



SANGFOR

11 Business Intelligence

IAG 13.0.80 - Associate





- 1 BI Product Introduction
- 2 Composition and Implementation of BI
- 3 Compare the Original Datacenter
- 4 Introduction to the Applications
- 5 Upgrade, Authorize, Admin Account
- 6 Sync Logs

PART 1

BI Product Introduction

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.

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:

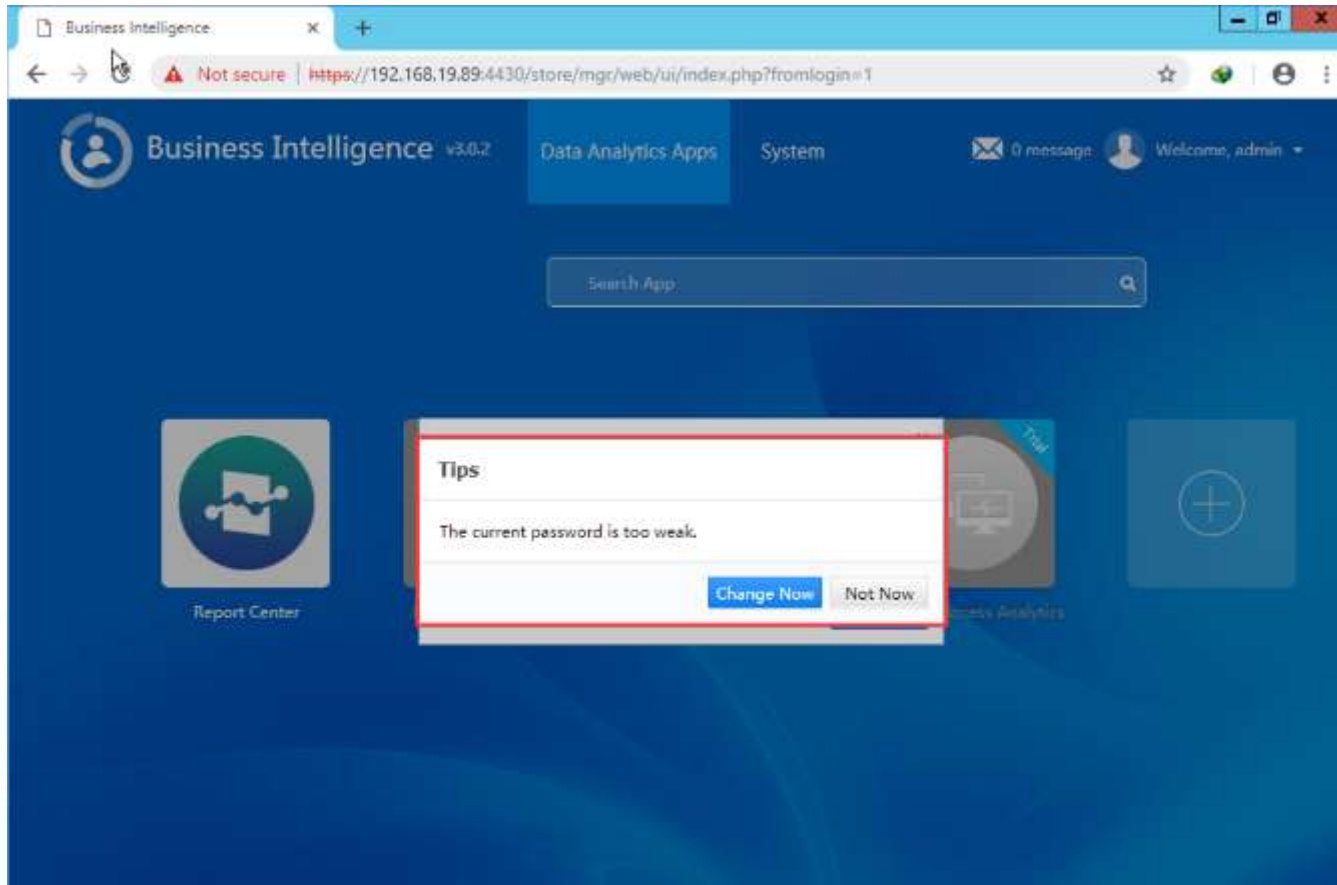


SANGFOR_IAM_V12.0.13_BI Installation and Update Configuration Steps.pdf

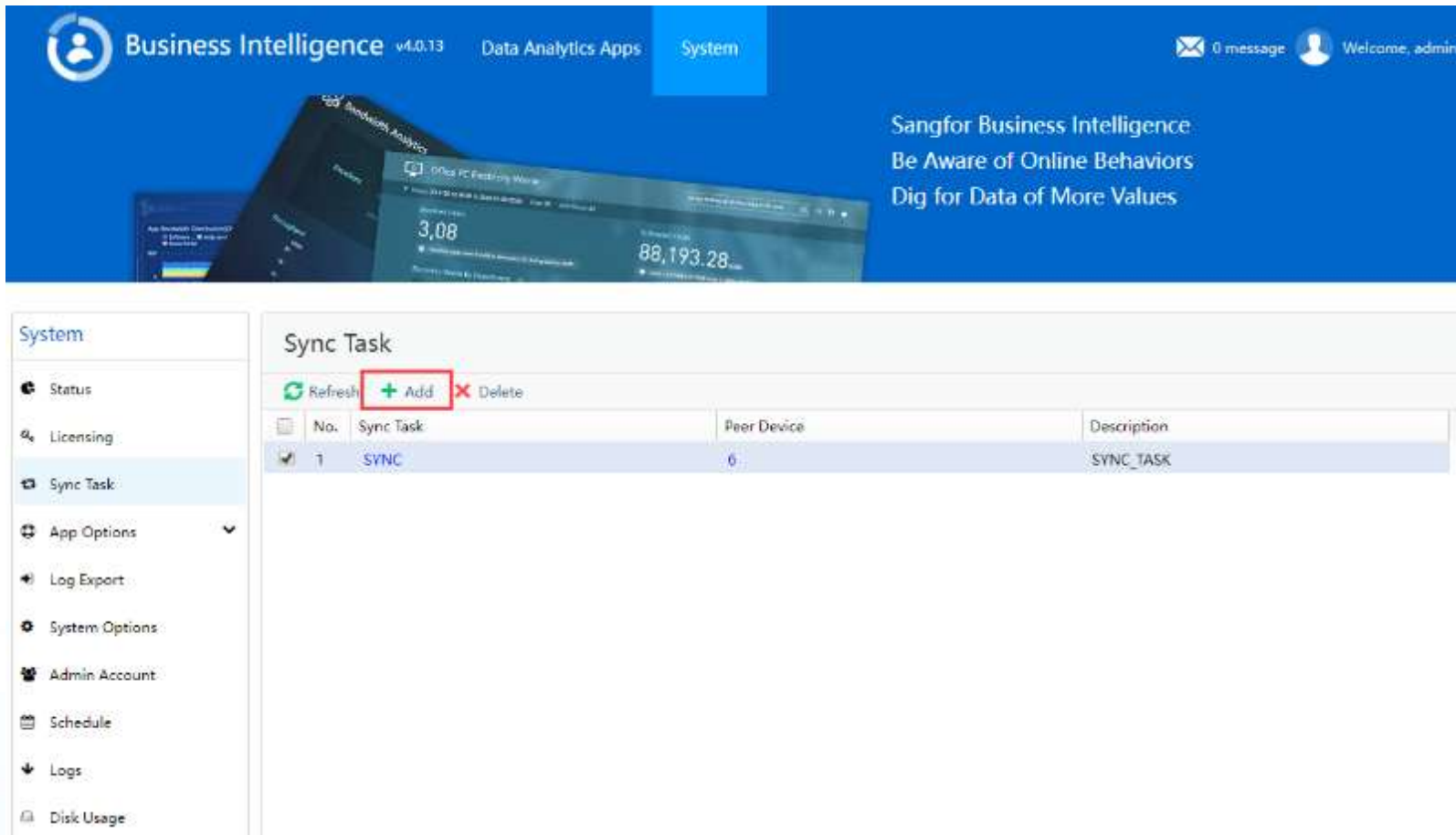
Installation



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



3.Go to System > Sync Task.



The screenshot shows the Sangfor Business Intelligence v4.0.13 interface. The top navigation bar includes 'Business Intelligence v4.0.13', 'Data Analytics Apps', and 'System'. The 'System' tab is active. The main header area displays 'Sangfor Business Intelligence Be Aware of Online Behaviors Dig for Data of More Values' along with a message icon and a welcome message for 'admin'.

The left sidebar contains the following menu items: Status, Licensing, Sync Task (highlighted), App Options, Log Export, System Options, Admin Account, Schedule, Logs, and Disk Usage.

The main content area is titled 'Sync Task' and features a table with the following structure:

No.	Sync Task	Peer Device	Description
1	SYNC	6	SYNC_TASK

At the top of the table, there are three buttons: 'Refresh' (green circular arrow), '+ Add' (highlighted with a red box), and 'Delete' (red X).

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.

Add Sync Task

Sync Task

Name:

SYNC

Password:

.....

Retype PWD:

.....

Description:

SYND

Sync Options

More...

Sync logs generated since

2021-08-22

Select Logs:

☒ All

☒ Activities

- ☒ Website Browsing
- ☒ File Upload ⓘ
- ☒ IM Chats
- ☒ Application

☒ Duration

- ☒ Traffic
- ☒ Online Duration

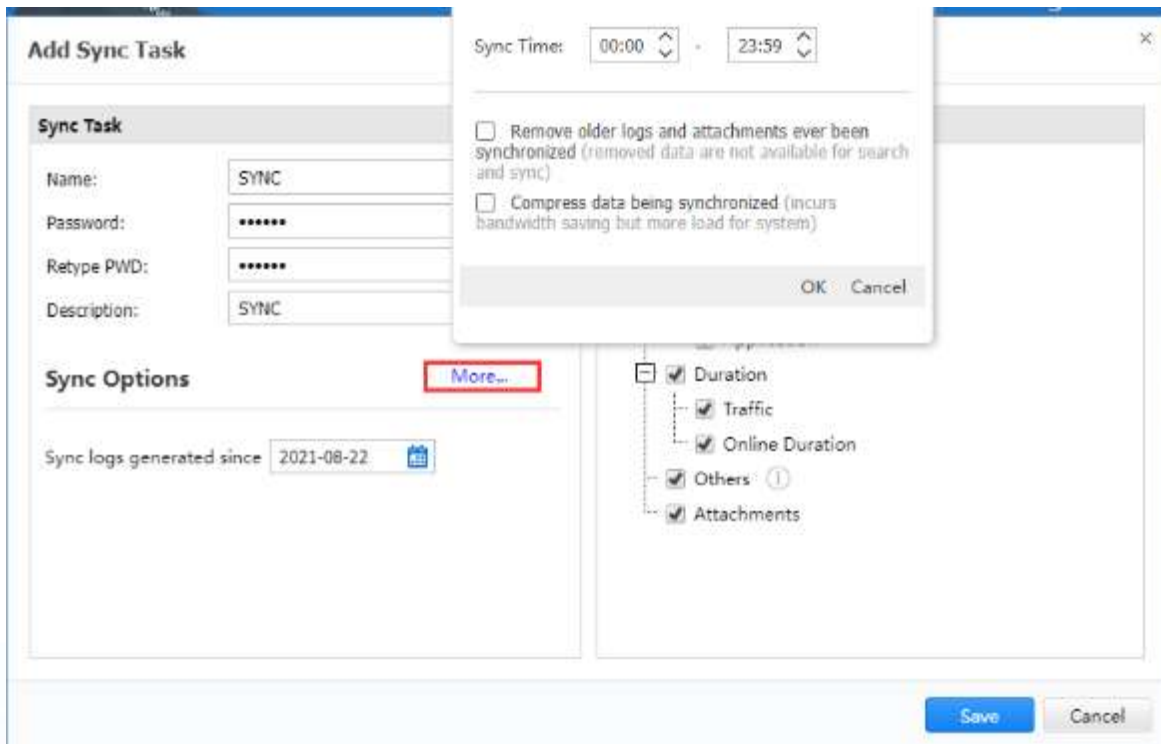
☒ Others ⓘ

☒ Attachments

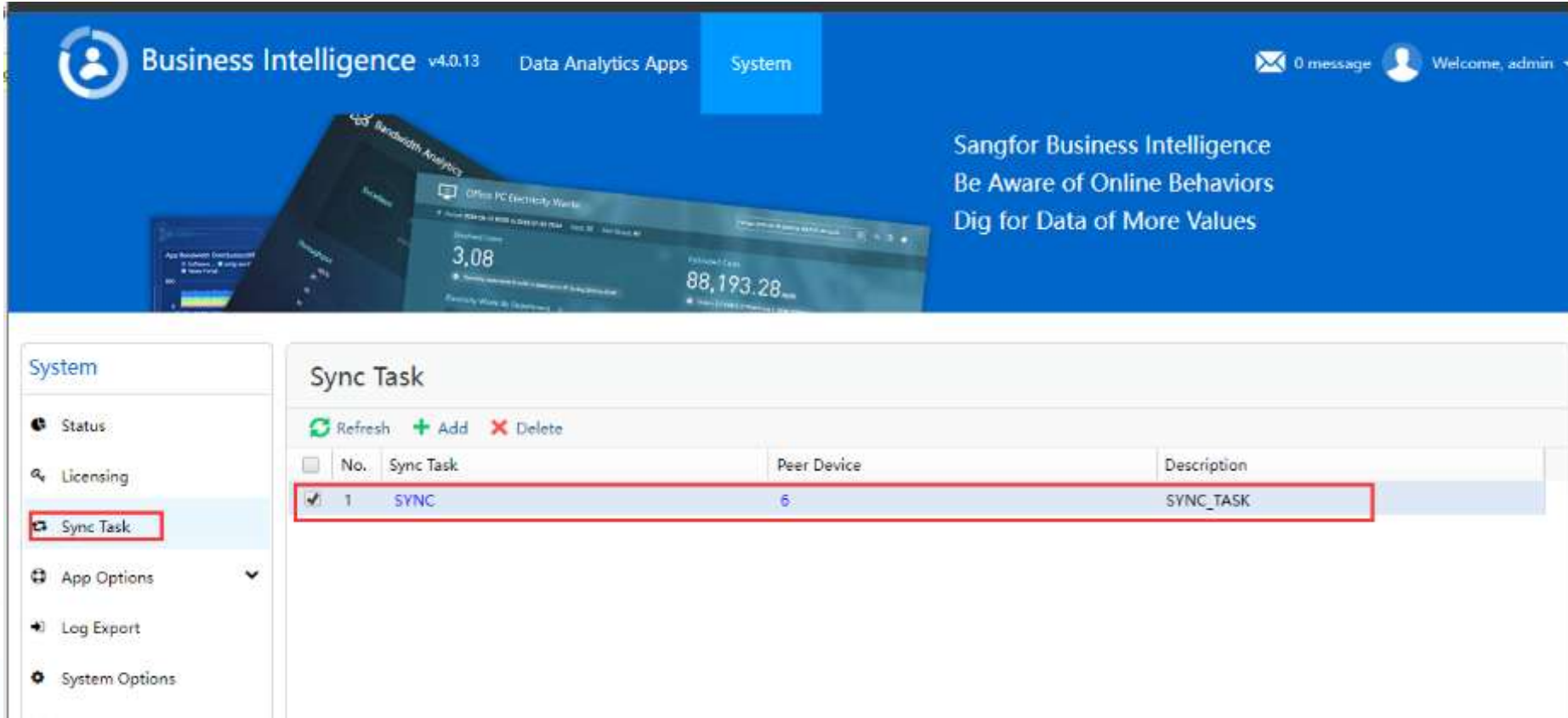
Save

Cancel

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.



3. The sync policy is now created.



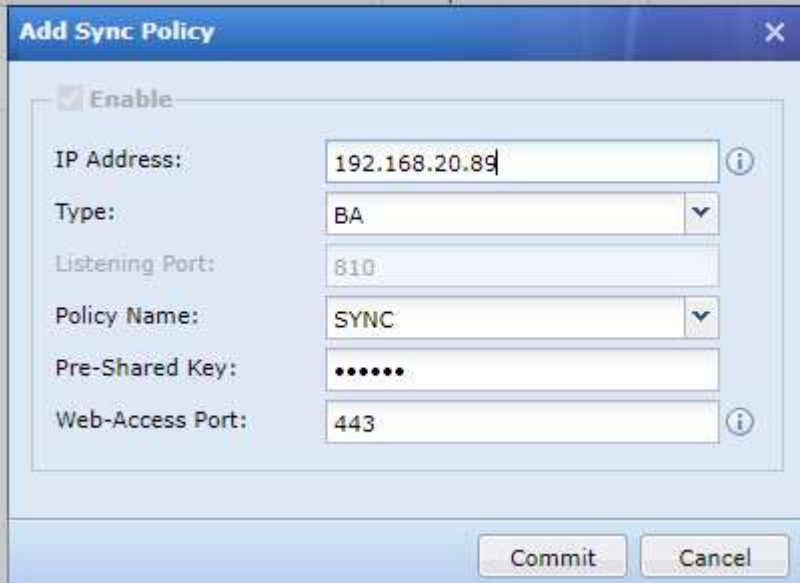
The screenshot shows the Sangfor Business Intelligence v4.0.13 System page. The left sidebar contains the following menu items: Status, Licensing, Sync Task (highlighted with a red box), App Options, Log Export, and System Options. The main content area is titled "Sync Task" and includes a table with the following data:

No.	Sync Task	Peer Device	Description
1	SYNC	6	SYNC_TASK

The table is highlighted with a red border. The top of the page features a blue header with the Sangfor Business Intelligence logo, version information, and navigation links. The right side of the header includes a message icon and a user profile dropdown.

4. Configuration on IAG

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

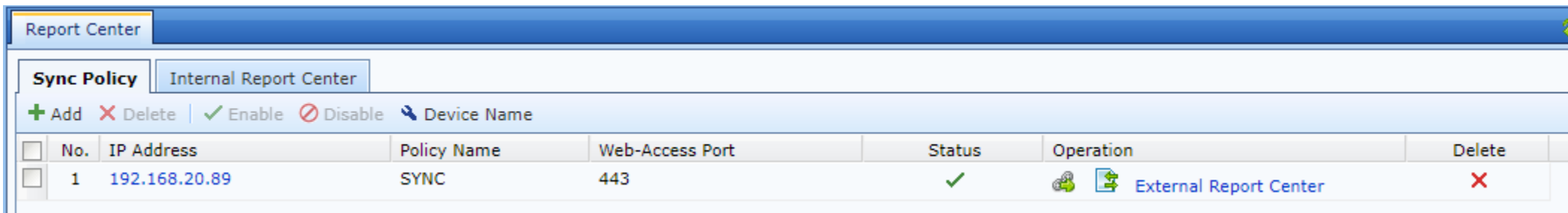


The image shows a screenshot of the 'Add Sync Policy' dialog box in the IAG WebUI. The dialog has a title bar with 'Add Sync Policy' and a close button. Inside, there is a checkbox labeled 'Enable' which is checked. Below this, there are several input fields: 'IP Address' with the value '192.168.20.89', 'Type' with a dropdown menu showing 'BA', 'Listening Port' with the value '810', 'Policy Name' with a dropdown menu showing 'SYNC', 'Pre-Shared Key' with a masked field of seven dots, and 'Web-Access Port' with the value '443'. Information icons (i) are present next to the IP Address and Web-Access Port fields. At the bottom of the dialog are two buttons: 'Commit' and 'Cancel'.

Enable	☒
IP Address:	192.168.20.89
Type:	BA
Listening Port:	810
Policy Name:	SYNC
Pre-Shared Key:	•••••••
Web-Access Port:	443

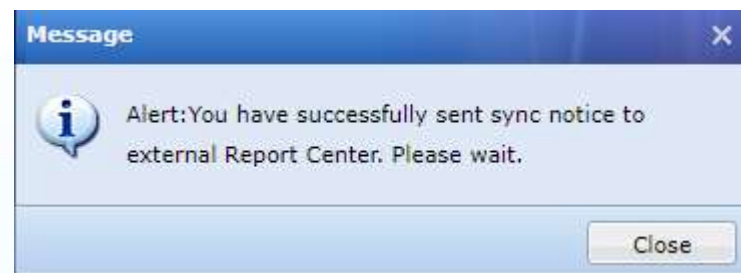
Commit Cancel

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



The screenshot shows the 'Report Center' window with the 'Sync Policy' tab selected. Below the tab are buttons for '+ Add', 'X Delete', '✓ Enable', '✗ Disable', and a search icon for 'Device Name'. A table lists the sync policies.

No.	IP Address	Policy Name	Web-Access Port	Status	Operation	Delete
1	192.168.20.89	SYNC	443	✓	 External Report Center	✗

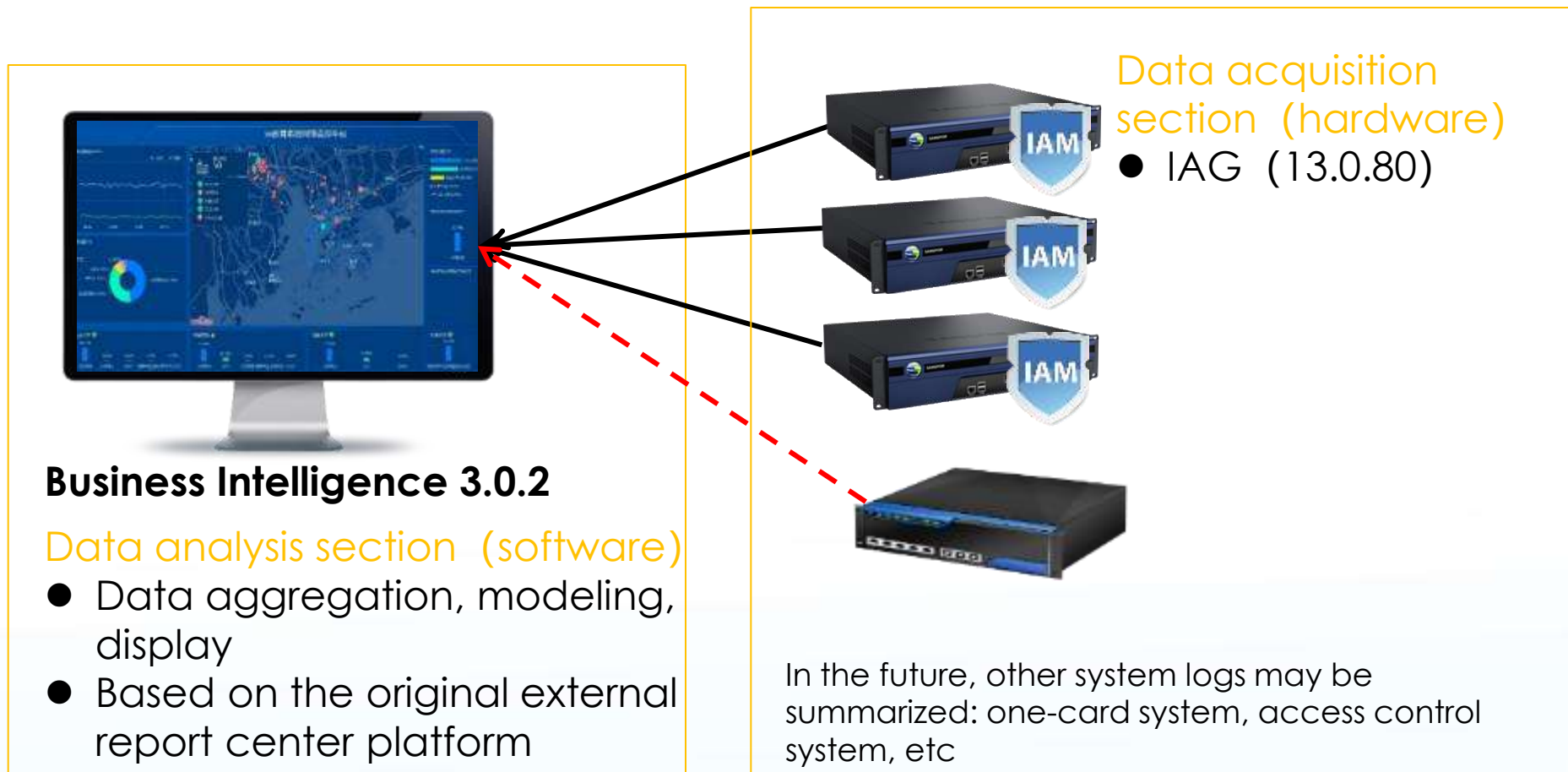


4. Now you can check the Peer Device number will become 1 which means one device connected with this Business Intelligence.

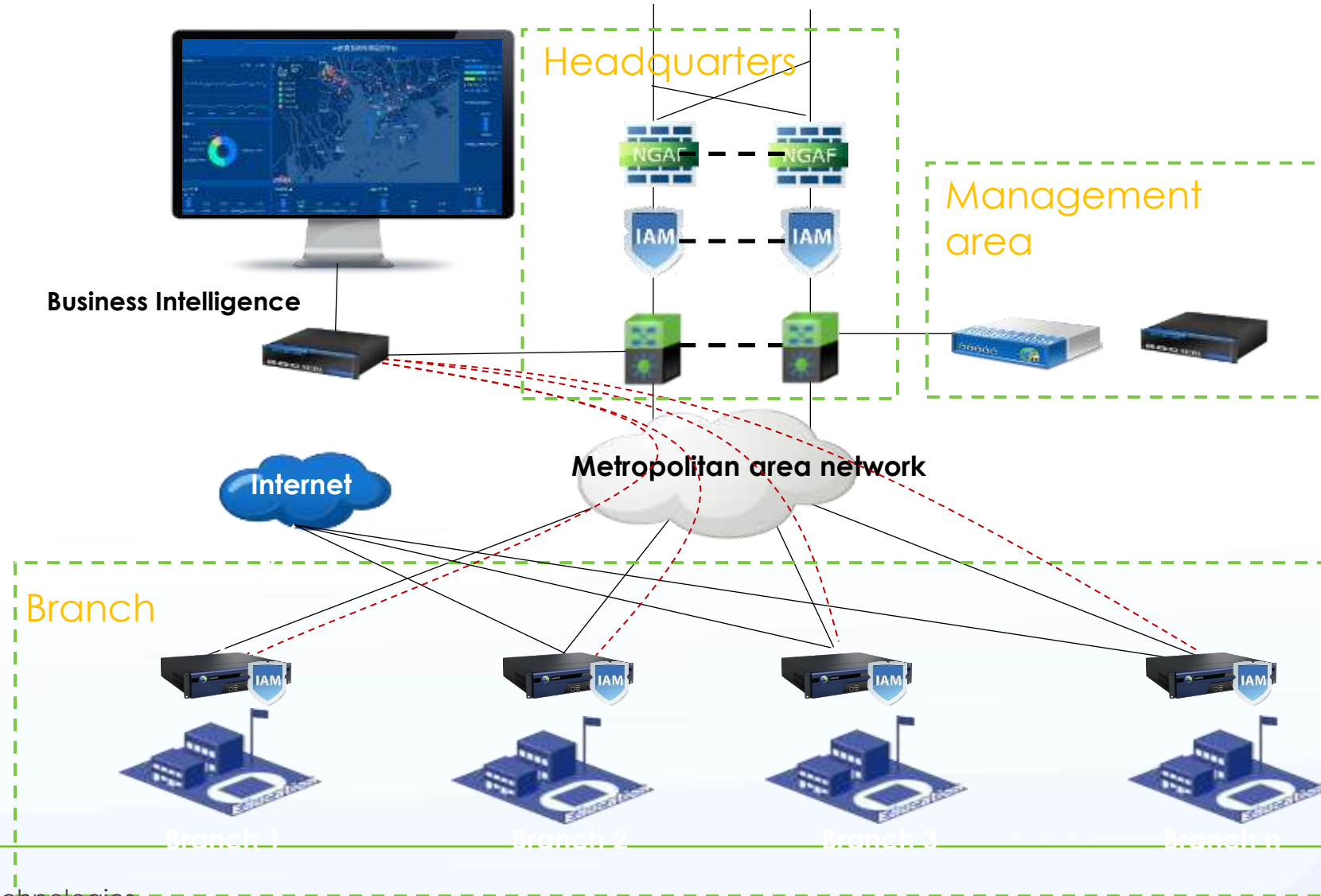
System		Sync Task			
Status		Refresh Add Delete			
Licensing					
Sync Task					
		No.	Sync Task	Peer Device	Description
		1	SYNC	6	SYNC_TASK

PART 2

Composition and Implementation of BI



Implementation of BI



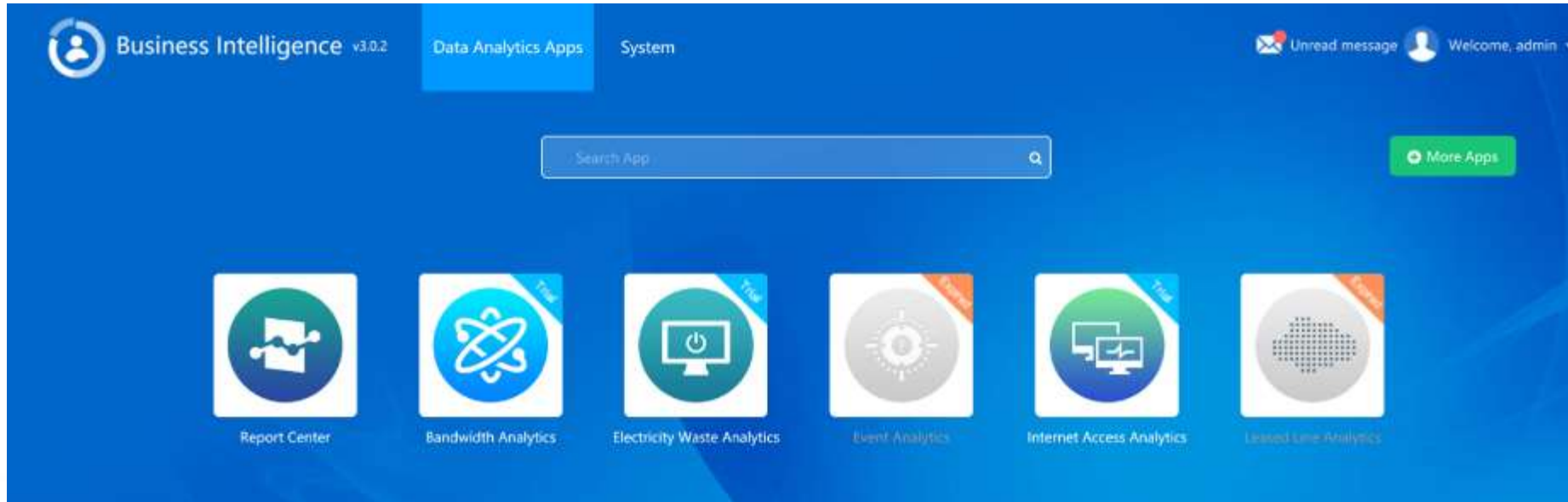
PART 3

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.

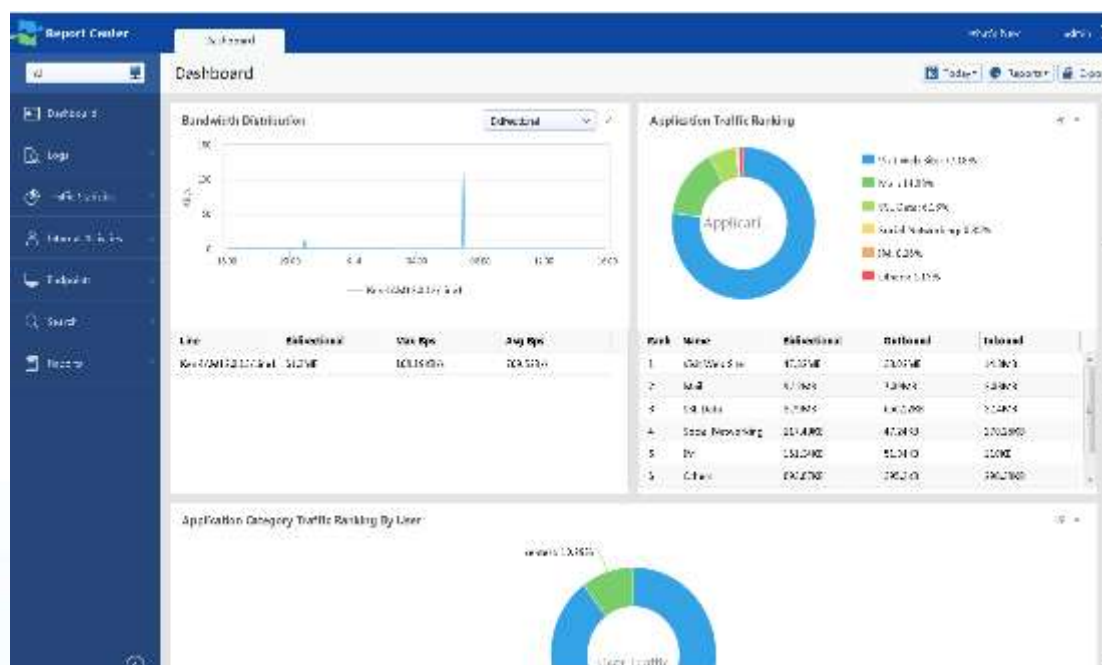
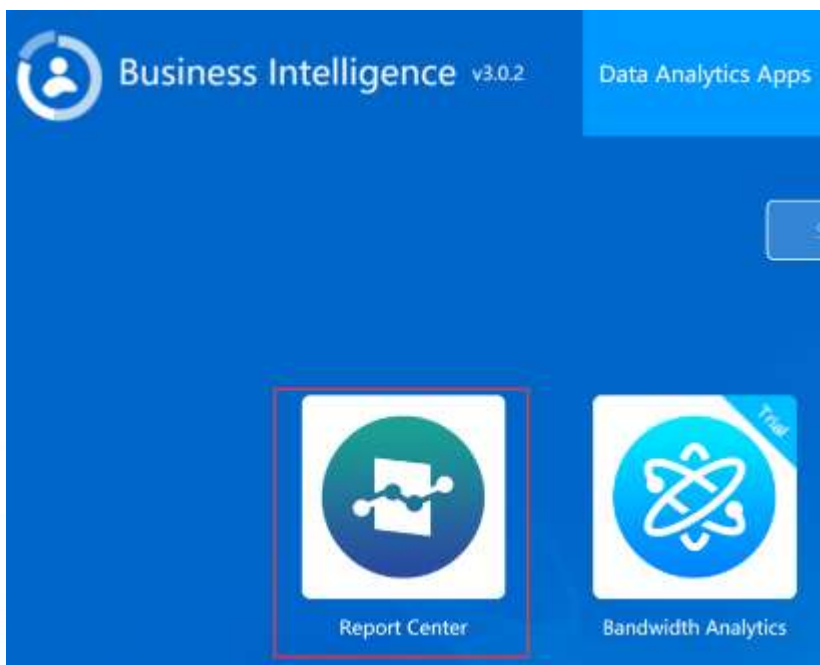
Compare the Original Datacenter

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

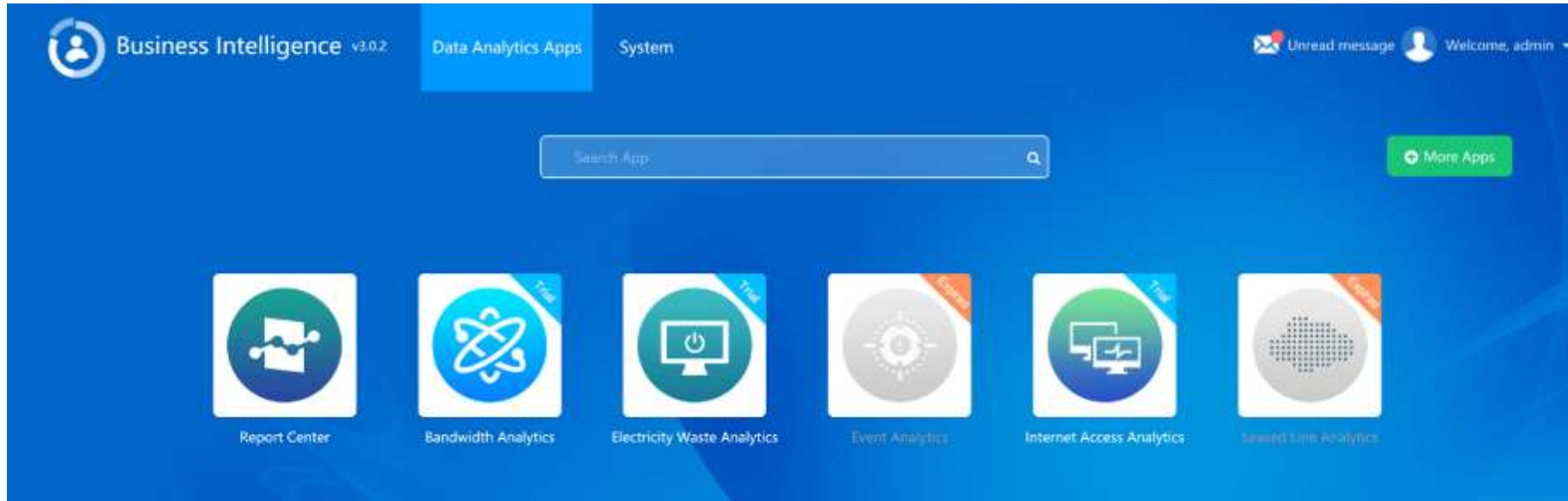


PART 4

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:

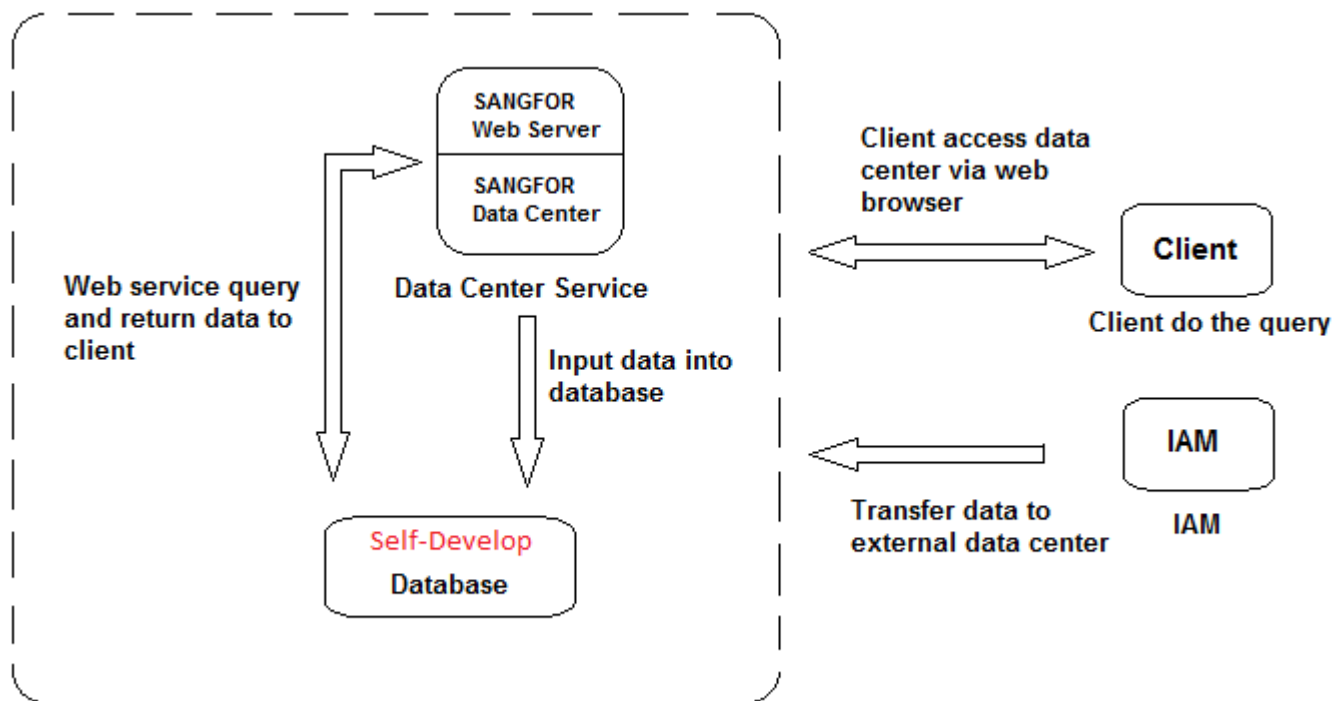


Report Center is used to record **data and statistics of Internet users**. Business Intelligence is divided into internal and external Business Intelligence, **the device comes with built-in Business Intelligence**, because storage space is limited, **if customers want to save a lot of logs, we recommend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



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.

Scenario Background

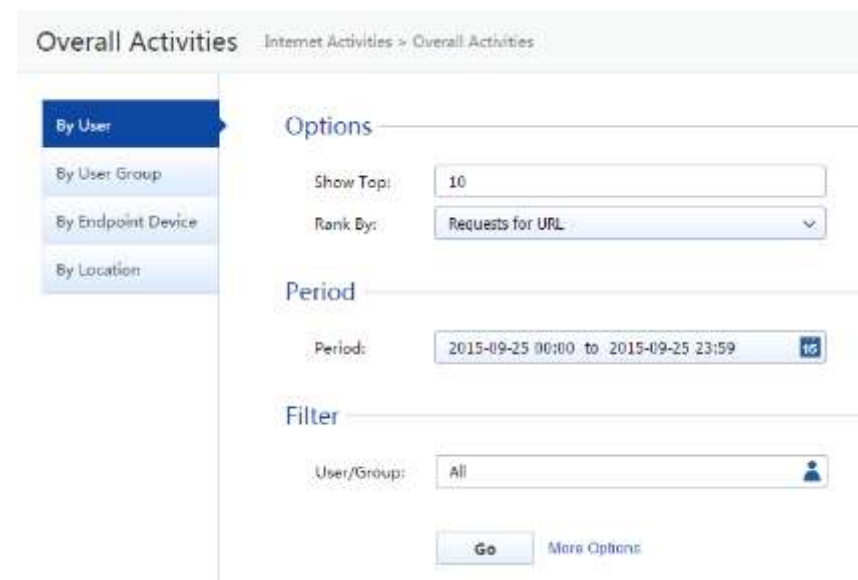
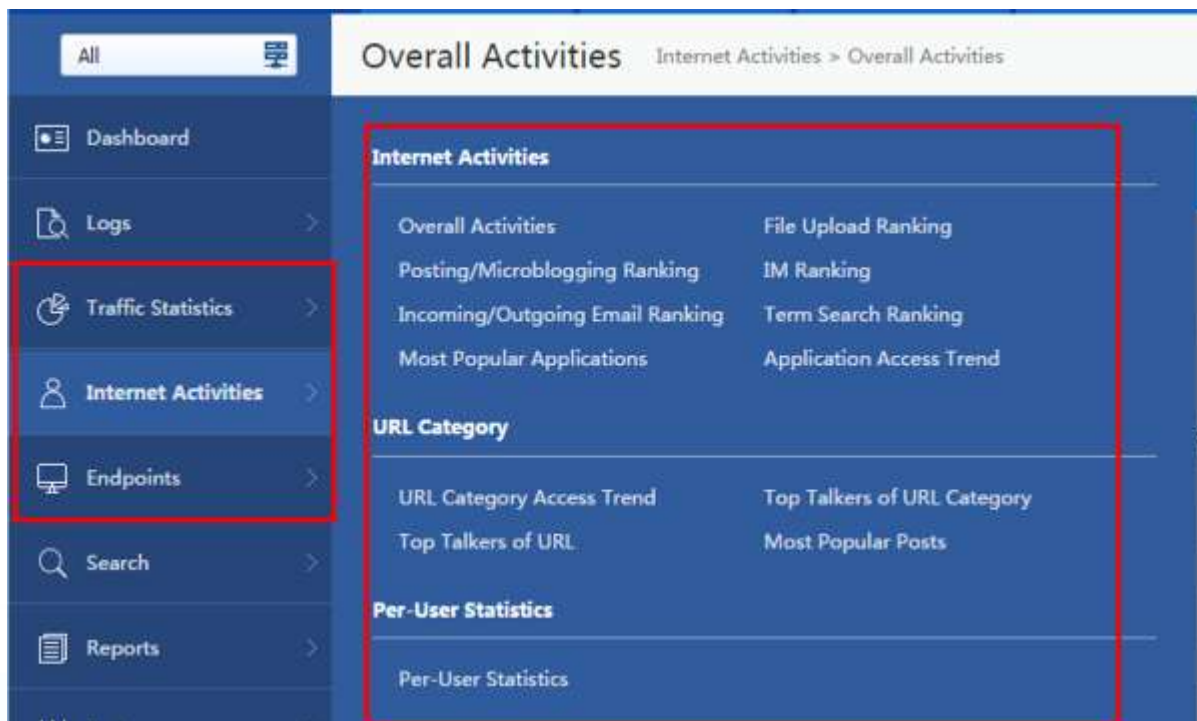
Customer requirement :

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

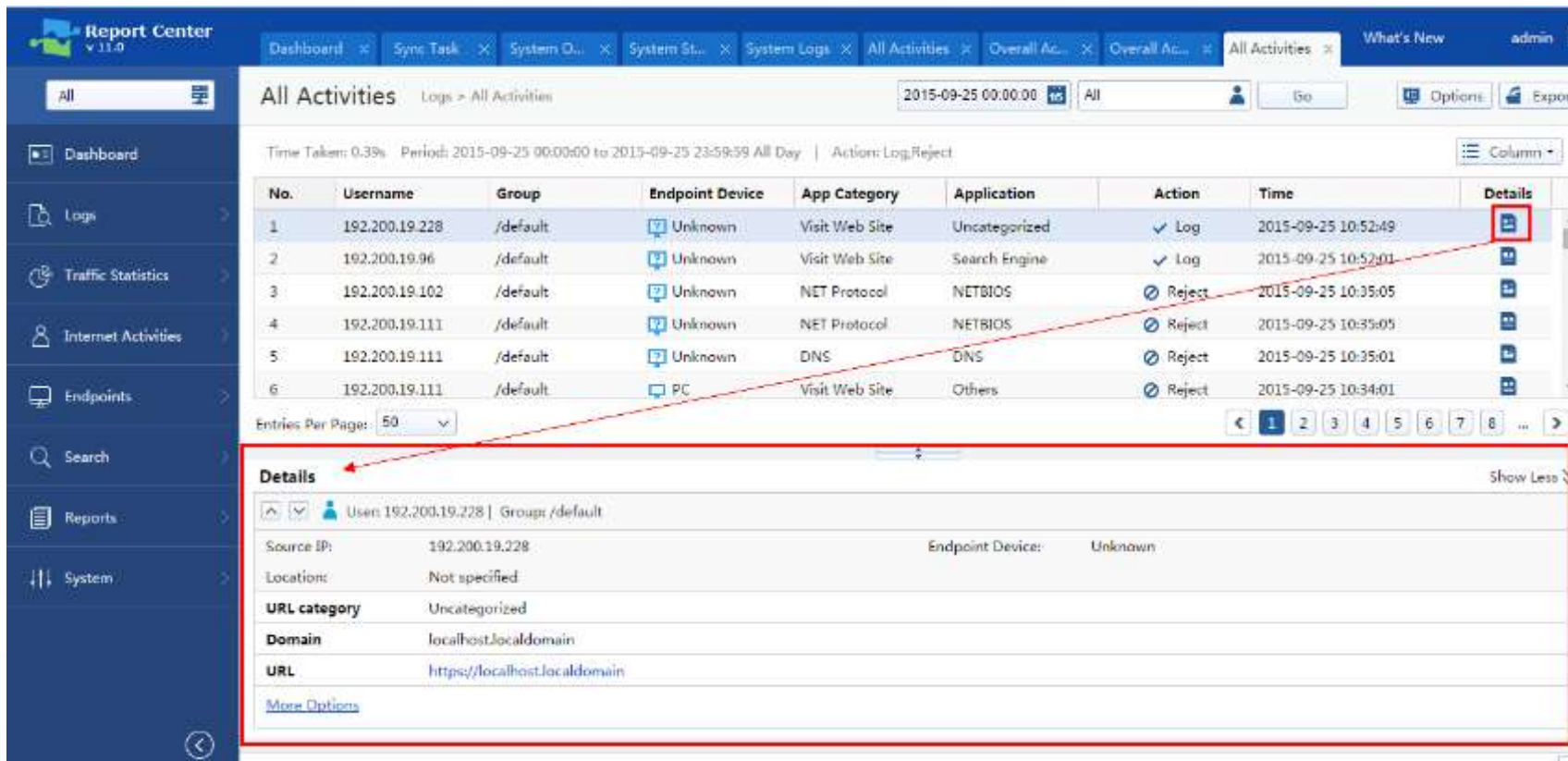
Requirement analysis :

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.

How to use external report center ?



How to use external report center ?



The screenshot displays the Sangfor Report Center interface. The top navigation bar includes tabs for Dashboard, Sync Task, System Overview, System Settings, System Logs, All Activities, Overall Activity, and Overall Activity. The left sidebar contains links to Dashboard, Logs, Traffic Statistics, Internet Activities, Endpoints, Search, Reports, and System. The main content area shows the 'All Activities' log for the period 2015-09-25 00:00:00 to 2015-09-25 23:59:59. The log table has columns for No., Username, Group, Endpoint Device, App Category, Application, Action, Time, and Details. A red box highlights the 'Details' column for the first entry. Below the table, a red box highlights the 'Details' section, which provides a breakdown of the activity for the user 192.200.19.228. The details include Source IP, Location, URL category, Domain, and URL.

No.	Username	Group	Endpoint Device	App Category	Application	Action	Time	Details
1	192.200.19.228	/default	Unknown	Visit Web Site	Uncategorized	✓ Log	2015-09-25 10:52:49	
2	192.200.19.96	/default	Unknown	Visit Web Site	Search Engine	✓ Log	2015-09-25 10:52:01	
3	192.200.19.102	/default	Unknown	NET Protocol	NETBIOS	⊗ Reject	2015-09-25 10:35:05	
4	192.200.19.111	/default	Unknown	NET Protocol	NETBIOS	⊗ Reject	2015-09-25 10:35:05	
5	192.200.19.111	/default	Unknown	DNS	DNS	⊗ Reject	2015-09-25 10:35:01	
6	192.200.19.111	/default	PC	Visit Web Site	Others	⊗ Reject	2015-09-25 10:34:01	

Entries Per Page: 50

Details [Show Less](#)

User: 192.200.19.228 | Group: /default

Source IP:	192.200.19.228	Endpoint Device:	Unknown
Location:	Not specified		
URL category	Uncategorized		
Domain	localhost.localdomain		
URL	https://localhost.localdomain		

[More Options](#)

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.

Detailed configuration

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

Description

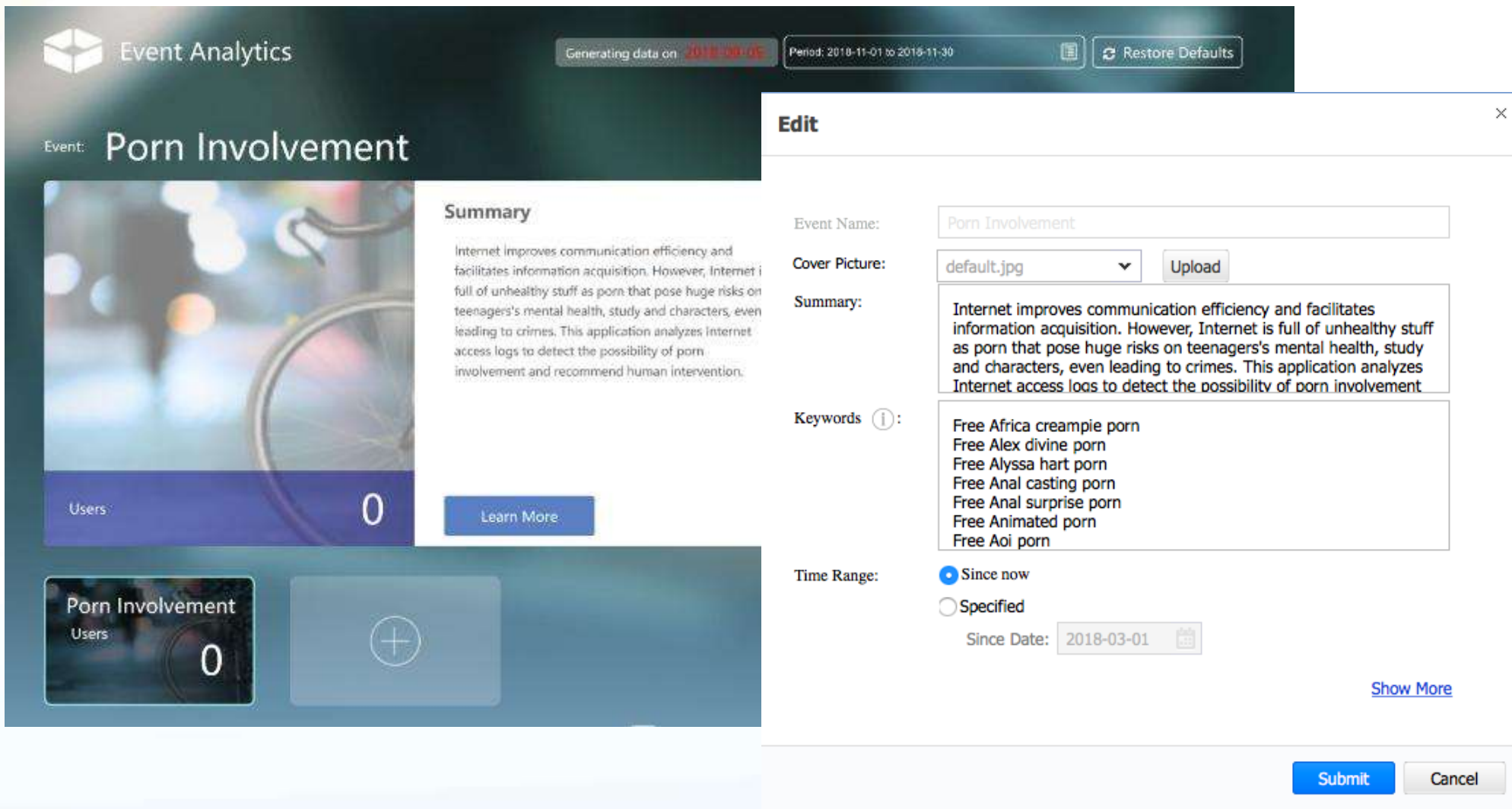
BI is a keyword-based versatile analysis template, more of which is reflected in the risk warning, the risk of the epidemic, and the risk of students participating in a vicious event. The instability caused by national emotions, etc., through the deployment of BI, can sense the risk in advance and achieve 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



The screenshot displays the 'Event Analytics' web interface. At the top, there's a header with the 'Event Analytics' logo, a status bar indicating 'Generating data on 2018-08-05', a date range 'Period: 2018-11-01 to 2018-11-30', and a 'Restore Defaults' button. The main content area features a large card for the event 'Porn Involvement'. This card includes a cover image, a summary paragraph, a 'Users' count of 0, and a 'Learn More' button. Below this card is a smaller version of the same card and a button with a plus sign. An 'Edit' modal window is open on the right, allowing for configuration changes. The modal contains fields for 'Event Name' (set to 'Porn Involvement'), 'Cover Picture' (set to 'default.jpg' with an 'Upload' button), 'Summary' (a text area with the same paragraph as the main card), 'Keywords' (a list of terms like 'Free Africa creampie porn'), and 'Time Range' (set to 'Since now' with a 'Since Date' of '2018-03-01'). A 'Show More' link is also present. At the bottom of the modal are 'Submit' and 'Cancel' buttons.

Event Analytics

Generating data on: 2018-08-05 | Period: 2018-11-01 to 2018-11-30 | Restore Defaults

Event: **Porn Involvement**

Summary

Internet improves communication efficiency and facilitates information acquisition. However, Internet is full of unhealthy stuff as porn that pose huge risks on teenagers's mental health, study and characters, even leading to crimes. This application analyzes Internet access logs to detect the possibility of porn involvement and recommend human intervention.

Users: 0 [Learn More](#)

Porn Involvement
Users: 0 [+](#)

Edit

Event Name: Porn Involvement

Cover Picture: default.jpg [Upload](#)

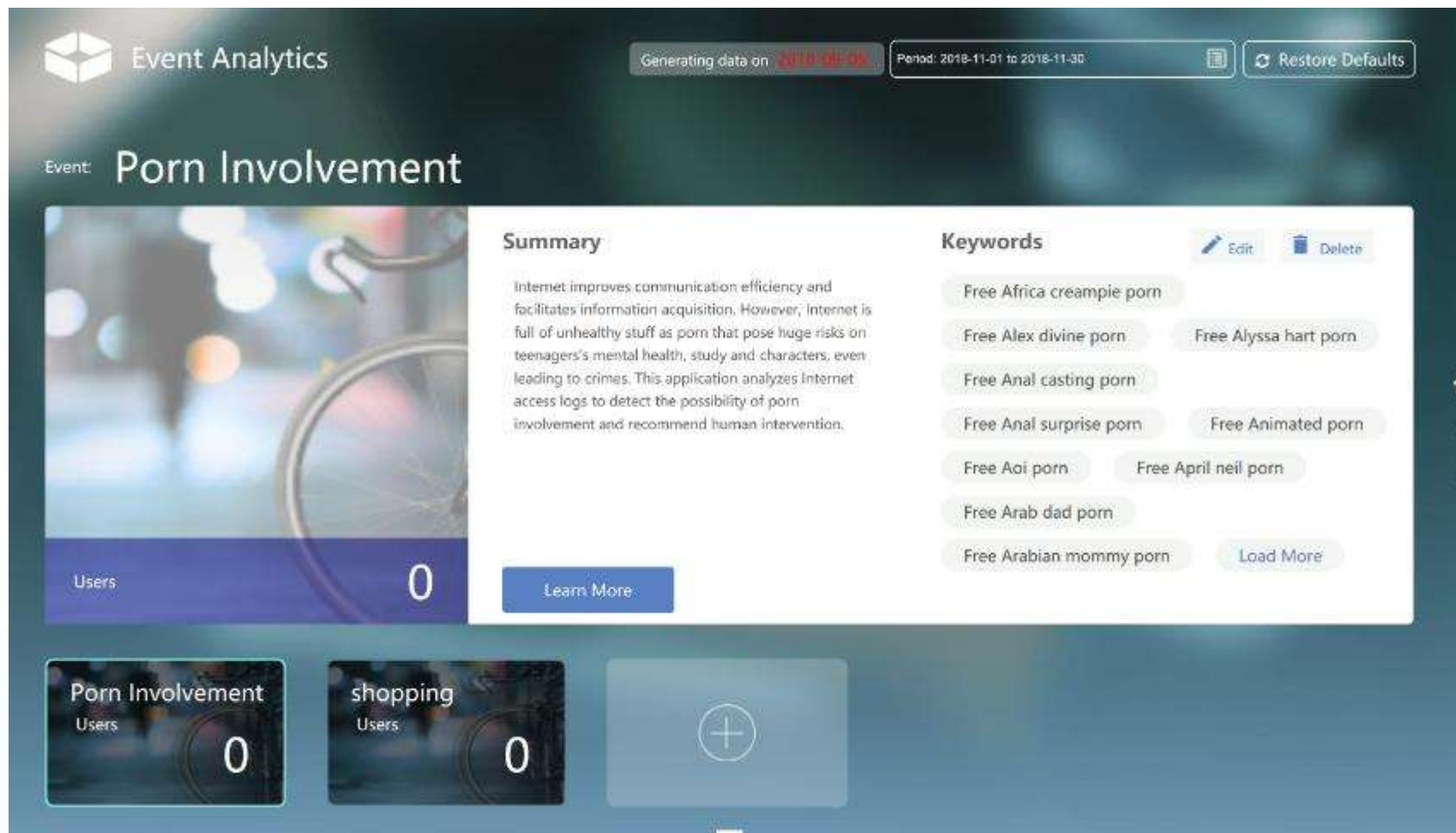
Summary: Internet improves communication efficiency and facilitates information acquisition. However, Internet is full of unhealthy stuff as porn that pose huge risks on teenagers's mental health, study and characters, even leading to crimes. This application analyzes Internet access logs to detect the possibility of porn involvement

Keywords ⓘ: Free Africa creampie porn
Free Alex divine porn
Free Alyssa hart porn
Free Anal casting porn
Free Anal surprise porn
Free Animated porn
Free Aoi porn

Time Range: ☒ Since now ☐ Specified
Since Date: 2018-03-01 [Show More](#)

[Submit](#) [Cancel](#)

Application effect is as follows



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:

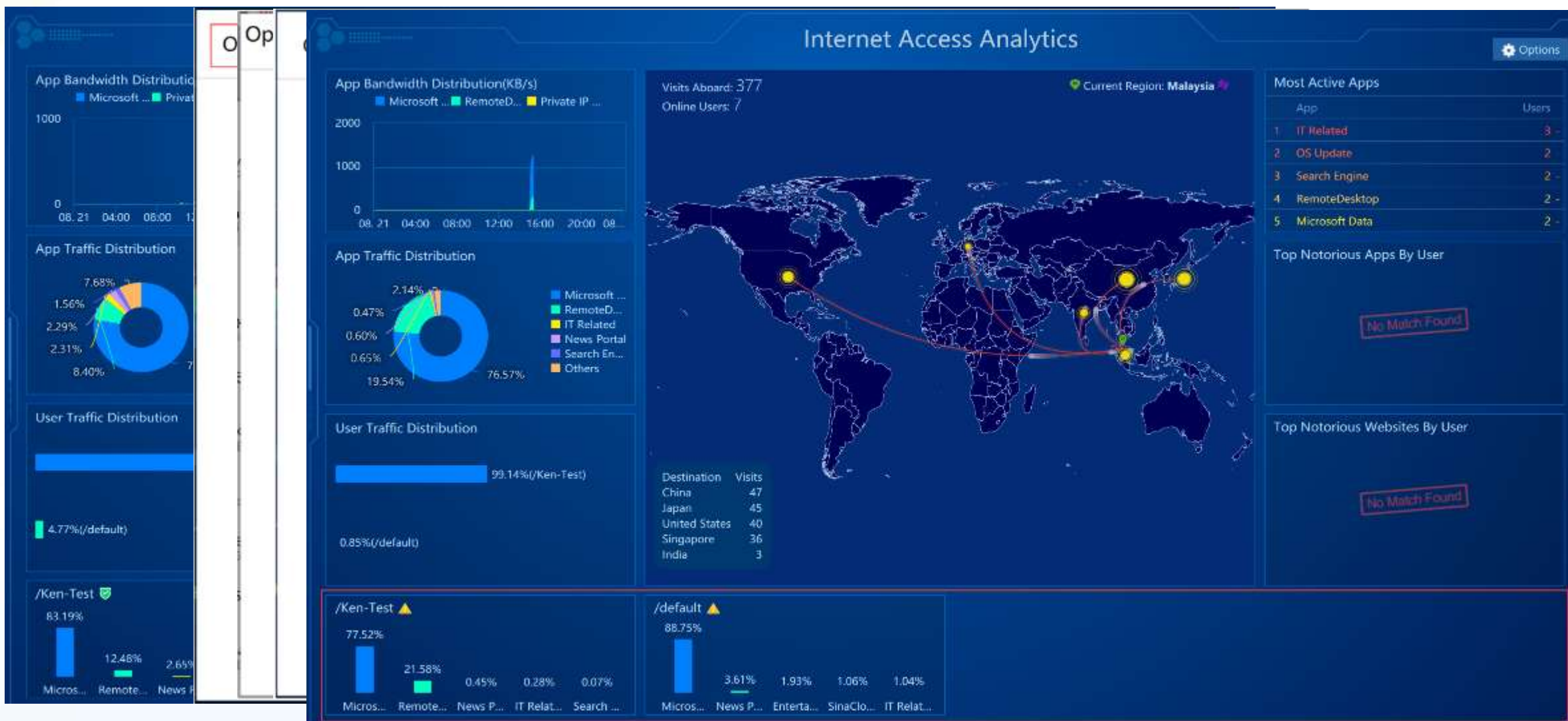
governments, enterprises, colleges and universities, operators, etc

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



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

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

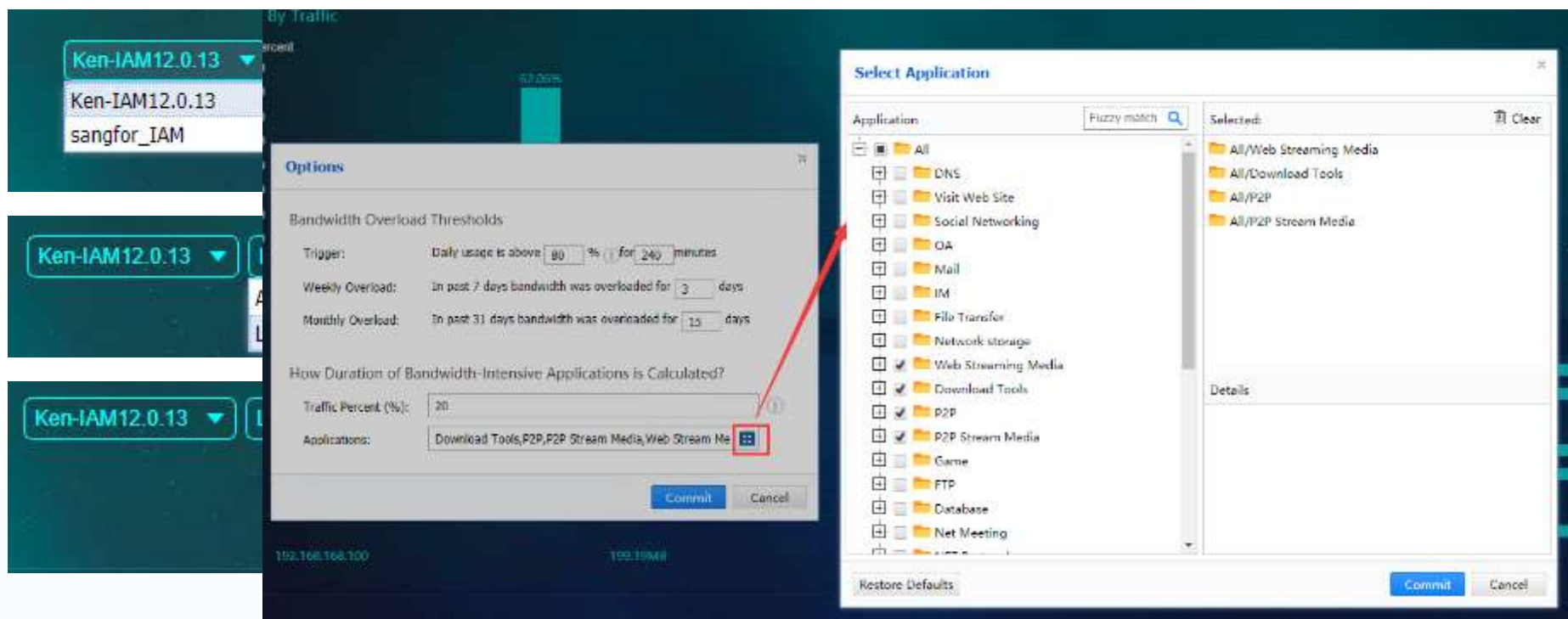
Principle of implementation

Collect IAG bandwidth usage data

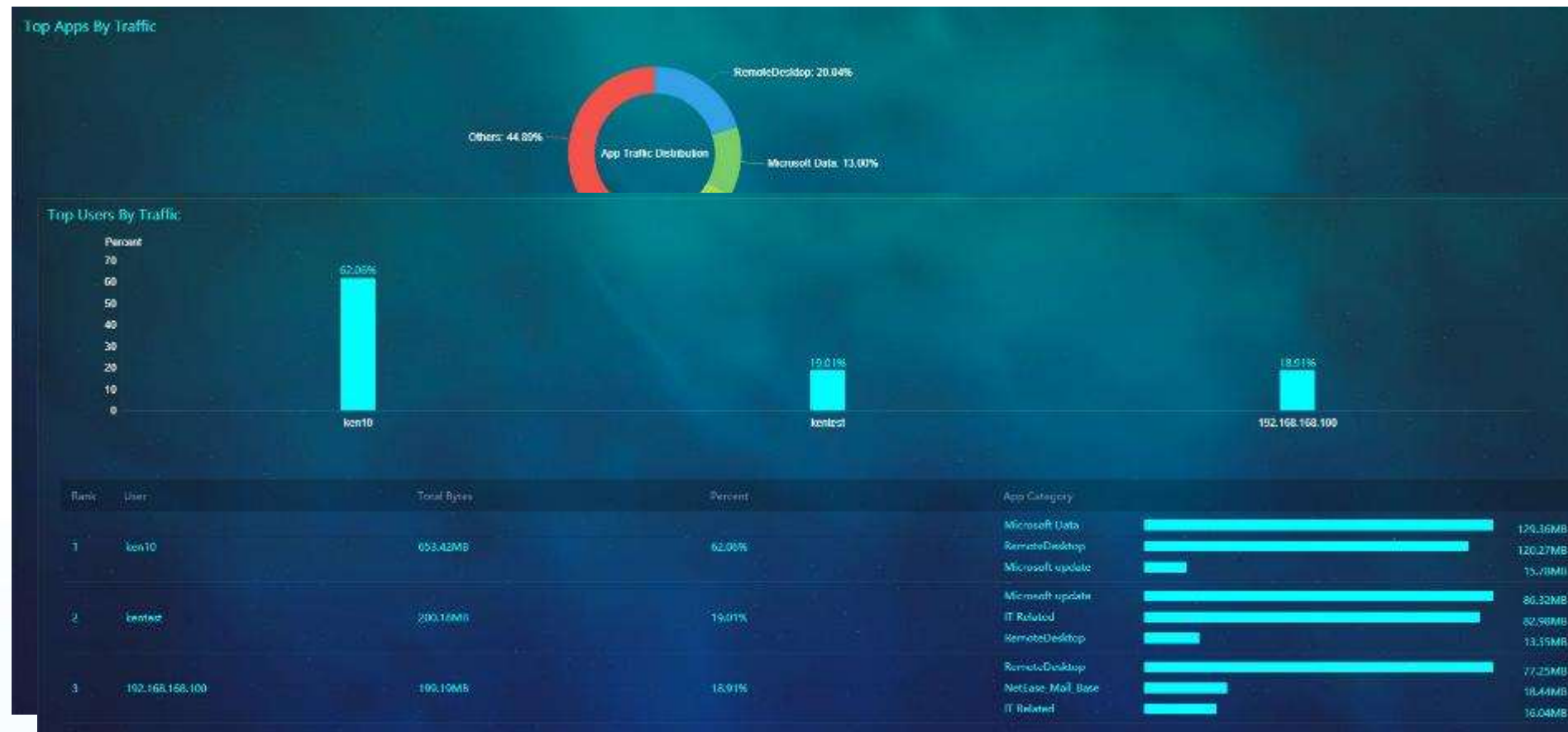
Instructions

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.



Application effect



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.

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.

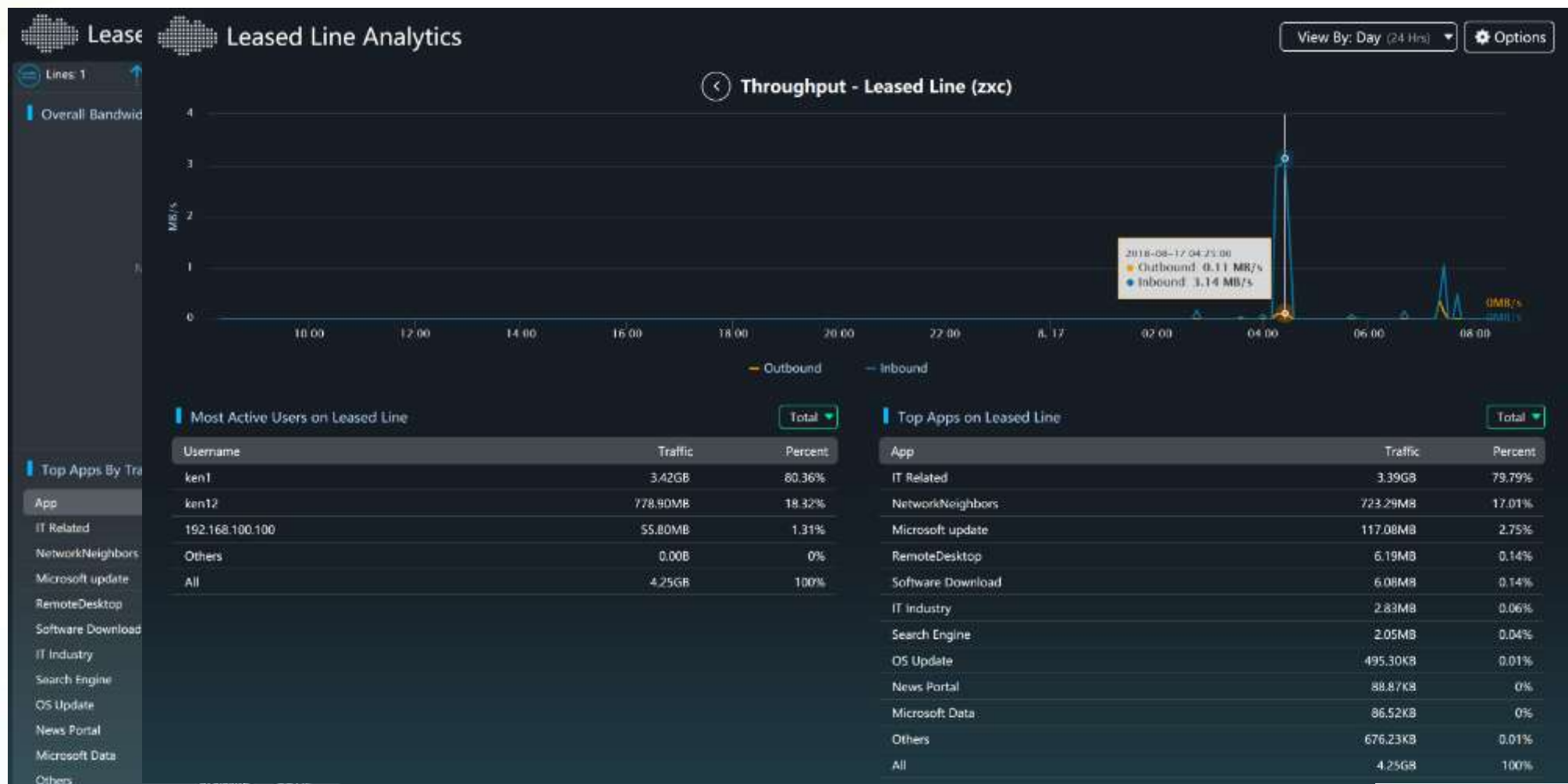
Scenes to be used

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.

Application effect



Background

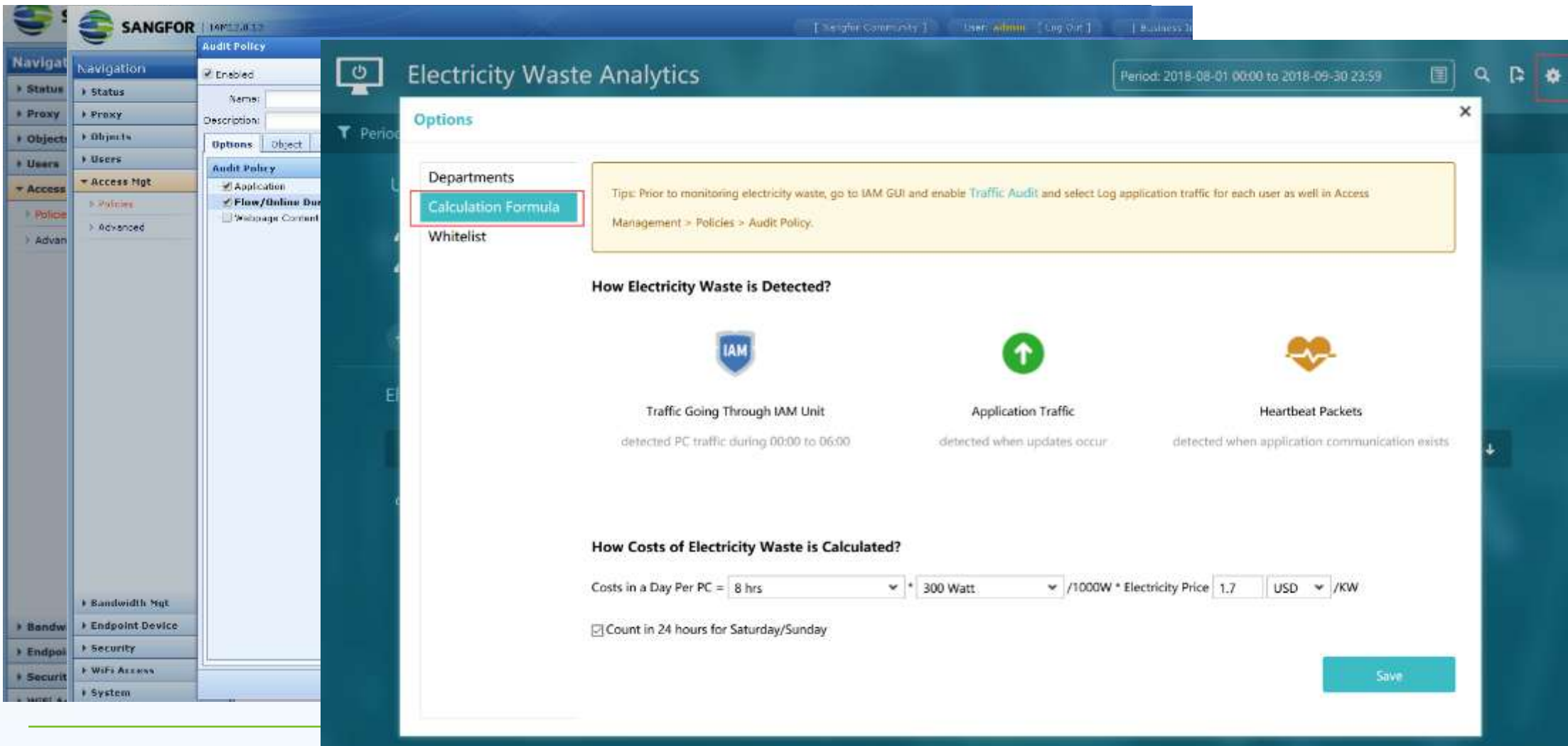
With the popularization of electronic office development and the improvement of office efficiency, some employees' bad work habits have caused waste of resources. By analyzing the online behavior of employees, they identify users who have not shut down and provide reference data for enterprises. Used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

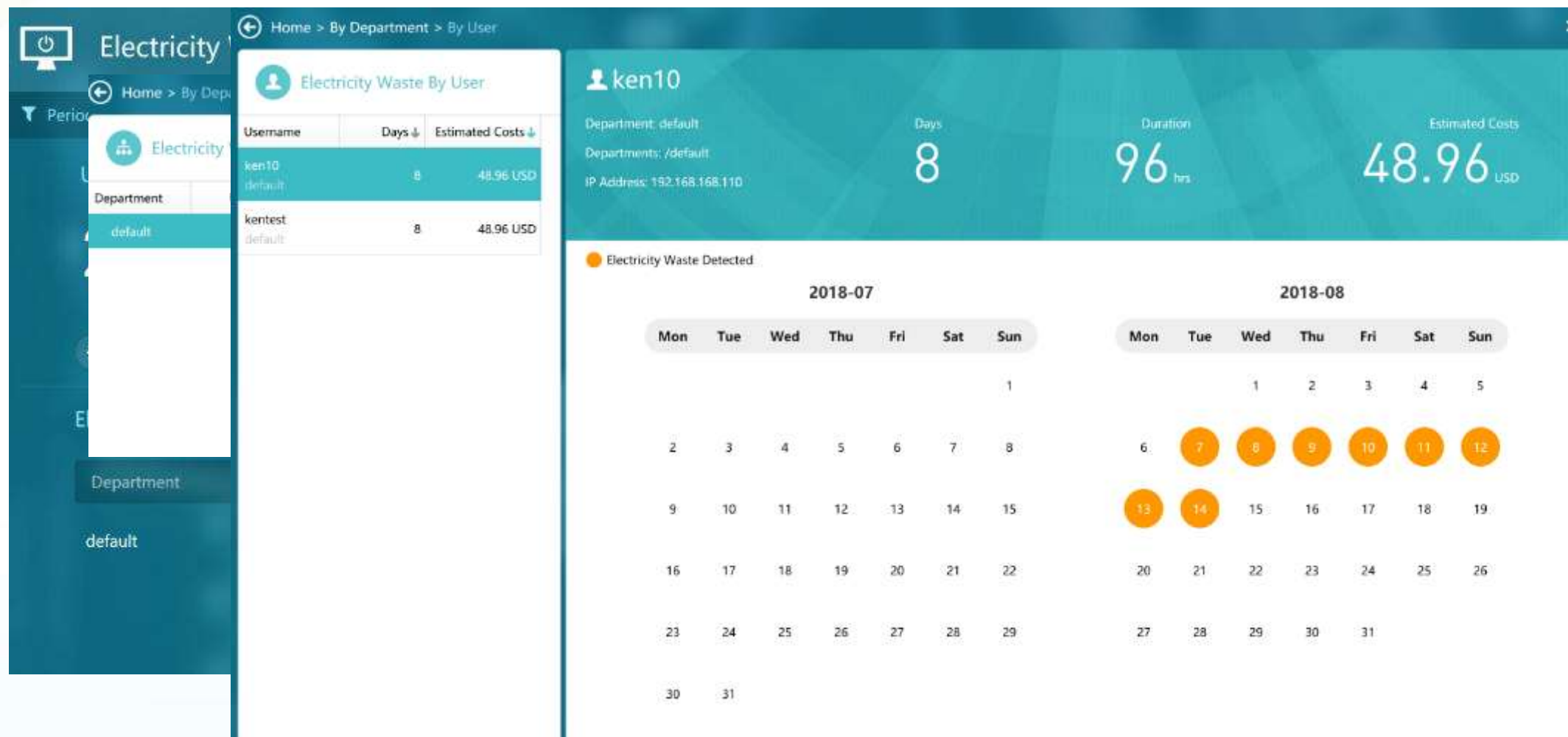
1. Online audit policy configuration Application and Flow/Online Duration audit
2. Do not shut down the definition, confirm the analysis department



The screenshot displays the Sangfor IAM GUI. On the left, a navigation pane shows the 'Access' menu with 'Access Mgt' expanded, and 'Audit Policy' selected. The main area shows the 'Electricity Waste Analytics' configuration window. The 'Options' tab is active, with 'Calculation Formula' highlighted. A tip box states: 'Tip: Prior to monitoring electricity waste, go to IAM GUI and enable Traffic Audit and select Log application traffic for each user as well in Access Management > Policies > Audit Policy.' Below this, the 'How Electricity Waste is Detected?' section shows three methods: 'Traffic Going Through IAM Unit' (detected PC traffic during 00:00 to 06:00), 'Application Traffic' (detected when updates occur), and 'Heartbeat Packets' (detected when application communication exists). The 'How Costs of Electricity Waste is Calculated?' section shows a formula: 'Costs in a Day Per PC = 8 hrs * 300 Watt / 1000W * Electricity Price 1.7 USD /KW'. A checkbox 'Count in 24 hours for Saturday/Sunday' is checked. A 'Save' button is at the bottom right.

Electricity Waste Analytics

Application effect



PART 5

Upgrade, Authorize, Admin Account

The BI software upgrade principle after Report Center 11.0

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

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

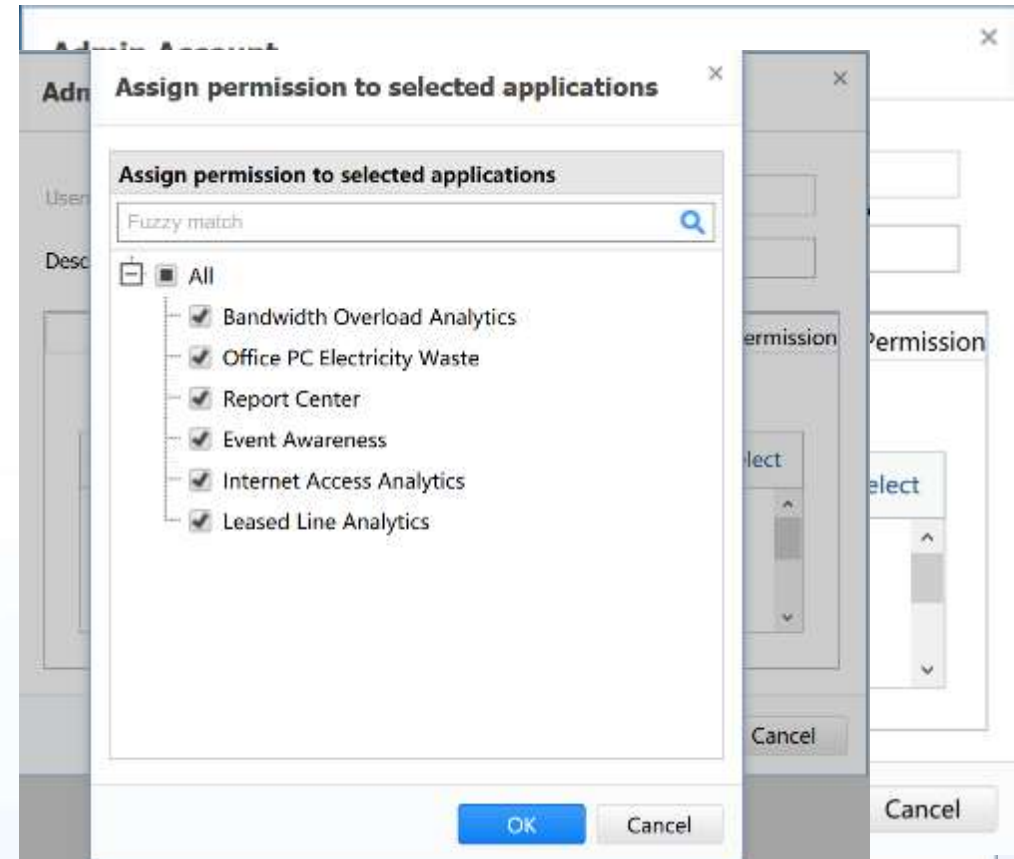
Only check the Search for logs, only the log center app permissions, you can only view the Home, Log Query, report center, all other apps are hidden

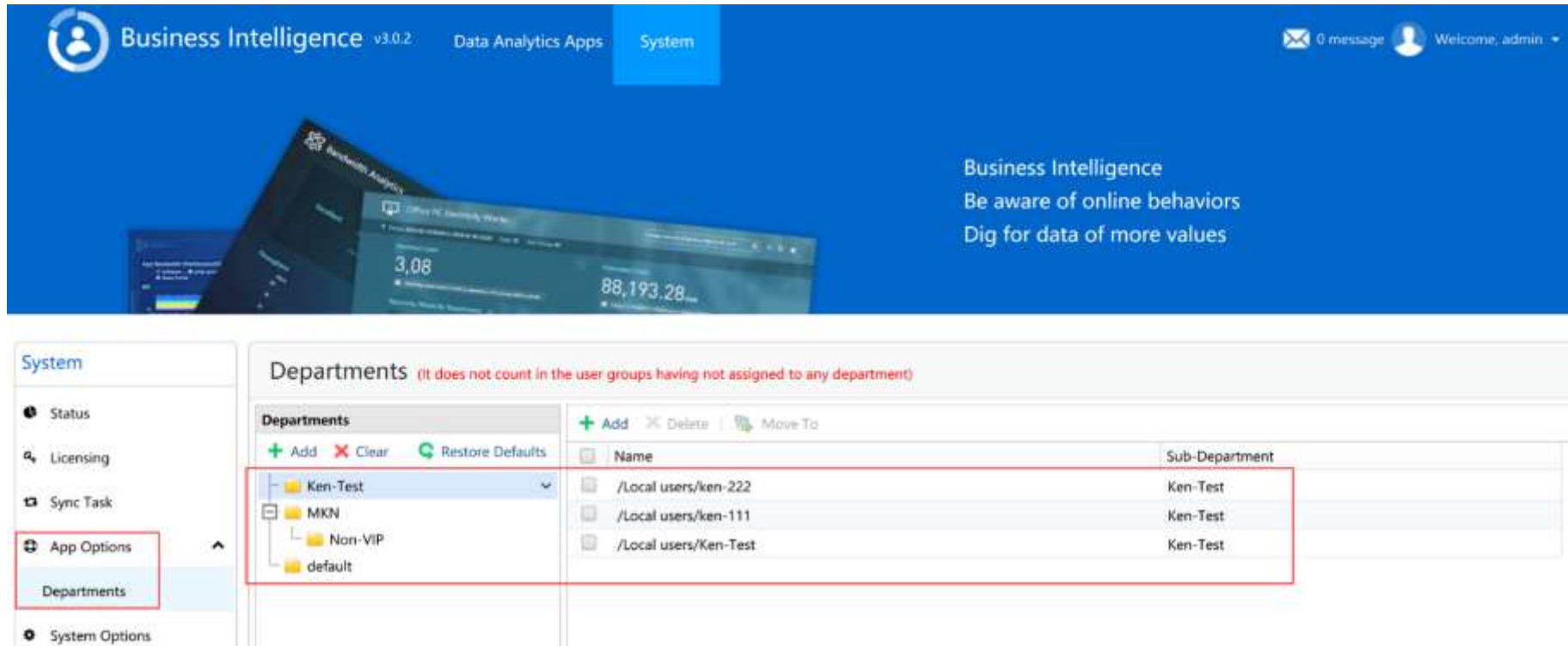
Only check Make statistics and reports, the app has permission to access, and the log center hides Log Query and report center

Hide System without checking System

APP Permission

Assign permission to selected applications





The screenshot displays the Sangfor Business Intelligence System interface. The top navigation bar includes 'Business Intelligence v3.0.2', 'Data Analytics Apps', and 'System'. The main header area features a blue background with the text 'Business Intelligence', 'Be aware of online behaviors', and 'Dig for data of more values'. On the left, a sidebar menu lists 'System', 'Status', 'Licensing', 'Sync Task', 'App Options' (highlighted with a red box), 'Departments', and 'System Options'. The 'Departments' page is active, showing a tree view on the left with 'Ken-Test' selected. The main content area displays a table of departments with columns 'Name' and 'Sub-Department'.

Name	Sub-Department
/Local users/ken-222	Ken-Test
/Local users/ken-111	Ken-Test
/Local users/Ken-Test	Ken-Test

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:

Licensing

USB Key ID

Current ID: AA658E7E [\(View Devices Able to Authorize This System\)](#)
ID Type: Gateway ID
Delay Time: Normal

Trial License

[Disable Alarm on License Expiration](#)
Trial Licenses: -
Status: **Free Promotion**
Max Users: No limit

Leased Line Analytics

License Status: Free

Time Remaining: 172 day(s)

Event Awareness

License Status: Free

Time Remaining: 172 day(s)

View Devices Able to Authorize This System

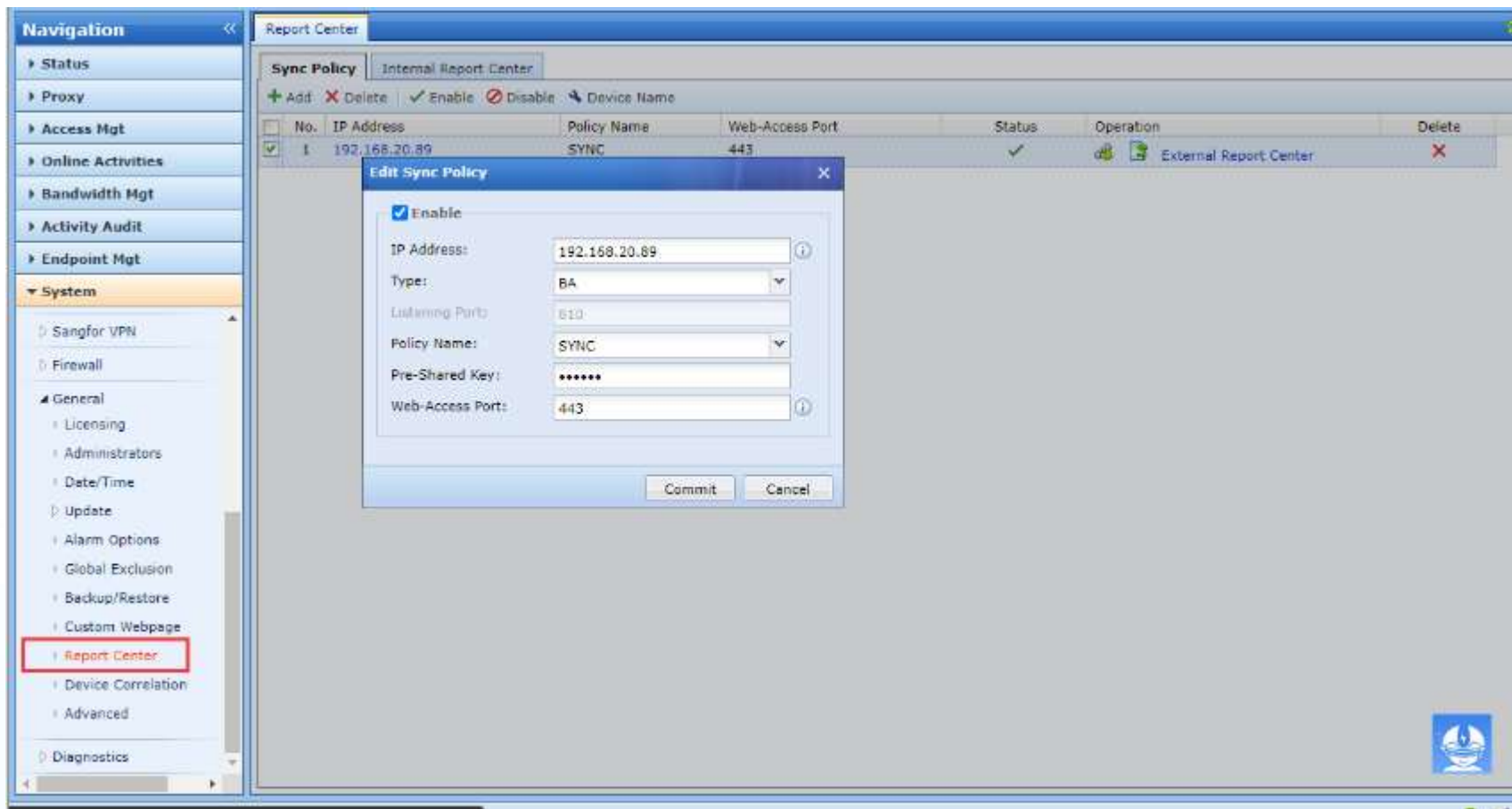
No.	Device Name	Gateway ID	Device Type
1	Ken-IAM12.0.13	AA658E7E	Authorized
2	sangfor_IAM	79175E73	Authorized

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.

Log Export

Log Export

System > Log Export

☒ Enable log export

Log Option

Servers

Syslog Server

☒ Enable Syslog server ⓘ

Syslog Server:

One entry per row. IP address and port are separated by colon (:), examples:
200.200.20.1:514
[2001:4008::1]:514

ⓘ

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.

The screenshot displays the 'Log Export' configuration page in a web interface. The page has a blue header with 'Log Export' and a breadcrumb 'System > Log Export'. Below the header, there's a section 'Log Export' with a checkbox 'Enable log export' which is checked. Under 'Log Option', the 'Servers' tab is selected. The 'Syslog Server' section includes a checkbox 'Enable Syslog server' (checked) and a text area for 'Syslog Server' with examples: '200.200.20.1:514' and '[2001:4008::1]:514'. The 'FTP Server' section has a checkbox 'Enable FTP server' (checked) with a note: '(Logs will be exported to specified server every 5 minutes after enabling it)'. It contains 'Basic Settings' with fields for 'Server Address', 'Server Port' (set to 21), and 'Export to Path'. There's also a checkbox for 'FTP Server Authentication' with 'Username' and 'Password' fields, and a 'Test Validity' button. The 'Advanced Settings' section includes a checkbox 'Send email alarm when FTP server encounters error' with a link to 'SMTP Server', a checkbox 'Compress exported logs', and a 'File Format' dropdown menu set to '.rar'.

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