

# **NSFOCUS Unified Threat Sensor User Guide**



Version: V2.0R00F05 (2023-09-28)

---

■ Copyright © 2023 NSFOCUS Technologies, Inc. All rights reserved.

---

Unless otherwise stated, **NSFOCUS Technologies, Inc.** holds the copyright for the content of this document, including but not limited to the layout, figures, photos, methods, and procedures, which are protected under the intellectual property and copyright laws. No part of this publication may be reproduced or quoted, in any form or by any means, without prior written permission of **NSFOCUS Technologies, Inc.**

---

#### ■ 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

---

<b>Preface .....</b>	<b>1</b>
<b>1 Product Overview .....</b>	<b>4</b>
1.1 Introduction .....	4
1.2 Typical Deployment .....	5
1.3 Management Modes .....	7
1.3.1 Web-based Management .....	7
1.3.2 Console-based Management .....	10
1.3.3 SSH-based Management .....	10
<b>2 Getting Started.....</b>	<b>11</b>
<b>3 Data Center.....</b>	<b>15</b>
3.1 Threat Analysis.....	15
3.1.1 Threat Event Analysis .....	15
3.2 Metadata Log .....	17
3.3 Full Traffic Forensics .....	25
<b>4 Policies .....</b>	<b>27</b>
4.1 Threat Detection.....	27
4.1.1 Basic Detection .....	27
4.1.2 DDoS Detection .....	30
4.1.3 Scanning and Brute Force Detection.....	31
4.1.4 Advanced Threat Detection.....	34
4.1.5 5G Threat Detection.....	40
4.1.6 Other Threat Detection.....	42
4.2 Rule Configuration.....	46
4.2.1 Rule Management .....	46
4.2.2 Rule Templates.....	50
4.3 Restoration Configuration .....	51
4.3.1 Metadata Restoration .....	51
4.3.2 File Restoration.....	51
4.3.3 5G Log-related Switches.....	52
4.4 Traffic Management .....	53
4.4.1 Traffic Storage.....	53
4.4.2 Allowlist.....	54

4.4.3 Suspicious List .....	55
4.5 SSL Configuration.....	56
4.5.1 SSL Connection Configuration .....	56
4.5.2 SSL Certificate Management .....	56
4.6 Alert Allowlist .....	57
4.7 Out-of-Path Blocking .....	58
4.7.1 Out-of-Path Blocking Policies .....	58
4.7.2 Custom Blocking Policy .....	60
<b>5 Assets.....</b>	<b>63</b>
5.1 Internal Network .....	63
5.1.1 Network Segment.....	63
5.1.2 Node.....	64
5.1.3 IP Pool.....	64
5.1.4 Port.....	65
5.2 Asset Discovery.....	65
5.3 Asset Tree.....	66
5.4 5G NE .....	69
<b>6 System .....</b>	<b>71</b>
6.1 Diagnostic Tools.....	71
6.1.1 Ping/TraceRoute/Network Connection Status/Network Card Status/Routing Information/Playback Testing.....	71
6.1.2 Packet Capture .....	72
6.1.3 One-Click Diagnosis .....	73
6.1.4 Fault Diagnosis .....	74
6.2 System Configuration.....	74
6.2.1 Interface .....	74
6.2.2 Static Route.....	76
6.2.3 DNS .....	77
6.2.4 Device .....	77
6.2.5 Special Parameters .....	78
6.2.6 Encryption.....	79
6.2.7 Log Configuration.....	79
6.2.8 Cloud Environment Adaptation.....	80
6.2.9 Custom Product Name and Logo .....	80
6.3 System Upgrade .....	81
6.3.1 Update.....	81
6.3.2 Online Upgrade.....	82
6.3.3 Offline Upgrade .....	84
6.4 Backup and Restoration .....	85
6.4.1 Backup .....	85
6.4.2 Restoration.....	85

6.5 System Control.....	85
6.6 Storage Management.....	86
<b>7 Administration .....</b>	<b>88</b>
7.1 Account Management.....	88
7.1.1 Account Management .....	88
7.1.2 Configuring Login Parameters .....	91
7.1.3 API Account Configuration.....	91
7.2 Log Forwarding Management.....	92
7.2.1 Log Plugin Configuration .....	93
7.2.2 A Interface Channel Configuration .....	94
7.3 License Management.....	97
7.4 SNMP.....	100
7.4.1 System Configuration Information .....	100
7.4.2 Agent Access Control.....	100
7.4.3 Trap .....	102
<b>8 Audit.....</b>	<b>104</b>
8.1 Logs.....	104
8.2 Configuring Log Storage.....	105
<b>A Console-based Management.....</b>	<b>106</b>
A.1 Login to the Console .....	106
A.2 Keyboard Operations.....	108
A.3 Configuration on the Console.....	109
A.3.1 Configuring the Management Interface and Gateway.....	109
A.3.2 Binding Hardware Information .....	109
A.3.3 Resetting the Web Login Password of the Administrator.....	109
A.3.4 Resetting the Web Login Password of the Auditor.....	110
A.3.5 Enabling/Disabling SSH Access .....	110
A.3.6 Viewing the IP Address of the Management Interface .....	111
A.3.7 Initializing the System.....	111
A.3.8 Rebooting the System .....	112
A.3.9 Shutting Down the System.....	112
A.3.10 Formatting Disks .....	112
A.3.11 Stopping the Service.....	115
A.3.12 Changing the HTTPS Port .....	115
A.3.13 Adding Disks to LVM Partitions .....	115
A.3.14 Resizing LVM Partitions .....	115
A.3.15 Exiting the Console.....	116
<b>B Default Parameters.....</b>	<b>117</b>
B.1 Management Interface .....	117
B.2 Default Accounts .....	117

B.3 Communication Parameters of the Console Port .....	117
<b>C Remote Assistance Configuration .....</b>	<b>118</b>

# Preface

---

This document describes the functions and usage of NSFOCUS Unified Threat Sensor (UTS for short).

This document is provided for reference only. It may slightly differ from the actual product due to version upgrade or other reasons.





## Organization

Chapter	Description
<a href="#">1 Product Overview</a>	Describes the characteristics, deployment modes, and management methods of UTS.
<a href="#">2 Getting Started</a>	Describes the initial configuration of UTS.
<a href="#">3 Data Center</a>	Describes how to view threat analysis logs and metadata logs, configure full traffic forensics, and conduct global search for various logs.
<a href="#">4 Policies</a>	Describes how to configure security policies.
<a href="#">5 Assets</a>	Describes how to configure internal network objects, 5G network elements, and assets.
<a href="#">6 System</a>	Describes how to configure system parameters.
<a href="#">7 Administration</a>	Describes how to configure accounts on the UTS web-based manager, log forwarding, and SNMP and how to manage licenses.
<a href="#">8 Audit</a>	Describes how to view audit logs and store logs. Note that these operations are available for the auditor account only.
<a href="#">A Console-based Management</a>	Describes how to log in to the UTS console-based manager via the console port and conduct management.
<a href="#">B Default Parameters</a>	Describes the default settings of UTS.
<a href="#">C Remote Assistance Configuration</a>	Describes how to use remote assistance.

## Change History

Version	Description
V2.0R00F05	Initial release.

## Conventions

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

## Customer Support

Hardware and Software Support

Email: [support@nsfocusglobal.com](mailto:support@nsfocusglobal.com)

Cloud Mitigation Support

Email: [cloud-support@nsfocusglobal.com](mailto: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](mailto:info-support@nsfocus.com)

# 1 Product Overview

This chapter contains the following topics:

Topic	Description
<a href="#">Introduction</a>	Introduces UTS.
<a href="#">Typical Deployment</a>	Describes typical deployment modes of UTS.
<a href="#">Management Modes</a>	Describes methods of managing UTS.

## 1.1 Introduction

With the wide application of new technologies, including 5G, the Internet of Things (IoT), and artificial intelligence, attack methods are emerging endlessly, posing numerous challenges to traditional threat detection solutions. To effectively handle the increasing number of diverse attacks, NSFOCUS has launched Unified Threat Sensor (UTS) that is built on its years of security research and threat detection capabilities. UTS is a full-traffic threat detection probe suitable for all industries. It incorporates a range of cutting-edge technologies such as rule engines, virtual sandboxes, threat intelligence, and machine learning. With wide recognition and precise detection capabilities and excellent interoperability, UTS is capable of identifying and analyzing advanced threats in diverse scenarios and tracing security events.

UTS has the following features:

- **Accurate detection of advanced threats**  
With multiple built-in detection engines, including intrusion detection, web threat detection, encrypted traffic detection, malicious file detection, dynamic sandbox, 5G threat detection, anomalous behavior detection, and threat intelligence, UTS can accurately detect advanced threats in different scenarios.
- **Fast traceback and forensics**  
Offers comprehensive threat traceback and forensics capabilities. In addition to storing full traffic and alert logs, it can store session-based full traffic and malicious traffic. UTS can utilize logs and raw PCAP files to effectively identify attacks and perform forensics timely.
- **Flexible interoperability with third-party platforms**  
Offers flexible and customizable log plugins and supports popular interface protocols, enhancing customers' ability to perform full traffic detection and analysis.

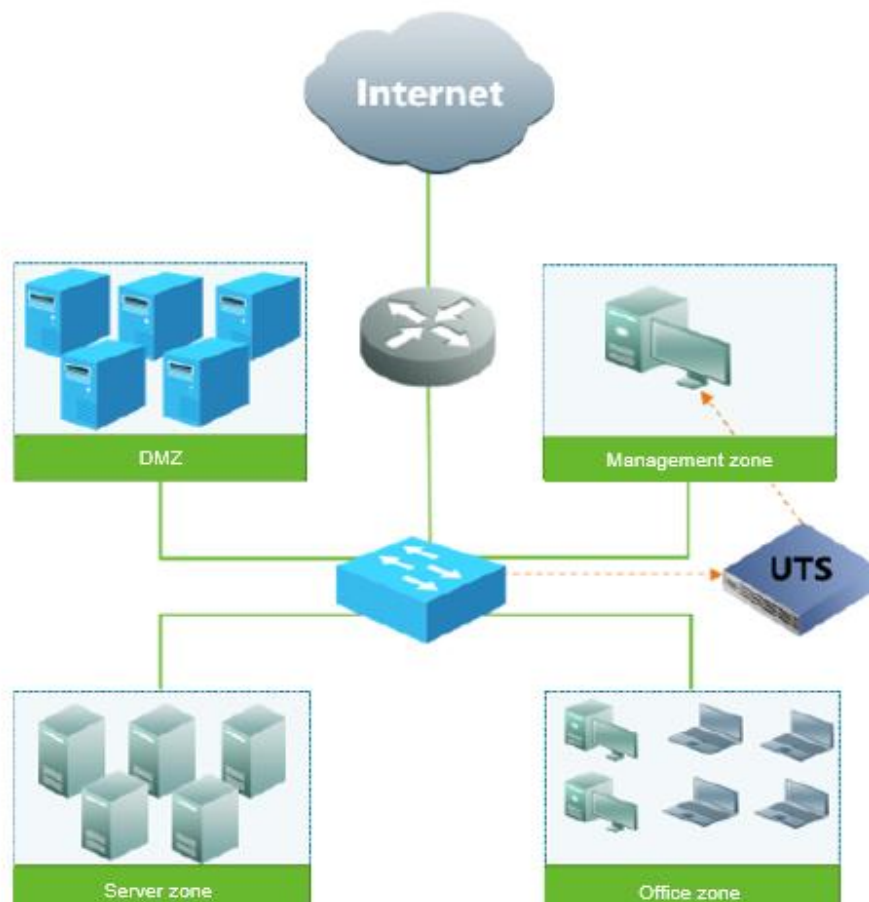
## 1.2 Typical Deployment

UTS is generally deployed in out-of-path mode in actual network environments. There are three typical application scenarios.

### Unknown Threat Detection Scenario

UTS performs full traffic collection, storage, and detection, blocks attacks in an out-of-path manner, and supports traceback analysis and forensics, as shown in [Figure 1-1](#).

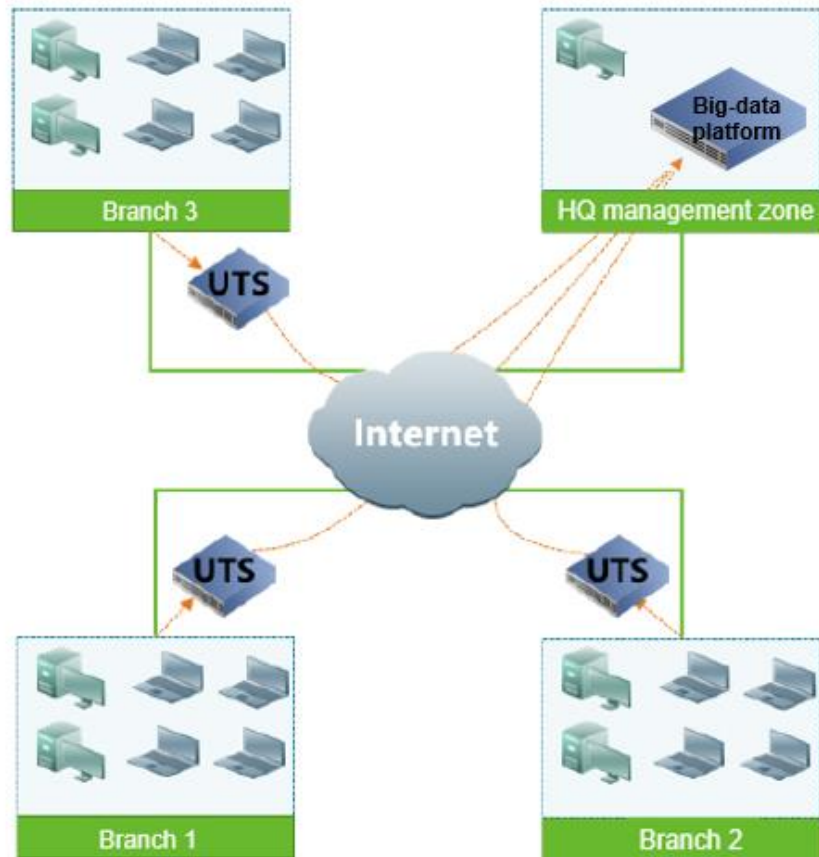
Figure 1-1 Topology of implementing unknown threat detection



### Threat Situation Awareness Scenario

UTS can collaborate with NSFOCUS Intelligent Security Operations Platform (ISOP) or a third-party platform to constitute a distributed situational awareness platform that can identify and analyze threats to the security of multi-region traffic, as shown in [Figure 1-2](#).

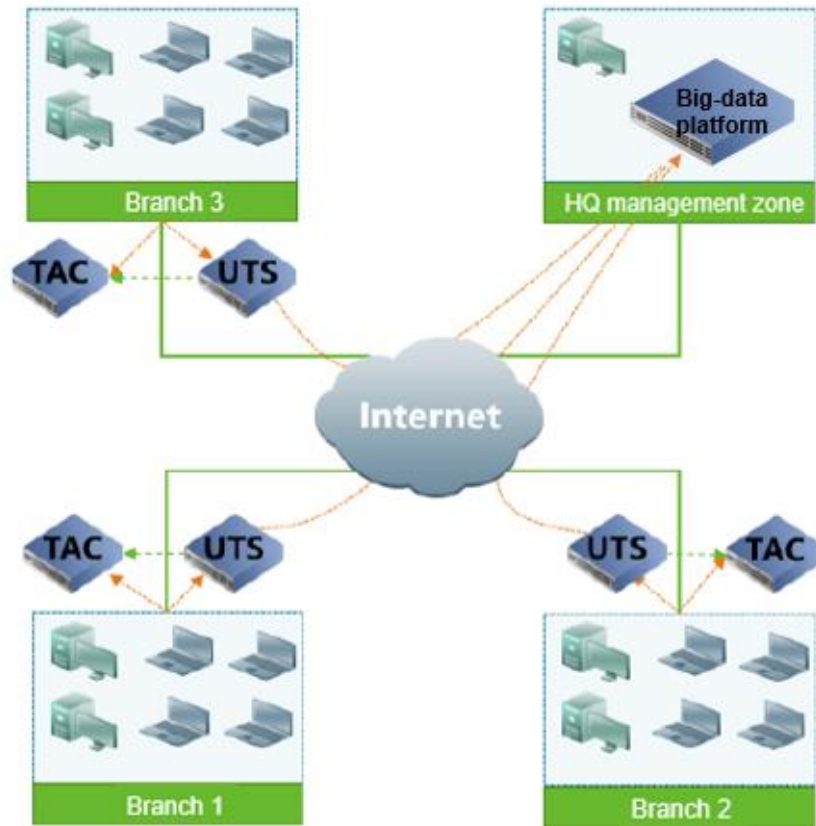
Figure 1-2 Topology of configuring threat situation awareness



## Comprehensive Threat Situation Awareness Scenario

UTS can collaborate with a TAC sandbox and ISOP or a third-party platform to constitute a comprehensive situational awareness platform that can detect unknown threats to secure multi-region traffic and aggregate traffic from multiple regions for analysis, as shown in [Figure 1-3](#).

Figure 1-3 Comprehensive Threat Situation Awareness Scenario



## 1.3 Management Modes

UTS can be managed in one of the following ways:

- Web-based management  
Offers an intuitive human-machine interface to provide comprehensive function management.
- Console-based management  
Manages UTS using command lines via the console port.
- SSH-based management  
Manages UTS from a remote management client via the Secure Shell protocol (SSH).

### 1.3.1 Web-based Management

The UTS web-based manager provides an intuitive Graphic User Interface for users to manage and configure UTS. The following describes the system users, login method, page layout of, and management methods of UTS.

### 1.3.1.1 System Users

UTS users fall into administrator, auditor, account manager, operator, and ordinary user. These five types of users are all allowed to log in to the web-based manager, and their privileges are described in [Table 1-1](#).

For details on default user names and their passwords, see [Default Accounts](#).

Table 1-1 System users and their privileges

Role	Account	Privileges
Super administrator	<b>admin</b> (default)	<ul style="list-style-type: none"> <li>• Has no privilege to view audit logs.</li> <li>• Has privileges to manage operators and user accounts.</li> <li>• Has all configuration privileges.</li> </ul>
Auditor	<b>auditor</b> (default)	Has privilege to only view audit logs.
Account manager	Created by the admin user.	Has the privileges of the operator and user only
Operator	Created by the admin or account manager	<ul style="list-style-type: none"> <li>• Has no privileges to configure accounts, account login parameters, or API accounts.</li> <li>• Has no privilege to view audit logs.</li> <li>• Other configuration privileges are supported.</li> </ul>
User	Created by the admin user or account manager	<ul style="list-style-type: none"> <li>• Has privileges to view the data center, policy configuration, assets, and the system.</li> <li>• Has no privilege to view audit logs.</li> <li>• Has no privilege to configure policies.</li> </ul>

### 1.3.1.2 Web Login

Before login, ensure that UTS is properly connected to the network.

Open a browser and access the IP address of the management port via HTTPS, for example, **https://192.168.1.1**. After accepting prompted risks, you are directed to the web login page. Type a correct user name and password, and click **Log In**.

Upon the initial login, you are required to import a license file. See [Getting Started](#).

### 1.3.1.3 Layout of the Web-based Manager

The layout of the web-based manager is shown in [Figure 1-4](#).


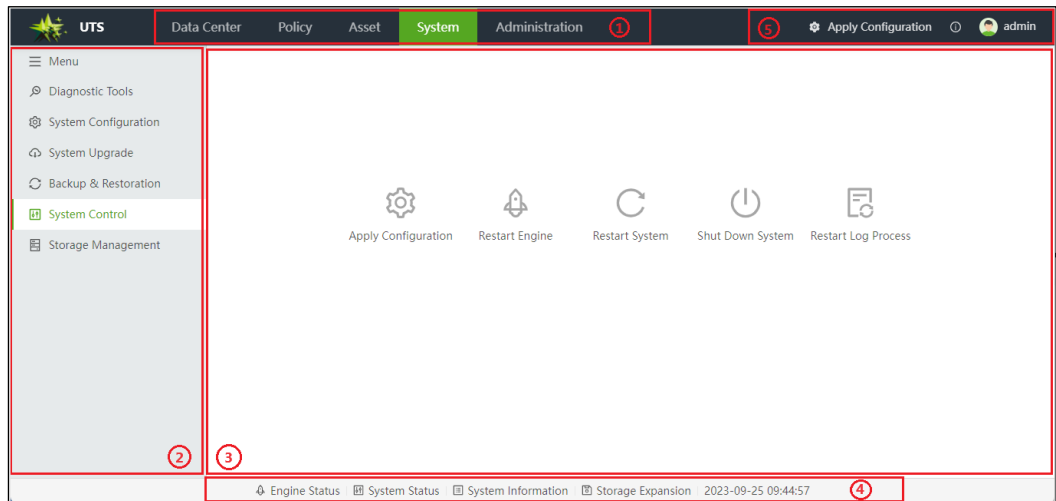

 <b>Note</b>	The menus and the work area vary with user privileges.
--	--

Figure 1-4 Layout of the web-based manager



No.	Area	Description
①	Level 1 menu bar	Top function menu bar
②	Level 2/Level 3 menu bar	Secondary/Tertiary function menu bar. Click  to hide the secondary/tertiary menu text and only display the secondary menu icons. Click  again to restore the complete level 2/level 3 menu bar.
③	Work area	Area where you can perform configurations and operations and view data.
④	Status bar	<p>Displays information about the system operation status in real time.</p> <ul style="list-style-type: none"> <li><b>Engine Status:</b> displays whether the engine is functioning properly.</li> <li><b>System Status:</b> displays the CPU usage, memory usage, as well as the usages and total capacities of the system space, raw log space, session-based storage space, and backup space.</li> <li><b>System Information:</b> displays the engine version, intrusion detection rule version, web application rule version, threat intelligence rule version, antivirus detection package version, system license status, device hash value, remote assistance status, device name, device location, and uptime.</li> <li><b>Storage Expansion:</b> displays information about the mounted extended storage servers.</li> <li>Time: displays the current system time.</li> </ul>
⑤	Quick access bar	<ul style="list-style-type: none"> <li><b>Remaining Validity Days:</b> displays the remaining validity days of the system license. This information becomes visible when the remaining validity is 30 days until the license expires. Hover the mouse here to display the remaining validity days of each module.</li> <li><b>Apply Configuration:</b> click <b>Apply Configuration</b> to make the configuration take effect.</li> <li>: displays the current system version, technical support, and end-user license agreement.</li> <li>: displays the current login account. Hover the mouse over the account to perform one of the following operations.</li> </ul>

No.	Area	Description
		<ul style="list-style-type: none"> <li>✓ <b>Change password:</b> changes the login password of the current account. <b>Change time zone:</b> changes the time zone of the current account.</li> <li>✓ <b>Logout:</b> logs out of the web-based manager.</li> </ul> <p> <b>Note</b></p> <ul style="list-style-type: none"> <li>• For security concern, you are advised to click <b>Logout</b> to log out of the web-based manager.</li> <li>• If the remaining license validity days are displayed, contact NSFOCUS for a new license and import it in time. Otherwise, the device will not function properly once the validity expires. Before the new license is imported, a message appears on the web-based manager every time you log in, reminding you that the license will expire soon.</li> </ul>

## 1.3.2 Console-based Management

You can log in to the console-based management interface of UTS via the console port. The console-based management interface provides certain functions such as initial system configuration, status detection, and initial configuration restoration. Some functions that are unavailable on the web-based manager can be performed via the console port.

- For details on the default console user name and password, see [Default Accounts](#) and [Communication Parameters of the Console Port](#).
- For information on how to log in to the UTS console-based management interface and perform configurations, see [Console-based Management](#).

## 1.3.3 SSH-based Management

In addition to the web-based manager and console-based management, you can perform remote management of UTS via SSH through certain management software, such as SecureCRT and PuTTY. Contact NSFOCUS technical support for the user name and password of the SSH administrator. Use SSH management under the guidance of the technical support personnel.



# 2 Getting Started

---

To get started on the UTS web-based manager, you are required to perform the following configurations:

- Step 1** Check that the management host communicates properly with UTS. (Open port 443 if the traffic needs to go through a firewall).
- Step 2** Open your browser and access UTS via HTTPS by typing the management IP address of UTS, for example, **https://192.168.1.1**, in the address bar.
- Step 3** Click **Advanced** and click **Proceed to IP address (unsafe)** to jump to the login page of the UTS web-based manager.
- Step 4** Type a correct user name and password and click **Log In**.

Upon the initial login, use the default **admin** account. For the initial administrator account and password, see [Default Accounts](#).

- Step 5** When you log in to the UTS web-based manager with the default password for the first time, the system will force a password change. Change the password, and click **OK**.
- Step 6** Import a license.

After you log in again with the changed password, the **Import License** dialog box pops up, as shown in [Figure 2-1](#). You are required to import a correct license file before continuing to use this device.

UTS supports two license authorization modes:

- a. Local authorization

As shown in [Figure 2-1](#), select **Local authorization**. After choosing the correct license file, click **OK** to import the license. Then click **OK** in the displayed dialog box, as shown in [Figure 2-2](#).

Figure 2-1 License authorization dialog box

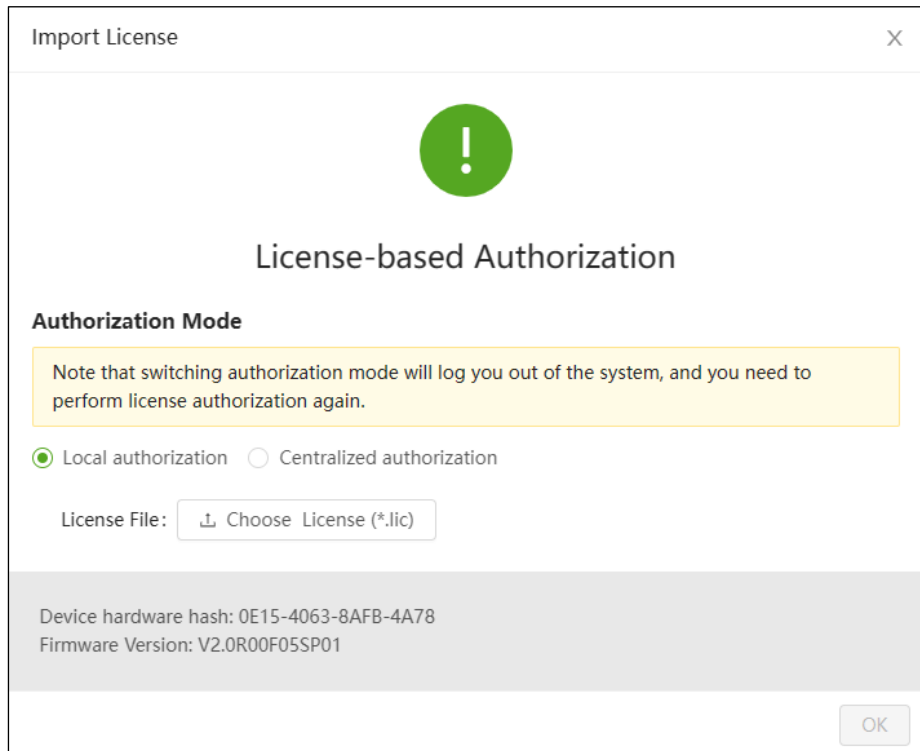
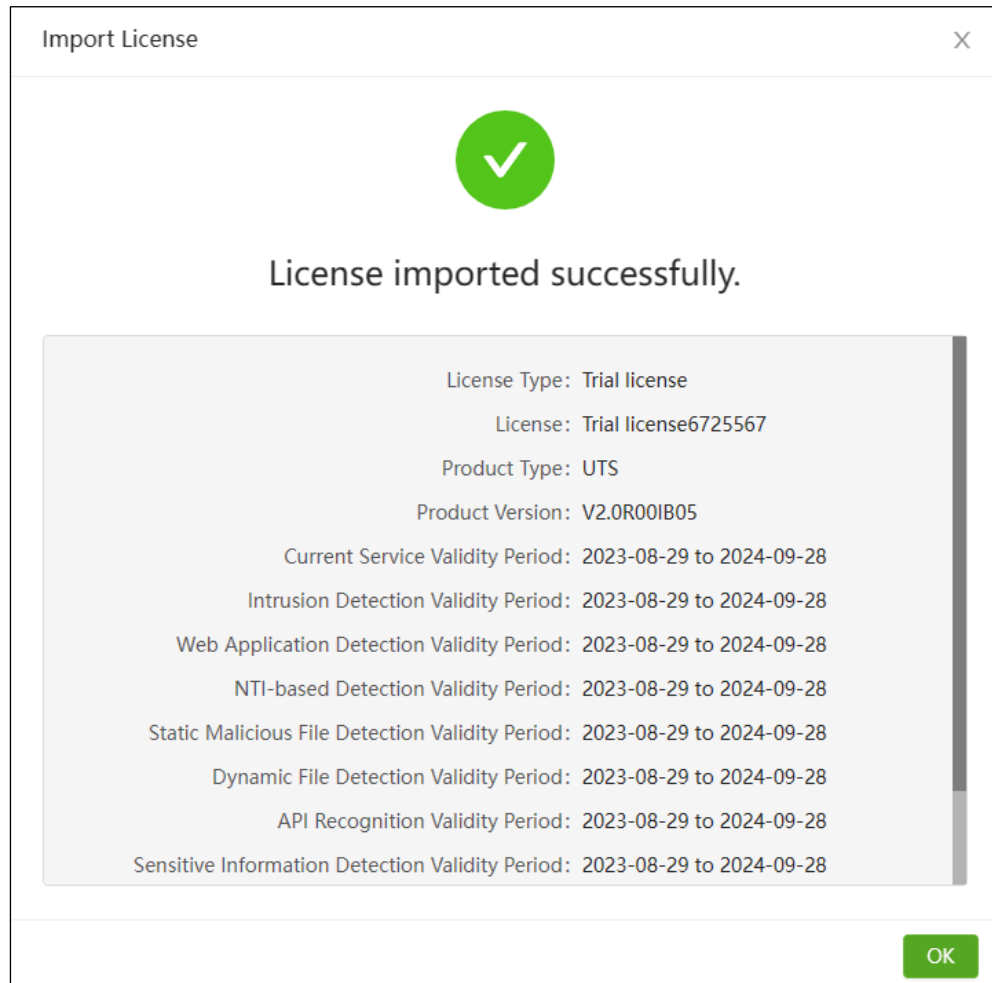


Figure 2-2 Prompt of license imported successfully




b. Centralized authorization

As shown in [Figure 2-1](#), select **Centralized Authorization**. Type the address and port of NSFOCUS Enterprise Security Platform (ESP-C) and click **OK**. Then UTS will collaborate with ESP-C for authorization. After ESP-C issues an authorization license to UTS, refresh the UTS page and log in to it, as shown in [Figure 2-3](#).

Figure 2-3 Centralized authorization dialog box

Import License





License-based Authorization

**Authorization Mode**


Local authorization   
  Centralized authorization

**Authorization Device Information**

\* HOST :

\* Port :

This product is ready for use after the authorization license is imported.  
 Use NSFOCUS Enterprise Security System (ESP-C) to perform centralized authorization. You need to provide ESPC information.  
 Device Hardware Hash: B438-2E06-E2B7-3734  
 Firmware Version: V2.0R00IB05

 <b>Note</b>	<ul style="list-style-type: none"> <li>Before login, check whether the check box of blocking pop-ups or disabling JavaScript is selected in your browser. If yes, deselect the check box.</li> <li>You are advised to use the latest Chrome browser or Firefox browser and set the screen resolution to 1024 x 768 or higher.</li> <li>When using this device for the first time, you can use the default administrator account to log in.</li> </ul>
--	---

----End

# 3 Data Center

This chapter contains the following topics:

Topic	Description
<a href="#">Threat Analysis</a>	Describes how to view threat events.
<a href="#">Metadata Log</a>	Describes how to view metadata logs.
<a href="#">Full Traffic Forensics</a>	Describes how to perform full traffic forensics.



By default, all data from the past 24 hours is displayed in the data center. You can set query criteria to filter data.

- Specify the query criteria at the top of the page.
- For more precise filtering, click **Advanced Search** and use more query criteria.
- Click **Reset** to clear all current query criteria.

## 3.1 Threat Analysis

After merging alert logs and events, UTS displays the statistical results of threat analysis from different perspectives under **Data Center > Threat Analysis**.

### 3.1.1 Threat Event Analysis

Choose **Data Center > Threat Analysis > Threat Event** to view threat event information. By default, the threat event page displays various threat events generated in the past 24 hours, as shown in [Figure 3-1](#). You can specify time ranges.

Figure 3-1 Threat event analysis

First Discovered	Last Discovered	Src IP	Dst IP	Alert Name	Alert Type	Rule ID	Threat Frequency	Operation
2023-09-22 17:45:18	2023-09-22 17:45:18	10.67.9.26	10.67.10.202	XPath injection xpath_injection	System service scan	3145730	Low	<a href="#">Details</a>
2023-09-22 17:42:39	2023-09-22 17:42:39	10.67.9.26	10.67.10.207	Illegal upload	Upload vulnerability	0	Low	<a href="#">Details</a>

Table 3-1 describes information in the threat event list.

Table 3-1 Description of the threat event list

Parameter	Description
First Discovered	Time when this event was first reported.
Last Discovered	Time when this event was last reported.
Src IP	Attack source IP address of this event.
Dst IP	Attack destination IP address of this event.
Alert Name	Name of the alert triggered by this event.
Alert Type	Type of alert triggered by this event.
Rule ID	ID of the rule that matches this alert. Click the ID to view the rule details. For alerts generated by intranet scanning, DGA alerts, phishing emails, covert channels, routing protocols, 5G security, or attacks, it is not supported to view rule details.
Threat Frequency	Probable frequency at which the threat occurs in a specified time range.
Occurrences	Number of event occurrences
Severity	Alert level of this event.
Attack Result	Attack result of this event.
Attack Stage	Kill chase stage of this event.
Operation	Click <b>Details</b> to view the details of the event. See <a href="#">Viewing Threat Event Details</a> .

## Viewing Threat Event Details

In the event details page, you can perform the following operations:

- View associated alert information.  
Click the text link in the **Alert Details** column to view the content of the alert hitting the alert signature.
- Query raw alert logs.  
Click **Details** in the **Operation** column to view the details of the alert log associated with the event.

## Downloading/Clearing Logs

- Click **Download Logs** to export the threat event information in the current list to an Excel file.
- Click **Clear Logs** to clear the threat event information in the current list.

## 3.2 Metadata Log

Choose **Data Center > Metadata Log** to view the logs generated when UTS restores packets of various protocols and files. By default, only session logs and HTTP logs are displayed, as shown in [Figure 3-2](#).

Figure 3-2 Metadata log (session log)

Time	Src IP/Port	Dst IP/Port	Application Protocol	Uplink Traffic	Downlink Traffic	Uplink Packets	Downlink Packets	Operation
2023-09-25 10:51:09	10.68.5.105/40152	10.68.5.102/143	IMAP	134Bytes	183.47KBytes	36 Packets	137 Packets	Details PCAP forensics
2023-09-25 10:51:08	10.68.5.105/8827	10.68.5.105/80	HTTP	544Bytes	17.71KBytes	7 Packets	15 Packets	Details PCAP forensics
2023-09-25 10:51:07	10.66.30.106/61496	10.66.250.142/5920	SSH	2.42KBytes	6.07KBytes	22 Packets	25 Packets	Details PCAP forensics
2023-09-25 10:51:00	10.245.25.149/4500	222.97.145.240/4500	NonIP	254.47KBytes	305.78KBytes	766 Packets	869 Packets	Details PCAP forensics

## Configuring Metadata Log Display Settings

At the top of the page as shown in [Figure 3-2](#), only the **Session Log** and **HTTP Log** tabs are displayed by default. Click + to add new metadata log category tabs and then click **OK**. The selected metadata log category tabs appear on the page. [Table 3-2](#) describes metadata log display parameters.

Click a log category tab to view the corresponding log information and perform related operations.

Table 3-2 Parameters for configuring metadata log display settings

Parameter	Description
Log Category	At least one log category should be selected.
Log Classification	You can select a log classification to quickly display all log categories under the classification. Multiple log classifications can be selected simultaneously.

## Viewing Metadata Log Display Content

After setting the metadata log display parameters, click a specific log category tab to view the corresponding log list.

### Session Log

[Table 3-3](#) describes parameters in the session log.

Table 3-3 Description of the session log list

Parameter	Description
Time	Session log generation time.
Src IP/Port	Source IP and source port number of the session log.
Dst IP/Port	Destination IP and destination port number of the session log.
Application Protocol	Application layer protocol.
Uplink Traffic	Length of the payload information in the received message in this session.
Downlink Traffic	Length of the payload information in the sent message in this session.
Uplink Packets	Number of messages received by this session.
Downlink Packets	Number of messages sent by this session.
Device Hash	This parameter is displayed only when UTS is set to work in master node mode. When the slave UTS sends logs to the master UTS, this field is displayed in the logs on the master UTS. You can learn about the log source based on the device hash.
Operation	<ul style="list-style-type: none"> <li>• <b>Details:</b> Click to view the details of the log.</li> <li>• <b>PCAP forensics:</b> Click to download the PCAP file for this log. Before downloading, check that <b>Full Flow Storage</b> is enabled. For details, see <a href="#">Traffic Storage</a>.</li> </ul>

## HTTP Log

[Table 3-4](#) describes parameters in the HTTP metadata log list.

Table 3-4 Description of the HTTP metadata log list

Parameter	Description
Time	HTTP log generation time.
Src IP/Port	Source IP and source port number of the HTTP log.
Dst IP/Port	Destination IP and destination port number of the HTTP log.
Request Method	HTTP request method.
HOST	Host in the HTTP request.
URI	URI in the HTTP request.
User Agent	User agent in the HTTP request.
Device Hash	This parameter is displayed only when UTS is set to work in master node mode. When the slave UTS sends logs to the master UTS, this field is displayed in the logs on the master UTS. You can learn about the log source based on the device hash.
Operation	The operation method is basically the same as that of the session log. For details, see <a href="#">Operation (Session Log)</a> .



## Email Log

Table 3-5 describes parameters in the email log list.

Table 3-5 Description of the email metadata log list

Parameter	Description
Time	Email log generation time.
Src IP/Port	Source IP and source port number of the email log.
Dst IP/Port	Destination IP and destination port number of the email log.
Sender	Sender's email address.
Recipient	Recipient's email address.
CC Recipient	Recipients that receive a copy of the email.
Email Subject	Subject of the email.
Email Body	Message body of the email.
Attachment	Name of the attachment in the email.
Device Hash	This parameter is displayed only when UTS is set to work in master node mode. When the slave UTS sends logs to the master UTS, this field is displayed in the logs on the master UTS. You can learn about the log source based on the device hash.
Operation	The operation method is basically the same as that of the session log. For details, see <a href="#">Operation (Session Log)</a> .

## Telnet Log

Table 3-6 describes parameters in the Telnet metadata log list.

Table 3-6 Description of the HTTP metadata log list

Parameter	Description
Time	Telnet log generation time.
Src IP/Port	Source IP and source port number of the Telnet log.
Dst IP/Port	Destination IP and destination port number of the Telnet log.
Application Protocol	Application layer protocol.
Command	Telnet command name.
User Name	Telnet login user name.
Direction	Indicates the transfer direction of data. <ul style="list-style-type: none"> <li>If only the source IP matches an internal network object, the transfer direction is <b>Internal to external</b>.</li> </ul>

Parameter	Description
	<ul style="list-style-type: none"> <li>If only the destination IP matches an internal network object, the transfer direction is <b>External to internal</b>.</li> <li>If neither the source IP nor destination IP match internal network objects, the transfer direction is <b>Internal to internal</b>.</li> <li>If neither the source IP nor destination IP do not match any internal network object, the transfer direction is <b>External to external</b>.</li> </ul>
Device Hash	This parameter is displayed only when UTS is set to work in master node mode. When the slave UTS sends logs to the master UTS, this field is displayed in the logs on the master UTS. You can learn about the log source based on the device hash.
Operation	The operation method is basically the same as that of the session log. For details, see <a href="#">Operation (Session Log)</a> .

## Authentication Log

[Table 3-7](#) describes parameters in the authentication log list.

Table 3-7 Description of the authentication log list

Parameter	Description
Time	Authentication log generation time.
Src IP/Port	Source IP and source port number of the authentication log.
Dst IP/Port	Destination IP and destination port number of the authentication log.
User Name	User name for LDAP authentication.
Command	Records the interaction process during LDAP authentication.
Device Hash	This parameter is displayed only when UTS is set to work in master node mode. When the slave UTS sends logs to the master UTS, this field is displayed in the logs on the master UTS. You can learn about the log source based on the device hash.
Operation	The operation method is basically the same as that of the session log. For details, see <a href="#">Operation (Session Log)</a> .

## Database Log

[Table 3-8](#) describes parameters in the database log list.

Table 3-8 Description of the database log list

Parameter	Description
Time	Database log generation time.

Parameter	Description
Src IP/Port	Source IP and source port number of the database log.
Dst IP/Port	Destination IP and destination port number of the database log.
Application Protocol	Application layer protocol.
User Name	Database user name.
Database Type	Database type.
Database Name	Database name.
Database Operation	Records SQL statements executed.
Device Hash	This parameter is displayed only when UTS is set to work in master node mode. When the slave UTS sends logs to the master UTS, this field is displayed in the logs on the master UTS. You can learn about the log source based on the device hash.
Operation	The operation method is basically the same as that of the session log. For details, see <a href="#">Operation (Session Log)</a> .

## Login Log

[Table 3-9](#) describes parameters in the login log list.

Table 3-9 Description of the login log list

Parameter	Description
Time	Login time.
Src IP/Port	Source IP and source port number of the login user.
Dst IP/Port	Destination IP and destination port number of the login user.
User Name	Login user name
Login Result	Login result.
Device Hash	This parameter is displayed only when UTS is set to work in master node mode. When the slave UTS sends logs to the master UTS, this field is displayed in the logs on the master UTS. You can learn about the log source based on the device hash.
Operation	The operation method is basically the same as that of the session log. For details, see <a href="#">Operation (Session Log)</a> .

## SSL&TLS Log

[Table 3-10](#) describes parameters in the SSL&TLS metadata log list.

Table 3-10 Description of the SSL&amp;TLS metadata log list

Parameter	Description
Time	SSL&TLS log generation time.
Src IP/Port	Source IP and source port number of the SSL&TLS log.
Dst IP/port	Destination IP and destination port number of the SSL&TLS log.
Certificate Name	The SSL name of the certificate.
Certificate Content	Content of the SSL certificate.
Certificate Issuer	SSL certificate issuer.
Device Hash	This parameter is displayed only when UTS is set to work in master node mode. When the slave UTS sends logs to the master UTS, this field is displayed in the logs on the master UTS. You can learn about the log source based on the device hash.
Operation	The operation method is basically the same as that of the session log. For details, see <a href="#">Operation (Session Log)</a> .

## FTP Log

[Table 3-11](#) describes parameters in the FTP metadata log list.

Table 3-11 Description of the FTP metadata log list

Parameter	Description
Time	FTP log generation time.
Src IP/Port	Source IP and source port number of the FTP log.
Dst IP/port	Destination IP and destination port number of the FTP log.
User Name	FTP user name.
FTP Command	FTP command used.
Device Hash	This parameter is displayed only when UTS is set to work in master node mode. When the slave UTS sends logs to the master UTS, this field is displayed in the logs on the master UTS. You can learn about the log source based on the device hash.
Operation	The operation method is basically the same as that of the session log. For details, see <a href="#">Operation (Session Log)</a> .

## SNS Account Log

[Table 3-12](#) describes parameters in the SNS account log list.

Table 3-12 Description of the SNS account log list

Parameter	Description
Time	SNS account log generation time.
Src IP/Port	Source IP and source port number of the SNS account log.
Dst IP/port	Destination IP and destination port number of the SNS account log.
User Account	User name of the SNS account service user.
Device Hash	This parameter is displayed only when UTS is set to work in master node mode. When the slave UTS sends logs to the master UTS, this field is displayed in the logs on the master UTS. You can learn about the log source based on the device hash.
Operation	The operation method is basically the same as that of the session log. For details, see <a href="#">Operation (Session Log)</a> .

## DNS Log

[Table 3-13](#) describes parameters in the DNS metadata log list.

Table 3-13 Description of the DNS metadata log list

Parameter	Description
Time	DNS log generation time.
Src IP/Port	Source IP and source port number of the DNS log.
Dst IP/Port	Destination IP and destination port number of the DNS log.
Domain Name	Domain name requested in the DNS query.
Answer	Details of the DNS response message.
Answer RRs	Number of response records in the DNS response section.
Authority RRs	Number of authorization records in the DNS authorization section.
Additional RRs	Number of additional resource records.
Device Hash	This parameter is displayed only when UTS is set to work in master node mode. When the slave UTS sends logs to the master UTS, this field is displayed in the logs on the master UTS. You can learn about the log source based on the device hash.
Operation	The operation method is basically the same as that of the session log. For details, see <a href="#">Operation (Session Log)</a> .

## ICMP Log

[Table 3-14](#) describes parameters in the ICMP metadata log list.

Table 3-14 Description of the ICMP metadata log list

Parameter	Description
Time	ICMP log generation time.
Src IP/Port	Source IP and source port number of the ICMP log.
Dst IP/Port	Destination IP and destination port number of the ICMP log.
Reply Type	ICMP reply type.
Reply Code	ICMP reply code.
Request Type	ICMP Request type.
Request Code	ICMP request code.
Device Hash	This parameter is displayed only when UTS is set to work in master node mode. When the slave UTS sends logs to the master UTS, this field is displayed in the logs on the master UTS. You can learn about the log source based on the device hash.
Operation	The operation method is basically the same as that of the session log. For details, see <a href="#">Operation (Session Log)</a> .

## File Restoration Log

[Table 3-15](#) describes parameters in the file restoration metadata log list.

Table 3-15 Description of the file restoration metadata log list

Parameter	Description
Time	File restoration log generation time.
Src IP/Port	Source IP and source port number of the file restoration log.
Dst IP/Port	Destination IP and destination port number of the file restoration log.
File Name	Name of the file to be restored.
File Size (bytes)	File size.
File Type	File type.
MD5 Value	MD5 value of the file to be restored.
Device Hash	This parameter is displayed only when UTS is set to work in master node mode. When the slave UTS sends logs to the master UTS, this field is displayed in the logs on the master UTS. You can learn about the log source based on the device hash.
Operation	The operation method is basically the same as that of the session log. For details, see <a href="#">Operation (Session Log)</a> .

## 5G Log

Table 3-16 describes parameters in the 5G metadata log list.

Table 3-16 5G metadata log list description

Parameter	Description
Time	5G log generation time.
Src IP/Port	Source IP and source port number of the 5G log.
Dst IP/Port	Destination IP and destination port number of the 5G log.
Application Protocol	Application layer protocol.
Interface Type	Interface type.
Src NE Type	Source NE type.
Dst NE Type	Destination NE type.
Process Type Code	Process type code.
Request Status	Request status, which can be success, failure, timeout, or unknown.
Device Hash	This parameter is displayed only when UTS is set to work in master node mode. When the slave UTS sends logs to the master UTS, this field is displayed in the logs on the master UTS. You can learn about the log source based on the device hash.
Operation	The operation method is basically the same as that of the session log. For details, see <a href="#">Operation (Session Log)</a> .



In addition to the preceding metadata logs, UTS can display logs of such protocols as DHCP, SIP, Kerberos, NNTP, NFS, Samba, SSH, RDP, Rlogin, VNC, and MQTT.

## 3.3 Full Traffic Forensics

Under **Full Traffic Forensics**, you can issue a forensics task, delete the task, and download the forensics data file.



After the full traffic storage function is enabled and the storage function is enabled for related applications (for details, see [Traffic Storage](#)), click **PCAP forensics** in the **Operation** column in the metadata log list to issue a forensics task. For details, see Metadata Log. After issuing the task, you can view the task information and download the data file on the **Full Traffic Forensics** page.

### Issuing a Forensics Task

**Step 1** Choose **Data Center > Full Traffic Forensics**.

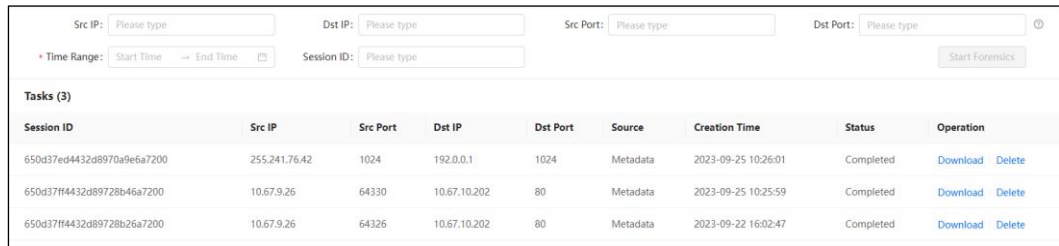
**Step 2** At the top of the page, configure full traffic forensics parameters. [Table 3-17](#) describes parameters for configuring full traffic forensics.

Table 3-17 Parameters for configuring full traffic forensics

Parameter	Description
Src IP/Port	Specifies the source IP and source port number for full traffic forensics.
Dst IP/Port	Specifies the destination IP and destination port number for full traffic forensics.
Time Range	Specifies the start time and end time of the full traffic forensics process.
Session ID	Specifies the ID of the session for full traffic forensics.

**Step 3** Click **Start Forensics** to issue a task, which will be displayed in the task list, as shown in [Figure 3-3](#).

Figure 3-3 Full traffic forensics task



The screenshot shows a configuration form at the top with fields for Src IP, Dst IP, Src Port, Dst Port, Time Range (Start Time to End Time), and Session ID. A 'Start Forensics' button is located to the right of the Session ID field. Below the form is a table titled 'Tasks (3)' with the following columns: Session ID, Src IP, Src Port, Dst IP, Dst Port, Source, Creation Time, Status, and Operation. Three tasks are listed, all with a status of 'Completed' and 'Metadata' as the source.

Session ID	Src IP	Src Port	Dst IP	Dst Port	Source	Creation Time	Status	Operation
650d37ed4432d8970a9e6a7200	255.241.76.42	1024	192.0.0.1	1024	Metadata	2023-09-25 10:26:01	Completed	<a href="#">Download</a> <a href="#">Delete</a>
650d37ff4432d89728b46a7200	10.67.9.26	64330	10.67.10.202	80	Metadata	2023-09-25 10:25:59	Completed	<a href="#">Download</a> <a href="#">Delete</a>
650d37ff4432d89728b26a7200	10.67.9.26	64326	10.67.10.202	80	Metadata	2023-09-22 16:02:47	Completed	<a href="#">Download</a> <a href="#">Delete</a>

---End

## Downloading Forensics Data

Only after the full traffic storage function is enabled and the storage function is enabled for related applications, you can download forensics data corresponding to a protocol. For details, see [Traffic Storage](#).

In the full traffic forensics task list, click **Download** in the **Operation** column for tasks marked as **Completed** to download forensics results.

## Deleting a Forensics Task

In the full traffic forensics task list, click **Delete** in the **Operation** column to delete a task.



# 4 Policies

UTS audits network traffic based on policies, which comprise different sets of rules. The device matches data flowing through it against related rules in real time to monitor whatever is happening in the network. In the Policy module, you can configure and manage various policies and rules.

This chapter contains the following topics:

Topic	Description
<a href="#">Threat Detection</a>	Describes how to configure policies for detecting various threats.
<a href="#">Rule Configuration</a>	Describes how to configure rules for detecting intrusion, web application threats, and other threats, and how to configure custom rules, custom protocol rules, and rule templates.
<a href="#">Restoration Configuration</a>	Describes how to restore metadata and files of different protocols and applications, and how to enable detection and storage of different types of 5G logs.
<a href="#">Traffic Management</a>	Describes how to enable traffic storage and how to configure an allowlist and suspicious list.
<a href="#">SSL Configuration</a>	Describes how to configure SSL connections and manage SSL certificates.
<a href="#">Alert Allowlist</a>	Describes how to configure an alert allowlist.
<a href="#">Out-of-Path Blocking</a>	Describes how to configure an out-of-path blocking policy and a custom blocking policy.

## 4.1 Threat Detection

Besides conventional detection of intrusion and web application attacks, UTS can detect distributed denial-of-service (DDoS) attacks, scans/brute force attacks, advanced threats, 5G threats, and other threats.

### 4.1.1 Basic Detection

On UTS, basic detection policies can be configured to detect intrusion and web application threats. After detecting threats, UTS generates log messages. If UTS is connected to NSFOCUS Intelligent Security Operations Platform (ISOP) for collaboration, these log messages will also be sent to ISOP.

### 4.1.1.1 Intrusion Detection Policy

UTS can detect known attacks, unknown attacks, and various hacker attacks, including the following:

- Buffer overflow
- SQL injection
- Brute-force guessing
- DoS
- Scan detection
- Unauthorized access
- Worm and virus
- Botnet

After detecting intrusion behavior, UTS generates intrusion alerts.

Choose **Policy > Threat Detection > Basic > Intrusion Detection**. Intrusion detection is disabled by default. To enable this function, turn on **Intrusion Detection & Alert** and then click **Apply Configuration** in the upper-right corner of the page. Then UTS will detect intrusion behavior by checking traffic against built-in rules.

If out-of-path blocking is enabled and **Intrusion detection, alerting, and blocking** is selected, UTS will take actions specified in related intrusion detection rules against intrusion connections.



Note

- For details about intrusion detection rules and the configuration method of actions in such rules, see [Intrusion Detection Rules](#).
- For the configuration method of out-of-path blocking policies, see [Out-of-Path Blocking Policies](#).

### 4.1.1.2 Web Threat Detection Policy

UTS can detect web application threats from HTTP and HTTPS traffic. For HTTPS traffic inspection, you must configure a Secure Sockets Layer (SSL) certificate under **Policy > SSL Configuration**.

Web application threats can be detected in the following ways:

- Rule-based detection  
UTS detects web application threats by matching web traffic with its built-in web application rules. When finding a match, UTS generates a web application threat alert. If out-of-path blocking is enabled and **Web application detection, alerting, and blocking** is selected, UTS will take actions specified in related detection rules of web application threats against attacking connections.
- Algorithm-based detection  
UTS detects web application threats based on built-in algorithms. When finding a match, it generates a web application threat alert.

To configure rules for detecting web application threats, follow these steps:


**Step 1** Choose **Policy > Threat Detection > Basic > Web Threat Detection**.

Web application threat detection is enabled by default.

**Step 2** In the **Basic Configuration** area, set basic parameters.

- a. After configuring parameters, click **OK** to commit the settings.
- b. The engine automatically restarts.

Table 4-1 Basic configuration parameters for detecting web application threats

Parameter	Description
Rule-based Detection	Specifies one or more rule types for detecting web application threats. UTS will detect web application threats based on the selected rule types.
Algorithm-based Detection	Specifies one or more algorithm types for detecting web application threats. UTS will detect web application threats based on the selected algorithm types.   <b>Note</b>  The types of algorithm-based detection selected here determine which functions can be edited in the <b>Advanced Configuration</b> area. That is to say, if a type of algorithm-based detection is not selected here, the related function in the <b>Advanced Configuration</b> area cannot be edited.

**Step 3** (Optional) Set advanced parameters.

- a. After configuring parameters, click **OK** to commit the settings.
- b. Click **Apply Configuration** in the upper-right corner to make the settings take effect.

Table 4-2 Advanced configuration parameters for detecting web application threats

Parameter	Description	
Illegal Upload	<b>File Type:</b> specifies one or more file types prohibited from being uploaded.  When detecting a specified type of file being uploaded, UTS generates an alert.	
Illegal Download	<b>File Type:</b> specifies one or more file types prohibited from being downloaded.  When detecting a specified type of file being downloaded, UTS generates an alert.	
Scan Detection	Fingerprint Recognition	After this is enabled, UTS will check for scanners by matching traffic data with the built-in fingerprint database.
	Alerts per Second	Specifies the maximum number of alerts allowed per second. When this threshold is reached, UTS determines that an attack is taking place. The value range is 10–100.



- For details about detections rules of web application threats and the configuration method of actions in such rules, see [Web Application Threat Detection Rules](#).
- For the configuration method of out-of-path blocking policies, see [Out-of-Path Blocking Policies](#).

---End

## 4.1.2 DDoS Detection

On UTS, you can configure DDoS detection policies to detect flood, ping sweep, Address Resolution Protocol (ARP) spoofing, HTTP flood, and port scan attacks.

DDoS detection is disabled by default. After it is enabled, UTS will check for DDoS attacks and, upon detecting such an attack, will generate an intrusion alert.

### 4.1.2.1 Flood Detection Policy

In a flood attack, an attacker initiates a large number of fake requests to the target. The attack target exhausts its resources to process these fake requests and therefore fails to process legitimate ones. This causes denial-of-service conditions.

Using flood detection policies, UTS can effectively detect main flood attacks, including ping, User Datagram Protocol (UDP), SYN, Domain Name System (DNS) reply, and DNS request flood attacks.

Choose **Policy > Threat Detection > DDoS > Flood**. Turn on the detection function, configure parameters, and click **OK**. Then click **Apply Configuration** in the upper-right corner to make the settings take effect. The following table describes parameters for configuring a flood detection policy.

Table 4-3 Parameters for configuring a flood detection policy

Parameter	Description
Detection Threshold	Specifies the minimum number of packets to trigger an alert. When detecting that the number of packets sent to a target host reaches or exceeds this threshold in a detection period, UTS deems that a flood attack is ongoing. The value range is 1–99999999, in packets.
Detection Period	Specifies the period of time for UTS to detect flood attacks. The value should be an integer ranging from 1 to 99999999, in seconds.
Reset Period	Specifies the interval at which UTS clears detection data and starts a new round of detection. The value should be an integer ranging from 1 to 99999999, in seconds.

### 4.1.2.2 Ping Sweep Detection Policy

In a ping sweep attack, an attacker tries to discover live hosts on a network by sending Internet Control Message Protocol (ICMP) echo requests to multiple hosts. The purpose is to find out services provided by and potential vulnerabilities in live hosts, thereby preparing for further intrusion.

Choose **Policy > Threat Detection > DDoS > Ping Sweep**. The configuration method of ping sweep detection is similar to that of flood detection policies. For details, see [Flood Detection Policy](#).

### 4.1.2.3 ARP Spoofing Detection Policy

In an ARP spoofing attack, an attacker implements ARP spoofing via forged IP addresses and media access control (MAC) addresses. This kind of attacks causes network instability, or

worse, interruption. In addition, the attacker can further launch man-in-the-middle (MITM) attacks to steal user names and passwords for access to online gaming, online banking, and file services.

Choose **Policy > Threat Detection > DDoS > ARP Spoofing**. The configuration method of ARP spoofing detection is similar to that of flood detection policies. For details, see [Flood Detection Policy](#).

#### 4.1.2.4 HTTP Flood Detection Policy

With appropriate HTTP flood detection policies configured, UTS can effectively detect HTTP GET and POST flood attacks.

Choose **Policy > Threat Detection > DDoS > HTTP Flood**. The configuration method of HTTP flood detection is similar to that of flood detection policies. For details, see [Flood Detection Policy](#).

#### 4.1.2.5 Port Scan Detection Policy

In a port scan attack, an attacker scans TCP or UDP ports on target hosts to identify services running on these hosts for further intrusion. Port scanning detection policies allow UTS to prevent TCP and UDP port scans.

Choose **Policy > Threat Detection > DDoS > Port Scan**. The configuration method of port scan detection is similar to that of flood detection policies. For details, see [Flood Detection Policy](#).

### 4.1.3 Scanning and Brute Force Detection

UTS can detect brute-force cracking, host scans, and anomalous behavior.

#### 4.1.3.1 Brute Force Detection Policy

UTS can detect brute-force attacks on File Transfer Protocol (FTP), email, HTTP, database, and other applications. When detecting such an attack, UTS generates an intrusion alert.

The brute force detection function is enabled by default.



Besides enabling brute force detection here, you should select **Alert** for brute force detection rules under **Policy > Rule Configuration > Rule Management > Intrusion Detection**. For example, for detection of brute-force cracking against the Telnet application, you must select the **Alert** action for rule 30473.

Choose **Policy > Threat Detection > Scan & Brute Force > Brute Force**. The brute force detection function is enabled by default. Configure parameters, click **OK**, and then click **Apply Configuration** in the upper-right corner to make the settings take effect. The following table describes brute force detection parameters.

Table 4-4 Brute force detection parameters

Parameter	Description
Failed Login Attempt Threshold	Within a detection period, when the number of login attempts reaches or exceeds the threshold specified here, UTS generates a brute force alert.

Parameter	Description
	The value range is 1–65535, with <b>10</b> as the default.
Detection Period	Specifies the period of time for brute force detection. The value range is 1–65535, in seconds, with <b>1</b> as the default.

### 4.1.3.2 Host Scanning Detection Policy

UTS allows you to configure detection of intranet host scans. After configuration, when detecting such a scan, UTS generates an intrusion alert.

Choose **Policy > Threat Detection > Scan & Brute Force > Host Scan**. Turn on the host scan detection function, configure parameters, and click **OK**. Then click **Apply Configuration** in the upper-right corner to make the settings take effect. The following table describes host scan detection parameters.

Table 4-5 Host scan detection parameters

Parameter	Description
Statistical Period	Specifies the period of time for detecting host scanning from a source IP address. If a threshold is reached or exceeded within a statistical period, UTS, at the end of the period, determines that a host scan is taking place. After that, the next statistical period starts. The value range is 1–999999999, in seconds.
Netmask Filter	Specifies the netmask of hosts. UTS checks whether a host scan is ongoing only when the netmask of hosts matches this value. The scanned hosts and the scanner must be on the same network segment, which is represented with the network filter specified here, to trigger host scan detection. To disable this filter, set it to <b>0.0.0.0</b> .
ARP Threshold/ARP Dst IP Threshold	Within a statistical period, if the hosts match the netmask filter (not <b>0.0.0.0</b> ) and the number of ARP packets and that of destination IP addresses in these packets both reach or exceed the thresholds, UTS generates a host scan alert. <ul style="list-style-type: none"> <li>• <b>ARP Threshold</b>: minimum number of ARP packets to trigger an alert. The value range is 1–65535.</li> <li>• <b>ARP Dst IP Threshold</b>: minimum number of different destination IP addresses in ARP packets to trigger an alert. The value range is 1–256.</li> </ul>
ICMP Threshold/ICMP Dst IP Threshold	Within a statistical period, if the hosts match the netmask filter (not <b>0.0.0.0</b> ) and the number of ICMP packets and that of destination IP addresses in these packets both reach or exceed the thresholds, UTS generates a host scan alert. <ul style="list-style-type: none"> <li>• <b>ICMP Threshold</b>: minimum number of ICMP packets to trigger an alert. The value range is 1–65535.</li> <li>• <b>ICMP Dst IP Threshold</b>: minimum number of different destination IP addresses in ICMP packets to trigger an alert. The value range is 1–256.</li> </ul>
SYN Threshold/SYN Dst IP Threshold/SYN Dst Port Threshold	Within a statistical period, if the hosts match the netmask filter (not <b>0.0.0.0</b> ) and the number of SYN packets, that of destination IP addresses, and that of destination ports in these packets all reach or exceed the thresholds, UTS generates a host scan alert. <ul style="list-style-type: none"> <li>• <b>SYN Threshold</b>: minimum number of SYN packets to trigger an alert. The value range is 1–65535.</li> </ul>

Parameter	Description
	<ul style="list-style-type: none"> <li>• <b>SYN Dst IP Threshold:</b> minimum number of different destination IP addresses in SYN packets to trigger an alert. The value range is 1–256.</li> <li>• <b>SYN Dst Port Threshold:</b> minimum number of different destination ports in SYN packets to trigger an alert. The value range is 1–256.</li> </ul>

### 4.1.3.3 Anomalous Behavior Detection Policy


UTS provides the following types of anomalous behavior detection. When detecting such anomalous behavior, UTS generates an intrusion alert.



- **TCP port detection**  
UTS counts the number of SYN packets sent externally from an intranet to determine whether intranet hosts are zombies controlled by an attacker.
- **UDP port detection**  
UTS counts the number of UDP packets sent externally from an intranet to determine whether intranet hosts are zombies controlled by an attacker.
- **Encrypted proxy detection**  
UTS checks encrypted proxy traffic for anomalous behavior, such as use of a proxy server to access websites blocked by the GFW.

Choose **Policy > Threat Detection > Scan & Brute Force > Anomalous Behavior**.

Anomalous behavior detection switches are off by default. Turn on these switches, configure parameters, and click **OK** in respective areas. Then click **Apply Configuration** in the upper-right corner to make the settings take effect. The following table describes anomalous behavior detection parameters.

Table 4-6 Anomalous behavior detection parameters

Parameter		Description
TCP Port Detection	Enable	Controls whether to enable detection of anomalous behavior related to TCP ports.
	Detection Threshold	Minimum number of SYN packets to trigger an alert. When detecting that the number of SYN packets sent externally by an intranet host reaches or exceeds the threshold set here in a detection period, UTS suspects that the host is a zombie and generates an anomalous behavior alert. The value range is 1–999999999, in packets.
	Detection Period	Period of time for detecting anomalous behavior related to TCP ports. The value range is 1–999999999, in seconds.
	IP Object	Specifies one or more IP objects for TCP port detection, including network segments, nodes, and IP pools. For information on how to configure IP objects on an intranet, see <a href="#">Network Segment</a> , <a href="#">Node</a> , and <a href="#">IP Pool</a> .   <b>Note</b> This field can be left empty, but cannot be 0.0.0.0.
UDP Port	Enable	Controls whether to enable detection of anomalous behavior related to UDP ports.

Parameter		Description
Detection	Detection Threshold	Minimum number of UDP packets to trigger an alert. When detecting that the number of UDP packets sent externally by an intranet host reaches or exceeds the threshold set here in a detection period, UTS suspects that the host is a zombie and generates an anomalous behavior alert. The value range is 1–999999999, in packets.
	Detection Period	Period of time for detecting anomalous behavior related to UDP ports. The value range is 1–999999999, in seconds.
	IP Object	Specifies one or more IP objects for UDP port detection, including network segments, nodes, and IP pools. For information on how to configure IP objects on an intranet, see <a href="#">Network Segment</a> , <a href="#">Node</a> , and <a href="#">IP Pool</a> .   <b>Note</b>  This field can be left empty, but cannot be 0.0.0.0.
	Service	Specifies one or more service objects for UDP port detection, which are combinations of the source port, destination port, and protocol. For information on how to configure a service object, see <a href="#">Port</a> .
Encrypted Detection	Proxy	Controls whether to enable detection of anomalous behavior related to encrypted proxy traffic.   <b>Note</b>  If the detection rate is unacceptably low, you should tune up the <b>Encrypted Traffic Sampling Ratio</b> value under <b>System &gt; System Configuration &gt; Special Parameters</b> . A higher value promises a higher rate of detection. Modifying settings of special parameters may cause system or network exceptions. You are advised to modify these parameters under the guidance of NSFOCUS technical personnel.

## 4.1.4 Advanced Threat Detection

UTS provides NTI-based detection and other advanced detection functions against the following threats:

- Malicious file
- Phishing email
- Covert channel
- DGA domain name
- Web shell

### 4.1.4.1 Threat Intelligence-based Detection Policy

UTS can detect attacks based on threat intelligence from the following sources. When detecting an attack, it generates a threat intelligence alert.

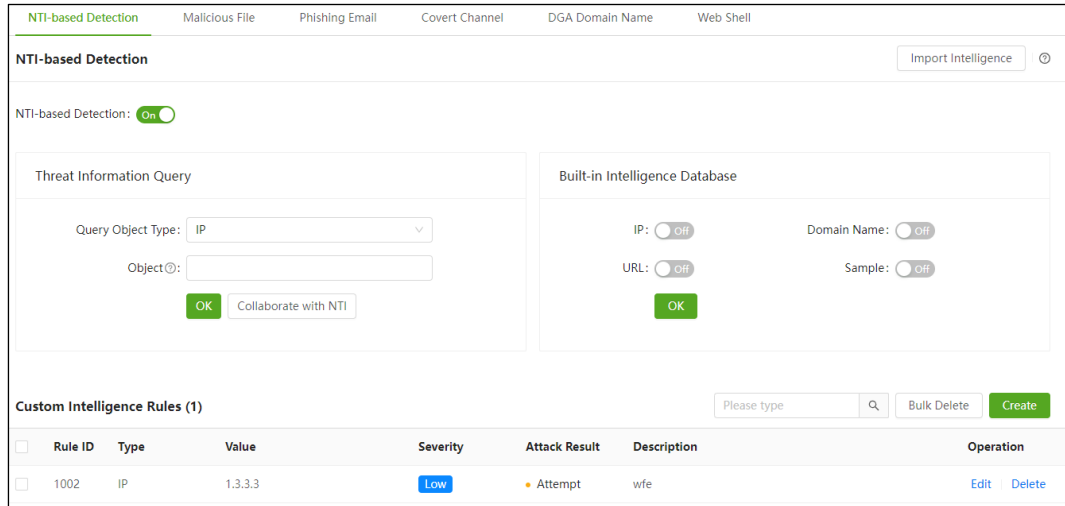
- Intelligence database: UTS does not come with the intelligence database. You need to ask NSFOCUS technical support for the intelligence database file and then import it to UTS. For information on how to import the file, see [Offline Upgrade](#).
- Custom intelligence: refers to threat intelligence manually created by users.



Custom intelligence has a higher priority than the intelligence database. Custom intelligence rules should be enabled before being used for threat detection. After hitting a custom intelligence rule, the traffic will not be checked again against the intelligence database.

Choose **Policy > Threat Detection > Advanced Threat > NTI-based Detection**. The NTI-based detection switch is off by default. After turning on this switch, you can query threat information of an IP address, Uniform Resource Locator (URL), domain, or sample, configure the intelligence database, import intelligence, and create custom intelligence rules, as shown in the following figure.

Figure 4-1 NTI-based Detection page



## Querying Threat Information

In the **Threat Information Query** area, set query conditions to query threat information of an IP address, URL, domain, or sample. UTS provides two query methods:

- **Offline query:** After configuring query conditions, click **OK**. Then UTS checks its own intelligence database for threat information of the specified IP address, domain, URL, or sample.
- **Online query:** If UTS can access the Internet, after configuring query conditions, click **Collaborate with NTI**. Then you are redirected to NSFOCUS Threat Intelligence (NTI), where threat information of the specified object is displayed.

Table 4-7 Threat information query parameters

Parameter	Description
Query Object Type	Specifies the type of query object, which can be <b>IP</b> , <b>URL</b> , <b>Domain Name</b> , or <b>Sample</b> .
Object	Specifies the query object of the specified type as follows: <ul style="list-style-type: none"> <li>• <b>IP:</b> specifies an IPv4 or IPv6 address.</li> <li>• <b>URL:</b> specifies a valid URL, for example, <b>test/test/1.html</b>.</li> <li>• <b>Domain Name:</b> specifies a valid domain name, for example, <b>http://xxx.com</b>.</li> </ul>

Parameter	Description
	<ul style="list-style-type: none"> <li><b>Sample:</b> specifies a sample, represented with a 32-bit MD5 string of 0–9, a–z, and A–Z.</li> </ul>

## Configuring the Intelligence Database

In the **Built-in Intelligence Database** area, choose which types of intelligence to detect and click **OK** to commit the settings.

## Configuring Custom Intelligence Rules

After enabling NTI-based detection, you can create custom intelligence rules in the **Custom Intelligence Rules** area.

Click **Create**, configure parameters, and click **OK**. Then click **Apply Configuration** in the upper-right corner of the page to make the settings take effect. [Table 4-8](#) describes parameters for creating a custom intelligence rule.

A custom intelligence rule, after being created, can be edited, queried, and deleted.

Table 4-8 Parameters for creating a custom intelligence rule

Parameter	Description
Category	Category of intelligence, which can be <b>Noncompliant website</b> or <b>Other</b> .
Type	Specific intelligence type under the specified category.
Custom Rule ID	ID of the custom intelligence rule, ranging from 1000 to 1099.
Severity	Severity of the intelligence, which can be <b>Low</b> , <b>Medium</b> , or <b>High</b> .
Enable	Whether to enable this rule. A rule can work only after being enabled.
Attack Result	Result of the attack hitting this rule. Options include <b>Attempt</b> , <b>Success</b> , and <b>Failure</b> .
Value	Data of the specified intelligence type.
Description	<ul style="list-style-type: none"> <li>For the category of <b>Noncompliant website</b>, "Noncompliant website" is displayed here and cannot be modified.</li> <li>For the <b>Other</b> category, type descriptive information of this rule with no more than 128 characters, excluding special characters such as the following: &amp; &gt; &lt; \ ' ,</li> </ul>

## Importing Intelligence

UTS allows you to import IP, domain, URL, and sample intelligence to its intelligence database. After an intelligence file is successfully imported, related intelligence can be used to detect threats. When finding a match in the imported intelligence, UTS generates a threat intelligence alert.

Click **Import Intelligence**, choose an intelligence file from a local disk drive, and complete the import. The newly imported intelligence will overwrite the existing intelligence.



Note

Note the following when compiling an intelligence file:

- The file must be named with the intelligence type, such as **ip.txt**, **domain.txt**, **url.txt**, or **sample.txt**.
- Each entry of intelligence should be in a separate line.

For example, to import IP intelligence, you should upload a file named **ip.txt**, which contains IPv4 and/or IPv6 addresses, each in a separate line.

#### 4.1.4.2 Malicious File Detection Policy

UTS can detect a variety of malicious files. After detecting a malicious file, it generates a malicious file alert.

Choose **Policy > Threat Detection > Advanced Threat > Malicious File**, enable static file detection, and click **Save**.

Figure 4-2 Configuration page of malicious file detection



Note



For malicious file detection, you must enable the file restoration function first. For details, see [File Restoration](#).

#### 4.1.4.3 Phishing Email Detection Policy

UTS can detect phishing emails by checking emails against built-in check items. Specifically, it calculates the sum of weighted value of each check item and compares it with the weighted value of the specified detection level. If the sum is greater than the latter, UTS determines that the current email is a phishing email. At the same time, it generates an intrusion alert.

Choose **Policy > Threat Detection > Advanced Threat > Phishing Email**. The phishing email detection switch is off by default. Turn on the switch, configure parameters, and click **OK**. Then click **Apply Configuration** in the upper-right corner to make the settings take effect. The following table describes phishing email detection parameters.

Table 4-9 Phishing email detection parameters

Parameter	Description
Email Header Detection	After this is enabled, UTS will check email headers. When detecting an attack, it logs a phishing email event.
Email Body Detection	After this is enabled, UTS will check email bodies. When detecting an attack, it logs a phishing email event.
Collaborate with NTI	<p>After this is enabled, UTS logs a phishing email event in any of the following cases:</p> <ul style="list-style-type: none"> <li>The email body contains a malicious domain name (starting with <b>http://</b> or <b>https://</b>) or URL listed in NTI's database.</li> <li>The source or destination IP address of email session packets has a match in NTI's database.</li> <li>The attachment matches a malicious sample in NTI's database.</li> </ul> <p> <b>Note</b></p> <p>Before using the collaborative detection function, you must upgrade NTI's database. For details, see <a href="#">Offline Upgrade</a>.</p>
Email Attachment Detection	<p>After this is enabled, UTS will check email attachments. When detecting a malicious file, it logs a phishing email event.</p> <p> <b>Note</b></p> <p>Before using the email attachment detection function, you must enable malicious file detection. For details, see <a href="#">Malicious File Detection Policy</a>.</p>
Detection Level	<p>Specifies the detection level of phishing emails. Different levels have different weights. When determining that the severity of a phishing email reaches the level specified here, UTS generates an alert.</p> <p>Options include <b>High</b>, <b>Medium</b>, and <b>Low</b>. A higher level indicates a stricter condition for determining that an email is a phishing email.</p>
Sensitive Words	<p>Specifies sensitive words to be detected in email bodies and subjects.</p> <p>Sensitive words can be added, edited, and deleted. Multiple words should be separated by the carriage return.</p>

#### 4.1.4.4 Covert Channel Detection Policy

UTS can detect covert channels of the Internet Control Message Protocol (ICMP) and DNS. Besides, it can restore files transferred through these covert channels. After detecting a covert channel, UTS generates an intrusion alert.

Choose **Policy > Threat Detection > Advanced Threat > Covert Channel**. The covert channel detection switches are off by default. Turn on the switches, configure parameters, and click **OK**. Then click **Apply Configuration** in the upper-right corner to make the settings take effect. The following table describes covert channel detection parameters.

Table 4-10 Covert channel detection parameters

Parameter	Description
DNS Covert Channel Detection	After this is enabled, UTS checks DNS packets and restores files from packets transmitted through DNS covert channels.
ICMP Covert Channel Detection	After this is enabled, UTS checks ICMP packets and restores files from packets transmitted through ICMP covert channels.
Detection Level	Detection level of covert channels, which can be <b>Low</b> , <b>Medium</b> , or <b>High</b> . A higher detection level indicates stricter matching conditions. A lower detection level will lead to more false positives.


**Note**

Covert channel detection is based on metadata logs. This means that, to use this function, you must first enable metadata restoration of ICMP and DNS, as described in [Metadata Restoration](#).

#### 4.1.4.5 DGA Domain Name Detection Policy

UTS can detect domain names generated with domain generation algorithms (DGAs). Such domain names may be included in DNS queries, the host field of HTTP requests, or email bodies. When detecting a DGA domain name, UTS generates an intrusion alert.

Choose **Policy > Threat Detection > Advanced Threat > DGA Domain Name**. The DGA domain name detection switch is off by default. Turn on the switch and click **Apply Configuration** in the upper-right corner of the page to make the setting take effect.

#### 4.1.4.6 Web Shell Detection Policy

UTS can detect the following types of web shell attacks and generate web shell alerts:

- Web shell files: including .php, .jsp, .jspx, and .jpg files restored from traffic
- Web shell communication traffic: web shells carried in HTTP traffic
- Encrypted web shell communication traffic: web trojans in encrypted malicious traffic, including Behinder, Godzilla, and Antsword


**Note**

To use the web shell detection function, you must first enable HTTP file restoration, as described in [File Restoration](#).

Web shell detection switches are off by default. To enable and configure these functions, follow these steps:

**Step 1** Choose **Policy > Threat Detection > Advanced Threat > Web Shell**.

Figure 4-3 Web Shell Detection page

**Webshell Detection**

Web Shell File Detection:

Web Shell Communication Traffic Detection:

Encrypted Web Shell Communication Traffic Detection :

**Encrypted Web Shell Suspicious Lists (1)** Create

Web Server Name	Web Server IP	Description	Operation
12323	10.12.1.2	test	<a href="#">Edit</a> <a href="#">Delete</a>

**Step 2** Enable the following functions:

- a. Web shell file detection (smart engine)
- b. Web shell communication traffic detection (smart engine)
- c. Encrypted web shell communication traffic detection

**Step 3** Configure a suspicious list of encrypted web shells.

Detection of encrypted web shell communication traffic, after being enabled, is implemented in different ways, depending on whether a web server is specified:

- a. No web server specified: UTS checks all encrypted traffic for web shells.
- b. Web server specified: UTS checks whether encrypted traffic carries the IP address of the specified web server and, if yes, continues to check such traffic for web shells. When detecting a web shell, UTS generates a web shell alert.

- Click **Create**.
- Type the name, IP address, and description of the new web server.
- Click **OK**.

A web server, after being added, can be edited and deleted.

**Step 4** Click **Apply Configuration** in the upper-right corner to make the settings take effect.

---End

## 4.1.5 5G Threat Detection

UTS can detect 5G threats, including N12 authentication attacks, signaling storms, and user equipment (UE) anomalies.

### 4.1.5.1 Policy for Detecting N12 Authentication Attacks

UTS detects and alerts users to N12 authentication attacks based on the intrusion detection rule of 5G N12 authentication attacks.

To configure a policy for detecting N12 authentication attacks, follow these steps:

**Step 1** Choose **Policy > Threat Detection > 5G Threat > N12 Authentication Attack**.

**Step 2** Configure parameters.

Table 4-11 N12 authentication attack detection parameters

Parameter	Description
Statistics Table Size	Size of the authentication statistics table. The value range is 1000–100000.
Statistical Period	Period of time for detecting failed N12 authentication attempts. The value range is 1–3600, in seconds.
Authentication Attempt Threshold	Minimum number of N12 authentication failures to trigger an alert. When the number of replayed N12 authentication failures reaches or exceeds the threshold set here in a statistical period, UTS generates an N12 authentication failure alert. The value range is 1–65535.

**Step 3** Click **Save**.

**Step 4** Choose **Policy > Rule Configuration > Rule Management > Intrusion Detection**.

- a. Search for the "5G N12 Authentication DDoS" rule.
- b. Select actions of the rule and click **Save**.

For more information about intrusion detection rules, see [Intrusion Detection Rules](#).

**Step 5** Click **Apply Configuration** in the upper-right corner to make the settings take effect.

----End

### 4.1.5.2 Signaling Storm Detection Policy

UTS can detect and alert users to 5G signaling storms. To use this function, you must first configure actions for the 5G signaling storm detection rule and apply the configuration.

To configure a policy for signaling storm detection, follow these steps:

**Step 1** Choose **Policy > Threat Detection > 5G Threat > Signaling Storm**.

**Step 2** Configure parameters.

Table 4-12 Signaling storm detection parameters

Parameter	Description
Statistics Table Size	Size of the signaling storm statistics table. The value range is 1000–100000.
Detection Period	Period of time for detecting signaling storms. The value range is 1–3600, in seconds.
Signaling Threshold	Storm Minimum number of UE access times to trigger an alert. When the number of UE access times reaches or exceeds the threshold set here in a detection period, UTS generates a signaling storm alert. The value range is 0–65535.

**Step 3** Click **Save**.

**Step 4** Choose **Policy > Rule Configuration > Rule Management > Intrusion Detection**.

- a. Search for the "5G Signaling Storm" rule.
- b. Select actions of the rule and click **Save**.

For more information about intrusion detection rules, see [Intrusion Detection Rules](#).

**Step 5** Click **Apply Configuration** in the upper-right corner to make the settings take effect.

---End

### 4.1.5.3 UE-related Anomaly Detection Policy

UE refers to any device directly used by an end user to communicate. UTS can detect UE-related anomalies.

Choose **Policy > Threat Detection > 5G Threat > UE Anomaly**, configure parameters, and click **Save**. Then click **Apply Configuration** in the upper-right corner of the page to make the settings take effect. The following table describes parameters for detecting UE-related anomalies.

Table 4-13 UE-related anomaly detection parameters

Parameter	Description
Statistics Table Size	Maximum number of UE nodes per process.
Detection Period	Period of time for detecting UE-related anomalies.
Online/Offline Count Threshold	Threshold for the number of times a UE goes online and offline in a detection period. When such number reaches or exceeds the threshold set here, UTS determines that an anomaly occurs.
Shutdown Count Threshold	Threshold for the number of times a UE is turned on and off in a detection period. When such number reaches or exceeds the threshold set here, UTS determines that an anomaly occurs.
Connection Request Count Threshold	Threshold for the number of connection requests from a UE in a detection period. When such number reaches or exceeds the threshold set here, UTS determines that an anomaly occurs.
Signaling Interaction Anomaly Count Threshold	Threshold for the number of signaling interaction failures of a UE in a detection period. When such number reaches or exceeds the threshold set here, UTS determines that an anomaly occurs.
Signaling Interaction Count Threshold	Threshold for the number of signaling interactions of a UE in a detection period. When such number reaches or exceeds the threshold set here, UTS determines that an anomaly occurs.
Handoff Count Threshold	Threshold for the number of handoffs of a UE in a detection period. When such number reaches or exceeds the threshold set here, UTS determines that an anomaly occurs.

## 4.1.6 Other Threat Detection

Besides the preceding types of threats, UTS can detect routing protocol attacks, Fraggle attacks, slow HTTP attacks, and custom weak passwords. In addition, it supports VXLAN parsing.

### 4.1.6.1 Policy for Detection of Routing Protocol Attacks

UTS can detect attacks on the following routing protocols: Routing Information Protocol (RIP) and Open Shortest Path First (OSPF). When detecting such an attack, UTS generates an intrusion alert.



Choose **Policy > Threat Detection > Other > Routing Protocol**. The routing vulnerability detection switch is off by default. Turn on the switch, configure parameters, and click **OK**. Then click **Apply Configuration** in the upper-right corner to make the settings take effect. The following table describes parameters for detecting routing protocol attacks.

Table 4-14 Parameters for detecting routing protocol attacks

Parameter	Description
Statistical Period	Period of time for detecting routing packets. When detecting that the number of RIP or OSPF packets within a statistical period reaches or exceeds the corresponding threshold, UTS generates an alert at the end of the period. Then the next statistical period starts. The value range is 1–65535, in seconds.
RIP Packet Threshold	Minimum number of RIP packets to trigger an alert in a statistical period. The value range is 1–65535.
OSPF Packet Threshold	Minimum number of OSPF packets to trigger an alert in a statistical period. The value range is 1–65535.

### 4.1.6.2 Fraggle Attack Detection Policy

A Fraggle attack (computer virus attack) is a simple variation of a Smurf attack by using UDP instead of ICMP echo reply packets. UTS can detect Fraggle attacks and generate intrusion alerts.

Choose **Policy > Threat Detection > Other > Fraggle Attack**. The Fraggle attack detection switch is off by default. Turn on this switch and click **Save**. Then click **Apply Configuration** in the upper-right corner to make the settings take effect. The following table describes Fraggle attack detection parameters.

Table 4-15 Fraggle attack detection parameters

Parameter	Description
Fraggle Attack Detection	Controls whether to enable Fraggle attack detection.
Match Broadcast Address	Controls whether to match the broadcast address. The destination IP address matching the broadcast address is a prerequisite for UTS to generate alerts. This switch is on by default. If Fraggle attack detection is disabled, <b>Match Broadcast Address</b> does not work even if it has been enabled.

### 4.1.6.3 Slow HTTP Attack Detection Policy

UTS can detect slow HTTP attacks and generate intrusion alerts.

Choose **Policy > Threat Detection > Other > Slow HTTP Attack**. The slow HTTP attack detection switch is off by default. Turn on this switch, configure parameters, and click **Save**. Then click **Apply Configuration** in the upper-right corner to make the settings take effect. The following table describes slow HTTP attack detection parameters.

Table 4-16 Slow HTTP attack detection parameters

Parameter	Description
Slow HTTP Attack Detection	Controls whether to enable slow HTTP attack detection.
Min Session Duration	Minimum duration for check of HTTP sessions for slow attacks. The value range is 5–300, in seconds.
Min Avg Request Length	Minimum number of bytes in a normal HTTP request packet. The value range is 1–256, with <b>64</b> as the default.
Min Avg Response Read Length	Minimum number of bytes in a normal HTTP response packet. The value range is 1–256, with <b>64</b> as the default.

#### 4.1.6.4 Weak Password Detection Policy

UTS allows you to create weak password detection policies for detecting weak passwords in HTTP, Telnet, FTP, POP3, Simple Mail Transfer Protocol (SMTP), and Internet Message Access Protocol (IMAP) services. When detecting a weak password, UTS generates an intrusion alert and logs a weak password event.

Choose **Policy > Threat Detection > Other > Custom Weak Password**. The weak password detection switch is off by default. Turn on the switch, click **Create**, configure parameters, and click **OK** to go back to the previous page. Click **Validate All Rules** and wait until the new rule takes effect. The following table describes weak password detection parameters.

A weak password detection rule, after being created, is enabled by default. Such rules can be edited, deleted, queried, disabled, exported, and imported.

Table 4-17 Weak password detection parameters

Parameter	Description
Enable	Controls whether to enable the weak password detection rule.
Name	Name of the weak password detection rule.
Match Type	Specifies how the weak password detection rule will be matched. Options include <b>Character string</b> and <b>Regular expression</b> .
Weak Password	Specifies the weak password with a character string or regular expression, depending on the selected matching type.



You have to wait a while for weak password detection rules to take effect. Do not click **Validate All Rules** again before the operation is complete.

#### 4.1.6.5 VXLAN Parsing Policy

UTS can identify Virtual Extensible LANs (VXLANs). Specifically, it checks traffic against VXLAN parsing rules and, if a match is found, it parses packets to get the real IP address and generates a metadata log about this VXLAN event.



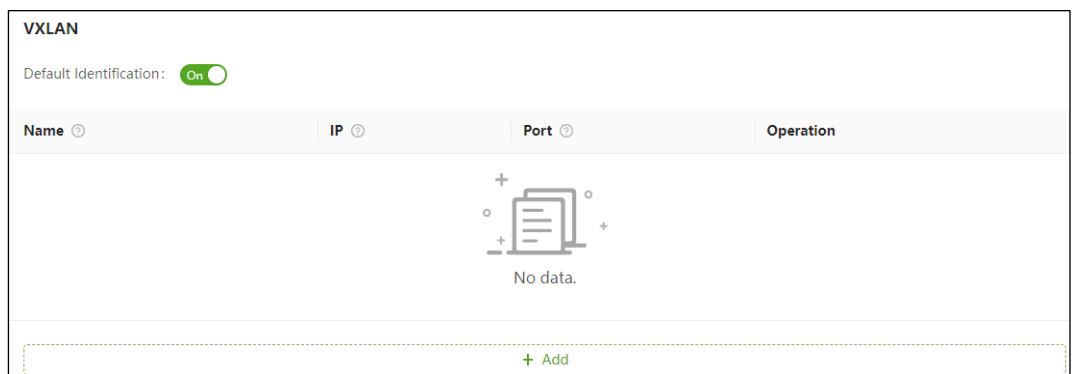
Turning on the default identification switch enables UTS to perform VXLAN parsing for all traffic. If this switch is turned off, UTS will check for VXLANs against the configured rules. If no rule is configured, UTS will not perform VXLAN parsing at all.

VXLAN parsing is turned off by default. To enable this function and configure related rules, follow these steps:

**Step 1** Choose **Policy > Threat Detection > Other > VXLAN Parsing**.

**Step 2** Turn on the default identification switch.

Figure 4-4 VXLAN Parsing page



**Step 3** Click **Add** and configure parameters.

The following table describes VXLAN parsing parameters.

Table 4-18 VXLAN parsing parameters

Parameter	Description
Name	Name of the VXLAN parsing policy, which cannot contain special characters, including the following: @ % ! &
IP	Source IP address in CIDR notation for VXLAN parsing, like 191.168.1.0/24. Both IPv4 and IPv6 addresses are supported.
Port	Destination port, ranging from 1 to 65535.

**Step 4** Click **Save** in the **Operation** column.

- a. To create more rules, repeat the preceding steps.
- b. A VXLAN parsing rule, after being added, can be edited and deleted.

**Step 5** Click **Apply Configuration** in the upper-right corner to make the settings take effect.

---End

## 4.2 Rule Configuration


This module allows you to configure four types of rules and various rule templates.

### 4.2.1 Rule Management

Under **Policy > Rule Configuration > Rule Management**, you can manage intrusion, web application threat, custom, and custom protocol detection rules.

#### 4.2.1.1 Intrusion Detection Rules

UTS uses built-in rules to detect intrusion behavior. You can keep the rule base up to date by uploading and installing the latest rule package.

 <b>Note</b>	<ul style="list-style-type: none"> <li>For information on how to enable or disable intrusion detection, see <a href="#">Intrusion Detection Policy</a>.</li> <li>For information on how to upgrade built-in rule bases, see <a href="#">Offline Upgrade</a>.</li> </ul>
--	---

Choose **Policy > Rule Configuration > Rule Management > Intrusion Detection**. Initially, built-in intrusion detection rules are listed. You cannot create or delete built-in rules, but can only query, enable, and disable such rules and set actions for UTS to take when detecting traffic matching these rules.

Figure 4-5 Intrusion detection rules

Intrusion Detection									
Event Name: <input type="text" value="Please type"/>		ID: <input type="text" value="Please type"/>		CVE-ID: <input type="text" value="Please type"/>		CNNVD-ID: <input type="text" value="Please type"/>			
Severity: <input type="text" value="Please select"/>		Confidence: <input type="text" value="Please select"/>		Reset		Query		Advanced Search^	
Rules (10368)									
ID	Event Name	Alert Category	Severity	Confidence	CVE-ID / CNNVD-ID	Alert	Block	Capture	
10000	IP Fragment Overlap Teardrop Denial ...	DoS / Other DoS a...	Medium	High	CVE-1999-0015 / CNNV...	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
10013	Microsoft IIS WebDAV PROPFIND De...	DoS / Application...	Medium	Medium	- / -	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
10017	Microsoft FTP Server STAT Command...	DoS / Application...	Medium	High	CVE-2002-0073 / CNNV...	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
10035	Malformed Stream ACK/FIN Small Pa...	DoS / ACK flood	Medium	Medium	- / -	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
10036	mstream ACK/FIN Small Packets Floo...	DoS / ACK flood	Medium	Medium	- / -	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
10039	Windows System TCP/IP OOB Urgent...	DoS / Other DoS a...	High	High	CVE-1999-0153 / CNNV...	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

### Querying Rules

At the top of the page shown in [Figure 4-5](#), set query conditions and click **Query** to query intrusion detection rules. Clicking **Reset** clears query conditions and displays all intrusion detection rules.

Table 4-19 Parameters for querying intrusion detection rules

Parameter	Description
Rule ID	ID of the intrusion detection rule to be queried.
Event Name	Name of the event covered by the rule. Fuzzy matching is supported.
CVE-ID	Common Vulnerabilities and Exposures (CVE) ID of the vulnerability covered by the rule.
CNNVD-ID	Chinese National Vulnerability Database (CNNVD) ID of the vulnerability covered by the rule.
Severity	Severity level of the event covered by the rule, which can be <b>High</b> , <b>Medium</b> , or <b>Low</b> . <b>All</b> indicates no restriction to the severity level.
Confidence	This, together with <b>Severity</b> , is displayed only when you click <b>Advanced Search</b> . Options of this field are <b>High</b> , <b>Medium</b> , and <b>Low</b> . <b>All</b> indicates no restriction to the confidence level.

## Querying Rule Details

On the page shown in [Figure 4-5](#), click the event name of an intrusion detection rule. Then details of this rule are displayed on a separate page.

## Configuring Actions

On the page shown in [Figure 4-5](#), select one or more actions for UTS to take when it detects intrusion and click **Save**. [Table 4-20](#) describes actions to be taken against intrusion.

Clicking **Bulk Operation**, you can configure actions for all rules in bulk.

Table 4-20 Actions that can be taken against intrusion

Parameter	Description
Alert	Selecting or deselecting the <b>Alert</b> check box enables or disables this action for a rule. Intrusion detection rules can work only after the intrusion detection function is enabled. After the <b>Alert</b> action is selected for a rule, UTS will generate alerts on events matching the rule.
Block	Selecting or deselecting the <b>Block</b> check box enables or disables this action for a rule. After this action is selected for a rule, UTS will block packets matching this rule. The <b>Block</b> action, if selected, can take effect only after <b>Alert</b> is also selected.
Capture	Selecting or deselecting the <b>Capture</b> check box enables or disables this action for a rule. After this action is selected for a rule, UTS will save packet capture (PCAP) files for traffic matching this rule. Such files are available for download in log details of various threats. Besides, ISOP adds a function to allow users to download original PCAP data (complete packet data). If packet capture has not been conducted, the PCAP file downloaded is empty (without any data). The <b>Capture</b> action, if selected, can take effect only after <b>Alert</b> is also selected.

## 4.2.1.2 Web Application Threat Detection Rules

UTS uses built-in rules to detect web application threats. You can keep the rule base up to date by uploading and installing the latest rule package.

Choose **Policy > Rule Configuration > Rule Management > Web Threat Detection**. Built-in rules for detecting web application threats are listed by default. Their management methods are similar to those for intrusion detection rules. For details, see [Intrusion Detection Rules](#).



**Note**

- For information on how to enable/disable and configure web application threat detection, see [Web Threat Detection Policy](#).
- For information on how to upgrade the detection rule base of web application threats, see [Offline Upgrade](#).

## 4.2.1.3 Custom Rules

UTS allows you to create custom rules to detect malicious traffic not covered by built-in rules. This makes up for the shortage of built-in rules, enabling the device to quickly spot whatever is suspicious in traffic.

Choose **Policy > Rule Configuration > Rule Management > Custom Rule**. The custom rule-based detection function is disabled by default. Enable this function, click **Create**, configure parameters, and click **Save** to go back to the previous page. Click **Validate All Rules** to make the settings take effect. [Table 4-21](#) describes parameters for creating a custom detection rule.

After custom rules are configured and enabled, UTS will check traffic against these rules in the order in which they were created. Once detecting a match, UTS handles the traffic according to the rule and will not forward such traffic for checks against other rules. Meanwhile, it generates an alert and logs the event.

Custom rules can also be edited, deleted, imported, exported, queried, enabled, and disabled. Besides, you can specify which columns are displayed in the list of custom rules.

Table 4-21 Parameters for configuring a custom rule

Parameter		Description
Basic Information	Enable	The new rule can take effect only after this is turned on.
	Custom Alert Name	Rule name, which cannot contain special characters like the semicolon (;), single quotation mark ('), and double quotation mark (").
	Description	Description of the custom rule.
	Alert Category/Sub-category	Specifies level 1 and level 2 alert types defined by telcos.
	CVE-ID	Specifies the CVE ID of the vulnerability covered by the custom rule. The format of the CVE ID is CVE-year/year+month-number, like CVE-2001-01 or CVE-202211-0123. Multiple CVE IDs should be separated by the semicolon.
	CNNVD-ID	Specifies the CNNVD ID of the vulnerability covered by the custom rule.

Parameter		Description
		The format of the CNNVD ID is CNNVD-year/year+month-number, like CNNVD-2001-01 or CNNVD-202211-0123. Multiple CNNVD IDs should be separated by the semicolon.
	Severity	Specifies the severity level of the vulnerability covered by the custom rule, which can be <b>High</b> , <b>Medium</b> , or <b>Low</b> .
	Confidence	Specifies the confidence level of the vulnerability covered by the custom rule, which can be <b>High</b> , <b>Medium</b> , or <b>Low</b> .
	Attack Assessment	Specifies the result of events matching this rule, which can be <b>Attempt</b> , <b>Success</b> , or <b>Failure</b> .
5-Tuple Information	Transport Protocol	Specifies a transport layer protocol, which can be <b>TCP</b> , <b>UDP</b> , <b>ICMP</b> , or <b>SCTP</b> (Stream Control Transmission Protocol).
	Application Protocol	Specifies one or more application layer protocols. Your selection will determine which options are displayed for <b>Matching Position</b> in <b>Signature Information</b> . If <b>SCTP</b> or <b>ICMP</b> is selected as the transport layer protocol, <b>Application Protocol</b> cannot be configured.
	Src IP/Dst IP	Specifies the source and destination IPv4 or IPv6 addresses. For information on how to type these IP addresses, see the related tooltips.
	Src Port/Dst Port	Specifies the source and destination ports. The value range is 0–65535. For information on how to type these ports, see the related tooltips. If <b>ICMP</b> is selected as the transport layer protocol, <b>Src Port</b> and <b>Dst Port</b> are unavailable.
	Detection Direction	If <b>TCP</b> or <b>SCTP</b> is selected as the transport layer protocol, you should also specify the detection direction.
Signature Information (optional; can be added as required)	Match Type	Specifies how the packet payload will be matched. Options are <b>Character string</b> , <b>Hexadecimal value</b> , <b>Regular expression</b> , and <b>Character string + hexadecimal value</b> .
	Matching Content	Specifies the signature to be matched in the form specified with <b>Match Type</b> .
	Configuration Option	An option, once selected, is enabled. Multiple options can be selected, including <b>Case-insensitive</b> , <b>Invert</b> , and <b>GBK encoding</b> .
	Matching Position	Specifies what content UTS will check for the signature.
	Offset/Depth/Distance/Within	For information on how to set these fields, see the related tooltips. If <b>Regular expression</b> is selected as the matching type, these fields are unavailable.


**Note**

Custom rules can only be used for inspection of traffic transmitted in plaintext.

### 4.2.1.4 Custom Protocols

UTS allows you to create custom protocol rules to detect malicious traffic of those protocols.

Choose **Policy > Rule Configuration > Rule Management > Custom Protocol**. The custom protocol detection function is disabled by default. To configure a custom protocol rule, you should enable this function first. For the specific configuration method, see [Custom Rules](#).

### 4.2.2 Rule Templates

Rule templates are classified into the following types:

- Built-in templates: including rule templates (common rules and comprehensive rules) of NSFOCUS Intrusion Prevention System (IPS) and Web Application Firewall (WAF)
- Custom rule templates: user-defined rule templates

Choose **Policy > Rule Configuration > Rule Template**. Initially, built-in rule templates are listed.

Figure 4-6 Rule template list

Rule Templates (9)					
* Template Name: <input type="text" value="Please type"/>		Type: <span>All</span> <input type="button" value="Query"/>	<input type="button" value="Reset"/>	<input type="button" value="Import"/>	<input type="button" value="Create"/>
Name	Description	Type	Creation Time	Operation	
Common IPS Rule Template	It is derived from the Comprehensive IPS...	Intrusion rule	2021-04-06 18:24:49	<a href="#">Details</a>	<a href="#">Enable</a>
Comprehensive IPS Rule Template	Comprehensive IPS Rule Template	Intrusion rule	2021-04-06 18:24:49	<a href="#">Details</a>	<a href="#">Enable</a>
IPS Frequent, Risky Event Rule Templ...	IPS Frequent, Risky Event Rule Template ...	Intrusion rule	2021-04-06 18:24:49	<a href="#">Details</a>	<a href="#">Enable</a>
<span>Enabled</span> IPS Routine Operations R...	Earlier versions of IPS rules and high-sen...	Intrusion rule	2021-04-06 18:24:49	<a href="#">Details</a>	

Click **Create** in the upper-right corner of the page. On the **Create Rule Template** page, configure parameters and click **Save**. Then the new template is displayed in the template list. Click **Apply Configuration** in the upper-right corner of the page to make the new template take effect. The following table describes parameters for creating a custom rule template.

Custom templates can also be viewed, edited, deleted, imported, exported, queried, enabled, and disabled. Built-in templates cannot be edited or deleted.

Table 4-22 Parameters for configuring a custom rule template

Parameter	Description
Base Template	Select an existing rule template, edit it, and then save it as a custom template.
Template Name	Name of the custom rule template.
Description	Brief description of the custom rule template.
Rule	Select rules covered by the template by selecting one or more actions ( <b>Alert</b> , <b>Block</b> , and <b>Capture</b> ).
	<p><b>Note</b></p> <p>In the upper part of the <b>Rule List</b> area, you can search for rules by rule ID, event name, or severity. You can also click  in <b>Alert</b>, <b>Block</b>, and <b>Capture</b> columns to filter rules.</p>



## 4.3 Restoration Configuration

The Restoration Configuration module provides the following functions:

- Metadata restoration: restores packets of transport layer protocols and application layer protocols.
- File restoration: restores files from packets transmitted over various application layer protocols.
- 5G log detection: allows you to control the general switch of 5G log detection as well as switches for detection and storage of various types of signaling.

### 4.3.1 Metadata Restoration

UTS can parse layer 4 traffic and data of application layer protocols, extract metadata, and assemble such metadata into logs and send them to ISOP.

Choose **Policy > Restoration Configuration > Metadata Restoration**. Turn on or off the metadata restoration switch of each network/transport layer protocol and session/application layer protocol, and click **Save**. Then click **Apply Configuration** in the upper-right corner of the page to make the settings take effect.



Note

- TCP, UDP, and ICMP session logs can be generated only after the TCP, UDP, and ICMP data restoration switches are turned on.
- For packets matching traffic allowlists, UTS will not perform metadata restoration.

### 4.3.2 File Restoration

UTS can identify, decode, and extract file contents from data transmitted over application layer protocols, namely HTTP, FTP, SMTP, POP3, IMAP, Samba, and Webmail. Then it sends these files to ISOP, which, in turn, sends them to TAC for malicious behavior analysis.

File types that UTS can restore include executables, files, compressed files, and web files.

Choose **Policy > Restoration Configuration > File Restoration**. In the **Application Protocols** area and **Transferred File Types and Formats** area, turn on or off the switches as required and click **Save** in these areas. Then click **Apply Configuration** in the upper-right corner of the page to make the settings take effect. After that, UTS will restore enabled file types from data transmitted over enabled protocols.



Note

Note the following when turning on or off switches for file restoration:

- Switches in the **Application Protocols** area are master switches, while those in the **Transferred File Types and Formats** area are subordinate ones.
- After a switch in the **Application Protocols** area is turned off, even if its subordinate switches in the **Transferred File Types and Formats** area are turned on, no related file restoration logs will be generated.

For files restored by UTS, note the following:

	<ul style="list-style-type: none"> <li>• The default size of files that can be restored is 10 MB, which can be increased to 30 MB. Files larger than 30 MB will not be restored. For information on how to configure the file size, see <a href="#">Special Parameters</a>.</li> <li>• When the restored files use 90% of the maximum space allowed, UTS will delete files older than 48 hours, 24 hours, 12 hours, 6 hours, 1 hour, and 30 minutes in sequence.</li> <li>• For packets matching traffic allowlists, UTS will not perform file restoration.</li> </ul>
--	--

### 4.3.3 5G Log-related Switches

This module allows you to turn on the general switch of 5G protocol parsing and then turn on or off switches for detection and storage of various types of signaling.

Choose **Policy > Restoration Configuration > 5G Log Detection**, turn on the general switch, turn on or off switches for detection and storage of various types of signaling, and click **OK**. Then click **Apply Configuration** in the upper-right corner of the page to make the settings take effect. The following table describes 5G log-related switches.

Table 4-23 5G log-related switches

Parameter	Description
5G Log Detection	General switch of 5G signaling logs, which is off by default.
NGAP Detection	Controls whether to generate signaling logs of N1 and N2 interfaces.
PFCP Detection	Controls whether to generate signaling logs of the N4 interface.
HTTP/2 Detection	Controls whether to turn on the HTTP 2.0 log switch. Signaling logs of N5, N7, N8, N10, N11, N12, N13, N14, N15, N20, N21, N22, N28, and N40 interfaces can be detected only after this switch is turned on. <ul style="list-style-type: none"> <li>• <b>On:</b> Logs of the preceding interfaces can be detected.</li> <li>• <b>Off:</b> Logs of the preceding interfaces cannot be detected.</li> </ul>
GTP Detection	Controls whether to generate signaling logs of the N26 interface.
NE Discovery	Controls whether to enable automatic discovery of network elements (NEs). After this switch is turned on, the system will identify the NE type according to related protocols and specifications and record such information in the 5G NE list.
Local NGAP Log Storage	Controls whether to save NG Application Protocol (NGAP) logs to a local disk drive.
Local PFCP Log Storage	Controls whether to save Packet Forwarding Control Protocol (PFCP) logs to a local disk drive.
Local HTTP/2 Log Storage	Controls whether to save HTTP/2 logs to a local disk drive.
Local GTP V2 Log Storage	Controls whether to save logs of General Packet Radio Service (GPRS) Tunneling Protocol Version 2 (GTPv2) to a local disk drive.

## 4.4 Traffic Management

By default, UTS inspects all traffic, but does not store traffic. The Traffic Management module allows you to configure malicious traffic detection and storage policies.

- Traffic storage: disabled by default. For traffic storage, you should choose whether to store all traffic or only malicious traffic.
- Allowlist: disabled by default. After this is enabled, you should configure rules to specify which packets are excluded from inspection.
- Suspicious list: disabled by default, indicating that UTS inspects all traffic.



After the suspicious list function is enabled, UTS will inspect only traffic matching suspicious lists. Exercise caution when enabling this function.



- The suspicious list has a higher priority than the allowlist. That is to say, when both are enabled, UTS checks whether traffic matches any suspicious lists before checking for an allowlist match.
- For traffic matching only suspicious lists, UTS generates related logs.
- For traffic matching both a suspicious list and allowlist, UTS does not generate any logs.

### 4.4.1 Traffic Storage

By default, UTS does not store inspected traffic. The Traffic Storage module allows you to configure traffic storage policies.

- Full traffic storage: stores all traffic. When collaborating with ISOP, UTS can receive query tasks dispatched by ISOP, store query results in PCAP files, and then inform ISOP of the download links.
- Malicious traffic storage: stores only packets associated with intrusion alerts, web application threat alerts, and custom rule-triggered alerts.





For information on how to configure UTS to collaborate with ISOP, see [API Account Configuration](#) and [A Interface Channel Configuration](#).

Traffic storage is disabled by default. To enable and configure the function, follow these steps:

**Step 1** Choose **Policy > Traffic Management > Traffic Storage**.

- For storage of only malicious traffic, skip step 3.
- For full traffic storage, skip step 2.

**Step 2** Enable malicious traffic storage.

 indicates that the function is enabled, while  indicates that it is disabled. Clicking the icon turns on or off the switch.

**Step 3** Enable full traffic storage.

- a. After this is enabled, 5-tuple data is stored and available for query (based on 5-tuples and session IDs (SIDs)) and download.
- b. Configure other parameters.

Table 4-24 Full traffic storage parameters

Parameter	Description
Storage by Application Type	Specifies application protocols for UTS to store related traffic.
Storage by Transport Protocol	Specifies transport protocols for UTS to store related traffic. SCTP is available only when both 5G log detection and NGAP detection switches are turned on. For information on how to turn on the two switches, see <a href="#">5G Log-related Switches</a> .

**Step 4** Click **Save** to commit the settings.

**Step 5** Click **Apply Configuration** in the upper-right corner to make the settings take effect.

---End

## 4.4.2 Allowlist

UTS allows you to configure allowlists of IP addresses, domains, ports, email addresses, or 4-tuples (source IP address, destination IP address, source port, and destination port). Then it will let traffic from or to allowed entities pass without storing it.


Choose **Policy > Traffic Management > Allowlist Management**. The allowlist function is disabled by default. Turn on the switch, click **Create**, configure parameters, and click **OK**. Then click **Apply Configuration** in the upper-right corner of the page to make the settings take effect. The following table describes allowlist parameters.

An allowlist, after being created, can be edited, queried, deleted, and exported. Besides, you can import an allowlist.

Table 4-25 Allowlist parameters


Parameter	Description
Type	Type of entities on the new allowlist, which can be any of the following: <ul style="list-style-type: none"> <li>• <b>IP</b>: allowlist of IPv4 or IPv6 addresses.</li> <li>• <b>Port</b>: allowlist of transport-layer ports.</li> <li>• <b>Domain Name</b>: domain name allowlist, applicable to logging and storage of metadata of HTTP traffic and DNS traffic.</li> <li>• <b>Email</b>: allowlist of email addresses. When either a sender's or recipient's email address is found on the allowlist, no log will be generated. In the case of multiple recipients, when one is found on the allowlist, no log will be generated.</li> </ul>

Parameter	Description
	<ul style="list-style-type: none"> <li><b>4-tuple</b>: indicates that UTS determines whether to generate logs based on four elements, namely the source IP address, destination IP address, source port, and destination port.</li> </ul>
Content	Specifies the allowed IP addresses, ports, domains, email addresses, or 4-tuples. For the 4-tuple allowlist, values should be typed as follows: <ul style="list-style-type: none"> <li>The four values should be separated by the comma and arranged in sequence, like "source IP address,destination IP address,source port,destination port". At least one non-empty value should be provided.</li> <li>If you do not want UTS to check the source or destination IP address, type <b>0.0.0.0</b>.</li> <li>If you do not want UTS to check the source or destination port, type <b>0</b>.</li> </ul>
Description	Brief description of the allowlist. This cannot contain special characters, including the following: ` ~ ! @ # \$ % ^ & { } * , /   ; '

 <b>Note</b>	When importing an allowlist, note the following: <ul style="list-style-type: none"> <li>You need to first export an allowlist, modify the exported file as required, and then import this file.</li> <li>The allowlist to be imported must contain the type, content, operator account, and timestamp.</li> </ul>
--	---

### 4.4.3 Suspicious List

UTS allows you to configure suspicious lists of IP addresses, ports, or IP addresses + ports. Then it will parse and inspect only traffic from or to entities on suspicious lists.

 <b>Caution</b>	UTS deems network traffic not matching any suspicious lists to be safe and trusted. Therefore, exercise caution when configuring suspicious lists.
---	--

Choose **Policy > Traffic Management > Suspicious List Management**. The suspicious list function is disabled by default. Turn on the switch, click **Create**, configure parameters, and click **OK**. Then click **Apply Configuration** in the upper-right corner of the page to make the settings take effect. The following table describes suspicious list parameters.

A suspicious list, after being created, can be edited, queried, deleted, and exported. Besides, you can import a suspicious list.

Table 4-26 Suspicious list parameters

Parameter	Description
Type	Type of entities on the new suspicious list, which can be <b>IP</b> , <b>Port</b> , or <b>IP + port</b> .
Content	Specifies IP addresses, ports, or IP addresses + ports:

Parameter	Description
	<ul style="list-style-type: none"> <li>• <b>IP:</b> specifies one or more IPv4 or IPv6 address ranges, host addresses, or network addresses. Multiple values should be separated by the carriage return. Note that all objects typed must be of the same type.</li> <li>• <b>Port:</b> specifies one or more ports in the range of 1–65535. Multiple values should be separated by the carriage return.</li> <li>• <b>IP + port:</b> specifies one or more IPv4/IPv6 address + port pairs. Elements in each pair should be separated by the colon and multiple pairs should be separated by the carriage return. Ports must be in the range of 1–65535.</li> </ul>
Description	Brief description of the suspicious list. This description cannot contain special characters, including the following: ` ~ ! @ # \$ % ^ & { } * , /   ; ' `

## 4.5 SSL Configuration

UTS can decrypt SSL traffic. After you configure parameters (IP address, port, and SSL certificate) of an HTTPS website, UTS can inspect traffic to and from the website for web application attacks.

### 4.5.1 SSL Connection Configuration

UTS can be configured to decrypt and inspect SSL traffic to and from specified HTTPS websites.

Choose **Policy > SSL Configuration > SSL Configuration**. Click **Create**, configure SSL connection parameters, and click **OK** to commit the settings. Choose **System > System Control** and click **Restart Engine** to make the settings take effect. The following table describes SSL connection parameters.

An SSL connection, after being created, can be edited, queried, reset, and deleted.

Table 4-27 SSL connection parameters

Parameter	Description
IP	Specifies the IPv4 or IPv6 address of an HTTPS website.
Port	Specifies the port used by the HTTPS website for encrypted communication. The value range is 0–65535.
Select Certificate	Specifies an SSL certificate for decryption of the server. This requires you to import the SSL certificate of this website in advance. For details, see <a href="#">Allowlist</a> .

### 4.5.2 SSL Certificate Management

Before specifying an SSL-secured HTTPS website for detecting web application attacks, you must configure the SSL certificate of this website.

Choose **Policy > SSL Configuration > SSL Certificate Management**. Click **Choose File**, select the correct certificate file, and click **Upload** to import the SSL certificate.

An SSL certificate, after being uploaded, can be deleted.



The SSL certificate to be imported must be a .cer or .key file no larger than 100 KB.

## 4.6 Alert Allowlist

Alert allowlists are effective for reduction of false positives of intrusion, web application threat, and sensitive information alerts. After an alert allowlist is configured for a detection rule, traffic matching the rule does not trigger any alerts or generate any logs.

Choose **Policy > Alert Allowlist**. The alert allowlist function is disabled by default. Turn on the switch, click **Create**, configure parameters, and click **OK**. Then click **Apply Configuration** in the upper-right corner of the page to make the settings take effect. The following table describes alert allowlist parameters.

An alert allowlist, after being created, can be edited, enabled, disabled, queried, and deleted.

Table 4-28 Alert allowlist parameters

Parameter	Description
Name	Name of the alert allowlist.
Rule ID	Rule ID covered by the alert allowlist. The rule ID should be an integer in the range of 1–99999999, identifying an intrusion detection rule or web application threat detection rule.
Priority	Priority of the alert allowlist, ranging from 0 to 32. A higher value indicates a higher level of priority.
Src IP	Source IPv4 or IPv6 address. <b>0.0.0.0</b> indicates any IP addresses.
Src Port	Source port, ranging from 0 to 65535. <b>0</b> indicates any ports.
Dst IP	Destination IPv4 or IPv6 address. <b>0.0.0.0</b> indicates any IP addresses.
Dst Port	Destination port, ranging from 0 to 65535. <b>0</b> indicates any ports.
URL	URL, which cannot exceed 255 characters.
Enable	Controls whether to enable the new allowlist.
URL Match Mode	Specifies how the URL is matched: <ul style="list-style-type: none"> <li>• <b>Exact match:</b> UTS does not generate any alerts or logs when the requested URL is exactly the same as the one specified here.</li> <li>• <b>Fuzzy match:</b> UTS does not generate any alerts or logs when part of the requested URL is the same as the one specified here.</li> </ul>

## 4.7 Out-of-Path Blocking

UTS provides the out-of-path blocking function. After this function is enabled and the blocking policy is selected for a type of threats, UTS sends an RST packet to terminate the connection between the client and the server when detecting such a threat.

On UTS, you can configure the following types of blocking policies:

- **Alerting and blocking policy:** You can enable or disable out-of-path blocking for various threats. After the policy is selected for a type of threats, UTS, when detecting such a threat, sends an RST packet to terminate the connection between the client and the server.
- **Custom blocking policy:** UTS allows you to configure and enable custom blocking policies. When detecting matching traffic, UTS terminates the connection and, if configured, sends the blocking log to ISOP.

### 4.7.1 Out-of-Path Blocking Policies

Choose **Policy > Out-of-Path Blocking > Out-of-Path Blocking**. The out-of-path blocking function is disabled by default. After enabling it, you can configure specific out-of-path blocking policies and layer 3 subinterface forwarding.

Figure 4-7 Out-of-Path Blocking page

The screenshot shows the configuration page for Out-of-Path Blocking. The 'Enable' toggle is turned on. Under 'Blocking Policies', there are five options, all of which are currently unchecked. Below this is an 'OK' button. The 'VLAN' section has its 'Enable' toggle turned on. The 'Layer 3 Subinterface Forwarding' section has its 'Enable' toggle turned on and a 'MAC Address' field with the example value '00:01:6C:06:A6:29'. A 'Save' button is next to the MAC address field. The 'Layer 3 Subinterface' section shows a table with columns for ID, Start IP, End IP, VLAN, and Operation. There are 'Bulk Delete' and 'Create' buttons at the top right of this section.


### Configuring Out-of-Path Blocking Policies

On the page shown in the preceding figure, enable the out-of-path blocking function, select policies, and click **OK**. Selecting or deselecting a policy enables or disables the blocking



function for the related module. Selecting the **Select all** check box enables the blocking function for all modules. The following table describes these policies.

Table 4-29 Out-of-path blocking policies

Policy Name	Description
Intrusion detection, alerting, and blocking	<p>After this is selected, UTS will block intrusion when the following conditions are simultaneously met:</p> <ul style="list-style-type: none"> <li>The traffic matches an intrusion detection rule. For details, see <a href="#">Intrusion Detection Policy</a>.</li> <li>The matched rule has the <b>Block</b> action selected. For details, see <a href="#">Intrusion Detection Rules</a>.</li> </ul>
Web application detection, alerting, and blocking	<p>After this is selected, UTS will block web application threats when the following conditions are simultaneously met:</p> <ul style="list-style-type: none"> <li>The traffic matches a web application threat detection rule. For details, see <a href="#">Web Threat Detection Policy</a>.</li> <li>The matched rule has the <b>Block</b> action selected. For details, see <a href="#">Web Application Threat Detection Rules</a>.</li> </ul>
Malicious file detection, alerting, and blocking	<p>To enable malicious file detecting, alerting, and blocking, you must select the following options:</p> <ul style="list-style-type: none"> <li>Malicious file detection, alerting, and blocking</li> <li>Custom detection, alerting, and blocking</li> </ul> <p> <b>Note</b></p> <p>After this function is enabled, when traffic matches a malicious file detection policy (see <a href="#">Malicious File Detection Policy</a>), a custom blocking policy is automatically added on the <b>Custom Blocking Policy</b> page (see <a href="#">Custom Blocking Policy</a>) and subsequent sessions will be blocked.</p>
Threat intelligence-based detection, alerting, and blocking	<p>After this is enabled, traffic matching a threat intelligence-based detection policy (see <a href="#">Threat Intelligence-based Detection Policy</a>) will be blocked.</p>
Custom detection, alerting, and blocking	<p>After this is enabled, you need to further configure a policy. For details, see <a href="#">Custom Blocking Policy</a>.</p>

## Configuring Layer 3 Subinterface Forwarding

A layer 3 subinterface forwarding policy is used to map the destination IP address of a packet to a specific virtual local area network (VLAN).

On the page shown in [Figure 4-7](#), enable layer 3 subinterface forwarding. Then configure the MAC address for the layer 3 subinterface on the peer device and create a layer 3 interface forwarding policy as follows:

### Configuring the MAC Address of the Layer 3 Subinterface

Decide whether to configure a MAC address depending on the type of interface on the switch or router that the blocking interface of UTS connects to.

- Layer 2 interface: No MAC address needs to be configured.
- Layer 3 interface: The MAC address of the layer 3 interface on the peer device must be configured; otherwise, the peer device would drop RST packets.

On the page shown in [Figure 4-7](#), type the MAC address of the layer 3 subinterface and click **Save** to complete the configuration.

### Creating a Layer 3 Subinterface Forwarding Policy

UTS inspects and handles RST packets according to layer 3 subinterface forwarding policies. Specifically, it checks the destination IP address of an RST packet. If the destination IP address is within the IP range specified in a policy, UTS adds the VLAN ID of the corresponding layer 3 subinterface to the RST packet.

Click **Create**, configure parameters, and click **OK** to configure a layer 3 subinterface forwarding policy. The following table describes these parameters.

A layer 3 subinterface forwarding policy, after being created, can be edited and deleted.

Table 4-30 Parameters for configuring a layer 3 subinterface forwarding policy

Parameter	Description
Start IP/End IP	Specifies the start IP address and end IP address of a destination IP range. Both IPv4 and IPv6 are supported.
VLAN	VLAN ID, ranging from 1 to 4094. If the destination IP address of a packet is within the specified IP range, UTS adds this VLAN ID to the outbound RST packet.

## 4.7.2 Custom Blocking Policy

You can create a custom blocking policy and configure UTS to send blocking logs to ISOP.

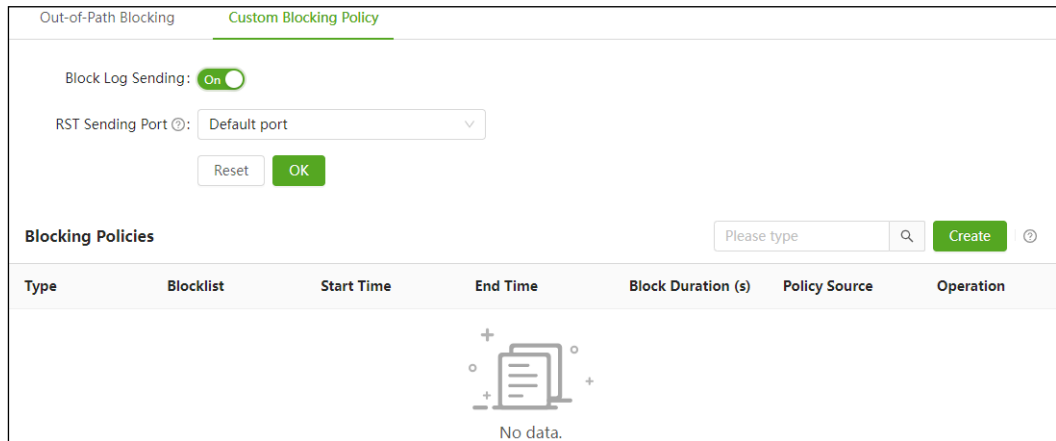


**Note**

The custom blocking policy can take effect and the blocking policies dispatched by ISOP can be saved only after the general switch of out-of-path blocking is turned on and **Custom detection, alerting, and blocking** is selected.

Choose **Policy > Out-of-Path Blocking > Custom Blocking Policy**. Enable blocking log sending, specify a port for sending RST packets, and create a blocking policy.

Figure 4-8 Custom Blocking Policy page



## Configuring General Parameters of Blocking Policies

At the top of the page shown in the preceding figure, configure general parameters of blocking policies and click **OK**. The following table describes these general parameters.

Table 4-31 General parameters of blocking policies

Parameter	Description
Block Log Sending	Controls whether to send logs generated upon triggering of custom blocking policies to ISOP. This is disabled by default.
RST Sending Port	Specifies a port to send RST packets. If the default port is selected, RST packets will be sent through the port where traffic is received. Using the default part will prolong the latency and significantly reduce the success rate of blocking. Therefore, you are advised not to select this option.

## Creating a Custom Blocking Policy


On the page shown in [Figure 4-8](#), click **Create**, configure parameters, and click **OK**. Then click **Apply Configuration** in the upper-right corner of the page to make the settings take effect. The following table describes parameters for configuring a custom blocking policy.

A custom blocking policy, after being created, can be queried, edited, and deleted.

Table 4-32 Parameters for configuring a custom blocking policy

Parameter	Description
Type	Type of the object to be blocked, which can be an IP address, IP range, session, or domain.
Time	Specifies a blocking duration.
Content	Specifies the object as follows:


Parameter	Description
	<ul style="list-style-type: none"> <li>• <b>IP:</b> specifies an IPv4 or IPv6 address.</li> <li>• <b>IP Range:</b> specifies an IPv4 or IPv6 range.</li> <li>• <b>Session:</b> specifies a session in the format of "source IP destination IP destination port". The source port is <b>0</b> by default. For IP addresses, both IPv4 and IPv6 are supported.</li> <li>• <b>Domain Name:</b> specifies a domain like www.xxx.com.</li> </ul>

 <b>Note</b>	<ul style="list-style-type: none"> <li>• Custom blocking policies can be created only after the general switch of out-of-path blocking is turned on and <b>Custom detection, alerting, and blocking</b> is selected.</li> <li>• When the blocking duration of a custom blocking policy expires, the policy is automatically deleted.</li> <li>• After a custom blocking policy is edited, with changes made, a new policy is automatically created. If no change is made, the current policy is automatically updated.</li> </ul>
--	---

## Viewing the Source of a Custom Blocking Policy

On the page shown in [Figure 4-8](#), you can view the source of a custom policy in the list of blocking policies. The following table describes the sources of custom policies.

Table 4-33 Sources of custom blocking policies

Policy Source	Description
WEB	Policy created on the web-based manager of UTS. For the configuration method, see <a href="#">Creating a Custom Blocking Policy</a> .
Internal policy	Policy automatically added upon triggering of a malicious file alert. When the blocking duration (180 seconds) expires, this policy is automatically deleted.
API	Policy dispatched by ISOP. For information on how to configure an API account, see <a href="#">API Account Configuration</a> .  <div style="display: flex; align-items: center;">  <div style="margin-left: 5px;"> <b>Note</b>                           When UTS collaborates with ISOP, you can use an API account to dispatch, cancel, and query blocking policies from ISOP.                     </div> </div>

# 5 Assets

Policies on UTS are configured based on asset objects. You need to define asset objects before configuring policies.

This chapter contains the following topics:

Topic	Description
<a href="#">Internal Network</a>	Describes how to configure an internal network object.
<a href="#">Asset Discovery</a>	Describes how to configure asset discovery-related parameters.
<a href="#">Asset Tree</a>	Describes how to configure and view asset trees.
<a href="#">5G NE</a>	Describes how to configure 5G network elements.

## 5.1 Internal Network

Internal network objects include network segments, nodes, IP pools, and ports.

### 5.1.1 Network Segment

Choose **Asset > Internal Network > Network Segment**. The default built-in network segments are **10**, **192.168**, and **172**, as shown in [Figure 5-1](#). You can add, edit, delete, query, import, and export network segments.

Figure 5-1 Network segment list

Network Segments (3)							Please type	Q	Import	Export	Bulk Delete	Add
<input type="checkbox"/>	No.	Name	Network Segment	Description	Invert	Operation						
<input type="checkbox"/>	110001	10	10.0.0.0/8	Default	No	<a href="#">Edit</a> <a href="#">Delete</a>						
<input type="checkbox"/>	110002	192.168	192.168.0.0/16	Default	No	<a href="#">Edit</a> <a href="#">Delete</a>						
<input type="checkbox"/>	110003	172	172.16.0.0/12	Default	No	<a href="#">Edit</a> <a href="#">Delete</a>						

### Adding a Network Segment

Click **Add** to add a network segment. Configure parameters and click **OK**. Then click **Apply Configuration** in the upper-right corner of the page to make the configuration take effect. [Table 5-1](#) describes parameters for adding a network segment.

Table 5-1 Parameters for adding a network segment

Parameter	Description
Name	Name of the network segment, which must be unique.
IP Address	IP address of the network segment in the format of IP address/mask. Both IPv4 and IPv6 addresses are supported.
Invert	Controls whether to invert the specified IP address segment. If <b>Yes</b> is selected, other IP addresses than the specified address segment are used.
Description	Description cannot contain special characters including `~!@#\$\$%^&{}*;/ ;`

## Exporting Network Segments

Click **Export** to export all current network segments locally.

## Importing Network Segments

In addition to creating network segments online, you can import a network segment file to bulk import network segments. The file must be an .xls file and named in the format of network\_YYMMDD-HH-MM-SS. For details, see the note on the **Import Network Segment Asset File** page.

## Editing a Network Segment

In the network segment list, click **Edit** to edit a built-in or custom network segment.

## Deleting a Network Segment

In the network segment list, click **Delete** to delete a built-in or custom network segment.

Click **Bulk Delete** to bulk delete selected network segments.

### 5.1.2 Node

Choose **Asset > Internal Network > Node** to add and configure a node. The configuration and operation methods for nodes are similar to those for network segments. For details, see [Network Segment](#).

### 5.1.3 IP Pool

An IP pool is a range of consecutive IPv4 or IPv6 addresses, defined by a start IP address and an end IP address.

Choose **Asset > Internal Network > IP Pool**. Click **Add** to add an IP pool. Configure parameters and click **OK**. Then click **Apply Configuration** in the upper-right corner of the page to make the configuration take effect. [Table 5-2](#) describes parameters for adding an IP pool.

The operation methods for IP pools are similar to those for network segments. For details, see [Network Segment](#).

Table 5-2 Parameters for adding an IP pool

Parameter	Description
Name	Name of the IP pool, which must be unique.
Start IP	Start IP address of the IP pool. Both IPv4 and IPv6 addresses are supported.
End IP	End IP address of the IP pool. Both IPv4 and IPv6 addresses are supported.
Invert	Controls whether to invert the specified IP pool. If <b>Yes</b> is selected, other IP addresses than the specified IP pool are used.
Description	Description cannot contain special characters including `~!@#%&^&{}*./;`

## 5.1.4 Port

A port object is used for anomalous behavior detection on UTS, which is bound to a protocol, and source/destination port pair.

Choose **Asset > Internal Network > Port**. Click **Add** to add a port. Configure parameters and click **OK**. Then click **Apply Configuration** in the upper-right corner of the page to make the configuration take effect. [Table 5-3](#) describes parameters for adding a port.

The operation methods for ports are similar to those for network segments. For details, see [Network Segment](#).

Table 5-3 Parameters for adding a port

Parameter	Description
Protocol	Protocol to be bound to the port. Options include <b>TCP</b> and <b>UDP</b> .
Name	Name of the port, which must be unique. It should be a maximum of 128 characters long and cannot contain special characters including !#<>
Src Port	Source port number. The value range is 0–65535, where the value of 0 indicates that it can match any port.
Dst Port	Destination port number. The value range is 0–65535, where the value of 0 indicates that it can match any port.
Description	Description cannot contain special characters including !#<>

## 5.2 Asset Discovery

UTS supports passive asset discovery within a specified IP network segment, and outputs the asset discovery result to the **Asset Tree** page (see Asset Tree) after a learning cycle ends.

Choose **Asset > Asset Discovery** to enable asset discovery. By default, the asset discovery function is disabled. After the asset discovery is enabled, you can find the built-in asset

discovery task list, as shown in [Figure 5-2](#). You can create asset discovery tasks, and edit, delete, and query them.

Figure 5-2 Asset discovery

Asset Discovery Tasks (3)							
Task Name	Start IP	End IP	Public IP	Learning Cycle	Asset Group	Operation	
1	10.0.0.0	10.255.255.255	No	120	10	<a href="#">Edit</a>	<a href="#">Delete</a>
2	172.16.0.0	172.31.255.255	No	120	172	<a href="#">Edit</a>	<a href="#">Delete</a>
3	192.168.0.0	192.168.255.255	No	120	192	<a href="#">Edit</a>	<a href="#">Delete</a>

After the asset discovery function is enabled, click **Add** to create an asset discovery task. Configure parameters and click **OK**. Then click **Apply Configuration** in the upper-right corner of the page to make the configuration take effect. [Table 5-4](#) describes parameters for creating an asset discovery task.

Table 5-4 Description of asset discovery parameters

Parameter	Description
Task Name	Asset discovery task name, which should be a maximum of 32 characters long and cannot contain special characters.
Start IP	Start IP address for asset discovery. Both IPv4 and IPv6 addresses are supported.
End IP	End IP address for asset discovery. Both IPv4 and IPv6 addresses are supported.
Learning Cycle	Period of time allocated for discovering assets in an asset discovery task. The value range is 100–2048, in seconds.
Asset Group Name	Asset group name, which should be a maximum of 32 characters long and cannot contain special characters.
Public IP	Specifies whether the addresses within this IP address range are public IPs.

## 5.3 Asset Tree

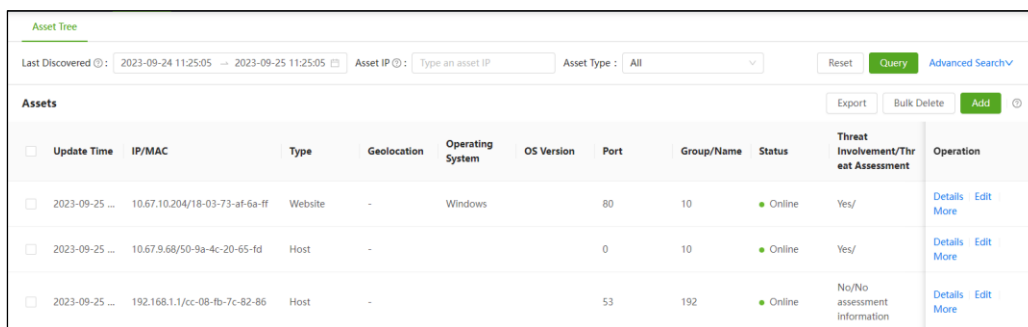
The asset tree encompasses the following two types of assets:

- Auto discovered assets: After an asset discovery task (see [Asset Discovery](#)) is created, UTS will learn asset information from the mirrored traffic. When a learning cycle ends, UTS will display the asset discovery result in the asset tree list. The attributes of discovered assets will change with the actual situation.
- Manually added assets: The asset information is manually added by the user. The attributes of manually added assets will not change.

Choose **Asset > Asset Tree > Asset Tree**. The asset tree list displays auto discovered assets and manually added assets, as shown in [Figure 5-3](#). You can view, query, add, edit, and delete asset information, and can also view threat information associated with asset IPs.



Figure 5-3 Asset tree list



Update Time	IP/MAC	Type	Geolocation	Operating System	OS Version	Port	Group/Name	Status	Threat Involvement/Threat Assessment	Operation
2023-09-25 ...	10.67.10.204/18-03-73-af-6a-ff	Website	-	Windows		80	10	Online	Yes/	Details Edit More
2023-09-25 ...	10.67.9.68/50-9a-4c-20-65-1d	Host	-			0	10	Online	Yes/	Details Edit More
2023-09-25 ...	192.168.1.1/cc-08-fb-7c-82-86	Host	-			53	192	Online	No/No assessment information	Details Edit More

## Viewing Asset Information

Table 5-5 describes parameters in the asset tree list shown in Figure 5-3.

Table 5-5 Description of asset information

Parameter	Description
Update Time	Time when the asset was discovered.
IP/MAC	IP and MAC addresses of the asset.
Type	Asset type. Options are <b>Host</b> , <b>Website</b> , and <b>Network</b> .
Geolocation	Geographical location of the asset. After the GeoIP database is imported offline, UTS can query the geographic location of an asset based on its IP address. For information on how to import the GeoIP database, see <a href="#">Offline Upgrade</a> .
Operating System	Name of the operating system (OS) installed on the asset.
OS Version	Operating system version.
Port	Port of the asset used for providing a service.
Asset Group	Asset group to which the asset belongs.
Status	Status of the asset. Options are <b>Online</b> and <b>Offline</b> . For an automatically discovered asset, if UTS does not receive any traffic from the asset within 24 hours, the asset's status will change to <b>Offline</b> . On the other hand, if UTS receives traffic from the asset within 24 hours, the status will be displayed as <b>Online</b> .
Threat Involvement/Threat Assessment	<ul style="list-style-type: none"> <li><b>Threat Involvement:</b> Specifies whether the asset is involved in a threat, which may be an attack source or attack target. Options are <b>Yes</b> and <b>No</b>.</li> <li><b>Threat Assessment:</b> Specifies the attack result for the asset.</li> </ul>
Operation	You can perform the following operations: <ul style="list-style-type: none"> <li>Edit the asset information.</li> <li>Delete the asset information.</li> <li>If an asset is involved in threats, click <b>IP associated threats</b> to view the threat analysis information associated with the asset IP.</li> </ul>

## Querying Assets

The asset tree query section as shown in Figure 5-3 provides basic asset query criteria. Click **Advanced Search** for more precise queries. Table 5-6 describes parameters for setting query conditions.

Table 5-6 Description of asset query parameters

Parameter	Description
Last Discovered	Specifies the time range for asset discovery or manual addition.
Asset IP	Specifies a single IP address for an asset query. Both IPv4 and IPv6 addresses are supported.
Asset Type	Options include <b>All</b> , <b>Host</b> , <b>Website</b> , and <b>Network</b> .
Asset Endpoint	Expand the asset group to select an asset endpoint. Multiple selections are supported.

## Manually Adding an Asset

Click **Add** to add an asset. Configure asset parameters and click **OK**. Then click **Apply Configuration** to make the configuration take effect. Table 5-7 describes parameters for adding an asset.

Table 5-7 Parameters for adding an asset

Parameter	Description
Name	Name of the asset. It should be a maximum of 32 characters long and cannot contain special characters.
IP	IP address of the asset. Only IPv4 addresses are supported.
MAC	MAC address of the asset.
Asset Type	Type of the asset. Options are <b>All</b> , <b>Host</b> , <b>Website</b> , and <b>Network</b> .
Asset Endpoint	You can expand the asset group to select options.
Asset Group	After you select the asset endpoint, the asset group is filled in automatically and cannot be modified manually.
Status	Status of the asset, which can be either <b>Online</b> or <b>Offline</b> .
Threat Involvement	Specifies whether the asset is involved in threats as an attack source or attack target.
Assessment Result	Specifies the attack result.

## Exporting Assets


Click **Export** to export all assets that meet the specified query criteria locally.

## 5.4 5G NE

UTS can recognize 5G network element (NE) information from mirrored traffic and can detect IP addresses in 5G traffic based on the 5G NE configuration. If a matching IP address is detected, the **Source NE Type** or **Destination NE Type** in the 5G metadata log will be displayed as the NE type.

The 5G NE information in the 5G NE list is categorized into two types:

- **Automatically learned information:** Once 5G traffic is detected in mirrored traffic, UTS will automatically parse the source or destination NE types based on the traffic and generate 5G NE information, which is then displayed in the 5G NE list.
- **Manually added information:** It refers to the 5G NE information that users manually add or import. It also includes that automatically learned 5G NE information confirmed by users.

 <b>Note</b>	Manually configured 5G NE information has higher priority than automatically recognized 5G NE information. When finding multiple matches, the system will prioritize the manually configured 5G NE information entry.
--	---

Choose **Asset > 5G NE**. The 5G NE list displays manually configured 5G NE information and automatically learned 5G NE information. You can edit, delete, query, and confirm 5G NE information, as shown in [Figure 5-4](#).

Figure 5-4 5G NE list

5G NEs								
IP	Port	NE Type	MAC Address	Details	Update Time	Confirm	Operation	
<input type="checkbox"/>	2000:23	80	SMSF	00:0c:29:35:d0:c1c	-	2023-09-25 10:33:53	Confirmed	Edit Delete
<input type="checkbox"/>	2000:21	0	AMF	00:0c:29:f6:5d:fa	-	2023-09-25 10:33:14	Confirmed	Edit Delete
<input type="checkbox"/>	10.130.70.65	0	AMF	fa:16:3e:e2:dd:dc	-	2023-09-25 10:32:27	Confirmed	Edit Delete
<input type="checkbox"/>	10.130.70.80	80	NRF	88:df:9e:32:f2:d1	-	2023-09-25 10:31:46	Confirmed	Edit Delete

### Manually Adding 5G NEs

If 5G traffic signatures of an NE are not enough for UTS to determine its NE type, you can manually add this NE to the 5G NE list. You can manually add and import 5G NEs. The following describes how to manually add a 5G NE.

Click **Add**, configure 5G NE parameters, and click **OK**. Then click **Apply Configuration** to make the configuration take effect. [Table 5-8](#) describes parameters for adding a 5G NE.

Table 5-8 Parameters for adding a 5G NE

Parameter	Description
IP	IP address of the 5G NE.
Port	Port number of the 5G NE.

Parameter	Description
NE Type	Type of the 5G NE.
MAC Address	MAC address of the 5G NE.
Details	Provides a description of the 5G NE.

## Confirming 5G NEs

In the 5G NE list, 5G NEs marked as **Unconfirmed** are automatically learned by UTS.

Click **Confirm** in the **Operation** column to confirm the accuracy of the information. After confirmation, 5G NEs are marked as **Confirmed**. The priority of these NEs is equivalent to that of manually configured NEs.

# 6 System

This chapter contains the following topics:

Topic	Description
<a href="#">Diagnostic Tools</a>	Describes how to use built-in diagnostics tools.
<a href="#">System Configuration</a>	Describes how to configure system parameters.
<a href="#">System Upgrade</a>	Describes online and offline upgrade methods for system engines and system rule bases.
<a href="#">Backup and Restoration</a>	Describes how to back up and restore system data.
<a href="#">System Control</a>	Describes several control operations on UTS, which include applying configuration, restarting the engine, restarting the system, shutting down the system, and restarting the logging process.
<a href="#">Storage Management</a>	Describes how to configure storage on UTS.

## 6.1 Diagnostic Tools

UTS offers basic network diagnostic tools, packet capture, and one-click diagnosis capabilities to assist users in troubleshooting network problems.

### 6.1.1 Ping/TraceRoute/Network Connection Status/Network Card Status/Routing Information/Playback Testing

Choose **System > Diagnostic Tools** and click the following tabs to use tools: **Ping**, **Traceroute**, **Network Connection Status**, **NIC Status**, **Routing Information**, and **PACP Playback**. For example, you can use these tools to detect whether the connection is normal between the system and the target network. [Table 6-1](#) describes the usage of diagnostic tools.

Table 6-1 Diagnostic tools

Tool Name	Parameter	Purpose
Ping	<b>IP Address:</b> IPv4 address of the target.	Checks the connection, response time, and domain name resolution accuracy between the system and the target host.
Traceroute	<b>IP Address:</b> IPv4 address of the target.	Displays the path taken by a data packet from the source host to the target host and

Tool Name	Parameter	Purpose
		also provides information about the time it arrives at each intermediate node.
Network Connection Status	None.	Displays network connection information, including the protocol and port.
NIC Status	None.	Views the NIC status of a specified device to help users troubleshoot NIC faults.
Routing Information	None.	Displays the real-time routing information of the system.
PCAP Playback	<ul style="list-style-type: none"> <li>• <b>PCAP File:</b> Click <b>Upload File</b> to choose a PCAP file and upload it.</li> <li>• <b>Playback Interface:</b> From the drop-down list, select a monitoring interface through which data will flow during the playback test.</li> </ul>	UTS allows users to access packet capture files and view playback data through the playback interface, thereby assisting in the analysis of network data.

## 6.1.2 Packet Capture

Choose **System > Diagnostic Tools > Packet Capture** to configure packet capture on a specified device interface. The captured file can be used for analyzing and debugging related issues during network deployment.

To capture packets, follow these steps:

### Step 1 Configure packet capture parameters.

- a. In the **Parameter Settings** area, configure packet capture parameters. [Table 6-2](#) describes the packet capture parameters.
- b. Click **OK** to save the settings.

You can also click **Restore Defaults** to restore the default settings.

Table 6-2 Parameters for configuring a packet capture task

Parameter	Description
Duration (s)	Duration of the packet capture task. The packet capture will stop once the specified duration expires. By default, the duration is set to <b>0</b> , which means that there is no limit on the packet capture duration.
Number of Packets	Number of packets to be captured. The packet capture will stop once the specified value is reached. By default, it is set to <b>0</b> , which means that there is no limit on the number of packets.
Max Bytes (KB)	Number of bytes to be captured. The packet capture will stop once the specified value is reached. By default, it is set to <b>0</b> , which means that there is no limit on the number of bytes.

### Step 2 Configure filtering rules.

- a. In the **Filtering Rules** area, click **Create**.

- b. Configure filtering rule parameters. [Table 6-3](#) describes parameters for creating a filtering rule.
- c. Click **OK**.
- d. When a packet capture filtering rule is created, it is enabled by default. You can disable, edit, and delete the rule.

Table 6-3 Parameters for configuring a packet capture filtering rule

Parameter	Description
File Name	Name of the packet capture task. Data packets that meet the filtering rule will be saved in this file. The name can only contain lowercase and uppercase letters and digits.
Interface	Specifies an interface from which packets are captured. The default value is <b>any</b> , which means that packets are captured on all interfaces except the management interface.
Protocol	Specifies a protocol. Packets of this protocol will be captured. Options are <b>any</b> , <b>IP</b> , <b>TCP</b> , <b>UDP</b> , and <b>ICMP</b> . The default value is <b>any</b> , which means that packets of all types of protocols are captured.
Tx/Rx Interface	Specifies the direction from which packets are captured in the network interface. <ul style="list-style-type: none"> <li>• Rx interface: indicates that incoming packets are captured from the interface.</li> <li>• Tx interface: indicates that outgoing packets are captured from the interface.</li> </ul>
Src IP/Mask/Src port	Specifies the source IP or source port where the packet capture task starts. Both IPv4 and IPv6 addresses are supported. By default, there is no limit on the source IP address.
Dst IP/Mask/Dst port	Specifies the destination IP or destination port where the packet capture task starts. Both IPv4 and IPv6 addresses are supported. By default, there is no limit on the destination IP address.

**Step 3** Start the packet capture task.

- a. In the **Control** area, click **Start** to start capturing packets.
- b. When the rule is enabled, if the packet capture task starts, the system will capture all data packets that match the rule and save them in the specified file.

**Step 4** Stop the packet capture task.

- a. UTS automatically stops packet capture once any of the following values is reached: the packet capture duration, the number of packets, or the number of bytes.
- b. During packet capture, you can click **Stop** to terminate the ongoing capture task.

**Step 5** In the **Control** area, click **Download** to download the captured file locally for analysis.

---End

### 6.1.3 One-Click Diagnosis

Choose **System > Diagnostic Tools > One-Click Diagnosis**. Then click **Download** to download collaboration logs locally for troubleshooting.

## 6.1.4 Fault Diagnosis

Choose **System > Diagnostic Tools > Fault Diagnosis** to send fault diagnosis information to designated email addresses through email.


This function is available only to NSFOCUS technical support personnel for debugging purposes. You can ignore it.

## 6.2 System Configuration

Choose **System > System Configuration** to configure network interfaces, static routing, DNS, device, special parameters, encryption methods, log-related parameters, cloud environment adaptation parameters, and custom product name and logo.

### 6.2.1 Interface

On the **Interface** tab page under **System Configuration**, you can manage the monitoring and management interfaces of UTS.

 <b>Note</b>	Monitor interfaces of UTS can be configured to function as management interfaces.
---	---

Choose **System > System Configuration > Interface** to view the interface list of UTS. The page may vary with the type of device used.

[Figure 6-1](#) shows the interface list of UTS (hardware edition), and [Figure 6-2](#) shows the interface list of UTS (virtual machine edition).

Figure 6-1 Interface list of UTS (hardware version)

Interfaces (10)							
Interface Name	IPv4 Address	IPv6 Address	Netmask	Duplex Mode	Connection Rate (Mbps)	Interface Type	Operation
M	10.67.5.145/22		255.255.252.0	auto	auto	Management	<a href="#">Edit</a>
H1	192.168.2.1/24		255.255.255.0	auto	auto	Management	<a href="#">Edit</a>
T2/1	0.0.0.0/0		0.0.0.0	auto	auto	Monitor	<a href="#">Edit</a> <a href="#">Enable</a> <a href="#">Disable</a>
T2/2	0.0.0.0/0		0.0.0.0	auto	auto	Monitor	<a href="#">Edit</a> <a href="#">Enable</a> <a href="#">Disable</a>
T2/3	0.0.0.0/0		0.0.0.0	auto	auto	Monitor	<a href="#">Edit</a> <a href="#">Enable</a> <a href="#">Disable</a>
T2/4	0.0.0.0/0		0.0.0.0	auto	auto	Monitor	<a href="#">Edit</a> <a href="#">Enable</a> <a href="#">Disable</a>
G1/1	0.0.0.0/0		0.0.0.0	auto	auto	Monitor	<a href="#">Edit</a> <a href="#">Enable</a> <a href="#">Disable</a>
G1/2	0.0.0.0/0		0.0.0.0	auto	auto	Monitor	<a href="#">Edit</a> <a href="#">Enable</a> <a href="#">Disable</a>
G1/3	0.0.0.0/0		0.0.0.0	auto	auto	Monitor	<a href="#">Edit</a> <a href="#">Enable</a> <a href="#">Disable</a>
G1/4	0.0.0.0/0		0.0.0.0	auto	auto	Monitor	<a href="#">Edit</a> <a href="#">Enable</a> <a href="#">Disable</a>



Figure 6-2 Interface list of UTS (virtual machine version)

Interfaces (3)							
Interface Name	IPv4 Address	IPv6 Address	Netmask	Duplex Mode	Connection Rate (Mbps)	Interface Type	Operation
M	10.67.5.204/22		255.255.252.0	auto	auto	Management	<a href="#">Edit</a>
H1	192.168.2.1/24		255.255.255.0	auto	auto	Management	<a href="#">Edit</a>
T1/1	0.0.0.0/0		0.0.0.0	auto	auto	Monitor	<a href="#">Enable</a> <a href="#">Disable</a>

## Configuring Management Interfaces

UTS has two management interfaces: M interface and H1 interface. M interface is generally used for management, while H1 interface is used for collaboration with ISOP.

Choose **System > System Configuration**. In the interface list, click **Edit** to edit a management interface and click **OK**. Then click **Apply Configuration** in the upper-right corner of the page to make the configuration take effect. [Table 6-4](#) describes interface parameters.

Table 6-4 Description of interface parameters

Parameter	Description
Interface Name	Name of the interface, which cannot be changed.
Interface Type	Type of the interface. Options are: <ul style="list-style-type: none"> <li>• <b>Management</b>: This interface type cannot be changed.</li> <li>• <b>Monitor</b>: This interface type can be changed to <b>Management</b>.</li> </ul> After the interface type is changed, restart the engine to make the configuration take effect.
IPv4 Address	IPv4 address of the interface. The IP address should not be in the same network segment as the management ports (including M port).
IPv4 Mask	IPv4 mask of the interface.
IPv6 Address	IPv6 address of the interface and its prefix. Example: 2001:abcd:123:1::/64.

## Configuring a Monitor Interface to Function as a Management Interface

This feature is available only on UTS hardware edition.

In the interface list, click **Edit** in the **Operation** column. Set the interface type of a **Monitor** interface to **Management**, and configure an IP address and netmask. Click **OK**. [Table 6-4](#) describes parameters for configuring interfaces.

## Enabling/Disabling a Monitor Interface

In the interface list, click **Enable** or **Disable** in the **Operation** column of an interface to enable or disable this interface.

## 6.2.2 Static Route

A static route is a route manually configured by the administrator. Such routes are used for small-scale networks that are not changed constantly. As static routes cannot be adaptive to network changes, you must manually adjust them after the network topology changes.

Default routes are a special type of static routes, with 0.0.0.0/0 as the destination IP address. The routing device uses a default route to forward packets for which no matching route is found in the routing table. If no default route is configured, the routing device will drop such packets.




- When configuring an IPv4 static route, you can configure a default route by specifying 0.0.0.0 as the destination address and 0.0.0.0 as the netmask. If the destination address of IPv4 packets fails to match any route in the routing table, these packets are forwarded via the default IPv4 route.
- When configuring an IPv6 static route, you can configure a default route by specifying 0::0 (with the prefix of 0) as the destination address. If the destination address of IPv6 packets fails to match any route in the routing table, these packets are forwarded via the default IPv6 route.

Choose **System > System Configuration > Static Route**. Click **Create**. Configure static route parameters and click **OK**. Then click **Apply Configuration** in the upper-right corner of the page to make the configuration take effect. [Table 6-5](#) describes parameters for configuring a static route

After a static route is created, you can query, edit, and delete it.

Table 6-5 Parameters for configuring a static route

Parameter	Description
Static Route Name	Specifies the name of the static route.
Destination IP	Specifies the destination address or network of data packets. You can type an IPv4 address and its subnet mask for an IPv4 route or an IPv6 address and its prefix for an IPv6 route.   The static route 0.0.0.0/0 (IPv4) or ::/0 (IPv6) serves as the default route, indicating that when packets fail to match any route in the routing table, packets will be forwarded based on the default route.
Gateway	Specifies the gateway of the static route. It is usually set to the ingress IP address of the next-hop device.
Interface	Specifies the egress interface for forwarding packets.
Priority	Specifies the priority of the static route. The value range is 1–30. A smaller value indicates a higher priority.  When there are multiple static routes to the same destination IP address, the route with the highest priority is chosen as the optimal one.

## 6.2.3 DNS

As an essential component of the Internet infrastructure, the Domain Name System (DNS) service is responsible for mapping domain names to their IP addresses. As a DNS client, UTS can request the domain name resolution service from a designated DNS server.

Choose **System > System Configuration > DNS**. Configure IP addresses for the DNS servers and click **OK**. Click **Apply Configuration** in the upper-right corner of the page to make the configuration take effect. [Table 6-6](#) describes parameters for configuring DNS servers.

Table 6-6 Parameters for configuring DNS servers



Parameter	Description
DNS Server 1	Specifies the IP address of the preferred DNS server. Both IPv4 and IPv6 addresses are supported. This field is required.
DNS Server 2	Specifies the IP address of the alternate DNS server. Both IPv4 and IPv6 addresses are supported. This field is required.


## 6.2.4 Device

Choose **System > System Configuration > Device** to configure device parameters.

**Step 1** Configure parameters. [Table 6-7](#) describes parameters for configuring the device.

Table 6-7 Parameters for configuring a device

Parameter	Description
HTTPS Port	Specifies the port number used for HTTPS login to UTS. By default, it is <b>443</b> and ranges from 1024 to 65535.  <b>Note</b> After changing the port number, you need to log in again.
Firewall Ports to Block	Specifies the port to be blocked on the built-in firewall of UTS. Multiple ports can be blocked. After these ports are blocked, external connections will not be able to access these internal ports.  <b>Note</b> Note that blocking certain ports may cause some UTS functions to fail to work properly. Therefore, use this feature with caution. For example, disabling port 22 will cause SSH remote connection to be unavailable. Disabling port 443 may cause web pages to be inaccessible.
Remote Assistance	It is available only to NSFOCUS technical support personnel for network debugging purposes. You can ignore it. For details, see <a href="#">错误!未找到引用源。</a> .
Allowed IP	When <b>Remote Assistance</b> is set to <b>Yes</b> , add the IP address of the client for remote connection to this UTS device. Click <b>Add</b> to add up to three allowed IP addresses. Both IPv4 and Ipv6 addresses are supported.

Parameter	Description
Ping (ICMP)	<ul style="list-style-type: none"> <li>• <b>Yes:</b> indicates that UTS responds to ICMP requests, thereby facilitating device debugging.</li> <li>• <b>No:</b> indicates that UTS does not respond to ICMP requests.</li> </ul>
Time Sync	The accuracy of the system time is crucial for the logging and alerting functions. The system provides the time configuration function to ensure the accuracy of the system time. Two methods are offered: <ul style="list-style-type: none"> <li>• <b>Auto:</b> automatically synchronizes the system time with the designated time synchronization server.</li> <li>• <b>Manual:</b> manually configures the system time and time zone.</li> </ul>
Time Sync Server	Specifies the IP address of the time synchronization server when <b>Time Sync</b> is set to <b>Auto</b> . Ensure the proper communication between the management interface and the time synchronization server (NTP server).
Sync Interval	Specifies the interval at which UTS automatically synchronizes its time with the NTP server when <b>Time Sync</b> is set to <b>Auto</b> . The interval is expressed in seconds.
Time	When <b>Time Sync</b> is set to <b>Manual</b> , you need to configure the clock of UTS.  Note After configuration, restart the system to make the configuration take effect.
Time Zone	When <b>Time Sync</b> is set to <b>Manual</b> , you need to configure the time zone where the UTS device is currently located.
Device Name	Device name. After the configuration takes effect, click <b>System Information</b> in the system status bar at the bottom of the page to view the device name.
Device Location	Device location. After the configuration takes effect, click <b>System Information</b> in the system status bar at the bottom of the page to view it.

## Step 2 Submit the configuration.

- a. When the remote assistance function is enabled, click **Save and Generate Remote Assistance Key**. The login QR code and login key will appear on the page.
  - Scan the QR code to generate a login key, or directly copy the login key displayed on the page.
  - Use the login key to calculate and generate the remote assistance login password, which is exclusively accessible to NSFOCUS technical support personnel.
- b. When the remote assistance function is disabled, click **Save**.

## Step 3 Click **Apply Configuration** in the upper-right corner of the page to make the configuration take effect.

---End

## 6.2.5 Special Parameters

Special parameters are offered to fine-tune UTS for special network environments. Under normal conditions, users do not need to modify them. Modifying special parameters may lead to system or network exceptions. To avoid any issues, you are advised to seek assistance from NSFOCUS technical personnel when you need to modify these parameters.

## 6.2.6 Encryption

You can configure encryption settings to specify how an exported PCAP file and malicious file are encrypted. After the encryption method is specified, the exported PCAP file and malicious files will be encrypted accordingly for security purposes.

Choose **System > System Configuration > Encryption**. Specify an encryption method and click **OK**. Then click **Apply Configuration** in the upper-right corner of the page to make the configuration take effect. [Table 6-8](#) describes the encryption parameters.

Table 6-8 Description of encryption parameters

Parameter	Description
Encryption Method	<ul style="list-style-type: none"> <li><b>None</b>: Exported PCAP files and malicious files are not encrypted. Choosing this option poses a security risk.</li> <li><b>AES</b>: Exported PCAP files and malicious files are AES encrypted.</li> <li><b>Chacha20</b>: Exported PCAP files and malicious files are Chacha20 encrypted.</li> </ul>
AES Password	When the encryption method is set to <b>AES</b> , you need to configure an AES password of 16 characters long.
Offset	When the encryption method is set to <b>AES</b> , you need to configure a 16-bit AES offset.
ChaCha20 Password	When the encryption method is set to <b>ChaCha20</b> , you need to configure a ChaCha20 password of 32 characters long.
Random Number	When the encryption method is set to <b>ChaCha20</b> , you need to configure an 8-bit ChaCha20 random number.

## 6.2.7 Log Configuration

Log configuration includes the settings of local log storage as well as log forwarding to ISOP through the A interface channel.

Choose **System > System Configuration > Log Configuration**. Configure local log storage, log generation, and anomalous behavior logging, and click **OK**. Click **Apply Configuration** in the upper-right corner of the page to make the configuration take effect. [Table 6-9](#) describes log configuration parameters.

Table 6-9 Description of log configuration parameters

Parameter	Description
Local log storage parameters	<p>Log Types to Save</p> <p>Specifies the type of logs to be saved on UTS.</p> <ul style="list-style-type: none"> <li><b>None</b>: does not store any logs.</li> <li><b>Threat log</b>: stores threat alert logs only.</li> <li><b>Threat log + threat related metadata</b>: stores threat alert logs and threat-related metadata logs only.</li> <li><b>All logs</b>: store all logs. In general, <b>All logs</b> is not recommended. It is only applicable for low-volume traffic scenarios. For example, traffic throughput is below 100 Mbps.</li> </ul>

	Max Batch Size	Whenever the number of log entries reaches the threshold, a batch storage is performed. The value range is 500–100000.
	Timeout	When the batch storage period expires, the storage action will be automatically executed for log entries, regardless of whether the number of log entries reaches the maximum batch storage threshold.  To achieve optimal storage performance, the default timeout period is set to <b>5</b> seconds.
Log generation parameters	Log Types to Generate	Specifies the type of logs generated by UTS and that to be forwarded by UTS. <ul style="list-style-type: none"> <li>• <b>All logs:</b> forwards all logs.</li> <li>• <b>Threat log + threat related metadata:</b> forwards threat alert logs and threat-related metadata logs only.</li> <li>• <b>Threat log:</b> forwards threat alert logs only.</li> </ul>
Anomalous behavior logging parameters	Anomalous Behavior Logging	After it is enabled, a log will be generated for any anomalous behaviors.

## 6.2.8 Cloud Environment Adaptation

UTS supports cloud environment adaptation, and the agent of NSFOCUS Unified Endpoint Security Management (UES) can capture cloud threat traffic. The agent transmits encrypted and compressed mirrored traffic to UTS for protocol resolution, threat detection, full traffic retention, and response management of threat events.

Choose **System > System Configuration > Cloud Environment Adaption**. Configure cloud environment parameters and click **OK**. Then click **Apply Configuration** in the upper-right corner of the page to make the configuration take effect. [Table 6-10](#) describes cloud environment adaptation parameters.

Table 6-10 Cloud Environment Adaptation

Parameter	Description
Enable Adaptation	Click to enable or disable the cloud environment adaptation function.
Server IP	Specifies the IP address of the server. Only IPv4 addresses are supported. Generally, it is the IP address of the management port of UTS. By default, it is set to <b>0.0.0.0</b> , which indicates all addresses.
Port	Specifies the port number of the server, ranging from 1 to 65535. The port number is determined through the negotiation between UTS and UES during deployment.

## 6.2.9 Custom Product Name and Logo

Choose **System > System Configuration > Custom Product Name & Logo** to customize the product name, abbreviation, and logo, which are displayed on the web-based manager.

## Changing the Product Name and Abbreviation

After changing the product name and abbreviation, click **OK**. [Table 6-11](#) describes product name parameters.

Table 6-11 Description of product name parameters

Parameter	Description
Product Name	Product name that is displayed on the login page and operation page of the web-based manager. By default, it is set to <b>UTS</b> . When you customize the product name, ensure that no special characters are included.
Abbreviation	Abbreviated version of the product name that is displayed on the web login page. By default, it is set to <b>UTS</b> . When you change it to another abbreviation, ensure that no special characters are included.

## Changing the Product Logo

After customizing the login logo and product logo, click **Upload**. Then click **Apply Configuration** in the upper-right corner of the page to make the configuration take effect. [Table 6-12](#) describes product name parameters.

Click **Restore Defaults** to restore them to factory settings.

Table 6-12 Parameters for configuring the login logo and product logo

Parameter	Description
Custom Login Logo	Click <b>+logo</b> to upload the login page logo of the UTS web-based manager. The name of the image file must be <b>logo.png</b> , and the minimum image resolution should be 50 x 23.
Custom Product Logo	Click <b>+ns_logo</b> to upload the product logo, which will be displayed in the upper left corner of the operation page. The name of the image file must be <b>ns_logo.png</b> , and the minimum image resolution should be 176 x 27.

## 6.3 System Upgrade

UTS supports online upgrade and offline upgrade.

### 6.3.1 Update

Choose **System > System Upgrade > Update** to view information about the current system engine version and system rule base version. If the current UTS device can connect to the NSFOCUS software upgrade link at <http://update.nsfocus.com/>, you can see the automatically downloaded upgrade packages here.

## 6.3.2 Online Upgrade

If the UTS device can access the Internet, choose **System> System Upgrade> Online Upgrade** to upgrade the system engine and system rule base online. Both instant and automatic upgrades are supported.



Note

- A prerequisite for the two types of upgrades is that UTS can access the Internet. You need to configure a correct DNS server's IP address on UTS so that UTS can connect to the NSFOCUS website for update. For details, see [DNS](#).
- The DNS server's IP address should not be used for interface configuration. Otherwise, an IP address conflict would occur and the update would fail. For interface configuration methods, see [Interface](#).

### Instant Upgrade

In the **Instant Upgrade** area, configure instant upgrade parameters and click **Upgrade Now** to immediately upgrade the system engine and system rule base. Click the **Online Upgrade History** tab in the lower half of the page to view the history of instant upgrades. [Table 6-13](#) describes instant upgrade parameters.

To change the upgrade address only, change the upgrade URL and click **Modify Address**.

Table 6-13 Parameters for configuring instant upgrade

Parameter	Description
Upgrade URL	Network address where the system upgrade package is located, which is <b>update.nsfocus.com</b> by default. The value must be a URL without http://.
Include Engine	Controls whether to upgrade the system engine during the upgrade. <b>Yes:</b> upgrades both the system engine and system rule base during online upgrade. <b>No:</b> upgrades the system rule base only during online upgrade.


### Automatic Upgrade

If scheduled upgrade is enabled, the system automatically checks for new updates. If a new update is detected, the system will upgrade both the engine and system rule base at the specified time. The entire update process requires no manual intervention.

In the **Automatic Upgrade** area, configure automatic upgrade parameters, and click **OK**. Click **Apply Configuration** to make the configuration take effect. Click the **Online Upgrade History** tab in the lower half of the page to view the history of automatic upgrades. [Table 6-14](#) describes parameters for configuring automatic upgrade.




Table 6-14 Parameters for configuring automatic upgrade

Parameter	Description
Automatic Upgrade	<ul style="list-style-type: none"> <li>• <b>Auto:</b> The system automatically checks for updates and the system will be automatically upgraded once a new upgrade package is detected.</li> <li>• <b>Scheduled:</b> The system automatically checks for the latest upgrade package and the system will be upgraded at the specified time. When scheduled upgrade is enabled, you need to specify the day of the week and the specific hourly time for the upgrade.</li> <li>• <b>Disable:</b> By default, the scheduled upgrade function is disabled.</li> </ul>  <p><b>Note</b></p> <p>It is recommended that you choose a specific time period during the night when network traffic is at its minimum for smooth automatic upgrade.</p>
Include Engine	<p>When either of <b>Auto</b> and <b>Scheduled</b> is selected, you need to choose whether to upgrade the system engine during the process.</p> <ul style="list-style-type: none"> <li>• <b>Yes:</b> Upgrades both the system engine and system rule base during online upgrade.</li> <li>• <b>No:</b> Upgrades the system rule base only during online upgrade.</li> </ul>
Frequency	<p>When scheduled upgrade is selected, you need to choose the specific day of the week to initiate it.</p> <p>If <b>Daily</b> is selected, it means that a scheduled upgrade is performed every day.</p>
Time	<p>When scheduled upgrade is selected, you also need to select the time at which the scheduled upgrade is started.</p>

## Collaboration with NTI

After collaboration with NTI is enabled, if UTS can access the Internet, the NTI intelligence database can be updated online at the scheduled time.

 <b>Note</b>	<p>The update of NTI intelligence database fully overwrites the existing threat information. This means that the intelligence information within the current storage cycle will overwrite the intelligence information from the previous storage cycle, ensuring that the information remains up to date.</p>
--	---

In the **Collaboration with NTI** area, configure collaboration parameters, and click **OK**. Click **Apply Configuration** to make the configuration take effect. Click the **NTI Upgrade History** tab in the lower half of the page to view the history of automatic NTI updates. [Table 6-15](#) describes parameters for configuring collaboration with NTI.

Table 6-15 Parameters for configuring collaboration with NTI

Parameter	Description
Collaboration	After collaboration with NTI is enabled, the NTI intelligence database will be updated online according to the settings.

Parameter	Description
Confidence	During online intelligence information update, UTS saves only intelligence information with a credibility level above the set value in the intelligence database. The range is 0–100, with <b>80</b> as the default.
Credibility	During online intelligence information update, UTS saves only intelligence information with a credibility above the set value in the intelligence database . The range is 1–5, with <b>3</b> as the default.
Severity	During online intelligence information update, UTS saves only intelligence information in the intelligence database with a severity above the set value. The range is 1–5, with <b>5</b> as the default.
Retention Period	Specifies a duration for which NTI information is retained during online upgrade. The value range is 1–30, in days, with <b>7</b> as the default.


### 6.3.3 Offline Upgrade

You can access NSFOCUS's official website to download the system upgrade files, rule base upgrade files, WAF upgrade files, NTI database upgrade files, geodatabase upgrade files, virus signature database upgrade files, and assessment rule base upgrade files to local disk drive. Then you can import these upgrade files offline to upgrade UTS.

Choose **System > System Upgrade > Offline Upgrade** . Select the upgrade file type from the drop-down list, click **Choose File** to import the upgrade file, and click **Upload**. Then follow the prompts to complete the offline upgrade. [Table 6-16](#) describes the upgrade file types.

After offline upgrade, you can view the current version information about the system, various rule bases, virus database, and geodatabase in the middle section of the page. At the bottom of the page, you can view the history of offline upgrades.

Table 6-16 Upgrade file types

Parameter	Description
System (*.bin)	Imports the system engine upgrade file to upgrade the system engine of UTS. Restart the system after the upgrade.
Rule base (*.rule)	Imports the system rule base upgrade file (including the intrusion detection rule base) to upgrade the built-in intrusion detection rule base on UTS. After the file is imported, the engine automatically loads the file, which will take effect immediately.
Web application rule base (*.wcl)	Imports the WAF rule upgrade package to upgrade the built-in WAF rule base on UTS. Restart the engine after the WAF rule base upgrade.   <b>Note</b> The WAF rule base upgrade package must be WAF 6.0.7.1 or later.
NTI database (*.nti)	Imports the offline NTI upgrade package to upgrade the built-in threat intelligence database on UTS.

Parameter	Description
	After the file is imported, the engine automatically loads the file, which will take effect immediately.
Geodatabase (*.geo)	Imports the offline geodatabase upgrade package. After the geodatabase upgrade file is imported, UTS can identify the region to which the external IP belongs. You can view the resolution results in <a href="#">Threat Detection</a> . After the file is imported, the engine automatically loads the file, which will take effect immediately.
Virus signature database (*.av)	Imports the virus signature database upgrade package to upgrade the built-in virus signature database on UTS. After the file is imported, the engine automatically loads the file, which will take effect immediately.
Assessment rule base (*.judge)	Imports the assessment rule upgrade package to upgrade the built-in assessment rule base on UTS. After the file is imported, the engine automatically loads the file, which will take effect immediately.

## 6.4 Backup and Restoration

Through backup and restoration, you can back up and restore engine parameter files, interface parameter files, system running status files, domain name allowlist, and certificate files.

### 6.4.1 Backup

Choose **System > Backup & Restoration > Backup**. On the **Backup** page, select the type of files to be backed up from the drop-down list and click **Download** to download the selected file locally to complete the backup.

### 6.4.2 Restoration

Choose **System > Backup & Restoration > Restoration**. Click **Choose File** to select a file to be restored, and click **Upload** to restore the file.



Only backed-up files can be restored. It is recommended that you should use the backup and restoration functions only on the same device of the same version.

## 6.5 System Control

Choose **System > System Control** to perform control operations as required. [Table 6-17](#) describes the system control functions.

Table 6-17 System control functions

Operation	Description
Apply Configuration	Reloads all policies and makes them take effect immediately.
Restart Engine	Restarts the UTS engine system. After the engine is restarted, all policies and configuration settings are reloaded and become effective.
Restart System	Restarts the hardware system of UTS.
Shut Down System	Shuts down the entire hardware system of UTS.
Restart Logging Process	Restarts the logging process of UTS. After log plugins are configured (see <a href="#">Log Plugin Configuration</a> ), the system automatically restarts the logging process.

## 6.6 Storage Management

Choose **System > Storage Management** to perform the following operations:

- Configure storage parameters.
- View UTS local partition status.
- Configure extended storage servers.

### Configuring Storage Parameters

At the top of the page, configure the storage parameters, and click **Save** to submit the configuration. [Table 6-18](#) describes storage parameters.

Table 6-18 Parameters for configuring storage

Parameter	Description
Retention Period	Specifies the maximum duration for logs to be retained in the database. Once the period expires, the logs will be automatically deleted. The value range is 1–180, in days, with <b>30</b> as the default.
Cleanup Start Threshold	When the database partition space usage reaches the set value, the system starts to clean up the database log space. That is, the system automatically deletes the oldest data. The range is 1%–95%, with <b>80%</b> as the default.
Cleanup Stop Threshold	When the database partition space usage reaches the set value, the system stops cleaning up the database log space. That is, the system automatically stops deleting data. The range is 1%–90%, with <b>60%</b> as the default.

### Viewing Local Partition Status

Choose **System > Storage Management**. In the **Local Partition Status** area, you can view the space usage of various partitions on UTS. They are:

- Total capacity, used capacity, and usage percentage of the system disk.


- Total capacity, used capacity, and usage percentage of the event log space.
- Total capacity, used capacity, and usage percentage of the log cache plugin space.
- Total capacity, used capacity, and usage percentage of the backup space.
- Total capacity, used capacity, and usage percentage of the raw log storage space.
- Total capacity, used capacity, and usage percentage of the session-based storage space.

## Configuring an Extended Storage Server

In the extended storage server list, click **Add**, configure the parameters, and click **OK** to add a Network File System (NFS) server as the extended data storage space. [Table 6-19](#) describes parameters for configuring the extended storage server.

After an extended storage server is added, you can also remove it.

Table 6-19 Parameters for adding an extended storage server

Parameter	Description
Storage Server IP	IPv4 address of the storage server.
Store Logs/Malicious PCAP/Session PCAP	Controls whether to store logs, malicious PCAP files, or session PCAP files in the extended storage server.   <b>Note</b>  All three options can be selected simultaneously.
Collaborative UTS IP	IPv4 address of UTS's management interface.
Storage Server Mount Directory	Directory used by the extended storage server to store UTS data. The directory will be mounted on UTS.



After the extended storage server is removed, UTS will not automatically delete data stored in the NFS server. The data will remain saved in the NFS server. If the extended storage server is reconnected to the original UTS, the original UTS has read and write permissions.

# 7 Administration

This chapter contains the following topics:

Topic	Description
<a href="#">Account Management</a>	Describes how to configure user accounts, API accounts, and login security settings.
<a href="#">Log Forwarding Management</a>	Describes how to configure log plugins and the A interface channel.
<a href="#">License Management</a>	Describes how to import or export system licenses and view license information.
<a href="#">SNMP</a>	Describes how to configure SNMP on UTS.

## 7.1 Account Management

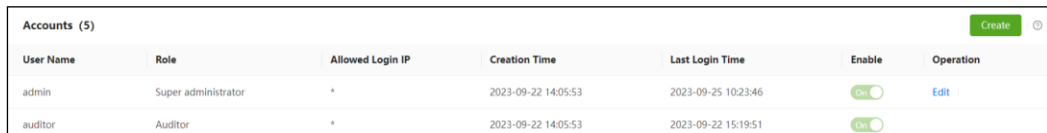
Only the **admin** and **account manager** have privileges to manage accounts.

- **admin**: can perform all configuration operations.
- **account manager**: can configure accounts with the **operator** or **user** role only.

### 7.1.1 Account Management

Choose **Administration > Accounts > User Management** to create new accounts. By default, there are two built-in accounts: **admin** and **auditor**. The **admin** user can create accounts, enable, disable, edit, and delete these accounts.


Figure 7-1 Account management



Accounts (5) <span style="float: right;">Create</span>						
User Name	Role	Allowed Login IP	Creation Time	Last Login Time	Enable	Operation
admin	Super administrator	*	2023-09-22 14:05:53	2023-09-25 10:23:46	<input checked="" type="checkbox"/>	<a href="#">Edit</a>
auditor	Auditor	*	2023-09-22 14:05:53	2023-09-22 15:19:51	<input checked="" type="checkbox"/>	

### Enabling the Auditor Account

By default, the built-in auditor account is disabled. Only the **admin** user has the privilege to enable the auditor account. Once enabled, it cannot be disabled.



In the account list, click the  icon to enable the auditor account. For information on its initial password, see [Default Accounts](#). Upon initial login as the auditor account, the system will require a password change.


## Creating an Account

Initially, only the **admin** user has privilege to create accounts. After the **admin** user creates an account manager, the account manager can create accounts with the **operator** or **user** role.

Take the **admin** user as an example to create a new account. The steps are as follows: Choose **Administration > Accounts > User Management**. Click **Create**, configure account parameters, and click **OK**. [Table 7-1](#) describes parameters for creating an account.

Table 7-1 Parameters for creating an account

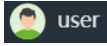
Parameter	Description
User Name	Specifies a unique user name. It can contain lowercase letters, uppercase letters, and/or digits and should be 4–32 characters long. After an account is successfully created, its user name cannot be changed.
Authentication Mode	Specifies the login authentication mode. Only local authentication is supported.
Password/Confirm Password	Follow the prompts to set the login password.
Password Age (days)	<p>Specifies the valid period of the password, with a value range of 0–90, in days. The value of 0 indicates that the password is always valid. For example, the value of 30 means that you need to change the password every 30 days.</p> <p> <b>Note</b></p> <ul style="list-style-type: none"> <li>The <b>admin</b> user will be prompted to change the password after the password validity expires. If the password is not changed after 30 seconds, the <b>admin</b> user will be automatically logged out. Upon subsequent login attempts, the system will prompt a password change until the password change is completed.</li> <li>Non-admin login users will be prompted that the admin user will forcibly change the password of this account once the password validity expires.</li> </ul>
Allowed Login IP	<p>Specifies a range of IP addresses that are allowed for login with a specific account. Any login attempts from the IP address outside the range will be denied. The allowed log IP can be IPv4 addresses, IPv6 addresses, subnet masks, or network segments. Multiple entries must be separated by commas.</p> <p>The default value is *, which means that the account is allowed to log in to the system through any IP address.</p>
Single-Device Login	<p>After this feature is enabled, the current account user can log in to the system from one device at a time.</p> <p> <b>Note</b></p> <p>Only single-device login is allowed for the <b>admin</b> user.</p>
Email	Email address of the account.
Role	<p>Specifies a role for the account. Options include <b>Account manager</b>, <b>Operator</b>, and <b>User</b>. Different roles have different privileges.</p> <p>For details, see <a href="#">System Users</a>.</p>

Parameter	Description
	 <b>Note</b> The account manager has privilege to configure operator accounts and user accounts.

## Editing Account Information

The account information includes user name, login password, and role. The following describes how to edit account information and the precautions.

### Editing the Login Password of the Current Account


All accounts can change their login password by clicking  in the upper-right corner of the page. For details, see [Layout of the Web-based Manager](#).

### Resetting the Built-in Account's Password

If you forget the login passwords for the built-in accounts (**admin** and **auditor**), you can reset the password through the device's Console port management interface. For details, see [Resetting the Web Login Password of the Administrator](#).


### Editing Other Information of Accounts

In the account list, click **Edit** in the **Operation** column to edit the account information.

 <b>Note</b>	Pay attention to the following precautions when modifying account information: <ul style="list-style-type: none"> <li>• The <b>auditor</b> account is an independent and unique account whose account information cannot be changed.</li> <li>• The <b>admin</b> user and account manager can modify their own account information as well as the information of accounts they have created except user names.</li> <li>• Operators and users can modify their account information except user names.</li> </ul>
--	--

## Deleting an Account

In the account list, click **Delete** in the **Operation** column to delete an account.

 <b>Note</b>	Pay attention to the following precautions when deleting accounts: <ul style="list-style-type: none"> <li>• Only the super administrator <b>admin</b> and account manager have privilege to delete accounts.</li> <li>• Only accounts created by the <b>admin</b> user and account manager can be deleted.</li> <li>• Built-in accounts <b>admin</b> and <b>auditor</b> cannot be deleted.</li> </ul>
--	---




## 7.1.2 Configuring Login Parameters

You can configure login parameters of accounts for security purposes.

Choose **Administration > Accounts > Security Settings**. Configure login parameters, and click **OK** to save the configuration. [Table 7-2](#) describes login parameters.

Table 7-2 Description of login parameters


Parameter	Description
Max Failed Login Attempts	Specifies the maximum number of consecutive failed login attempts allowed before a user is locked out. The value range is 1–3.
Lockout Period (min)	Specifies the lockout duration for unsuccessful login to the system after a specified number of login verification failures. The value range is 1–60, in minutes.
Action upon Max Login Failures	<ul style="list-style-type: none"> <li>After this feature is enabled, the system will lock accounts when the number of login authentication failures reaches the specified value. Even if users change their IP address and log in again, they will still be locked out until the specified lockout time expires.</li> <li>By default, this feature is disabled, which means that users can change their IP addresses to log in to the system after exceeding the number of login authentication failures.</li> </ul> <p> <b>Note</b></p> <p>When a user account is locked, an audit log is generated that can be viewed by the auditor.</p>
Min Password Length	Specifies the minimum password length. The value must be an integer in the range of 8–32.
Password Complexity	Specifies the password complexity. Option can be <b>1, 2, 3, or 4</b> .
Idle Timeout (min)	<p>If an account user remains inactive for a period of time that exceeds the specified duration, the system will automatically log the user out. To continue the operation, the user needs to log in again.</p> <p>The value range is 1–10, in minutes. By default, it is <b>3</b> minutes. The value of 0 indicates that the account user with no activity will not be automatically logged out. However, note that the account user is still subject to the operating system's hibernation, power policy, and browser hibernation settings, which could result in an automatic logout.</p>

## 7.1.3 API Account Configuration

UTS provides the API interface for collaboration with NSFOCUS Intelligent Security Operations Platform (ISOP). The interactions between them are described as follows:

- UTS receives a query request from ISOP through the API interface. When UTS completes the query, it will return a download link to ISOP for downloading the corresponding PCAP file.

- ISOP delivers a one-click blocking policy to UTS through the API interface. Upon receiving the request, UTS executes the blocking action and subsequently sends a blocking log to ISOP once the blocking process is complete.

 <b>Note</b>	<ul style="list-style-type: none"> <li>• This function requires configuring UTS as a data source and configuring API account information of UTS on ISOP. For more information, see <i>NSFOCUS ISOP User Guide</i>.</li> <li>• To retrieve and download traffic from UTS to ISOP, you need to enable the traffic storage function. For details, see <a href="#">Traffic Storage</a>.</li> <li>• To utilize the one-click blocking policy feature of ISOP, you need to enable <b>Out-of-Path Blocking</b> and enable <b>Custom detection, alerting, and blocking</b> under <b>Out-of-Path Blocking</b> on UTS. For details, see <a href="#">Custom Blocking Policy</a>.</li> </ul>
--	--


Choose **Administration > Accounts > API Account Configuration**. Configure API account parameters and click **OK**. Then click **Apply Configuration** in the upper-right corner of the page to make the configuration take effect. [Table 7-3](#) describes parameters for creating an API account.

Table 7-3 Description of API account parameters

Parameter	Description
User Name	Specifies a unique API account user name. It must be 4–32 characters long and can contain only lowercase letters, uppercase letters, digits, and/or the special characters. The allowed special characters are .@!%#_&\$*~ After an API account is successfully created, its user name cannot be changed.
Enable	<b>Yes:</b> indicates that the account is valid.
Password/Confirm Password	Specifies the login password for the API account. It can be 8–32 characters long, must include at least one of lowercase letters, uppercase letters, digits, or special characters, and cannot contain spaces.
Description	Provides a description that cannot contain special characters, including `~!@#%&^&{ }*,./ ;`

## 7.2 Log Forwarding Management

UTS offers log forwarding management that allows users to enable or disable various log plugins and customize their parameters for storing logs in different ways.

 <b>Note</b>	<p>After log plugins are enabled in the <b>Log Plugin Configuration</b> section, the corresponding configuration tabs will appear. For details, see <a href="#">Log Plugin Configuration</a>.</p>
--	---

## 7.2.1 Log Plugin Configuration

You can enable log plugins for storage purposes according to your actual situation.

To configure log plugins, follow these steps:

**Step 1** Choose **Administration > Log Forwarding > Log Plugin Configuration**. The **Log Plugin Configuration** page is shown in [Figure 7-2](#).

Figure 7-2 Log plugin configuration

**Step 2** (Optional) Configure the local IP address of UTS.


- a. The local IP address is used to identify the device from which logs are forwarded.
- b. Set it to the IP address of the M or H interface, and click **OK**.

If the local IP address is not configured, UTS will automatically set the IP address to 192.168.2.1 for forwarding logs.

**Step 3** Configure plugin options and log filtering settings.

Select log plugins that you want to use and enable log filtering as required. [Table 7-4](#) describes the parameters.

Table 7-4 Parameters for configuring log plugins

Parameter	Description
Plugin	<p>Select log plugins that need to be enabled. Different types of plugins forward logs to the corresponding devices in different ways.</p> <ul style="list-style-type: none"> <li>• <b>Local channel</b>: Logs are saved locally on UTS. By default, it is enabled.</li> <li>• <b>A interface channel</b>: Logs are sent to ISOP in JSON format. By default, it is enabled.</li> </ul>
Filter	<p>Choose which types of plugin logs to filter.</p> <p>After log plugins are enabled, UTS filters session logs, DNS logs, and ICMP logs based on built-in filtering rules before forwarding or storing logs through these plugins, thereby improving log availability.</p> <p> <b>Note</b></p> <p>For logs forwarded through the A interface, UTS will also forward them to ISOP based on the specified log sending level.</p>

**Step 4** Click **OK**.

**Step 5** (Optional) Specify the methods for forwarding various logs via the A interface channel, as shown in [Figure 7-3](#).

Figure 7-3 Methods for forwarding various logs via the A interface channel

The screenshot displays the 'Log Channel Configuration' window. It features a tree view on the left with 'Local channel' expanded and 'A interface channel' selected. The main area shows configuration options for various log types, each with a 'func\_type' field containing two radio buttons: 'SendMesg' and 'SendMesgEx'. The 'SendMesgEx' option is selected for all categories: status, dns, http, threat, unfiled, session, and file. A green 'Save' button is located at the bottom left of the configuration area.

**Step 6** Click **Save**. A dialog box appears, prompting the configuration success.

**Step 7** Restart the logging process. For details, see [System Control](#).

**Step 8** Click **Apply Configuration** in the upper-right corner of the page to make the configuration take effect.

---End

## 7.2.2 A Interface Channel Configuration

The A interface channel refers to the channel used by UTS to register with ISOP and forward logs to ISOP. Before UTS forwards logs to ISOP, you should complete the registration of UTS with ISOP. For information on how to register, see [Registering UTS with ISOP](#).

Choose **Administration > Log Forwarding > A Interface Channel** to view the A interface version information and configure ISOP parameters as well as log types to forward, as shown in [Figure 7-4](#). [Table 7-5](#) describes the page content.

Figure 7-4 A interface channel

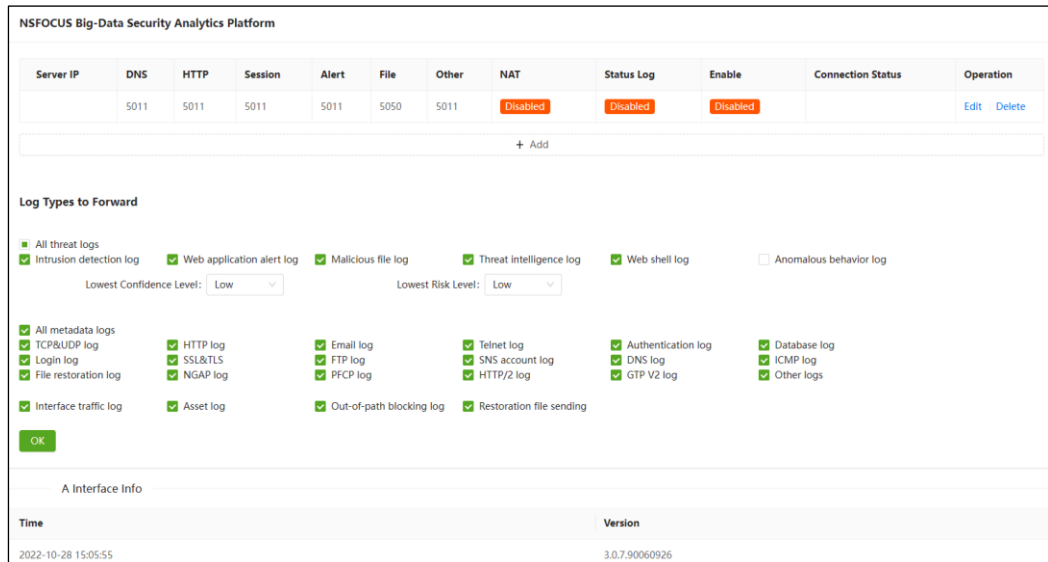


Table 7-5 Description of A interface channel page

Parameter	Description
NSFOCUS Big-Data Security Analytics Platform	Configure the parameters of ISOP where UTS is registered. For details, see <a href="#">Configuring NSFOCUS Big-Data Security Analytics Platform</a> .
Log Types to Forward	Specifies the types of logs to be forwarded from UTS to ISOP. For details, see <a href="#">Configuring Log Types to Forward (Through the A Interface Channel)</a> .
A Interface Info	Displays the version information and version update time of the A interface. UTS connects to ISOP through the A interface.

## Registering UTS with ISOP

Before UTS forwards logs to ISOP, you need to complete the registration of UTS with ISOP. The following two registration methods are supported:

- UTS initiates registration with ISOP: In this case, you need to configure ISOP parameters in the UTS web-based manager. For details, see [Configuring NSFOCUS Big-Data Security Analytics Platform](#).
- ISOP initiates registration of UTS: In this case, you should first add UTS in ISOP and then register UTS. After that, the ISOP information will be automatically added to the UTS web-based manager.

After being successfully registered with ISOP, UTS can perform the following interactions with ISOP:

- UTS forwards logs to ISOP based on the configuration information for log analysis . For configuration details, see [Configuring Log Types to Forward \(Through the A Interface Channel\)](#).
- ISOP receives PCAP files from UTS and conducts analysis. This feature requires configuring an API account. See [API Account Configuration](#) for information on how to configure API accounts.

## Configuring NSFOCUS Big-Data Security Analytics Platform

UTS supports registration with up to three ISOPs.

Choose **Administration > Log Forwarding > A Interface Channel**. On the upper part of the page, click **Add** to add an ISOP and configure its parameters. Click **Save** in the **Operation** column. If **Enable** is enabled and the ISOP parameters are configured, UTS will actively initiate a connection to the corresponding ISOP. After successful connection, the connection status becomes **Connected**. [Table 7-6](#) describes parameters for configuring ISOP.

After an ISOP is added, you can edit and delete it.

Table 7-6 Description of ISOP parameters

Parameter	Description
Server IP	Specifies the IP address of ISOP. Both IPv4 and IPv6 addresses are supported.
DNS	Specifies the port number for ISOP to receive DNS logs. The range is 1–65535, with <b>5011</b> as the default.
HTTP	Specifies the port number for ISOP to receive HTTP logs. The range is 1–65535, with <b>5011</b> as the default.
Session	Specifies the port number for ISOP to receive session logs. The range is 1–65535, with <b>5011</b> as the default.
Alert	Specifies the port number for ISOP to receive alert logs. The range is 1–65535, with <b>5011</b> as the default.
File	Specifies the port number for ISOP to receive files restored by UTS. The range is 1–65535, with <b>5050</b> as the default.
Other	Specifies the port numbers for ISOP to receive file restoration logs and other logs. The range is 1–65535, with <b>5011</b> as the default.
NAT	When UTS is in the internal network and needs to undergo NAT address conversion before collaborating with the external platform, this option needs to be selected.
Status Log	Controls whether ISOP receive status logs forwarded from UTS. There are two types of status logs: <ul style="list-style-type: none"> <li>• Heartbeat log: is used to log whether UTS is online.</li> <li>• Monitoring log: is used to log the usage of CPU, memory, CF card, and disk, as well as traffic sending status of UTS.</li> </ul>
Enable	Controls whether UTS actively initiates a connection to ISOP. <ul style="list-style-type: none"> <li>• If <b>Enable</b> is not selected, the configuration is not effective.</li> <li>• If <b>Enable</b> is selected and the configuration is saved, UTS will actively initiate a connection to ISOP.</li> </ul>

## Configuring Log Types to Forward (Through the A Interface Channel)

In the **Log Types to Forward** area, specify the log type to forward, and click **OK**. The logs of selected types will be forwarded to ISOP. [Table 7-7](#) describes parameters for configuring log types to forward.

Table 7-7 Parameters for configuring log types to forward (through the A interface channel)

Parameter	Description
Threat log types to forward	Specifies the type of threat logs to be forwarded. Multiple values are supported.
Lowest Confidence Level	Specifies the lowest confidence level of logs to be forwarded. Options are <b>Low</b> , <b>Medium</b> , and <b>High</b> . For example, selecting <b>Medium</b> means that only threat logs with confidence levels of <b>Medium</b> and <b>High</b> will be forwarded to ISOP.
Lowest Risk Level	Specifies the lowest risk level of logs to be forwarded. Options are <b>Low</b> , <b>Medium</b> , and <b>High</b> . For example, selecting <b>Medium</b> means that only threat logs with threat risk levels of <b>Medium</b> and <b>High</b> will be forwarded to ISOP.
Metadata logs to forward	Specifies the type of metadata logs to be forwarded. Multiple values are supported.
Interface traffic log	When it is selected, the log of interface traffic between UTS and ISOP is forwarded to ISOP.
Asset log	When it is selected, UTS forwards the asset log to ISOP.
Out-of-path blocking log	When it is selected, UTS forwards the out-of-path blocking log to ISOP.
Restoration file sending	When it is selected, UTS forwards the restoration file log to ISOP.

## 7.3 License Management

UTS licenses are classified into two types:

- Trial license  
When this type of license expires, users cannot continue to use UTS.
- Paid license  
When this type of license expires, users can still use UTS, but cannot update it.

Choose **Administration > License** to view the current license information. You can import and export licenses, as shown in [Figure 7-5](#).

Figure 7-5 License management

License Information				Export License	Import License
License Status	Normal	License Type	Trial license	Product Model	UTS
Serial Number	B438-2E06-E2B7-3734	Licensee	Trial license6725567	Current Service Validity	2023-08-29 to 2024-09-28
Authorization Mode	Local authorization	Bound Device Hash	B438-2E06-E2B7-3734	Current Device Hash	B438-2E06-E2B7-3734
Validity Periods of Modules					
Intrusion Detection	Web Application Detection	NTI-based Detection	Static Malicious File Detection		
2023-08-29 to 2024-09-28	2023-08-29 to 2024-09-28	2023-08-29 to 2024-09-28	2023-08-29 to 2024-09-28		
Dynamic File Detection	API Recognition	Sensitive Information Detection			
2023-08-29 to 2024-09-28	2023-08-29 to 2024-09-28	2023-08-29 to 2024-09-28			

## Viewing License Status

As shown in [Figure 7-5](#), you can view functional modules supported by the current UTS device and their validity periods. [Table 7-8](#) describes the license information.

Table 7-8 Parameters on the license page

Parameter	Description
License Status	Indicates whether the license status is normal.
License Type	UTS licenses are classified into two types: <ul style="list-style-type: none"> <li>• Trial license: When this type of license expires, users cannot continue to use UTS.</li> <li>• Paid license: When this type of license expires, users can still use UTS, but cannot update it.</li> </ul>
Product Model	Indicates the product model covered by this license.
Serial Number	Indicates the unique number of the license.
Licensee	Indicates the unique authorization code of the current license user.
Current Service Validity	The current UTS device can be upgraded only within this time frame.
Validity Periods of Modules	Displays the authorization status and validity periods of various modules on the current UTS device.

## Importing a License

There are two situations where licenses need to be imported:

- During the initial login, you must import the license; otherwise, you cannot use UTS.
- When the license expires and needs to be renewed, or when a new function module is purchased, a new license needs to be imported.

Choose **Administration > License**. Click **Import License**. Configure related parameters to import a specified license. [Table 7-9](#) describes the parameters for importing a license.



Figure 7-6 Importing a license

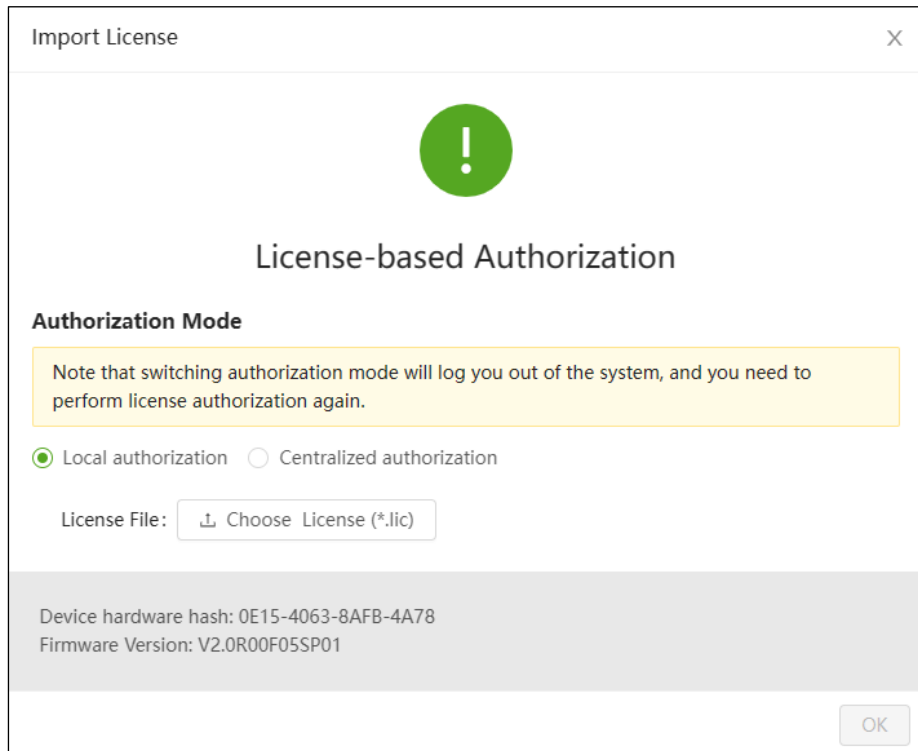



Table 7-9 Description of parameters for importing a license

Parameter	Description
Authorization Mode	<p>Two authorization modes are supported:</p> <ul style="list-style-type: none"> <li>• <b>Local authorization:</b> authorizes UTS by using a local authentication license file.</li> <li>• <b>Centralized authorization:</b> authorizes UTS through NSFOCUS Enterprise Security Platform (ESP-C).</li> </ul> <p> <b>Note</b></p> <p>Switching the license authorization mode will log you out of the system and requires re-authorization.</p>
License File	When the local authorization mode is selected, click <b>Choose License (*.lic)</b> to select a proper license file and import it.
Authorization Device Information	<p>When the centralized authorization mode is selected, you need to configure the information of the authorization device as follows:</p> <ul style="list-style-type: none"> <li>• <b>Host:</b> specifies the IP address of NSFOCUS Enterprise Security Platform (ESP-C). Only IPv4 addresses are supported.</li> <li>• <b>Port:</b> specifies the port number of ESP-C. The value range is 0–65535.</li> </ul>
Device Hardware Hash/Firmware Version	Indicates the hardware hash value and firmware version number of the current UTS device. They are required for centralized authorization and should be typed on ESP-C.

## Exporting a License

Click **Export License** to export the current license file.

## 7.4 SNMP

UTS supports Simple Network Management Protocol (SNMP). UTS can serve as an agent to respond to queries from the SNMP manager and send trap messages to the SNMP manager.

UTS supports SNMPv3, and is compatible with SNMPv1 and SNMPv2c. When SNMP queries are performed using SNMPv1 and SNMPv2c protocols, only the community string is required. However, these versions of SNMP do not provide encryption for transferred authentication and management data and there is no identification mechanism during data receiving and sending, which can expose the network to various security risks. When SNMPv3 queries are performed, the transferred messages are encrypted using the DES or AES symmetric-key algorithm. In addition, an authentication key is configured to verify user identities on UTS, thereby enhancing the security of SNMP management.

UTS supports popular SNMP management software, such as MIB Browser and Solarwind.

### 7.4.1 System Configuration Information

UTS supports SNMP management. To configure SNMP management, follow these steps:

Choose **Administration > SNMP > System Configuration Info**. Configure basic SNMP parameters, and click **Apply Configuration** to complete the configuration. [Table 7-10](#) describes basic parameters for configuring SNMP.

Click **Download** to download the MIB file of the SNMP agent locally.

Table 7-10 Description of basic SNMP parameters

Parameter	Description
System Location	Specifies the location of UTS in the network environment.
System Contact	Specifies the information of the contact person responsible for the current UTS device. It can be a phone number or email address. By default, it is the email address of NSFOCUS technical support.
System Description	Provides descriptive information about the current UTS device.
SnmpTrap	Controls whether to enable UTS to proactively send traps to SNMP manager. After it is enabled, the settings configured under <b>SNMP &gt; Trap</b> take effect. For details, see <a href="#">Trap</a> .
SnmpAgent	Controls whether to enable UTS to accept management from the SNMP manager. After it is enabled, the settings configured under <b>SNMP &gt; Agent Access Control</b> take effect. For details, see <a href="#">Agent Access Control</a> .

### 7.4.2 Agent Access Control

After the SNMP agent service is enabled on UTS and agent access control parameters are properly configured, the SNMP manager can perform management and UTS can generate

SNMP traps. For information on how to enable SNMP agent, see [System Configuration Information](#). The following describes how to configure agent access control parameters.

UTS supports SNMPv1/v2c and SNMPv3 agents.

### 7.4.2.1 SNMPv1/v2c

Choose **Administration > SNMP > Agent Access Control > SNMPv1/v2c**. Click **Create** to configure the agent access control parameters, and click **OK**. Click **Apply Configuration** in the upper-right corner of the page to make the configuration take effect. [Table 7-11](#) describes the SNMPv1/v2c agent access control parameters.

After the agent access control parameters are created, they can be edited and deleted.

Table 7-11 Parameters for configuring SNMPv1/v2c agent access control

Parameter	Description
Community Name	Specifies the community string used by UTS for accessing the SNMP manager after the SNMPv1/v2c agent is enabled on UTS. The community name should be at least 8 characters long. It is recommended that the community name should consist of lowercase and uppercase letters, digits, and underscores.  After being created, the community name is displayed as an asterisk symbol (*).
Request Source	Specifies the source IP address of the SNMP manager. Both IPv4 and IPv6 are supported. * indicates that there is no limit on the source IP.
MIB Subtree	Specifies the SNMP manager's permission to access the MIB subtree on UTS. The access permission is represented by an Object identifier (OID), for example, 1.3.6.1.4.1.19849.2. The value of 1 indicates access to all nodes.
R/W Access	Specifies the SNMP manager's read/write permission to the MIB subtree on UTS. Only the read permission is supported.

### 7.4.2.2 SNMPv3

Choose **Administration > SNMP > Agent Access Control > SNMPv3**. Click **Create** to configure the agent access control parameters, and click **OK**. Click **Apply Configuration** in the upper-right corner of the page to make the configuration take effect. [Table 7-12](#) describes the SNMPv3 agent access control parameters.

After the agent access control is created, you can edit and delete it.

Table 7-12 Parameters for configuring SNMPv3 agent access control

Parameter	Description
User Name	Specifies the user name of the SNMPv3 service. It is recommended that the user name should consist of lowercase and uppercase letters, digits, and underscores.
MIB Subtree	Specifies the SNMP manager's permission to access the MIB subtree on UTS. The access permission is represented by an Object identifier (OID), for example, 1.3.6.1.4.1.19849.2. The value of 1 indicates access permissions to all nodes.
R/W Access	Specifies the SNMP manager's read/write permission to the MIB subtree on UTS. Only the read permission is supported.
Security Level	Specifies an access security level. Options are <b>NoAuthNoPriv</b> , <b>Auth</b> , and <b>AuthPriv</b> .

Parameter	Description
	<b>NoAuthNoPriv</b> indicates communication without authentication and encryption. <b>Auth</b> indicates communication with authentication only. <b>AuthPriv</b> indicates communication with authentication and encryption.
Authentication Protocol	When the security level is set to <b>Auth</b> and <b>AuthPriv</b> , you need to specify the authentication protocol. Options are <b>MD5</b> and <b>SHA</b> .
Authentication Key	When the security level is set to <b>Auth</b> and <b>AuthPriv</b> , you need to specify the authentication key used for one-way hash calculation.  The authentication key should be at least 8 characters long. It is recommended that the authentication key should consist of lowercase and uppercase letters, digits, and underscores.
Privacy Protocol	When the security level is set to <b>AuthPriv</b> , you need to specify a privacy algorithm for encrypting transmitted information. Options are <b>DES</b> and <b>AES</b> .
Privacy Key	When the security level is set to <b>AuthPriv</b> , you need to specify the privacy key used for information encryption.  The privacy key should be at least 8 characters long. It is recommended that the privacy key should consist of lowercase and uppercase letters, digits, and underscores.

## 7.4.3 Trap

Trap is an unsolicited SNMP message sent from the device to the SNMP manager. As an SNMP agent, UTS can proactively send traps about its own situation to the SNMP manager.

After the SNMP trap service is enabled and related parameters are properly configured, UTS can notify the SNMP manager of its situation.

UTS supports SNMPv1/v2c and SNMPv3 traps. For information on how to enable the SNMP trap function, see [System Configuration Information](#). The following describes how to configure SNMP traps.

### 7.4.3.1 SNMPv1/v2c Access Control

Choose **Administration > SNMP > Trap > SNMPv1/v2c**. Click **Create** to configure the trap parameters, and click **OK**. Click **Apply Configuration** in the upper-right corner of the page to make the configuration take effect. [Table 7-13](#) describes the SNMPv1/v2c trap parameters.

After the trap is created, you can edit and delete it.

Table 7-13 Parameters for creating an SNMPv1/v2c trap

Parameter	Description
Target Host	Specifies the IP address of the host that receives the SNMP traps sent by UTS. Both IPv4 and IPv6 addresses are supported.
Port	Specifies the port for receiving SNMP traps.
Protocol Version	Specifies the version of the SNMP protocol. Options include <b>v1</b> and <b>v2c</b> .
Agent Address	When the protocol version is set to <b>v1</b> , you need to configure the IP address of the agent. Only IPv4 addresses are supported.
Community	Specifies the community name string of the host that receives SNMP traps.

Parameter	Description
Name	<p>After the SNMP trap service is enabled on UTS, you need to type the community string of the host for receiving SNMP traps. The community name should be at least 8 characters long. It is recommended that the community name should consist of lowercase and uppercase letters, digits, and underscores.</p> <p>After being created, the community name is displayed as an asterisk symbol (*).</p>

### 7.4.3.2 SNMPv3 Access Control

Choose **Administration > SNMP > Trap > SNMPv3**. Then click **Create** to configure the trap parameters, and click **OK**. Click **Apply Configuration** in the upper-right corner of the page to make the configuration take effect. [Table 7-14](#) describes parameters for creating an SNMPv3 trap.

After the trap is created, you can edit and delete it.

Table 7-14 Parameters for creating an SNMPv3 trap


Parameter	Description
Target Host	Specifies the IP address of the host that receives SNMP traps sent by UTS. Both IPv4 and IPv6 addresses are supported.
Port	Specifies the port for receiving SNMP traps.
User Name	<p>Specifies the user name of the SNMPv3 service.</p> <p>The user name should be at least 8 characters long. It is recommended that the user name should consist of lowercase and uppercase letters, digits, and underscores.</p>
Engine ID	<p>Specifies the ID of the SNMP engine.</p> <p>The ID must be a 16-bit hexadecimal value, for example, 0x800000001020304.</p>
Security Level	Specifies an access security level. Options are <b>NoAuthNoPriv</b> , <b>Auth</b> , and <b>AuthPriv</b> . <b>NoAuthNoPriv</b> indicates communication without authentication and encryption. <b>Auth</b> indicates communication with authentication only. <b>AuthPriv</b> indicates communication with authentication and encryption.
Authentication Protocol	When the security level is set to <b>Auth</b> and <b>AuthPriv</b> , you need to specify the authentication protocol. Options are <b>MD5</b> and <b>SHA</b> .
Authentication Key	<p>When the security level is set to <b>Auth</b> and <b>AuthPriv</b>, you need to specify the authentication key used for one-way hash calculation.</p> <p>The authentication key should be at least 8 characters long. It is recommended that the authentication key should consist of lowercase and uppercase letters, digits, and underscores.</p>
Privacy Protocol	When the security level is set to <b>AuthPriv</b> , you need to specify the privacy algorithm for encrypting transmitted information. Options are <b>DES</b> and <b>AES</b> .
Privacy Key	<p>When the security level is set to <b>AuthPriv</b>, you need to specify the privacy key used for information encryption.</p> <p>The privacy key should be at least 8 characters long. It is recommended that the privacy key should consist of lowercase and uppercase letters, digits, and underscores.</p>

# 8 Audit

Only the auditor can perform the audit operation.

This chapter contains the following topics:

Topic	Description
<a href="#">Logs</a>	Describes how to view and manage audit logs.
<a href="#">Configuring Log Storage</a>	Describes how to configure log storage.

 <b>Note</b>	The auditor account is disabled by default. For information on how to enable it, see <a href="#">Enabling the Auditor Account</a> .
--	---

## 8.1 Logs

Audit logs include login logs, operation logs, and system startup logs.

After the auditor logs in to the system, choose **Audit > Logs** to view, query, download, and import audit logs, as shown in [Figure 8-1](#).

Figure 8-1 Audit logs

User Name: <input type="text"/>	Login IP: <input type="text"/>	Event: <input type="text"/>		
Time: <input type="text"/> Start Time → End Time <input type="text"/>	<input type="button" value="Reset"/>	<input type="button" value="Query"/> <input type="button" value="Download Logs"/> <input type="button" value="Import Logs"/>		
Time	User Name	Login IP	Event	Event Outcome
2023-09-25 11:14:20	auditor	10.8.12.135	Login succeeded: uuid: 0ba0fd4da1047c4bb85adef3c59655a, user name: auditor, login ip: 10.8.12.135.	Operation successful
2023-09-25 11:09:21	admin	10.8.12.135	Security Center - Log Plugin Configuration - Log Plugin Configuration Modified Successfully	Operation successful
2023-09-25 11:02:40	admin	10.8.12.135	Login succeeded: uuid: c5d2df057fb9435182b5920cc69dbc91, user name: admin, login ip: 10.8.12.135.	Operation successful
2023-09-25 10:44:59	zhaoxionghui	10.67.19.27	Login succeeded: uuid: bcf83ee91e0f4841bc6d37d6d21c5ff0, user name: zhaoxionghui, login ip: 10.67.19.27.	Operation successful
2023-09-25 10:34:14	zhaoxionghui	10.67.19.27	Disabled allowlist configuration.	Operation successful
2023-09-25 10:33:54	admin	10.8.12.135	Updated 5G NE information to [IP: 2000-23, port: 80, NE type: SMSF, MAC address: 00:0c:29:35:dc1c].	Operation successful

## 8.2 Configuring Log Storage

You can specify the retention period of logs stored on UTS. After the retention period expires, logs are automatically deleted in the chronological order.

After the auditor logs in to the system, choose **Audit > Log Storage** to specify the retention period. Then click **OK**. The value range is 1–180, in days. By default, it is set to **180** days.

# A Console-based Management

---

After connecting to the console port, the console administrator (**conadmin**) can access the console-based manager of UTS and perform basic operations, such as initialing system settings, binding working interfaces of the device, and resetting web login passwords. When failing to log in to the web-based manager or to perform certain management via the web-based manager, you can log in to the console to manage UTS.

This chapter contains the following topics:

Topic	Description
<a href="#">Login to the Console</a>	Describes how to log in to the console-based manager.
<a href="#">Keyboard Operations</a>	Describes the keys used for console-based management.
<a href="#">Configuration on the Console</a>	Describes how to manage and configure UTS on the console.

## A.1 Login to the Console

Before logging in to the console, you must prepare the following:

- One PC
- VNC Viewer (client software)

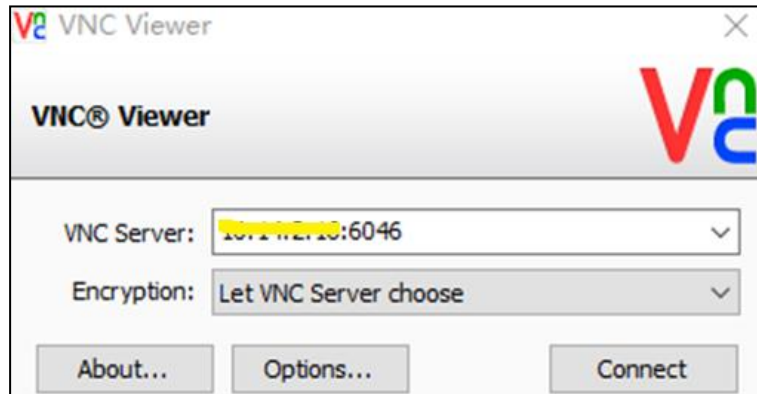
To use VNC Viewer to log in to the console, follow these steps:

**Step 1** Open VNC Viewer.

**Step 2** Type the IP address of the host and the VNC port number.



Figure A-1 Configuring parameters for connection to the console



Run the **virsh edit uts** command to view the VNC port number.

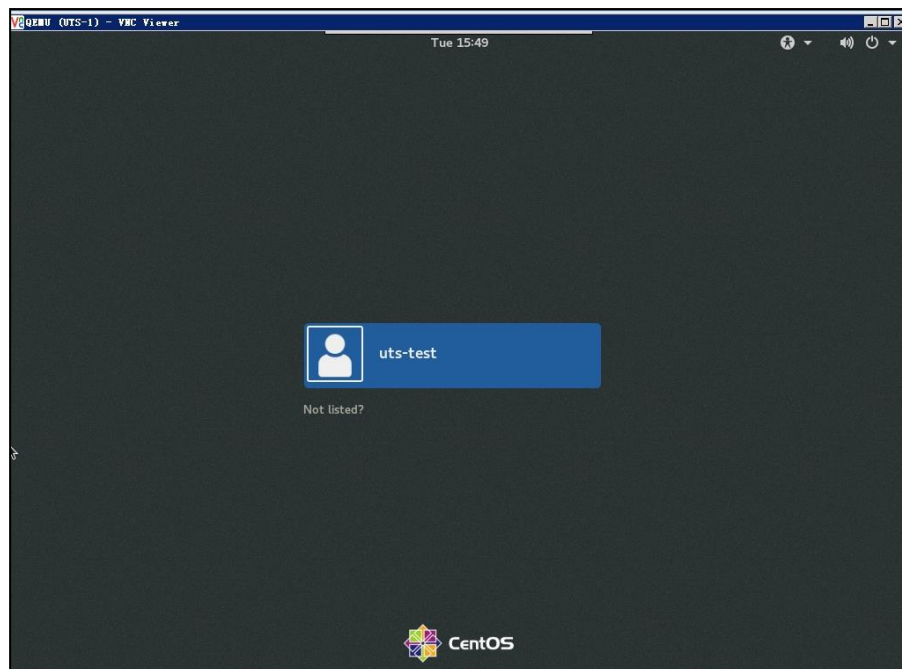
Figure A-2 Viewing the VNC port number

```
<graphics type='vnc' port='9080' autoport='no' listen='0.0.0.0'>  
<listen type='address' address='0.0.0.0' />  
</graphics>  
<video>
```

**Step 3** Click **Connect** to connect to the console of UTS.

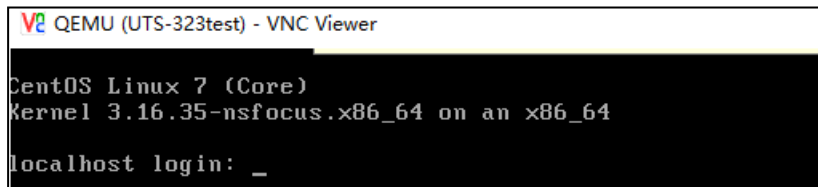
If the connection is successfully set up, the following window appears.

Figure A-3 UTS console connected



**Step 4** Press **Ctrl+Alt+F2** to switch to the console of UTS.

Figure A-4 Console login window



```
QEMU (UTS-323test) - VNC Viewer
CentOS Linux 7 (Core)
Kernel 3.16.35-nsfocus.x86_64 on an x86_64
localhost login: _
```

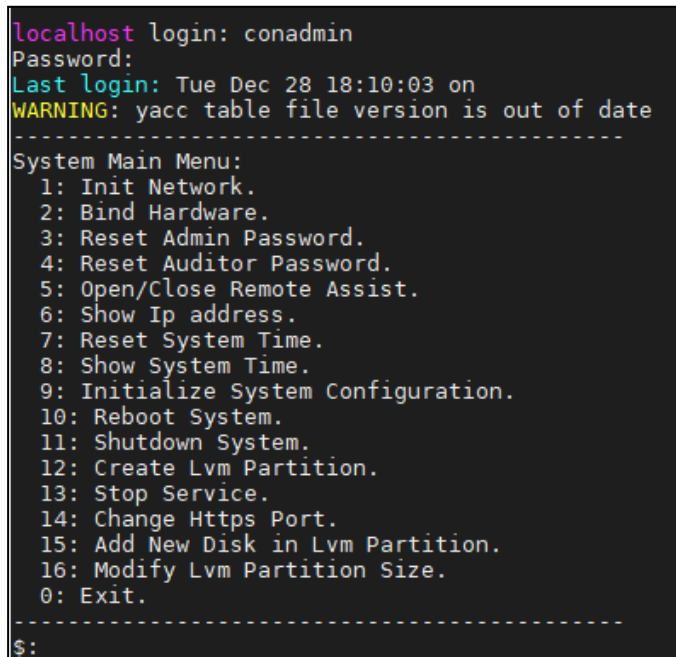
**Step 5** Type the user name and password of the console administrator and press **Enter**.

The main menu appears, as shown in the following figure.

On your first login, you must change the password.

- For account information of the console administrator, see [错误!未找到引用源。](#)
- For information on how to configure the console, see [Configuration on the Console](#).

Figure A-5 Main menu of the console



```
localhost login: conadmin
Password:
Last login: Tue Dec 28 18:10:03 on
WARNING: yacc table file version is out of date
-----
System Main Menu:
 1: Init Network.
 2: Bind Hardware.
 3: Reset Admin Password.
 4: Reset Auditor Password.
 5: Open/Close Remote Assist.
 6: Show Ip address.
 7: Reset System Time.
 8: Show System Time.
 9: Initialize System Configuration.
10: Reboot System.
11: Shutdown System.
12: Create Lvm Partition.
13: Stop Service.
14: Change Https Port.
15: Add New Disk in Lvm Partition.
16: Modify Lvm Partition Size.
 0: Exit.
-----
$:
```

---End

## A.2 Keyboard Operations

On the console, you can perform operations only with the keyboard. The following table describes common keyboard operations.

Table A-1 Meanings of keys for console-based management

Key	Meaning
↑	(1) Switches to the input field. (2) Moves up.
↓	(1) Switches to <b>OK</b> . (2) Moves down.
←	(1) Switches to <b>OK</b> . (2) Moves left.
→	(1) Switches to <b>Cancel</b> . (2) Moves right.
Esc	Cancels an operation.
Enter	Confirms an operation.
Tab	Switches between an input field, <b>OK</b> , and <b>Cancel</b> .
BackSpace	Deletes the character to the left of the cursor.

## A.3 Configuration on the Console

The following sections describe how to configure UTS on the console.

### A.3.1 Configuring the Management Interface and Gateway

On the main menu shown in [Figure A-5](#), type **1** and press **Enter**. Type the IP address (IP/netmask length) of the management interface and the gateway IP address.

Figure A-6 Configuring the management interface and gateway

```
$:1
ip address(192.168.1.1/16):10.14.45.66/16
Gateway:10.14.255.254
Init OK.
```

### A.3.2 Binding Hardware Information

On the main menu shown in [Figure A-5](#), type **2** and press **Enter** to bind hardware information to UTS.

Figure A-7 Binding hardware information

```
$:2
[ 233.547882] Program prod tried to access /dev/mem between ff000->101000.
Bind OK.
```

### A.3.3 Resetting the Web Login Password of the Administrator

On the main menu shown in [Figure A-5](#), type **3** and press **Enter** to reset the web login password of the **admin** account to the default. For the default password of **admin**, see [错误! 未找到引用源。](#).

Figure A-8 Resetting the web login password of the administrator

```
$:3  
Password updated successfully.
```

### A.3.4 Resetting the Web Login Password of the Auditor

On the main menu shown in [Figure A-5](#), type **4** and press **Enter** to reset the web login password of the **auditor** account to the default. For the default password of **auditor**, see [错误!未找到引用源。](#).

Figure A-9 Resetting the web login password of the auditor

```
$:4  
auditor Password updated successfully.  
$:
```

### A.3.5 Enabling/Disabling SSH Access

On the main menu shown in [Figure A-5](#), type **5** and press **Enter**. Then you can enable or disable SSH access, as shown in [Figure A-10](#).

Type different numbers to implement different functions:

- **501**: displays the port for remote assistance.
- **502**: displays IP addresses allowed for remote assistance.
- **503**: displays the password for remote assistance.
- **504**: displays the QR code for remote assistance.
- **505**: disables remote assistance.
- **506**: goes back to the main menu.

Figure A-10 Enabling/Disabling SSH access

```
CentOS Linux 7 (Core)
Kernel 3.16.35-nsfocus.x86_64 on an x86_64

localhost login: conadmin
Password:
Last login: Wed Dec 29 17:04:43 on ttyS0
WARNING: yacc table file version is out of date
-----
System Main Menu:
 1: Init Network.
 2: Bind Hardware.
 3: Reset Admin Password.
 4: Reset Auditor Password.
 5: Open/Close Remote Assist.
 6: Show Ip address.
 7: Reset System Time.
 8: Show System Time.
 9: Initialize System Configuration.
10: Reboot System.
11: Shutdown System.
12: Create Lvm Partition.
13: Stop Service.
14: Change Https Port.
15: Add New Disk in Lvm Partition.
16: Modify Lvm Partition Size.
 0: Exit.
-----
$:5
/opt/nsfocus/bin/rlmc.py:25: CryptographyDeprecationWarning: Python 2 is
xt release.
  from cryptography.hazmat.backends import default_backend
-----
Now Remote Assist Open status SubMenu:
501: Display Remote Assist Port.
502: Display Remote Assist White IP.
503: Display Remote Assist Secret.
504: Display Remote Assist Secret-Qrcode.
505: Close Remote Assist.
506: Return Main Menu.
-----
s:|
```

### A.3.6 Viewing the IP Address of the Management Interface

On the main menu shown in [Figure A-5](#), type **6** and press **Enter** to view the IP address of the management interface.

Figure A-11 Viewing the IP address of the management interface

```
$:6
IPv4:10.67.5.145
IPv6:
```

### A.3.7 Initializing the System

On the main menu shown in [Figure A-5](#), type **9** and press **Enter** to initialize the system, that is, restore system settings to factory defaults.

Figure A-12 Initializing the system

```
$:9
Init ok
Please reboot system.
```

## A.3.8 Rebooting the System

On the main menu shown in [Figure A-5](#), type **10** and press **Enter** to reboot the system.

Figure A-13 Rebooting the system

```

$:10
[ OK ] Started Show Plymouth Reboot Screen.
[ OK ] Stopped Login Service.
[ OK ] Stopped firewalld - dynamic firewall daemon.
      Stopping D-Bus System Message Bus...
[ OK ] Stopped D-Bus System Message Bus.
[ OK ] Stopped LVM2 PV scan on device 8:33.
    
```

## A.3.9 Shutting Down the System

On the main menu shown in [Figure A-5](#), type **11** and press **Enter** to shut down the system.

## A.3.10 Formatting Disks

On the main menu shown in [Figure A-5](#), type **12** and press **Enter**. Then type disk space percentages in the sequence of backup | clickhouse | hdfs\_pcap | pg\_log | sftp\_out | ssn\_pcap | threat\_pcap, which are described as follows:

- **backup**: backup partition
- **clickhouse**: space for storing raw logs
- **hdfs\_pcap**: space for storing big data
- **pg\_log**: space for storing event logs
- **sftp\_out**: log buffer space
- **ssn\_pcap**: space for storing session-based packet capture files
- **threat\_pcap**: space for storing malicious files

You can configure the space percentages as required or use the default values shown in the following figure.

Figure A-14 Formatting disks

```

$:12
configd pid is 56423 result 1
==== disk name: /dev/sda, disk size: 64023257088
==== disk name: /dev/sdc, disk size: 12000138625024
==== disk name: /dev/sdd, disk size: 12000138625024
==== disk name: /dev/sde, disk size: 12000138625024
==== disk name: /dev/sdb, disk size: 2000398934016
All available disk size is 38064838066176.
Does disk need array a soft raid? Now only support raid0
Disk /dev/sdc: 12000.1 GB, 12000138625024 bytes, 23437770752 sectors
Disk /dev/sdd: 12000.1 GB, 12000138625024 bytes, 23437770752 sectors
Disk /dev/sde: 12000.1 GB, 12000138625024 bytes, 23437770752 sectors
Disk /dev/sdb: 2000.4 GB, 2000398934016 bytes, 3907029168 sectors
Please input yes|no for array a soft raid(default yes):no
Ok. No soft raid

Does disk need encrypt?
Note: Disk encryption will loss 20%-50% disk performance
Please input yes|no for disk encrypt:no
Please input size percentages such as(10|25|5|15|5|20|20) in order (backup|clickhouse|hdfs_pcap|pg_log|sftp_out|ssn_pcap|threat_pcap):
    
```



- Before formatting disks, [stop the service](#).
- After formatting disks, [reboot the system](#).

## Creating RAID 0

If UTS has multiple data disks, you can create a redundant array of independent disks mode 0 (RAID 0) to improve the read/write speed of disks. This is useful when you need to enable full traffic storage on UTS. To create RAID 0, follow these steps:

**Step 1** Make sure that the device has more than one data disk.

If only one disk exists, RAID 0 cannot be created.

**Step 2** Type **yes** for the question of "Continue creating array?" to proceed with the operation.

Figure A-15 Creating RAID 0

```

Allocating group tables: done
Writing inode tables: done
Creating journal (32768 blocks): done
Writing superblocks and filesystem accounting information: done

mdadm: /dev/sdb1 appears to contain an ext2fs file system
       size=1863016584K mtime=Thu Jan 1 08:00:00 1970
mdadm: /dev/sdc1 appears to contain an ext2fs file system
       size=18446744067705682412K mtime=Thu Jan 1 08:00:00 1970
mdadm: /dev/sde1 appears to contain an ext2fs file system
       size=18446744067705682412K mtime=Thu Jan 1 08:00:00 1970
mdadm: /dev/sdd1 appears to contain an ext2fs file system
       size=18446744067705682412K mtime=Thu Jan 1 08:00:00 1970

Continue creating array? yes
mdadm: Defaulting to version 1.2 metadata
mdadm: array /dev/md127 started.
cmd exec: lvcreate -L 8640206M -n lvm_clickhouse uts_disk_vg
cmd status:0
cmd exec: lvcreate -L 6912154M -n lvm_ssn_pcap uts_disk_vg
WARNING: ext4 signature detected on /dev/uts_disk_vg/lvm_ssn_pcap at offset 1080. Wipe it? [y/n]: y
cmd status:0
cmd exec: lvcreate -L 1728001M -n lvm_hdfs_pcap uts_disk_vg
WARNING: ext4 signature detected on /dev/uts_disk_vg/lvm_hdfs_pcap at offset 1080. Wipe it? [y/n]: y
cmd status:0
cmd exec: lvcreate -L 6912154M -n lvm_threat_pcap uts_disk_vg
WARNING: ext4 signature detected on /dev/uts_disk_vg/lvm_threat_pcap at offset 1080. Wipe it? [y/n]: y
cmd status:0
cmd exec: lvcreate -L 1728001M -n lvm_sftp_out uts_disk_vg
WARNING: ext4 signature detected on /dev/uts_disk_vg/lvm_sftp_out at offset 1080. Wipe it? [y/n]: y
cmd status:0
cmd exec: lvcreate -L 3456052M -n lvm_backup uts_disk_vg
WARNING: ext4 signature detected on /dev/uts_disk_vg/lvm_backup at offset 1080. Wipe it? [y/n]: y
cmd status:0
cmd exec: lvcreate -L 5184103M -n lvm_pg_log uts_disk_vg
WARNING: ext4 signature detected on /dev/uts_disk_vg/lvm_pg_log at offset 1080. Wipe it? [y/n]: y
cmd status:0

Lvm Partition Ok.
    
```

**Step 3** Decide whether to encrypt data disks.

Figure A-16 Deciding whether to encrypt data disks

```

configd: no process found
configd pid is 32332 result 1
==> disk name: /dev/vda, disk size: 8019099648
==> disk name: /dev/vdb, disk size: 107374182400
All available disk size is 115393282048.
Does disk need array a soft raid? Now only support raid0
Disk /dev/vdb: 107.4 GB, 107374182400 bytes, 209715200 sectors
Please input yes/no for array a soft raid(default yes):no
OK. No soft raid

Does disk need encrypt?
Note: Disk encryption will loss 20%-50% disk performance
Please input yes/no for disk encrypt:no
Please input size percentages such as(25|25|5|5|10|25) in order (backup|clickhouse|hdfs_pcap|pg_log|sftp_out|ssn_pcap|threat_pcap):5|65|5|5|5|10|5
Lvm Partition begin, please wait some minutes.....
/opt/nsfocus/bin/init_disk_lvm.py:1097: SyntaxWarning: name 'g_logger' is assigned to before global declaration
  global g_logger
WARNING: yacc table file version is out of date
    
```

**Step 4** (Optional) If the firmware version of UTS is earlier than F03, after restoring the firmware, manually delete Logical Volume Manager (LVM) partitions in the background.

----End

## Deleting LVM Partitions

To delete LVM partitions, follow these steps:

**Step 1** Run the following command to view LVM partitions:

```
fdisk -l
```

Figure A-17 Viewing LVM partitions

```
Develop>fdisk -l
Disk /dev/vda: 8019 MB, 8019099648 bytes, 15662304 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: dos
Disk identifier: 0x00000000

   Device Boot      Start         End      Blocks   Id  System
/dev/vda1            32         98303        49136   83   Linux
/dev/vda2           98304       15662079       7781888   83   Linux
WARNING: fdisk GPT support is currently new, and therefore in an experimental phase. Use at your own discretion.

Disk /dev/vdb: 214.7 GB, 214748364800 bytes, 419430400 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: gpt
Disk identifier: 4206F192-E7DB-4FC2-8A54-5F7DCCA21196

#           Start          End              Size Type              Name
# 1          34          400000000       190.8G Microsoft basic /dev/vdb1

Disk /dev/mapper/encrypted_root: 7966 MB, 7966556160 bytes, 15559680 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

Disk /dev/mapper/uts_disk_vg-lvm_clickhouse: 51.1 GB, 51149537280 bytes, 99901440 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

Disk /dev/mapper/uts_disk_vg-lvm_ssn_pcap: 40.9 GB, 40907046912 bytes, 79896576 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
```

**Step 2** Run the following commands to delete all LVM partitions:

```
lvremove /dev/mapper/uts_disk_vg-lvm_clickhouse
lvremove /dev/mapper/uts_disk_vg-lvm_ssn_pcap
lvremove /dev/mapper/uts_disk_vg-lvm_hdfs_pcap
lvremove /dev/mapper/uts_disk_vg-lvm_threat_pcap
lvremove /dev/mapper/uts_disk_vg-lvm_sftp_out
lvremove /dev/mapper/uts_disk_vg-lvm_backup
lvremove /dev/mapper/uts_disk_vg-lvm_pg_log
```

**Step 3** Run the following command to format the disk (change the drive letter to the one actually used):

```
mkfs.ext4/dev/sdb
```

**Step 4** [Rebooting the System](#)

**Step 5** .

----End



### A.3.11 Stopping the Service

On the main menu shown in [Figure A-5](#), type **13** and press **Enter**. Type **Y** to stop the service or **N** to cancel the operation.

Figure A-18 Stopping the service

```
$:13
you will stop service? Y/N: Y
stop service...
kill daemon process:
ps aux|grep /opt/nsfocus/bin/daemon_heartbeat_check.py|grep -v grep|awk
'{print $2}'|xargs kill -9: ok
```

### A.3.12 Changing the HTTPS Port

On the main menu shown in [Figure A-5](#), type **14** and press **Enter**. Type the new port number as prompted.

Figure A-19 Changing the HTTPS port

```
$:14
Input Https Port(Available ports:443,1024-65535 .Please do not use 8081,
8083,8805,8084,4500,10002,10003,12345,5432,8088,6565,8080,They are in us
ed ):█
```

### A.3.13 Adding Disks to LVM Partitions

On the main menu shown in [Figure A-5](#), type **15** and press **Enter**. Add one or more disks to LVM partitions.

Figure A-20 Adding disks to LVM partitions

```
$:15
configd: no process found
configd pid is 35281 result 1
Please input new disk in list:[], Multiple split with '|'
Please input lvm partition to be extended some of ('backup', 'clickhouse', 'hdfs_pcap', 'pg_log', 'sftp_out', 'ssn_pcap', '')
```



- When adding one or more disks to multiple partitions, equally divide the total space of the new disk(s) among partitions.
- When adding disks, you can decide whether to encrypt them. Even if the original data disk is not encrypted, a new disk can be independently encrypted.

### A.3.14 Resizing LVM Partitions

On the main menu shown in [Figure A-5](#), type **16** and press **Enter**. Change the sizes of LVM partitions as prompted.

Figure A-21 Resizing LVM partitions

```
$:16
configd pid is 40937 result 1
====> disk_name: /dev/sda, disk_size: 64023257088
====> disk_name: /dev/sdb, disk_size: 2000398934016
====> disk_name: /dev/sdc, disk_size: 12000138625024
====> disk_name: /dev/sde, disk_size: 12000138625024
====> disk_name: /dev/sdd, disk_size: 12000138625024
All available disk size is 38064838066176.
Please input size percentages such as (10|25|5|15|5|20|20) in order (backup|clickhouse|hdfs_pcap|pg_log|sftp_out|ssn_pcap|thre
eat_pcap):
```

### A.3.15 Exiting the Console

After completing the configuration, on the main menu shown in [Figure A-5](#), type **0** and press **Enter** to exit the console. To modify the settings, you need to log in to the console again.

# B Default Parameters

---

The following tables list the initial settings of the management interface as well as initial accounts for login to the web-based manager and console.

## B.1 Management Interface

<b>IP Address (Interface M)</b>	192.168.1.1
<b>Netmask</b>	255.255.255.0

## B.2 Default Accounts

<b>Role</b>	<b>User Name</b>	<b>Password</b>
Super administrator of the web-based manager	admin	admin2022.Uts
Auditor of the web-based manager	auditor	auditor2022Uts.
Console administrator	conadmin	conadmin
SSH administrator	Contact NSFOCUS technical support for the user name and password and use the SSH function under their guidance.	

## B.3 Communication Parameters of the Console Port

<b>Baud Rate</b>	115200
<b>Data Bits</b>	8

# C Remote Assistance Configuration

To enable and configure remote assistance, follow these steps:

**Step 1** Choose **System > System Configuration > Device**.

**Step 2** Select **Yes** for remote assistance to enable the function.

Figure C-1 Enabling remote assistance

The screenshot shows the configuration page for enabling remote assistance. The 'Remote Assistance' option is selected as 'Yes'. A blue information box provides instructions on how to generate a login key. Below this, there is a field for 'Allowed IP 1' with a placeholder 'IPv4/IPv6 address' and an 'Add' button. Other settings include 'Ping (ICMP)' set to 'Yes', 'Time Sync' set to 'Manual', and 'Device Name' set to 'NSFOCUS UTS'. A green button at the bottom is labeled 'Save and Generate Remote Assistance Key'.

HTTPS Port: 443

Firewall Ports to Block:  22  443  4500  5050  5051  
 5432  6565  8080  8081  8083  
 8088  8805  10002  10003  
 12345

Remote Assistance:  Yes  No

Type and save the IP address of the client that needs to remotely connect to this device. Then, scan the QR code through WeCom to generate a login key, or directly copy the login key on the web-based manager. Calculate the device's remote assistance login password through the login key.

Allowed IP 1 \* IPv4/IPv6 address Add

Ping (ICMP):  Yes  No

Time Sync:  Auto  Manual

Time: 2023-09-20 15:18:10

Time Zone: (GMT+08:00) Beijing, Chongqing, Hong Kong, ...

Device Name: NSFOCUS UTS

Device Location: Beijing

Save and Generate Remote Assistance Key

**Step 3** Configure allowed IP addresses.

- Configure **Allowed IP 1**. Both IPv4 and IPv6 are supported.
- If multiple IP addresses need to remotely access UTS, click **Add** and type at most two more IP addresses.

Figure C-2 Specifying IP addresses allowed for remote access to UTS

Remote Assistance:  Yes  No

Type and save the IP address of the client that needs to remotely connect to this device. Then, scan the QR code through WeCom to generate a login key, or directly copy the login key on the web-based manager. Calculate the device's remote assistance login password through the login key.

Allowed IP 1 \*  [Delete](#)

Allowed IP 2 \*  [Delete](#)

Allowed IP 3 \*  [Delete](#)

**Step 4** Click **Save and Generate Remote Assistance Key**.

The system automatically generates and displays a QR code and key for remote login.

Figure C-3 Generating a QR code and key for remote login

12345

Remote Assistance:  Yes  No

Login QR Code



Login Key

```
6171b548fba408479a5d60fb1ea33711sMJNZ5a
dpwvXufqYHeWVcwhVmfidHVQkQIKVFF1+LBGil
2zJ9bb3bDRy1LWwLrLnZO2UyHJgYVGPoqfBys4
NYPUIInzjmwLD8YJHOzHaZN8AUfHebglZdjRL/k
OZinLbwgFofWAbBxLkduQFLDZwtXnmZEh3ATpi
gRLBvdwJBcp33QxOK9MfowSLwNlw855qy8fSYe
jNsSzbTIIVb7
/TXPKcXNp+v7yBtcB3v8SSE25rkPTJw5cvdUFpSb
c99yhkloiZGA8XIYk7S07nPoCs+ttaaObCGeyVJP
3w3VZdjAm1Gf3RyytzpGjWinXnS8+knC8HGF6N
KPUdzmFZ6wO+7SA==
```

Ping (ICMP):  Yes  No

Time Sync:  Auto  Manual

**Step 5** Use an appropriate mobile app to scan the QR code to generate a key or copy and paste the key on the page when remotely logging in to UTS.

---End