

# nChronos

Network Performance Analysis System

Getting Started Guide



Copyright © 2024 Colasoft. All rights reserved. Information in this document is subject to change without notice. No part of this document may be reproduced or transmitted in any form, or by any means, electronic or mechanical, including photocopying, for any purpose, without the express written permission of Colasoft.

Colasoft reserves the right to make changes in the product design without reservation and without notification to its users.

## Contact Us

### **Sales**

[sales@colasoft.com](mailto:sales@colasoft.com)

### **Technical Support**

[support@colasoft.com](mailto:support@colasoft.com)

### **Website**

<https://www.colasoft.com/>

## Contents

Copyright .....	i
Contents .....	ii
Preface.....	1
Introduction.....	3
Installation and Activation .....	4
Installing nChronos Console.....	4
Configuring nChronos Server .....	5
Logging Server from a browser.....	5
Configuring storage settings .....	5
Configuring interface .....	6
Adding a network link .....	7
Running a network link .....	9
Adding an account.....	9
Adding and Connecting nChronos Server .....	10
Console User Interface.....	10
Adding nChronos Server .....	11
Connecting nChronos Server .....	11
Analyzing Network Link.....	12
Retrospectively analyzing a network link.....	12
The Link Analysis window .....	12
Time Window .....	13
Analysis views.....	14
Monitoring Network Link.....	17
Monitoring a network link in real-time.....	17
The link monitor window .....	17
Configuring Network Link .....	19
How to add a network segment.....	19
How to add an application .....	20
How to add a traffic alarm .....	21

# Preface

## Summary

This guide is provided to guide the usage of nChronos. It is recommended to read this guide chapter by chapter, which are arranged according to usage and difficulty.

## Who should read this paper

This guide is written for the beginners of nChronos.

## Glossary

The commonly used terms in this guide are described in Table 1.

Table 1 Glossary

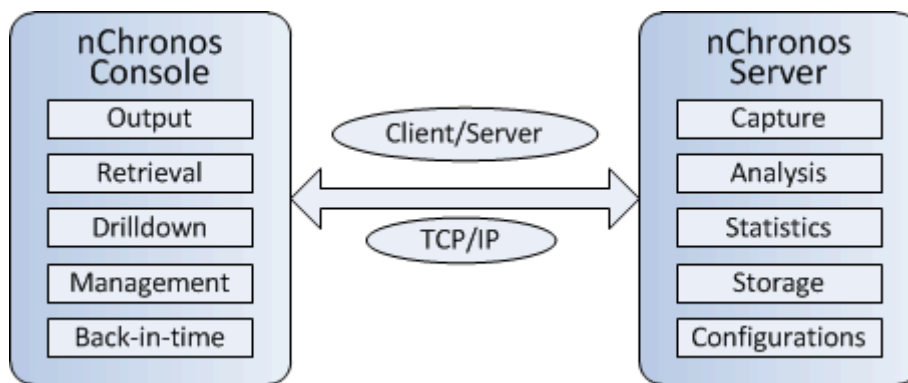
Term	Description
<b>nChronos Server</b>	The core of nChronos, for capturing, analyzing and storing the traffic data of target network which is also called as network link. Communicates with nChronos Console via the communication port. Also called as <i>Server</i> .
<b>nChronos Console</b>	A data presentation platform. Connects to nChronos Server, provides various statistics for users to view and analyze the network traffic status, and provides retrospective analysis, new analysis and data drilldown. Also called as <i>Console</i> .
<b>Analysis object</b>	The network elements, including protocols, addresses, ports, conversations, applications, hosts, network segments, target network, and other elements.
<b>Capture interface</b>	A network interface/port on nChronos Server, generally connected with the mirror port, for capturing the traffic of the target network.
<b>Management interface</b>	A network interface/port on nChronos Server, generally for accessing the Internet such that nChronos Consoles and third-party apps can access the nChronos Server to obtain statistics and analysis data.
<b>Network link</b>	A network object for nChronos to collect captured network traffic and to make statistics and analysis.
<b>Back-in-time analysis</b>	Also called as retrospective analysis. Provides detailed analysis presentation, data drilldown, new analysis and various statistics for historical network data.
<b>Time Window</b>	A time range with specific span which could be 4 minutes, 20 minutes, 1 hour, 4 hour and other time spans. Smaller time span provides less data volume and finer data

Term	Description
	granularity. With the Time Window, network data of historical time can be retrieved easily.
<b>Filter</b>	A group of user-defined data screening conditions or rules to accept the required data.
<b>IP pair</b>	A pair of IP addresses, without the identification of source address and destination address.
<b>Drilldown</b>	Level-by-level progressive analysis on selected network objects which include applications, network segments, addresses and conversations.
<b>Expert Analyzer</b>	A packet-level analysis system. Provides lots of statistics about selected network objects and original decoding information of the packets.
<b>Web application</b>	URL-based applications and defined by host name, IP address, port number and URL parameters.
<b>Signature application</b>	Applications defined by the feature codes of original data flow, in ASCII, Hex, UTF-8 or UTF-16.
<b>Performance analysis</b>	The analysis on the service performance of an application.

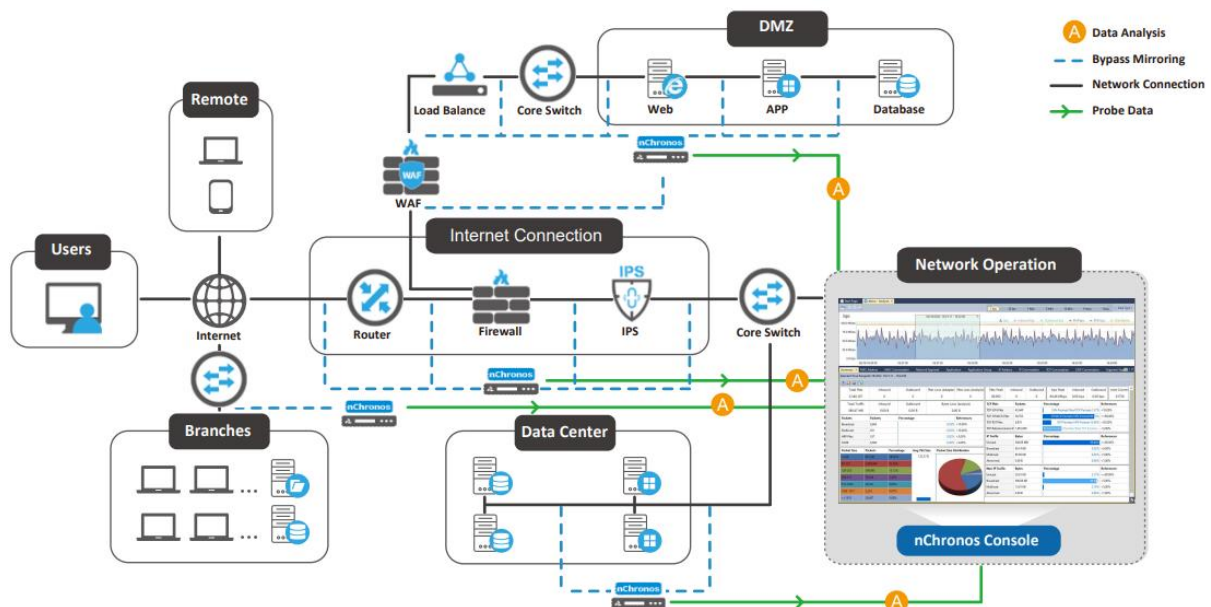
## Introduction

Colasoft nChronos consists of nChronos Server and nChronos Console. nChronos Server is the core of nChronos, for capturing, analyzing and storing the packets of target network. nChronos Console is a data presentation platform, for accessing nChronos Server to obtain statistics and other analysis data for presentation. Users should first deploy nChronos Server, and then connect the nChronos Server to a Console to view data.

The functional architecture of nChronos Consoles and nChronos Servers is described as the following figure:



The deployment of nChronos is visualized as the following figure:



To capture traffic effectively, the traffic sources are must from appropriate network devices. Managed switches are the perfect choice because you can use their port mirroring/SPAN function to copy the packets to a monitor port. This function is called as *Port Mirroring* (Cisco calls it *SPAN*).

## Installation and Activation

This chapter introduces nChronos Console installation. nChronos Console can be used without activation since version 6.0.

### Installing nChronos Console

#### System requirements

The recommended system requirements for nChronos Console are:

- 4-core processor
- 8GB RAM
- Independent network adapter
- Chrome 50+ or Firefox 63+

#### Installation steps

Before installing nChronos Console, you should:

- Make sure your machine meets the minimum system requirements.
- Close all running applications on your machine.
- Uninstall any earlier or trial versions of nChronos Console.

To install nChronos Console:

1. Double-click the installation file of nChronos Console, and then the Setup wizard appears. Click **Next**.
2. On the License Agreement page, review the License Agreement and, if you agree, select the **I accept the agreement** check box, and then click **Next**.
3. Review the product updates, and then click **Next**.
4. Specify an installation directory. By default, the installation directory is C:\Program Files\Colasoft CSRAS Console x.x.x. To specify another directory, use the field provided or click **Browse** to locate an installation folder. Then click **Next**.
5. Specify the folder name on the **Start**, and then click **Next**.
6. Specify whether to create a desktop icon and a quick start icon, and then click **Next**.
7. On the Ready to Install page, review the installation information and, if all information are correct, click **Install** to install nChronos Console to the computer.
8. Review the Readme, and then click **Next**.
9. Click **Finish** to complete the installation. By default, the **Launch Program** check box is selected to launch the program after the installation.

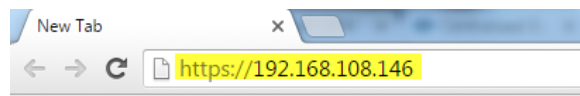
## Configuring nChronos Server

To capture useful traffic and analyze efficiently, you need to configure nChronos Server first. This chapter describes the necessary configurations of nChronos Server to start analysis, and all these configurations are done on webpages. So, you should first login nChronos Server from a browser.

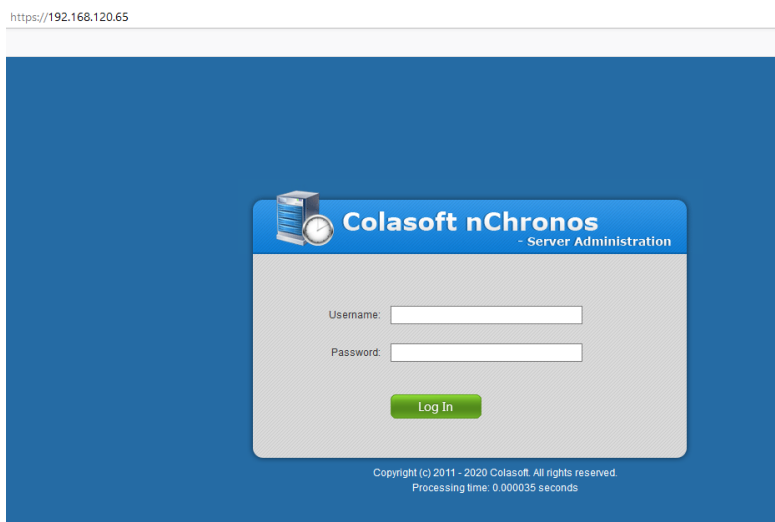
### Logging Server from a browser

You can log nChronos Server from the browsers at both the Server side and the Console side. To log in a Server from a browser, follow the steps below:

1. Launch a browser, in the address bar input <https://IP> and then press ENTER. The IP is the IP address of the management interface of nChronos Server.



2. On nChronos Server login portal, input the user name *admin* and the password *D&^4Vs!()*, and then press ENTER.



3. Click **Log In** to log in the Server.

### Configuring storage settings

You should further configure the storage space to store data.

To allocate the storage space,

1. Login the Server from a browser.
2. Click **Storage Settings** on the left navigation bar to get into the **Storage Settings** page:



**Storage Settings**

Disk Space

Device	Mount Point	Total Space	Available Space	Storage Space Used	Storage Space Configured	Export Data Space
/dev/sda1	/	90GB	38GB	0GB	0 GB	0 GB
/dev/sdb1	/data	6415GB	6291GB	5225GB	6310 GB	5 GB

Analysis Space

Storage Area	Statistics Space	Packet Space	Transaction Logs Space	Alarm Logs Space
Default storage area	200GB	5000GB	10GB	10GB

[New Storage Area](#)

OK

3. Enter an integer for the Storage Space Configured box to set the space for storing nChronos Data.
4. Click New Storage Area to create a storage area.
5. Click **OK** to save settings.

## Configuring interface

Due to the architecture of nChronos, there should be at least two network interfaces/ports on the machine where nChronos Server is installed, one being taken as the Capture interface and the other as Management interface. The Capture interface is for capturing traffic and delivering it to nChronos Server and the Management interface is for nChronos Console to communicate with nChronos Console.

You have no permission to open this shortcut. Please contact the administrator.

To specify the capture interface and the management interface,

1. Login the Server from a browser.
2. Click **Interface Settings** on the left navigation bar to get into the **Interface Settings** page, which lists all available adapters:

**Interface Settings**

Name	bps	Speed (Mbps)	Type	Transmission Medium	Identify IP Layer	Operation
eth0(192.168.9.177)	31.144 Kbps	1000	Managemen			Edit
eth1(0.0.0.0)	0.000 bps	100	Capture in	Ethernet	Second la	Edit
eth2(0.0.0.0)	401.338 Mbps	1000	Capture in	Ethernet	First layer	Edit
eth3(0.0.0.0)	0.000 bps	100	Capture in	Ethernet	First layer	Edit

OK

3. Under the **Type** column, select an appropriate interface type for the adapters.
4. Click **OK** to save the settings.

After specifying the Capture interface and the Management interface, if you need to modify the settings of the Management interface, follow the steps below:

1. Click **Edit** following the Management interface to get into the setup page, like the following figure:

**Interface Settings/Set Management Interface**

Management1 (192.168.26.1)

---

IP address:	<input type="text" value="192.168.5.160"/>
Subnet mask:	<input type="text" value="255.255.255.0"/>
Gateway:	<input type="text" value="192.168.5.1"/>
DNS server:	<input type="text" value="8.8.8.8"/>

---

2. Enter the IP address, subnet mask, gateway, and DNS server address, and then click **Save**.

If you need to set up a virtual capture interface, just click the **Edit** button following the capture interface to go to the Virtual Interface page, and then set up a virtual interface.

## Adding a network link

To add a network link, follow the steps below:

1. Login the Server from a browser.
2. Click **Link Configuration** on the left navigation bar to get into the **Link Configuration** page
3. Click **New Link** to show the following page:

**Basic Information**

Link name:  Network link name cannot contain the following characters \/: ? \< > |

Network link type:

Storage area:

**Inbound/Outbound Traffic Capturing Interface**

Network Interface	Transmission Medium	IP Address	bps	Speed (Mbps)
<input checked="" type="checkbox"/> eno33559296	Ethernet	0.0.0.0	0.000 bps	1000
<input checked="" type="checkbox"/> eno50338560	Ethernet	0.0.0.0	0.000 bps	1000

**Inbound/Outbound Network Segment**

0.0.0.0

**Instructions:**

Enter network segment rules to identify internal IP addresses, with one entry per line.

**Examples for network segment rules:**

IP/subnet: 192.168.0.0/24 or 192.168.0.0/255.255.255.0 or 2001:3ef0::80  
 IP address range: 192.168.0.0-192.168.1.255 or 2001:3ef0:0001-2001:3ef0:0005  
 Single IP address: 192.168.0.100 or 2001:3ef0:0001  
 One segment per line.  
 Segment cannot be duplicated.

**Analysis Operation**

Enable switch timestamp analysis

ARISTA     VSS monitoring     Gigamon

Export data in CSV format

Enable millisecond traffic statistics

Specify IP statistics layer

Specify virtual network ID statistics layer

Innermost layer     Outermost layer     Innermost layer and Outermost layer   

4. Enter the link name and select a link type. The following list describes the link types.

- **Switch (mirrored bidirectional traffic):** nChronos captures traffic from the switch which has mirrored traffic, including inbound and outbound.
- **Switch (mirrored unidirectional traffic):** nChronos captures traffic from the switch which has mirrored one-way traffic, inbound or outbound.
- **Standard tap:** A network tap which only mirrors one-way traffic, inbound or outbound.
- **Aggregation tap:** A network tap which mirrors bidirectional traffic, including inbound and outbound.

5. Select a storage area for the network link. The data of multiple network links can be stored on one storage area.

6. Set capture interface and network segments:

If you select Switch (mirrored bidirectional traffic) or Aggregation tap, follow the steps below:

- 1) Select the capture interfaces which are connected with the mirror port of the switch or the tap.
- 2) Set the network segment, which is for identifying the transmission direction of the packets to further get accurate inbound and outbound traffic statistics. You should enter the IP addresses and the segments that should be recognized as internal addresses.

If you select Switch (mirrored unidirectional traffic) or Standard tap, follow the steps below:

- 1) Select the capture interfaces that are connected with the outbound mirror port of the switch or the tap for capturing outbound traffic.

- 2) Select the capture interfaces that are connected with the inbound mirror port of the switch or the tap for capturing inbound traffic.
7. Set up whether to use switch timestamp, whether to export data, whether to enable millisecond analysis.
8. Set bandwidth. Enter the inbound bandwidth, outbound bandwidth, and the total bandwidth. You should type the actual bandwidth to get accurate bandwidth utilization.
9. Click **OK** to complete the network link.

## Running a network link

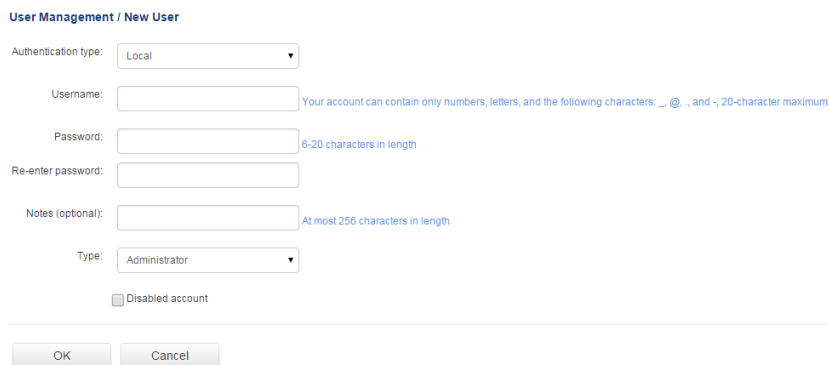
To view real-time, dynamic, up-to-the-second network data at the Console side, to get the analysis statistics of the network traffic, or to download packets from the Server, you must monitor the network link to make the link running.

To run a network link, just click the button **Run** on the **Link Configuration** page.

## Adding an account

To add an account, follow the steps below:

1. Login the Server from a browser.
2. Click **User Management** on the left navigation bar to get into the **User Management** page
3. Click **New Account** on the **User Management** page to show the following page.



4. Enter the user name, the password for the account, and the notes.
5. Select the account type:
  - **Administrator:** An administrator has the administrator authority, can login the Server from both the Console and browsers, and can configure the Server and the link settings.
  - **User:** A user can login the Server from the Console, but cannot configure the link settings.
  - **Auditor:** An audit can only login the Server from browsers, but can only view the audit logs.
6. Click **OK** to completely add an account.

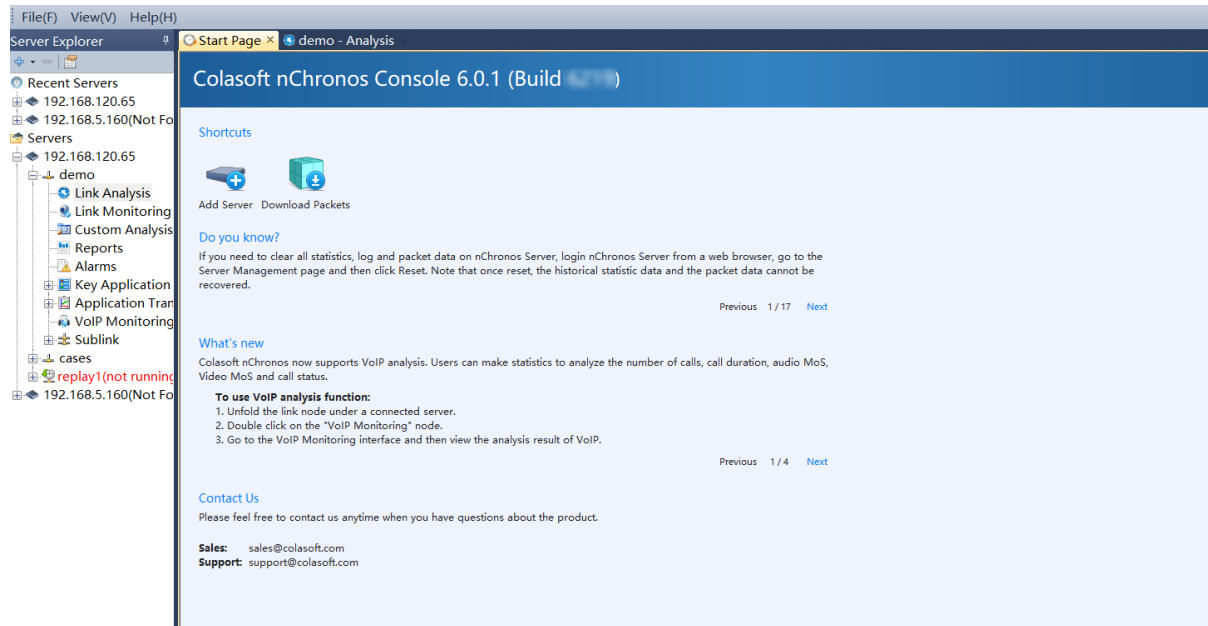
## Adding and Connecting nChronos Server

As a result of the architecture of nChronos, to view traffic and data on nChronos Server, you must add and connect the nChronos Server to the Console.

### Console User Interface

After the installation, to start nChronos Console, click **Start** > Colasoft nChronos Console.

Then the program appears:



The Console user interface includes three parts: Menu bar, Server Explorer pane, and Start Page.




#### Menu bar

The Menu bar includes four menus: File, View, Window, and Help.

#### Server Explorer pane

The Server Explorer lists all added Servers and server groups and, if you select a Server or a network link, shows the basic information of the Server or the network link at the bottom of the Server Explorer.

The list below describes the icon buttons on the Server Explorer.

-  : Adds a Server or a server group to the Console.
-  : Removes the selected Server from the Explorer pane.
-  : Views the properties of the selected item.


When a Server is connected, the network links on the Server display under the Server.

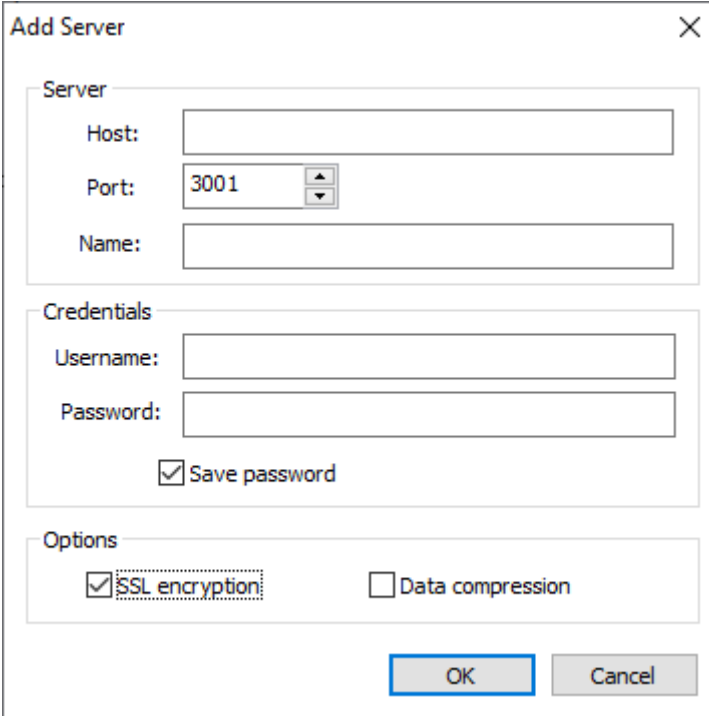
#### Start Page

The Start Page is the main interface you see when launching nChronos Console, providing tips, features and other information about the program.

## Adding nChronos Server

To add nChronos Server, follow the steps below:

1. On the Server Explorer, click **Servers**, then click  and click **Add Server**; the **Add Server** dialog box appears.



The screenshot shows the 'Add Server' dialog box with the following fields and options:

- Server**
  - Host: [Text box]
  - Port: 3001 [Spin box]
  - Name: [Text box]
- Credentials**
  - Username: [Text box]
  - Password: [Text box]
  - Save password
- Options**
  - SSL encryption
  - Data compression

Buttons: **OK** and **Cancel**

*\* If SSL is not configured, do not check SSL encryption.*

2. Enter the IP address of nChronos Server and type the username and password.
3. Click **OK** after completing the **Add Server** dialog box. Then the added Server will display on the Server Explorer.

## Connecting nChronos Server

To connect to nChronos Server, right-click the server name and click **Connect**.

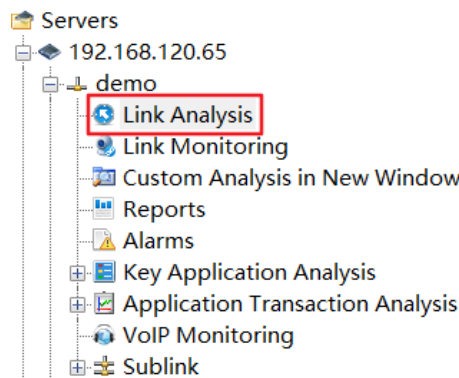
## Analyzing Network Link

With retrospective analysis, the network status of past time can be displayed. This chapter describes how to retrospectively analyze a network link.

### Retrospectively analyzing a network link

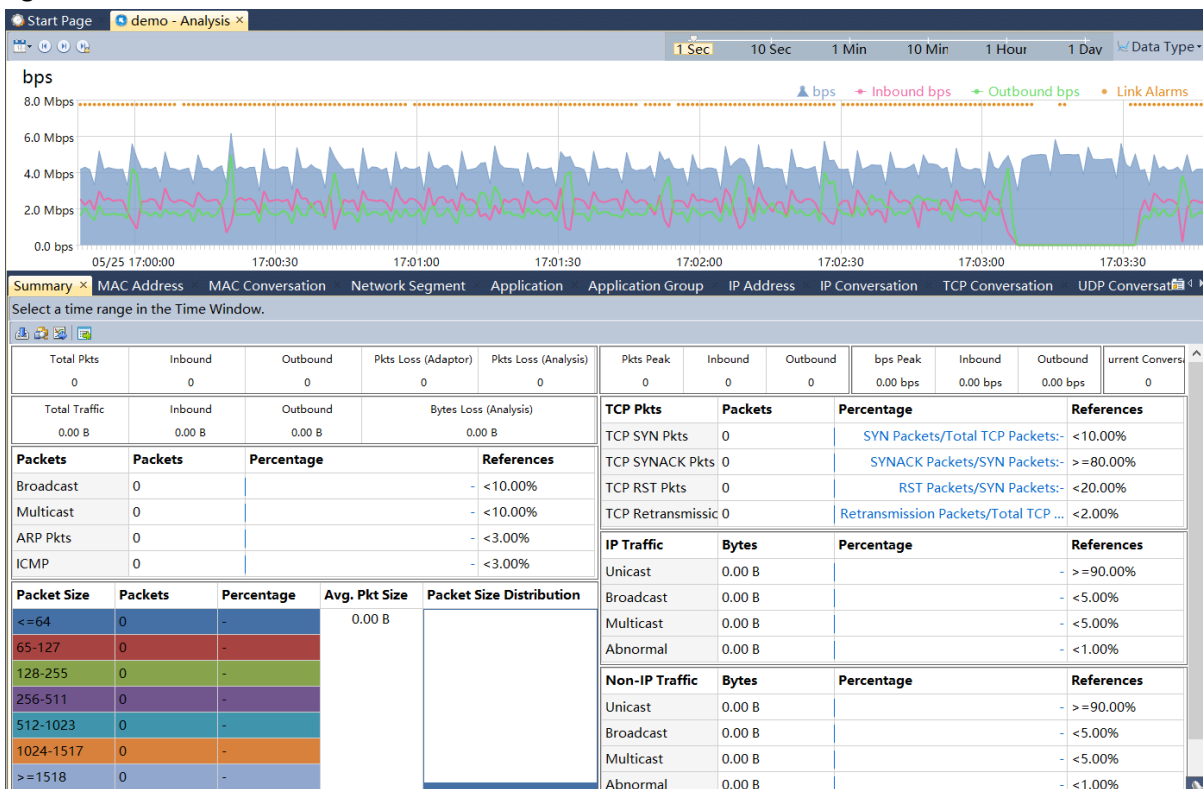
To retrospectively analyze a network link:

1. Connect a Server, and then network links created for the Server displays under the Server on the Server Explorer.
2. Double-click the node **Link Analysis** under the network link to open the Link Analysis window.



### The Link Analysis window

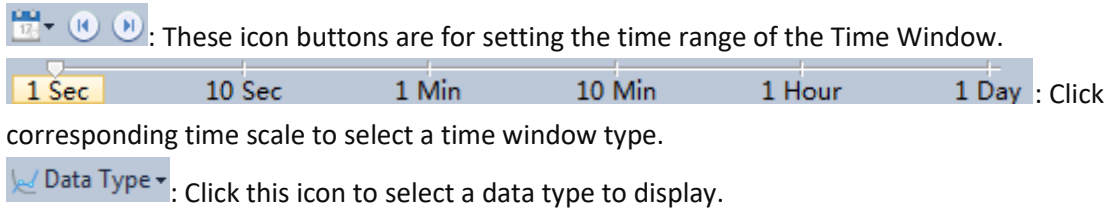
The Link Analysis window is the main workbench of retrospective analysis, showing as the following figure:



The Link Analysis window includes a Time Window pane, and an analysis views pane.

## Time Window

The following list describes the icon buttons on the Time Window.



### Draggable Time Window

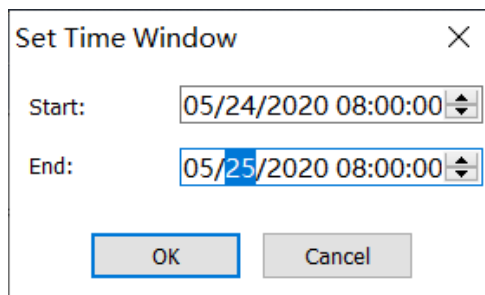
You can drag the Time Window to view network data of past time range. To drag the Time Window, move your mouse on the time scales of the charts, and drag when the mouse becomes .

### Setting the Time Window

You can choose to set the Time Window or to set the selected time range.

To set the Time Window, follow the steps below:

1. Click and select **Set Time Window**. The **Set Time Window** dialog box appears.

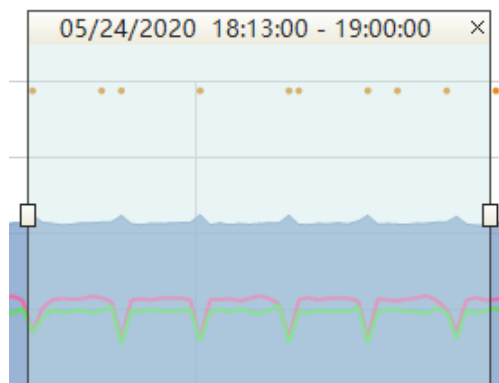


2. Set the start time in the Start field and set the end time in the End field.
3. Click **OK**.

### Selecting a time range

The analysis views below the Time Window display the data of selected time range on the Time Window.

To select a time range, just drag your mouse on the Time Window, and then the range will be framed with two handles and a time bar, just like the following figure:



You can drag the handles to widen or narrow the time range.



## Analysis views

There are several analysis views to display the statistics in different types. They work together with trend charts and time range selection on it to reduce statistic data volumes and let you focus on analyzing and drilldown to look into network issues.

### Icon Buttons on the toolbars of the views

There is a toolbar on the top of each analysis view and the same buttons on different toolbars have the same functions.

The following list describes some buttons on the toolbar.



: Downloads packets of current time range. For more information about downloading packet, see *Download Packets dialog box* in this section.



: Launches the Expert Analyzer to analyze the packets of selected time range.



: Saves the current statistical list as a .csv file. For more information about exporting statistics, see *Export Statistics dialog box* in this section.



: Click to generate a temporary report based on the statistics on the current view.



: Click to generate a graph based on the statistics on the current view. Click the icon again to close the graph back to list data.

### The Summary view

The Summary view provides overall summary statistics of alarms, utilization, traffic, packets and TCP packets of selected time range on the trend chart.

### The MAC Address view

The Physical Address view displays the traffic of the network according to MAC addresses, as well as bytes, and packets. Right-click the column header and click the appropriate column, then you can view the statistics in the form of other statistical fields.

### The MAC Conversation view

The Physical Conversation view displays the traffic of the network according to physical communication nodes, as well as node bytes, and packets.

### The Network Segment view

The Network Segment view provides the statistics and analysis of the traffic according to network segments which are defined when configuring the network link.

### The Application view

The Application view provides statistics of network applications, including system applications and custom applications. The system applications are uploaded to the library when configuring the Server at the Server side and the custom applications can be customized when configuring network link at the Console side. The custom applications have priority over the system applications.

The Application view displays the traffic of the network according to applications name, as well as bytes, packets, and average packet size. Right-click the column header and click the appropriate column, then you can view the statistics in the form of other statistical fields.

### **The Application Group view**

The Application Group view displays network traffic statistics based on application groups which are defined when configuring the network link.

### **The IP Address view**

The IP Address view provides the statistics and analysis of the traffic according to IP addresses. By default, this view displays the statistics of internal IP. You can click External IP to view the statistics of external network.

The IP Address view displays the traffic of the network according to IP addresses, as well as bytes, packets, and average packet size. Right-click the column header and click the appropriate column, then you can view the statistics in the form of other statistical fields.

### **The IP Conversation view**

The IP Conversation view provides the statistics and analysis of the traffic according to IP conversations.

### **The TCP Conversation view**

The TCP Conversation view displays the traffic of the network according to communication nodes, as well as node geographic location, port number, application, round-trip time, bytes, packets, and average packet size.

### **The UDP Conversation view**

The UDP Conversation view displays the traffic of the network according to communication nodes, as well as node geographic location, port number, application, bytes, packets, and average packet size.

### **The Segment-Segment view**

The Segment-Segment view provides the statistics and analysis of the traffic according to network segments which are defined when configuring the network link.

### **The Service Access view**

The Service Access view displays application access statistics of the monitored network link, including server/client IP, service port number, application, traffic, and TCP packets.

### **The Service Port view**

The Port view includes two tabs: TCP Service Port and UDP Service Port, displaying port access statistics based on IP address + port number.

### **The Port view**

The Port view provides the statistics and displays of port information in the selected time period.

### **The Link Alarms view**

The Link Alarms view displays the link alarm logs according to alarm types which include traffic alarm, email alarm, domain alarm, and signature alarm. All link alarm logs are listed with trigger time, alarm category, alarm name, severity, and trigger condition, etc.

**The Virtual Network view**

The Virtual Network view displays Virtual Network statistics based on Virtual Network ID, as well as traffic and TCP packets. According to types, there are VLAN, MPLS VPN, VXLAN and All Virtual Network.

**The DSCP view**

The DSCP view displays network traffic statistics based on DSCP markings.

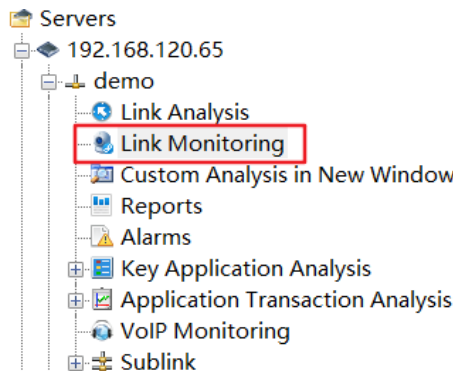
## Monitoring Network Link

Once nChronos Server is connected, the Server Explorer displays the network links under the Server, and then you can choose to monitor the network link in real-time or retrospectively analyze the network link. This chapter describes how to monitor a network link and the elements on the link monitor window.

### Monitoring a network link in real-time

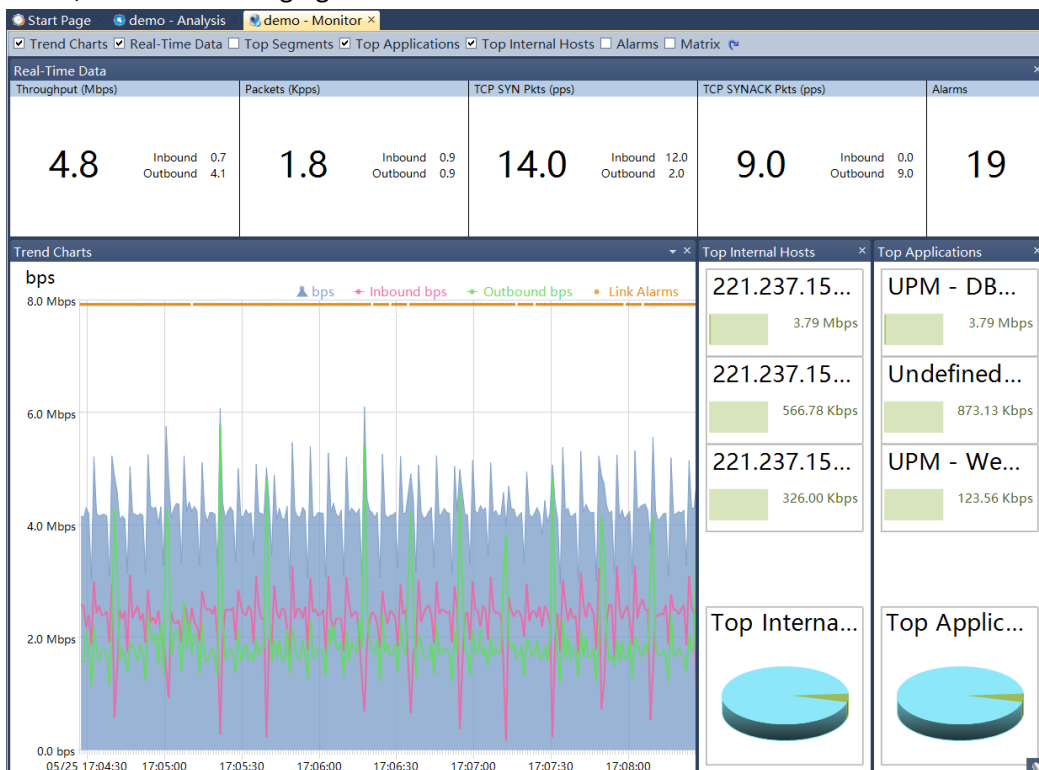
To monitor the network link in real-time:

1. Connect a Server, and then network links created for the Server displays under the Server on the Server Explorer.
2. Double-click the node **Link Monitor** under the network link to open the Monitor window.




### The link monitor window

Once a network link is monitored, a link monitor window appears to show the real-time status of the network link, like the following figure:



The link monitor window includes a top bar and several panes: the Real-Time Data pane, the Trend Charts pane, the Top Segments pane, the Top Internal Hosts pane, the Top Applications pane, the Alarms pane, and the Matrix pane.

The top bar includes checkboxes to show or hide the seven panes, a Default Layout button, and a Back-in-Time button. Select the checkbox in front of a pane to show the pane. Click  to display the link monitor window in the default layout.

To close a pane, just click the close button on the top right corner on each pane or cancel the selection on the check box in front of the pane name on the top bar of the link monitor window.

### **The Real-Time Data pane**

The Real-Time Data pane displays the real-time data of the network link, including throughput, packets, bandwidth utilization, TCP SYN packets, TCP SYNACK packets, and alarm quantity.

### **The Trend Charts pane**

The trend charts on the link monitor window display the real-time status of the network link, with a horizontal axis marked with time scales and a vertical axis marked with value scales. The trend charts update automatically from right to left, displaying the latest data. By trend charts, you can get a direct view of the network status.

### **The Top Segments pane**

The Top Segments pane lists the top network segments according to the traffic of them, and the traffic is displayed by bar charts as well as real-time figures just below the segments. The segments are defined when you configuring the network settings.

### **The Top Internal Hosts pane**

The Top Internal Hosts pane lists the top internal hosts according to the traffic of them, and the traffic is displayed by bar charts as well as real-time figures just below the hosts. The hosts are displayed as names or IP addresses, which is determined according to the setting in the View menu.

### **The Top Applications pane**

The Top Applications pane lists the top applications according to the traffic of them, and the traffic is displayed by bar charts as well as real-time figures just below the applications.

### **The Alarms pane**

The Alarms pane lists all alarms triggered in the one second, including trigger time, alarm category, alarm object, alarm name, alarm severity, and trigger condition.

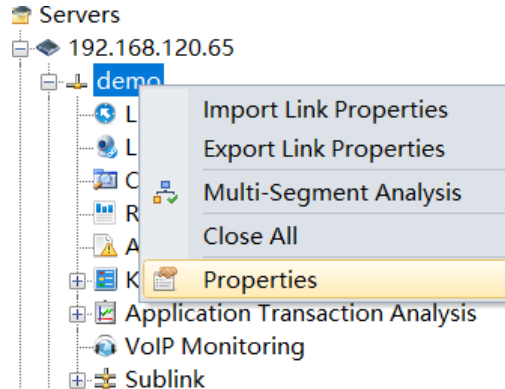
### **The Matrix pane**

The Matrix pane shows the network communication in peer map.

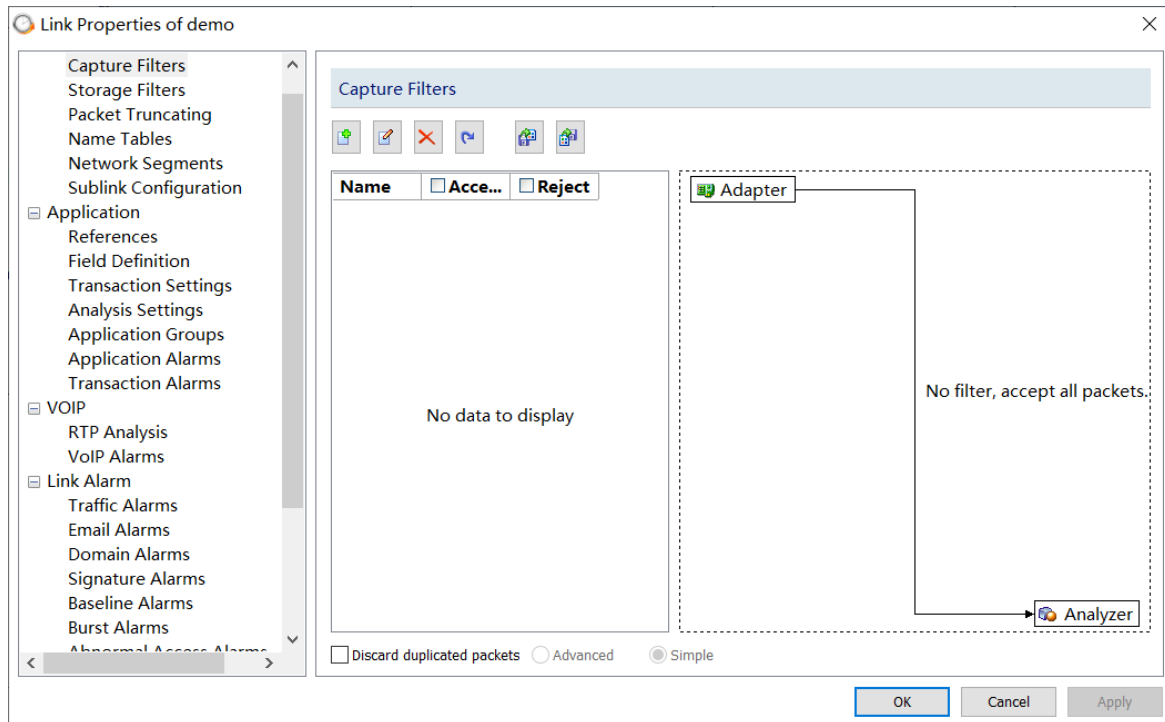
By default, the matrix pane displays the peer map of the communications between IP addresses. Right-click the matrix and select MAC Matrix to display the peer map of the communications between MAC addresses.

## Configuring Network Link

To get effective analysis and statistics, you can configure the properties of a network link. To set a network link, right-click the network link and select **Properties**:



Then the Link Properties dialog box pops up:



For information on how to set up a filter, how to define an application, how to configure an alarm, please refer to the User Guide.

**Note** Link properties are specific to a network link, regardless of the Console on which the settings are made. Furthermore, the network properties under one nChronos Server could have different settings.

## How to add a network segment

Users can add network segments according to geographical location, subnet, or IP address range. The system will do the statistics according the user-defined network segments, which helps users to know network traffic from segment perspective and facilitates traffic analysis.

To add a network segment, follow the steps below:

1. On the **Link Properties** box, click the tab **Network Segments**, and then click the button  to open **Network Segment** dialog box:

Network Segment ✕

---

**Definition**

Name:

Geolocation:

Type:

---

**Rule**

---

**Bandwidth settings**

Inbound bandwidth:  Mbps

Outbound bandwidth:  Mbps

Total bandwidth:  Mbps

2. On the **Network Segment** dialog box, enter the name and the geographical location, and then enter the segment rules and segment bandwidth.
3. Click **OK** on the **Network Segment** dialog box, and then click **OK** on the **Network Segments** tab.


On the Network Segment view, you can see the statistics information for that network segment. If no segments are defined, all IP addresses will be grouped as *Undefined Segment*.

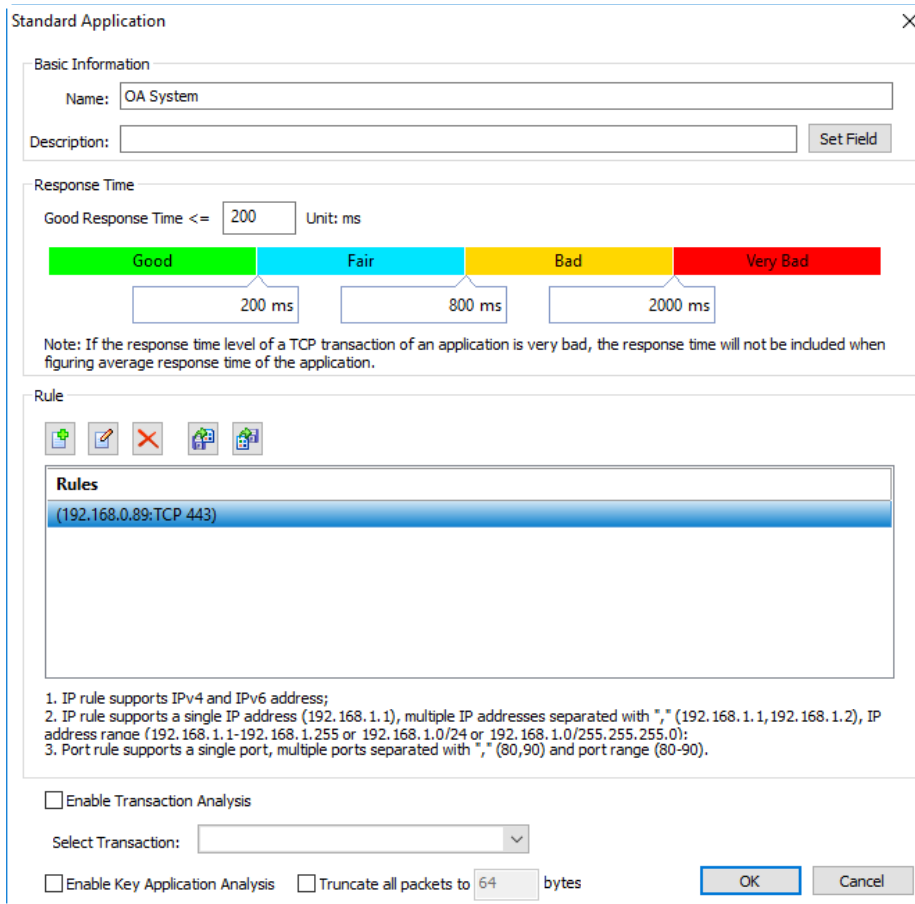
Segment	Geolocation	Type	Total Bandwidth	Inbound Bandwid...	Outbound Bandwidth	Total Bytes	Tx Bytes	Rx Bytes
UPM - Chengdu	Chengdu	Subnet Mask	1000	1000	1000	29.21 MB	12.00 MB	15.12 MB
UPM - segment 2	Segment 2	1	100	100	100	29.21 MB	13.46 MB	15.72 MB
UPM - Beijing	Beijing	Subnet Mask	1000	1000	1000	8.53 MB	4.22 MB	4.31 MB
UPM - Shanghai Branch	Shanghai Branch	Subnet Mask	1000	1000	1000	6.91 MB	4.22 MB	2.68 MB
Undefined Segment	-		1000	1000	1000	6.57 MB	4.37 MB	2.15 MB
UPM - HK Office	HK Office	Subnet Mask	1000	1000	1000	4.30 MB	1.93 MB	2.37 MB
<b>Test</b>	<b>HQ</b>		<b>1000</b>	<b>1000</b>	<b>1000</b>	<b>874.75 KB</b>	<b>385.50 KB</b>	<b>489.24 KB</b>
UPM - segment 1	Segment 1	1	100	100	100	2.45 KB	0.00 B	2.45 KB

## How to add an application

Users can define applications according to application scenarios. Take standard application for example here.


To add a standard application, follow the steps below:

1. Click  on the **Analysis Settings** tab to open the **Standard Application** dialog box as the following figure:



The dialog box is titled "Standard Application" and contains the following sections:

- Basic Information:** Name: OA System; Description: (empty); Set Field button.
- Response Time:** Good Response Time <= 200 Unit: ms. A color-coded scale shows Good (green, 0-200ms), Fair (cyan, 200-800ms), Bad (yellow, 800-2000ms), and Very Bad (red, >2000ms).
- Rule:** Includes icons for adding, editing, deleting, and applying rules. A list of rules shows "(192.168.0.89:TCP 443)".
- Notes:**
  1. IP rule supports IPv4 and IPv6 address;
  2. IP rule supports a single IP address (192.168.1.1), multiple IP addresses separated with "," (192.168.1.1,192.168.1.2), IP address range (192.168.1.1-192.168.1.255 or 192.168.1.0/24 or 192.168.1.0/255.255.255.0);
  3. Port rule supports a single port, multiple ports separated with "," (80,90) and port range (80-90).
- Options:**
  - Enable Transaction Analysis
  - Select Transaction: (dropdown menu)
  - Enable Key Application Analysis
  - Truncate all packets to 64 bytes

2. On the **Standard Application** dialog box, enter the application name.
3. Click  to add an application rule, which could be the combination of a single port, multiple ports, port range, an IP address, multiple IP addresses, and IP address range.
4. Enable Key Application Analysis.
5. Click **OK** on the **Analysis Settings** tab to save the settings.


On the Application view, you can see the statistics information for that application.

Application	Total ...	Uplink Byt...	Downlink Byt...	Inbound Byt...	Outbound Byt...	Total Pkts	Uplink Pk...	Downlink P...	Inbound Pkts	Outbound Pkts	Avg. Pkt Si...
Undefined TCP Application	283.3 GB	1.24 GB	1.10 GB	1.42 GB	934.67 MB	24553559	12513383	12040176	13757169	10788806	101.95 B
UPM - Web Server	577.94 MB	423.57 MB	254.36 MB	423.57 MB	254.36 MB	6792779	3691516	3101263	3691516	3101263	104.65 B
UPM - DB Server	563.34 MB	93.95 MB	569.39 MB	93.95 MB	569.38 MB	1437966	666457	771509	666457	771492	483.71 B
OA System	238.41 MB	146.13 MB	90.28 MB	146.18 MB	90.23 MB	2402658	1200006	1202652	1200870	1201788	103.17 B
Undefined UDP Application	200.43 MB	147.92 MB	52.51 MB	123.38 KB	1.02 MB	575647	411061	164586	611	14800	365.10 B
Test(Deleted)	51.69 MB	25.65 MB	26.04 MB	31.18 MB	20.51 MB	528533	254358	274175	292740	235793	102.54 B
NTP	51.55 MB	25.74 MB	25.81 MB	25.74 MB	25.81 MB	575040	287147	287893	287129	287911	94.00 B
WEB	36.99 MB	11.56 MB	25.43 MB	18.64 MB	8.35 MB	385420	164562	220858	163167	123933	100.63 B
Undefined Application	6.87 MB	6.66 MB	214.21 KB	0.00 B	0.00 B	109033	106191	2842	0	0	66.04 B
UPM - App Server	3.77 MB	2.08 MB	1.69 MB	1.69 MB	2.08 MB	45831	26650	19181	19181	26650	86.23 B
ICMP	3.11 MB	1.41 MB	1.70 MB	37.55 KB	14.21 KB	35297	15809	19488	440	168	92.35 B

## How to add a traffic alarm

The metrics displayed on nChronos Console can be defined as alarm trigger conditions. Here take traffic alarm for example.

To add a traffic alarm, follow the steps below:

1. On the Traffic Alarms tab, click the button  to open the **Traffic Alarms-Add** dialog box as



the following figure:

**Traffic Alarms-Test1**

**Basic Information**

Name:  Creator:

Description:

Category:  Type:

Severity:

**Triggering Condition**

Time Bucket:  Duration:

**Triggering Action**

Send to email   Send to SYSLOG

You should finish alarm sending settings in server before sending

2. Set the trigger condition. Click the buttons to add condition.
3. Click **OK** to save the settings.

When the alarm is triggered, users can check alarm logs on the **Link Alarms** view.

Name	Statistic Time	Start Time	Duration	Sever...	Type	Category	Trigger Condition	IP Address	MAC Address	Application	Application Group	Seg
Test1	07/17/2019 10:39:38	07/17/2019 10:39:36	-		Global	Abnormal Transmission	bps : 4.60 Mbps >= 4.00 Mbps	-	-	-	-	-
<input checked="" type="checkbox"/> Test1	07/17/2019 10:39:39	07/17/2019 10:39:37	-		Global	Abnormal Transmission	bps : 4.63 Mbps >= 4.00 Mbps	-	-	-	-	-
Test1	07/17/2019 10:39:40	07/17/2019 10:39:38	-		Global	Abnormal Transmission	bps : 4.60 Mbps >= 4.00 Mbps	-	-	-	-	-
Test1	07/17/2019 10:39:41	07/17/2019 10:39:39	-		Global	Abnormal Transmission	bps : 4.57 Mbps >= 4.00 Mbps	-	-	-	-	-
Test1	07/17/2019 10:39:42	07/17/2019 10:39:40	-		Global	Abnormal Transmission	bps : 4.50 Mbps >= 4.00 Mbps	-	-	-	-	-