SANGFOR

11 Business Intelligence

IAG 13.0.80 - Associate

PART 1

BI Product Introduction

What is BI ?

The full name of BI is called business intelligence. Sangfor BI is an important manifestation of the Sangfor IAG team's core value proposition. It is an important product of the Sangfor IAG team's continuous innovation around the core value proposition of the product.

Sangfor BI is based on the new architecture of the original convinced IAG external report center, based on massive online logs, and provides a variety of behavior-aware applications based on the application store. Each application helps customers solve a business problem.

How to install BI ?

1. Installation Environment

Hardware requirement

a)Software installation: Between 8GB to 16GB; Required free disk space: 90GB above (Higher is better)

b)Recommendation PC specification: Quad Core with RAM 8G ram and above.

c)Disk format: NTFS

d)Do not support installation/backup to network drive.

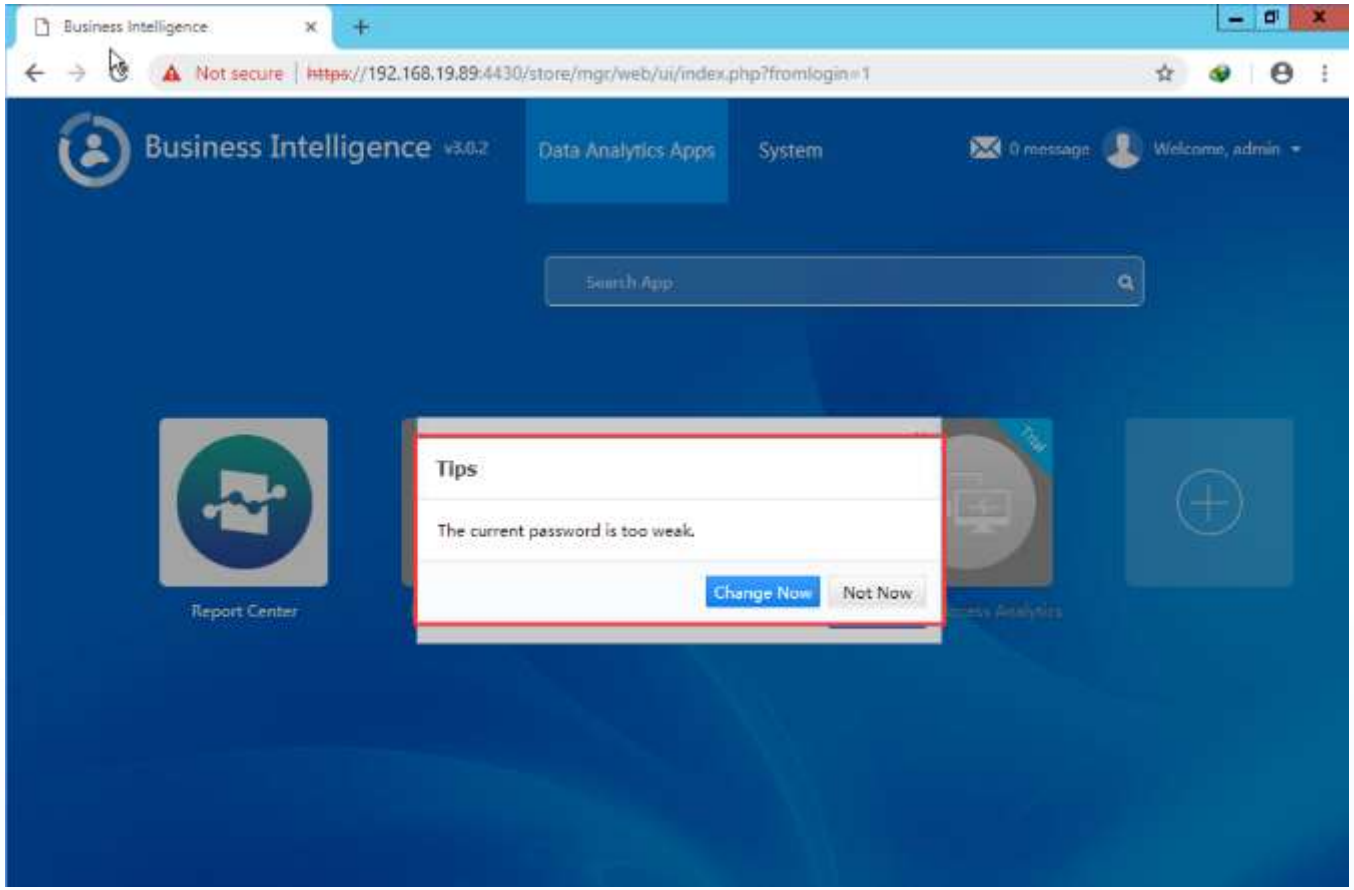
e)Must be installing at Window Server 2008 R2 /2012 with 64-bits OS and later, support data synchronization from lower DC version to higher version using updater package

As the shown below:

SANGFOR_IAM_V12.0.13_BI Installation and Update Configuration Steps.pdf

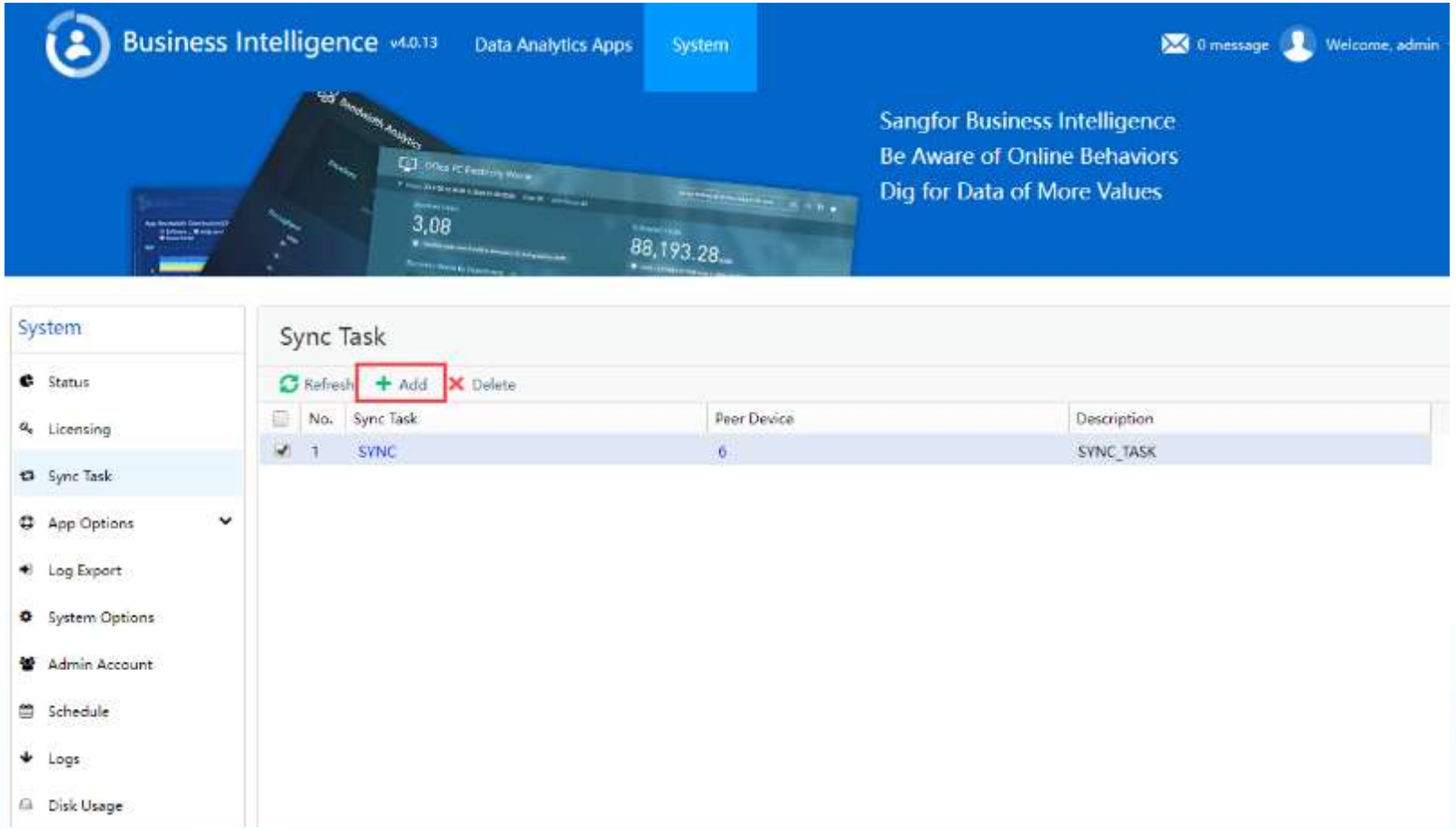
Installation

2. After installation complete, access the BI and the password will be the same as the previous Report Center's password. You will be prompt to change password upon login



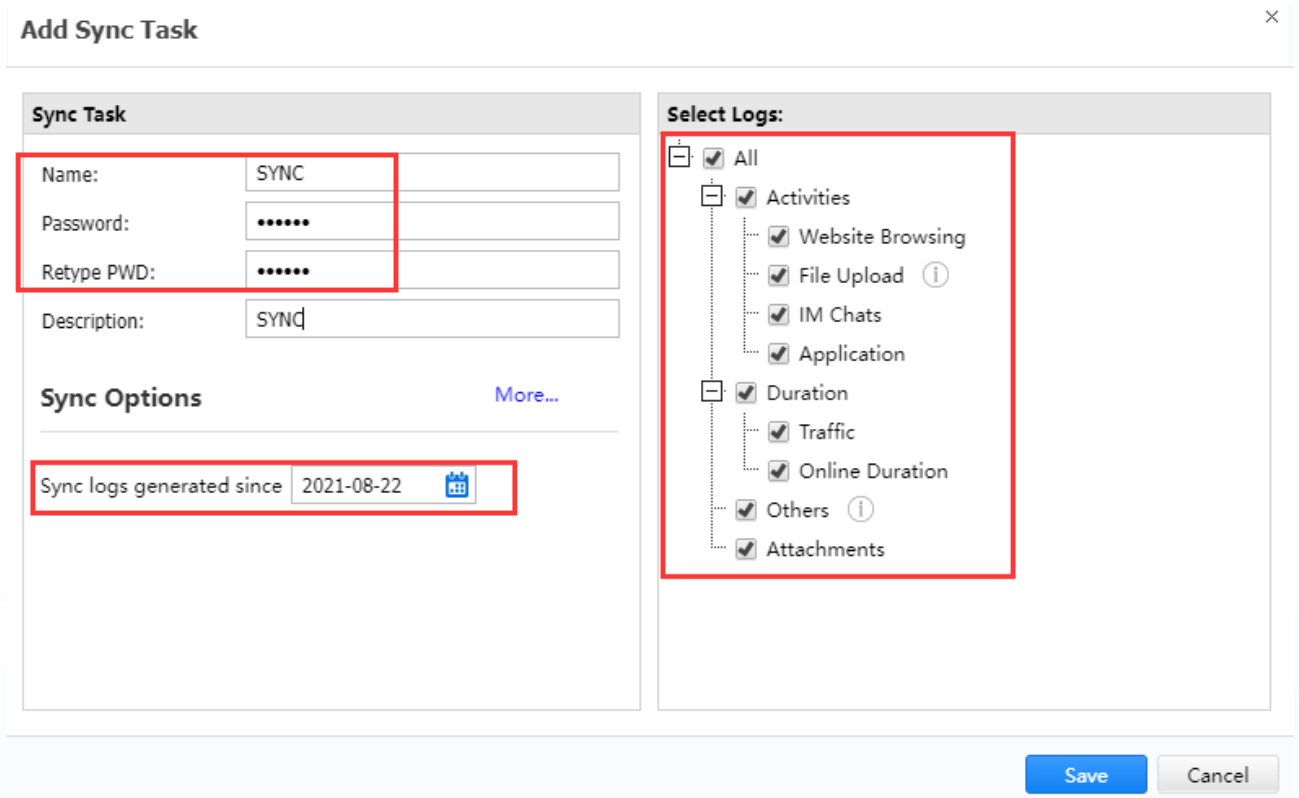
Configuration

3.Go to System > Sync Task.



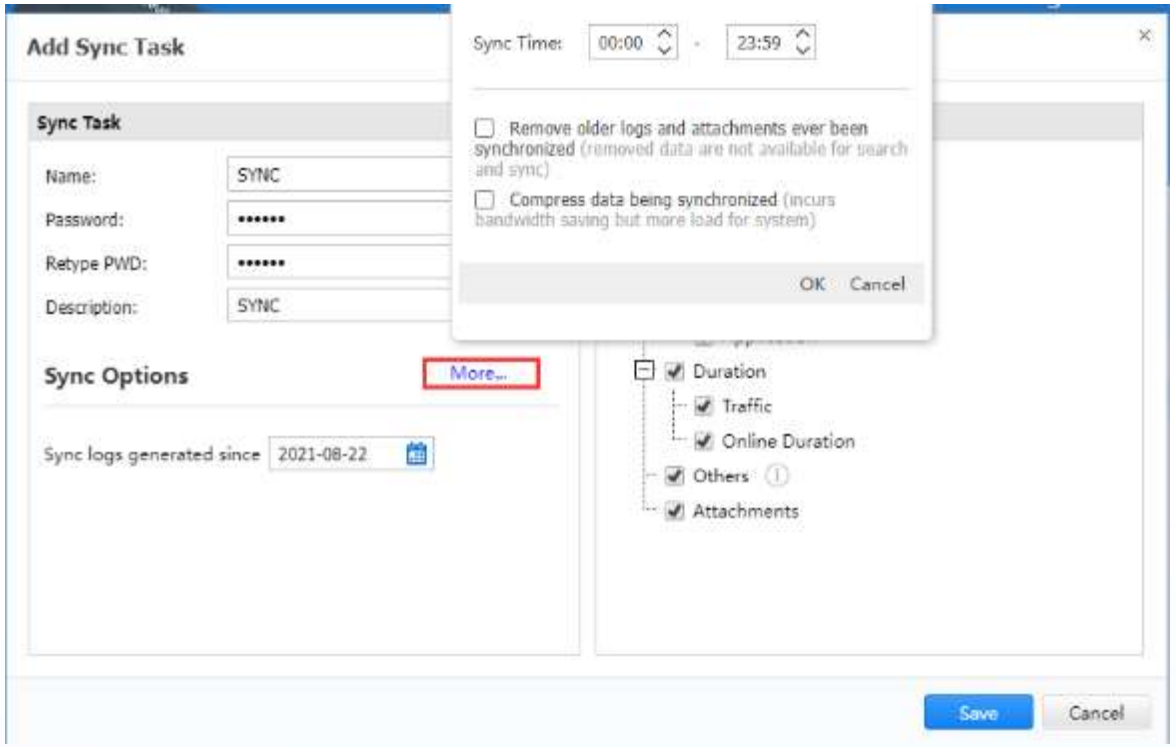
Configuration

3. Enter the Name, Password and Description. You can select which date that you want to start to sync the logs and what type of logs that you want to sync. Click “More” for other sync options.



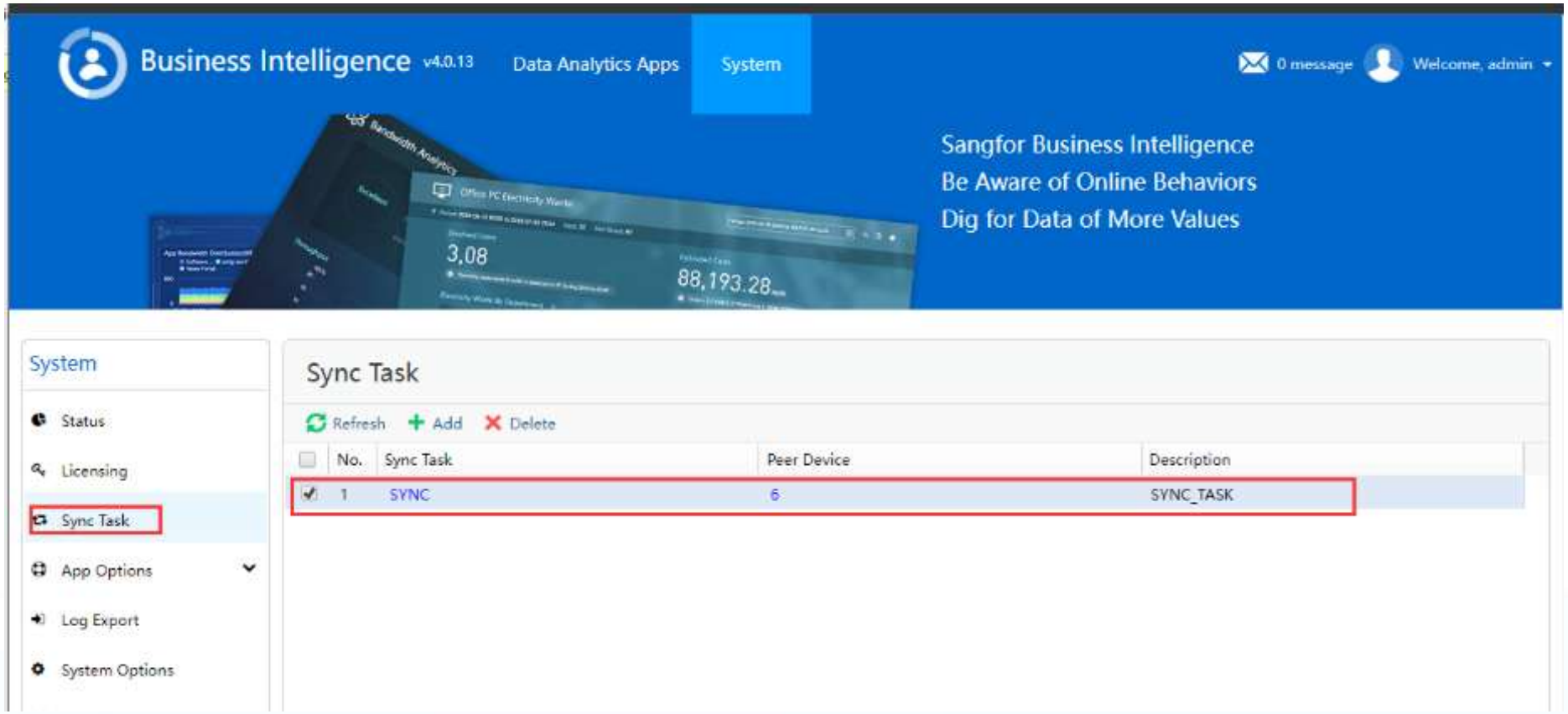
Configuration

3. After clicked the “More”, you able to select the sync time that you want. Besides, you also can remove older logs and attachments by tick the first option and also select the second option to compress the data being synchronized.



Configuration

3. The sync policy is now created.



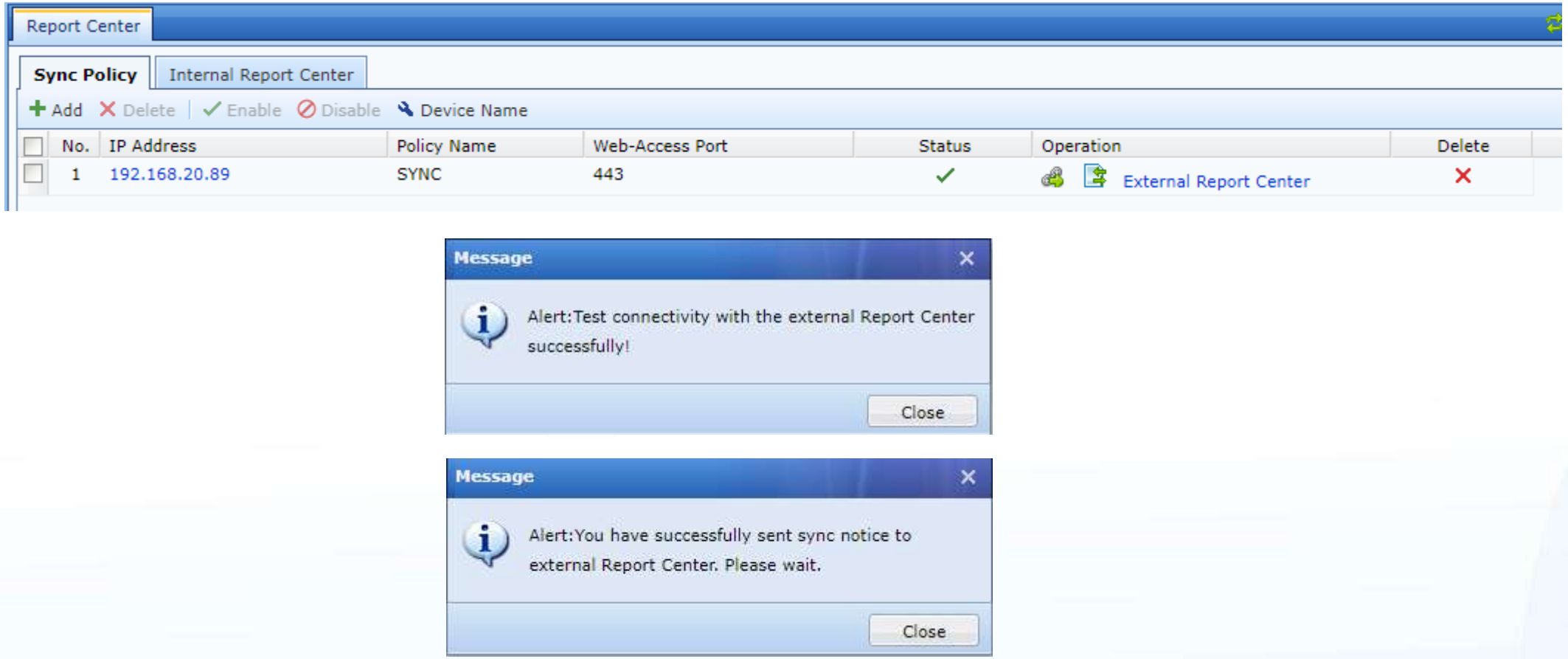
Configuration

4. Configuration on IAG

Path: Go to IAG WebUI, System > General > Report Center and Click Add.

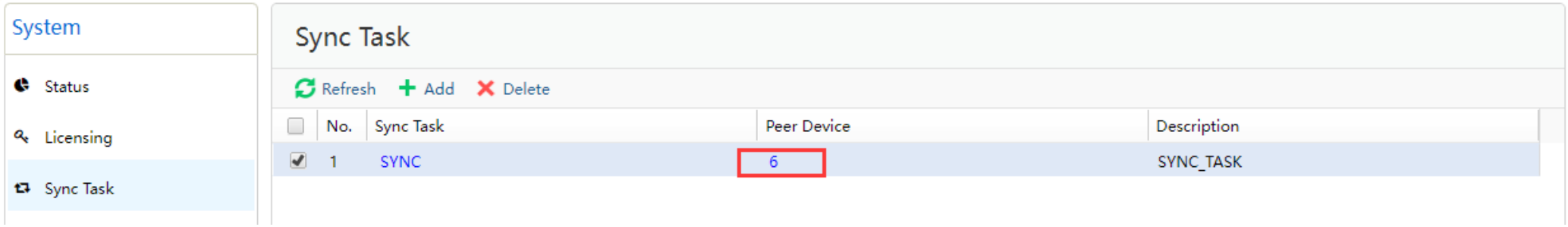
Configuration

4. After that, test the connectivity and you able to start to sync the logs.



Configuration

4. Now you can check the Peer Device number will become 1 which means one device connected with this Business Intelligence.



PART 2

Composition and Implementation of BI

Implementation of BI

Business Intelligence 3.0.2

Data analysis section (software)

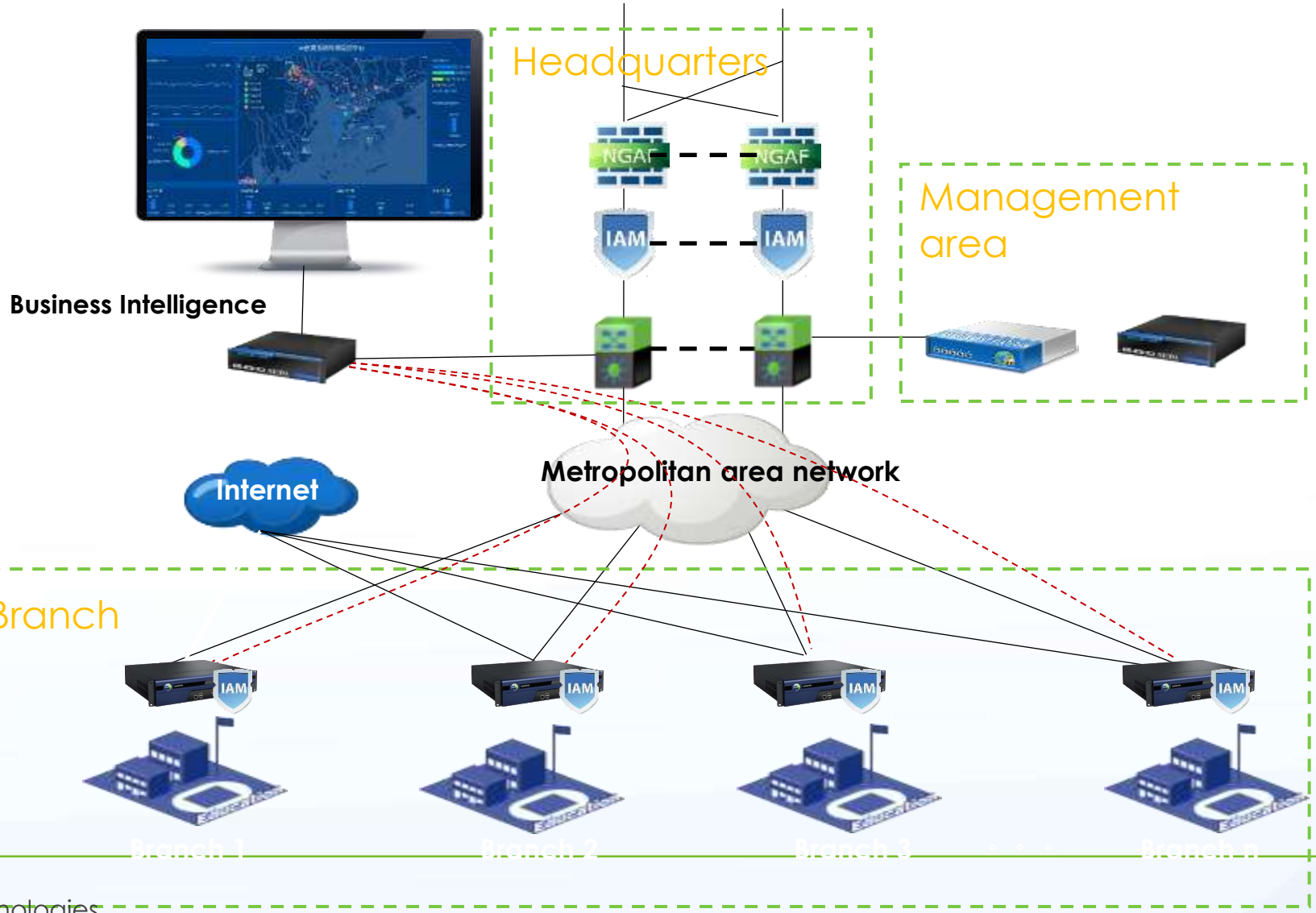
- Data aggregation, modeling, display
- Based on the original external report center platform

Data acquisition section (hardware)

- IAG (13.0.80)

In the future, other system logs may be summarized: one-card system, access control system, etc

Implementation of BI



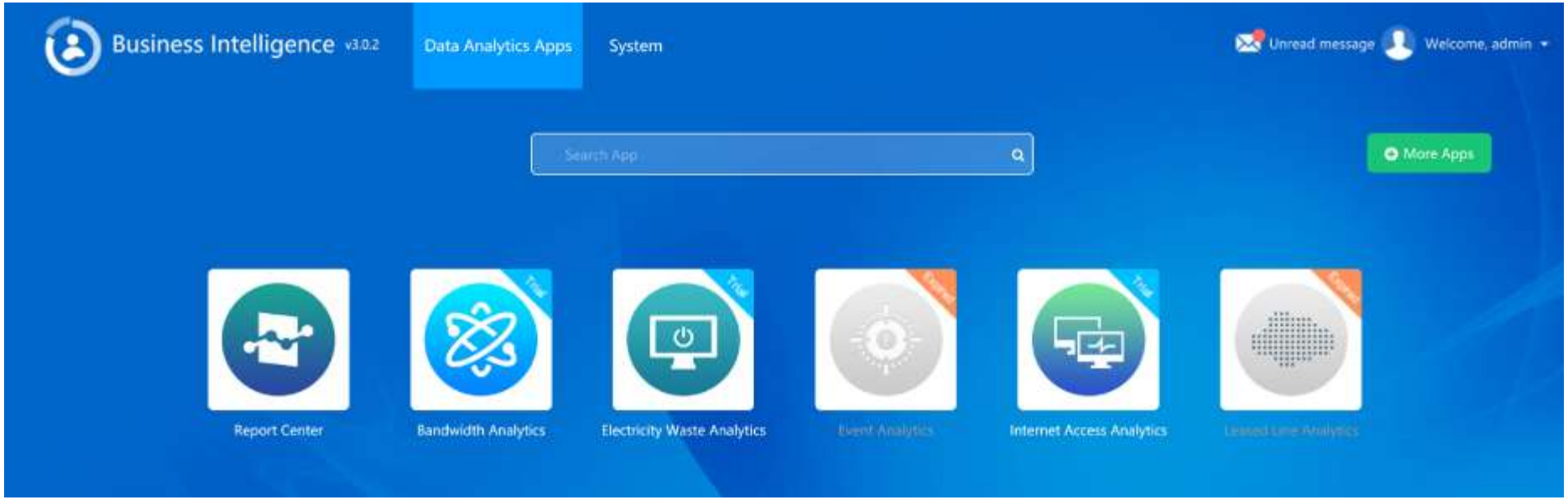
PART 3

Compare the Original Datacenter

New system Interface

Continuously develop applications and explore the value of data in a systematic manner

The new system interface, as shown below



What are the Applications?

With the rapid development of information technology, education/government/enterprise has entered the era of big data,
corresponding to this, How to make massive amounts of data for daily decision making, and make data better for education/government/enterprise services.
For a new research direction.

Report Center

Event Analytics

Internet Access Analytics

Bandwidth Analytics

Leased Line Analytics

Electricity Waste Analytics

Compare the Original Datacenter

Major improvements:

UI is more experience-oriented, design style is more cool

The underlying framework is rectified, the application coding is simpler, and the requirements are raised to land more quickly.

Able to receive more kinds of data, not limited to IAG, such as one-card system, access control system, etc.

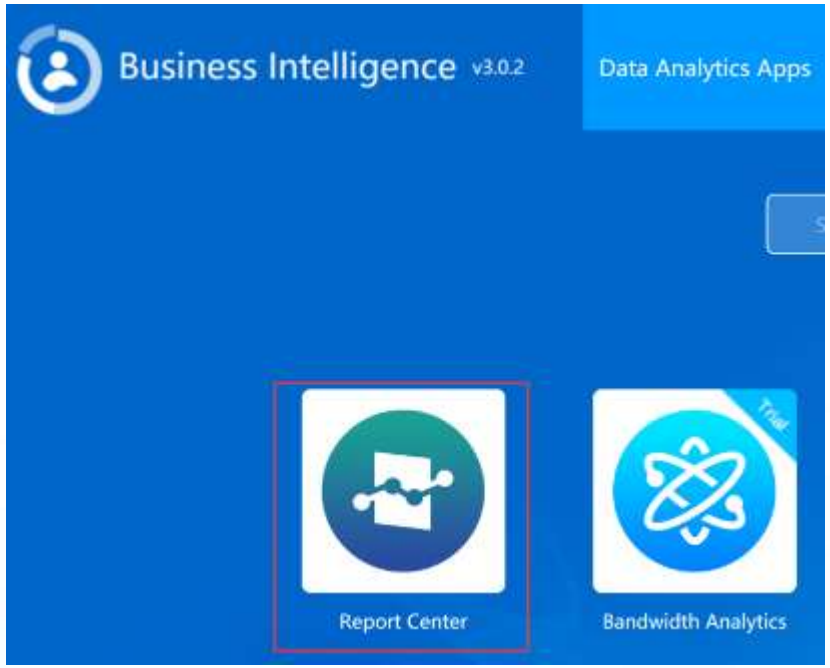
Compare the Original Datacenter

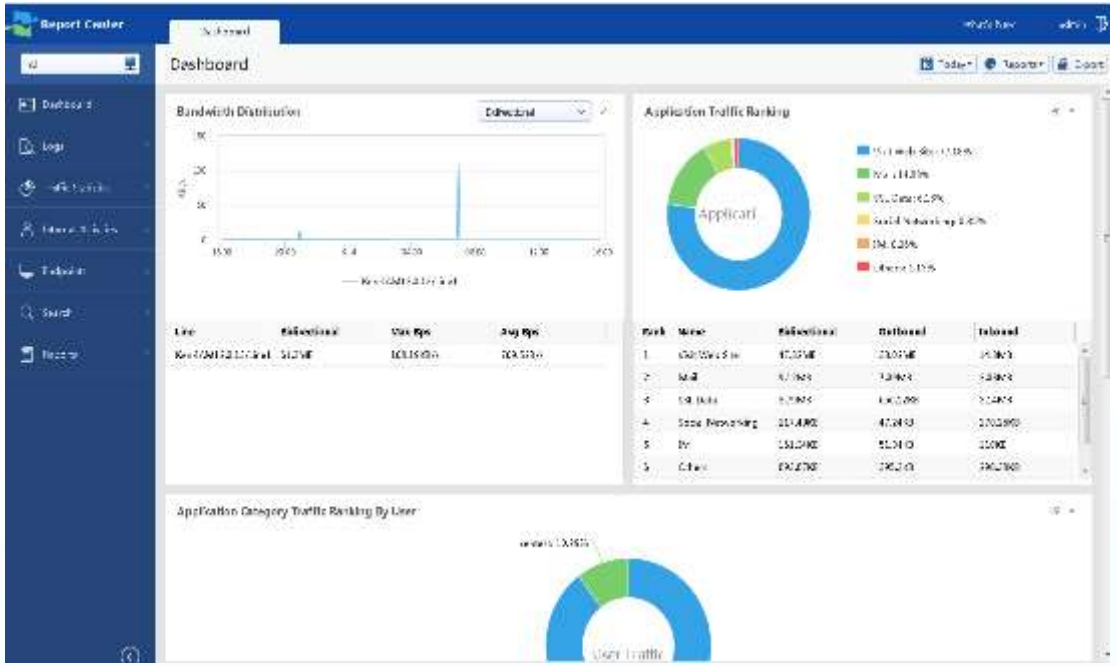
The original report center is presented as an application

Smooth setup of system settings, the same way of operation

Docking built-in IAG, with external deployment

BI system configuration is equivalent to DC system management



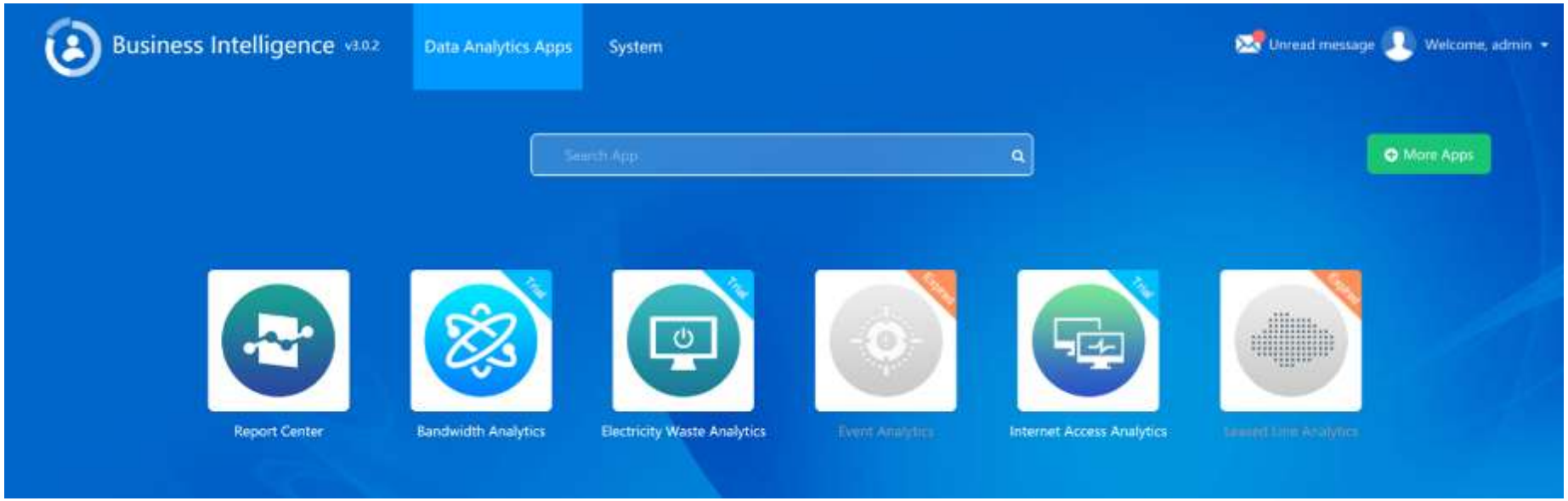


PART 4

Introduction to the Applications

Introduction to the Applications

The new applications are Event Analytics, Internet Access Analytics, Bandwidth Analytics, Leased line Analytics, Electricity Waste Analytics, as shown below:



Report Center

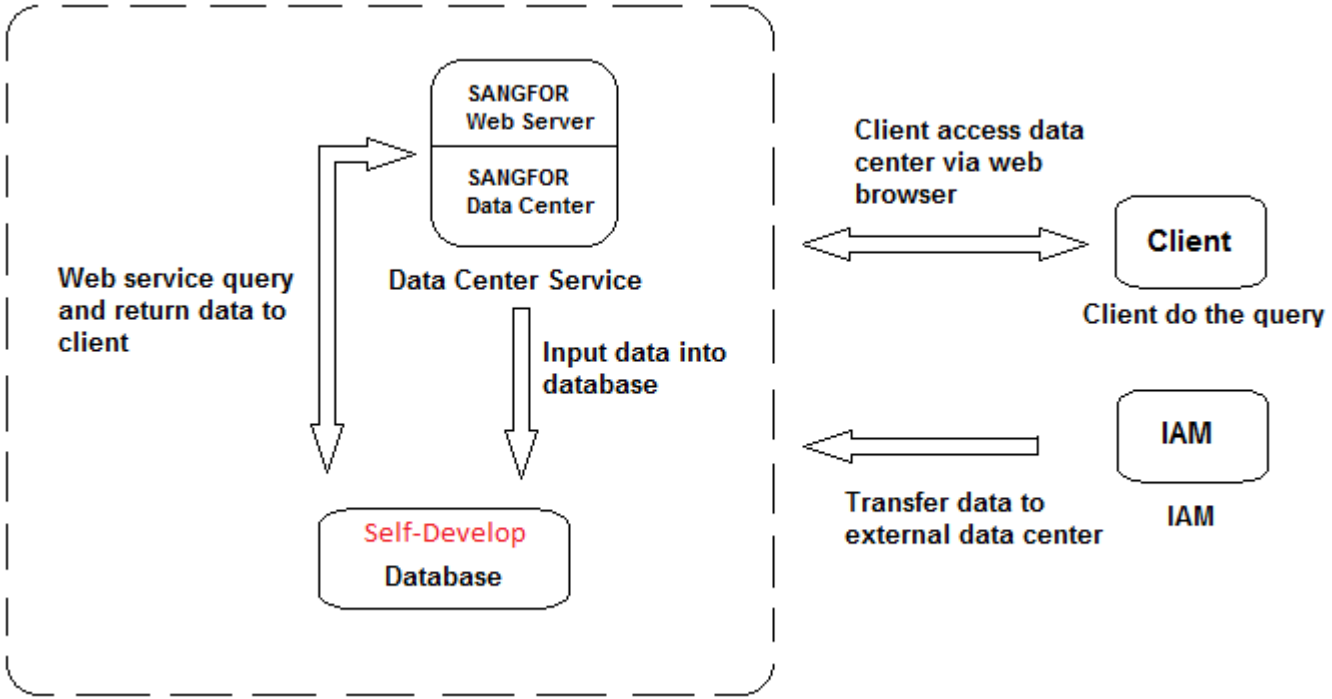
Report Center is used to record data and statistics of Internet users. Business Intelligence is divided into internal and external Business Intelligence, the device comes with built-in Business Intelligence, because storage space is limited, if customers want to save a lot of logs, we recommend installing an external Business Intelligence.

Business Intelligence will be accessing using port 443 which is "https" protocol.

Business Intelligence able to support other browsers other than IE, such as Firefox, Google chrome, and all other browsers that supporting osx by default.

Business Intelligence needs to be installed on a separate server, synchronize the log generated by the IAG, for customers do queries, export, and other operations.

Report Center



BI consists of below three items:
1. Data Center program: for data synchronization
2. Database programs: used to store data
3. WEB service: Query user data

When to use External Report Center?

1. User want to keep logs for long term, but Internal Report Center has limited storage.

2. External Report Center has attachment files indexing function, Internal Report Center does not have.

Report Center-User Requirement

Scenario Background

Customer requirement :

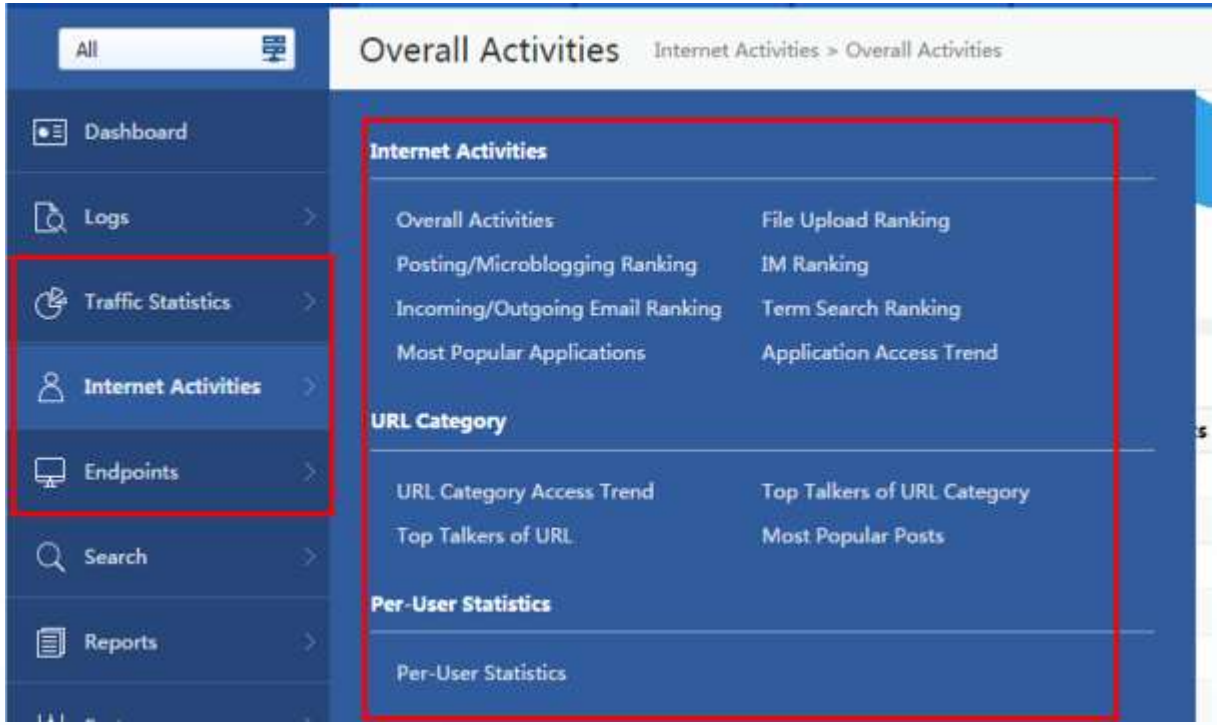
1. Audit IAG online behavior, including e-mail attachments.
2. Reporting statistics, through keyword search logs
3. The audit logs need to keep at least 60 days

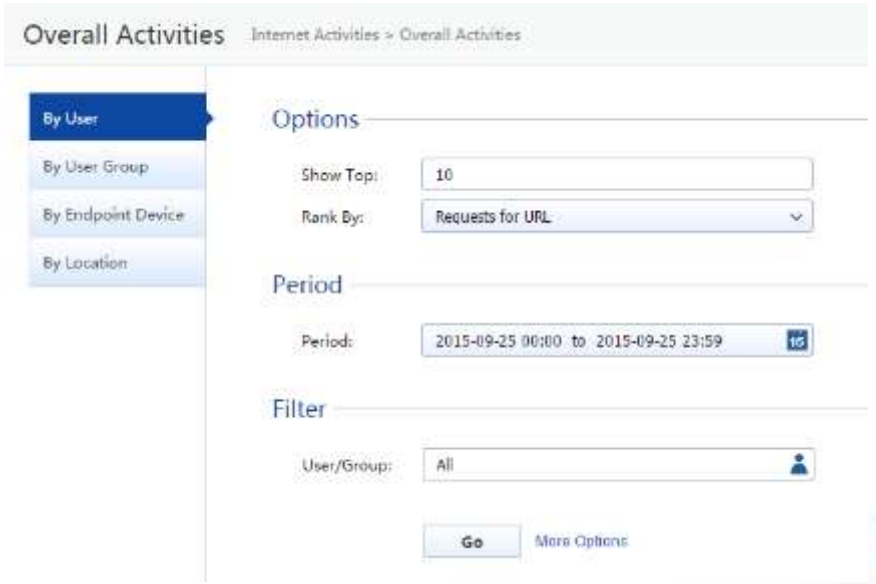
Requirement analysis :

From observation,1 day's log will consume 1.5GB for internal report center, thus it needs 90GB to save 60 days logs. But customer device only have 80GB, thus we need install external report center.

Report Center

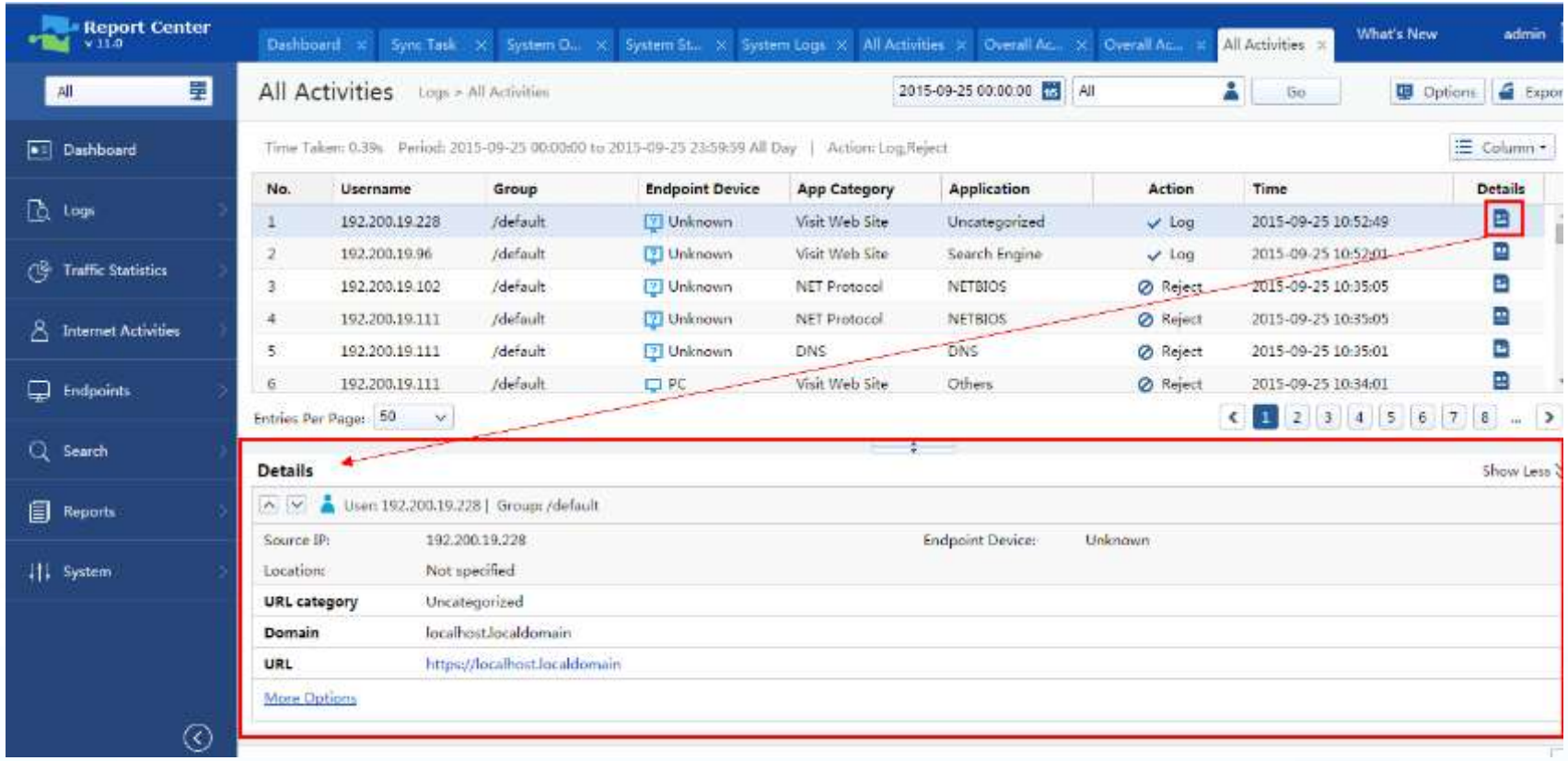
How to use external report center ?





Report Center

How to use external report center ?



Event Analytics

Usage scenarios

1. Infectious epidemiological analysis can avoid large-area infections, can be perceived in advance, and can be intervened in advance.
2. Analysis of vicious incidents, using the network to conduct personal attacks on others, such as personal attacks, such as the principal
3. More additional events, which can be analyzed with custom keyword phrases

Principle of implementation

It is suitable for analyzing whether a certain type of event occurs according to a specific keyword group, providing data analysis, showing the person who generates the network behavior of a specific keyword and its details, facilitating tracking of certain types of events and intervening related personnel, and preventing certain classes The occurrence of the event.

Event Analytics

Detailed configuration

1. Set the keyword phrase of the event
2. Through the analysis of access to the website, IM, mail, microblogging forums and other logs appear in the keyword phrase (remove interference)
3. Give the person who has the most access to the keyword phrase

Event Analytics

Description

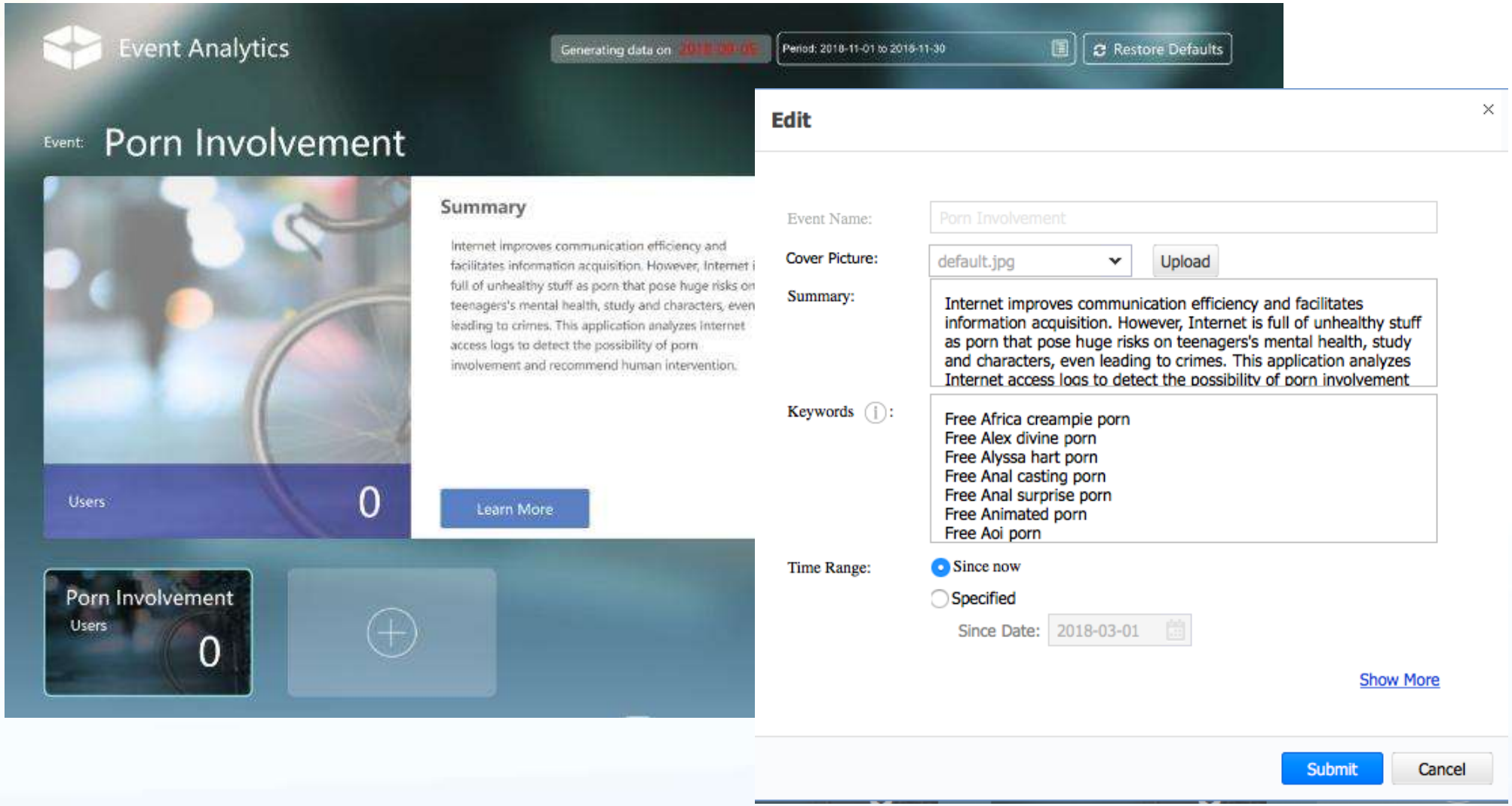
BI is a keyword-based versatile analysis template, more of which is reflected in the risk warning, the risk of the epidemic, and the risk of students participating in a vicious event. The instability caused by national emotions, etc., through the deployment of BI, can sense the risk in advance and achieve the purpose of early intervention and early processing. It is not only applied to colleges and universities, but other similar governments and enterprises must have similar needs.

Precautions:

1. An event-aware template is built into the system: Porn Involvement
2. A total of 30 events can be added
3. The event-aware app does not currently support report export

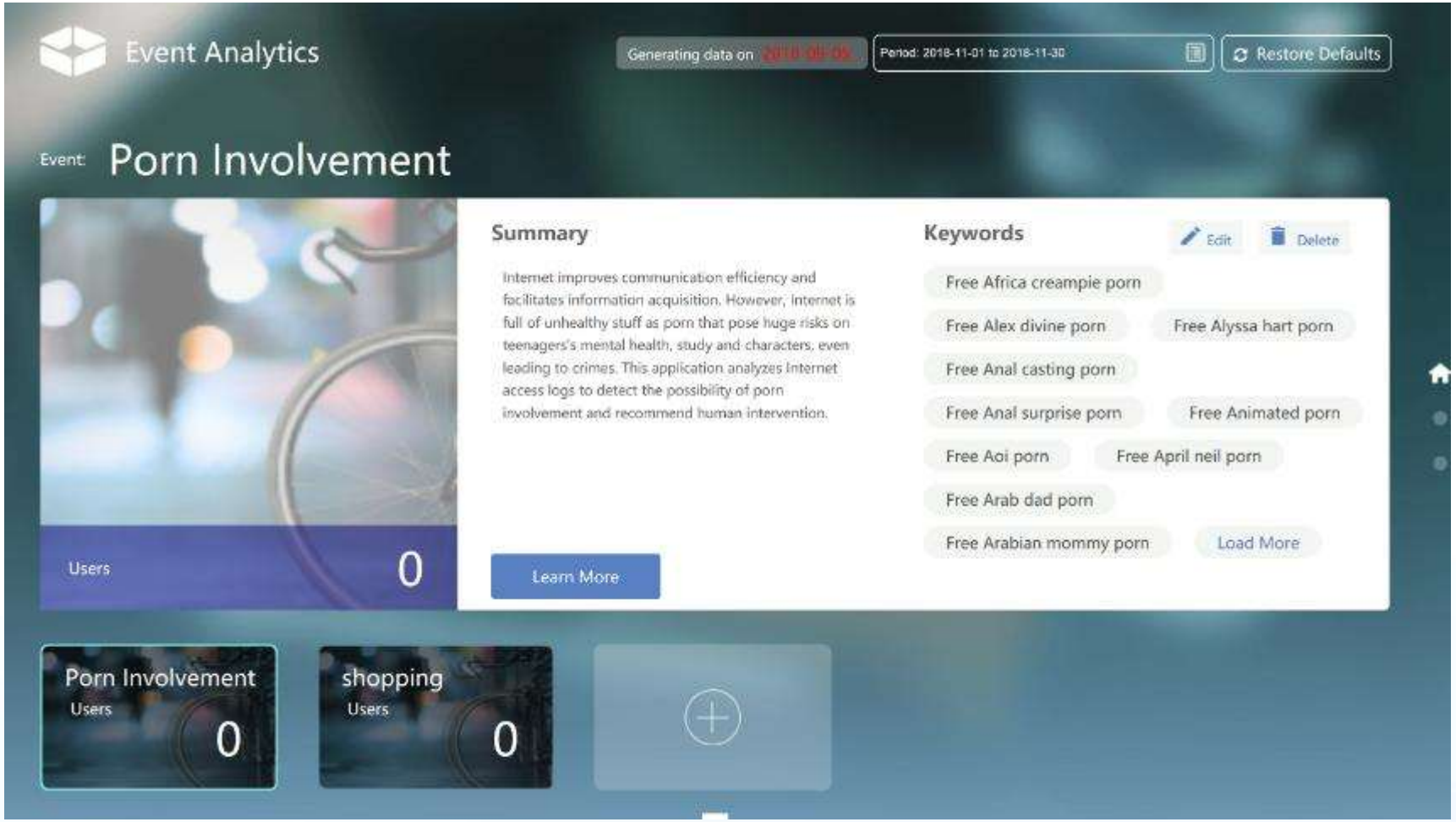
Event Analytics

Configuration is as follows



Event Analytics

Application effect is as follows



Internet Access Analytics

Background

1.The operation and maintenance personnel are expected to be able to intuitively grasp the traffic distribution of the intranet users online and whether the configuration compliance policy is effective; whether there are bad network behaviors; whether there is a security risk;
2.How to reflect the value of operation and maintenance personnel on the operation of equipment

Target customers:

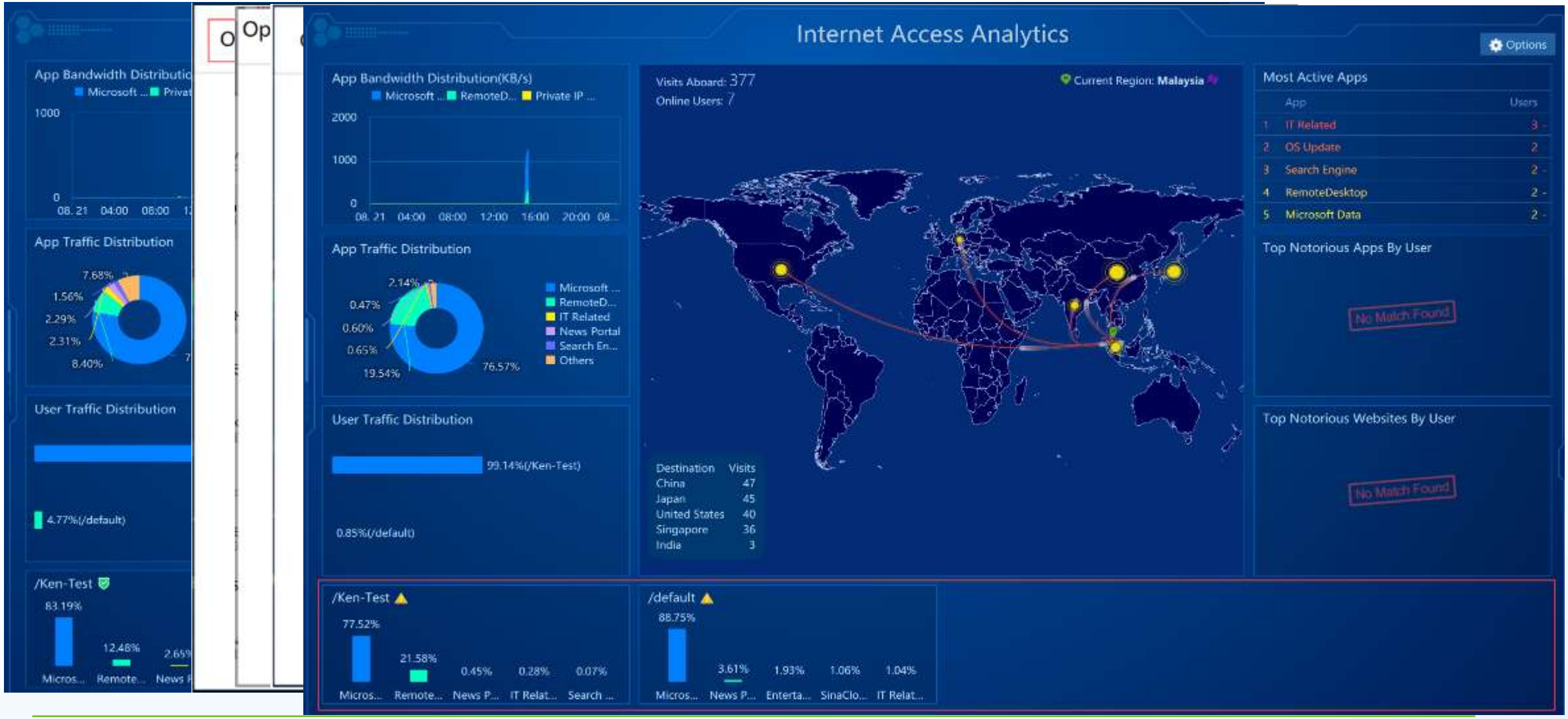
goverments, enterprises, colleges and universities, operators, etc

Value

1.Monitor the overall network traffic status, traffic distribution and Internet behavior status of each user.
2.Performance of work

Internet Access Analytics

Application effect is as follows



Bandwidth Analytics

Background

The operation and maintenance personnel cannot grasp the network bandwidth usage:
Want to know if the internal network bandwidth is sufficient, and what is the application of high bandwidth consumption?
Understand traffic usage from the app and user dimensions

Bandwidth Analytics

Target customers

Operation and maintenance personnel

Value

Operation and maintenance personnel grasp the utilization of equipment bandwidth:
Intuitive display of intranet bandwidth overload information, high bandwidth consumption applications
Rank traffic from the app and user dimensions

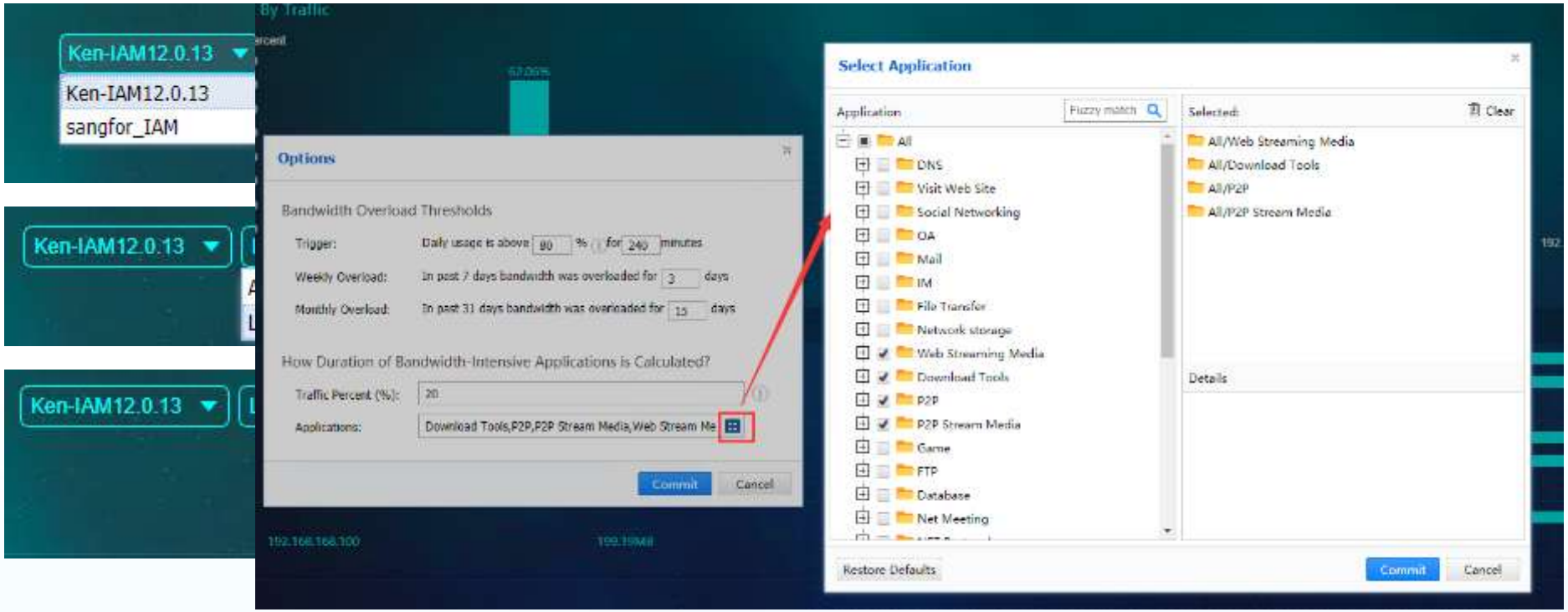
Principle of implementation

Collect IAG bandwidth usage data

Bandwidth Analytics

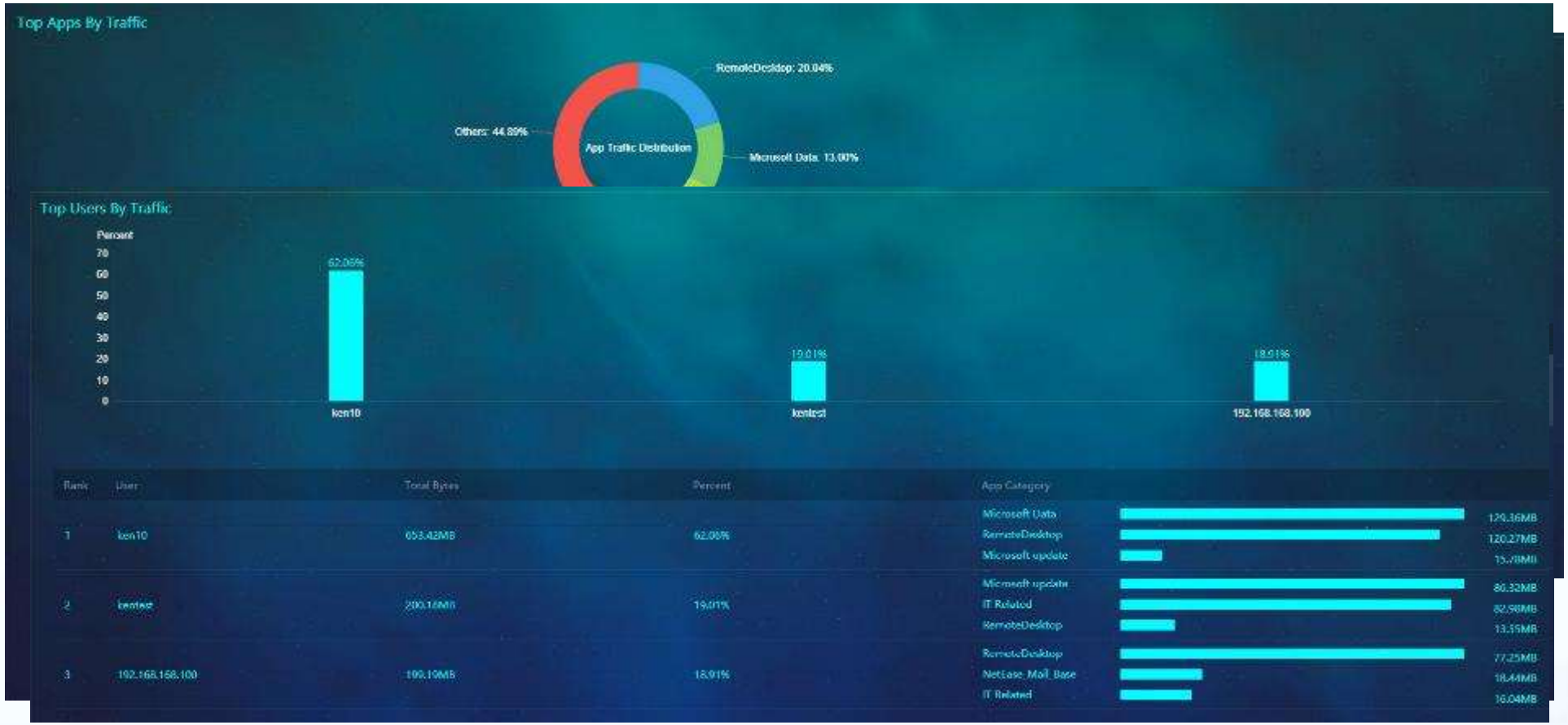
Instructions

After the branches are successfully connected to the BI, the bandwidth analysis application is analyzed for a single device.
When analyzing different branch devices, you need to [Reset] related configuration.



Bandwidth Analytics

Application effect



Leased Line Analytics

Background

The IT operation and maintenance personnel cannot evaluate whether the bandwidth of each leased line is sufficient and whether bandwidth needs to be increased.
The IT operation and maintenance personnel cannot evaluate whether the bandwidth usage of each dedicated line is reasonable, and whether the bandwidth of the service application bandwidth is good enough.

Leased Line Analytics

Target customers
Customers with multiple leased lines

Value
Evaluate whether each leased line bandwidth is sufficient and whether it needs to increase bandwidth
Evaluate whether the bandwidth usage of each leased line is reasonable
Evaluate the bandwidth quality of each leased line service application

Principle of implementation
Analyze the real-time traffic of the leased line and evaluate the duration of the load above the upper and lower limits
At the same time, it is analyzed by what application the dedicated line is occupied by which users.

Leased Line Analytics

Scenes to be used

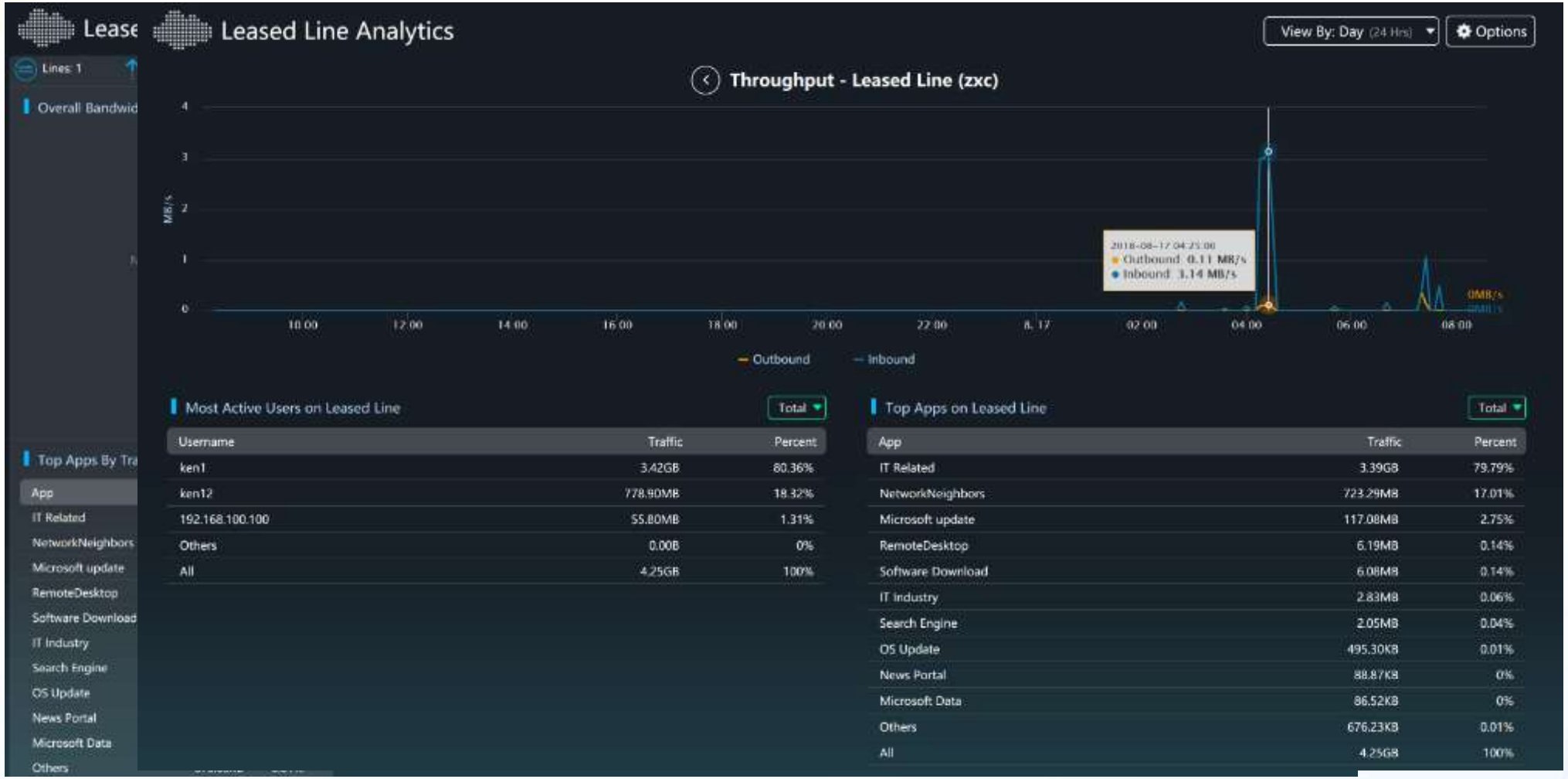
There are multiple lines in the customer environment

Leased line traffic through IAG device

The leased line traffic does not pass through the IAG device, but the traffic can be mirrored to the IAG device.

Leased line Analytics

Application effect



Electricity Waste Analytics

Background

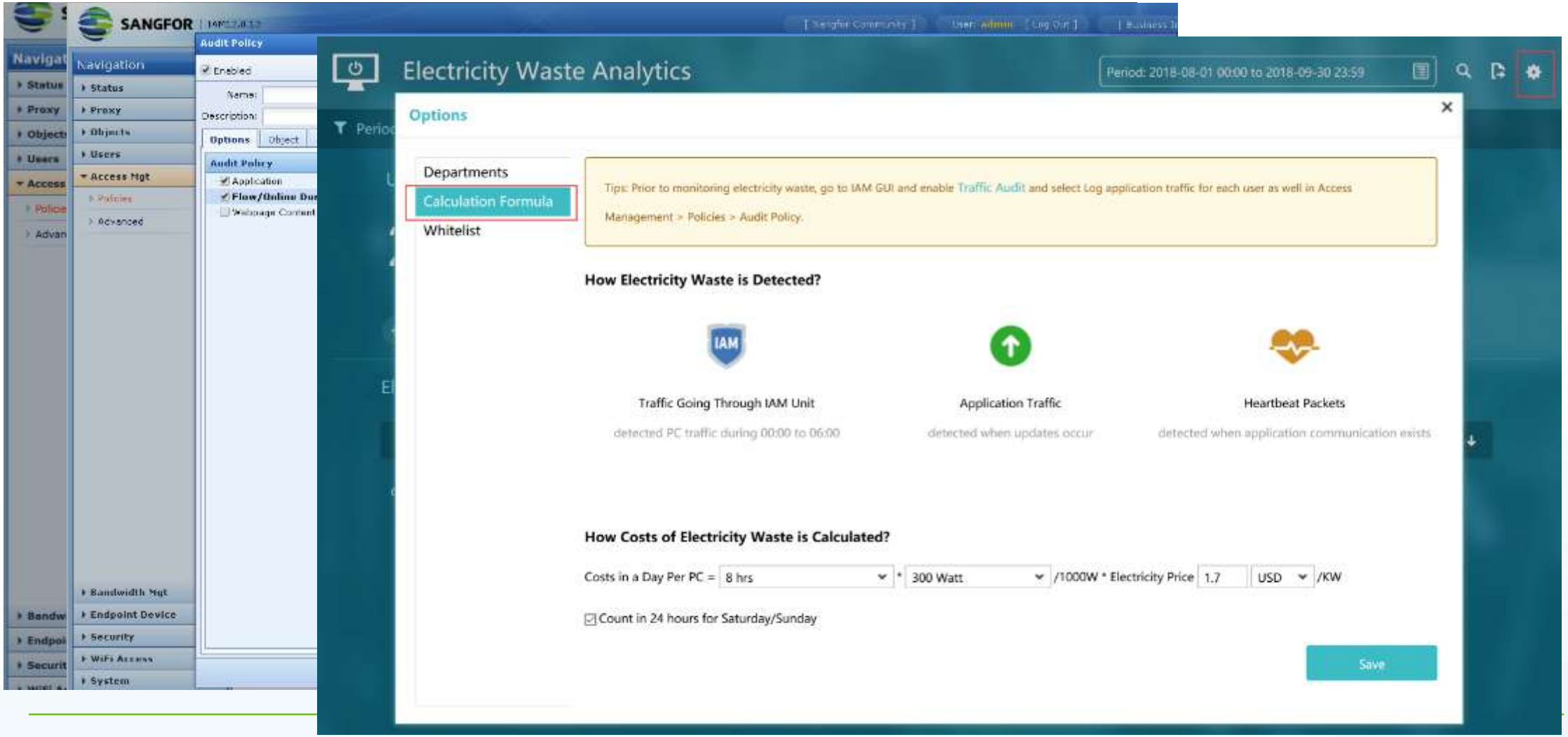
With the popularization of electronic office development and the improvement of office efficiency, some employees' bad work habits have caused waste of resources. By analyzing the online behavior of employees, they identify users who have not shut down and provide reference data for enterprises. Used to internalize internal resources

Value

Through the Office PC Electricity Waste, you can know how many people in the internal network do not have the habit of shutting down after work, so the wasted resources can also be known, providing a visual reference to the unit.

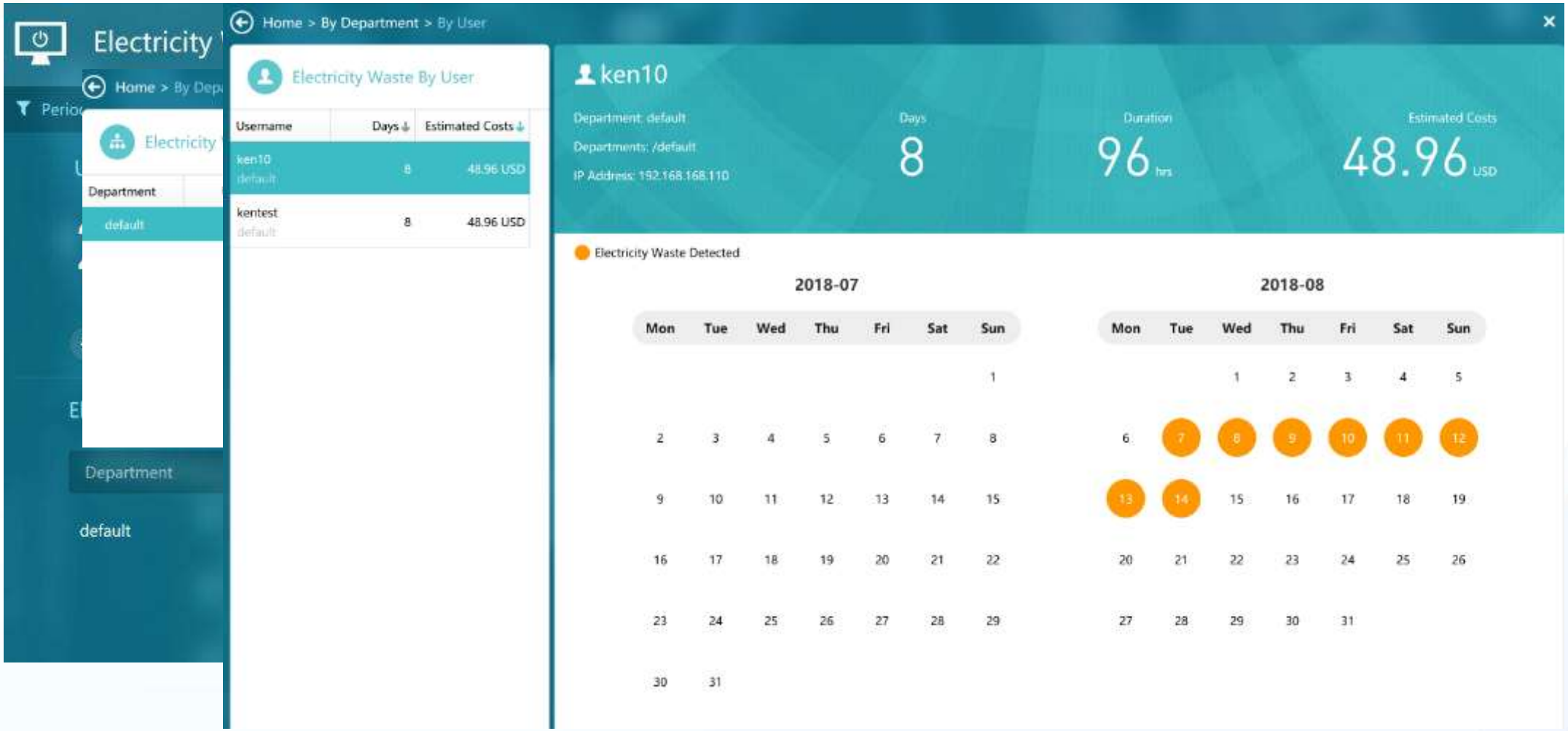
Electricity Waste Analytics

1. Online audit policy configuration Application and Flow/Online Duration audit
2. Do not shut down the definition, confirm the analysis department



Electricity Waste Analytics

Application effect



PART 5

Upgrade, Authorize, Admin Account

Upgrade

The BI software upgrade principle after Report Center 11.0

Authorization

- Currently only supports testing
- Authorization for official purchase has not been provided yet
- Temporary authorization time for paid apps is 180 days

Admin account

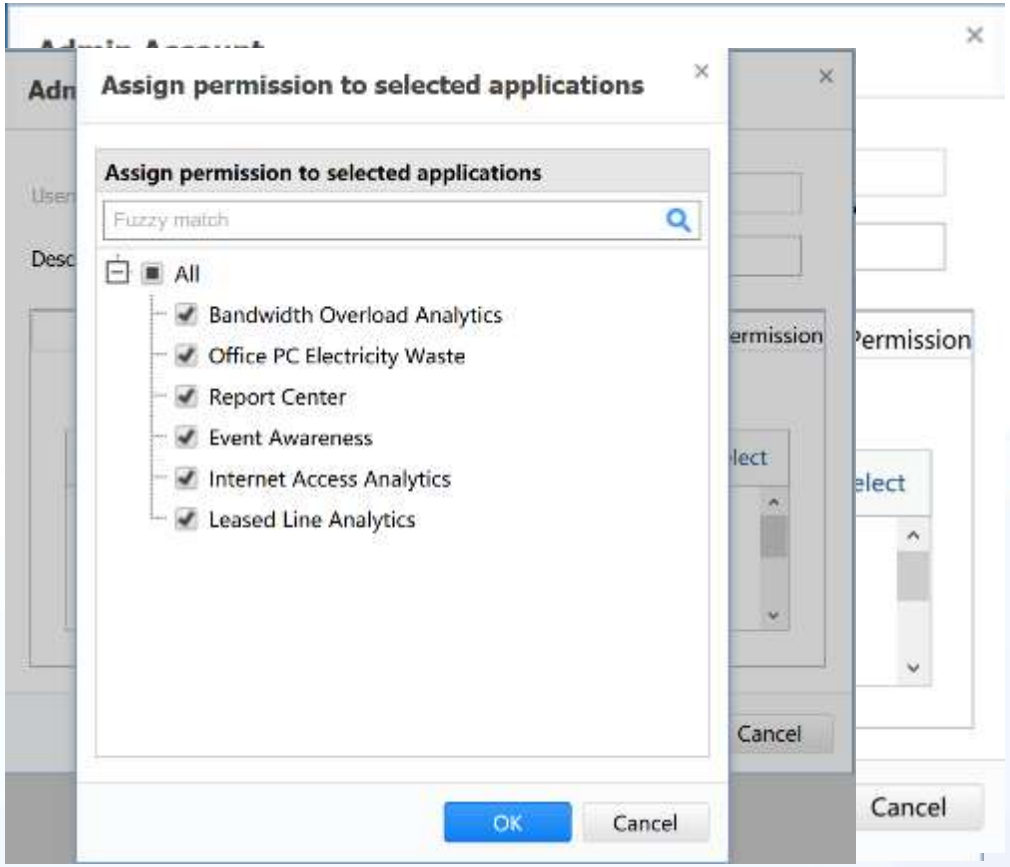
Auditing and querying user network behavior is likely to infringe on the right to freedom of communication and privacy. In this case, the corresponding authorization management is involved:

Permission
Only check the Search for logs, only the log center app permissions, you can only view the Home, Log Query, report center, all other apps are hidden

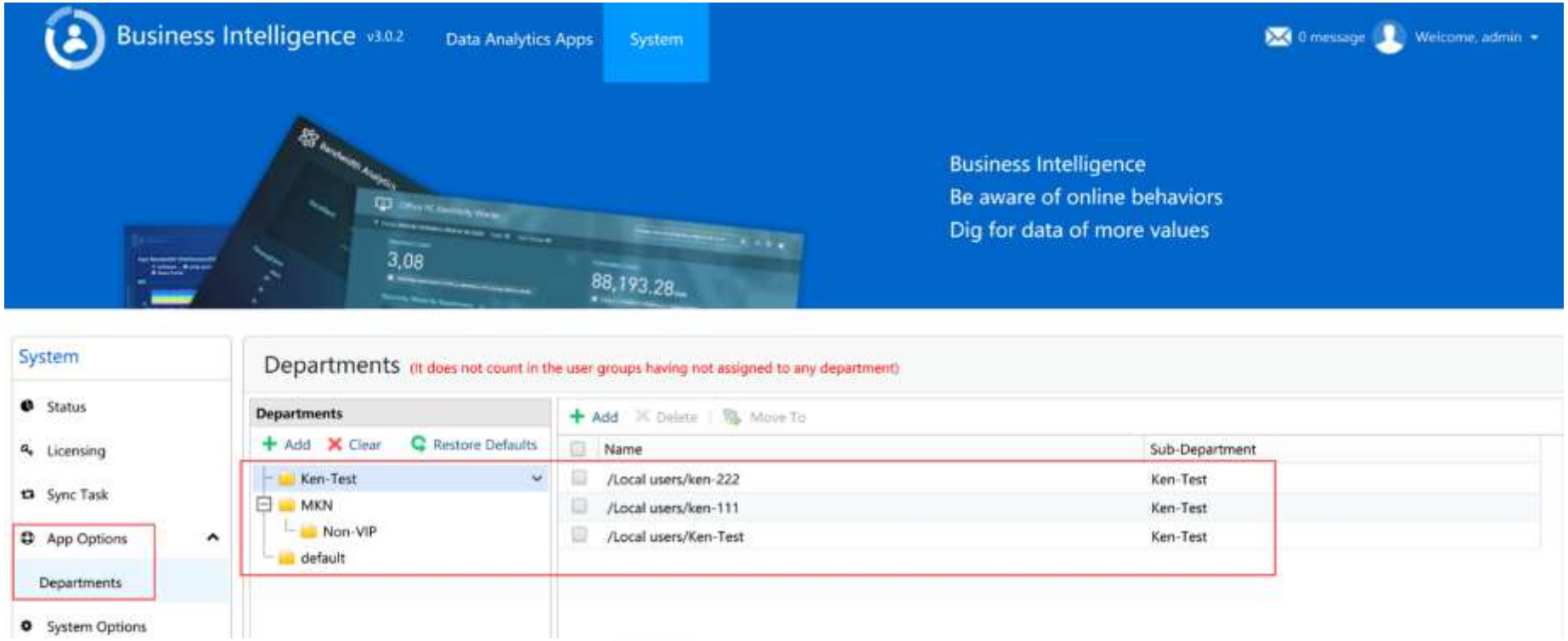
Only check Make statistics and reports, the app has permission to access, and the log center hides Log Query and report center

Hide System without checking System

APP Permission
Assign permission to selected applications



App Options


Business Intelligence v3.0.2
Data Analytics Apps
System
0 message
Welcome, admin
Business Intelligence
Be aware of online behaviors
Dig for data of more values
System
Status
Licensing
Sync Task
App Options
Departments
System Options
Departments (It does not count in the user groups having not assigned to any department)
Departments
Add
Clear
Restore Defaults
Ken-Test
MKN
Non-VIP
default
Add
Delete
Move To
Name
Sub-Department
/Local users/ken-222
Ken-Test
/Local users/ken-111
Ken-Test
/Local users/Ken-Test
Ken-Test

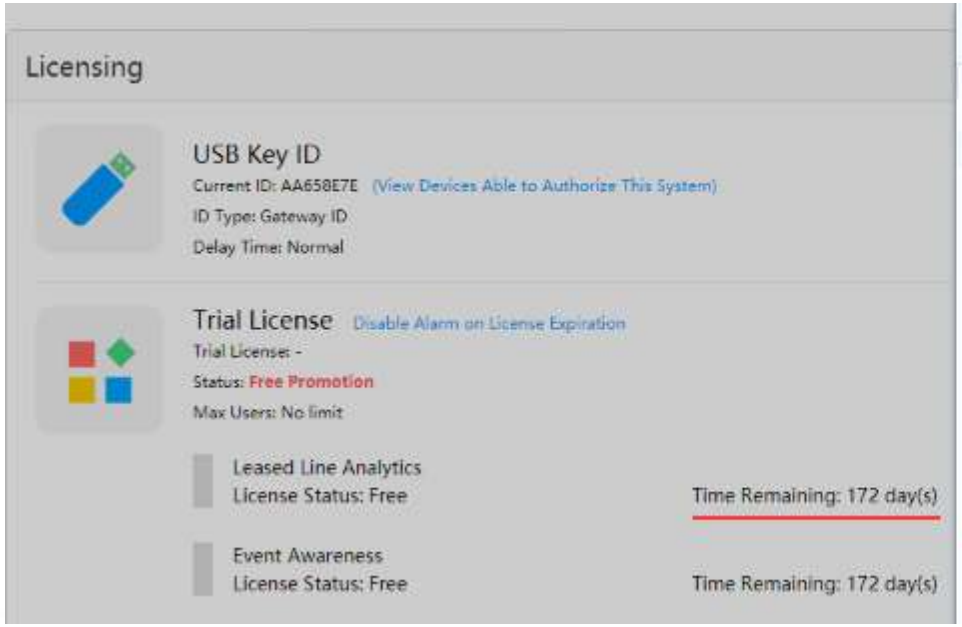
Application update

1.BI realizes networking and uses IAG as a springboard to access the network.
2.Get technical support expiration date and app update are all done through IAG
3.Get the technical support expiration date and app update is synchronized to the BI through the synchronization function to achieve the update (port 810)

Precautions:
1. BI and IAG devices are connected, and you need to release the TCP 810 port
2. When BI uses a bandwidth analysis application to connect to a multi-branch IAG device, you need to release the TCP 801 port

Licensing Scheme

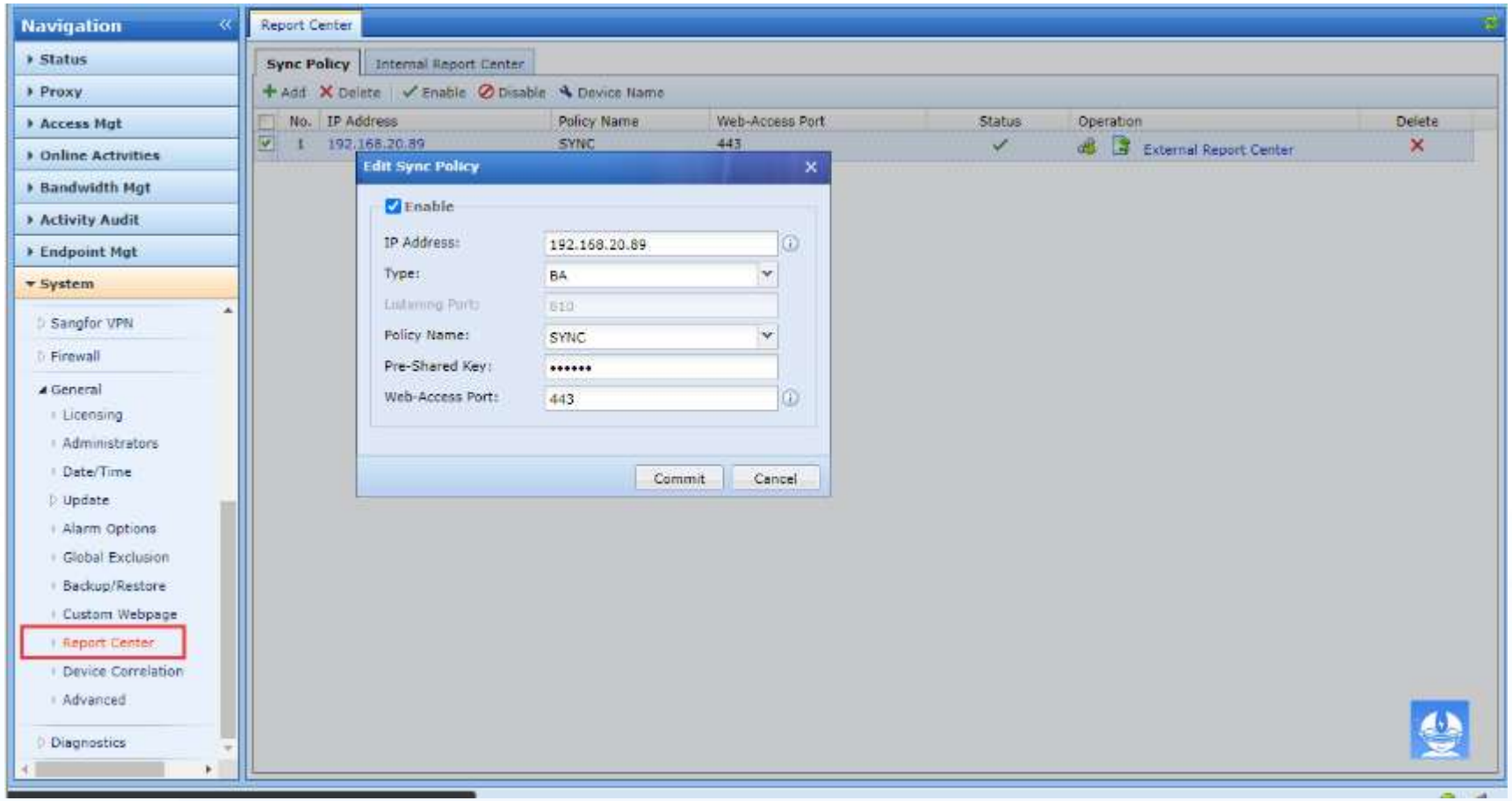
All application-paid applications can be used by simply giving the IAG device an application license. Go to System > Licensing, as the shown bellow:



PART 6 Sync Logs

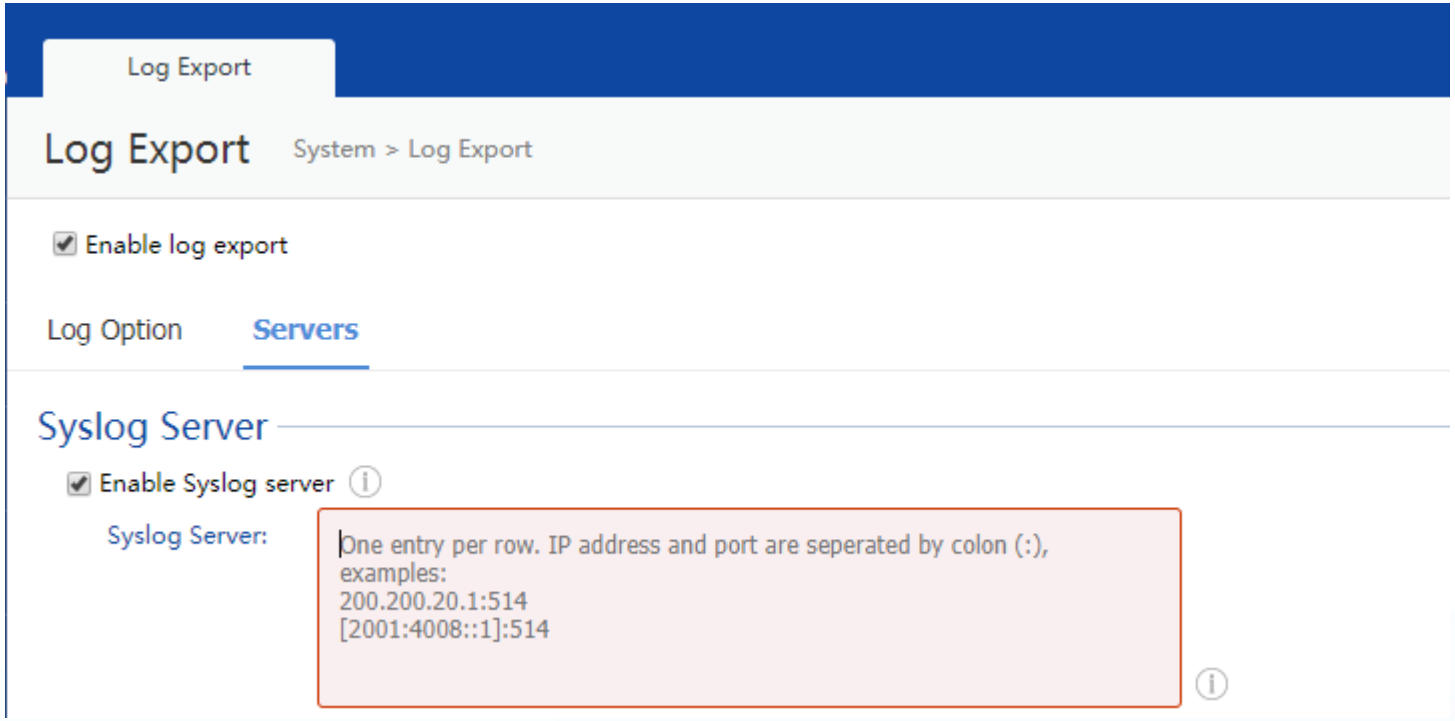
Synchronize logs to external BI

IAG has limited storage space. It is usually recommended to synchronize logs to external BI. External BI can expand storage space as needed and reduce the load on the IAG device itself.



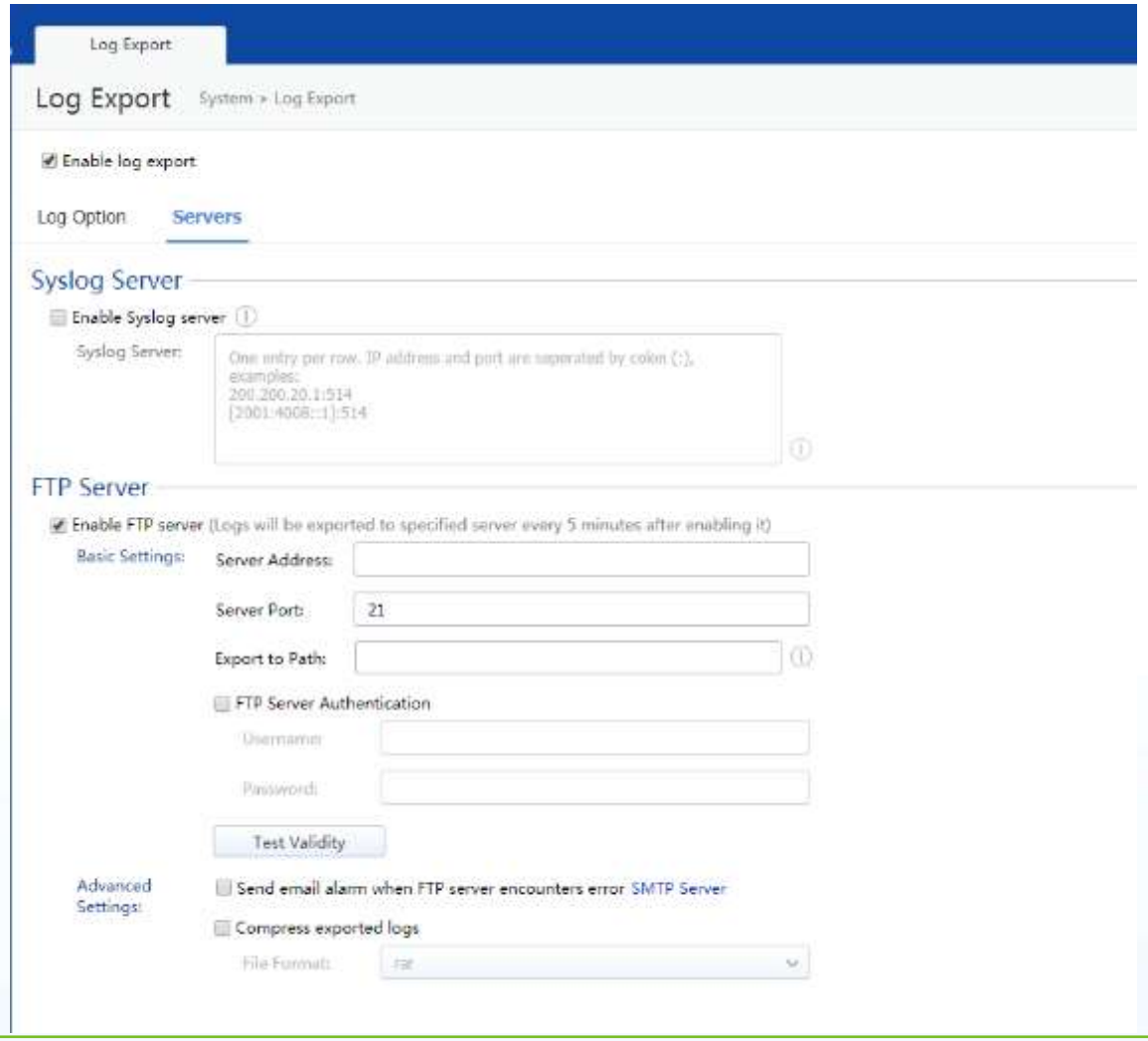
Synchronize logs to Syslog Server

Support importing logs to syslog server. Note: IAM12.0.27 and BI3.0.8 and newer versions support this feature.



Synchronize Logs to FTP Server

Support importing logs to FTP server. Note: IAM12.0.27 and BI3.0.8 and newer versions support this feature.



Question

1. What kinds of application analysis are included in BI?
2. Which two application analysis requires activation licensing?

THANK YOU

Technical Support Service

Email: tech.support@sangfor.com

Community: community.sangfor.com