

DIS APSCNLAN Support

Contents

Overvierw	3
Dashboard	3
Getting Started with Reports	5
Calculating Browse Time	7
Viewing Reports	8
Viewing Reports Online	8
Grid Chart	10
Viewing Grid Data	10
Graphical Charts	12
Downloading PDF or CSV Reports	14
Pre-Defined Searches	15
Searches by Type	15
Application Analysis	15
Bandwidth Analysis	15
Block Analysis	16
Browse Time Analysis	16
Browser Analysis	16
Category Analysis	17
Facebook Analysis	17
Group Analysis	17
Host Analysis	17
Legal Liability Analysis	17
Malware Analysis	17
Security Analysis	18
User Analysis	18
Filtering Reports	19
Adding Filters to a Search	19
Adding a Filter	19
Activating and Deactivating Filters	21
Removing Filters	21
Reporting Attributes	21
Attributes List	21
Portal 2.0	31

Dashboard	32
Quick Analysis Reports	
Quick Analysis Reports	

Overvierw

Dashboard

The dashboard gives you an overview of web activity at your organization over the last 24 hours.

Click the **Dashboard** tab to display the following data:

- All blocks
- Facebook usage
- Spyware blocks
- Web Filtering blocks
- Web Virus blocks

The following data is displayed:

- All blocks
- Top 10 users by blocks



Use the drop-down menu to select one of the following options to filter the results:

- Facebook Usage Show breakdown by application Facebook hits over time Show only blocke Facebook usage Users making the most hits Top applications by hits 10.112.104.38 10.112.104.27 10.112.104.27 10.112.104.187 10.112.104.183 10.112.104.53 10.112.104.69 10.112.106.119 56,000 42,000 28,000 14,000 1,831 Activity by hits g the most bandwidt - Like/Tag, 19 ~ All Spyware blocks Top 10 users by Spyware block 3,200 2,400 1,600 All Web Filtering block Top 10 users by Web Filtering blocks 64,0 48,000 32,00 16.00 - 112.104 10.112.106.1 × All Web Virus blocks Top 10 users by Web Virus block
- Spyware blocks

•

٠

Web Filtering blocks

Web Virus blocks •

Getting Started with Reports

The reporting functionality in Cisco ScanCenter is accessed from the **Reports** tab. Reports enable you to analyze:

GMT-06:00

Custom

 $\mathbf{\vee}$

 $\mathbf{\vee}$ From: 10-05-2016 00 · : 00 · + To: 11-05-2016 00 · : 00 ·

Home Dashboard Web Virus Spyw

Reports

Auto Run Report

View as

Create Report

e Web Filtering Admin

Download

Notifications 22

Time Zone

Time Period

You have not created any custom reports.

Predefined Reports

(+) Application Analysis 🕀 Bandwidth Analysis

🕀 Block Analysis Howse Time Analysis Browser Analysis

🕀 Category Analysis 🕀 Facebook Analysis

🕀 Group Analysis 🕀 Host Analysis 🕀 Legal Liability Analysis

🕀 Malware Analysis 🕀 Security Anal

Reports

- Applications .
- Bandwidth .
- Blocks •
- Browse Time •
- Browsers .
- Categories •
- Facebook
- Groups •
- Hosts •
- Legal Liability •
- Malware •
- Security .
- Users .

There are three gene

	🛞 User Analysis	
eric types of	report	
Notifications 22	Home Dashboard Web Virus Spyware Web Filtering	Admin Reports
Time Ze Time Pe From: [Select A Select Add at Internal	Search I Time Analysis I Detailed Search Add Filter Remove Activate Desctivate Save Filter Set Select None Add Filter Remove Activate Desctivate Save Filter Set ilter type: Filter IP V is equal to V 10.112.104.10 ×	Auto Run Report
View fir	st 10 User sorted by <u>Hits</u> (<u>descending</u>), and their first <u>5 Host</u> sorted by <u>Hits</u> (<u>descending</u>)	

- Standard reports use conditions, and up to two attributes to provide more detailed information for a chosen time . period.
- Time Analysis reports provide similar information to standard reports but for a single attribute over a chosen time . period.
- Detailed reports use conditions and multiple attributes to provide a higher level of detail than standard reports for a • chosen time period.

There are also two special report types:

- Allowed Traffic
- User Audit Reports

Reports are generated by running searches. Cisco provides an extensive range of pre-defined searches. You can use these as the starting point for creating your own searches, or you can create searches from scratch.

Notifications 22	Home Dashboard Web Virus Spyware	Web Filtering	Admin Reports
Reports Reports Search Filter Sets Composite Reports	Select Search	:	Select Reports
Scheduled Reports Recipients Allowed Traffic User Audit	Custom ▼ 016 00 ▼ : 00 ▼ ↔ To: 11-05-2016 00 ▼ : 00 ▼ om reports.		Auto Run Report <u>Create Report</u>
Predefined Reports		Download	View as
Application Analysis			
🕀 Bandwidth Analysis			
Block Analysis			
🕀 Browse Time Analysis			

The main steps to create any type of report are the same:

Procedure

Notifications 22	Home Dashboard Web Virus Spyware Web Fi	Itering Admin Reports
Reports		
Time Zone GMT-06:00	Set your time period	
Time Period Custom From: 10-05-2016 00 Choose		Auto Run Report
Filter Refect filter type:	Choose Internal IP Choose is equal to	× Enter IP Address
Add attribute filter Internal IP	▼ is equal to	× Add
View first 10 User sorte	ed by <u>Hits</u> (<u>descending</u>), and their first 5 <u>Host</u> sorted by <u>Hits</u> (<u>descending</u>)	Click Add
Click Laund	ch Search	

- **Step 1** Choose a time period for the search, from the last hour to the last year.
- **Step 2** Choose a pre-defined search or saved search, or create a new search.
- **Step 3** Add filters based on reporting attributes or metrics.
- **Step 4** Choose the number of results to view, from 10 to 1000.
- **Step 5** Choose a reporting attribute by which to group the results.

- **Step 6** Choose to sort the results by name, bandwidth, browse time, bytes sent, bytes received, or hits.
- **Step 7** Choose to view the top or bottom results.
- **Step 8** (Optional) Add a second reporting attribute by which to group the results.
- **Step 9** Choose to view the report as a grid, bar, column, pie or line chart.
- Step 10 Click Launch search.
- **Step 11** Store the search for future use.

There are more than 60 unique attributes to choose from, so it is best to start by using pre-defined searches.

In addition to creating and modifying searches, from the **Reports** pane you can:

- Create and manage sets of filters.
- Combine searches into composite reports.
- View reports online and print or export them.
- Download reports to view offline or import into a spreadsheet or word processor.
- Schedule reports for delivery by email to groups of recipients.

Note The reporting functionality requires Adobe Flash 10 (or higher).

Calculating Browse Time

Because it not possible to tell when a user is away from their computer, or viewing a page that has finished loading, browse time is calculated based on web requests made within a distinct minute.

Any distinct minute in which one or more web requests are made is counted as a single minute of browse time. For example, if a complex web page results in 100 web requests made within a distinct minute, it will count as one minute of browse time.

The actual time taken for a web page to load is not measured. If a web page takes one and a half minutes to load, then web requests will be made across two distinct minutes measured as two minutes of browse time. However, if a user spends an hour reading a simple web page that loaded within a distinct minute that does not refresh itself, this is measured as one minute of browse time

When you create a reports including browse time, you should always use Host instead of URL to generate the most accurate report.

Note Browse Time should not be relied on as a metric in two-level reports because this can result in the double counting of requests. For example, if a site is classified in more than one category, or if different Web requests are made in the same minute. It is not possible to determine if a web page refreshed itself.

Viewing Reports

Viewing Reports Online

Reports are generated from predefined or previously saved searches. They can be viewed online or downloaded as a PDF. When a report has been generated you can refine the search by adding filters or changing the conditions of the search. You can store your changes as a new search or replace a previously stored search.

Procedure

Step 1 Click the **Reports** tab to display the **Reports** page. Alternatively, in the **Reports** menu, click **Reports**. The available searches are displayed in two tables:

		Provide a second s	<u>Create a ne</u>	w repo
	Custom reports	Download	View a	15
	(g) My Reports			_
	My First Report		Grid	•
	Predefined reports	Download	View a	15
Custom and a sta	Application Analysis			
Custom reports	Bandwidth Analysis			
	Block Analysis			
Predefined reports	Browse Time Analysis			
r redefined reports	Category Analysis			
	G Group Analysis			
	What were the Top 10 Groups consuming the most Bandwidth?	ŧ	Grid	•
	What were the Top 10 Groups by Hits?	±	Grid	•
	Who were the Top 10 Users with the highest Browse Time for the Top 10 Groups?	±	Grid	•
	Host Analysis			
	(Legal Liability Analysis			
	Malware Analysis			
	Security Analysis			
	(1) Her Analysis			

- **Step 2** Searches do not include time period information so you must provide this each time you generate a report. In the **Time Zone** drop-down list, choose a time zone. The default is UTC.
- **Step 3** In the **Time Period** drop-down list, choose a predefined time period. The predefined time periods are:
 - Previous hour
 - Previous day (yesterday)
 - Previous week (the last full week)
 - Last *n* hours (12, 24, 48, or 72)
 - Last week (the previous seven days)
 - Last *n* weeks (2 or 3)
 - Last month
 - Last *n* months (2, 3, 4, 5, 6, 9, or 12)

Alternatively, click **Custom** and enter the required start and end dates and times:

Reports	4						
			\$ Search	1 Time Ana	alysis Detaile	ed Search	
	Time Zone	GMT-06-00		S	et your ti	me period	
	Time Deried	Custom	N. I.	_	1		

- a. Enter a start date in the box or click the **Calendar** icon to choose a date.
- b. Choose a start time using the hour and minute drop-down lists. The time is shown using the 24-hour clock.
- c. Enter an end date in the box or click the **Calendar** icon to choose a date.
- d. Choose an end time using the hour and minute drop-down lists.
- **Step 4** Select the **Auto Run Report** check box to run the search as soon as the report is opened. Alternatively, clear the check box to prevent the search running automatically.
- **Step 5** Click a folder to show or hide the searches for that folder.
- **Step 6** In the **View as** drop-down list, choose a chart type. The available charts depend on the type of report and may include:
 - Bar
 - Column
 - Grid
 - Pie
- **Step 7** Click **Launch Search** to generate and view a report. Alternatively, click the **Download** icon to download the report in PDF format.

Grid Chart

The grid chart is the default way of viewing reports. From here you can change the data that is displayed in the other charts.

Which were the top ten categories that consumed the most bandwidth?							
Show 50 💌	rows per page << first	< prev 1 n	ext > last >>	10 results			
+ - Category	Bandwidth (Bytes) 🔻	Browse Time (Min)	Bytes Received	Bytes Sent	Hits		
Totals for Category	73,025,701,669	23,993	71,182,427,262	1,843,274,407	1,125,160		
streaming video	35,121,163,469	610	34,632,021,669	489,141,800	82,670		
infrastructure and content delivery	6,288,785,532	1,101	6,123,835,729	164,949,803	77,676		
computers and internet	6,137,630,620	1,422	5,624,292,648	513,337,972	103,254		
education	4,444,147,937	1,184	4,333,788,010	110,359,927	41,009		
streaming audio	3,158,113,479	841	3,146,141,633	11,971,846	22,648		
social networking	2,779,702,979	1,087	2,696,264,790	83,438,189	76,947		
business and industry	1,840,159,186	960	1,702,942,140	137,217,046	121,222		
entertainment	1,806,306,131	424	1,800,450,261	5,855,870	8,124		
games	1,795,537,396	504	1,787,284,229	8,253,167	33,730		
safe for kids	1,458,940,653	319	1,458,429,009	511,644	63,197		
safe for kids Show 50 💌	1, 458, 940, 653 rows per page <	319	1,458,429,009	511, 644 10 results	63,197		
0.0 ()							
Custom (from May 10, 2016 at 00:00 AM to May 11, 2016 at	: 00:00 AM) View: Bandwidth (By	tes)					
report as: 🔀 PDF 📾 CSV							

Note The first line of the table always displays the overall totals for all data, not just that included in the report.

Viewing Grid Data

Choose the number of results to display per page from the **Show** list. The available options are:



Navigate through the pages using the first, prev, next and last buttons.

Show	Refine you search	ch by clickin	g10	results	
Response Major Content	an attribute an	d Selecting	tes Received	Bytes Sent	Hits
Totals for Response Major Co	is equa	I to.	,409,888,770	2,161,507,738	1,317,803
Refine search 🖶	Click Launch	Search to	,592,089,571	2,111,928,082	503,655
A Response Major Content Type	is equal to applicati display the ref	ined report	,577,063,530	5,988,331	143,26
OR Response Major Content Type	is not equal to app	incu report	,417,786,662	0	6,06
		675	7,628,106,038	1,092,465	316,02
audio	4,176,018,438	504	4,176,018,438	0	13,02
text	1,807,629,381	1,440	1,768,643,125	38,986,256	239,99
-	126,885,411	771	123,372,807	3,512,604	94,40
flv-application	96,175,199	11	96,175,199	0	5
binary	13,152,174	36	13,152,174	0	80
font	9,591,295	93	9,591,295	0	304
Show [io 🔽 rows per page <<< first < prev	1 next >	last >> 10	results	

You can refine your search by clicking entries in the attribute columns. Click an entry, then click **is equal to** to include only that entry in the report. Alternatively, click **is not equal to** to exclude the entry. When you have made your changes, click **Launch search** to display the refined report.

Graphical Charts

There are three types of graphical charts:

	Wh	ich were the top ten cate	gories that consumed th	e most bandwidth?		
	Show 50 🔽	rows per page << first	< prev 1 n	ext > last >>	10 results	
	+ - Category	Bandwidth (Bytes) 🔻	Browse Time (Min)	Bytes Received	Bytes Sent	Hits
	Totals for Category	73,025,701,669	23,993	71,182,427,262	1,843,274,407	1,125,160
	streaming video	35,121,163,469	610	34,632,021,669	489,141,800	82,670
	infrastructure and content delivery	6,288,785,532	1,101	6,123,835,729	164,949,803	77,676
	computers and internet	6,137,630,620	1,422	5,624,292,648	513,337,972	103,254
• Bar	education	4,444,147,937	1,184	4,333,788,010	110,359,927	41,009
	streaming audio	3,158,113,479	841	3,146,141,633	11,971,846	22,648
 Column 	social networking	2,779,702,979	1,087	2,696,264,790	83,438,189	76,947
• Pie	business and industry	1,840,159,186	960	1,702,942,140	137,217,046	121,222
	entertainment	1,806,306,131	424	1,800,450,261	5,855,870	8,124
	games	1,795,537,396	504	1,787,284,229	8,253,167	33,730
	Graphical Charts	1,458,940,653	319	1,458,429,009	511,644	63,197
	Show 50 Show 50 me range: Qustom (from May 10, 2016 at 00:00 AM to May 11, 2016 at ownload report as: PDF @ CSV	rows per page << first : 00:00 AM) View: Bandwidth (Byt	< prev 1 n	ext > last >>	10 results	

Click the hyperlink at the top of the chart to change the sort metric. The available metrics are:



- Bandwidth (Bytes)
- Browse Time (Min)
- Bytes Received
- Bytes Sent
- Hits

Bar Chart

The bar chart displays the data as horizontal bars.

Right Click the Bar Chart to print or save.



What was the bandwidth consumed by major content type? For each 'Response Major Content Type', show the <u>Bandwidth (Bytes</u>) (click to change)

Column Chart

The column chart displays the data as vertical bars.

Right Click the Bar Chart to print or save.

Pie Chart

The pie chart displays the data as a 2D or 3D pie chart.

Right Click the Bar Chart to print or save.



Additional commands are available when you right-click the pie chart.

Click **Enable Rotation** to enable the chart to be rotated by clicking and dragging the chart. You cannot move slices while you are rotating the chart.

Click **Enable Slicing Movement** to enable the chart's slices to be moved by clicking them. You cannot rotate the chart while you are moving slices.

Click View 2D to view a two-dimensional representation of the chart.

Click **View 3D** to view a three-dimensional representation of the chart.

Downloading PDF or CSV Reports

To download a report in PDF format, view the report on-screen as normal and then click the **PDF** icon to download the report. Alternatively, you can download a report in PDF format without viewing the report on-screen.

Downloading a report in CSV (comma separated value) format enables you to open the report in a spreadsheet.

page << first < prev width (Bytes) ▼ Browse T ,025,701,669 ,121,163,469 ,288,785,532 ,137,630,620 ,444,147,937	1 next> Fime (Min) Bytes 23,993 71,14 610 34,63 1,101 6,12 1,422 5,63	last >> 10 m Received By 82,427,262 1,8 32,021,669 4 23,835,729 1	esults tes Sent 43,274,407 1,1 89,141,800 64,949,803	H its 125,160 82,670
vidth (Bytes) ▼ Browse 1 ,025,701,669 ,121,163,469 ,288,785,532 ,137,630,620 ,444,147,937	Fine (Min) Bytes 23,993 71,14 610 34,63 1,101 6,13 1,422 5,63	Received By 82,427,262 1,8 32,021,669 4 23,835,729 1	tes Sent I 43,274,407 1,1 89,141,800 64,949,803	Hits L25,160 82,670
,025,701,669 ,121,163,469 ,288,785,532 ,137,630,620 ,444,147,937	23,993 71,18 610 34,63 1,101 6,13 1,422 5,63	82,427,262 1,8 32,021,669 4 23,835,729 1	43,274,407 1,1 89,141,800 64,949,803	L25,160 82,670
,121,163,469 ,288,785,532 ,137,630,620 ,444,147,937	610 34,63 1,101 6,12 1,422 5,62	32,021,669 4 23,835,729 1	89,141,800 64,949,803	82,670
,288,785,532 ,137,630,620 ,444,147,937	1,101 6,12 1,422 5,62	23,835,729 1	64,949,803	
,137,630,620 ,444,147,937	1,422 5,62			77,676
,444,147,937		24,292,648 5.	13,337,972 1	103,254
	1,184 4,33	33,788,010 1	10,359,927	41,009
,158,113,479	841 3,1	46,141,633	11,971,846	22,648
,779,702,979	1,087 2,6	96,264,790	83,438,189	76,947
,840,159,186	960 1,70	02,942,140 1	37,217,046 1	121,222
,806,306,131	424 1,80	00,450,261	5,855,870	8,124
,795,537,396	504 1,78	87,284,229	8,253,167	33,730
,458,940,653	319 1,45	58,429,009	511,644	63,197
nane << first	1 next >	last >> 10 m	esults	
1	page << first < prev	page << first < prev 1 next > I View: Bandwidth (Bytes)	page <<< first < prev 1 next > last >> 10 n	page << first < prev 1 next > last >> 10 results

Pre-Defined Searches

otifications 22	Home	Dashboard	Web Virus	Spyware	Web Filtering	Admin	Reports
Reports (
Time Zone GMT-06:00							
Time Period Custom							
From: 10-05-2016 00 · : 00 · + To: 1	11-05-2016	00 🗸 : 00 🗸]			🖌 Auto	Run Report
'ou have not created any custom reports.						Create	Report 쏬
Predefined Reports					Download	View as	
Application Analysis							
🕀 Bandwidth Analysis							
🕀 Block Analysis							
🕀 Browse Time Analysis							
Browser Analysis							
Category Analysis							
🛨 Facebook Analysis							
Group Analysis							
Host Analysis							
🛨 Legal Liability Analysis							
🕀 Malware Analysis							
Security Analysis							

Searches by Type

Application Analysis

- What were the top ten applications by browse time?
- What were the top ten applications that consumed the most bandwidth?
- What were the top ten blocked applications and activities?
- Who were the top ten blocked users and from which applications?
- Who were the top ten blocked users and for which activities?
- Who were the top ten users by activity?
- Who were the top ten users that consumed the most bandwidth on media sites?
- Who were the top ten users that consumed the most bandwidth on social networking sites?

Bandwidth Analysis

- What was the bandwidth consumed by major content type?
- What was the bandwidth consumed by category?
- Which were the top ten categories that consumed the most bandwidth?
- What were the top ten social networking sites by bandwidth?
- What were the top ten multimedia sites by hits?

- Which groups consumed the most bandwidth in streaming media?
- Which groups consumed the most bandwidth?
- Which hosts consumed the most bandwidth for the top ten users?
- Which of the organization's offices consumed the most bandwidth by internal subnets?
- Which of the organization's offices consumed the most bandwidth?
- Which users consumed the most bandwidth?
- Who were the top ten users by number of hits?
- Who were the top users of streaming media?

Block Analysis

- What adware was blocked?
- What malware was blocked?
- What spyware was blocked?
- What viruses were blocked?
- What were the top ten blocked sites by hits?
- Which were the top ten blocked categories?
- Which hosts were blocked the most for the top ten users?
- Which users were blocked the most by which rules?
- Which users were blocked the most?
- Which Web filtering rules generated the most blocks and who were the top users for those blocks?
- Which Web filtering rules generated the most blocks?

Browse Time Analysis

- What was the browse time for the most popular hosts?
- Which users spent the most time on possible business use sites?
- Which users spent the most time on possible productivity reduction sites?
- Which users spent the most time online?

Browser Analysis

- What were the top ten user agents?
- What were the top ten browsers?
- What were the top ten user agent strings by hits by external IP?
- What were the top ten user agent strings by hits by groups?

Category Analysis

- What was the total number of hits for all categories?
- Which were the top ten categories visited by each internal subnet?

Facebook Analysis

- Which were the top ten categories visited by each internal subnet?
- What were the top ten Facebook applications that consumed the most bandwidth?
- What were the top ten blocked Facebook applications and activities?
- Who were the top ten blocked users from which Facebook applications?
- Who were the top ten blocked users for which Facebook activities?
- Who were the top ten users that consumed the most bandwidth on Facebook?

Group Analysis

- Which were the top ten groups by hits?
- Which were the top ten groups that consumed the most bandwidth?
- Who were the top ten users with the highest browse time for the top ten groups?

Host Analysis

- What was the number of hits for each of the most popular hosts?
- What were the top ten hosts by hits?
- What were the top ten hosts visited for each category?

Legal Liability Analysis

- What was the legal liability risk by category?
- Who were the top ten users browsing for illegal downloads?
- Who were the top ten users browsing in adult categories?

Malware Analysis

- How many phishing blocks were there over time?
- How many threat blocks were there over time?
- Which were the top ten groups with the highest number of spyware blocks?
- What were the top ten blocked adware hosts?
- What were the top ten blocked phishing hosts?
- What were the top ten blocked spyware hosts?
- What were the top ten threats blocked over HTTPS?
- What were the top ten threats blocked per protocol?
- Who were the top ten users browsing spyware hosts?

- Who were the top ten users making outbound spyware requests?
- Who were the top ten users with the highest number of virus blocks?
- Which were the top ten categories where users were blocked by Web Reputation?
- Which were the theat types blocked by Web Reputation?
- Who were the top ten users with the highest number of Web Reputation blocks?
- How many Web Reputation blocks were there over time?
- What malware was blocked by AMP?

Security Analysis

- Which were the top ten blocked categories for malware?
- Which were the top ten categories where users were blocked for spyware?
- Who were the top ten users blocked by Outbound Content Control?
- Who were the top ten users for each risk category?

User Analysis

- Who were the top ten users that browsed the leisure categories?
- Who were the top ten users by hits?
- Who were the top ten users that browsed the most?

Filtering Reports

Filters enable you to refine searches by reporting attributes, metrics, or a combination of both. They can be used to narrow a predefined or saved search or applied when you are creating a search.

Activating and deactivating filters enables you to experiment to find the best set of filters to get the information you want, but only the active filters will be saved. You can also save the filters, separately from the search, as a filter set.

Adding Filters to a Search

Adding a Filter

Notifications	s 22 Home	Dashboard	Web Virus Spyware	e Web Filtering	Admin Reports
Reports					
	↓ <u>Search</u> ↓ <u>Tim</u>	e Analysis	d Search		
	Time Zone GMT-06:00 V Time Period Custom V From: 10-05-2016 10-02 00 Image: 11-05	2016			Auto Run Report
Choose Attribute	elect All Select None Add Filter	ictivate Save Fil	Select Add Filt	er	
Filler	Attribute Filter Choose	nternal IP	Choose is equa	al to Ente	er IP Address
	Add attribute filter Internal IP V is equal to		▼ 10.112.104.10	×	Add
	View first 10 User sorted by <u>Hits</u> (descending), a	nd their first 5	Host sorted by <u>Hits</u>	(descending) 🔽	Click Add
	Click Launch Search	Launch Search			

Procedure

Step 1 Click Add Filter.

Step 2 In the Select filter type drop-down list, choose the required type. The available options are

		Reports (
		Search Search Search Ime Analysis Search
		Time Zone GMT-06:00 ▼ Time Period Custom ▼ From: 10-05-2016 100 ↔ To: 11-05-2016 100 ↓ 00 ↓
•	Attribute Filter	Select All Select None Add Filter Remove Activate Deactivate Save Filter Set
•	Metric Filter	Select filter type:
•	Filter Set	Attribute Filter Metric Filter Filter Set
		View first 10 <u>Category</u> sorted by <u>Bandwidth (Bytes)</u> (descending), and their first
		Launch Search

Step 3 If you are adding an attribute filter:

- a. In the **Select attribute** list, click the required attribute.
- b. In the Select operator list, click the required operator. The available operators are:
 - contains
 - does not contain
 - is equal to
 - is not equal to
 - in list (equals)
 - is not in list (does not equal)
 - in list (contains)
 - is not in list (does not contain)
 - is null
 - is not null
 - starts with
 - does not start with

"Equal to" indicates a full match while "contains" indicates a partial match.

Step 4 If you are adding a metric filter:

- a. In the **Select metric** drop-down list, choose the required metric. The available options are:
 - Bandwidth (Bytes)
 - Browse Time (Min)
 - Bytes Received
 - Bytes Sent
 - Hits
- b. In the **Select operator** drop-down list, choose the required operator. The available options are:
 - = (equal to)
 - > (greater than)
 - >= (greater than or equal to)
 - <> (not equal to)
 - <= (less than or equal to)
 - < (less than)

Step 5 If you are adding an attribute or metric filter, enter a value in the box.

Step 6 Click Add to add and activate the filter

Activating and Deactivating Filters

Active filters are shown with a green triangle. Inactive filters are shown with a red warning sign.

To activate a filter, click the filter then click Activate.



To deactivate a filter, click the filter then click **Deactivate**.



You can click Select All to select all the filters or Select None to clear the selected filters.

Removing Filters

To remove a filter, click Remove. You will not be prompted to confirm your action.

Reporting Attributes

Reporting attributes are the main filter applied to searches to generate reports.

Attributes List

The contents of the majority of attributes are normalized to lower case. However, for some attributes you may wish to view the original string as entered by the user. Attributes listed with "Original" in parentheses are available in normalized and original form.

Adware

The name of the adware block.

AMP Threat Name

The name of the malware detected and blocked by AMP.

Application Activity

The activity or web application.

Application Name

The name of the web application.

Application Name With Unclassified

The name of the web application or an unclassified result.

Block Type

The pattern, specified in the filter, that generated the block. It can be one of the following:

- adware
- amp_malware
- category (HTTP)
- category (HTTPS)
- content type
- domain/URL
- file type
- phishing
- possibly unwanted applications (PUAs)
- spyware
- virus
- webrep

Note If more than one pattern is matched, the value of Block Pattern will be "multiple patterns."

Block Value

The string that matched the block pattern. It can be one of the following:

- adware name
- AMP threat name
- category name
- full URL
- MIME type
- name of the content type
- name of the file type
- phishing name
- possibly unwanted application (PUA) name
- spyware name
- virus name
- webrep name

Note Where the block was generated by an exception or by more than one pattern, the value of Block String will be "multiple strings."

Category

The web filtering category.

When changes are made to the categories, existing customer data is not migrated. When creating reports, you must include the old and new category names with the "Category in list" filter to ensure that all the results are returned. Composite reports do not need to be updated because they will inherit the settings of the included reports.

Pre-defined reports are updated for you. For example, the "User Analysis" report "Where were the Top 10 Users browsing in the Categories Shopping, Music, Cinema/TV and Sport" originally included the filter "Category in list music, cinema/tv, online shopping, sports." It now includes the filter "Category in list music, cinema/tv, online shopping, sports, entertainment, shopping, sports and recreation."

Cipher Suite

Authentication and encryption types, e.g. TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384, TLS_DHE_RSA_WITH_AES_256_CBC_SHA, SSL_RSA_WITH_RC4_128_SHA, TLS_ECDHE_RSA_WITH_RC4_128_SHA, TLS_RSA_WITH_AES_128_CBC_SHA256.

Company Name

Name of the company associated with the data traffic.

Company/Group

Group for the company users, e.g. Active Directory.

Company/User

User associated with a given data traffic.

Connector ID

ID of the Connector software being used to monitor users, e.g. AnyConnect.

Connector Mode

The mode reported by Connector.

Connector OS Name (Original)

The name of the operating system reported by Connector.

Connector OS Version (Original)

The version of the operating system reported by Connector.

Connector ReUse ID

Flag specifying the reuse of the user authentication headers associated with a given connector in TCP connections.

Connector Version

Logs the version of Connector used to embed the directory information. Can be used to easily find out which versions of Connector are deployed in your environment.

Content SHA256

A SHA256 hash of the content sent to or uploaded by the user.

Country Dst Code

The two-letter ISO code of the country where the web server is located, derived from its IP address.

Country Src Code

The two-letter ISO code of the country where the client web browser is located, derived from its IP address.

Day of Month

Used for time series plotting (1 to 31).

Day of Week

Used for time series plotting (monday to sunday).

Destination IP

The IP address of the remote web server.

Domain Username (Original)

The username under which the user is logged in to the domain.

External IP

The IP address that Cisco Cloud Web Security gets from the customer (also known as the egress IP address), for example 192.0.2.0. Alternatively, the subnet of the IP address that Cisco Cloud Web Security gets from the customer (also known as the egress IP address subnet), for example 192.0.2.0/24.

forwarded for

IP address used to locate the origin of a request. For example, if given there is no DC in Africa, users connect to Brazil and are forwarded. This attribute identifies that the user requests actually originated in Africa.

Group (Original)

The name of the directory group logged, for example WinNT://US\SALES.

Note Multiple directory groups can be logged for each user.

Group Domain

The name of the domain logged for the user.

Group Name Part (Original)

The name of directory group (not including either LDAP://<*domain*> or WinNT://<*domain*>), for example for WinNT://US\SALES, the group name part is SALES.

Host (Original)

The host part of the URL string, for example, for news.example.com/sport, the host is news.example.com.

Note Hosts are case insensitive.

Hour

Used for time series plotting.

Inbound File Extension

The file extension part of any inbound URL using the HTTP(S) protocol, for example, for index.html the file extension is html.

Inbound File Name

The filename part of any inbound URL using the HTTP(S) protocol, for example, index.html.

Internal IP

The IP address the Connector sees from the internal user, for example 192.168.2.10. Alternatively, the IP address subnet that the Connector sees from the internal user, for example 192.0.2.0/24.

Note If an internal user is routed through a NAT device before reaching the internal proxy, the IP address, or subnet, that arrives at the Connector is logged.

Malware

The name of the malware block.

Minute

Used for time series plotting (00 to 59).

Month

Used for time series plotting (january to december).

Outbound File Extension

The file extension part of any outbound POST using the HTTP(S) protocol, for example for resume.doc the file extension is doc.

Outbound File Name

The filename part of any outbound POST using the HTTP(S) protocol, for example resume.doc.

Path

The path part of the URL string, for example, for news.example.com/sport, the path is /sport.

Pattern Name

See the Block Value attribute.

Pattern Type

See the Block Type attribute.

Phishing

The name of the phishing block.

Policy Violation

The block value where a web filtering rule resulted in a block.

Port

Port number of web request, for example, 80 or 443.

Protocol

- FTP
- HTTP
- HTTPS

PUA

Possibly Unwanted Application name.

Query

The query part of the URL string, for example, for

```
http://www.example.com/search?hl=en&q=free+screensavers&btnG=Example+Search&meta=&aq=f&oq=, the
query is hl=en&q=free+screensavers&btnG=Example+Search&meta=&aq=f&oq=.
```

Note Using this attribute will increase the time that reports take to generate by a considerable amount.

Referrer Host (Original)

The host part of the referrer URL string, for example, for news.example.com/sport, the host is news.example.com.

Referrer Path

The path part of the referrer URL string, for example, for news.example.com/sport, the path is /sport.

Referrer Port

Port number of referrer, for example 80 or 443.

Referrer Protocol

- FTP
- HTTP
- HTTPS

Referrer Query

The query part of the referrer URL string, for example, for

http://www.example.com/search?hl=en&q=free+screensavers&btnG=Example+Search&meta=&aq=f&oq=, the
query is hl=en&q=free+screensavers&btnG=Example+Search&meta=&aq=f&oq=.

Referrer Second Level Domain

Normally the referrer organization, for example, in www.example.com, the second level domain is example.

Referrer Top Level Domain

Normally the last part of the referrer domain, for example, com, net, org, gov, and co.uk.

Referrer URL (Original)

The full referrer URL string.

Request Content MD5

The MD5 checksum of the user request.

Request Content Type (Original)

The request MIME type, for example, image/gif, application/pdf, text/html, application/EDI-X12.

Request Major Content Type

The type of request content, for example, if the response content type is application/pdf, then the corresponding major content type is application. Examples include:

- application
- audio
- image
- text
- video

Request Method (Original)

- CONNECT
- GET
- POST

Request Version (Original)

The request version, for example, HTTP/1.0 or HTTP/1.1.

Response Content Type (Original)

The response MIME type, for example, image/gif, application/pdf, text/html, application/EDI-X12.

Response Major Content Type

The type of response content, for example, if the response content type is application/pdf, the corresponding major content type is application. Examples include:

- application
- audio
- image
- text
- video

Response Status Code

Enables you to filter by the response status code, for example, to find all web requests to pages that did not exist, you can filter by 404.

Response Version (Original)

The response version, for example, HTTP/1.0 or HTTP/1.1.

Risk Class

The superclass under which the risk is grouped:

- possible business usage
- possible productivity reduction
- heavy bandwidth usage
- potential legal liability
- potential security risk

Rule Action

There are five rule actions you can choose from:

- allow
- authenticate
- block
- warn
- inspect

Note If a website does not respond to a request, no Rule Action is assigned, but the request is still stored.

Rule Engine

The rule engine that generated the rule action:

- policy evaluator
- scanlet

Rule Name (Original)

The Cisco ScanCenter policy rule name.

Rule Stage

The part where the rule was applied, e.g. response_headers, response_body_start, reqmod.'

Second Level Domain

Typically the organization, for example, in www.example.com, the second level domain is example.

SHA256 Source

Indicates whether the Content SHA256 is a hash of the HTTP request post data or response data: request, response, or N/A.

Spyware

The name of the spyware block.

Threat Type

Each record can include multiple threat types from the following:

- adware
- category
- content type
- extension
- file match
- filter protocol
- phishing
- possibly unwanted applications (PUAs)
- quota
- regular expression
- spyware
- virus

Time Stamp

The time at which the rule action was applied in minutes and seconds. Available only in Detailed Search.

Top Level Domain

Typically the last part of the domain, for example, com, net, org, gov, and co.uk.

URL (Original)

The full URL string.

User (Original)

The logged username (if applicable). It can be in the form of WinNT://<username> or a custom text name.

User Agent (Original)

The complete user agent string, for example, Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1).

User Agent Application Name

The user agent application name, for example, Mozilla. See User Agent.

User Agent Application Version

The user agent application version, for example, 4.0. See User Agent.

User Agent Comp Platform

The user agent platform token, for example, Windows NT 5.1. See User Agent.

User Agent Comp Version

The user agent version token, for example, MSIE 7.0. See User Agent.

User Agent Compatibility

The user agent compatibility flag, for example, compatible. See User Agent.

User Domain Name

The domain where the user that made the request belongs.

User Domain Name Part

A lowercase substring of the user domain name.

Via

A list of IP addresses identifying the intermediate proxies processing the user request.

Virus

The name of the Virus block, for example, Trojan.Downloader.abg.

Web Reputation Threat

See the Block Value attribute, given Block Type is webrep.

Year

Used for time series plotting.

Portal 2.0

Overview

Portal 2.0 offers you more flexibility in customizing the data you are shown and drilling down into metrics for faster response and greater efficiency when analyzing your traffic. To view the next generation portal, click the **Launch Portal** button on the Cisco ScanCenter Home page.

Cli	ck on Home and click the Launch Portal		
Launch Portal for	Dashboard, Drilldown and A	Analysis	
Users	Data Usage 🔻	Hosts	Data Usage
user 97	. 924 Mb	tacebook.com	924 N
	723 MB		

Note Some functionality may not be present in your account, depending on your region, vendor, and licensing. Contact your Cisco sales representative for further information.

Near the upper left corner of the page, click the main menu icon to choose:

TOP OVERVIEW DASHBOARD				
FROM 10/MAY/2016 16:39 🛗 TO 11/MAY/2016 16:39	Ê			×
Bandwidth 74.12 GB Blocks		÷,	✿	5
	DASHBOARD	ANALYSIS	PREFERENCES	PORTAL 1.0

- Dashboard—Opens the Top Overview Dashboard page.
- Analysis—Opens the reporting pages: Quick Analysis, Detailed Analysis, and Saved Reports. Saved Reports include predefined reports (such as bandwidth analysis, application analysis, and block analysis) and favorite reports (custom report templates that have been created and saved).
- **Preferences**—Opens the User Preferences page where you can select your time zone, date format, and preferred language.
- **Portal 1.0**—Opens the Cisco ScanCenter Home page. Portal 2.0 is implemented in phases so that you can continue using Portal 1.0.

Dashboard

	IEW DASHBOARD				9 0
FROM 10/MAY/2016 16	TO 11/MAY/2016 16	Time Zone			Edit widgets
Bandwidth BAYDWIDTH Widgets are customiz	74.12 GB Blocks Traffic Allowed	220,849 нітs Traffic Blocked			
The horizontal timeline Above the horizontal ti Below the horizontal to Drill down for more sp	e shows the number of blocks and a imeline are filters you can click to di imeline are widgets that display data becifics by clicking on any information	amount of bandwidth during each hour. — isplay the blocked (Blocks) or allowed (Bar a metrics you choose to view.	idwidth) traffic.		
16:00 18:00 BLOCKS	20:00 22:00 0	0:00 02:00 04:00	06:00 08:00	10:00	12:00 14:00 16:00
User	Bandwidth 🗸	Application Name With Unc	Bandwidth 🗸	Category	Bandwidth -
10.112.106.109	4.3GB	Unknown	30.06GB	Streaming Vide	o31.01GB
10.112.106.2	3.59GB	Netflix	18.56GB	Infrastructure and Co	7.47GB

The Top Overview Dashboard shows an overview of web activity in your network over the last 24 hours.

- The horizontal timeline shows the number of blocks and amount of bandwidth during each hour.
- Above the horizontal timeline are filters you can click to display the blocked (Blocks) or allowed (Bandwidth) traffic.
- Below the horizontal timeline are widgets that display data metrics you choose to view.
- Widgets are customizable.
- Drill down for more specifics by clicking on any information bar within the widgets.

Procedure

- Step 1 In the Portal 2.0 main menu, select Dashboard.
- **Step 2** Select a time zone from the drop-down list. The dashboard time period covers the previous 24 hours.
- **Step 3** You may choose to view data for all traffic allowed or blocked by using the selectable filters above the horizontal timeline.
- **Step 4** Within each widget, from the upper-right drop-down list, choose a metric to sort the data shown.
- **Step 5** (Optional) Click **Edit widgets** to make widget changes. Click **Save** to save your changes for the current admin user.
 - a. Add a widget by clicking **New widget**.
 - b. Remove a widget by clicking its circled **x** icon.
 - c. To reorder the widgets, click the directional icon to drag-and-drop each widget.
 - d. Edit a widget by clicking its pencil icon. You can then choose its chart type.

Drill Down



Drill down into the widgets for more focused information. For example, to view more detail on a particular user, click on that user listed within a widget. A new page is displayed showing information related only to that user. A user filter is added to the filters header. Then, to filter the data shown on that user, click on any information within the widgets. The widgets are updated and a second filter is added to the filters header. At any point, you can click the circled **x** icon in any filter to remove it from the header and update the data shown. Furthermore, if desired, click on more information to add a third filter to the filters header, which then automatically opens the Detailed Analysis page.



Quick Analysis Reports

Procedure

Step 1 In the Portal 2.0 main menu, select **Analysis** and click the **Quick** analysis tab.



- **Step 2** Select a time zone from the drop-down list.
- **Step 3** Select a predefined time period, or click **Custom** and enter the required start and end dates and times:
 - Click the **From** box to choose a start date.
 - Click the clock icon to choose a start time using the hour and minute selector arrows. The time is shown using the 24-hour clock.
 - Click the **To** box to choose an end date.
 - Click the clock icon to choose an end time using the hour and minute selector arrows.



Step 4 Select a type of report:

- Single-level report with one reporting attribute
- Dual-level report with two attributes
- Time-based trending report
- User audit report

Single attribute report
Dual attribute report
Time based report
User audit report

Step 5 For the type of report, select at least one reporting attribute.

Select an attribute

Select an attribute	
Suggested Attributes	~
Block Value	
Category	
Group	
Internal IP	
Threat Type	
User	~

Step 6 For the type of report, select at least one sorting metric. Sorted by

Select a metric	
Bandwidth (Bytes)	
Browse Time (Min)	
Bytes Received	
Bytes Sent	
Hits	
Blocks	

Step 7 Select a number from 1 to 20,000 of records to be shown.

Number of records shown	
10	×

Step 8 Select a filter set from the drop-down list. If the list is empty, create and add filters.

Select a filter set	-
	Select Internal IP
Select an attribute or	or User
Suggested Attributes	~
Block Value	
Category	
Group	
Internal IP 🧖	
Threat Type	
User	~
Select a filter set	-
Select an attribute or	a metric
	Select
Select an operator	Select is equal to
Select an operator	Select is equal to
Select an operator is equal to is not equal to	Select is equal to
Select an operator is equal to is not equal to is null	Select is equal to
Select an operator is equal to is not equal to is null is not null	Select is equal to
Select an operator is equal to is not equal to is null is not null contains	Select is equal to
Select an operator is equal to is not equal to is null is not null contains does not contain	Select is equal to
Select an operator is equal to is not equal to is not null contains does not contain starts with	Select is equal to
Select an operator is equal to is not equal to is not null contains does not contain starts with Internal IP	Select is equal to
Select an operator is equal to is not equal to is null contains does not contain starts with Internal IP is equal to	Select is equal to
Select an operator is equal to is not equal to is not null contains does not contain starts with Internal IP is equal to 10.112.108.47	Select is equal to

- a. Select an attribute or a metric.
- b. Select an operator.
- c. Enter a value.
- d. Click **Add** to add the filter you have created to the current set.
- e. Optionally, repeat these steps to create and add more filters as needed to the current set.
- f. To enable or disable filters, click the corresponding toggle switch to the right of that filter.
- g. To delete individual filters out of a set, click the circular **x** button to the right of that filter.
- h. To save the set, click **Save filters** and enter a name for the filter set.

Filter Name	Click Save If you wish to save this filter set, Name the Filter Set and
Back Save	Click Save

Step 9 Click **Search** to generate and display the results table.

	QUICK	DETAILE	Ð					8	Q	1
FROM	11/MAY/201	6 12:34 🛗	ТО	12/MAY/2016 12:34 🛗			Show saved repo	orts	Searc	h
Custo	m	▪ Am	erica/C	hicago	•				<u></u>	
10.1	112.108.47 INTERNAL IP	•					~			
Single	e attribute repor	t	s	elect an attribute						
Dual	attribute report			Block Value	•					
			S	Papdwidth (Putes)						
Time	based report			bandwidth (bytes)						
User	audit report		N	10						
Select	t a filter set	-					All filters)
				Internal IP	is equal to	10.112.108.47) ×)

- **Step 10** Optionally, click the sorting arrows in any column header to sort the table rows according to the data in that column.
- **Step 11** Optionally, rearrange the columns by clicking and dragging by their headers.

Click the + sign in the filter header to expand or minimize the section for modifying the report or filter parameters.

To save yourself time spent having to replicate the search, click **Save Report**, enter a descriptive name, and click **Save**. This saves the report search template you have created to the Favorite Reports section of the Saved Reports page.



Click Export to download the report to your device as a CSV or PDF file.

Quick Analysis Reports

Procedure

- Step 1 In the Portal 2.0 main menu, select Analysis and click the Quick analysis tab.
- **Step 2** Select a time zone from the drop-down list.
- **Step 3** Select a predefined time period, or click **Custom** and enter the required start and end dates and times:
 - Click the **From** box to choose a start date.
 - Click the clock icon to choose a start time using the hour and minute selector arrows. The time is shown using the 24-hour clock.
 - Click the **To** box to choose an end date.
 - Click the clock icon to choose an end time using the hour and minute selector arrows.
- **Step 4** Select a type of report:
 - Single-level report with one reporting attribute
 - Dual-level report with two attributes
 - Time-based trending report
 - User audit report
- **Step 5** For the type of report, select at least one reporting attribute.
- **Step 6** For the type of report, select at least one sorting metric.
- **Step 7** Select a number from 1 to 20,000 of records to be shown.
- **Step 8** Select a filter set from the drop-down list. If the list is empty, create and add filters.
 - a. Select an attribute or a metric.
 - b. Select an operator.
 - c. Enter a value.
 - d. Click Add to add the filter you have created to the current set.
 - e. Optionally, repeat these steps to create and add more filters as needed to the current set.

- f. To enable or disable filters, click the corresponding toggle switch to the right of that filter.
- g. To delete individual filters out of a set, click the circular **x** button to the right of that filter.
- h. To save the set, click **Save filters** and enter a name for the filter set.
- **Step 9** Click **Search** to generate and display the results table.
- **Step 10** Optionally, click the sorting arrows in any column header to sort the table rows according to the data in that column.
- **Step 11** Optionally, rearrange the columns by clicking and dragging by their headers.

Click the + sign in the filter header to expand or minimize the section for modifying the report or filter parameters.

To save yourself time spent having to replicate the search, click **Save Report**, enter a descriptive name, and click **Save**. This saves the report search template you have created to the Favorite Reports section of the Saved Reports page.

Click **Export** to download the report to your device as a CSV or PDF file.