.
Concurrent Threads	Specifies the number of concurrent threads of web scan plugins. A larger value

Parameter	Description
	indicates a higher scanning speed. Note When specifying the value, consider the network bandwidth and the processing capability of the server. An inappropriately large value would affect the proper running of the target server.
Timeout	Specifies the maximum time allowed for scanning a page.
Max Request Attempts	Specifies the allowed number of attempts to send a scan request.
Web Encoding Method	Specifies the web encoding method of websites to be crawled. The value must be correct so that RSAS can properly access the target. • **Auto detect**: RSAS automatically matches the web encoding method. • **Manual detect**: You need to specify the web encoding method used by the specified scan target. Options include **Simplified Chinese (GB18030)**, **BIG5**, and **Unicode(UTF-8)**.
Custom User-Agent	Specifies the browser or search engine through which RSAS accesses the scan target. You need to first turn on the switch and then define the user agent in the text box.
Custom Header	Specifies the header of a custom request used for crawling and scanning websites. You can click **Add** to create a header. For websites that require a specific header for vulnerability scanning, configure this parameter.

Table 4-11 Web detection policy parameters for a web application scanning task

Parameter	Description
DNSLog	Controls whether to enable the built-in DNSLog platform. This function determines the existence of vulnerabilities based on whether a specific DNS is requested, because remote code execution vulnerabilities such as Fastjson and Log4j2 are not echoed but trigger specific DNS requests. By default, DNSLog is not enabled.
Custom Weak Password	Detects whether websites have a weak password. • You can click **Add** to configure a custom account and weak password. • You can click **Click to Upload** to import a TXT file of weak passwords.

Table 4-12 Web crawling policy parameters for a web application scanning task

Parameter	Description
Crawling Sequence	Specifies the preferable method to obtain URLs during scanning.
Files in a Single Directory	Specifies the maximum number of files to be scanned in each directory when page deduplication is configured. The value is an integer equal to or greater than -1, with **-1** indicating no limit.
Directory Depth	Specifies the number of directory levels that will be crawled. • The value **-1** indicates no limit.

Parameter	Description
	- The directory depth equals the number of slashes (/) following the website name, counted from the root directory. A greater depth value indicates a wider scan scope and a longer scan time. Therefore, you need to set a proper value.
Total Links	Specifies the total number of URLs to be obtained. The value is an integer equal to or greater than -1, with **-1** indicating no limit.
Excluded Extension	Specifies file name extensions that should not be crawled. The extension is a string of digits and letters. Multiple extensions must be separated by a comma (,).
Case-Sensitive	Controls whether the system distinguishes between uppercase and lowercase letters for URLs to be scanned.
Parse Flash File	Controls whether to scan Flash files. Currently, only files of Flash earlier than V10 can be parsed.
Execute JavaScript	Controls whether to execute JavaScript code on pages to obtain the URL during crawling. - Enable: JavaScript code will be executed and simulate various events. - Disable: JavaScript code will not be executed, which will improve the scanning speed but miss out some links.
Link Deduplication Policy	Specifies the level of the link deduplication policy. Generally, a URL is a quintuplet that consists of the page, method, query-name, query-value, and post-data. The URL deduplication level determines the elements based on which RSAS distinguishes URLs. The URL http://www.nsfocus.com/test.php?login=admin is used as an example to describe URL deduplication. Elements of this URL are listed as follows: - page=http://www.nsfocus.com/test.php (page = protocol + domain name + path file) - method=GET - query-name=login - query-value=admin - post-data=NULL For this URL, the deduplication level is described as follows: - **Sensitive to pages**: The deduplication is based on the page. - **Sensitive to page and request methods**: The deduplication is based on the page and method. - **Sensitive to pages, request methods, and parameter names**: The deduplication is based on the page, method, and query-name. - **Sensitive to pages, request methods, parameter names, and GET parameter values**: The deduplication is based on the page, method, query-name, and query-value. - **Sensitive to pages, request methods, parameter names, GET parameter values**, **and POST data**: The deduplication is based on the page, method, query-name, query-value, and posted data. A higher deduplication level indicates that more elements are compared for deduplication. For example, if the deduplication level is **Sensitive to pages**, two URLs with the same page element are considered identical.
Directory Guess Scope	Specifies the guess scope of common sensitive directories and files in each directory. - The value **0** indicates that no directories or files will be guessed.

Parameter	Description
	• A larger value indicates more directories and files to be guessed but a longer scanning time.
Directory Guess Depth	Specifies the link depth of sensitive directories or files to be guessed. This value cannot be greater than that of **Directory Depth** as described in Table 4-12.
Backup File Check Type	Specifies the types of files that will be checked for backups. Multiple types should be separated by the comma (,).
Backup File Extension	Specifies the extensions of files that will be checked for backups. This parameter is used with **Backup File Check Type**. Multiple file name extensions should be separated by the comma (,).
Form Filling	Controls whether to fill in page forms to scan more URLs for more vulnerability information during the execution of a web application scanning task. After **Form Filling** is enabled, you need to specify names and values so that RSAS matches page forms with the specified names and assigns the specified values to the matched names. Clicking **Add** can add a name and its value.
Rendered Crawling Policy (visible when RSAS memory is no less than 8 GB)	After it is enabled, the crawler will simulate human interaction to intelligently analyze crawled web pages. You are advised to enable this function for a web 2.0 website whose front end is separate from its backend.
	Intelligent Form Filling: RSAS automatically fills in data that complies with form specification to obtain more links.
	Concurrent Pages: limits the total number of concurrent pages for rendered crawling. Its value varies with device models. • Hardware edition: The value is 1–5 for models E and H, and 1–2 for model S. • Virtual edition: depending on the memory size. This parameter is unavailable if the memory is less than 8 GB. The value is 1–2 for memory ranging from 8 GB (inclusive) to 16 GB, and 1–5 for memory greater than 16 GB.
	• **Crawling Filtering Policy**: When finding that a link matches the crawling filter, RSAS stops crawling it for more links • **Result Filtering Policy**: When finding that a link matches the result filter, RSAS stops scanning it for vulnerabilities and will not include related information in the scanning report. RSAS neither crawls new links nor performs vulnerability scanning and result display for a link that matches both policies.
	localStorage Configuration: This parameter is required for websites that use the localStorage authentication so that RSAS can obtain more links after login to websites. For how to obtain the configuration, hover over ? next to the parameter.
	Session Storage Configuration: This parameter is required for websites that use the sessionStorage authentication so that RSAS can obtain more links after login to websites. For how to obtain the configuration, hover over ? next to the parameter.

Table 4-13 Report export parameters for a web application scanning task

Parameter	Description
Report Format	Specifies the format of the report to be generated, which can be **HTML**, **WORD**,

Parameter	Description
	EXCEL, **PDF**, and/or **XML**.
Report Type	- **Summary Report**: provides a general analysis of the web application scanning task and describes and displays risks by type. It presents risk statistics graphs and vulnerability distribution from different perspectives and also presents the reference criteria. - **Website Report**: provides a risk analysis and detailed description of a single website, including risk statistics by type, web risk distribution, and vulnerability details. To analyze issues discovered during task execution, you need to generate a website report.
Summary Rpt Template/Website Rpt Template	If no suitable report template is available, you can click **Report Template Management** and add a report template on the **Report Template Management** page. For how to add a report template, see Report Template.
Auto Generation	If it is enabled, an offline report of the specified type will be generated when the task is complete and this report will be sent to the given email address. In addition, the offline reports will be added to Report List. Whether auto generation is enabled or not, an online report of the HTML format will be generated when the task is complete. For details, see Web Application Scanning Task Report.
Upload via FTP	This parameter can be configured only after **Auto Generation** is enabled. If this option is enabled, RSAS automatically uploads offline reports to the specified report FTP server. In this case, you must configure the report FTP server. For details, see Report FTP.
Send Report	This parameter can be configured only after **Auto Generation** is enabled. If this option is enabled, RSAS automatically sends offline reports to the specified email address. In this case, you must configure the email server. For details, see Mail Server. - **Report Format**: specifies the format of the report file. - **Email**: specifies the email address for receiving reports. A maximum of five email addresses can be configured. Multiple email addresses should be separated by the comma (,), semicolon (;), carriage return, or space.

4.1.4 Configuration Scanning Task

A configuration scanning task checks the scan target for possible noncompliant configuration items. After task execution, RSAS sends the scan results to the specified email address or FTP server, notifying the administrator of remediation. Also, RSAS provides task reports for the administrator to download for asset configuration risk analysis.

Online Configuration Scan

Online configuration scanning is applicable only to online target hosts. To configure such a task, choose **New Task > Task Types > Configuration Scanning** and configure parameters, as described in Table 4-1 to Table 4-6.

Offline Configuration Scan

To check the configuration compliance of an offline host, you need to download an offline check tool from RSAS to use this tool on the target host for local configuration scanning, and then import the scanning result to RSAS.

Offline check tools are associated with the imported certificate. Only authorized offline check tools can be downloaded.

The following describes how to configure local configuration scanning. For how to use other offline check tools, see the TXT file in the decompressed package. To configure local configuration scanning, follow these steps:

Step 1 Download an offline check tool from RSAS.

a. Choose **New Task** > **Task Types** > **Configuration Scanning** > **Offline Scan**, and click **Click to download an offline check tool**.

b. Choose **Knowledge Base** > **Offline Check**. Click **Download** in the **Operation** column of an offline check tool.

(Optional) If the configuration template of the downloaded offline check tool belongs to the MLPS group, you need to select an MLPS level.

Step 2 Perform the local configuration check task on the target host.

Open SecureCRT and choose **Script** > **Run**. In the dialog box that appears, select the downloaded offline check tool. After the script is successfully executed, a configuration check result file (*IP_UUID_chk.xml*) will be generated in the same directory of the local offline check tool.

Step 3 Import the offline check result to RSAS.

The system will automatically generate a task, display it in the task list, and save the local configuration check result.

- Choose **New Task** > **Task Types** > **Configuration Scanning** > **Offline Scan**. Click **Click to Upload** and browse to the offline check result file.
- Choose **Scanning** > **Task List** and click **Import**.

Note	Only .xml, .txt, and .zip files can be imported.

----End

4.1.5 Image Scanning Task

Image scanning tasks check Docker image files for possible system vulnerabilities and noncompliant configuration items. Currently, each image scanning task supports scanning three image labels at most.

Choose **New Task** > **Task Types** > **Image Scanning** and configure parameters. Table 4-14 describes parameters for creating an image scanning task.

Table 4-14 Parameters for configuring an image scanning task

Parameter	Description
Scan Target	**Image Scanning**: scans image labels in public repositories. For details about how configure an image label, see the prompt on the UI.
	Repository: scans image labels in private repositories. • **Repository URL**: address of the private repository. Hover over ? next to the parameter to view the detailed format requirements. • **Repository User Name/Repository Password**: user name and password for access to the repository. • **Repository Type**: type of the repository, which can be **Harbor_API_V1.0** or **Harbor_API_V2.0**. • After the configuration of the image repository is complete, click **Obtain Image List** to display image labels in the configured repository.
Task Name	Specifies the name of the new task. After the scan target is specified, the task name will be generated automatically. Alternatively, you can specify a different name. It should be a string of 1–256 characters.
Execution Mode	• **Instant**: indicates that the task will be executed immediately after you complete the configuration. This is applicable where network security assessment should be immediately conducted. • **Scheduled**: indicates that the task will be executed as scheduled. This is applicable where network security assessment should be conducted during off hours. • **Daily, Weekly, Monthly (date)**, or **Monthly (day of the week)**: indicates that the task will be executed repeatedly as scheduled. This is applicable where network security assessment should be conducted regularly (daily, weekly, or monthly). • **Advanced configuration**: indicates that the task will be executed repeatedly as scheduled. You can set the cycle lengths and specify multiple scanning cycles by clicking **Add**.
Vulnerability Scan	Controls whether to perform vulnerability scanning for images.
Configuration Scanning	Controls whether to perform configuration compliance scanning for images. Click **View image configuration template** to open the **Image Template** page, where you can view the image configuration check templates available on RSAS.
Scheduling Priority	Specifies the priority of this task. RSAS determines the task priority based on the specified priority value and the background algorithm.

4.1.6 **Code Audit Task**

Code audit tasks discover security defects in code files and noncompliance with coding specifications.

Choose **New Task > Task Types > Code Audit** and configure parameters. Table 4-15 describe parameters for creating a code audit task.

Table 4-15 Parameters for configuring a code audit task

Parameter	Description
Task Name	Name of the code audit task. It should be a string of 1–256 characters.
Code Source	**Manually uploaded file**: audits local code files for security defects and compliance with coding specifications.
	SVN: audits code files obtained from SVN for security defects and compliance with coding specifications. • **Authenticate By**: Currently, only **Password** is available. • **Repository URL**: URL path of the SVN repository that stores code files. Hover over ? next to the parameter to view the detailed format requirements. • **User Name/Password**: user name and password for access to the SVN repository. • Click **Connectivity Test** to check whether RSAS is properly connected to the repository.
	GIT: audits code files obtained from GIT for security defects and compliance with coding specifications. • **Repository URL**: URL path of the GIT repository that stores code files. Hover over ? next to the parameter to view the detailed format requirements. • **Authenticate By**: authentication mode for login to the GIT repository to obtain code files. Parameter configuration varies with authentication modes. - **User Name/Password** (authenticated by **Password**): user name and password for access to the GIT repository. - **Key** (authenticated by **Key**): secret key for access to the GIT repository. - **TOKEN** (authenticated by **TOKEN**): authentication token for access to the GIT repository. - When **Authenticate By** is set to **None**, you can directly log in to the GIT repository without any authentication. • Click **Connectivity Test** to check whether RSAS is properly connected to the repository.
Defect Template	Specifies the defect template matching the programming language or content of code files to be audited.
Execution Mode	• **Instant**: indicates that the task will be executed immediately after you complete the configuration. This is applicable where network security assessment should be immediately conducted. • **Scheduled**: indicates that the task will be executed as scheduled. This is applicable where network security assessment should be conducted during off hours. • **Daily, Weekly, Monthly (date)**, or **Monthly (day of the week)**: indicates that the task will be executed repeatedly as scheduled. This is applicable where network security assessment should be conducted regularly (daily, weekly, or monthly). • **Advanced configuration**: indicates that the task will be executed repeatedly as scheduled. You can set the cycle lengths and specify multiple scanning cycles by clicking **Add**.
Scheduling Priority	Specifies the priority of this task. RSAS determines the task priority based on the specified priority value and the background algorithm.
Excluded File	Specifies the files that are excluded from code audit.

Parameter	Description
Excluded Folder	Specifies the folders that are excluded from code audit.
Task Description	Brief description of the code audit task. It should be a string of 0–256 characters.

4.1.7 Host Asset Detection Task

Host asset detection tasks detect information about hosts, such as status, open ports, and service applications. After detecting host information, RSAS records it under the device view and, at the same time, updates asset information in the organization view and OS view on the **Asset List** page accordingly.

Choose **New Task > Task Types > Host Asset Detection** and configure parameters. Table 4-1, Table 4-5, Table 4-6, and Table 4-16 describe parameters for creating a host asset detection task.

Table 4-16 Parameters for creating a host asset detection task

Tab Page	Parameter	Description
Basic Information	Scan Template	Specifies an asset label template used for scanning from the drop-down list.
	Associated Web Asset Detection	Controls whether to detect associated web assets. After it is enabled, RSAS also detects and records relevant information about web assets (websites) if the host opens a web port (that is, a web application exists).
Advanced Settings	Critical Pages	The value is **1**, indicating that RSAS only detects the URL corresponding to the open web port on the host asset. This parameter is available only when **Associated Web Asset Detection** is enabled on the **Basic Information** tab.

4.1.8 Web Asset Detection Task

Web asset detection tasks detect information about websites, such as the component framework, title, and logo. After detecting web information, RSAS records it under the device view and, at the same time, updates asset information in the organization view and OS view on the **Asset List** page accordingly.

Choose **New Task > Task Types > Web Asset Detection** and configure parameters. Table 4-7, Table 4-13, and Table 4-17 describe parameters for creating a web detection task

Table 4-17 Parameters for configuring a web detection task

Page	Parameter	Description
Basic Information	Associated Host Asset Detection	Controls whether to detect associated host assets. After it is enabled, RSAS updates information such as tge IP address, system, open ports, and service applications of the host related to the detected web asset (website) to the Asset module. If this function is not enabled, such information will not be updated.

Page	Parameter	Description
Advanced Settings	Critical Pages	The value is **1**, indicating that RSAS only detects the URL corresponding to the web asset.
	Plugin Timeout	A single plugin that does not end within specified time will be terminated by the scheduler. Value range: 1–300, in seconds.
	Debug Mode	This parameter is useful when an error occurs during scanning. If the debug mode is enabled, task execution information is recorded. When an error occurs, the error information will be exported and sent to the technical support personnel of NSFOCUS for analysis.

4.2 Common Scanning Policies

Common scanning policies help you quickly determine the application scenario and complete configurations, simplifying your operations. Table 4-18 lists scanning policies available on RSAS.

Choose **New Task**, click a required policy under **Common Scanning Policies**, and configure the scan target to quickly create a task. Click **Configure Common Scanning Policies** to manage the policies that are visible under **Common Scanning Policies**. A maximum of 10 policies are displayed.

Table 4-18 Common scanning policies

Name	Function	Parameter
Full Self-Check Policy	Assessment task that scans all vulnerabilities and ports	**Vuln Template** on the **Basic Information** tab: Full Vulnerability Scan **Port Scanning Policy** on the **Advanced Settings** tab: Full port scan
Accurate Supervision Policy	Assessment task that performs thorough vulnerability scanning to ensure accuracy	**Vuln Template** on the **Basic Information** tab: Thorough Scan
Emergency Vulnerability Scanning	Assessment task that scans new popular vulnerabilities	**Vuln Template** on the **Basic Information** tab: Critical Vulnerabilities Scan
High-Frequency & High-Risk Vulnerability Detection Policy (System)	Assessment task that scans high-frequency & high-risk system vulnerabilities frequently exploited in cyber exercises	**Vuln Template** on the **Basic Information** tab: Frequent, Risky Vulnerabilities for Cyber Exercises
High-Frequency & High-Risk Vulnerability Detection Policy (Web)	Web application scanning task that scans high-frequency & high-risk application vulnerabilities frequently exploited in cyber exercises	**Vuln Template** on the **Basic Information** tab: Frequent, Risky Vulnerabilities for Cyber Exercises
System Vulnerability Verification Policy	Assessment task that uses the proof of concept (PoC) to accurately check whether a vulnerability exists in assets	**Vuln Template** on the **Basic Information** tab: Verifiable Vulnerabilities Scan **Auto Vuln Verification** on the **Basic**

Name	Function	Parameter
		Information tab: enabled
Web Vulnerability Verification Policy	Web application scanning task that uses PoC to accurately check whether a vulnerability exists in web	**Vuln Template** on the **Basic Information** tab: Verifiable Vulnerabilities Scan **Auto Vuln Verification** on the **Basic Information** tab: enabled
Cloud Computing Vulnerability Scan Policy	Assessment task that scans the cloud computing components for vulnerabilities	**Vuln Template** on the **Basic Information** tab: Cloud computing vulnerability scan
Big Data Vulnerability Scan policy	Assessment task that scans common big data services for vulnerabilities	**Vuln Template** on the **Basic Information** tab: Big data vulnerability
IoT Vulnerability Scan Policy	Assessment task that scans common IoT devices for vulnerabilities	**Vuln Template** on the **Basic Information** tab: IoT vulnerability

5 Scan Management

A scanning policy is a task template, which generates a scanning task after policy execution. The New Task module provides a quick access to task creation and policy management. The Scanning module allows you to manage all scanning policies and tasks.

This chapter contains the following sections:

Section	Description
Scanning Policy	Describes how to manage scanning policies.
Task List	Describes how to manage scanning tasks.

5.1 Scanning Policy

Choose **Scanning** > **Scanning Policy**. Click **Create Policy** and configure parameters. Table 5-1 describes parameters for configuring a scanning policy. A maximum of 40 custom scanning policies can be created for each user. After creating a scanning policy, you can perform the following operations:

- Click **Create task** to generate a scanning task based on the policy.
- Click **Configure Common Scanning Policies** to display it under **Common Scanning Policies** on the **New Task** page.
- You can query, view, edit, or delete it, or save it as another scanning policy.

Table 5-1 Parameters for configuring a scanning policy

Parameter	Description
Policy Name	Name of the new scanning policy. It cannot contain more than 16 characters.
Policy Description	Brief description of the scanning policy. It cannot contain more than 64 characters.
Task Type	Specifies the task type to which the new policy is applied. Parameter configurations vary with the task type selected. For detailed parameters of scanning tasks, see New Task.

5.2 Task List

Choose **Scanning > Task List**. The **Task List** page appears.

The operations that can be performed on tasks vary with the task status, as described in Table 5-2. Operations allowed for tasks are described in Table 5-3.

Table 5-2 Allowed operations depending on the task status

Operation	Unstarted Task	Ongoing Task	Suspended Task	Complete Task	Abnormal Task	Imported Task	Parent Task	Child Task	Periodic Task
Edit	-	-	-	√	√	√	√	√	√
Delete	√	√	√	√	√	√	√	√	√
Stop	√	√	√	-		-	-	√	√
Suspend	-	√	-	-		-	-	√	√
Continue	-	-	√	-		-	-	√	√
Rescan	-	-	-	√	√	-	√	-	-
Resume	-	-	-	√	-	-	-	√	√
Verify	-	-	-	√	-	-	-	√	√

Table 5-3 Supported task operations

Operation	Description
Create Scan Task	Creates a scanning task. For details, see Task Type.
Import	Imports XML, TXT, or ZIP files. Afterwards, a report will be automatically generated. You can not only import the scan result file (an .xml file) of a single host, but also import the scan results (a .zip file) of multiple hosts sharing a template.
Suspend	Note that image scanning tasks cannot be suspended in batches.
Continue	Continues scanning a task that has been suspended.
Rescan	Creates a task by invoking original task parameters and performs the new task, with the original scan result retained. After rescanning, a parent task is generated with the original task and new task as its child tasks. The report of the parent task is a consolidated report of the last child tasks. The time the rescanning task starts and ends is taken as the start and end time of the parent task. Rescanning is applicable to stopped and completed tasks, imported tasks, and parent tasks generated by rescanning, but not to child tasks and periodic tasks. You can view the differences in scan results of child tasks through a comparative analysis of the parent task.
Resume	Resuming a scanning task means to rescan targets that failed to be covered by the complete task. After resuming, a new task is automatically generated. Code audit tasks, web application scanning tasks, periodic tasks, child tasks, and imported tasks cannot be resumed.
View	Displays a consolidated report, which covers the scan results of multiple tasks for

Operation	Description
Consolidated	unified analysis. For details, see Report Management. This function is inapplicable to code audit tasks.
Export Report	Generates reports for selected tasks. To export a task report, select tasks and click **Export Report**. For details, see Report Management.
Verify	Verifies vulnerabilities that were found by using PoCs. After the **Filter by verification** switch is turned on, only the tasks that support vulnerability verification are displayed in the task list. Clicking **Verify** or **Bulk Operation** > **Verify** re-executes a task or tasks. After the verification is complete, click **View results** to check the vulnerability verification status on the Host Information page of its summary report. For details, see Verifying Vulnerabilities in a host report.
Query	Only system administrators with access to the task list can search for scanning tasks issued by other users. Common administrators can only view tasks created by themselves.
Edit	You can manage a task by clicking its name in the task list and performing operations on the **Task Parameters** tab page. A code audit task cannot be managed in this way. - Change its name: Click **Rename** to rename the task. After the modification, a new task is automatically generated. - Download its logs: Click **Download Log** to download fault diagnosis logs to a local disk drive, and then send them to the technical support personnel of NSFOCUS for troubleshooting. - Export its debugging information: Click **Export Debug Info** to save debugging information to a local disk drive. - Export the task: Click **Export** to save it to a local disk drive. - Edit the scanning task: Click **Edit** to create a scanning task based on the scanning policy of this task.

6 Asset Management

Asset management allows the administrator to manage assets on the target network. Network assets are named in a normalized manner in the asset repository based on the structure and topology of the target network for centralized management by RSAS.

The default system administrator (**admin**) can operate on all assets. System administrators and common administrators with the viewing or management permission can view or manage only the assets within their privileges.

This chapter describes how to manage assets on RSAS. It contains the following sections:

Section	Description
Asset List	Describes how to logically classify and manage assets.
Asset Label Library	Describes how to view and query templates in the asset label library.

6.1 Asset List

Choose **Asset >Asset List** to manage assets.

6.1.1 Statistical Data and Asset Views

Statistical Data

RSAS presents risk statistics of all assets in the asset list. Table 6-1 describes the statistics you can view on the **Asset List** page.

Table 6-1 Risk statistics

Item	Description
Assets	Displays the total number of assets and the numbers of IP hosts and web assets.
Ports	Displays the numbers of open ports and vulnerable ports on assets.
Risk Score	Displays the overall risk score, vulnerability risk score, and configuration risk score of all assets.

Asset View

An asset view logically manages assets by category. Currently, RSAS supports the following asset views as describes in Table 6-2.

Table 6-2 Asset views

Tab	Asset View	Description	Allowed Operation
Host/Web	Organization View	Allows you to manage assets as required from the organizational structure dimension. You need to manually add a node and its asset. After an asset is added: • RSAS refreshes the host asset information scanned from Assessment Task, Host Asset Detection Task, and Web Asset Detection Task (with associated host assets detected) to this view on the **Host** tab. • RSAS refreshes the web asset information discovered from Web Application Scanning Task, Web Asset Detection Task, and Host Asset Detection Task (with associated web assets detected) to this view on the **Web** tab.	All operations on assets
Host	OS View	Allows you to manage assets as required from the operating system dimension. You need to manually add an asset. After an asset is added: RSAS refreshes the host asset information scanned from Assessment Task, Host Asset Detection Task, and Web Asset Detection Task (with associated host asset detected) to this view.	All operations on assets
Host	Device View	Allows you to manage assets as required from the device type dimension. RSAS provides default nodes, which cannot be modified. You need to manually add an asset. After an asset is added: RSAS refreshes the host asset information scanned from Assessment Task, Host Asset Detection Task, and Web Asset Detection Task (with associated host assets detected) to this view.	Refresh asset tree and add device

6.1.2 Adding an Asset

The asset view consists of network nodes and devices. A node logically manages assets by category. To manage assets, add a node and then add its assets. An asset added to any view will be mapped to other views that have related attributes.

Adding a Node

Choose **Asset >Asset List > Host/Web**. Select **Organization View**, click ⋮ > **New Node**, and configure parameters. Table 6-3 describes parameters for configuring a node.

Table 6-3 Parameters for adding a node

Parameter	Description
Node Name	Specifies the name of the node. It should contain a maximum of 40 characters.
IP Range	Specifies the IP address range of the host managed by the node, which can be IPv4 or IPv6 addresses. This parameter is required when the node is created for the organization view on the **Host** tab.
MLPS Level	Specifies the MLPS level of the node. For details, see MLPS. This parameter is required when the node is created for the organization view on the **Host** tab.
Node Administrator	Specifies the administrator of the node. The administrator name should contain a maximum of 30 characters.
Email	Specifies the email address of the node administrator. A maximum of five email addresses are allowed. Multiple email addresses should be separated by the comma (,).
Description	Supplementary information for this node.

Adding an Asset

Choose **Asset >Asset List**. Click ⋮ next to the view, select **New Device**, and configure parameters. Table 6-4 describes parameters for configuring a device.

Table 6-4 Parameters for adding a device

Parameter	Description
Device Name	Specifies the name of the asset. It should contain a maximum of 40 characters.
IP Address	Specifies the IP address of the asset, which can be an IPv4 or IPv6 address.
Add To	The management node is the upper-level network node and the ungrouped node is **Ungrouped** in the **Organization View**. If **Management node** is selected, the system categories the device to a node based on the device's IP address range. If no appropriate node is found, the device will be categorized to **Ungrouped**.
OS	Specifies the operating system of the asset.
Device Type	Specifies the device type of the asset.
MLPS Level	Specifies the MLPS level of the asset. For details about MLPS levels, see MLPS.
Weight	Specifies the weight for the criticality of the device. The weight is used to calculate the risk level of the host and network. As the weight increases, both the criticality and risk score of the device rise.
Device Admin	Specifies the administrator of the asset. It should contain a maximum of 30 characters.
Email	Specifies the email address of the asset administrator. A maximum of five email addresses are allowed. Multiple email addresses are separated by comma (,).
Description	Supplementary information for this asset.
Configure	Creates authentication for the IP address. For the description of parameters, see

Parameter	Description
authentication information	Table 9-1.

Operating on Assets

Choose **Asset >Asset List**. After adding an asset or a node, you can query, modify, or delete it, and perform other operations as described in Table 6-5.

Table 6-5 Allowed asset operations

Operation	Description
Import assets	Two import methods are supported. • **Full import**: clears existing assets and imports all assets in the file. • **Incremental import**: updates existing assets and adds new assets in the file to the asset list. Note To obtain the asset template, you can first export assets, edit the exported file, and save it as the asset file.
Export assets	Click **Export Assets** to save it to a local disk drive.
Clear assets	Click 🗑 and select items to be deleted. The options are as follows: • Clear basic information of management nodes and host assets. • Clear login authentication information associated with assets. • Clear configuration check information associated with assets.
Refresh assets	Click ⟳ to display the result of the current scanning task on the **Asset** page.
View	Click **View** to view the asset report. For details, see Asset Report.
Task	Click **Task** to issue an assessment task for the current node or asset. For how to configure an assessment task, see Assessment Task or Web Application Scanning Task.
Register/Deregister a device	Click **Register** or **Deregister** to register the the current asset in the database or deregister it, which is only for asset ledger statistics. RSAS automatically marks assets that are registered at the time of manual addition or import as registered assets. For assets that are not registered when you discover them in other ways or import them, you need to manually register them.

6.2 Asset Label Library

Templates provided in the asset label library are the basic scanning templates for host and web asset detection tasks. Currently, RSAS only allows you to use built-in templates, whose contents cannot be edited.

Choose **Asset >Asset label Library** to query and view templates and their information.

7 Report Management

RSAS provides reports on scanning task results. A report contains statistics in various aspects for the last scanning task and visualizes the network security status using graphs and texts.

This chapter describes how to manage reports. It contains the following sections:

Section	Description
Report Management	Describes how to generate a report and manage offline reports.
Report Template	Describes how to manage report templates.
Task Report	Describes online task reports in detail.
Asset Report	Describes online asset reports in detail.

7.1 Report Management

You can export the scan result as an offline report of the specified format based on the configured conditions. An offline report can be generated only after a task is complete.

Generating a Report

Table 7-1 lists offline report formats supported by RSAS.

Table 7-1 Offline report formats available on RSAS

Task Type	HTML HTML	WORD Word	EXCEL EXCEL	PDF PDF	XML XML
Assessment Task	√	√	√	√	√
Password Guess Task	√	√	√	√	√
Web Application Scanning Task	√	√	√	√	√
Configuration Scanning Task	√	√	√	√	√
Image Scanning Task	√	√	√	×	×
Code Audit Task	√	√	√	×	×

Task Type	HTML HTML	WORD Word	EXCEL EXCEL	PDF PDF	XML XML
Host Asset Detection Task	√	×	√	×	×
Web Asset Detection Task	√	×	√	×	×

Choose **Report** > **Report Management**. Click **Generate Report** and configure report export parameters. Table 7-2 describes parameters for generating an offline report.

- During the process, you can click **Stop** to stop the export.
- After the report is successfully exported, click HTML/Word/EXCEL/PDF/XML/**Download recent reports** to open the **Report Management** page, where you can view or download offline reports.

Table 7-2 Report export parameters

Item	Parameter	Description
Task	Output Scope	• **Common scan task**: indicates that an offline report will be generated based on the scanning data of an assessment task, password guess task, or local configuration scanning task. • **Web application scanning task**: indicates that an offline report will be generated based on the scanning data of a web application scanning task. • **Image scanning task**: indicates that an offline report will be generated based on the scanning data of an image scanning task. • **Code audit task**: indicates that an offline report will be generated based on the scanning data of a code audit task. • **Host asset detection task**: indicates that an offline report will be generated based on the scanning data of a host asset detection task. • **Web asset detection task**: indicates that an offline report will be generated based on the scanning data of a web asset detection task.
	Show recent	Specifies the number of recent tasks to be listed. The setting here determines how many tasks are displayed in the task list and how many scan targets displayed.
	Task list	You can select one or more scanning tasks from the task list.
	Filter Hosts/Filter Websites/Filter Images	Specifies the scan targets that are included in the reports. This parameter varies with the task type, which is available to the common scan task, web application scanning task, or image scanning task.
Offline Report	Report Format	Specifies the format of reports to be exported.
	Report Type	Specifies what types of reports to be exported. This parameter varies with the task type. For each report type, you need to specify the report template and report title. If no suitable report template is available, you can click **Report Template Management** and add a report template on the **Report**

Item	Parameter	Description
		Template Management page. For how to add a report template, see Report Template. Report templates cannot be modified for image scanning tasks and code audit tasks. Neither report template nor report title can be modified for host asset detection tasks or web asset detection tasks.
Consolidated Report	Single-Task Output	Specifies the report name for the selected single task. You only need to configure the report name.
	Multitask Output	For multitask output, you need to specify the output method and the report name. • **Combined output**: presents scanning data of all selected tasks in one report. • **Bulk output**: presents scanning data of each selected task in a separate report.
Subtask Mode	Subtask Mode	Controls the display scope of child tasks in a report. • Disable: presents only scanning data of the latest child task of the parent task in a report. • Enable: presents scanning data of all selected child tasks of the parent task in a report. In this case, you need to first select the child tasks.

You can view the generated reports on the Report Management page. Reports can also be generated in the following ways:

- Configuring report export during task creation
  - This method is unavailable to image scanning tasks and code audit tasks.
  - For details about how to configure report export when creating a task, see New Task.
- Exporting a report from a specific statistics page
  - A report exported from the **Summary** page is of the default structure.
  - Choose **Scanning** > **Task List**. Click a task name or select multiple tasks of the same type and then click **View Consolidated** to navigate to the **Summary** page. Click **Generate** and select a desirable report format.
- Exporting a report from the **Task List** page
  - A report exported from the **Task List** page is of the default HTML structure.
  - Choose **Scanning** > **Task List**. Select multiple tasks of the same type, click **Export Report**, type a name for the combined report, and click **Combined output**.

Report List

All generated reports are saved to the report list. Choose **Report** > **Report Management**, where you can query, filter, download, and delete generated reports.

7.2 Report Template

You can configure a report template to specify what to be contained in a scanning report. On RSAS, report templates are classified as follows:

- Assessment task report templates, presented for assessment tasks, are divided into the following types:
  - Summary report template: for reports that reflect the security status of the target network
  - Host report template: for reports that reflect the security of an individual device
- Web scanning task report templates, presented for web application scanning tasks, are divided into the following types:
  - Summary report template: for reports that reflect the security status of target websites
  - Website report template: for reports that reflect the security of a single website

Choose **Report > Report Template** > **Assessment Task Report Template/WebScan Task Report Template > Summary Report/Host Report/Website Report**. Click **New Report Template** and configure report template parameters. A report template, after being created, can be viewed, edited, and deleted.

- Configure basic information.

  The name of the new template must be a string of 1 to 20 characters consisting of letters (case-sensitive), digits, Chinese characters, hyphens (-), and/or underscores (_). The template name must be unique.
- Click **Report Content** and select information to be displayed in a report.

7.3 Task Report

The default system administrator (**admin**) and system administrators with the report management permission can view online reports of all scanning tasks. Common administrators with the report management permission can view only reports of their own tasks. Whether the report of a task can be viewed depends on the task status:

- To-be-scheduled task

  As the task has not been performed yet, no scan result is available.
- Complete task, ongoing task, uncompleted task, and suspended task

  You can view the online report of such a task by clicking the task name in the task list.

Note

- An uncompleted task may be caused by an exception during scanning or manual intervention of an administrator.
- For an ongoing task, uncompleted task, or suspended task, the scanning process is incomplete. Therefore, the scan result is not exhaustive enough for you to determine the risk of the scan target.

7.3.1 Viewing Task Reports

You can view reports of an individual task and consolidated reports of multiple tasks.

On the **Summary** page of a task report, you can click **Refresh Cache** to refresh the current online report.

- Viewing the report of an individual task

  Choose **Scanning > Task List**. Click a task name to view its report. The **Summary** tab page of the task report appears. Click different tabs to view the report from different dimensions.
- Viewing the consolidated report of multiple tasks

  Choose **Scanning > Task List**. Select multiple tasks of the same type whose reports you want to view and click **View Consolidated**. The **Summary** tab page of the task report appears. Click different tabs to view the report from different dimensions.

Note

If an IP address, website, image tag, or URL appears in multiple tasks, the scan result of the task with the largest task ID will be displayed.

7.3.2 Assessment Task Report

An assessment task report can be a summary report or a host report, presenting the scan result of a vulnerability scanning task, configuration scanning task, or weak password guess task.

7.3.2.1 Summary Report

A summary report, as a panoramic display of the scan result, presents the overall security status of the scanned network. Reports of different assessment tasks may contain different types of information. The following takes scanning data of an integrated task (covering vulnerability and configuration scanning and weak password guess) as an example to present you details of a task report.

Table 7-3 shows detailed report information

Table 7-3 Information presented on a summary report

Tab	Item	Description
Task Parameters	Basic Information	Displays parameters of an assessment task.
	Advanced Options/Buttons	Presents operations allowed for the task. For details, see Table 5-3.
Summary	Task Information	Presents the network risk information (risk score and risk level), task name, task type, time statistics, vulnerability scanning template, configuration check template list, host statistics, and system version information.
	Risk Distribution	Presents the distribution of host vulnerabilities by risk level, distribution of overall host risks by level, distribution of host configurations by risk level, distribution of vulnerabilities by risk level, and distribution of noncompliant items by risk level.
	Vulnerability Risks	Presents the number of high-, medium-, and low-risk vulnerabilities by category (service, application, system, threat, time, and CVE year), and the overall statistics of vulnerabilities. Clicking the value in the table displays

Tab	Item	Description
		details about the corresponding vulnerabilities. Clicking the **All** tab, you can view statistics of all vulnerabilities displayed by category on the same page.
	Configuration Risks	Presents the distribution of noncompliant items in applications and in operating systems.
	Asset Overview	Presents the number and proportion of operating systems running on assets.
Host Information	Hosts by Risk Level	Provides risk information of all scanned hosts. • If a large number of hosts are involved, you can filter them by specifying the risk level (very vulnerable, vulnerable, safe, and/or very safe). • Clicking + before an IP address displays the scanning template used. • Clicking an IP address displays the corresponding host report. For details, see Host Report. • If RSAS collaborates with NSFOCUS Next-Generation Firewall (see Collaboration with NF), you can view the details of the protection associated with NF. If the system or web vulnerability verification scanning (see Verifying Vulnerabilities) is performed, you can check the vulnerability verification status.
	Collaboration with NF	After RSAS collaborates with NF (see Collaboration with NF), you can view the number of vulnerabilities addressed by NF. • On the **Host Information** tab of a summary report, you can view the number of vulnerabilities addressed by NF. In the host risk level list, if the **High**, **Medium**, and **Low** columns for **Vulnerabilities Addressed by NF** are all displayed as - for an IP address, this IP address is excluded from protection by NF; if a number is displayed in one of the three columns, this IP address is protected by NF. The **Vulnerabilities** column shows the number of vulnerabilities of each risk level that are fixed for an IP address under the protection by NF. • Clicking an IP address on the Host Information tab displays the corresponding host report. In the **Vulnerability Information** > **Overview** section, if **Yes** is displayed in the **Protected by NF** column for a vulnerability, this vulnerability is already protected against by NF; if **No** is displayed in this column, this vulnerability is not yet protected against by NF; if - is displayed in this column, this vulnerability is excluded from protection by NF.
Vulnerability Info	Vulnerability Distribution	Lists vulnerabilities of all types detected in the current task, including the vulnerability name and occurrence frequency. • If a large number of vulnerabilities are involved, you can filter them by specifying the risk level (high, medium, and/or low). • The **Vulnerability verification** area displays the number of verified vulnerabilities and verifiable vulnerabilities. • Clicking + before a vulnerability displays details about this vulnerability. What parameters such details contain varies with the specific vulnerability. In vulnerability details, clicking an affected host displays the corresponding host report. For details, see Host Report. • A vulnerability found by thorough scan is identified by **Thorough Scan** in its name.

Tab	Item	Description
		• A vulnerability that can be verified is identified by **Verifiable** in its name. Clicking + before a vulnerability name displays the verification method about this vulnerability.
Configuration Information	-	Lists noncompliant configuration items of all risk levels for the current task. Clicking a noncompliant host displays the corresponding host report. For details, see Host Report.
Configuration Hardening	-	You can view noncompliant items and then harden or roll back them only if your license covers the hardening module, a configuration scanning task is executed, and the scanning template chosen supports hardening. Whether a noncompliant check point can be hardened or not depends on the hardening knowledge base. RSAS can only harden your selected or all check items that are hardenable. Also, RSAS allows rollback of a hardened check item, restoring its configuration to the state before it is hardened. You can choose to roll back all or some of hardened check points. • You can harden one or more check items that are hardenable by following these procedures: On the noncompliance information list, click + before an IP address to view details of noncompliant check items and their check points. You can reconfigure hardening parameters as required or leave them at default settings. Select one or more handenable check items and click **Harden**. Then the hardening process starts. After hardening is complete, the **Hardening Status** and **Rollback Status** columns of these check items will be respectively displayed as **Hardened** and **Rollbackable**. • You can roll back one or more check items that are hardened by following these procedures. On the noncompliance information list, click + before an IP address to view details of hardened noncompliant check items and their check points. Select check items to be rolled back. Click **Roll Back**. Then the rollback process starts. • On the noncompliance information list, click + before an IP address to view its hardening information. Click **Hardened** in the **Hardening Status** column to view hardening details of a check item. • On the noncompliance information list, click + before an IP address to view its rollback information. Click **Rolled back** in the **Rollback Status** column to view rollback details of a check item. • The hardening configuration page will present the last hardening or rollback operation that is performed. On the noncompliance information list, click + before an IP address to view the last hardening or rollback operation. Click **Last operation: Hardening** to view details of the last operation.
Vulnerable Accounts	Vulnerable Application Accounts	Lists all vulnerable accounts detected in the current task. Clicking an IP address displays the corresponding host report. For details, see Host Report.
Reference Criteria	-	Presents reference standards for assessing system risks, including the following: • Risk level metrics for a single vulnerability

Tab	Item	Description
		• Risk level metrics for a single configuration item • Risk level metrics for a host • Risk level metrics for a network • Security recommendations
Comparative Analysis	-	The **Comparative Analysis** tab page, which is displayed only for a parent task, provides information about the child tasks with the largest ID among all complete child tasks. By default, comparative data of the last two child tasks is displayed. • You can select child tasks from the drop-down list of the parent task to compare their scanning data. • Clicking + before a vulnerability in the **Vulnerabilities** area displays details about this vulnerability. What parameters such details contain varies with the specific vulnerability. • Clicking an affected host in the **Vulnerabilities** area or an IP address in the **Vulnerable Accounts** area displays the corresponding host report. For details, see Host Report.

7.3.2.2 Host Report

You can view the detailed risk report of a host (that is, host report), obtaining information about the host, vulnerabilities, noncompliant configuration items, and status compliance.

The "Host Overview" section also displays **Data Source** and **Agent Data Collected at** if you turn on the **Full Agent Scan** switch for the assessment task.

In addition, RSAS identifies and displays the following asset types.

- Camera brands like Hikvision, Dahua, YAAN, Tiandy, Hanbang, Sunell, and D-link are displayed in section 1 "Host Overview".
- Homegrown operating systems like Deepin and NeoKylin are displayed in section 5.2 "Operating System Type".
- Homgrown applications like DedeCMS, PHPCMS, and Kingdee are displayed in section 5.6 "Software Info".
- Homegrown databases like Dameng and KingbaseES are displayed in section 5.4 "Port Banner".

Viewing Host Reports

You can view a host report by using one of the following methods:

- On the **Host Information** tab page of a summary report, click an IP address in the **Host Risks by Level** list. For details about the summary report, see Summary Report.
- On the **Vulnerability Info** tab page of a summary report, click + before a vulnerability to show its details, and then click an affected host.
- On the **Configuration Information** tab page of a summary report, click a noncompliant host in the **NC Host** column.
- On the **Vulnerable Accounts** tab page of a summary report, click an IP address.

- On the **Comparative Analysis** tab page of a summary report, click an affected host in the **Vulnerabilities** area or an IP address in the **Vulnerable Accounts** area.

Verifying Vulnerabilities

RSAS supports verification of some vulnerabilities so that administrators can confirm and fix them. If the vulnerability verification has been performed, the icon ✓ next to the vulnerability indicates that the verification succeeded (pointing to the icon displays the success prompt); the icon ✕ next to the vulnerability indicates that the verification failed (point to the icon to view the cause of failure).

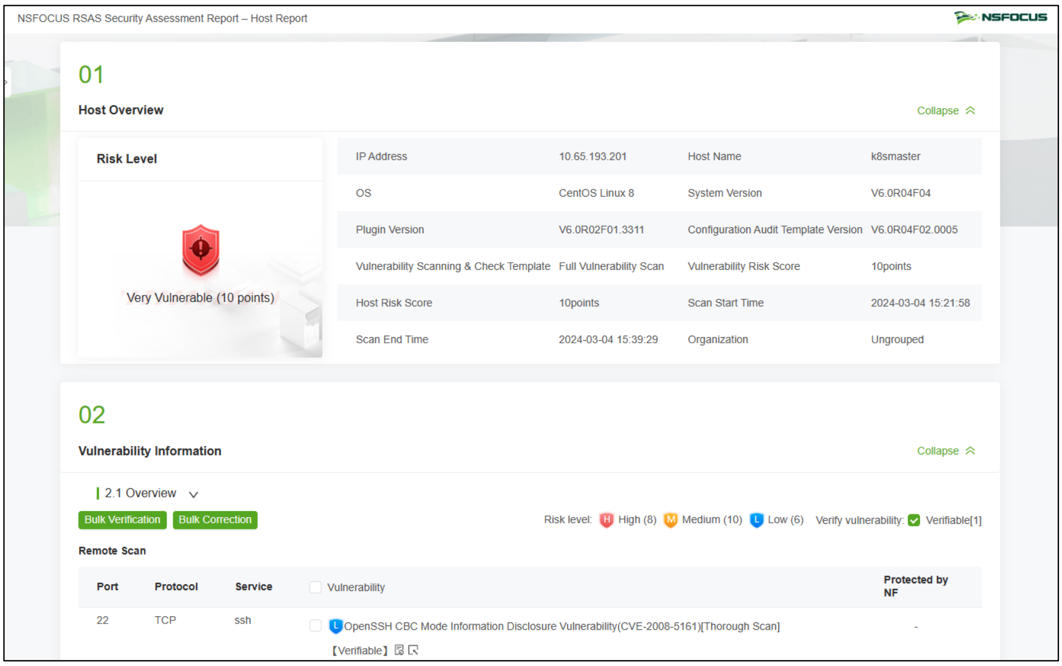
To manually verify a vulnerability, follow these steps:

Step 1 In a host report, choose **Vulnerability Information** > **Overview** to expand this section.

Step 2 Select **Verifiable** next to **Verify vulnerability**.

Then the list only displays vulnerabilities that can be verified, as shown in Figure 7-1.

Figure 7-1 Verifiable vulnerabilities



NSFOCUS RSAS Security Assessment Report – Host Report

01

Host Overview

Collapse

Risk Level

Very Vulnerable (10 points)

IP Address	10.65.193.201	Host Name	k8smaster
OS	CentOS Linux 8	System Version	V6.0R04F04
Plugin Version	V6.0R02F01.3311	Configuration Audit Template Version	V6.0R04F02.0005
Vulnerability Scanning & Check Template	Full Vulnerability Scan	Vulnerability Risk Score	10points
Host Risk Score	10points	Scan Start Time	2024-03-04 15:21:58
Scan End Time	2024-03-04 15:39:29	Organization	Ungrouped

02

Vulnerability Information

Collapse

2.1 Overview

Bulk Verification Bulk Correction

Risk level: H High (8) M Medium (10) L Low (6) Verify vulnerability: ☑ Verifiable[1]

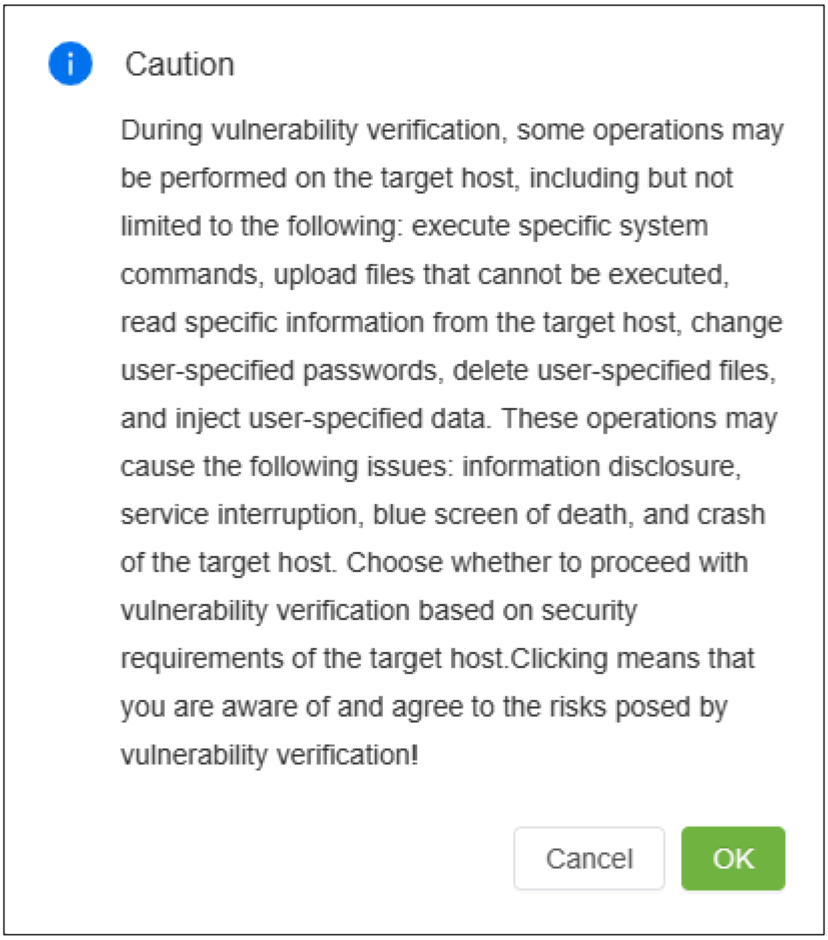
Remote Scan

Port	Protocol	Service	□ Vulnerability	Protected by NF
22	TCP	ssh	□ L OpenSSH CBC Mode Information Disclosure Vulnerability(CVE-2008-5161)[Thorough Scan] 【Verifiable】	-

Step 3 Configure parameters for RSAS to perform vulnerability verification and check whether vulnerabilities exist.

- Bulk verification: In the vulnerability list, select multiple vulnerabilities to be verified and click **Bulk Verification**. A warning pop-up appears, as shown in Figure 7-2. Click **OK** to confirm the operation. RSAS verifies the selected vulnerabilities against the default verification parameters.

Figure 7-2 Bulk verification warning

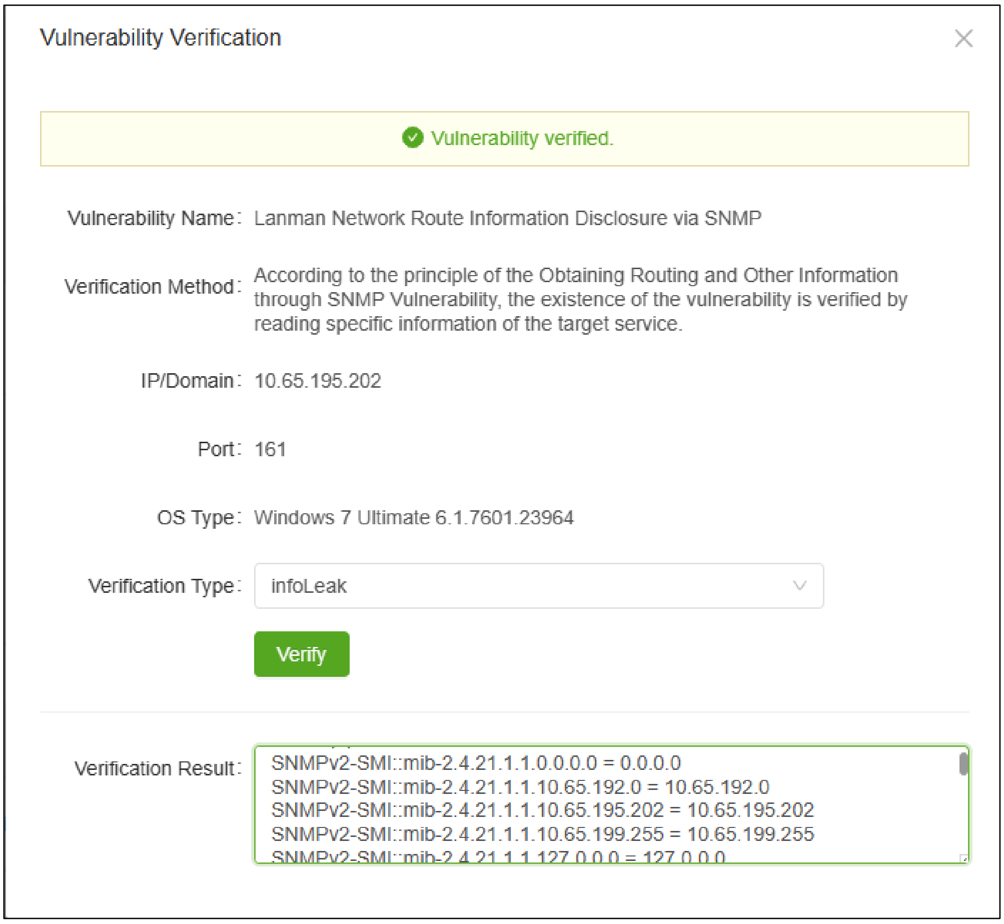


Caution

During vulnerability verification, some operations may be performed on the target host, including but not limited to the following: execute specific system commands, upload files that cannot be executed, read specific information from the target host, change user-specified passwords, delete user-specified files, and inject user-specified data. These operations may cause the following issues: information disclosure, service interruption, blue screen of death, and crash of the target host. Choose whether to proceed with vulnerability verification based on security requirements of the target host.Clicking means that you are aware of and agree to the risks posed by vulnerability verification!

- Individual verification: In the vulnerability list, click ⇱ to the right of a vulnerability. On the vulnerability verification dialog box, configure verification parameters and click **Verify**. A warning pop-up appears. Click **OK** to confirm the operation. Figure 7-3 indicates that the verification is complete.

Figure 7-3 Vulnerability verification



Vulnerability Verification

✓ Vulnerability verified.

Vulnerability Name：Lanman Network Route Information Disclosure via SNMP

Verification Method：According to the principle of the Obtaining Routing and Other Information through SNMP Vulnerability, the existence of the vulnerability is verified by reading specific information of the target service.

IP/Domain：10.65.195.202

Port：161

OS Type：Windows 7 Ultimate 6.1.7601.23964

Verification Type：infoLeak

Verify

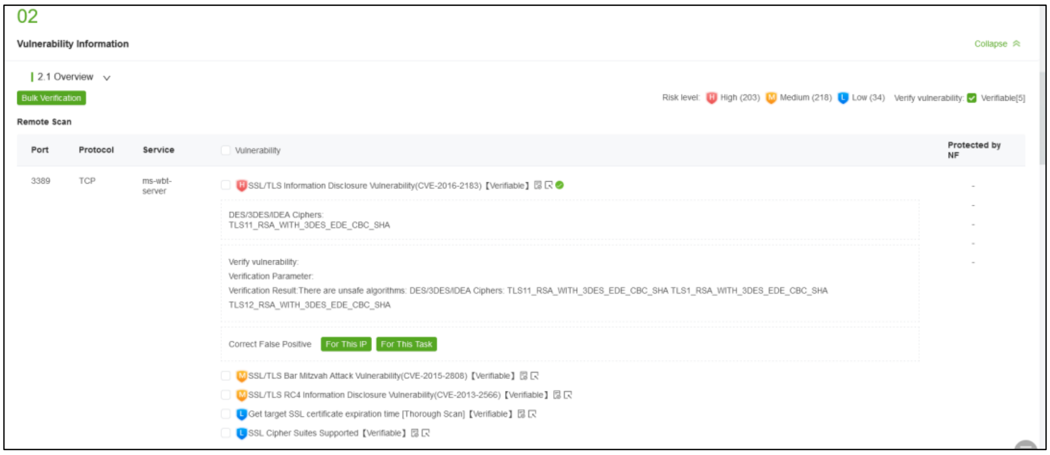
Verification Result：

```
SNMPv2-SMI::mib-2.4.21.1.1.0.0.0.0 = 0.0.0.0
SNMPv2-SMI::mib-2.4.21.1.1.10.65.192.0 = 10.65.192.0
SNMPv2-SMI::mib-2.4.21.1.1.10.65.195.202 = 10.65.195.202
SNMPv2-SMI::mib-2.4.21.1.1.10.65.199.255 = 10.65.199.255
SNMPv2-SMI::mib-2.4.21.1.1.127.0.0.0 = 127.0.0.0
```

Step 4 View the verification result

- For a succeeded verification, the icon ✓ is displayed to the right of the vulnerability. For a failed verification, the icon ✕ is displayed to the right of the vulnerability. Pointing to the icon displays the success prompt or cause of failure.
- Click the icon 📋 to view the specific vulnerability verification result, as shown in Figure 7-4.

Figure 7-4 Verification result



02

Vulnerability Information

Risk level: H High (203) M Medium (218) L Low (34) Verify vulnerability: ☑ Verifiable[5]

Remote Scan

Port	Protocol	Service	□ Vulnerability	Protected by NF
3389	TCP	ms-wbt-server	□ H SSL/TLS Information Disclosure Vulnerability(CVE-2016-2183) 【Verifiable】 DES/3DES/IDEA Ciphers: TLS11_RSA_WITH_3DES_EDE_CBC_SHA Verify vulnerability: Verification Parameter: Verification Result:There are unsafe algorithms: DES/3DES/IDEA Ciphers: TLS11_RSA_WITH_3DES_EDE_CBC_SHA TLS1_RSA_WITH_3DES_EDE_CBC_SHA TLS12_RSA_WITH_3DES_EDE_CBC_SHA Correct False Positive For This IP For This Task	-
			□ M SSL/TLS Bar Mitzvah Attack Vulnerability(CVE-2015-2808) 【Verifiable】	-
			□ M SSL/TLS RC4 Information Disclosure Vulnerability(CVE-2013-2566) 【Verifiable】	-
			□ L Get target SSL certificate expiration time [Thorough Scan] 【Verifiable】	-
			□ L SSL Cipher Suites Supported 【Verifiable】	-

----End

Fixing False Positives – Vulnerability

The scan result may contain false positives or you may want to ignore certain vulnerabilities. In this case, you can perform false positive correction. A vulnerability subject to false positive correction will be removed from the vulnerability list. However, after the related scanning task is executed again, this vulnerability reappears in the vulnerability list. To make it disappear, you need to perform the correction operation again.

In a host report, choose **Vulnerability Information** > **Overview** to display related information. Click ▤ to the right of a vulnerability. The return value and executable correction operation will be displayed.

- Select **For This IP**, indicating that this false positive found in the task will be fixed for this IP address.
- Select **For This Task**, indicating that this false positive found in the task will be fixed for all involved IP addresses**.**

Fixing False Positives – Configuration Item

The scan result may contain false positives or you may want to ignore certain noncompliant items. In this case, you can perform false positive correction. Noncompliant configuration items that are corrected will disappear from the list. However, after the related scanning task is executed, this configuration item reappears on the list. To make it disappear, you need to correct it again.

In a host report, click **Configuration Compliance** to display related information. Click **Correct this noncompliant item** to correct this noncompliant item found with the host.

7.3.3 Password Guess Task Report

A password guess task report can be a summary report or a host report, presenting details about the scan result.

A summary report is presented on two tabs: **Task Parameters** and **Vulnerable Accounts**. What is displayed on these two tabs is the same as that of an assessment task. For details, see corresponding descriptions in Summary Report.

For details about host reports, see Host Report.

7.3.4 Web Application Scanning Task Report

A web application scanning task report can be a summary report or a website report, presenting details about the result of a web application scanning task.

7.3.4.1 Summary Report

A summary report, as a panoramic display of the scan result, presents the security status of the scanned websites.

Table 7-4 Summary report for websites

Tab	Item	Description
Task Parameters	Basic Information	Displays parameters of a web application scanning task.
	Advanced Options/Buttons	Presents operations allowed for the task. For details, see Table 5-3.
Summary	Task Information	Displays detailed task information.
	Risk Distribution	Displays the distribution of risks, including the distribution of website risks by level (displayed only when two or more websites are scanned), distribution of web page risks by level, and distribution of vulnerabilities by risk level.
	Risk Type	Presents the number of vulnerabilities by risk level (high, medium, and low) and by category, and the overall statistics of vulnerabilities.
	Top 10 Vulnerable Web Pages	Displays the top 10 vulnerable web pages and the number of high-risk vulnerabilities.
Websites	Website Risks by Level	Lists vulnerability information of websites detected in the current task by default, including all websites scanned, number of scanned links for each website, scan duration, number of vulnerabilities by risk level (high, medium, and low), and risk score. • If a large number of websites are involved, you can filter them by specifying the risk level (very vulnerable, vulnerable, safe, and/or very safe). • Clicking a website name displays its scanning report. For details, see Website Report.
Vulnerabilities	Vulnerability Distribution	Lists vulnerabilities of all levels detected in the current task by default, including the vulnerability name, number of affected pages, and occurrence frequency. • If a large number of vulnerabilities are involved, you can filter vulnerabilities by specifying the risk level (high, medium, and/or low).

Tab	Item	Description
		• The **Vulnerability verification** area displays the number of verified vulnerabilities and verifiable vulnerabilities. • Clicking + before a vulnerability displays details about this vulnerability. What parameters such details contain varies with the specific vulnerability. In vulnerability details, clicking an affected website displays its scanning report. For details, see Website Report. • A vulnerability found by thorough scan is identified by **Thorough Scan** in its name. • A vulnerability that can be verified is identified by **Verifiable** in its name. Clicking + before a vulnerability name displays the verification method about this vulnerability.
Reference Criteria	-	Presents reference standards for assessing web application risks.
Comparative Analysis	-	The **Comparative Analysis** tab page, which is displayed only for a parent task, provides information about the child tasks with the largest ID among all complete child tasks. By default, comparative data of the last two child tasks is displayed about task information and vulnerability information. • You can select child tasks from the drop-down list of the parent task to compare their scanning data. • Clicking + before a vulnerability in the **Vulnerabilities** area displays details about this vulnerability. What parameters such details contain varies with the specific vulnerability. • Clicking an affected website in this area displays its scanning report. For details, see Website Report.

7.3.4.2 Website Report

You can view the detailed risk report of a website, that is, website report, which covers the website overview, risk statistics by level and category, web risk distribution, and website tree.

Viewing a Website Report

You can view a single-website report by using either of the following methods:

- On the **Websites** tab page of a summary report, click a website name in the list of website risks by level. For details about a summary report, see Summary Report.
- On the **Vulnerabilities** tab page of a summary report, click + before a vulnerability to show its details, and then click an affected website.

Verifying Vulnerabilities

RSAS supports verification of some vulnerabilities so that administrators can confirm and fix them. If the vulnerability verification has been performed, the icon ✓ next to the vulnerability indicates that the verification succeeded (pointing to the icon displays the success prompt); the icon ✖ next to the vulnerability indicates that the verification failed (point to the icon to view the cause of failure).

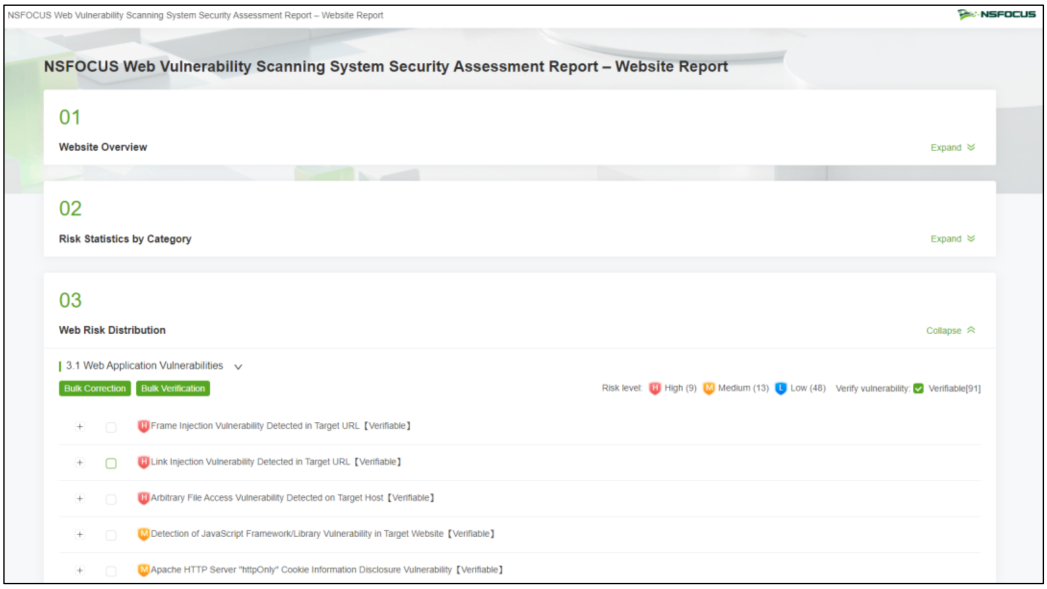
To manually verify a web vulnerability, follow these steps:

Step 1 In a single-website report, choose **Web Risk Distribution** > **Web Application Vulnerabilities** to show all vulnerabilities detected.

Step 2 Select **Verifiable** next to **Verify vulnerability**.

Then the list only displays vulnerabilities that can be verified, as shown in Figure 7-5.

Figure 7-5 Verifiable vulnerabilities



NSFOCUS Web Vulnerability Scanning System Security Assessment Report – Website Report

NSFOCUS Web Vulnerability Scanning System Security Assessment Report – Website Report

01

Website Overview

Expand

02

Risk Statistics by Category

Expand

03

Web Risk Distribution

Collapse

3.1 Web Application Vulnerabilities

Bulk Correction Bulk Verification

Risk level: H High (9) M Medium (13) L Low (48) Verify vulnerability: ☑ Verifiable[91]

+ □ H Frame Injection Vulnerability Detected in Target URL 【Verifiable】

+ □ H Link Injection Vulnerability Detected in Target URL 【Verifiable】

+ □ H Arbitrary File Access Vulnerability Detected on Target Host 【Verifiable】

+ □ M Detection of JavaScript Framework/Library Vulnerability in Target Website 【Verifiable】

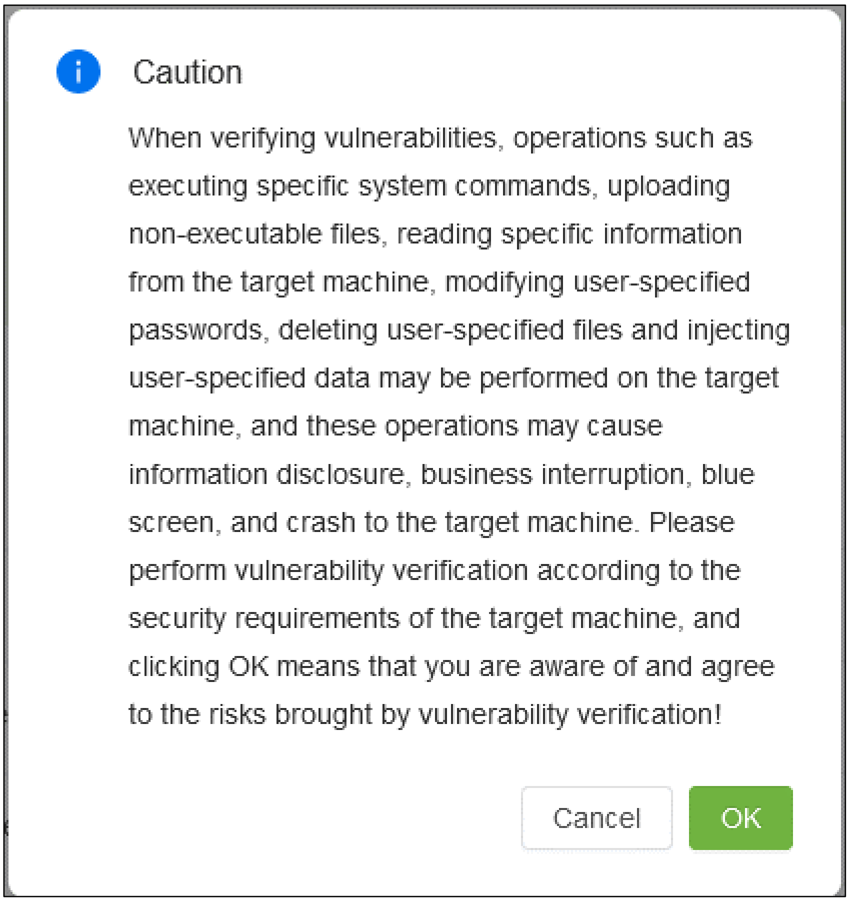
+ □ M Apache HTTP Server "httpOnly" Cookie Information Disclosure Vulnerability 【Verifiable】

Step 3 In the web vulnerability list, click + to show the related URLs of the verifiable vulnerability.

Step 4 Configure parameters for RSAS to perform vulnerability verification and detect whether vulnerabilities exist.

- Bulk verification: Select multiple vulnerabilities to be verified and click **Bulk Verification**. A warning pop-up appears, as shown in Figure 7-6. Click **OK** to confirm the operation. RSAS verifies the selected vulnerabilities against the default verification parameters.

Figure 7-6 Bulk verification warning

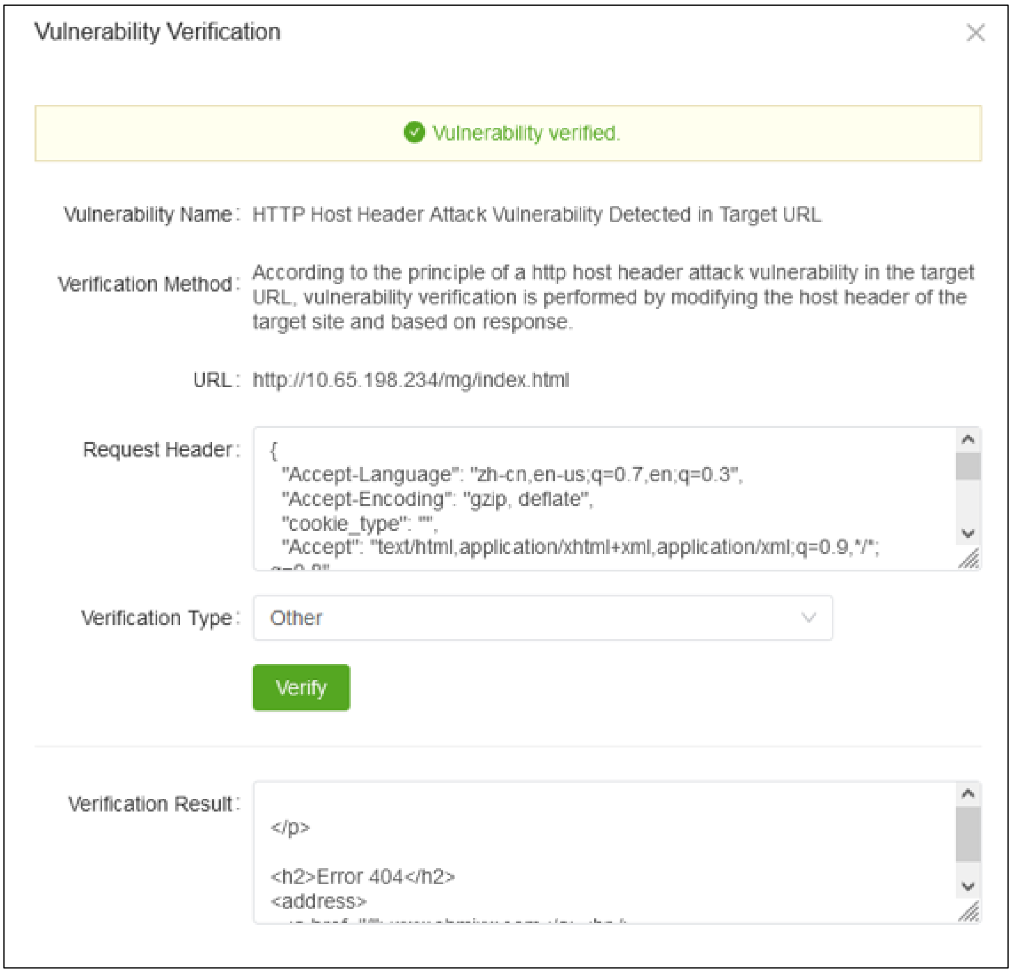


Caution

When verifying vulnerabilities, operations such as executing specific system commands, uploading non-executable files, reading specific information from the target machine, modifying user-specified passwords, deleting user-specified files and injecting user-specified data may be performed on the target machine, and these operations may cause information disclosure, business interruption, blue screen, and crash to the target machine. Please perform vulnerability verification according to the security requirements of the target machine, and clicking OK means that you are aware of and agree to the risks brought by vulnerability verification!

- Individual verification: Click ↖ next to the URL of the verifiable vulnerability. On the vulnerability verification dialog box, configure verification parameters and click **Verify**. A warning pop-up appears. Click **OK** to confirm the operation. Figure 7-7 indicates that the verification is complete.

Figure 7-7 Vulnerability verification



Vulnerability Verification

✓ Vulnerability verified.

Vulnerability Name: HTTP Host Header Attack Vulnerability Detected in Target URL

Verification Method: According to the principle of a http host header attack vulnerability in the target URL, vulnerability verification is performed by modifying the host header of the target site and based on response.

URL: http://10.65.198.234/mg/index.html

Request Header:

```
{
  "Accept-Language": "zh-cn,en-us;q=0.7,en;q=0.3",
  "Accept-Encoding": "gzip, deflate",
  "cookie_type": "",
  "Accept": "text/html,application/xhtml+xml,application/xml;q=0.9,*/*;
q=0.8",
```

Verification Type: Other

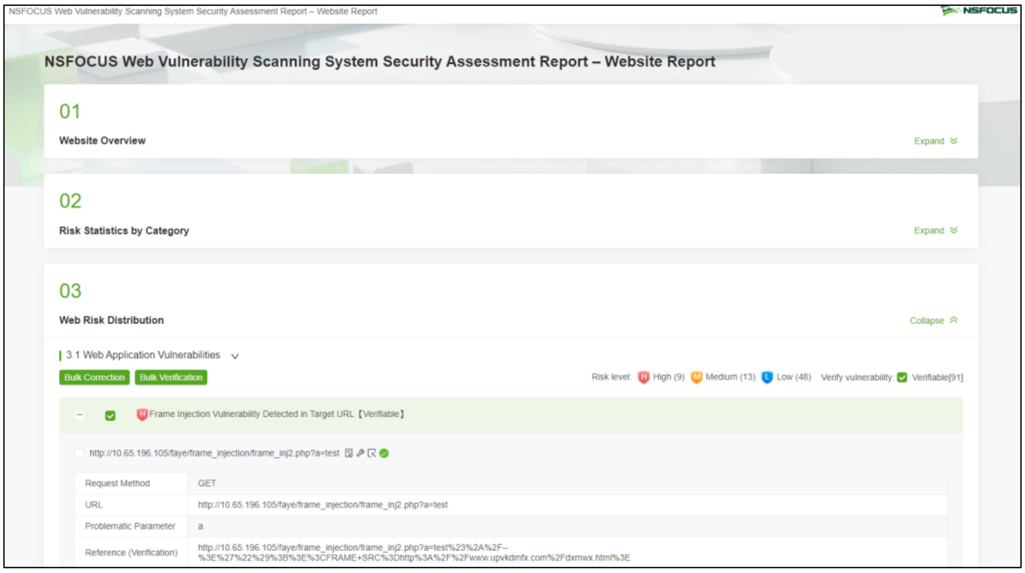
Verification Result:

```
</p>

<h2>Error 404</h2>
<address>
```

Step 5 View the verification result

- For a succeeded verification, the icon ✓ is displayed to the right of the URL. For a failed verification, the icon ✕ is displayed to the right of the URL. Pointing to the icon displays the success prompt or cause of failure.
- In the vulnerability list, view the specific vulnerability verification result, as shown in Figure 7-8.

Figure 7-8 Verification result



NSFOCUS Web Vulnerability Scanning System Security Assessment Report – Website Report

NSFOCUS Web Vulnerability Scanning System Security Assessment Report – Website Report

01 Website Overview — Expand

02 Risk Statistics by Category — Expand

03 Web Risk Distribution — Collapse

3.1 Web Application Vulnerabilities

Bulk Correction | Bulk Verification

Risk level: H High (9) M Medium (13) L Low (48) Verify vulnerability: ☑ Verifiable[91]

– ☑ H Frame Injection Vulnerability Detected in Target URL【Verifiable】

□ http://10.65.196.105/faye/frame_injection/frame_inj2.php?a=test

Request Method	GET
URL	http://10.65.196.105/faye/frame_injection/frame_inj2.php?a=test
Problematic Parameter	a
Reference (Verification)	http://10.65.196.105/faye/frame_injection/frame_inj2.php?a=test%23%2A%2F-- %3E%27%22%29%3B%3E%3CFRAME+SRC%3Dhttp%3A%2F%2Fwww.upvkdmfx.com%2Fdxmwx.html%3E

----End

Fixing False Positives

If you suspect that certain vulnerabilities are reported mistakenly, you can fix such false positives. Vulnerabilities addressed this way will disappear from the vulnerability list. However, after the related scanning task is executed again, this vulnerability reappears in the vulnerability list. To make it disappear, you need to perform the correction operation again.

In a single-website report, choose **Web Risk Distribution** > **Web Application Vulnerabilities** to show all vulnerabilities. Click + before a vulnerability to show its details and fix the false positive as follows:

- Click 🔧 to fix the false positive regarding this URL.
- Select all URLs whose vulnerabilities are false positives and click **Bulk Correction** to fix false positives in batches.

7.3.5 Configuration Scanning Task Report

A configuration scanning task report consists of a summary report and a host report, presenting details about the scan result.

The summary report content of a configuration scanning task is similar to that of an assessment task, consisting of all tab pages of the latter except for **Vulnerability Info**.

- For how to view the summary report of a configuration scanning task, see Summary Report.
- For details about the host report of a configuration scanning task, see Host Report.

7.3.6 Image Scanning Task Report

An image scanning task report consists of a summary report and an image report, presenting details about the scan result of vulnerability scanning and configuration check.

7.3.6.1 Summary Report

A summary report, as a panoramic display of the scan result, presents the overall security status of the scanned image file. Reports of different image scanning tasks may contain different types of information. The following takes scanning data of an integrated task (covering vulnerability scanning and configuration check) as an example to present you details of a task report.

Table 7-5 shows detailed report information for an image scanning task.

Table 7-5 Summary report for an image scanning task

Tab	Item	Description
Task Parameters	Basic Information	Displays parameters of an image scanning task.
	Icon/Button	Presents operations allowed for the task. For details, see Table 5-3.
Summary	Task Information	Presents the network risk information (risk score and risk level), task name, task type, time statistics, vulnerability scan template, configuration check template list, image statistics, and system version information.
	Risk Distribution	Presents the distribution of image vulnerabilities by risk level, distribution of overall image risks by level, distribution of image configurations by risk level, distribution of vulnerabilities by risk level, and distribution of noncompliant items by risk level.
	Vulnerability Risks	Presents the number of high-, medium, and low-risk vulnerabilities by category, and the overall statistics of vulnerabilities. Clicking the value in the table displays details about the corresponding vulnerabilities. Clicking the **All** tab, you can view statistics of all vulnerabilities displayed by category on the same page.
	Configuration Risks	Presents the distribution of noncompliant items in the virtual device category.
	Asset Overview	Presents the number and proportion of operating systems running on assets.
Image Information	Image Risk by Level	By default, provides risk information of all scanned images, including the image name, operating system, quantity of high, medium, and low risks, and risk score. • If a large number of images are involved, you can filter them by specifying the risk level (very vulnerable, vulnerable, safe, and/or very safe). • Clicking + before an image name displays the scanning template used. • Clicking an image name displays its scanning report. For details, see Image Report.
Vulnerability Info	Vulnerability Distribution	Lists vulnerabilities of all types detected in the current task by default, including the vulnerability name and occurrence frequency. • If a large number of vulnerabilities are involved, you can filter vulnerabilities by specifying the risk level (high, medium, and/or low). • Clicking + before a vulnerability displays details about this vulnerability. What parameters such details contain varies with the

Tab	Item	Description
		specific vulnerability. In vulnerability details, clicking an affected image displays its scanning report. For details, see Image Report.
Configuration Information	-	Lists noncompliant configuration items of all risk levels for the current task by default. Clicking a noncompliant image displays the corresponding image report. For details, see Image Report.
Reference Criteria	-	Presents reference standards for assessing system risks, including the following: • risk level metrics for a single vulnerability • a single configuration item • an image • a network • security recommendations
Comparative Analysis	-	The **Comparative Analysis** tab page, which is displayed only for a parent task, provides information about the child tasks with the largest ID among all complete child tasks. By default, comparative data of the last two child tasks is displayed. • You can select child tasks from the drop-down list of the parent task to compare their scanning data. • Clicking + before a vulnerability in the **Vulnerabilities** area displays details about this vulnerability. What parameters such details contain varies with the specific vulnerability. • In vulnerability details, clicking an affected image displays its scanning report. For details, see Image Report.

7.3.6.2 Image Report

You can view the detailed risk report of an image (that is, image report), obtaining information about the image, vulnerabilities, noncompliant configuration items, and status compliance.

Viewing a Single-Image Report

You can view an image report by using one of the following methods:

- On the **Image Information** tab page of a summary report, click an image in the **Image Risk by Level** list. For details about the summary report, see Summary Report.
- On the **Vulnerability Info** tab page of a summary report, click + before a vulnerability to show its details, and then click an affected image.
- On the **Configuration Information** tab page of a summary report, click a noncompliant image in the **Noncompliant Images** column.
- On the **Comparative Analysis** tab page of a summary report, click an affected image in the **Vulnerabilities** area.

Fixing False Positives – Vulnerability

The scan result may contain false positives or you may want to ignore certain vulnerabilities. In this case, you can correct false positives. A vulnerability subject to false positive correction will be removed from the vulnerability list. However, after the related scanning task is executed again, this vulnerability reappears in the vulnerability list. To make it disappear, you need to perform the correction operation again.

In an image report, choose **Vulnerability Information > Vulnerability Overview** to display related information. Click to the right of a vulnerability. The return value and executable correction operation will be displayed.

- Select **For This Image**, indicating that this false positive found in the task will be fixed for this image.
- Select **For Task**, indicating that this false positive found in the task will be fixed for all involved images.

Fixing False Positives – Configuration Item

The scan result may contain false positives or you may want to ignore certain noncompliant items. In this case, you can correct false positives. Noncompliant configuration items that are ignored will disappear from the list. However, after the related scanning task is executed, this configuration item reappears on the list. To make it disappear, you need to ignore it again.

In a host report, click **Configuration Compliance** to display related information. Click **Correct this noncompliant item** to correct this noncompliant item found with the image.

7.3.7 Code Audit Task Report

A code audit task only generates a summary report. Table 7-6 shows the information of a summary report for a code audit task.

Table 7-6 Summary report for code audit tasks

Tab	Item	Description
Task Parameters	Basic Information	Displays parameters of a code audit task.
	Icon/Button	Presents operations allowed for the task. For details, see Table 5-3.
Summary	Task Information	Presents the risk information (risk score and risk level), task name, scan template, system version information, rule base version, time statistics, and file statistics.
	Risk Distribution	Presents the distribution of file risks by level and distribution of defects by risk level.
	Defect Risks	Presents the number of high-, medium, and low-risk defects by category and the overall statistics of defects.
File List	File Risk by Level	Lists code files of all risk levels scanned in the current task by default. If a large number of code files are involved, you can filter them by specifying the risk level (very vulnerable, vulnerable, safe, and/or very safe).
Defect List	Defect Distribution	Lists security defects of all risk levels that are found in the current task by default.

Tab	Item	Description
		• If a large number of security defects are involved, you can filter them by specifying the risk level (high-risk, medium-risk, and/or low-risk). • Click + before a security defect to view its details. • Click **View details** in the **Code Details** column of a security defect to view the specific code that has a security defect. • If certain security defects are false positives, you can ignore these defects found in the current task. A security defect, after being ignored, will be removed from the defect list. However, after the related scanning task is executed again, this security defect reappears in the defect list. After a security defect is ignored, the risk level will be recalculated on the **Summary** tab of the current task.
Reference Criteria	-	Presents reference standards for measuring the risk level, including metrics for measuring the risk level of a single security defect, metrics for measuring file risks, and security suggestions.

7.3.8 Host Asset Detection Task Report

A host asset detection task report can be a summary report or host asset report.

7.3.8.1 Summary Report

Table 7-7 shows information of a summary report for a host asset detection task.

Table 7-7 Summary report for a host asset detection task

Tab	Item	Description
Task Parameters	Basic Information	Presents parameters of a host asset detection task, and operations allowed for the task. For details, see Table 5-3.
Summary	Task Information	Presents the execution status and basic information of the host asset detection task.
	Asset Statistics	Presents the total number of IPv4/IPv6 host assets, number of web assets (after **Associated Web Asset Detection** is enabled in the task creation. See Host Asset Detection Task), number of associated domains, and number of open ports.
	Operating System Distribution	Presents the distribution of operating systems detected in the task in a pie chart, including its name, assets involved, and proportion.
	Device Type Distribution	Presents the distribution of device types detected in the task in a pie chart, including its name, assets involved, and proportion.
	Top 10 Ports	Presents the top 10 ports opened on the most assets and the number of assets involved.
	Top 10 Services	Presents the top 10 services opened on the most assets and the number of assets involved.
Host	Statistical Data	Displays the total number of host assets detected and their

Tab	Item	Description
Asset Discovery		associated web assets.
	List	Lists the information of each host asset detected and its associated web assets. Clicking an IP address displays the corresponding host asset report. For details, see Host Asset Report.

7.3.8.2 Host Asset Report

A host asset report displays the information of detected host assets, open ports, and service applications, as described in Table 7-8.

Table 7-8 Report of a single host asset

Item	Description
Basic Information	Displays the IP address, operating system, associated web assets, task execution time, and other information of the live host detected.
Port Information	Displays the open ports and banner on the host asset.
Application Information	Displays the enabled services and CPEs on the host asset. If **Associated Web Asset Detection** is configured in a Host Asset Detection Task, this part also displays the information of the associated web assets.

7.3.9 Web Asset Detection Task Report

A web asset detection task report can be a summary report or web asset report.

7.3.9.1 Summary Report

Table 7-9 shows information of a summary report for a web asset detection task.

Table 7-9 Summary report for a web asset detection task

Tab	Item	Description
Task Parameters	Basic Information	Presents parameters of a web detection task and operations allowed for the task. For details, see Table 5-3.
Summary	Task Information	Presents the execution status and basic information of the web detection task.
	Asset Statistics	Displays the total number of detected domain names, number of web assets, and number of associated host assets.
	Web Service Distribution	Presents the distribution of web services detected in the task in a pie chart, including its name, assets involved, and proportion.
	Web Framework Distribution	Presents the distribution of web frameworks detected in the task in a pie chart, including its name, assets involved, and proportion.

Tab	Item	Description
	Programming Language Distribution	Presents the distribution of programing languages detected and assets involved in the task in a histogram.
Web Asset Discovery	Statistical Data	Displays the total number of web assets detected.
	List	Lists the information of each web asset detected. Clicking an URL address displays the corresponding web asset report. For details, see Web Asset Report.

7.3.9.2 Web Asset Report

A web asset report displays the information of detected web assets and associated host assets, as described in Table 7-10.

Table 7-10 Report of a single web asset

Item	Description
Basic Information	Displays the domain name, web server, web framework, programing language and other information of the live web asset (website and device) detected.
Associated Host Asset Information	• Overview: displays the IP addresses of the associated host assets and the total number of open ports on assets. • Port: displays the open ports and banner on the host assets. • Application: displays the enabled services and CPEs on the host assets.

7.4 Asset Report

The default system administrator (**admin**) and system administrators with the report management permission can view reports of all assets. Common administrators with the report management permission can view only reports of target assets covered by their own tasks. An asset report can be generated only after a task is complete.

An asset report can be a node report or a device report, presenting the scan result of a vulnerability scanning task, configuration scanning task, weak password guess task, or web application scanning task.

7.4.1 Node Report

Choose **Asset > Asset List**. Select a node, point to ⋮, and click **Overview**. Then the node report appears. A node report, as a panoramic display of the scan result, presents the overall security status of all assets under the node from various aspects.

Table 7-11 Node report

Tab	Item	Description
Summary	Risk Level	Displays the asset level and risk score.
	Risk Distribution	Displays the overall host risk distribution by level, distribution of

Tab	Item	Description
		host vulnerability risks by level, and distribution of host configuration risks by level
	Vulnerability Risks	Displays vulnerabilities detected in all assets under the node. Content in this part is similar to that of an assessment task report. For details, see the vulnerabilities risk by level on the **Summary** tab of a Summary Report.
Child Nodes	Child Nodes by Risk Level	Displays the risk of all child nodes of the current node.
	Risk Distribution	Displays the number and percentage of nodes with different risk levels in a pie chart.
Attributes	Node Attribute	Displays basic information of the current node.
Others	Host Information, System Vulnerabilities, Configuration Information, and Vulnerable Accounts	Displays risks, vulnerabilities, and noncompliant configuration items at various levels, and vulnerable accounts of all assets under the node. Content on these tab pages is similar to that of an assessment task report. For details, see Summary Report.
	Web Vulnerabilities	Displays high-risk, medium-risk, and low-risk vulnerabilities in web applications on assets of all websites under the current node. Content on this tab page is similar to that of a web application scanning task report. For details, see Summary Report.
Generate Report > HTML	-	Generates an offline report, which will be displayed on the Report List page.

7.4.2 Asset Report

An asset report is based on the IP or URL address, providing overall statistics of the asset covered by assessment tasks, password guess tasks, web application scanning tasks, host asset detection tasks, and web asset detection tasks.

Choose **Asset > Asset List**. Select a node in the left pane and click an asset name in the asset list that is displayed on the right pane of the page to view the asset report.

Table 7-12 Asset report

Tab	Description
Device Information	Displays the operating system, port, service and application, installed software, MAC address, host name, and other information detected on the asset.
Risks	Displays the host overview, system vulnerabilities (including system vulnerabilities and web application vulnerabilities), noncompliant configuration items, status compliance information, detailed website information, and other information such as ports and operating system types. Such data is sourced from the related host report and single-website report. For details, see sections Host Report and Website Report.
Risk Comparison	You can compare scanning data of an asset obtained at different times to know the security status changes of the asset. Specify a time frame for risk comparison and click **Compare**. Then comparison data is displayed below in four sections: **Overview**, **Vulnerabilities**, **Noncompliant**

Tab	Description
	Configurations, and **Scanned URLs**.
Historical Tasks	By default, data of the last scanning task is displayed. You can specify the host scanning time to view task information of the asset at the specified time. Note that what is displayed varies with the task type.
Attributes	Displays basic information of the current asset.
Associated Information	Displays the detected web assets (if **Associated Web Asset Detection** is configured in a host asset detection task) or host assets (if **Associated Host Asset Detection** is configured in a web asset detection task).
Generate Report > HTML	Generates an offline report, which will be displayed on the Report List page.

8 Knowledge Base Management

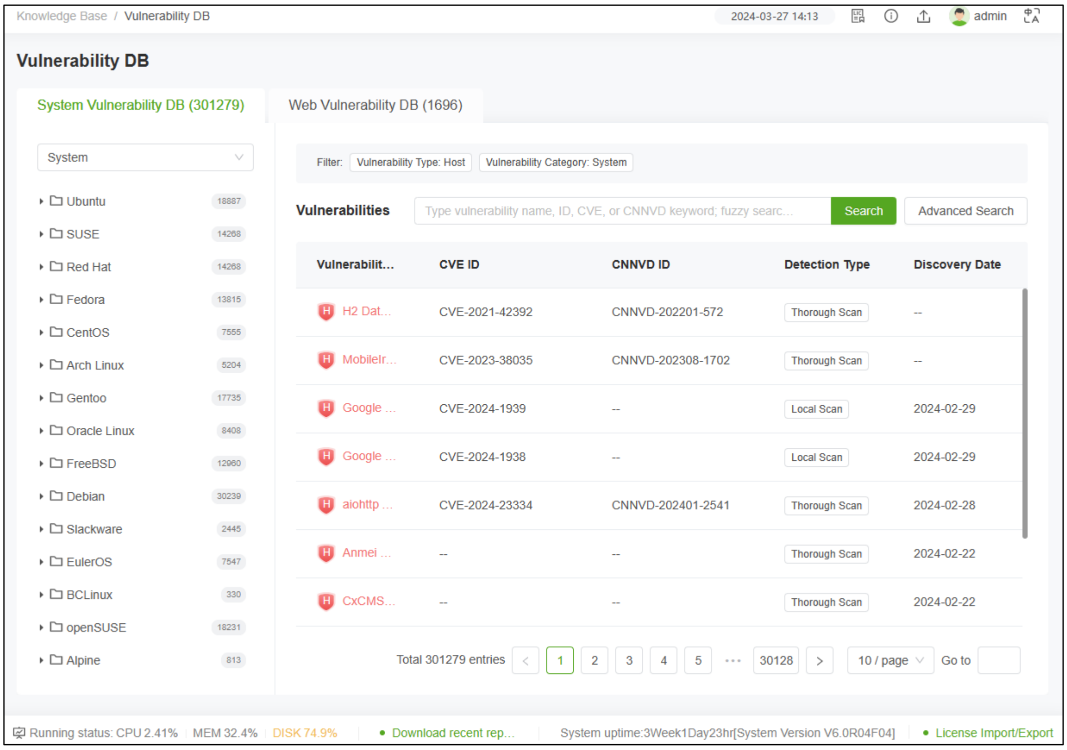
This chapter contains the following sections:

Section	Description
Vulnerability Database	Describes the database of vulnerabilities available on RSAS.
Template Management	Describes how to create a vulnerability template and related information.
Password Dictionary	Describes how to create a password dictionary.
Offline Check Tool	Describes how to use offline check tools.
Hardening Knowledge Base	Describes the hardening knowledge base provided by RSAS.
Offline Hardening Tool	Describes how to use offline hardening tools.
Port List	Describes ports involved in the port scanning and operations allowed for ports.

8.1 Vulnerability Database

Choose **Knowledge Base > Vulnerability DB** to view all currently available vulnerabilities and their attributes. In addition, you can search for a vulnerability by host, website, or keyword, as shown in Figure 8-1.

Figure 8-1 Vulnerability Database page



Knowledge Base / Vulnerability DB

2024-03-27 14:13 admin

Vulnerability DB

System Vulnerability DB (301279) Web Vulnerability DB (1696)

System

Ubuntu	18887
SUSE	14268
Red Hat	14268
Fedora	13815
CentOS	7555
Arch Linux	5204
Gentoo	17735
Oracle Linux	8408
FreeBSD	12960
Debian	30239
Slackware	2445
EulerOS	7547
BCLinux	330
openSUSE	18231
Alpine	813

Filter: Vulnerability Type: Host Vulnerability Category: System

Vulnerabilities

Type vulnerability name, ID, CVE, or CNNVD keyword; fuzzy searc... Search Advanced Search

Vulnerabilit...	CVE ID	CNNVD ID	Detection Type	Discovery Date
H2 Dat...	CVE-2021-42392	CNNVD-202201-572	Thorough Scan	--
MobileIr...	CVE-2023-38035	CNNVD-202308-1702	Thorough Scan	--
Google ...	CVE-2024-1939	--	Local Scan	2024-02-29
Google ...	CVE-2024-1938	--	Local Scan	2024-02-29
aiohttp ...	CVE-2024-23334	CNNVD-202401-2541	Thorough Scan	2024-02-28
Anmei ...	--	--	Thorough Scan	2024-02-22
CxCMS...	--	--	Thorough Scan	2024-02-22

Total 301279 entries < 1 2 3 4 5 ••• 30128 > 10 / page Go to

Running status: CPU 2.41% MEM 32.4% DISK 74.9% Download recent rep... System uptime:3Week1Day23hr[System Version V6.0R04F04] License Import/Export

8.2 Template Management

The Templates module allows you to manage various scanning templates in the RSAS system. When creating a task, you can specify a vulnerability template to let RSAS scan for related vulnerabilities.

8.2.1 Vulnerability Template

A vulnerability template is a collection of scanning plugins, based on which vulnerability scanning is implemented. RSAS provides almost all types of vulnerability scanning plugins. You can specify vulnerability plugins as required for vulnerability scanning. This can accelerate scanning and improve the accuracy and coverage of scan results.

Choose **Knowledge Base > Templates > Vulnerability Template**. Click **Create Vulnerability Template** and configure parameters in the drawer that appears from the right side. Table 8-1 and Table 8-2 describe parameters for configuring a vulnerability template.

A vulnerability template, after being created, can be queried, viewed, edited, deleted, exported, and imported. It can also be saved as another template.

Table 8-1 Basic parameters

Parameter	Description
Template Name	Name of the new template. It is a string of 1 to 50 characters consisting of letters (case-sensitive), digits, hyphens (-), and/or underscores (_). Templates can have the same name if created by different users.
Template Description	Brief description of the new template.

Table 8-2 Parameters for specifying template types

Parameter	Description
Add Vulnerability	Add the required vulnerability plugins to the template. The plugins are displayed under the vulnerability list.
Common Template	For this option, you need to select plugins of certain types for scanning tasks. All plugins supported by RSAS are available for selection. You can specify vulnerability plugins by using either of the following methods: • Query vulnerabilities and then select vulnerability plugins. • Select a plugin type from the drop-down vulnerability list and then select plugins necessary for your scanning tasks.
	Clicking **Advanced Search** displays the following query conditions: **CVE ID/BUGTRAQ ID/CNCVE ID/CNVD ID/CNNVD ID/NSFOCUS ID/MS ID** (unavailable for a web scanning template): ID of a vulnerability in a well-known vulnerability database. • **Risk Level**: risk level of vulnerabilities to be scanned • **Vulnerability Name** (for a system scanning template): name of the system vulnerability • **Vulnerability Description** (for a web scanning template): specific information of the web application vulnerability • **Dangerous Plugin**: selecting **Yes** means the plugin can cause system crash or service interruption • **Vulnerability Verification**: selecting **Yes** means RSAS supports verification of the vulnerability • **Discovery Date**: a period during which the vulnerabilities are detected. • **Vulnerability Category**: category to which the vulnerability belongs, which can be the system, threat, CVE year (unavailable for a web scanning template), service, application, or time
Advanced Template	You can filter plugins for scanning tasks by the following conditions: • **Risk Level**: risk level of vulnerabilities to be scanned • **Organization**: organization from which the vulnerabilities are sourced • **Discovery Time**: year when the target vulnerabilities are detected • **System Type**: operating system type that the target vulnerabilities affect • **Application Type**: application type that the target vulnerabilities affect • **Threat Type**: category of the target vulnerabilities After configuring the preceding conditions, click > to add it to **Selected Conditions**. Then scanning will be implemented based on the appropriate vulnerability plugins meeting these conditions. After filtering rules are configured, you can click **Preview** to view the selected scanning plugins.

8.2.2 Configuration Template

Configuration templates are used for configuration checks, covering configuration check points and their weights. You can customize configuration check templates for various target systems as required or according to industry standards.

8.2.2.1 Creating a Template Group

On RSAS, you can group custom templates to facilitate template management. For example, you can put configuration templates for checking a certain type of devices in one group.

Choose **Knowledge Base > Templates > Configuration Template > Operating System/Database/Application/Network Device/Virtual Device/Big Data**, and click **Manage Groups**. In the **Manage Groups** drawer that appears, click **Create**. Specify the group name, description, and type (for the meaning of MLPS, see MLPS). A group, after being created, can be edited and deleted.

8.2.2.2 Creating a Configuration Template

Creating a Template

Choose **Knowledge Base > Templates > Configuration Template**. Click **Template Configuration > Create/Create MLPS/Create MLPS 2.0** and configure template parameters.

- **Basic Attributes**: provides basic parameters for a configuration template.

Table 8-3 Basic parameters

Function	Parameter	Description
Basic Information	Template Name	Specifies the name of a new template, which must be unique.
	Template Group	Specifies the group to which the new template belongs.
	Check Type	Specifies the operating system covered by the new template.
	System Type/Template Type	Specifies the object to be checked against the new template and the suitable template type.
Variable List	Add Variable	Adds a custom variable.
	Referenced Name	Specifies the name used when referenced in a command.
	Screen Name	Specifies the name displayed on the task creation page.
	Type	Specifies how the variable is displayed. It can be either of the following: • **Text type**: indicates that the variable will be displayed in plaintext and the value of this variable will be logged. • **Password type**: indicates that the variable will be displayed in ciphertext (as a string of "*") and the value of this variable will not be logged.
	Description	Brief description of the new variable.
Initialization Command	Text box	The initialization command is a command executed by the system after login to the target host during a scanning task. It is applicable to

Function	Parameter	Description
		the scenario in which initialization is required, for example, switching to a higher-privilege account.

- **Configuration Check Items**: checks whether the configuration of a target host is compliant with relevant requirements. The check result is contained in the scanning reports.
  - The system checks a target host against the check items one by one from the first to the last item.
  - Click **Create** to create a check item in the dialog box that appears. Table 8-4, Table 8-5, and Table 8-6 describe parameters for configuring a check item.
  - A configuration check item, after being created, can be edited and deleted.
  - You can change the sequence of check items in the list by clicking ↑ or ↓ to move an item up or down.

Table 8-4 Parameters for creating a check item

Parameter	Description
Index	Index of the new check item, which is in numerical order, starting from 1. You can also specify a new number.
Check Item	Name of the new check item.
Check Item Category (only for an ordinary template)	Category of the new check item.
Risk Score	Risk level of the new check item. A larger value indicates a higher risk.
Control Point Index (only for an MLPS or MLPS 2.0 template)	Index of the control point.
Control Point Category (only for an MLPS or MLPS 2.0 template)	Specifies the configuration check type to which the control point belongs.
MLPS Level (only for an MLPS or MLPS 2.0 template)	Specifies the multilevel protection level of the control point.
Control Point Description (only for an MLPS or MLPS 2.0 template)	Describes what is to be checked at this control point.

Table 8-5 Parameters for creating a check point

Parameter	Description
Add Check Point	Adds a check point. A check point, after being created, can be edited, deleted and added to AND/OR rule.
Description	Brief description of the new check point.
Configuration Method	Configuration method of the new check point.

Parameter		Description
Check Method		• For Windows, check methods include the executive command, port check, file content check, registry check, XML configuration file check, and URL check. • For UNIX, check methods include the executive command, port check, file content check, XML configuration file check, file permission check, process check, and URL check.
Match Rule		Matching rule of the new check point.
Executive Command	Executive Command	Specifies a command for the system to obtain configuration information of target hosts.
	Regular Expression	Specifies a regular expression for the new check point. The system matches results returned by the command specified above line by line according to the regular expression, so as to find desired information. • Use of parentheses: indicates that the system will read content that matches the subexpression in parentheses in an expression like "DEBUG=(\d)". • No parentheses used: For an expression displayed in a separate line, the system will read the entire content that matches this expression. For an expression taking up more than one line, the system can still read the entire content as long as "\n" tails each line like "DEBUG=win\ndows".
	Expected Value	Expected value corresponding to the rule. This parameter is used with **Rule** to check whether the content matched by using the regular expression is compliant with relevant requirements. When a regular expression is used, you should type the expected value enclosed with slashes. For example, "/DEBUG=\d+/" indicates that the expected value is "DEBUG=\d+". • Case-insensitive match: //i. For example, "/DEBUG=\d+/i" indicates that the expression is case-insensitive. • Metacharacter (.) matching any characters: //s. For example, "/DEBUG=.*/s" indicates that "." matches any characters. • Multiline match: tails each line with "\n".
Port Check	Type	Specifies the transport protocol of the port to be checked.
	Port Number	Port number to be checked.
	Expected Value	Expected value corresponding to the rule. This parameter is used with **Match Rule** to check whether the content matched by **Type** and **Port Number** is compliant with relevant requirements.
File Content Check	File Path	Specifies the absolute path of the file to be checked.
	File Content	Specifies a regular expression. The system matches results returned by the command specified above line by line according to the regular expression, so as to find desired information. • Use of parentheses: indicates that the system will read content that matches the subexpression in parentheses in an expression like "DEBUG=(\d)". • No parentheses used: indicates that the system will read the entire content that matches this expression.
	Expected Value	Expected value corresponding to the rule. This parameter is used with **Match Rule** to check whether the content matched by **File Content** is compliant with relevant requirements.

Parameter		Description
File Permission Check	File Path	Specifies the absolute path of the file to be checked.
	Expected Value	Expected value corresponding to the rule. This parameter is used with **Match Rule** to check whether the content matched by **File Path** is compliant with relevant requirements.
Process Check	Process Name	Specifies the name of the process to be checked.
	Expected Value	Expected value corresponding to the rule. This parameter is used with **Match Rule** to check whether the content matched by **Process Name** is compliant with relevant requirements.
XML Configuration File Check	XML File Path	Specifies the complete path of the XML file that contains desired data.
	Node	Specifies the node where the XML file resides (standard XPath syntax is supported; attribute value may be left empty).
	Attributes	Specifies the attribute of the node where the XML file resides. This parameter is optional.
	Expected Value	Expected value corresponding to the rule. This parameter is used with **Match Rule**.
Debug		Tests whether the system can perform checks on target hosts and return the check result. In the debugging process, you can click **Stop** to stop the operation. For parameters for debugging check points, see Table 4-3.
Edit Hardening Information		Manages hardening points. In the dialog box that appears, click **Add Hardening Point** to create a hardening point. Parameters in the **Add Hardening Point** dialog box are described in detail on the UI. A hardening point, after being created, can be edited and deleted.

Table 8-6 Configuring logical relationship between check points

Parameter	Description
AND	Logical AND operator.
OR	Logical OR operator.
NOT	Logical NOT operator.
(and)	Used to raise the priority, indicating that checks in parentheses are performed preferentially.
←	Used to remove the last symbol typed in the configuration box.
Add to rule	Used to add the check point to the configuration box of logical expressions.
Text box	Click **Add to rule**, **AND**, **OR**, **NOT**, **(**, **)**, or ← to configure a logical relationship between check points. The check result of each check item depends on the logical relationship between check points. For example, "a and b" indicates that the check result is **True** (compliant) only when the result of both check points a and b is **True**.

- **Additional Check Items**: obtains information about target hosts and then displays it as **Other Information** in scanning reports. Additional check items are not used to check whether the configuration of target hosts is compliant with relevant requirements.
  - Click **Create** and configure parameters. Table 8-7 describes parameters for configuring an additional check item.
  - An additional check item, after being created, can be edited and deleted.

Table 8-7 Parameters for adding an additional check item

Parameter	Description
Check Item	Name of the new additional check item.
Executive Command	Command for enumerating information.
Line Match Expression	Regular expression used to match an entry. When each entry takes up one line, you can use "+". When multiple entries are in one line, you can type them as required.
Column Name	Column name. You can click **Add** to add a column name in the text box.
Column Splitting Expression	Used for matching fields to be extracted from an entry. The use of parentheses indicates a column field to be extracted (having a one-to-one mapping with the column name), for example, (column1)\s+(column2)\s+(column3). When entries are in different formats, you can type multiple expressions for matching column fields. You can click **Add** to add an expression in the text box.

Other Operations

- The default system administrator (**admin**) and new system administrators have the privilege of managing all configuration templates. Common administrators can manage only configuration templates created by themselves. However, when creating a task, an administrator can use any templates.
- If the template fails to be generated immediately after you complete the configuration, the system automatically saves the configured template to the template list for you to edit or generate later. Note that you cannot use a template that has not been generated during task creation.
- A configuration template, after being created, can be queried, viewed, edited, deleted, and exported. It can also be saved as another template.
- To import a configuration template, click **Import**, select the .dat file, and then upload this template to the system. Configuration templates on an RSAS device can be imported into another RSAS with the same template groups and template authorization.

8.2.3 Defect Template

Defect templates are used for code audit tasks, which discover security defects and noncompliance in code files against defect rules.

8.2.3.1 Creating a Defect Template

The administrator can manage a type of security defects or those of concern in a defect template as required.

Choose **Knowledge Base > Templates > Defect Template > Defect Template**. Click **Create Defect Template** and configure parameters in the drawer that appears from the right side. Table 8-8 describe parameter for configuring a defect template.

A defect template, after being created, can be queried, viewed, edited and deleted.

Table 8-8 Parameters for creating a defect template

Parameter	Description
Template Name	Name of the new defect template. It should be a string of 1–64 characters.
Template Description	Brief description of the new defect template. It should be a string of 0–256 characters.
Defect List	Click **Add Defect** and select security defect rules to be managed. For details about how to add a defect rule, see Creating a Defect Rule.

8.2.3.2 Creating a Defect Rule

The defect rule database manages the code security defects and illegitimate code that RSAS detects. A defect may contain multiple detection rules.

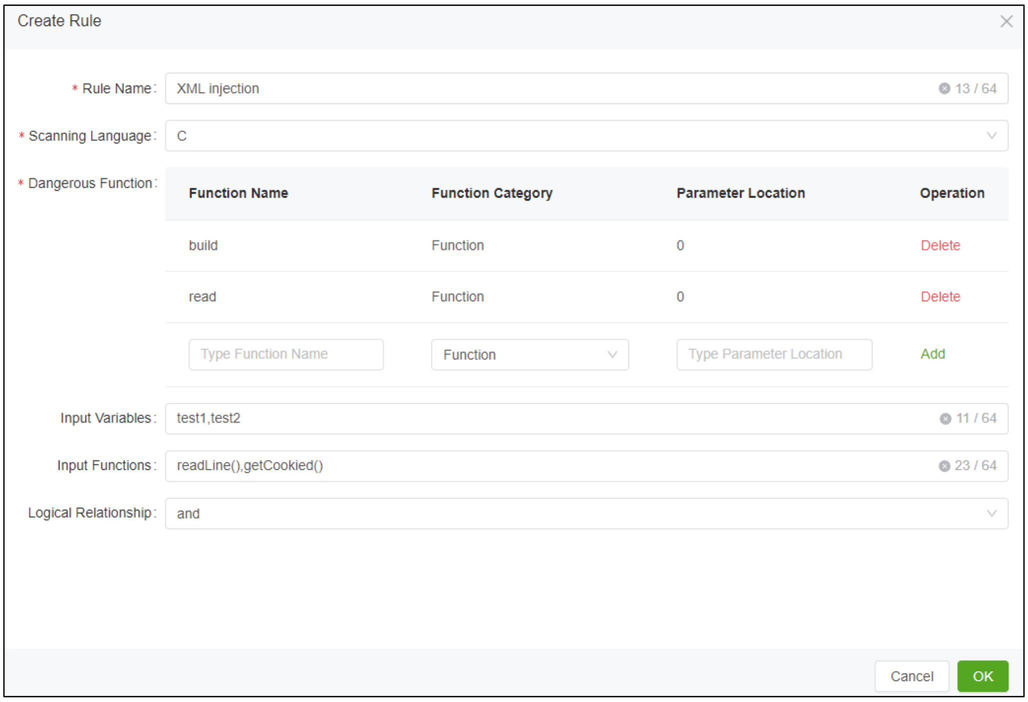
Choose **Knowledge Base > Templates > Defect Template > Defect Rule DB**. Click **Add Defect** and configure parameters in the drawer that appears from the right side. Table 8-9 describes parameters for configuring a defect.

A defect, after being created, can be queried, viewed, edited and deleted.

Table 8-9 Parameters for creating a defect

Parameter	Description
Defect Name	Name of the security defect. It should be a string of 1–50 characters.
Defect Category	Type of the security defect.
CWE ID	CWE ID of the security defect.
Defect Description	Descriptive information of the security defect.
Vulnerability Score	Risk score of the security defect. A greater score indicates higher risk.
Defect Example	Example of the security defect.
Solution	Solution to the security defect.
Rule List	Click **Create Rule** and configure rule parameters. The functions and variables vary with programming languages. The language C is used as an example to describe how to add a rule, as shown in Figure 8-2.

Figure 8-2 Adding a rule



Create Rule

* Rule Name: XML injection (13 / 64)

* Scanning Language: C

* Dangerous Function:

Function Name	Function Category	Parameter Location	Operation
build	Function	0	Delete
read	Function	0	Delete
Type Function Name	Function	Type Parameter Location	Add

Input Variables: test1,test2 (11 / 64)

Input Functions: readLine(),getCookied() (23 / 64)

Logical Relationship: and

8.2.4 Image Template

Image templates are used for configuration checks during image scanning tasks. Currently, RSAS only allows you to use built-in templates, whose contents cannot be edited.

Choose **Knowledge Base** > **Templates** > **Image Template** > **Image Configuration Audit Template**. Click **View** in the **Operation** column of a configuration check template to view its basic settings, automatic check items, and additional check items. Under **Auto Check Item**, click **View** in the **Operation** column to view details of this check item.

8.2.5 Status Template

By default, all vulnerable accounts and ports on a target host are taken as illegitimate during scanning. You can add trusted accounts on the target host to the account allowlist and add open ports on such host to the port allowlist to prevent RSAS from taking them as risky during scanning.

Choose **Knowledge Base** > **Templates** > **Status Template**. Click **Add** and configure parameters in the drawer that appears from the right side. Table 8-10 describes parameters for configuring a status template.

A status template, after being created, can be queried, viewed, edited, deleted, exported, and imported. It can also be saved as a new template.

Table 8-10 Parameters for creating a status template

Parameter	Description
Name	Specifies the template name. It should be a string of 1–20 characters.

Parameter	Description
Account	Specifies the account allowlist. Select accounts that will be ignored in risk scanning. Click **Add**, type the account and description, and click **Save**.
Port/Process	Specifies the port allowlist. Select ports that will be ignored in risk scanning. Click **Add**, type the process name, port number, and description, and click **Save**.

8.3 Password Dictionary

You can configure password dictionaries listed in **Service Type** when creating a password guess task. Then RSAS will attempt to log in to target devices by using the password dictionary. If the login user name and password of a target device can be found in a password dictionary, the target device is considered to have a vulnerable account.

Password dictionaries include system ones (containing common vulnerable accounts, which can be viewed and saved as a new password dictionary, but cannot be edited or deleted) and custom ones.

Choose **Knowledge Base > Password Dictionary**. Click **Create** and configure parameters.

A password dictionary, after being created, can be viewed, edited, and exported. It can also be saved as another dictionary.

Table 8-11 Parameters for configuring a password dictionary

Parameter	Description
Dictionary Name	Name of the new dictionary. It is a string of 1 to 64 characters, consisting of letters (case-sensitive), digits, Chinese characters, hyphens (-), and/or underscores (_). The name of the new dictionary must be unique.
Category	• **User Name**: indicates that the dictionary contains weak user names for RSAS to scan. • **Password**: indicates that the dictionary contains weak passwords for RSAS to scan. • **User Name/Password**: indicates that the dictionary contains weak user names and passwords for RSAS to scan.
Content	User names, passwords, or user name/password pairs, which are separated by carriage returns. Up to 10,000 entries can be typed. If more entries are required, import a dictionary file. A user name/password pair should be typed in the format of user name:password, for example, administrator:nsfocus.
Dictionary File	Imports a .txt file. • The file name should consist of letters (case-sensitive), digits, hyphens (-), and/or underscores (_). • Content in the file should be in the same format as specified for **Content**. UTF-8 and ASCII encoded files are supported. • Select the password dictionary file, and then import it to the system. Note If an imported dictionary file contains incorrect information, such information will

Parameter	Description
	not be used during the execution of password guess tasks.
Description	Brief description of the new dictionary.

8.4 Offline Check Tool

Offline check tools are used to locally check the configuration of target hosts. For how to download an offline check tool and how to configure a local scanning task, see Offline Configuration Scan.

Templates for offline checks are generated from configuration templates. For how to configure a configuration template, see Configuration Template.

8.5 Hardening Knowledge Base

The hardening knowledge base provides support for configuration hardening operations. It consists of a detailed list of configuration check items and hardening operations. Currently, you can only view the hardening knowledge base and cannot perform other operations.

The following uses Linux configuration specifications as an example to show how to view the hardening knowledge base

Choose **Knowledge Base > Hardening KB**. Click the template name **Linux Configuration Specification** to display the list of check items for Linux hardening.

8.6 Offline Hardening Tool

To protect against the ransomware WannaCry, RSAS provides an offline hardening tool to automatically add a related rule on the host firewall to block this ransomware.

Choose **Knowledge Base > Offline Hardening** > **Windows Hardening Tools**. Click **One-Click Hardening Tool Against WannaCry** to download the tool to a local disk drive. Execute the .bat script as the administrator and then perform operations as prompted.

8.7 Port List

A port list displays the numbers, service types, and running protocols of the listening ports on the scanned device. For example, port 80 maps the HTTP service.

If a port scanning policy is configured during task creation, only ports in the port list will be scanned during the execution of the task.

The **Port List** page consists of two tabs: **System Ports** (information about common ports) and **Custom Ports**. In the **Custom Ports** tab, you can add ports that are not included in **System Ports**.

Choose **Template Management > Port List > Custom Ports**. You can add a port through manual operation or intelligent port discovery.

A port, after being created, can be queried, refreshed, edited and deleted.

- Manual operation: Click **Add Custom Port** and configure port parameters.

Table 8-12 Parameters for adding a port

Parameter	Description
Service Name	Specifies the name of the service running on the port. It must be a string of 1 to 18 characters consisting of letters (case-sensitive), digits, and/or -.
Port	Port number. The value is an integer ranging from 1 to 65535.
Protocol	Protocol that runs on the port.

- Intelligent port discovery: Click Intelligent Port Discovery to obtain all ports scanned in historical vulnerability scanning and configuration check tasks. For this purpose, you can choose either Overwrite Update or Incremental Update. The former will delete custom ports manually added, while the latter will not.

9 Authentication

Authentication management is focused on system scanning information. Authentication information correlates with IP addresses of assets. After you enter an IP address or IP address range during creation of a task, RSAS directly invokes authentication information for scanning.

The host authentication information can be added in the following ways:

- Manually added, imported, or updated.
- Select **Sync to authentication mgmt** during task creation. For detailed operations, see Assessment Task and Configuration Scanning Task.
- Click **Configure authentication information** when adding an asset. For detailed operations, see Adding an Asset.

The authentication information, after being added, can be exported, queried, edited, deleted, and cleared.

Manually Adding Authentication Information

Choose **Authentication**. Click **Add Host** and configure host authentication parameters.

Table 9-1 Parameters for configuring host authentication information

Item	Parameter	Description
System Login Information	IP	Specifies the IP address or IP address range of the scan target. The specified IP address or IP address range must be within the scan scope.
	• Domain Name/Domain User • Password (Domain Password)	Specifies the user name and password for login to the scan target. RSAS stores the user name and password in an encrypted way to ensure security.
	Obtain	You can click **Obtain** to obtain the host login password from OSMS that collaborates with RSAS. For how to configure collaboration with OSMS, see Authentication Management.
	Login Protocol/Login Port	Specifies the protocol and port used for login to the scan target. For login via HTTP, HTTPS, and WinRM, RSAS can only do

Item	Parameter	Description
		configuration checks, but cannot conduct vulnerability scanning.
	Host Jump	When RSAS can log in to multiple target hosts directly or using the same jump host, you can configure the same jump host after **Host Jump** is enabled. - If RSAS cannot directly log in to the target host, it can use the jump host for scanning. In this case, you need to configure the authentication information for the jump host in advance. - Make sure that the jump host can connect to the target host. This parameter is available only when **Login Protocol** is set to **SSH** or **Telnet**.
	Login Path/Site Cookie	Specifies the login path and website cookies (which record login session IDs) for login to the scan target via HTTP or HTTPS. You can click **Record** to set the browser proxy as prompted. After the proxy server is set, RSAS can capture cookies.
	Login Authentication	Clicking **Login Authentication** checks whether login information is correct to make sure that RSAS can log in to the target host for local scanning.
ORACLE Scanning Policy	Oracle	Controls whether to enable deep scan of vulnerabilities in Oracle. At the same time, you need to enable **Oracle Deep Scan** on the **Advanced Settings** tab (see Table 4-5) during task creation.
WebLogic Scanning Policy (Enables the deep scan of vulnerabilities in WebLogic.)	System Scanning	Controls whether to allow access to WebLogic via the management background of a device on which the WebLogic service resides. - **Linux/Windows**: operating system type - **WebLogic Version**: WebLogic version - **WebLogic Install Account**: user name for access to WebLogic - **WebLogic Opatch Install Dir**: installation path of WebLogic WLS
	Page Scanning	Controls whether to allow access to WebLogic via web. - **User Name/Password**: user name and password for access to WebLogic. - **Path**: WebLogic URL.
Configuration Template	Enable MLPS	Controls whether to enable the MLPS function. If it is enabled, you need to an MLPS level and select the corresponding MLPS template. For details about MLPS levels, see MLPS.
	Host	Indicates computers with an operating system installed. You can click a template name to add the template to the **Selected Templates** box and then configure template parameters. - **Operating system template**: configuration specifications of operating systems - **Virtual device template**: configuration specifications of virtual devices - **Application template**: configuration specifications of applications

Item	Parameter	Description
		• **Database template**: configuration specifications of databases • **Big data template**: configuration specifications of big data software or platforms
	Network device	Indicates physical entities connected to the network except for hosts, such as switches and routers. • You can click a template name to add the template to the **Selected Templates** box and then configure template parameters. • Select configuration specifications of network devices.
Status Template	Template	Specifies an allowlist of items that are deemed to be compliant. You can click **Status Template Management** to open the page for configuring a status template. For how to create a status template, see Status Template.

Importing Authentication Information

Choose **Authentication**. Click **Download Template** to save the authentication information template to a local disk drive. Click **Import** and select the template that has been edited and saved.

Updating Authentication Information

RSAS can collaborate with OSMS. After authentication information is configured, choose **Authentication** and click **Update** to obtain authentication information of the scanned hosts from OSMS. You can also configure the automatic update during configuration of authentication information.

- Click **Update** in the **Operation** column to update a single entry.
- Select multiple entries of authentication information and click **Bulk Operation** > **Update Selected** to update the selected entries.
- Click **Bulk Operation > Update All** to update all authentication information.

10 Administration

This chapter presents information about system management, containing the following sections:

Section	Description
Status	Describes how to view the system status and registered authorization information of RSAS.
Configuration	Describes how to configure network, routing, system, and task settings.
Services	Describes how to upgrade and restore the system, and manage system services.
Users	Describes user privileges and user management methods.
Common Tools	Describes how to use common tools available on RSAS.

10.1 Status

You can view the system status, registered authorization information, and network status of the current RSAS device. You can also perform basic operations on RSAS.

Viewing the System Status

Choose **Administration** > **Status** > **System Status** to view information about the system status of the current device. In addition, you can restart or shut down the system.

License Status

Registered Authorization Info

Choose **Administration** > **Status** > **License Status** to view the registered authorization of the system.

- The purchased detection languages are necessary for creating defect rules.
- By default, RSAS provides one management interface and one scan interface. Therefore, the number of authorized scan interfaces is 1 + number of scan interfaces you have purchased.
- By default, RSAS provides two CPUs. Therefore, the number of authorized CPUs is 2 + the number of CPUs you have purchased.

Caution

- The validity period of the license starts from 00:00 of **Start Date of Current Service** to 24:00 of **End Date of Current Service**.
- The validity period of a paid license refers to the period within which RSAS can be upgraded. The validity period of a trial license refers to the period within which RSAS can be used. In the English environment, the date format is YYYY-MM-DD, such as 2011-07-20.
- After a paid license expires, RSAS can still be used, but cannot be upgraded. After a trial license expires, RSAS cannot be used. In the latter case, RSAS automatically displays the page for importing a license, and no other operation can be performed before a license is imported. RSAS with a license (either a trial or paid license) can be upgraded before the license expires. For a customized RSAS, whether it can be upgraded depends on customization requirements.
- For a paid license, within 30 days before the license expires, RSAS displays a notification, prompting users to replace the license. After a paid license expires, RSAS notifies users of how many days have passed since expiration. For a trial license, RSAS does not display a notification before or after the license expires.

Importing and Exporting a License

A hardware RSAS only supports authentication by license, while vRSAS can be authenticated in one of the ways as described in Table 10-1.

- After RSAS is successfully authenticated, you cannot change the authentication method subsequently.
- For the license authentication and authentication by NSFOCUS Security Cloud, you can import the license to a local disk drive, or replace (import) a license for RSAS that runs properly.

Table 10-1 Supported authentication methods for vRSAS

Authentication Method	**Description**	**Import and Export**
Centralized authorization	If RSAS is managed by the centralized authentication and authorization (CAA) platform, you can obtain the license of RSAS from the platform. Note After RSAS is disabled for centralized management on the CAA platform, the authentication method you selected previously on RSAS remains unchanged, but RSAS cannot work anymore. If RSAS authenticated this way is offline, the device itself measures how long the offline status lasts: • If the device remains offline for no more than 7 x 24 hours, you can use other functions than generating offline reports, exporting tasks, performing upgrades, creating restore points, importing and exporting restore point files, and using secondary development interfaces. • If the device remains offline for more than 7 x 24 hours, the web-based manager is unavailable. After RSAS is offline, you can still use it after changing its IP	Export is supported but import is not supported.

Authentication Method	Description	Import and Export
	address. In this case, to have RSAS reauthenticated by the CAA platform, you need to change the current IP address back to the previous one.	
Security cloud-side authentication	RSAS regularly obtains authorization directives from the security cloud system to check its own availability. Note If RSAS authenticated this way is offline, the device itself measures how long the offline status lasts: • If the device remains offline for no more than 7 x 24 hours, you can use other functions than generating offline reports, exporting tasks, performing upgrades, creating restore points, importing and exporting restore point files, and using secondary development interfaces. • If the device remains offline for more than 7 x 24 hours, the web-based manager is unavailable. Each authentication license provided by Security Cloud applies to only one online RSAS. If you attempt to apply such license to multiple online devices, your license will be revoked. For details, contact technical support personnel of NSFOCUS.	Support
License-based authentication	This method applies to RSAS with a dongle and a license file.	Support
ESP-L certification	If RSAS is managed by the NSFOCUS Enterprise Security Platform –License (ESP-L) platform, you can obtain the license of RSAS from the platform.	Export is supported but import is not supported.

Running Status

Choose **Administration > Status > Running Status**. You can view the following status information:

- View the running status of services. In addition, you can restart the services as required.
- View the system resource usage, including the CPU, memory, and hard disk usage. When the usage of disk space reaches the threshold specified in Disk Usage Alert Threshold, you can click **Release space** in the **Operation** column to clean up data. After the **Optimize system resources** switch is turned on, RSAS automatically manages its CPU and memory by group to avoid resource overuse and reduced speed.
- View the network status. In the upper-right corner of the **Network Status** area, select an interface from the drop-down list to display the received and transmitted traffic of the specified interface in the last 20 minutes.
- View alerts. After selecting an alert type and specifying a period, you can view alerts about the memory, disk, and CPU usage.

10.2 Configuration

This covers network configuration, route configuration, system configuration, and task configuration.

10.2.1 Configuring Network Settings

The network configuration module allows you to configure and manage network scan interfaces and DNS servers. Network scan interfaces are used by RSAS to interact with other devices for exchange of scan results. Physical interfaces are interfaces that actually exist on a device, such as interfaces eth1 to eth6 supported by RSAS.

Note	The number of available scan interfaces depends on the license. You can configure only the authorized number of scan interfaces.

Configuring Local Network Interfaces

Choose **Administration** > **Configuration** > **Network**. Click **Edit** in the **Operation** column of an interface and edit interface parameters as described in Table 10-2. You can click **Enable** or **Disable** in the **Operation** column of an interface to enable or disable this interface.

Table 10-2 Parameters for configuring interfaces

Parameter	Description
Interface Name	Specifies the name of the interface, which cannot be edited.
IPv4 Config Mode	Specifies the mode for configuring the IPv4 address, which can be **Manual** or **Auto obtain**.
IPv4 Address	Specifies the IPv4 address of the interface. This parameter must be configured when **Manual** is selected.
IPv4 Netmask	Specifies the subnet mask of the specified IP address of the interface.
IPv4 Gateway	Specifies the IPv4 gateway of the interface. For scanning across network segments, you must properly configure the network gateway.
Default Gateway	Controls whether to enable the default IPv4 gateway.
IPv6 Config Method	Specifies the mode for configuring the IPv6 address, which can be **Manual** or **Auto obtain**.
IPv6 Address	Specifies the IPv6 address of the interface. This parameter must be configured when **Manual** is selected.
IPv6 Prefix Length	Specifies the prefix length of the specified IPv6 address of the interface. The prefix in an IPv6 address is the equivalent of the network ID in an IPv4 address. The prefix length indicates the route bits. For direct communications without a router, the devices' IPv6 addresses must have the same prefix.

Parameter	Description
IPv6 Gateway	Specifies the IPv6 gateway of the interface. For scanning across network segments, you must properly configure the network gateway.
Default Gateway	Controls whether to enable the default IPv6 gateway.
NIC Duplex Mode	Specifies the NIC duplex mode of the interface, which can be **Auto**, **Half-duplex**, or **Full-duplex**.
Connection Rate	Specifies the connection rate of the interface.

Configuring DNS Servers

Choose **Administration** > **Configuration** > **Network**. Under **DNS Server Configuration**, configure parameter. Table 10-3 describes DNS server parameters.

Table 10-3 Parameters for configuring DNS servers

Parameter	Description
Preferred DNS Server	Specifies the IP address of the preferred DNS server for the device. Some scanning plugins and system functions rely on the domain name resolution. Therefore, you must configure a correct domain name server.
Alternate DNS Server	Specifies the IP address of the alternate DNS server for the device. Some scanning plugins and system functions rely on the domain name resolution. Therefore, you must configure a correct domain name server.
Domain Name List	List of domain names to be accessed in the intranet. This is aimed at eliminating domain name resolving failures due to incomplete domain names of redirection addresses. Multiple domain names should be separated by the comma (,), semicolon (;), or space.

Configuring the Hosts File

The hosts file serves as a database by associating common domain names with their corresponding IP addresses. When scanning a domain name, RSAS automatically searches for its IP address from the hosts file configured here. If such an IP address is not found, RSAS submits the domain name to the DNS server for resolution.

Choose **Administration** > **Configuration** > **Network**. Under **System Host Configuration**, configure hosts as indicated on the UI.

10.2.2 Configuring Routing Settings

Routing refers to the process of selecting a path from a routing table for transmission of packets from a source address to a destination address. Routing on RSAS is to find the next-hop routing device or destination host for each packet passing through it before forwarding these packets. You can manually configure a static route on RSAS.

Choose **Administration > Configuration > Route Configuration**. Click **Add** and configure route parameters.

- A route, after being created, can be edited and deleted.
- Clicking **Route Info Table** redirects you to **Administration > Common Tools > Route Information** to view route details.

Table 10-4 Route parameters

Parameter	Description
Route Type	Specifies the route type, which can be **IPv4** or **IPv6**.
Destination IP	Specifies the IP address of the destination host or the destination network segment to which packets will be sent. The IP address set here must match the route type you selected.
Netmask/Prefix	Specifies the subnet mask of the specified IPv4 address or the prefix of the specified IPv6 address.
Gateway IP	Specifies the next-hop IP address of the network interface.
Priority	Specifies the priority of the static route, which is an integer from 1 to 9999. A smaller value indicates a higher priority. Setting the route priority aims at achieving load balancing among links with the same administrative distance to the destination.
Interface	Specifies the egress for RSAS to forward packets.

10.2.3 Configuring System Settings

This section describes how to configure system settings.

10.2.3.1 System Time Synchronization

The built-in system clock is the reference time for the system to record logs and dispatch scanning tasks. Therefore, the accuracy of system time has a direct impact on such events. To ensure time accuracy, RSAS provides the system time management function. You can set the system time only after a paid license is imported.

Choose **Administration > Configuration > System Configuration**. Under **System Time Sync**, configure parameter. Table 10-5 describes parameters in this area.

Table 10-5 System time parameters

Configuration Mode	Parameter	Description
Synchronization with NTP server	Time Server	Specifies the website or IP address of the time server. After the configuration, click **OK**.
	Auto synchronization	Synchronizes the system time automatically.
	Synchronize	Synchronizes the system time immediately.
Manual change	Change Current Time	Specifies the current date and time of RSAS, which should be in the format of YYYY-MM-DD HH:MM:SS such as 2013-05-

Configuration Mode	Parameter	Description
		08 10:27:04.

10.2.3.2 HTTPS Certificate Import

An HTTPS certificate is required to activate HTTPS authentication for encryption of data communications between clients and RSAS, thereby preventing information disclosure.

Choose **Administration** > **Configuration** > **System Configuration**. Under **HTTPS Certificate Import**, select an HTTPS certificate (.crt) and private key (.key) and import them to the system.

10.2.3.3 Login Failure Configuration

To prevent malicious login attempts for the sake of security, the system provides the login failure control function, allowing you to set the maximum number of failed login attempts and the action upon excessive attempts, and to lock or unlock IP addresses or accounts.

Choose **Administration** > **Configuration** > **System Configuration**. Under **Login Failure Config**, configure parameters. Table 10-6 describes login failure parameters.

To unlock IP addresses or accounts, you can click **Unlock IP**/**Account** and select IP addresses or accounts to be unlocked.

Table 10-6 Parameters for configuring login failure settings

Parameter	Description
Max Login Attempts	Specifies the maximum number of failed login attempts allowed. It is an integer ranging from 3 to 10.
Action upon Excessive Attempts	Specifies the action taken against the user whose number of login attempts exceeds the specified maximum. The value can be **Not process**, **Lock IP**, or **Lock account**.
Lockout Duration	Specifies the duration when the IP address or account remains locked. By default, it is **20** minutes. This parameter is available only after **Action upon Excessive Attempts** is set to **Lock IP** or **Lock account**.

10.2.3.4 Auto Logout

For the sake of device security, the system provides the auto logout time setting function. After login to the web-based manager, if you remain inactive until the specified auto logout time expires, the system logs you out automatically by taking you to the login page. To continue using the system, you must log in again.

Choose **Administration** > **Configuration** > **System Configuration**. Under **Auto Logout**, set the auto logout time. The value of **Time** should be within the range of 0–999999 in minutes. The value **0** indicates that auto logout is disabled. The default value is **10** minutes.

10.2.3.5 HTTP Host Header Configuration

Enabling HTTP host header defense can enhance the defense capability of RSAS. After this function is enabled, RSAS can be accessed only from the IP addresses or domain names included in the HTTP host list and network interface configuration.

Choose **Administration** > **Configuration** > **System Configuration**. Under **HTTP Host Header Configuration**, enable **HTTP Host Header Defense**, type a custom host header, and click **Add** to add it to the list.

For example, the IP address of RSAS is 10.65.20.172. After **aaa.com** is added as a custom host header, you can access RSAS by typing **https://aaa.com** in the address bar.

10.2.3.6 Special Parameters

Special parameters are used to control packet capture and remote assistance functions. For the function details, see sections Capturing Packets and Configuring Remote Assistance.

Choose **Administration** > **Configuration** > **System Configuration**. Under **Special Parameters**, enable special parameters. Then remote assistance and packet capture functions become available under **Administration** > **Service** > **System Service**.

10.2.3.7 Disk Usage Alert Threshold

When the disk space used by data reaches the threshold, the system notifies the administrator by generating an alert.

Choose **Administration** > **Configuration** > **System Configuration**. Under **Disk Usage Alert Threshold**, specify the percentage of disk usage for the system to generate an alert. The default value is **80%**.

10.2.3.8 SNMP Trap Configuration

RSAS supports management via the Simple Network Management Protocol (SNMP). RSAS can not only respond to queries from the SNMP manager as an agent by returning information about its running status, but also send trap messages to the SNMP manager.

Choose **Administration** > **Configuration** > **Network**. Under **SNMP Trap Configuration**, configure SNMP trap parameters as described in Table 10-7.

Table 10-7 Parameters for configuring SNMP traps

Parameter		Description
Status		Specifies the status of SNMP trap. Options include **Enable** and **Disable**.
Version		Specifies an SNMP version supported by RSAS. Options include **v1**, **v2**, and **v3**.
IP Type		Specifies the IP address type of the SNMP manager, which can be **IPv4** or **IPv6**.
IP		Specifies an IPv4 or IPv6 address. For the format of the IP address, see the prompt on the GUI.
Port		Specifies the port used for communication with the SNMP manager.
Interval		Specifies the interval for communication with the SNMP manager.
v1/v2	Community	Specifies the community string used by the SNMP manager for access to RSAS.
v3	User Name	Specifies the SNMPv3 user name. It must consist of at least 8 characters and

Parameter		Description
		cannot contain Chinese or special characters.
	Security Level	Specifies the security level of SNMPv3 authentication, which can be **Not authenticate or encrypt**, **Authenticate**, or **Authenticate and encrypt**.
	Authentication Protocol	Specifies the protocol used for authentication, which can be **MD5** or **SHA**.
	Authentication Key	Specifies the key used for authentication, which must be at least 8 characters long and contain only digits and letters.
	Encryption Protocol	Specifies the encryption algorithm used for transmitting messages, which can be **DES** or **AES**.
	Encryption Key	Specifies the key used for encryption, which must be at least 8 characters long and contain only digits and letters.
	EngineID	SNMP engine ID of the SNMP engine, which is a string of 10–64 hexadecimal characters, such as 0x1234567890.

10.2.3.9 System GUI Customization

Choose **Administration > Configuration > System Configuration**. Under **System GUI Customization**, configure system information. Table 10-8 lists system information that can be customized.

Table 10-8 Customizable system information

Parameter	Description
Company Logo	Specifies NSFOCUS's company logo on the login page.
HTTP Report Header Logo	Specifies the logo shown on the header of HTTP reports.
Product Name	Specifies the system name. All pages with the system name shown will be changed accordingly.
Company Name	Specifies the company to which RSAS belongs. All pages with the company name shown will be changed accordingly.
Login Page Copyright Info	Controls whether to display the copyright statement on the login page.
Home About Page	Controls whether to display information about NSFOCUS on the **About** page of the homepage.
Save settings	After modifying any of the foregoing parameters, click **OK** to make the settings take effect.

10.2.3.10 Mail Server

RSAS can store a specified number of offline reports for future query. Due to the limited hard disk space, RSAS supports the use of a mail server to store reports. The mail server can also be used for sending alert messages by email.

To use a mail server for saving reports or sending email alerts, you must configure it properly.

Choose **Administration** > **Configuration** > **System Configuration**. Under **Mail Server**, configure mail server parameters.

Table 10-9 Parameters for configuring a mail server

Parameter	Description
Authenticate By	Specifies the authentication mode for access to the mail server.
Mail Server Address	Specifies the address of the mail server. It can be an IP address (IPv4 or IPv6) or a domain name.
Port	Specifies the port for the mail server to send email messages.
Email	Specifies the email address for login to the mail server.
Password	Specifies the password for login to the mail server.
Test Email Configuration	You can click **Test Email Configuration** to make RSAS send a mail to the specified email account by RSAS, thus checking whether parameter settings are correct.

10.2.3.11 License Expiration Warning

To ensure the proper use of the system, RSAS automatically reminds users by popup or email to renew the license when the license is about to expire.

To receive a license expiration warning by email, you need to firstly configure a mail server as instructed in Mail Server and configure the following email parameters.

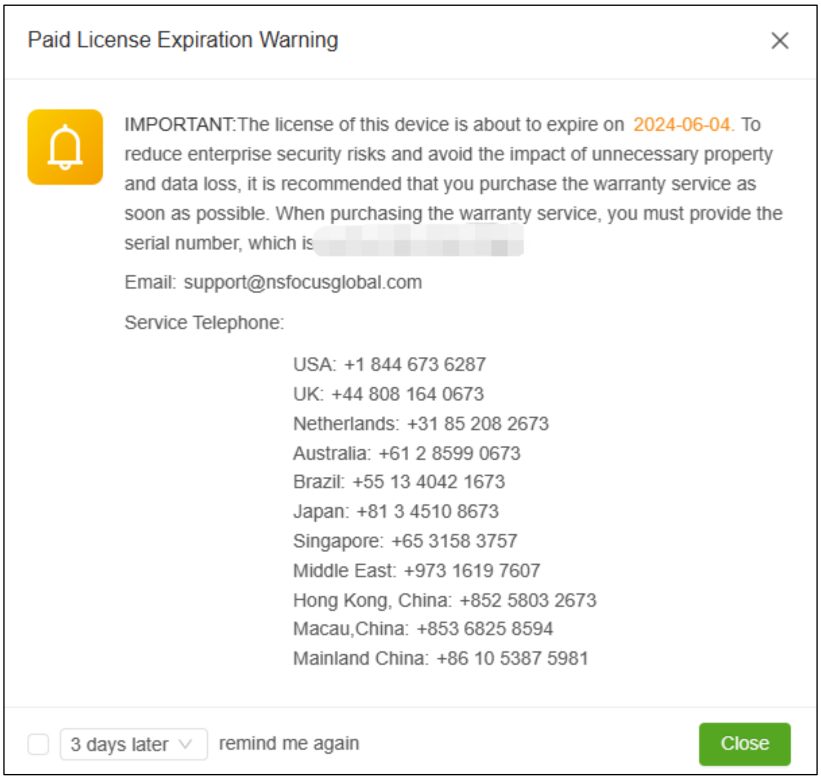
Choose **Administration** > **Configuration** > **System Configuration**. Under **License Expiration Warning**, configure the email address for receiving reminders, and specify the reminding frequency. The email content is the same as that provided on the UI, as shown in Figure 10-1.

Caution

The system displays a warning when the license is about to expire. You can set a period during which you will not be reminded again. To use RSAS properly, please timely import a new license as prompted.

- For a paid license, within 30 days before the license expires, the system displays the first warning. You will also receive the warning when the license has expired. You can choose to be reminded 1 month later, 1 week later, 3 days later, or never be reminded.
- For a trial license, within seven days before the license expires, the system displays the first warning. You can choose to be reminded 3 days later or never be reminded.

Figure 10-1 License expiration notification



Paid License Expiration Warning

IMPORTANT:The license of this device is about to expire on 2024-06-04. To reduce enterprise security risks and avoid the impact of unnecessary property and data loss, it is recommended that you purchase the warranty service as soon as possible. When purchasing the warranty service, you must provide the serial number, which is [redacted]

Email: support@nsfocusglobal.com

Service Telephone:

USA: +1 844 673 6287
UK: +44 808 164 0673
Netherlands: +31 85 208 2673
Australia: +61 2 8599 0673
Brazil: +55 13 4042 1673
Japan: +81 3 4510 8673
Singapore: +65 3158 3757
Middle East: +973 1619 7607
Hong Kong, China: +852 5803 2673
Macau,China: +853 6825 8594
Mainland China: +86 10 5387 5981

☐ 3 days later remind me again

10.2.3.12 Password Policy

To ensure system security based on login controls, you can set a password policy.

Choose **Administration** > **Configuration** > **System Configuration**. Under **Password Policy**, configure parameters. Table 10-10 describes parameters for configuring a password policy.

Table 10-10 Parameters for configuring a password policy

Parameter	Description
Password Length	Specifies the minimum length of the administrator's password. The length range is 8 to 32 characters.
Password Strength	Specifies the strength of the administrator's password. The value range is 1–4, indicating one to four types of the following characters: lowercase letters, uppercase letters, digits, special characters (@ # $ ^ _). • **1**: contains at least one of the acceptable character types. • **2**: contains at least two of the acceptable character types. • **3**: contains at least three of the acceptable character types. • **4**: contains all acceptable character types.
Password Age	Specifies how long a password can be used before the system requires the user to change it.
Account Inactivity Period	Specifies how long an account can remain unused before being disabled. Only the system administrator (**admin**) can enable accounts disabled this way.

10.2.3.13 Port Screening

You can specify ports that will be ignored by RSAS during scanning. However, IP addresses on the allowlist are not affected by port screening settings.

Choose **Administration** > **Configuration** > **System Configuration**. Under **Port Screening**, specify the following parameters:

- Port: specifies port numbers to be screened. You can type multiple port numbers separated by the comma (,) or a port range such as 11-200.
- IP allowlist: specifies IP addresses immune to port screening settings. You can type individual IP addresses, IP ranges, or IP segments in CIDR notation, separated by the comma or carriage return. Both IPv4 and IPv6 are supported.

10.2.3.14 Web Port Configuration

After a custom web port is enabled, you should access RSAS via this port.

Choose **Administration** > **Configuration** > **System Configuration**. Under **Web Port Configuration**, enable the custom web port and type the port number.

10.2.3.15 System Configuration

Choose **Administration** > **Configuration** > **System Configuration**. Under **System Configuration**, click **Click to Obtain** to download the package to a local disk drive. Type the decompression password (namely, the device hash displayed under **Administration** > **Status** > **System Status**) to view the system information.

10.2.3.16 Maximum Bandwidth

To ensure the proper functioning of the network, you can limit the maximum bandwidth assigned to RSAS for executing scanning tasks.

Choose **Administration** > **Configuration** > **System Configuration**. Under **Max Bandwidth (Mbps)**, set the maximum bandwidth in Mbps. The value is an integer in the range of 1–10000000.

10.2.3.17 Syslog Synchronization

RSAS supports sending audit logs to the syslog server.

Choose **Administration** > **Configuration** > **System Configuration**. Under **Syslog Sync**, enable syslog and configure syslog server parameters. Table 10-11 describes syslog server parameters.

Table 10-11 Parameters for configuring a syslog server

Parameter	Description
Syslog IP/Syslog Port	Specifies the IP address and port of the syslog server that receives audit logs from RSAS. The default port number is **514**.
Syslog Protocol	Specifies the protocol configured for the syslog server that receives audit logs from RSAS.

10.2.3.18 WSUS Configuration

Windows Server Update Services (WSUS) is a web-based solution for patch distribution. It allows users to manage the distribution of updates released for all Microsoft products, including Office and SQL Server. After WSUS is set for the intranet, all Windows updates are downloaded to the WSUS server from which intranet hosts obtain these updates. This avoids bandwidth usage for external network traffic and enables intranet hosts to update efficiently.

Choose **Administration > Configuration > System Configuration**. Under **WSUS Configuration**, configure WSUS server parameters, as described in Table 10-12.
Click **Download** to download the package to the target host and then run **wsus.reg**.

Table 10-12 Parameters for configuring a WSUS server

Parameter	Description
WSUS	Controls whether to enable the collaboration with the WSUS server.
WSUS IP	Specifies the IP address of the WSUS server.
Installation Mode	Specifies when to install the update after the collaboration configuration file is imported. • **Remind me**: asks users whether to install the update immediately after the collaboration configuration file is imported. • **Never remind me**: installs the upgrade immediately after the collaboration configuration file is imported.

Note	You can run the **unset-wsus.reg** command to remove WSUS settings.

10.2.4 Configuring Task Settings

This section describes how to configure task-related parameters.

10.2.4.1 Report FTP

To back up reports to an FTP/SFTP server, you must properly configure the FTP/SFTP server.

Choose **Administration > Configuration> Task Configuration**. Under **Report FTP**, configure server parameters.

Table 10-13 Parameters for configuring an FTP or SFTP server

Parameter	Description
FTP Server IP/FTP Server Port	Specifies the address and port of the FTP or SFTP server. It can be an IPv4 address or a domain name.
FTP Server Encoding	Specifies the encoding format used by the FTP or SFTP server for storing reports. For a Windows-based FTP or SFTP server with the UTF-8 encoding to properly receive reports of a scanning task, you must specify an English task name and

Parameter	Description
	enable both **Auto Generation** and **Upload via FTP**. For details about how to create a task, see New Task.
Path	Specifies the directory of the FTP or SFTP server for saving logs. If the root directory is used to save logs, set the path to /.
User Name/Password	Specifies the user name and password used for login to the FTP or SFTP server. This account must have the read-write permission.
Test FTP Configuration	You can click **Test FTP Configuration** to make RSAS upload a file to the FTP server, thus checking whether parameter settings are correct.

10.2.4.2 Concurrent Tasks

Concurrent tasks refer to multiple task execution requests that are processed simultaneously. RSAS supports concurrent tasks.

Choose **Administration > Configuration > Task Configuratio**n. Under **System Concurrency**, configure the following parameters:

- **Max Concurrent Scan Hosts**: specifies the maximum number of hosts that can be scanned simultaneously in a single scanning task.
- **Max Concurrent Scan Tasks**: specifies the maximum number of scanning tasks that can be executed simultaneously.
- **Max Concurrent Plugins**: specifies the maximum number of plugins that can be executed simultaneously.

10.2.4.3 Risk Metrics

Choose **Administration > Configuration> Task Configuration**. Under **Risk Metrics**, click **Configuration** to configure risk level metrics and risk score weights.

- Host Risk Level

  Host risk levels are graded based on the vulnerabilities and configuration risks of hosts. First, RSAS determines the risk score of a host by using the NSFOCUS Risk Assessment Model. Then it grades the host at the level of very vulnerable, vulnerable, safe, or very safe according to the host risk level metrics.
- Image Risk Level Metrics

  Image risk levels are graded based on the vulnerabilities and configuration risks of images. First, RSAS determines the risk score of an image by using the NSFOCUS Risk Assessment Model. Then it grades the image at the level of very vulnerable, vulnerable, safe, or very safe according to the image risk level metrics.
- Network Risk Level Metrics

  The network risk level is the weighted average of risk score of all hosts on the network. First, RSAS determines the network risk score by using the NSFOCUS Risk Assessment Model. Then it grades all hosts on the network at the level of very vulnerable, vulnerable, safe, or very safe according to the network risk level metrics
- Website Risk Level Metrics

  The website risk level is the weighted average of risk score of all websites on the network. First, RSAS determines the website risk score by using the NSFOCUS Risk

Assessment Model. Then it grades all websites on the network at the level of very vulnerable, vulnerable, safe, or very safe according to the website risk level metrics.

- Host Risk Weights

  RSAS calculates the general risk score of hosts by using the NSFOCUS Risk Assessment Model based on the proportions of vulnerabilities and configuration risks. Therefore, you must configure such proportions in the assessment model in advance.

- Images Risk Weights

  RSAS calculates the general risk score of images by using the NSFOCUS Risk Assessment Model based on the proportions of vulnerabilities and configuration risks. Therefore, you must configure such proportions in the assessment model in advance.

10.2.4.4 Authentication Management

RSAS can collaborate with OSMS. After OSMS information is properly configured, RSAS can obtain authentication information of the scanned hosts from OSMS.

Choose **Administration > Configuration > Task Configuration**. Under **Authentication Management**, configure parameters.

Table 10-14 OSMS Parameters

Parameter	Description
OSMS IP	Specifies the IP address of OSMS.
OSMS Port	Specifies the port number of the SSH service on OSMS, which must be the same as that set on OSMS. The default port is **22**.
OSMS Account	Specifies the account for login to OSMS.
OSMS Password	Specifies the password for login to OSMS.
Auto Update	Specifies how often RSAS obtains host information updates from OSMS automatically. By default, host information is updated daily. You can specify the time for the daily update.
Update Cycle	
Upgrade Time	

10.2.4.5 Default Task Parameters

Choose **Administration > Configuration > Task Configuration**. Under **Default Task Parameters**, you can enable or disable certain task parameters.

Table 10-15 Default task parameters

Parameter	Description
Debug Mode	By default, it is not enabled. This parameter is useful when an error occurs during the execution of a scanning task. If the debug mode is enabled, task execution information is recorded. When an error occurs, the error information will be exported and sent to the technical support personnel of NSFOCUS for analysis.
Password Guess	By default, it is not enabled. If password guess is enabled and login check is not performed on the host, RSAS checks the passwords on scan targets based on the password dictionary. For details

Parameter	Description
	about the password dictionary, see Password Dictionary.
Oracle Deep Scan	By default, it is enabled. • Disable: indicates that RSAS reports only the identification and thorough scan of vulnerabilities regarding the Oracle service. • Enable: indicates that RSAS reports all vulnerabilities, including local vulnerabilities regarding the Oracle service. In this case, you need to enable and configure Oracle parameters for the vulnerability scanning policy, in addition to manually adding the authentication information.
Login Check	By default, it is enabled. If this is enabled, **Login Check** is enabled by default for assessment tasks, indicating that RSAS checks whether the host configuration is compliant with relevant requirements.
Remote OpenSSH Version Scan	By default, it is not enabled. • Enable: indicates that RSAS remotely scans OpenSSH versions. • Disable: indicates that RSAS does not remotely scan OpenSSH versions.
Remote NTP Version Scan	By default, it is not enabled. • Enable: indicates that RSAS remotely scans NTP versions. • Disable: indicates that RSAS does not remotely scan NTP versions.

10.2.4.6 Code Audit Task Configuration

Code audit tasks discover security defects in code files and noncompliance against coding specifications. The code audit task configuration limits the code file size and scanned code quantity supported by RSAS.

Choose **Administration > Configuration > Task Configuration**. Under **Code Audit Task Configuration**, configure the allowable maximum size of the compressed code file to be uploaded and code lines to be scanned.

10.2.4.7 System Hardening/Rollback Concurrency

Choose **Administration > Configuration> Task Configuration**. Under **System Hardening/Rollback Concurrency**, set the maximum number of concurrent hardening/rollback tasks allowed.

10.2.4.8 Collaboration with NF

RSAS can collaborate with NF. To ensure that NF is properly connected to RSAS, you must configure required parameters on both RSAS and NF. Here, only the collaboration configuration on RSAS is described. For collaboration settings on NF, see the related user guide of NF.

After RSAS is successfully connected to NF, RSAS can obtain protection policies from NF and display information about protected IP addresses and vulnerabilities on RSAS. The final protection result will then be uploaded to NF.

Choose **Administration > Configuration > Task Configuration**. Under **Collaboration with NF**, configure parameters. Table 10-16 describes parameters for configuring collaboration with NF. After RSAS is connected to NF, **Collaboration Status** is displayed as **Connected**, indicating that RSAS now can collaborate with NF.

Table 10-16 Parameters for configuring collaboration with NF.

Parameter	Description
Collaboration Status	Shows whether RSAS is successfully connected to NF.
Collaborative IP	Specifies the IP address of NF to which RSAS will connect.
Password	Specifies the password, which should be the same as that set on NF.

10.3 Services

The module allows you to manage system upgrades, system restoration, and system services.

10.3.1 System Upgrade

RSAS supports both manual update and automatic update. For manual upgrade, you need to first obtain the update package and then install it. For automatic upgrade, you only need to configure related parameters so that the system can check update packages at a specified interval. When finding the latest one, the system installs it automatically.

Scheduled Upgrade

If RSAS can communicate with the upgrade server properly, the system can be automatically upgraded.

Choose **Administration > Service > System Upgrade**. Under **Scheduled Upgrade**, configure scheduled upgrade parameters as described in Table 10-17.

Table 10-17 Parameters for scheduled upgrade

Parameter	Description
Upgrade URL	Specifies the address of the upgrade server from which update packages will be obtained.
Upgrade Cycle	Indicates that the system checks whether a new update package is available on the upgrade server every day.
Upgrade Time	Specifies the time when the system checks whether a new update package is available on the upgrade server every day. The time should be in the format of HH:MM such as 12:38.
Installation Mode	Specifies how to install the new update package. Options include the following: • **Auto install**: When a new update package is detected, it will be submitted to the queue for an automatic upgrade. • **Remind me**: When a new update package is detected, the system prompts a message in the lower-right corner of the web-based manager. Clicking this prompt opens the **System Upgrade** page where you can instantly upgrade the device as required. For details about the instant upgrade, see Instant Upgrade.

Parameter	Description
	• **Disable auto upgrade**: indicates that the automatic upgrade function is disabled.
Use HTTP Proxy	Controls whether an HTTP proxy is used for RSAS to connect to the upgrade server. If yes, you need to turn on this switch and then set **Proxy Address**, **Port**, **User Name**, and **Password**.

Instant Upgrade

The instant upgrade refers to the process in which you check for new update packages manually and upgrade the device instantly when a new update package is available.

Choose **Administration** > **Service** > **System Upgrade**. Under **Instant Upgrade**, select the update packages and click **Upgrade**.

- Click **Check for Update**.

  The system will immediately connect to the upgrade server and check whether and how many update packages are available. If yes, you can click the number of available updates to view their details.
- Click **Historical Updates** to view the update results and all historical updates.

Manual Upgrade

When RSAS fails to connect to the upgrade server, you need to upgrade it manually.

Choose **Administration** > **Service** > **System Upgrade**. Under **Manual Upgrade**, select an update package and click **Upgrade**.

For the download path of update packages, see the information displayed on the UI.

Note	• You cannot upgrade the system manually while a scanning task is being executed. • You cannot upgrade the system manually while a system restoration is being performed. • During a manual upgrade, you need to install available update packages one by one from the earliest to the latest.

10.3.2 System Restoration

With the system restoration function, you can conveniently back up the system or restore the current system back to the state at a restore point.

System restoration: backs up configuration files and databases. With this function, you can use a backup file to restore only the system configuration of the same version on the same device.

You can manually create a restore point file, which is then saved in the system. The system saves only one restore point file that can be exported to a local disk drive. The restore point file name contains the product version and backup time.

Creating a Restore Point

Choose **Administration** > **Service** > **System Restoration**. Click **Create** to create a restore point. The new restore point will overwrite the previous one, and the most recent restore point file will be displayed.

Exporting a Restore Point File

RSAS saves only the latest restore point file. Therefore, you are advised to export each restore point file to a local disk drive for backup. Later, you can import such a file to restore the system to the state recorded in the file.

Choose **Administration** > **Service** > **System Restoration**. Click the restore point file name to export it to a specified local directory for backup.

Restoring the System

The system restoration function is used to restore the system to the state at a restore point. Note that only the restore point file of the same version as the current system can be used for system restoration.

Choose **Administration** > **Service** > **System Restoration**. You can restore RSAS to the state at a certain restore point in either of the following ways:

- Using a restore point file saved in the system
  - This can only restore the system to the state recorded in the latest restore point file.
  - Click **Restore** next to **User Restore Point** to restore the system to the state recorded in the latest restore point file.
- Using a local restore point file
  - This can restore the system to the state recorded in any restore point file.
  - Select a restore point file, and click **Restore** to restore the system to the state recorded in the restore point file.

10.3.3 System Service

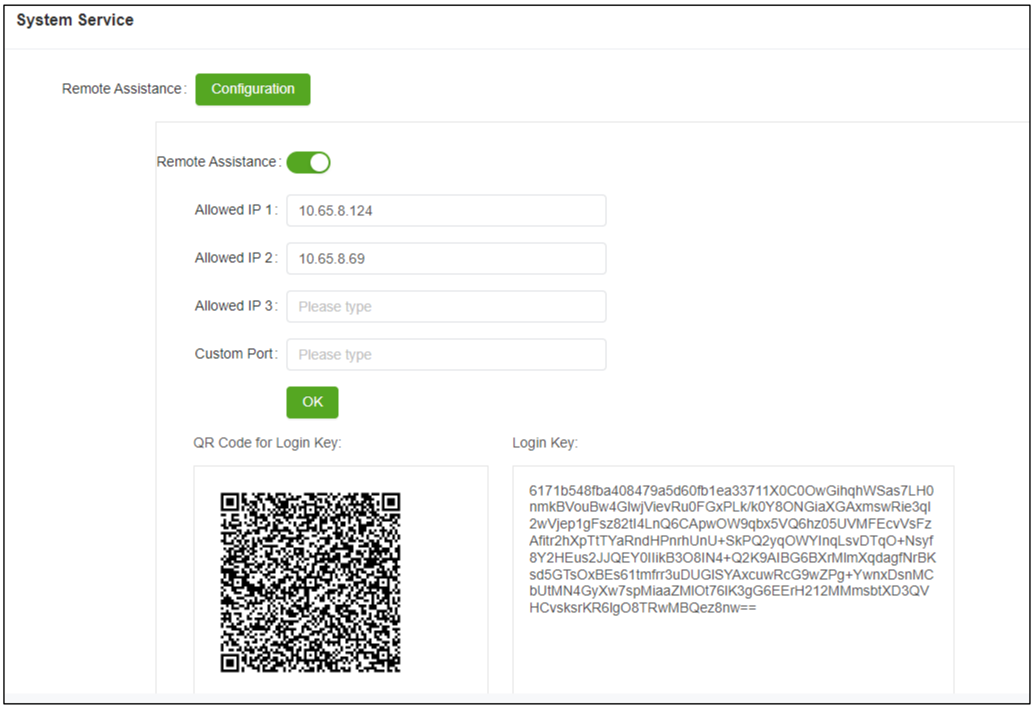
With the system service function, you can conveniently configure remote assistance, expert diagnosis, DNS cache, diagnosis log debug mode, diagnosis log download, and network packet capture parameters.

10.3.3.1 Configuring Remote Assistance

When a failure occurs in the system, you may need to contact NSFOCUS technical support for remote assistance. The technical support personnel of NSFOCUS can remotely log in to RSAS via SSH for troubleshooting.

After the Special Parameters function is enabled, choose **Administration** > **Service** > **System Service**. Click **Configuration** next to **Remote Assistance** to enable remote assistance and configure allowed IPv4 addresses. Then the login key used by the specified IP address for remote access to RSAS and its QR code are displayed below, as shown in Figure 10-2.

Figure 10-2 Remote assistance



System Service

Remote Assistance: Configuration

Remote Assistance: ●

Allowed IP 1: 10.65.8.124

Allowed IP 2: 10.65.8.69

Allowed IP 3: Please type

Custom Port: Please type

OK

QR Code for Login Key:

Login Key:

```
6171b548fba408479a5d60fb1ea33711X0C0OwGihqhWSas7LH0
nmkBVouBw4GlwjVievRu0FGxPLk/k0Y8ONGiaXGAxmswRie3ql
2wVjep1gFsz82tl4LnQ6CApwOW9qbx5VQ6hz05UVMFEcvVsFz
Afitr2hXpTtTYaRndHPnrhUnU+SkPQ2yqOWYlnqLsvDTqO+Nsyf
8Y2HEus2JJQEY0IlikB3O8IN4+Q2K9AIBG6BXrMlmXqdagfNrBK
sd5GTsOxBEs61tmfrr3uDUGISYAxcuwRcG9wZPg+YwnxDsnMC
bUtMN4GyXw7spMiaaZMlOt76lK3gG6EErH212MMmsbtXD3QV
HCvsksrKR6lgO8TRwMBQez8nw==
```

10.3.3.2 Configuring Expert Diagnosis

When RSAS is faulty and requires remote assistance, technical support personnel of NSFOCUS can remotely log in to RSAS via SSH for troubleshooting.

Choose **Administration** > **Service** > **System Service** and enable or disable expert diagnosis.

- Expert diagnosis is available only when RSAS can access the Internet.
  - If the faulty device can access the SSH server, the device will map its own SSH port to the SSH server.
  - If the faulty device cannot access the SSH server, but a host that is reachable from the device can access the SSH server, run **PortGo.exe** on this host and complete related settings. After that, the SSH port on the device can be mapped to the SSH server.
- If the faulty device cannot access the Internet, the expert diagnosis function is unavailable.

Note

PortGo.exe is provided and used by field engineers. Therefore, it is not delivered with RSAS.

A host for technical support can connect to multiple RSAS devices mapping to SSH clients, but multiple hosts for technical support cannot connect to such an RSAS device at the same time.

10.3.3.3 Configuring DNS Cache

The DNS cache is provided to improve the web scanning performance of RSAS. Specifically, the IP addresses corresponding to scanned domain names are saved in a local disk drive. The cache refreshes every 15 minutes. By default, this function is disabled.

Choose **Administration** > **Service** > **System Service** and enable or disable the DNS cache.

10.3.3.4 Configuring Diagnosis Log Debug Mode

By default, the system records diagnosis logs at the INFO level and above. After the diagnosis log debug mode is enabled, the system records diagnosis logs at the Debug level and above.

Choose **Administration** > **Service** > **System Service** and enable or disable the diagnosis log debug mode.

10.3.3.5 Downloading Diagnosis Logs

After an RSAS device becomes faulty, you can download fault diagnosis logs and then send them to technical support personnel of NSFOCUS for troubleshooting.

Choose **Administration** > **Service** > **System Service**. For **Diagnosis Log**, select the logs and click **Download Log** to save them to a local disk drive.

10.3.3.6 Capturing Packets

RSAS can capture packets on network interfaces for analysis and debugging.

After the Special Parameters function is enabled, choose **Administration** > **Service** > **System Service** and navigate to **Network Packet Capture**.

- Click **Start Capture** to enable RSAS to capture packets.

  RSAS will capture packets that pass all network interfaces that are enabled.
- Click **Stop Capture** to stop packet capture.

  RSAS can capture a maximum of 1 million packets each time. If you do not stop capturing packets when the maximum is reached, RSAS will stop the capture automatically.
- Click the packet capture file displayed below to download the captured packets.

10.4 Users

Permissions

Initially, the system only provides the default system administrator **admin** and audit administrator **auditor**. For information about the two accounts, see Default Parameters. Administrators fall into system administrators and common administrators. The default system administrator **admin** can create both types of administrators. Table 10-18 describes administrator permissions.

Table 10-18 Administrator permissions

Role	Permissions
admin	Has permissions except for log management.
auditor	By default, the audit administrator **auditor** is disabled and can be enabled only by **admin**. Once enabled, **auditor** should change his or her login password and cannot be disabled. **auditor** has the following permissions: • Manages logs. • Views and modifies his or her own information. • Imports and exports a license.
Custom system administrators (can be created only by **admin**)	• Have permissions assigned by **admin**. If **admin** does not assign permissions to custom system administrators, they, by default, have all permissions except for dashboard configuration and system management (user management) and log management. • View and modify their own information.
Common administrators (can be created only by **admin**)	• Have permissions assigned by **admin**. If **admin** does not assign permissions to common administrators, they, by default, have permissions of system status and common tools, and other permissions than system management, collaboration management, log management, and dashboard configuration. • View and modify their own information.

Creating an Account

Choose **Administration > User**. The **Administrator List** page appears. Click **Add** and configure administrator parameters as described in Table 10-19. The new administrator account is enabled by default. Table 10-20 describes operations that are allowed for an administrator account.

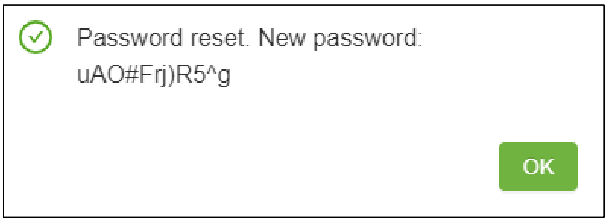
Table 10-19 Parameters for creating an administrator

Parameter	Description
User Name	Specifies the user name to be typed on the login page for access to RSAS. It is a string of no more than 20 characters and must start with a letter followed by letters, digits, and/or underscores.
Administrator Name	Specifies the name of the new administrator. It cannot contain more than 20 characters.
Password	Specifies the password typed on the login page for access to RSAS. For password security settings, see Password Policy.
Confirm Password	Requires you to type the password again for confirmation.
Email Address	Email address of the new administrator.
Role	User role of the new administrator. Two roles are available: **System administrator** and **Common administrator**.
Permissions	Grants permissions to the new administrator. You can select permissions from the drop-down list.

Parameter	Description
	Note • If **Role** is set to **System administrator**, the new administrator has configuration permissions of all modules. • If **Role** is set to **Common administrator**, the new administrator has certain permissions (authentication, system status, and common tools) by default. You can assign other permissions (asset management, data interface, and license management) as required.
Accessible IP Range	Specifies the IP addresses or address ranges that are allowed for login. *.*.*.* indicates any IP addresses. Both IPv4 and IPv6 addresses are allowed. Multiple IP addresses or IP address ranges should be separated by the comma (,), semicolon (;), carriage return, or space. An IP address preceded by an exclamation (!) is excluded from access to RSAS. • IPv4 addresses or address ranges can be typed as follows: 192.168.1.1 192.168.1.1–254 192.168-1/24 192.168.1.* 192.168.1–10.* !192.168.1.1 • IPv6 addresses or address ranges can be typed as follows: 2001::db8:2003 2001::db8:2003/96 !2001::db8:2003
Scannable IP Range	Specifies IP addresses or address ranges that the new administrator can take as scan targets. Requirements for typing IP addresses and IP address ranges here are the same as those for **Accessible IP Range**.
Account Validity Period	Specifies the validity period of the account. After the validity period expires, this administrator account will be invalid. The value range is 0–1000, in days. The default value is **0**, indicating no limit.

Table 10-20 Allowed operations on administrator accounts

Operation	Description
Enables/Disable	Click **Enable** or **Disable** in the **Operation** column of an administrator account to change its status.
Edit	Any administrator can manage his or her own information by clicking the user name in the quick access bar. **admin** can manage the information of **admin**, custom system administrators, and common administrators.
Delete	Only **admin** can delete an administrator account.
Reset Password	Only **admin** can reset the password for an administrator account. After you confirm to reset the password, RSAS randomly generates a new password, which cannot be queried later. Therefore, **admin** needs to manually copy the

Operation	Description
	password and notify the user.  Password reset. New password: uAO#Frj)R5^g

10.5 Common Tools

RSAS provides common tools for device diagnosis and troubleshooting. This section describes how to use these tools.

Choose **Administration > Common Tools**. You can use the following tools to check the connection status of the current network and the NIC status.

10.5.1 Ping

The **ping** command checks the operating status of the target device or the status of the connections between RSAS and other devices on the network. The command output facilitates network fault analysis and troubleshooting. Type the IPv4 address, IPv6 address, or host name of the target device in the text box and click **Ping**. Then the command output appears.

During the command execution, you can click ⊘ to stop running this command. In addition, you can turn on the **Scroll** switch to scroll through the command output.

10.5.2 Traceroute

The **Traceroute** command checks the number of routes between RSAS and the target IP address. Type the IPv4 address, IPv6 address, or host name of the target device in the text box and click **Traceroute**. Then the command output appears.

During the command execution, you can click ⊘ to stop running this command. In addition, you can turn on the **Scroll** switch to scroll through the command output.

10.5.3 Dig

As a part of the Bind suite (official website: http://www.isc.org), the **dig** command collects information from DNS servers for fault diagnosis. Type the IPv4 address, IPv6 address, or host name of a DNS server in the text box and click **Dig**. Then the command output appears.

During the command execution, you can click ⊘ to stop running this command. In addition, you can turn on the **Scroll** switch to scroll through the command output.

10.5.4 Nmap

Nmap (Network Mapper) is a port scanner used for network scanning and sniffing in the Linux environment. It provides three functions:

- Checking whether the host is online

- Scanning host ports to discover network services on such ports
- Determining the operating system running on the scanned hosts

Type the IPv4 address, IPv6 address, or name of a target host in the text box and click **Nmap**. Then the command output appears.

During the command execution, you can click ⊘ to stop running this command. In addition, you can enable the **Scroll** switch to scroll through the command output.

10.5.5 Telnet

Telnet is a standard protocol and a major way for remote login through the Internet. Here, it is mainly used for remote management of RSAS. Configure the host, port (**23** by default), user name, password, and command and then click **Execute**. If the user name and password are correctly typed, the command output is displayed.

During the command execution, you can click ⊘ to stop running this command. In addition, you can turn on the **Scroll** switch to scroll through the command output.

10.5.6 SSH

SSH here is used for remote management of RSAS. Configure the host, port (**22** by default), user name, password, and command and then click **Execute**. If the user name and password are correctly typed, the command output is displayed.

During the command execution, you can click ⊘ to stop running this command. In addition, you can turn on the **Scroll** switch to scroll through the command output.

10.5.7 Route Information

The route information here indicates the real-time route information of RSAS.

10.5.8 Curl

Curl an open-source command line tool and library for transferring data with URL syntax. It supports such protocols as FTP, FTPS, HTTP, and HTTPS. Currently, RSAS only allows users to use Curl 7.15.1 to obtain website information.

Type the URL (for the format specification, see the description on the UI) of the target website in the text box and click **Curl**. Then the command output appears.

During the command execution, you can click ⊘ to stop running this command. In addition, you can turn on the **Scroll** switch to scroll through the command output.

11 Collaboration Management

This chapter contains the following sections:

Section	Description
Security Center	Describes how to configure the collaboration between RSAS and security cnters.
Agent Management	Describes how to configure the collaboration between RSAS and an agent.

11.1 Security Center

RSAS can connect to NSFOCUS Enterprise Security Planning Customer V6 (ESPC V6), Threat and Vulnerability Management (TVM) Platform, NSFOCUS Intelligent Security Operations (ISOP) Platform, and NSFOCUS Cloud Security System (NCSS) for collaboration with these platforms. To ensure that the management platform is properly connected to RSAS, you must configure required parameters on both RSAS and the management platform. Here, only the collaboration configuration on RSAS is described. For collaboration settings on the management platforms, see their respective user guides.

Configuring Collaboration with ESPC V6

RSAS can connect to NSFOCUS ESPC V6, which is a centralized management platform for NSFOCUS products. The following features of NSFOCUS ESPC greatly improve the management efficiency:

- Unified monitoring of multiple products
- Configuration of tasks in a centralized manner
- Comprehensive management of reports

Choose **Collaboration** > **Security Center**. Configure the collaboration parameters with ESPC V6 as described in Table 11-1.

Note	Before RSAS is detected by ESPC and added to the latter, the status is displayed as **Connecting**. If collaboration with another device has been configured, when configuring collaboration with ESPC V6, you need to first disable the current collaboration, click **OK**, and then configure the collaboration parameters.

Table 11-1 Collaboration with ESPC V6

Type	Parameter	Description
Basic Configuration	Local IP	Specifies the IP address of RSAS for communication with ESPC V6.
	IP/Port	Specifies the IP address and port number of ESPC for communication with RSAS. Select **ESPC V6** for **Version**, and then enable the function.
Advanced Settings (When the connection to ESPC V6 requires authentication you need to expand **Advanced Options**).	NSFOCUS Enterprise Security Planning Customer (ESPC)	• If you set **Mode** to **SSL** or **TCP**, you can use the default port. If you want to use a different port, ensure that the port you set is the same as the one set on ESPC. • If you set **Mode** to **AES**, you need to ensure that this mode is also enabled on ESPC that connects to RSAS.

Configuring Collaboration with TVM/ ISOP

RSAS can collaborate with TVM and ISOP.

- TVM provides unified measurement, analysis, and management of the security factors of internal vulnerabilities and external threats, which can effectively defend against the changing security vulnerabilities.
- As an all-scenario intelligent security operations platform for traditional IT security, ISOP fully monitors security situations with real-time security threat alerts, and offers full lifecycle management on assets and vulnerabilities, and automated emergency response for security.

Choose **Collaboration** > **Security Center**. Configure the collaboration parameters with TVM/ISOP, as described in Table 11-2.

Note

Before RSAS is detected by TVM/ISOP and added to the latter, the status is displayed as **Connecting**.

If collaboration with another device has been configured, when configuring collaboration with TVM or ISOP, you need to first disable the current collaboration, click **OK**, and then configure the collaboration parameters.

Table 11-2 Parameters for collaboration with TVM and ISOP

Type	Parameter	Description
Basic Configuration	Local IP	Specifies the IP address of RSAS for communication with TVM or ISOP.
	IP/Port	Specifies the IP address and port number (**443** by default) of TVM or ISOP for communication with RSAS. Select **TVM/ISOP** for **Version**, and then enable the function.

Configuring Collaboration with WebSafe

RSAS can collaborate with WebSafe. WebSafe provides security event monitoring and vulnerability scanning services such as web defacement and web page trojans. It can accurately defend against known and unknown attacks, effectively protecting customers' website applications.

Choose **Collaboration** > **Security Center**. Configure the collaboration parameters with WebSafe, as described in Table 11-3.

Note

Before RSAS is detected by WebSafe and added to the latter, the status is displayed as **Connecting**.

If collaboration with another device has been configured, when configuring collaboration with WebSafe, you need to first disable the current collaboration, click **OK**, and then configure the collaboration parameters.

Table 11-3 Parameters for configuring collaboration with WebSafe

Type	Parameter	Description
Basic Configuration	Local IP	Specifies the IP address of RSAS for communication with WebSafe.
	IP/Port	Specifies the IP address and port number (**443** by default) of WebSafe for communication with RSAS. Select **WebSafe** for **Version**, and then enable the function.

Configuring Collaboration with NCSS

RSAS can collaborate with NCSS. As an abstracted security service in the resource pool of NCSS, RSAS can be combined with other services and published. Also, you can monitor RSAS and view its alerts on NCSS in a centralized manner.

Choose **Collaboration** > **Security Center**. Configure the collaboration parameters with NCSS, as described in Table 11-4.

Note

Before RSAS is detected by NCSS and added to the latter, the status is displayed as **Connecting**.

If collaboration with another device has been configured, when configuring collaboration with NCSS, you need to first disable the current collaboration, click **OK**, and then configure the collaboration parameters.

Table 11-4 Parameters for configuring collaboration with NCSS

Type	Parameter	Description
Basic Configuration	URL/IP	Specifies the domain name and IP address of NCSS for communication with RSAS. Then enable this function.

11.2 Agent Management

After an agent is installed on a target host, the agent communicates with RSAS or the platform by using heartbeats and reports specific information about the target host every four hours for vulnerability scanning of RSAS or the platform.

11.2.1 Collaboration Process

Table 11-5 shows the configuration process for collaboration with an agent.

Table 11-5 Collaboration with an agent

Solution Scenario	Standalone Scenario
1. Select **Platform** for **Collaboration Solution**. The **Agent List** and **Agent Download** tabs are unavailable on RSAS. 2. Log in to the platform to download and manage the agent. 3. Create an assessment task. For details, see Assessment Task.	1. Select **Stand-alone** for **Collaboration Solution**. The **Agent List** and **Agent Download** tabs are available on RSAS. 2. Download an agent on the **Agent Download** tab. 3. Manage the agent on the **Agent List** tab. 4. Create an assessment task. For details, see Assessment Task.

11.2.2 Configuring an Collaboration Solution

Choose **Collaboration** > **Agent** > **Collaboration Solution**. Select a scenario for collaboration between RSAS and the agent.

- **Platform**: The agent is managed on the platform. RSAS obtains agent data for scanning via an interface to the platform.
- **Stand-alone**: The agent is directly managed on RSAS. After dangling, RSAS obtains and manages agent data for scanning.

11.2.3 Downloading Agent Software

After an agent is downloaded and installed on a target host, it registers with RSAS through real-time heartbeat communication. After the registration is complete, the agent reports data of the target host to RSAS every four hours.

Downloading Agent Software

Choose **Collaboration** > **Agent** > **Agent Download**. Select the agent software that matches the operating system on the target host, and click **Download**.

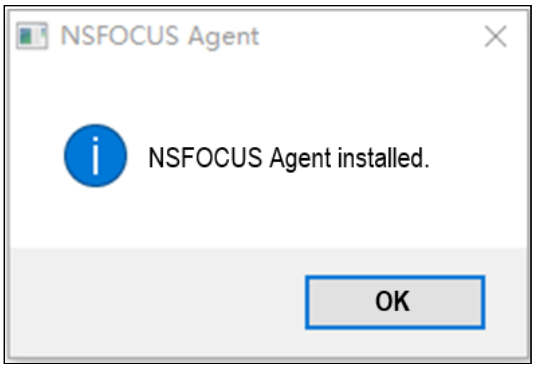
Installing/Uninstalling NSFOCUS Agent for Windows

Installation

For Windows, install NSFOCUS Agent as follows:

Double-click NSFOCUS Agent installation package to start the installation. If the agent is successfully installed, a message is prompted to indicate the success, as shown in the following figure. If the installation failed, an error message is prompted with an error code.

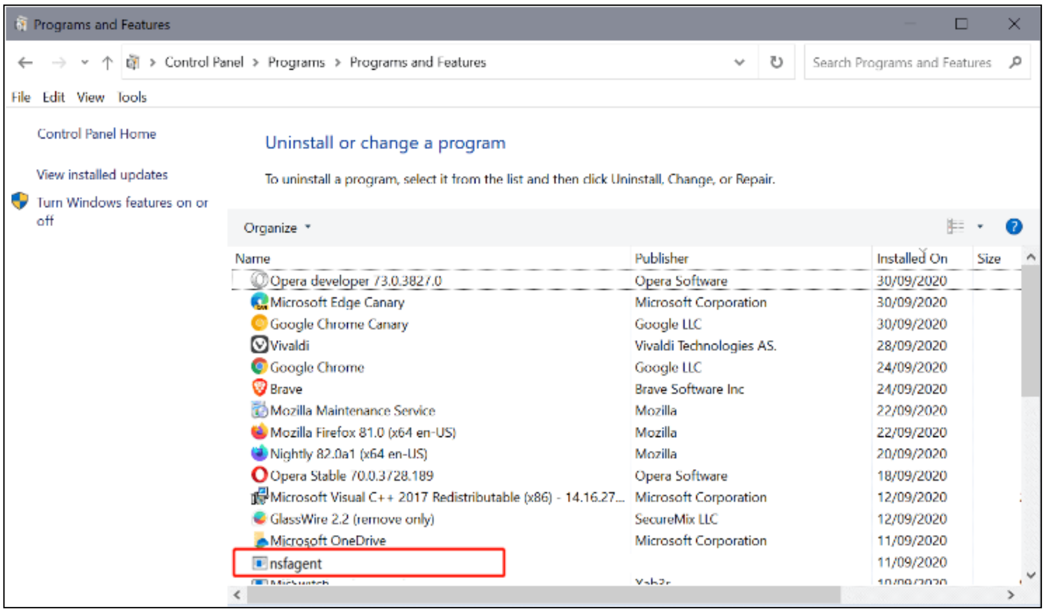
Figure 11-1 Successful installation



NSFOCUS Agent installed.

After NSFOCUS Agent is successfully installed, it is listed under **Control Panel > Programs > Programs and Features** with the name of **nsfagent**, as shown in the following figure.

Figure 11-2 Query result


Programs and Features
Control Panel > Programs > Programs and Features
Search Programs and Features
File Edit View Tools
Control Panel Home
View installed updates
Turn Windows features on or off
Organize

Uninstall or change a program

To uninstall a program, select it from the list and then click Uninstall, Change, or Repair.

Name	Publisher	Installed On	Size
Opera developer 73.0.3827.0	Opera Software	30/09/2020	
Microsoft Edge Canary	Microsoft Corporation	30/09/2020	
Google Chrome Canary	Google LLC	30/09/2020	
Vivaldi	Vivaldi Technologies AS.	28/09/2020	
Google Chrome	Google LLC	24/09/2020	
Brave	Brave Software Inc	24/09/2020	
Mozilla Maintenance Service	Mozilla	22/09/2020	
Mozilla Firefox 81.0 (x64 en-US)	Mozilla	22/09/2020	
Nightly 82.0a1 (x64 en-US)	Mozilla	20/09/2020	
Opera Stable 70.0.3728.189	Opera Software	18/09/2020	
Microsoft Visual C++ 2017 Redistributable (x86) - 14.16.27...	Microsoft Corporation	12/09/2020	
GlassWire 2.2 (remove only)	SecureMix LLC	12/09/2020	
Microsoft OneDrive	Microsoft Corporation	11/09/2020	
nsfagent		11/09/2020	

Uninstallation

Choose **Control Panel > Programs > Programs and Features**, click the agent name, and then click **Uninstall**.

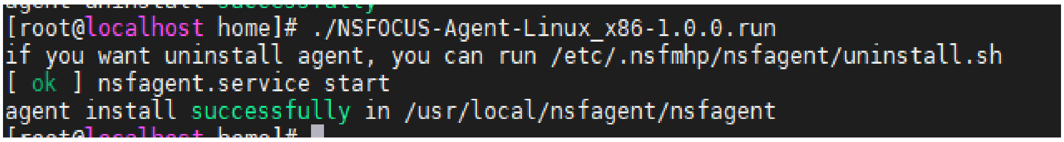
Installing/Uninstalling NSFOCUS Agent for Linux

Installation

For Linux, install NSFOCUS Agent as follows:

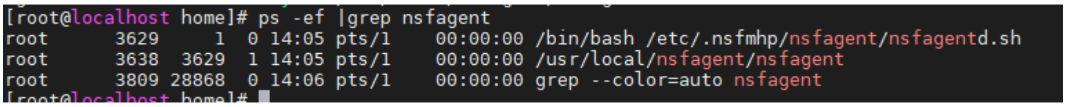
Navigate to the directory where the installation package is and run the following commands to install NSFOCUS Agent:

```
chmod +x NSFOCUS-Agent-Linux_x86-1.0.0.run              # Grants the permission.
./NSFOCUS-Agent-Linux_x86-1.0.0.run                     # Installs the agent.
```



```
[root@localhost home]# ./NSFOCUS-Agent-Linux_x86-1.0.0.run
if you want uninstall agent, you can run /etc/.nsfmhp/nsfagent/uninstall.sh
[ ok ] nsfagent.service start
agent install successfully in /usr/local/nsfagent/nsfagent
```

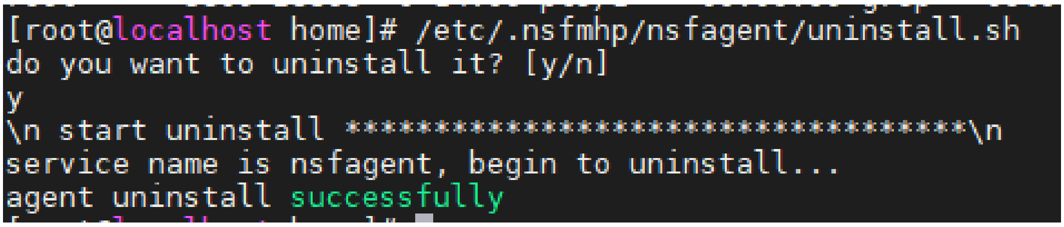
After NSFOCUS Agent is successfully installed, it appears in the **/usr/local/nsfagent/** directory.



```
[root@localhost home]# ps -ef |grep nsfagent
root      3629     1  0 14:05 pts/1    00:00:00 /bin/bash /etc/.nsfmhp/nsfagent/nsfagentd.sh
root      3638  3629  1 14:05 pts/1    00:00:00 /usr/local/nsfagent/nsfagent
root      3809 28868  0 14:06 pts/1    00:00:00 grep --color=auto nsfagent
```

Uninstallation

Run the **/etc/.nsfmhp/nsfagent/uninstall.sh** command to uninstall NSFOCUS Agent.



```
[root@localhost home]# /etc/.nsfmhp/nsfagent/uninstall.sh
do you want to uninstall it? [y/n]
y
\n start uninstall ************************************\n
service name is nsfagent, begin to uninstall...
agent uninstall successfully
```

11.2.4 Agent List

The agent downloaded is bound to RSAS's IP address. After being installed on a target host, the agent automatically sends a heartbeat message to RSAS's IP address for registration. After the registration is complete, you can view information about the target host on the **Agent List** page.

Viewing Agent Status

Choose **Collaboration** > **Agent** > **Agent List** to view the agent status.

- **Authorized**: maximum number of agents that can be managed by RSAS, which is the same as **Authorized Agents for Full Scan** shown on the License Status page.
- **Registered**: total number of agents registered.

- **Online**: total number of agents that are both registered and online.
- The online number is no greater than the registered number, and the registered number is no greater than the authorized number.

Managing a Registerable IP Range

If a registrable IP range is configured, only a new target with an agent installed in the IP range can be displayed on the **Agent List** page when the registered number is smaller than the number authorized by RSAS. An agent that is registered before the registrable IP range is configured but is not in the registrable IP range will become offline within a few minutes.

Choose **Collaboration** > **Agent** > **Agent List**. Click **Registrable IP** to specify an IP address range in which the target host can be registered. For details about the format, see the description on the UI. The symbol * indicates any IP address range.

Managing Agents

Choose **Collaboration** > **Agent** > **Agent List**. You can query and filter agents by status, and perform the following operations on agents:

- Click **Risk report** in the **Operation** column of a target host to view its last scan results if RSAS has executed a vulnerability or configuration scanning task on the target host installed with the agent.
- You can delete agents one by one or in batches. After the deletion, either of the following situations occurs:
  - The host within the registrable IP address range will be redisplayed in the list in a few minutes.
  - The host outside the registrable IP address range will no longer be redisplayed in the list.

12 Log Management

Only the audit administrator **auditor** has log management permissions. RSAS supports strict auditing on administrators' operations via management of logs, including login logs, operation logs, exception logs, and upgrade logs.

This chapter contains the following sections:

Section	Description
Log Audit	Describes how **auditor** queries, backs up, and clears logs.
Log Configuration	Describes how **auditor** configures log thresholds and backup methods.

12.1 Log Audit

Log Query

Choose **Logs** > **Log Audit**. You can filter logs according to specified query conditions. The auditor can obtain RSAS information by querying the following logs:

- Login log

  The login log records administrators' login (success and failure) and logout events, thereby enabling the auditor to detect unauthorized access in time.
- Operation log

  The operation log records administrators' operations such as license management, network configuration, and user management.
- Exception log

  The exception log records system exceptions such as network disconnection, engine exception, unexpected system restart, and other exceptions that cause the system to operate improperly. This type of logs helps locate system errors.
- Upgrade log

  The upgrade log records the system version and upgrade events.

Backing Up Logs

RSAS supports manual log backup. The auditor can back up all types of logs in the .txt format to a local computer, making it convenient to view logs and analyze system operating conditions.

Choose **Logs > Log Audit**. Click **Back Up** to set backup options, as described in Table 12-1.

Table 12-1 Log backup parameters

Parameter	Description
Backup Range	Specifies the scope of logs to be backed up. • **All logs**: backs up all logs. • **Current logs**: backs up logs that meet query conditions.
Post-Backup Handling	Specifies whether to delete logs that have been backed up. • **Delete**: deletes logs that are already backed up. • **Retain**: retains logs that are already backed up.

Clearing Logs

Choose **Logs > Log Audit**. Clicking **Clear** will delete all logs.

Note	A log is generated to record your log clearing operation.

12.2 Log Configuration

The auditor can configure the log backup method and backup thresholds.

Configuring Log Backup Thresholds

Backup thresholds are used to determine when to back up logs. When the specified cycle or log count is reached, the system will automatically back up logs or inform the auditor of manual backup. This section describes how to configure backup thresholds. For the backup method configuration, see Configuring Backup Methods.

Choose **Logs > Log Configuration**. Under **Backup Thresholds**, configure parameters, as described in Table 12-2.

Table 12-2 Log backup thresholds

Parameter	Description
Backup Cycle (days)	The system automatically backs up logs according to the specified cycle. The backup cycle range is 1–365 in days, with **30** as the default.
Log Count	If the number of logs reaches the specified threshold, the system automatically backs up logs and clears them after backup. The threshold range is 5000–50000, with **5000** as the default.

Configuring Backup Methods

The hard disk of RSAS can be used to save a certain number of logs. To avoid the usage of too much disk space, you can back up logs to a local disk drive or a dedicated FTP server.

Choose **Logs > Log Configuration**. Under **Backup Method**, configure parameters, as described in Table 12-3.

Table 12-3 Log backup parameters

Backup Method	**Parameter**	**Description**
Manual Backup	Manual backup	The auditor can manually back up logs only to the local computer through which RSAS is accessed. When the specified log thresholds are approached or reached, the system asks the auditor to back up logs manually.
Automatic Backup	Auto backup	In automatic backup mode, when backup conditions are met, the system automatically backs up logs to the specified FTP server and deletes logs under **Logs >Log Audit**. After automatic backup, the system will generate two audit logs: an automatic backup log and a clearing log.
	FTP Server IP	Specifies the IP address of the FTP server for log backup. Either an IPv4 or IPv6 address is allowed.
	FTP Server Encoding	Specifies the encoding format used by the FTP server, which can be **GBK**, **GB18030**, **UTF-8**, or **GB2312**.
	FTP File Path	Specifies the directory of the FTP server for saving logs. If the root directory is used to save logs, set the path to /.
	FTP Login User Name	User name used for login to the FTP server. This account must have the read-write permission.
	FTP Login Password	Password used for login to the FTP server.

13 Alert Management

To facilitate closed-loop management of scanning tasks, RSAS generates alerts for identified asset risks, including vulnerabilities, noncompliant configuration items, illegitimate processes, and weak system accounts.

Alert Configuration

After you set the alert parameters, the system, during scanning, generates alerts for risks that match such conditions.

Choose **Alert**, click **Configuration**, and set alert parameters. Table 13-1 describes the alert parameters.

Table 13-1 Alert parameters

Function	Parameter	Description
Alert Method	Alert Method	• **Pop-up message**: indicates that an alert message is displayed after the alert is triggered. • **Email alert**: indicates that an alert message is sent to the specified email address after the alert is triggered. By default, alerts are not sent by email. If you select **Email alert** and the asset is registered, the alert message will be sent to the asset administrator's email address; if the asset is not registered, the alert message will be sent to the node administrator's email address.
Alert Conditions	Vulnerability Alert Level	Specifies the level of system vulnerabilities for which RSAS will generate alerts.
	Web Vulnerability Alert Level	Specifies the level of configuration risks for which RSAS will generate alerts.
	Configuration Alert For	Specifies the types of configuration risks for which RSAS will generate alerts.
	Status Alert For	Specifies the types of status-related risks for which RSAS will generate alerts.
	Weak Password Alert	• **Yes**: indicates that RSAS generates alerts on weak passwords. • **No**: indicates that RSAS does not generate alerts on weak passwords.
Alert Object	Specify IP range	Specifies the IP address range of the alert object. Multiple IP addresses or address ranges should be separated by the comma (,), semicolon (;),

Function	Parameter	Description
(Data Source)		carriage return, or space. If an IP address or IP address range is preceded with an exclamation mark (!), it indicates that alerts will not be generated for this IP address or IP address range.
	Select from asset tree	Indicates that the asset is selected from the asset tree.

Alert Statistics

Choose **Alert** to view the overall alert statistics, as described in Table 13-2. This page presents data from the risk list of the alert platform, namely, data that triggered alerts as specified in Alert Configuration.

Table 13-2 Alert statistics

Item	Description
Total risks	Displays the total number of new and confirmed alerts and the number of alerts at each level (high, medium, and low).
Affected components	Displays the total number of risky components and the numbers of various components.
Affected assets	Displays the total number of the risky assets and the numbers of various assets.

Alert Handling

After receiving alerts, you can view alert details, and track and get involved in alert handling.

Choose **Alert**. Select alerts and click **Bulk Change Status** above the list or **Change Risk Status** in the **Operation** column to handle alerts and verify the handling results, as described in Table 13-3.

Table 13-3 Change the risk status

Risk Status	Description
New	Indicates that the alerted risk has not been processed.
Confirmed	Indicates that the alerted risk really exists.
False positive	Indicates that the alert is a false positive as confirmed by the asset administrator.
Ignored	Indicates that the alert is ignored. The ignored alerts will be deleted from the alert list. If the alert configuration conditions are not modified, such an alert will be generated again during the next scanning task.
Fixed	Indicates that the confirmed risk has been fixed by the asset administrator.
Corrected	Indicates that alert has been confirmed to be a false positive and the risk status is set to **Corrected**.
Correction	Dispatches a correction task for a risk whose **Risk Status** is displayed as **Fixed** or **Corrected**

Risk Status	**Description**
Task	to check whether the risk persists.

A Console-based Management

With serial connections, you can access the RSAS console to perform functions such as the initial configuration, status detection, and initialization restoration, which are unavailable on the web-based manager.

Section	Description
Login	Describes how to log in to the console.
Functions	Describes functions available on the console.

A.1 Login

Preparations

Before logging in to the console, prepare the following:

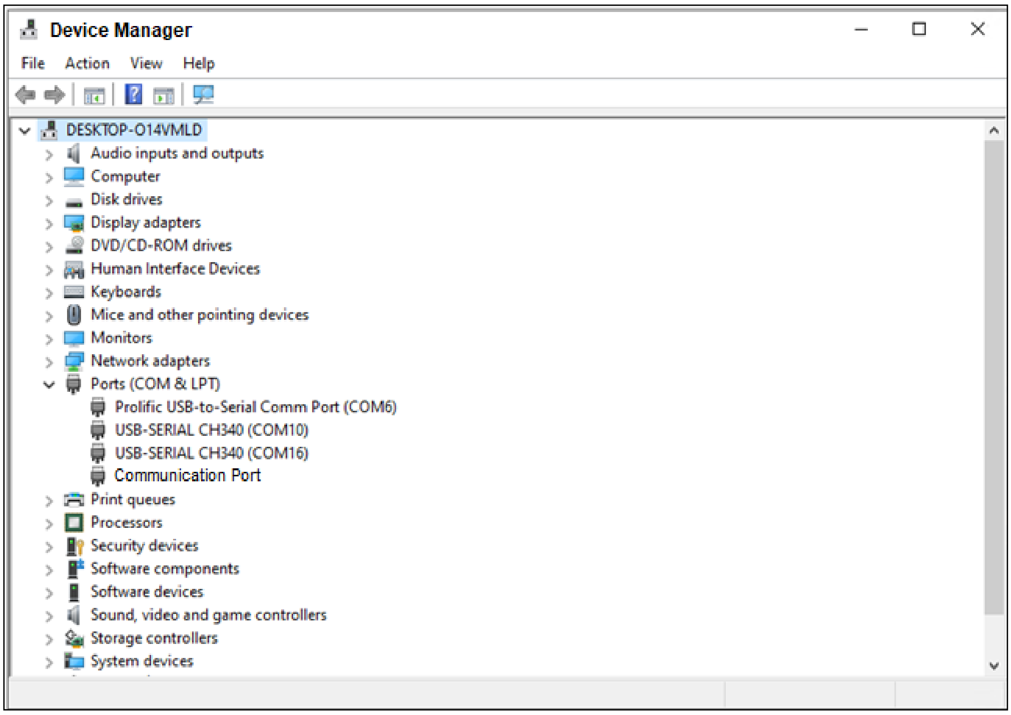
- One PC, on which terminal software, such as PuTTY, has been installed and can connect to the console.
- One serial cable (included in the accessory kit), with one end connecting to the device and the other to the serial port of the PC.
- Communication parameters, user name, and password (see Default Parameters).

Procedure

The following uses PuTTY as an example to describe how to log in to the console user interface.

Step 1 On the desktop of the PC, right-click **Computer/This Computer** and select **Properties** from the shortcut menu to open the device manager and view the serial port of the current machine.

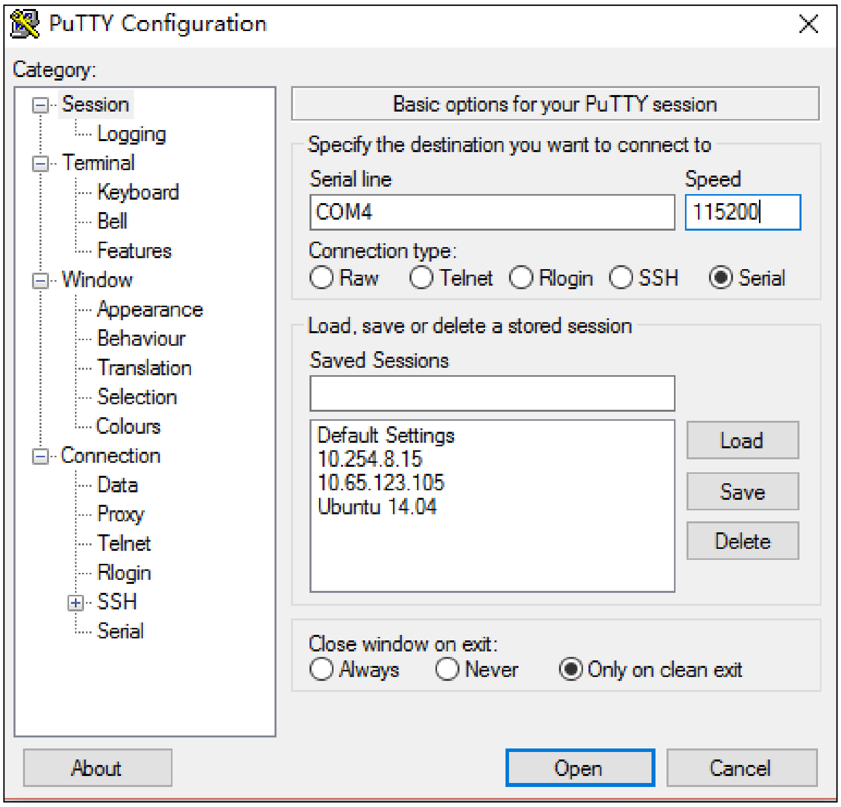
Figure A-1 Device manager



- DESKTOP-O14VMLD
  - Audio inputs and outputs
  - Computer
  - Disk drives
  - Display adapters
  - DVD/CD-ROM drives
  - Human Interface Devices
  - Keyboards
  - Mice and other pointing devices
  - Monitors
  - Network adapters
  - Ports (COM & LPT)
    - Prolific USB-to-Serial Comm Port (COM6)
    - USB-SERIAL CH340 (COM10)
    - USB-SERIAL CH340 (COM16)
    - Communication Port
  - Print queues
  - Processors
  - Security devices
  - Software components
  - Software devices
  - Sound, video and game controllers
  - Storage controllers
  - System devices

Step 2 Open PuTTY, configure connection properties of the serial port, and click **Open**.

Figure A-2 Selecting a port for connection



PuTTY Configuration

Category:

Basic options for your PuTTY session

Specify the destination you want to connect to

Serial line: COM4

Speed: 115200

Connection type: ○ Raw ○ Telnet ○ Rlogin ○ SSH ● Serial

Load, save or delete a stored session

Saved Sessions

Default Settings
10.254.8.15
10.65.123.105
Ubuntu 14.04

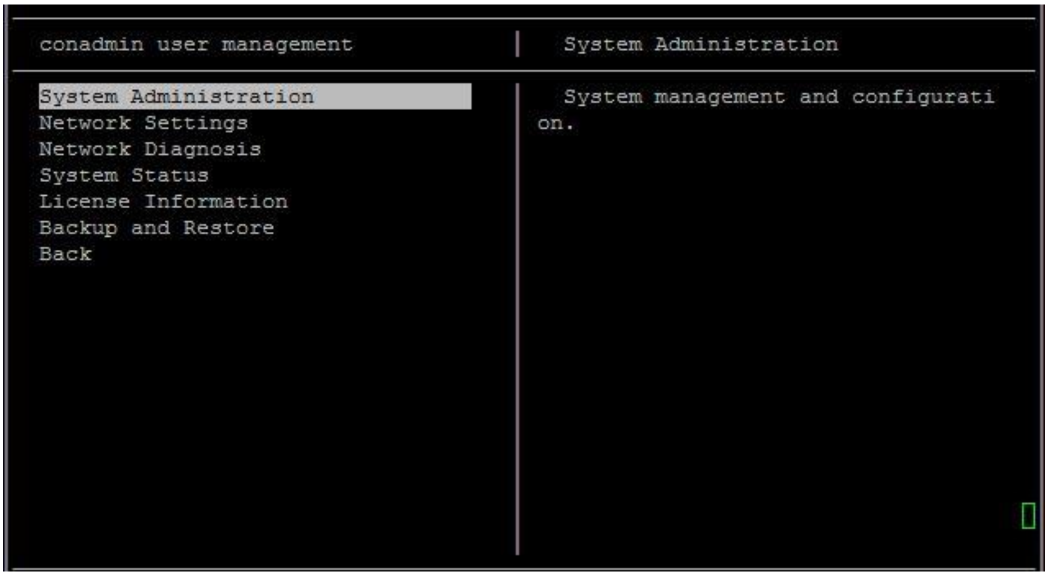
Close window on exit: ○ Always ○ Never ● Only on clean exit

Table A-1 Connection parameters of the serial port

Parameter	Value
Serial line	Specifies a COM port according to your computer system. For how to find out the serial port of the current computer, see Step 1.
Speed	Specifies the connection rate, which should be **115200** (bits per second).
Connection type	Specifies a connection type, which should be **Serial** here.

Step 3 Type the initial user name and password (both are **conadmin**) of the console administrator to log in to the console user interface.

Figure A-3 Console user interface



```
conadmin user management                | System Administration

System Administration                   |  System management and configurati
Network Settings                        | on.
Network Diagnosis
System Status
License Information
Backup and Restore
Back
```

----End

Meanings of Frequently Used Keys

On the console user interface, you can only perform operations with the keyboard. Table A-2 describes meanings of the frequently used keys.

Table A-2 Meanings of frequently used keys

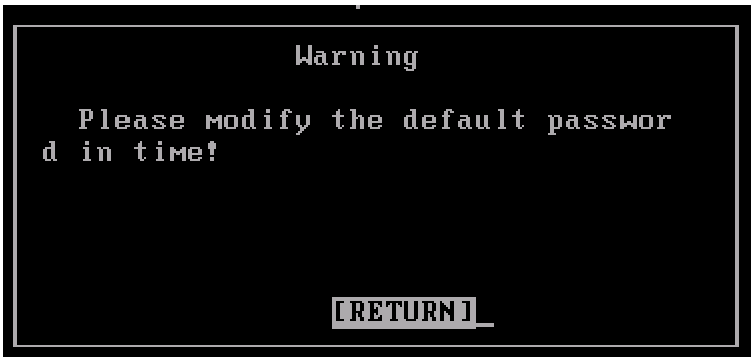
Keyboard	Meaning
↑	Moves up.
↓	Moves down.
←	Moves left.
→	Moves right.
ESC	Cancels an operation.
Enter	Confirms an operation.
Tab	Switches between the input box, **OK**, and **Cancel**.
Backspace	Deletes the character to the left of the cursor.

A.2 Functions

This section describes main functions available on the console.

On your first login as **conadmin**, change the initial login password. Otherwise, the system reminds you every time you log in.

Figure A-4 Password change reminder

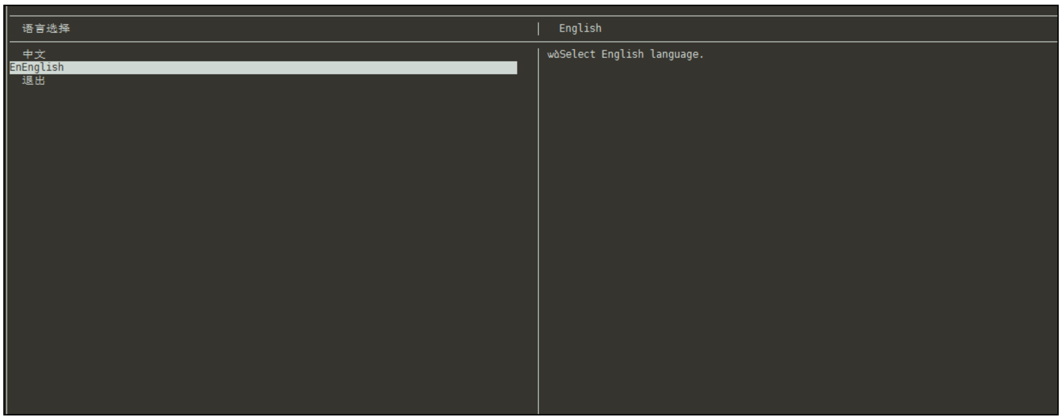


```
Warning

   Please modify the default passwor
d in time!



[RETURN]_
```

In either of the following cases, a window shown in Figure A-5 appears, prompting you to select a language:

- You do not change the initial password of the login account **conadmin** and click **RETURN**.
- You have changed the initial password of the login account **conadmin**.

Figure A-5 Selecting a language

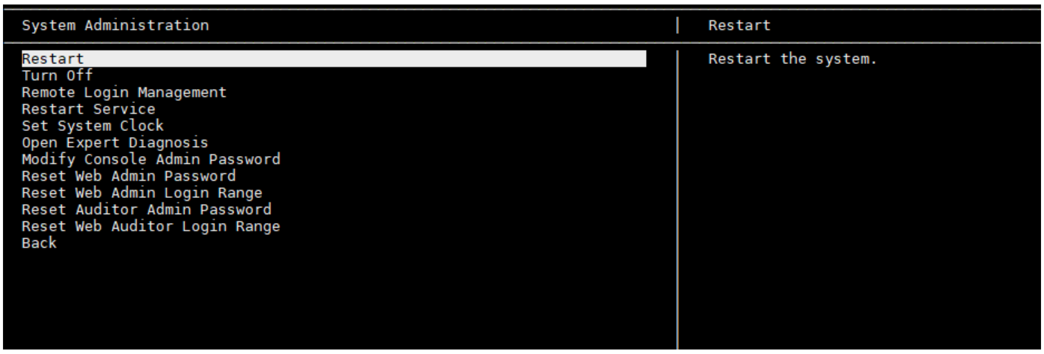


```
 语言选择                                   | English
 中文                                       | wბSelect English language.
EnEnglish
 退出
```

A.2.1 System Management

Select **System Administration** on the main menu. The **System Administration** menu expands, as shown in Figure A-6.

Figure A-6 Console-based management — system administration



```
System Administration                                        | Restart

Restart                                                      | Restart the system.
Turn Off
Remote Login Management
Restart Service
Set System Clock
Open Expert Diagnosis
Modify Console Admin Password
Reset Web Admin Password
Reset Web Admin Login Range
Reset Auditor Admin Password
Reset Web Auditor Login Range
Back
```

On this menu, you can perform the operations listed in Table A-3.

Table A-3 System administration operations on the console

Operation	Description
Restart	Restarts the RSAS system.
Turn Off	Shuts down the RSAS system.
Remote Login Management	After the SSH service is enabled, the technical support personnel of NSFOCUS can remotely log in to RSAS to diagnose faults. After it is enabled, type an IPv4 address and port number (in the range of 60000–65535) of the host that is accessible to RSAS. Then the login key and its QR code used for remote access to RSAS are displayed below.
Restart Service	Restarts RSAS services. When a system exception occurs, you can restart system services.
Set System Clock	Sets the date and time of the RSAS system.
Open Expert Diagnosis	When RSAS is faulty and requires remote assistance, technical support personnel of NSFOCUS can remotely log in to the faulty device via SSH and perform troubleshooting in the background.
Modify Console Admin Password	Changes the password of the console administrator. The password must contain 9 to 20 characters of at least two types of the following: letters, digits, and special characters (@ # $ ^ _).
Reset Web Admin Password	Restores the password for web login to the initial one when **admin** forgets it.
Reset Web Admin Login Range	Restores the default IP addresses through which the **admin** user can log in to RSAS.
Reset Auditor Admin Password	Restores the password for web login to the initial one when **auditor** forgets it.
Reset Web Auditor Login Range	Restores the default IP addresses through which **auditor** can log in to RSAS.

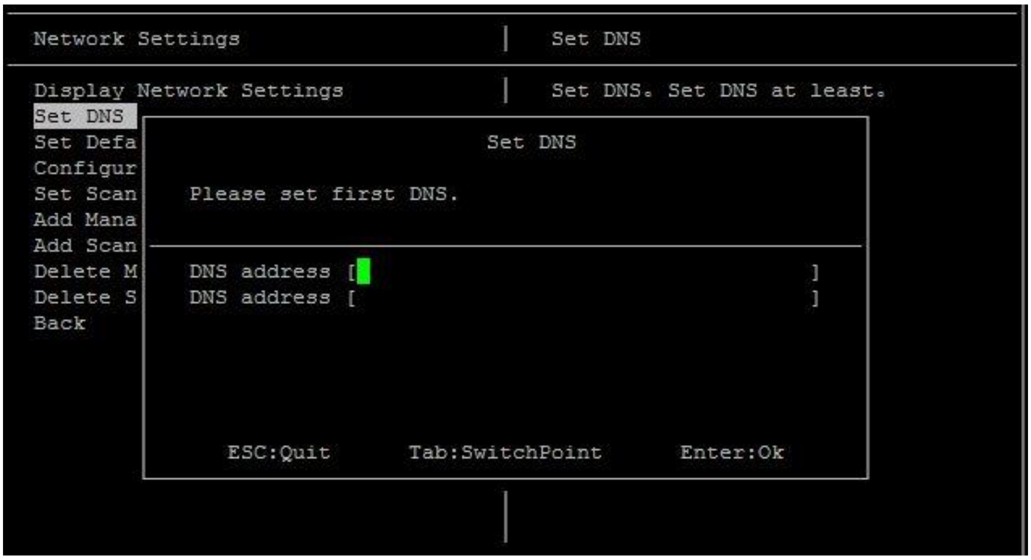
A.2.2 Network Configuration

RSAS provides a scan interface and a management interface. The scan interface is used for network scanning and the management interface is used for RSAS management. Also, the administrator can manage RSAS and perform task assessment only via the scan interface.

Configuring the DNS Server

Select **Network Settings** from the main menu and then select **Set DNS**, as shown in Figure A-7.

Figure A-7 Console-based management — setting a DNS server



```
Network Settings                       | Set DNS

Display Network Settings               | Set DNS. Set DNS at least.
Set DNS
Set Defa                     Set DNS
Configur
Set Scan     Please set first DNS.
Add Mana
Add Scan
Delete M     DNS address [                                  ]
Delete S     DNS address [                                  ]
Back



                ESC:Quit      Tab:SwitchPoint      Enter:Ok
```

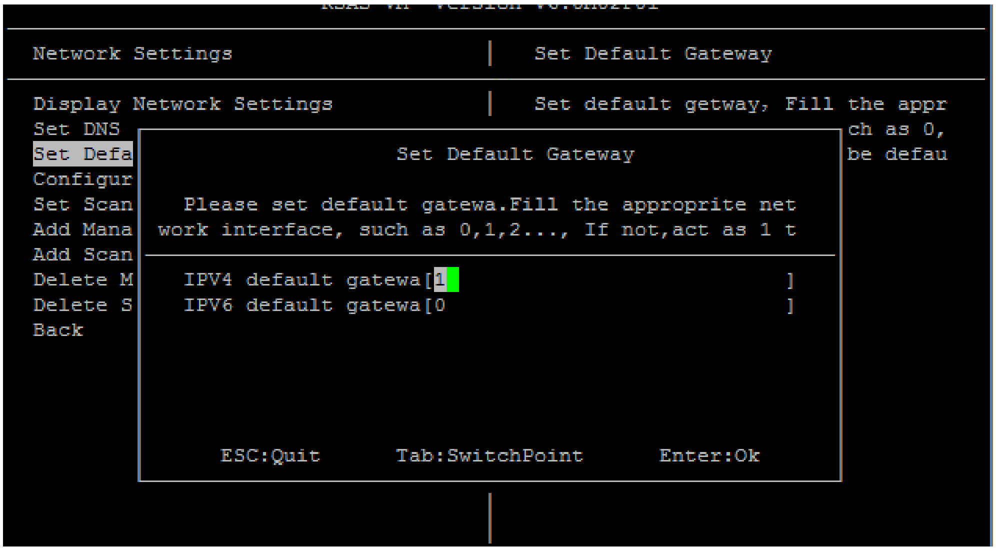
Pay attention to the following when configuring a DNS server:

- At least one DNS server should be configured.
- The first DNS address must be typed.

Setting the Default Gateway

Select **Network Settings** from the main menu and then select **Set Default Gateway**, as shown in Figure A-8.

Figure A-8 Console-based management — setting the default gateway



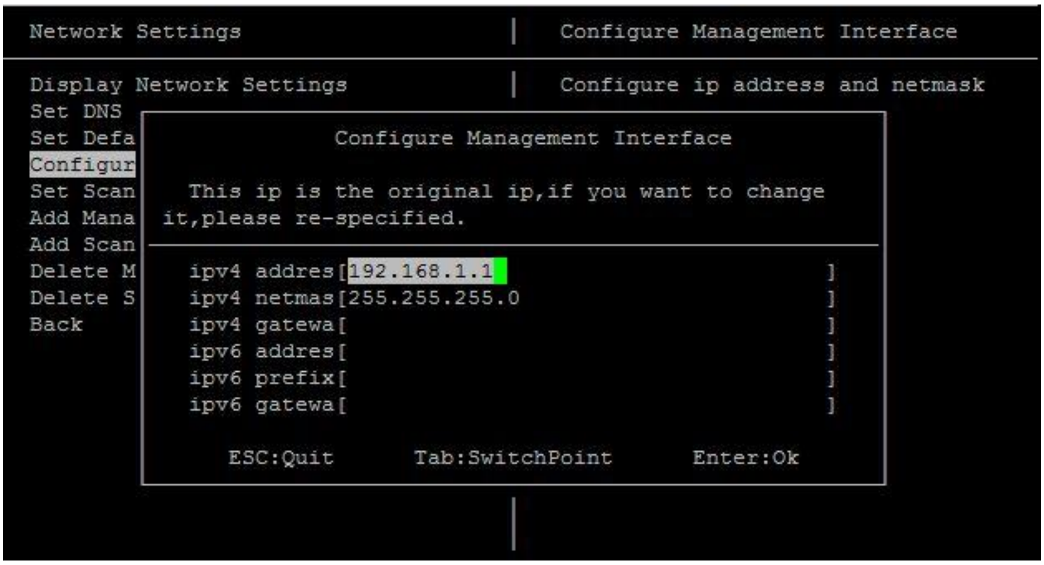
```
 Network Settings                  |  Set Default Gateway

 Display Network Settings          |  Set default getway, Fill the appr
 Set DNS                                                      ch as 0,
 Set Defa            Set Default Gateway                      be defau
 Configur
 Set Scan    Please set default gatewa.Fill the approprite net
 Add Mana   work interface, such as 0,1,2..., If not,act as 1 t
 Add Scan
 Delete M    IPV4 default gatewa[1                         ]
 Delete S    IPV6 default gatewa[0                         ]
 Back




               ESC:Quit       Tab:SwitchPoint       Enter:Ok
```

If the default gateway is not specified here, the system uses the gateway of scan interface 1 as the default gateway.

Configuring the Management Interface

Select **Network Settings** from the main menu and then select **Configure Management Interface**, as shown in Figure A-9.

Figure A-9 Console management — configuring the management interface



```
 Network Settings                  |  Configure Management Interface

 Display Network Settings          |  Configure ip address and netmask
 Set DNS
 Set Defa          Configure Management Interface
 Configur
 Set Scan    This ip is the original ip,if you want to change
 Add Mana   it,please re-specified.
 Add Scan
 Delete M    ipv4 addres[192.168.1.1                     ]
 Delete S    ipv4 netmas[255.255.255.0                   ]
 Back        ipv4 gatewa[                                ]
             ipv6 addres[                                ]
             ipv6 prefix[                                ]
             ipv6 gatewa[                                ]

               ESC:Quit       Tab:SwitchPoint       Enter:Ok
```

Pay attention to the following when configuring the management interface:

- IPv4 or IPv6 addresses are assigned via DHCP. After you press **Enter**, RSAS will automatically obtain the IP address of the scan interface.

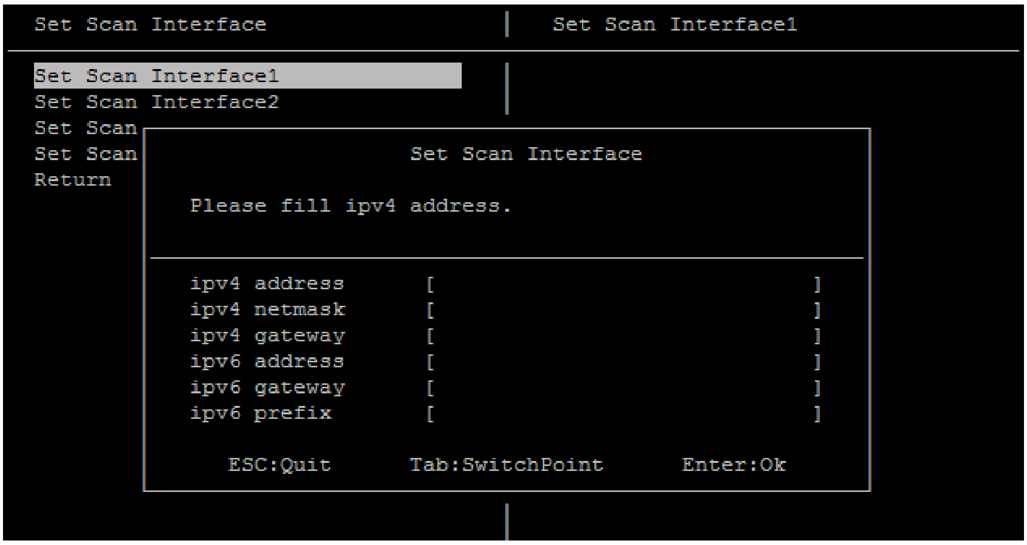
- Either an IPv4 or IPv6 address can be configured for the management interface. The default IPv4 address is **192.168.1.1/24**.
- If the IP address of the RSAS host is on a different network segment from the IP address of the management interface, you need to add a route for the management interface.
- The negotiation mode must be set for the management interface.

  After the configuration, click **OK** to make the settings take effect immediately.
- The management interface and scan interface cannot be configured in the same network segment.

Configuring the Scan Interface

Select **Network Settings** from the main menu and then choose **Set Scan Interface** > **Set Scan Interface1**, as shown in Figure A-10.

Figure A-10 Console management — configuring the scan interface



```
 Set Scan Interface                    |  Set Scan Interface1
------------------------------------------------------------------
 Set Scan Interface1                   |
 Set Scan Interface2                   |
 Set Scan
 Set Scan          Set Scan Interface
 Return
            Please fill ipv4 address.

            ipv4 address       [                              ]
            ipv4 netmask       [                              ]
            ipv4 gateway       [                              ]
            ipv6 address       [                              ]
            ipv6 gateway       [                              ]
            ipv6 prefix        [                              ]

               ESC:Quit       Tab:SwitchPoint       Enter:Ok
```

Pay attention to the following when configuring a scan interface:

- IPv4 or IPv6 addresses are assigned via DHCP. After you press **Enter**, RSAS will automatically obtain the IP address of the scan interface.
- Either an IPv4 or IPv6 address is allowed for a scan interface.

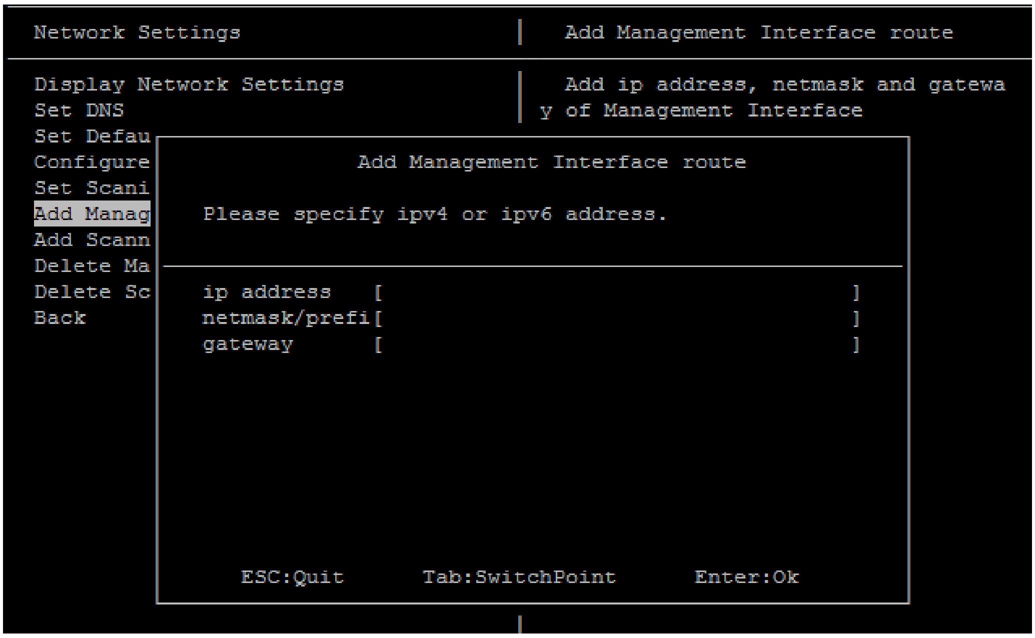
  After the configuration, click **OK** to make the settings take effect immediately.
- Make sure that the gateway and DNS server are properly configured if the online upgrade is necessary for RSAS.
- Parameters must be set in the correct format, for example, 255.255.255.0 as the IPv4 netmask.
- The management interface and scan interface, and any two scan interfaces must be configured in different network segments.

Creating a Route for the Management Interface

You can specify an access path to the network by creating or deleting a static route.

Select **Network Settings** from the main menu and then select **Add Management Interface Route**, as shown in Figure A-11.

Figure A-11 Console management — creating a route for the management interface



```
Network Settings                        |  Add Management Interface route

Display Network Settings                |  Add ip address, netmask and gatewa
Set DNS                                 | y of Management Interface
Set Defau
Configure              Add Management Interface route
Set Scani
Add Manag    Please specify ipv4 or ipv6 address.
Add Scann
Delete Ma
Delete Sc    ip address    [                                   ]
Back         netmask/prefi [                                   ]
             gateway       [                                   ]




                ESC:Quit       Tab:SwitchPoint       Enter:Ok
```

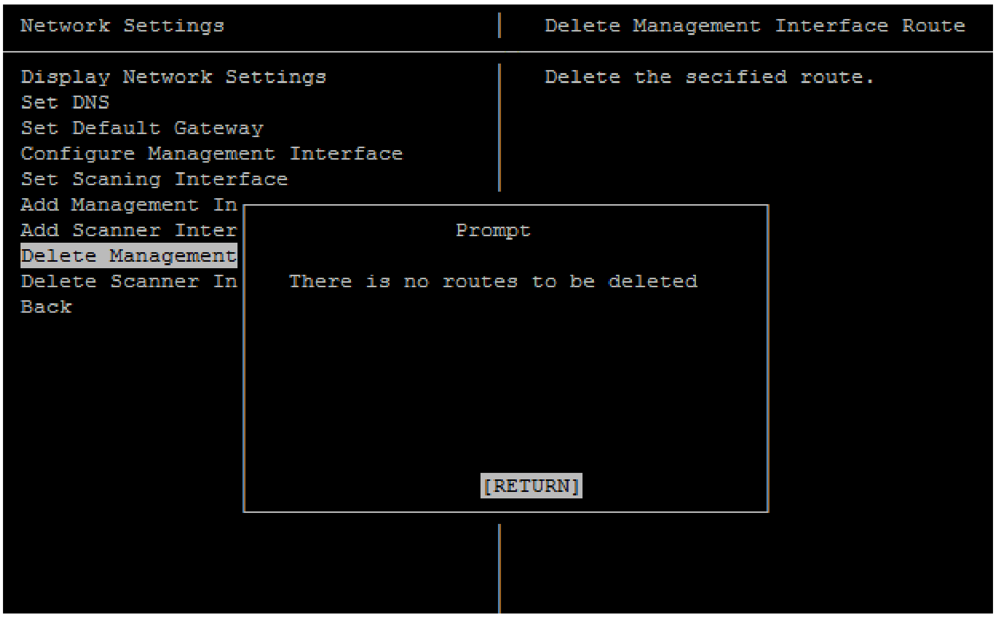
Pay attention to the following when creating a route:

- The default management interface is the M interface. Here, route parameters are set for this interface.
- After you set the IP address, subnet mask, and gateway address and click **OK**, the settings take effect immediately.
- If an error occurs after you click **OK**, check whether theIP address and gateway address are correct.

Deleting a Route of the Management Interface

Select **Network Settings** from the main menu and then select **Delete Management Interface Route**, as shown in Figure A-12.

Figure A-12 Console management — deleting a route of the management interface



```
Network Settings                          | Delete Management Interface Route

Display Network Settings                  | Delete the secified route.
Set DNS
Set Default Gateway
Configure Management Interface
Set Scaning Interface
Add Management In
Add Scanner Inter                 Prompt
Delete Management
Delete Scanner In     There is no routes to be deleted
Back

                                 [RETURN]
```

Pay attention to the following when deleting a route:

- After you select **Delete Management Interface Route**, the routing table of the management interface appears. Select the route that you want to delete.
- After you select the route and click **OK**, the deleted route immediately loses effect and disappears from the routing table.

Creating a Route for a Scan Interface

Select **Network Settings** from the main menu and then select **Add Scan Interface Route**. A route for a scan interface is added in the same way as that for the management interface. For details, see Creating a Route for the Management Interface.

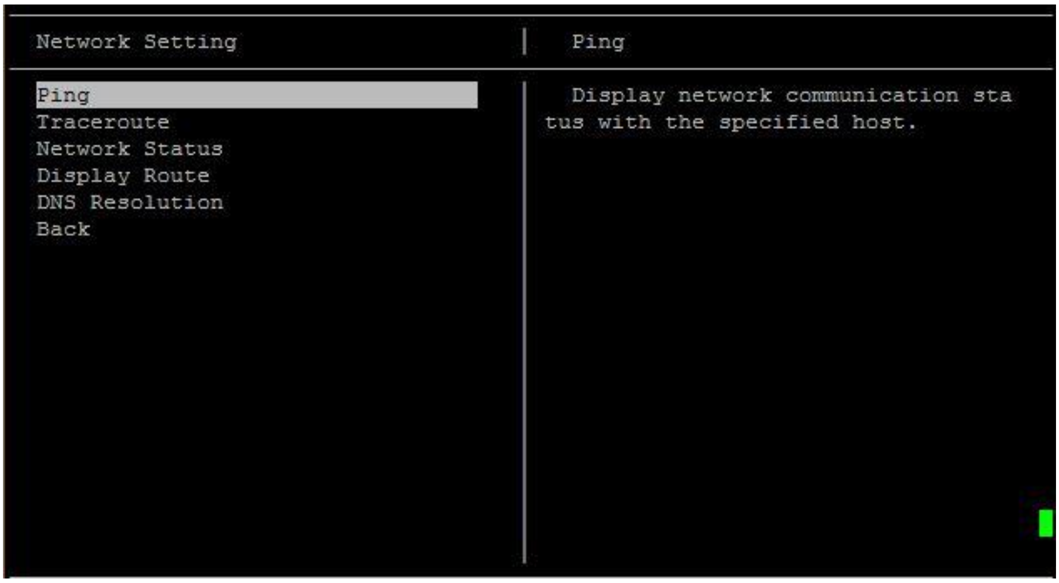
Deleting a Route of a Scan Interface

Select **Network Settings** from the main menu and then select **Delete Scan Interface Route**. A route of a scan interface is deleted in the same way as a route of the management interface. For details, see Deleting a Route of the Management Interface.

A.2.3 Network Diagnosis

Select **Network Diagnosis** from the main menu, as shown in Figure A-13.

Figure A-13 Console management — network diagnosis



```
Network Setting                 |  Ping

Ping                            |  Display network communication sta
Traceroute                      | tus with the specified host.
Network Status                  |
Display Route                   |
DNS Resolution                  |
Back                            |
```

Table A-4 lists network diagnosis tools available on RSAS.

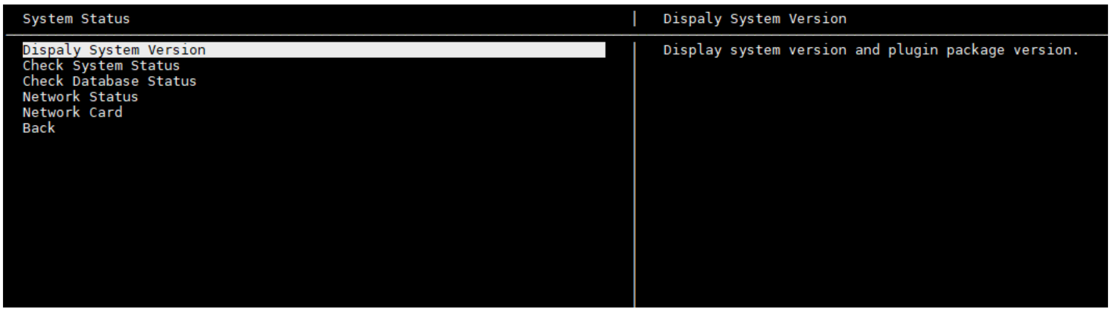
Table A-4 Network diagnosis tools on the console

Tool	Function
Ping	Checks the connection between RSAS and the target host. IPv4 and IPv6 addresses are acceptable.
Traceroute	Traces the hops between RSAS and the target host.
Network Status	Displays the network connection status of RSAS.
Display Route	Displays parameters of the interface used by the routing device to connect to RSAS.
DNS Resolution	Displays the domain name resolution information.

A.2.4 System Status

Select **System Status** from the main menu. The **System Status** menu expands, as shown in Figure A-14.

Figure A-14 Console-based management — system status



```
System Status                                       | Dispaly System Version

Dispaly System Version                              | Display system version and plugin package version.
Check System Status
Check Database Status
Network Status
Network Card
Back
```

On the **System Status** menu, you can view status information listed in Table A-5.

Table A-5 System status checking on the console

Operation	Description
Display System Version	Displays the system and plugin versions of RSAS.
Check System Status	Displays the system status of RSAS.
Check Database Status	Displays the background database status of RSAS.
Network Status	Displays the NIC configuration and routing table of RSAS. Usually, it is used to check the network configuration.
Network Card	Displays the IP address, MAC address, the number of bytes of data transmitted and received by the NIC. The information is usually used to check whether the NIC works properly.

Note

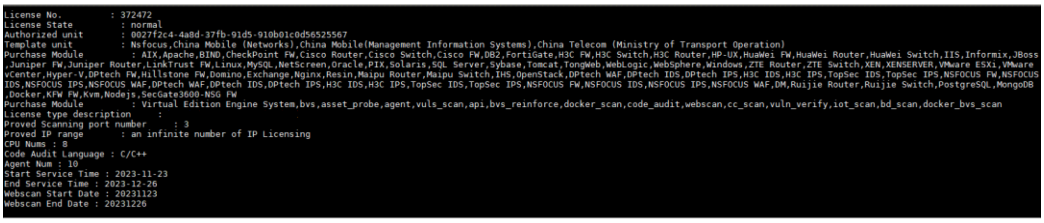
Ongoing assessment tasks will be stopped during the checking of the system status or database status. To avoid data loss, conduct status checks after all tasks are completed.

A.2.5 License Information

Select **License Information** from the main menu, as shown in Figure A-15.

You can check the information about the authorized license file of the current system, including the product type, the start date, end date, and expiry date of the license, as well as your purchased modules.

Figure A-15 License Information



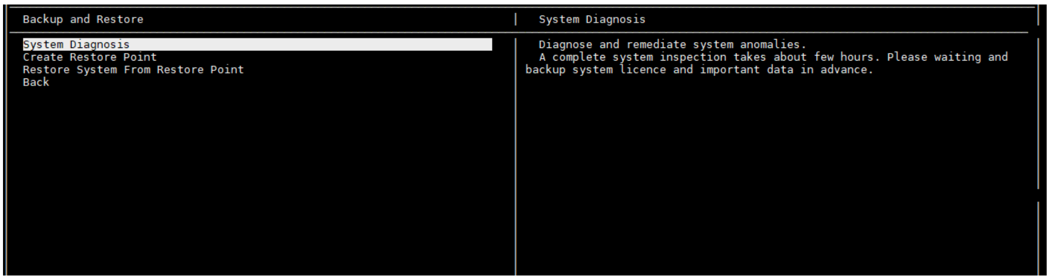
```
License No.         : 372472
License State         : normal
Authorized unit       : 0027f2c4-4a8d-37fb-91d5-910b01c0d56525567
Template unit         : Nsfocus,China Mobile (Networks),China Mobile(Management Information Systems),China Telecom (Ministry of Transport Operation)
Purchase Module         : AIX,Apache,BIND,CheckPoint FW,Cisco Router,Cisco Switch,Cisco FW,DB2,FortiGate,H3C FW,H3C Switch,H3C Router,HP-UX,HuaWei FW,HuaWei Router,HuaWei Switch,IIS,Informix,JBoss
,Juniper FW,Juniper Router,LinkTrust FW,Linux,MySQL,NetScreen,Oracle,PIX,Solaris,SQL Server,Sybase,Tomcat,TongWeb,WebLogic,WebSphere,Windows,ZTE Router,ZTE Switch,XEN,XENSERVER,VMware ESXi,VMware
vCenter,Hyper-V,DPtech FW,Hillstone FW,Domino,Exchange,Nginx,Resin,Maipu Router,Maipu Switch,IHS,OpenStack,DPtech WAF,DPtech IDS,DPtech IPS,H3C IDS,H3C IPS,TopSec IDS,TopSec IPS,NSFOCUS FW,NSFOCUS
IDS,NSFOCUS IPS,NSFOCUS WAF,DPtech WAF,DPtech IDS,DPtech IPS,H3C IDS,H3C IPS,TopSec IDS,TopSec IPS,NSFOCUS FW,NSFOCUS IDS,NSFOCUS IPS,NSFOCUS WAF,DM,Ruijie Router,Ruijie Switch,PostgreSQL,MongoDB
,Docker,KFW FW,Kvm,Nodejs,SecGate3600-NSG FW
Purchase Module         : Virtual Edition Engine System,bvs,asset_probe,agent,vuls_scan,api,bvs_reinforce,docker_scan,code_audit,webscan,cc_scan,vuln_verify,iot_scan,bd_scan,docker_bvs_scan
License type description      :
Proved Scanning port number      : 3
Proved IP range       : an infinite number of IP Licensing
CPU Nums : 8
Code Audit Language : C/C++
Agent Num : 10
Start Service Time : 2023-11-23
End Service Time : 2023-12-26
Webscan Start Date : 20231123
Webscan End Date : 20231226
```

A.2.6 **Backup and Restoration**

Backup and restoration are very important functions of RSAS as the two functions can restore data in time once the device breaks down.

Select **Backup and Restore** from the main menu, as shown in Figure A-16.

Figure A-16 Backup and restoration



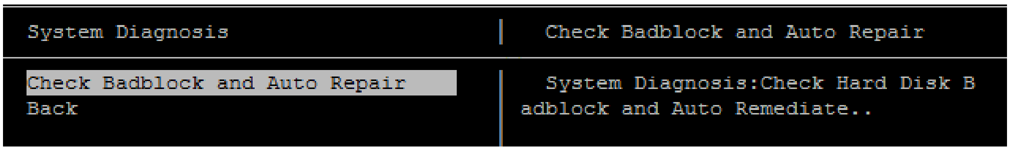
```
  Backup and Restore                                     |  System Diagnosis

  System Diagnosis                                       |  Diagnose and remediate system anomalies.
  Create Restore Point                                   |  A complete system inspection takes about few hours. Please waiting and
  Restore System From Restore Point                      | backup system licence and important data in advance.
  Back                                                   |
```

Performing System Diagnosis for Automatic Remediation

System diagnosis is to diagnose and fix system faults. The entire diagnosis process takes a long time. You must back up the system license and important scanning data in advance and patiently wait until the process is complete.

Select **Backup and Restore** from the main menu and then select **System Diagnosis**, as shown in Figure A-17.

Figure A-17 Console-based management — system diagnosis and automatic remediation



```
 System Diagnosis                      |  Check Badblock and Auto Repair

 Check Badblock and Auto Repair        |  System Diagnosis:Check Hard Disk B
 Back                                  | adblock and Auto Remediate..
```

This function checks and fixes the hard disk for bad blocks.

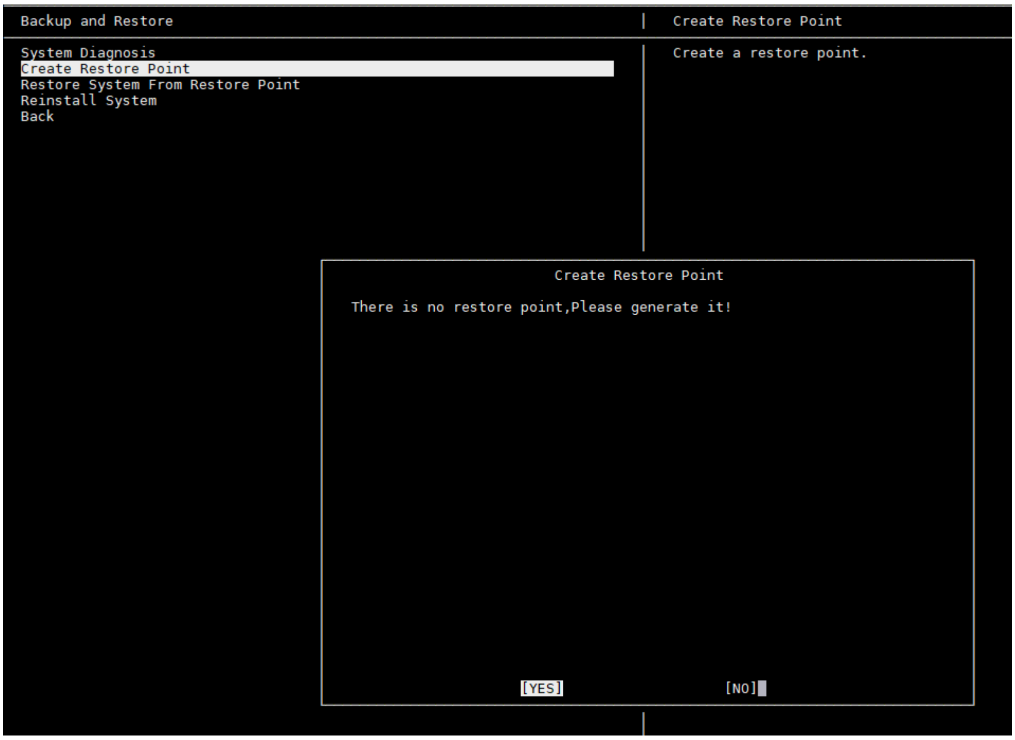
This process takes a long time, during which all services are stopped. After the process is complete, the system restarts automatically.

Creating a Restore Point

A restore point is created for system restoration. A restore point involves the following information: system configuration, asset information, scanning templates, scanning tasks, and user information.

Select **Backup and Restoration** from the main menu and then select **Create Restore Point** to create a restore point. The administrator can manually create a user restore file.

Figure A-18 Console-based management — creating a restore point



```
Backup and Restore                                          | Create Restore Point

System Diagnosis                                            | Create a restore point.
Create Restore Point
Restore System From Restore Point
Reinstall System
Back

                              Create Restore Point

                      There is no restore point,Please generate it!

                              [YES]                 [NO]
```

Note

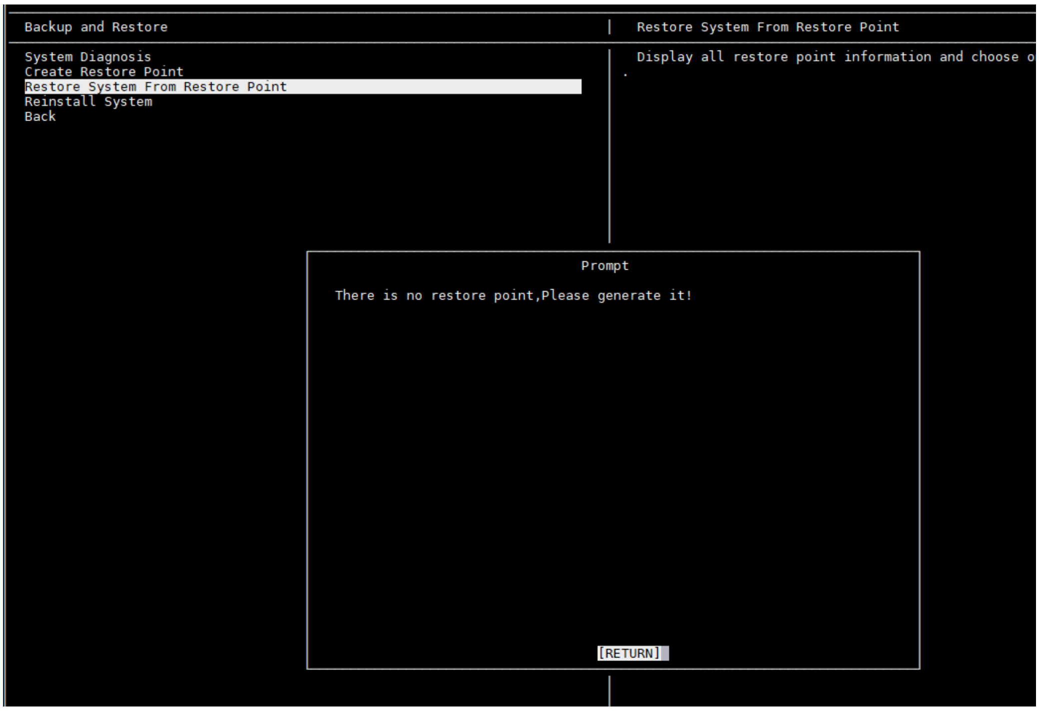
You can create only one restore point each time.

Restoring the System by Using a Restore Point

From the **Backup and Restoration** menu, you can choose to restore the system using a restore point file.

Select **Backup and Restore** from the main menu and then select **Restore System From Restore Point**, as shown in Figure A-19.

Figure A-19 Console-based management — restoring the system using a restore point



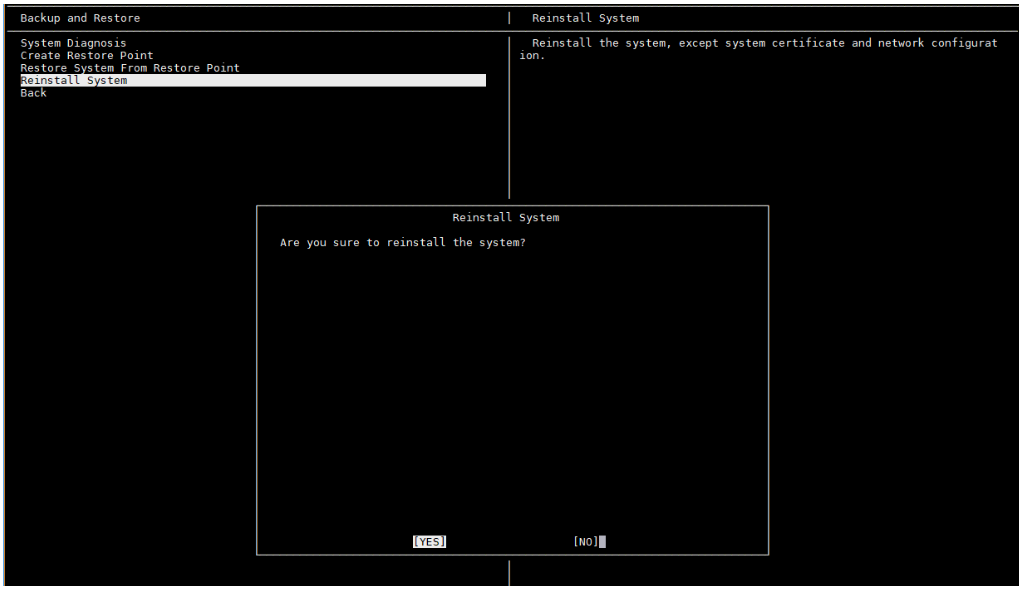
```
Backup and Restore                                  |  Restore System From Restore Point

System Diagnosis                                    |  Display all restore point information and choose o
Create Restore Point                                |  .
Restore System From Restore Point
Reinstall System
Back

                                 Prompt

                  There is no restore point,Please generate it!

                                 [RETURN]
```

Reinstalling the System

This function is available only to the RSAS hardware. System reinstallation means restoring the system to the default configuration. Except the network settings, license file, and the number of current scanned IP addresses, all data is restored to factory defaults during the process. This function can be used when RSAS is faulty.

Select **Backup and Restore** from the main menu and then select **Reinstall System**, as shown in Figure A-20.

Figure A-20 Console-based management — reinstalling the system



Reinstall the system, except system certificate and network configuration.

Are you sure to reinstall the system?

A.2.7 System Exiting

After configuring parameters for console-based management, return to the main menu, select **Back**, and then press **Enter**. For further configuration, log in to the system again.

B Default Parameters

Choose **Administration > Status** > **System Status** to check the factory version and view its factory defaults.

V6.0R02F00 and Later

Default Network Settings

Interface	IP Address	Subnet Mask
Management interface	192.168.1.1	255.255.255.0
Scan interface 1	192.168.2.1	255.255.255.0

Communication Parameters of the Console Port

User Name	Password	Baud Rate	Data Bits
conadmin	conadmin	115200	8

Default User Accounts

Role	User Name	Password
System administrator	admin	admin
Auditor	auditor	auditor

Versions Earlier Than V6.0R02F00

Default Network Settings

Interface	IP Address	Subnet Mask	Gateway IP Address	Negotiation Mode
Scan interface 1	192.168.1.1	255.255.255.0	192.168.1.254	auto
Management interface	1.1.1.1	255.255.255.0	N/A	N/A

Communication Parameters of the Console Port

User Name	Password	Baud Rate	Data Bits
conadmin	nsfocus	115200	8

Default User Accounts

Role	User Name	Password
System administrator	admin	nsfocus
Auditor	auditor	

C FAQ

This section allows you to query frequently asked questions (FAQs) and their answers.

C.1 System Management

Q1: Why Can I Not Access the Web-based Manager?

A: Please do as follows:

- Make sure that HTTPS instead of HTTP is used for the connection.
- Make sure that IP addresses, gateway addresses, and DNS parameters are properly set.
- Make sure that the network connection is correct.

Q2: Why Can I Not Log In to the Console by Using a Serial Cable?

A: Please do as follows:

- Make sure that a proper COM interface is used.
- Make sure that the port properties and other parameters are properly configured.
- Use a new serial cable.

Q3: What Permission Should I Have to Export a License?

A: To import or export a license, you should have the license management permission.

C.2 Scanning Task

Q1: Is the Scope of Scan Targets Limited When I Create an Assessment Task?

A: No. On an RSAS device, regardless of the model, you can specify any number of class B (not class A) IP addresses. But the number of IP addresses actually scanned depends on the license. Those IP addresses without the scan result are listed in online reports.

Q2: What Is a Scanning Task? What Operations Can Be Performed on It?

A: A scanning task covers the task configuration (including the scan target, scan policies, and parameters) and the scan result. The following operations can be performed on tasks: deletion, rescanning, duplication, export, import, and viewing of consolidated reports.

Q3: Why Is an Active Host Displayed as Not Alive in the Scan Result?

A: Check whether it is a scanning task involving multiple network segments. If so, a device such as a firewall or IPS may exist, dropping packets from RSAS. In this case, you are advised to modify network device settings to allow all packets from RSAS to pass through.

Q4: What Could Slow Down the Scanning Speed of an RSAS Device?

A: A lower scanning speed may be caused by:

- Firewalls
- Large scanning scope
- Scan policies
- Too large value for the maximum number of concurrent hosts

Q5: Why Should the Port Scanning Speed Be Set?

A: The Netscreen firewall takes RSAS's scanning as a SYN flood or connection flood and so blocks the IP address of RSAS that is performing a port scanning task. To prevent this from happening, you need to use the slow scan function to penetrate the Netscreen firewall.

Q6: Why Is the UDP Port Selected in the Port Scanning Policy Not Scanned?

A: The UDP port that is selected in the port scanning policy can be scanned only when **UDP Scan** is selected during the port scanning configuration of an assessment task.

Q7: What Is the Start Time for a Scanning Task That Is Resumed?

A: For a scanning task that is resumed, its start time is still the time when the task is launched initially.

Q8: Why Do Task IDs Not Progressively Increase by One?

A: This is because during the database remediation, the system background checks part of the database when detecting the database. This has no impact on the use of the product.

C.3 Scanning Report

Q: Which Scanning Tasks Can Be Exported and Have Corresponding Reports?

A: Assessment tasks, web application scanning tasks, password guess tasks, configuration scanning tasks, image scanning tasks, code audit tasks, host asset detection tasks, and web asset detection tasks can be exported and have corresponding reports.

C.4 Asset Management

Q1: Which Devices in the Asset Repository Support Scan Result Export?

A: Both registered and unregistered devices in the asset repository support the export of scan results.

Q2: Why Are Scanning Tasks Displayed for Devices Unavailable in the Asset Tree?

A: Please do as follows:

Make sure the IP address in the scanning task is alive and included in the IP address range of the asset tree. If so, click ⟳ to refresh the asset tree.

C.5 Product Model

Q1: Can I Create Scanning Tasks When the Number of Tasks on the Task List Reaches the Maximum?

A: No, you cannot. If you create a task when the number of tasks reaches the maximum, the system prompts that the maximum is reached. Prior to creating scanning tasks, you need to delete some in this case.

Q2: What Is the Relationship Between Authorized Scan Interfaces and Scan Interfaces on RSAS?

Scan interfaces are used to connect RSAS to the network. As RSAS provides one scan interface upon delivery from the factory, the number of authorized scan interfaces on RSAS is 1 + number of scan interfaces you have purchased

D MLPS

RSAS supports levels 1–4 security protection capabilities defined according to the Multi-Level Protection Scheme (MLPS) guideline in China.

Information systems at different security protection levels or even at the same level have different requirements for the security of business information and the continuity of system services. According to MLPS, information systems at levels 1–4 should be equipped with the following basic security capabilities:

- Level 1 security capabilities

  Should be able to protect the system from malicious attacks launched by individuals or threat actors with very limited resources, minor natural disasters, and other threats with equal impacts, which may cause damages to critical resources. The system, once compromised, can partially restore its functions.
- Level 2 security capabilities

  Should be able to protect the system from malicious attacks launched by small external groups or threat actors with limited resources, minor natural disasters, and other threats with equal impacts, which may cause damages to significant resources, and discover major security vulnerabilities and incidents. The system, once compromised, can partially restore its functions in a given period of time.
- Level 3 security capabilities

  Should be able to protect the system with unified security policies from malicious attacks launched by external organized groups or threat actors with fairly abundant resources, major natural disasters, and other threats with equal impacts, which may cause damages to major resources, and discover security vulnerabilities and incidents. The system, once compromised, can restore most functions quite quickly.
- Level 4 security capabilities

  Should be able to protect the system with unified security policies from malicious attacks launched by nation-state attackers, adversaries, or threat actors with abundant resources, critical natural disasters, and other threats with equal impacts, which may cause damages to resources, and discover security vulnerabilities and incidents. The system, once compromised, can quickly restore all functions.

Basic security requirements are raised for the basic protection capabilities that information systems at various levels should possess. According to the implementation manner, basic security requirements fall into basic technical requirements and basic administrative requirements. Basic technical requirements are subdivided into three categories:

- Information security requirements (**S** for short): protection of data from leakage, corruption, and unauthorized modifications during storage, transmission, and processing

- Service assurance requirements (**A** for short): protection of business continuity from unauthorized alterations and corruption that make the system unavailable
- General security protection requirements (**G** for short)

Information systems' capabilities to fulfill basic technical requirements can be combined to define security protection levels, as shown in Table A-6.

Table A-6 Security protection levels

Security Protection Level	**Information System Grading Result**
1	S1A1G1
2	S1A2G2, S2A2G2, S2A1G2
3	S1A3G3, S2A3G3, S3A3G3, S3A2G3, S3A1G3
4	S1A4G4, S2A4G4, S3A4G4, S4A4G4, S4A3G4, S4A2G4, S4A1G4