



CISCO UMBRELLA

Reporting

[Abstract](#)

Use Cisco Umbrella's reports to gain a better understanding of your Umbrella usage. Gain insights into request activity and blocked activity, determining which identities are generating requests that are being blocked. Reports help build actionable intelligence in addressing security threats including changes in trends over time.

Contents

Available Reports	2
Scheduling Reports	6
Schedule a Report	7
Understanding Security Categories	11
Security Overview Report	14
What is the Security Overview Report?	14
Accessing the Security Overview Report	14
Events – Security Blocks and All Security Events	18
Most Active Destination, Identity, or Request Type	20
Active Identities	22
Security Activity Report	23
What is the Security Activity Report?	23
Activity Search Report	32
What is the Activity Search Report?	32
View the Activity Search Report	32
Search for Activity	37
Identities Report	41
Accessing Identities Reports	41
Understanding an Identities Report	43

Getting Started with Reports

Use Cisco Umbrella's reports to gain a better understanding of your Umbrella usage. Gain insights into request activity and blocked activity, determining which identities are generating requests that are being blocked. Reports help build actionable intelligence in addressing security threats including changes in trends over time.

See also:

- [Report Retention](#)
- [Exporting Report Data to CSV](#)
- [Scheduling Reports](#)
- [Understanding Security Categories](#)

Available Reports

- [Security Overview](#)—Gives you a snapshot of your environment's security activities.
- [Security Activity](#)—Security-related activity in your environment, including malware, phishing, and all other security categories over the selected time period. Filterable by identity, destination, source IP, and security category.
- [Activity Search](#)—Activity from the identities in your environment over a selected time period. Filterable by identity name, destination, source IP, response, content category, and security category.
- [Destinations](#)—Lists the most active destinations within your dashboard for all identities, and that allows you to go further and find out how the traffic for this destination from your Identities compares to the traffic from all of the Umbrella global network.
- [Identities](#)—Lists your identities in the order of which is most active, then allowing you to drill down to find out more about that specific identity and what destinations they have visited, whether those destinations are malicious or not, and a trend of their overall traffic.
- [Cloud Services](#)—Overview of cloud services accessed by your organization over the selected time period. Filterable by cloud service name, identity, and classification.
- [Total Requests](#)—Total requests for destinations from your organization over the selected time period. Filterable by identity.
- [Activity Volume](#)—Total queries within your organization broken down by security categories and results over the selected time period. Filterable by identity. This report has two views: Snapshot (table) and Trend Over Time (graph).
- [Top Domains](#)—A list of the most requested domains within your organization over the selected time period. Filterable by identity, response, destination, content category, and security category.
- [Top Categories](#)—A list of the top content categories for your organization over the selected time period. Filterable by identity and response.
- [Top Identities](#)—A list of the top traffic-generating Identities over the selected time period. Filterable by identity and destination.

- [Admin Audit Log](#)—A record of any configuration changes made to your settings by any of your Umbrella administrators.

Report Retention

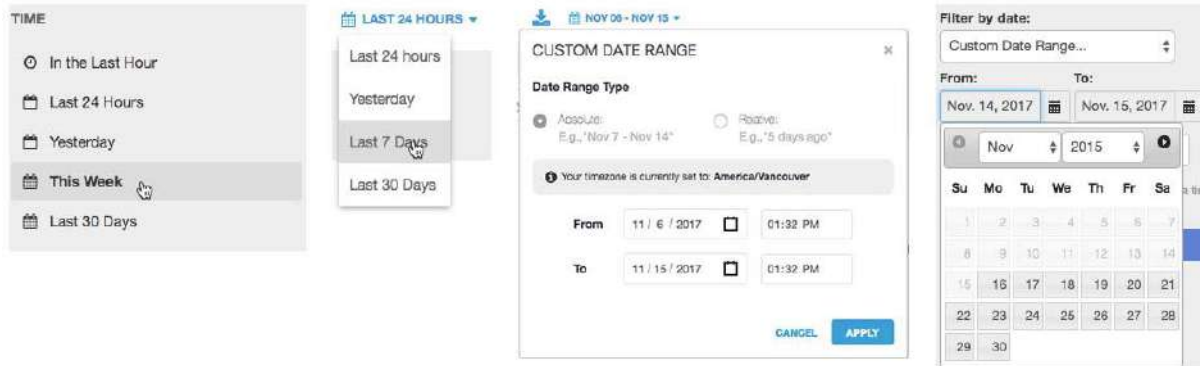
The reporting of information begins as soon as you start sending traffic to Umbrella.

The following reports are retained for two calendar years:

- Total Requests
- Top Domains
- Top Categories
- Top Identities

Activity Volume is retained for one calendar year.

You can review and filter reported data on various timelines. Timelines vary depending on the report, from the last hour to the last thirty days, and in some cases custom date ranges in increments of time—up to 30 or 90 days—going back one to two years.



The following reports are limited to a 30-day search window:

- Top Domains
- Total Requests
- Security Activity
- Activity Search

Note: *Umbrella does not retain Security Activity or Activity Search data for more than 30 days.

Admin Audit log Retention

The Admin Audit log retains data for one year. You can access data in three month increments. For more information, see the [Admin Audit Log Report](#).

Exporting Report Data to CSV

Some reports let you export the results of a query to the CSV format. This lets you create other reports and graphs by feeding this data to other tools.

Note: The timezone of exported data is always UTC, regardless of the user's timezone.

Exportable reports:

- Activity Search
- Cloud Services
- Top Domains
- Top Categories
- Top Identities

1. From the top of the report, click Download.



2. Give your report a good meaningful title, add the number of rows of data you want returned and click Export.

Note: Data is limited to 1,000,000 rows when exporting to CSV. If your report exceeds 1,000,000 rows, consider re-running the report with a shorter smaller time or with a more granular filter. It's a good idea to check the last row of your first report, then re-run the report from that time period for the next chunk of data.

Export Report to CSV ✕

Exporting the results of a report may take some time and will be done via a background process. Note: The timestamps in the exported CSV report will reflect UTC.

Report Title

Results Row Limit (1000000 max)

CANCEL
EXPORT

- When you click Export, you are taken to the Exported Reports page where you can download your CSV file.

Reporting / Management
Mike ▾

Exported Reports

Description	Date	Expires	Report Type	Download	
Exported Report Data Nov. 1, 2017	Nov. 17, 2017 1:03:39 PM	in 3 months	Top Domains		

- Click the Download icon.
Your CSV is automatically downloaded.



Scheduling Reports

Umbrella lets you set up a schedule of recurring reports that it emails to you from your Umbrella dashboard. This message includes an HTML version of the report, an attached CSV file containing the entire data set, and a link to a live version of the same report. See [Schedule a Report](#).

Previous Calendar Day Security Activity Report



Scheduled Reports <scheduled-reports-feedback@opendns.com> sent by [1 more](#)

Tuesday, November 14, 2017 at 6:30 AM

To: Mike

Good morning!

Your scheduled Security Activity report showed no activity for the specified time period.

[Click here to view a live version of this report in the Umbrella Web Dashboard.](#)

Security Activity - Default Site - cnn.com - All IPs - Nov 13, 2017 12:00 AM PST - Nov 13, 2017 11:59 PM PST (UTC-08:00) - All Security Categories

Security Activity				
Time	Resp.	Destination	Category	Identity
No results found.				

[Click here to manage this scheduled report.](#)

You can schedule the following reports:

- Activity Search—Activity in your environment over the selected time period. Filterable by Identity, destination, source IP, response, content category, and security category.
- Security Activity—Security-related activity in your environment, including malware, command and control, and all other security categories over the selected time period. Filterable by identity, destination, source IP, and security category.
- Cloud Services—Overview of cloud services accessed by your organization over the selected time period. Filterable by cloud service name, identity, and classification.
- Activity Volume—Total queries within your organization broken down by security categories and results over the selected time period. Filterable by identity.
- Total Requests—Total requests for destinations from your organization over the selected time period. Filterable by identity.
- Top Domains—Total requests for destinations from your organization over the selected time period. Filterable by identity.
- Top Categories—A list of the top content categories for your organization over the selected time period. Filterable by identity and response.
- Top Identities—A list of the top traffic-generating Identities over the selected time period. Filterable by identity, categories and security categories.
- Executive Summary—A graphical summary detailing blocked security threats, top security events, and cloud service use on your networks.

IMPORTANT NOTE: Cisco Umbrella uses MailGun as the service to deliver email. Some mail filters, either at the local level or even at a transport layer (like an ISP) may block communications from MailGun as marketing-related spam. If after scheduling your reports you do not receive them, check the spam filter at your mail server gateway. Whether your mail server gateway is hosted locally or in the cloud, it's likely the email was quarantined at that level.

Umbrella sends its reports from: scheduled-reports-feedback@opendns.com.

A scheduled report has a limit of 10,000 rows of information—one row per DNS request.

Schedule a Report

1. Navigate to Reporting > Management > Scheduled Reports and click Add. The Schedule wizard opens, listing the reports you can schedule. To see an example of a report, click See a sample report.

Reporting / Management
Scheduled Reports 1 Add

Q Type a report name, recipient, report type, or frequency... Advanced

1. Report Type 2. Filter 3. Recipients 4. Schedule 5. Description

- Activity Search** [See a sample report](#)
Activity in your environment over the selected time period. Filterable by Identity, destination, source IP, response, content category, and security category.
- Security Activity** [See a sample report](#)
Security-related activity in your environment, including malware, botnet, and all other security categories over the selected time period. Filterable by Identity, destination, source IP, and security category.
- Cloud Services** [See a sample report](#)
Overview of cloud services accessed by your organization over the selected time period. Filterable by Cloud Service Name, Identity, and Classification.
- Activity Volume** [See a sample report](#)
Total queries within your organization broken down by security categories and results over the selected time period. Filterable by Identity.
- Total Requests** [See a sample report](#)
Total requests for destinations from your organization over the selected time period. Filterable by Identity.
- Top Domains** [See a sample report](#)
A list of the most requested domains within your organization over the selected time period. Filterable by Identity, response, destination, content category, and security category.
- Top Categories** [See a sample report](#)
A list of the top content categories for your organization over the selected time period. Filterable by Identity and response.
- Top Identities** [See a sample report](#)
A list of the top traffic-generating Identities over the selected time period. Filterable by Identity, Categories and Security Categories.
- Executive Summary** [See a sample report](#)
A graphical summary detailing blocked security threats, top security events, and cloud service use on your networks.

CANCEL NEXT

2. Select the report you'd like scheduled and emailed and then click Next.

3. In step 2 Filter, select filters and then click Next.

It's important to add good filters so that you receive only the data that you need and that your reports don't exceed 10,000 rows. You want your scheduled report to be digestible and actionable by recipients. If you choose not to add any filters, the report will apply to all traffic types for that report across your entire environment. In Step 2 of the wizard, you can apply filters for an Identity and other key filters such as the security category or content setting, or the destination. The filters are different for each report type but match the filters that are already associated with the reports themselves. For example, if you select the Security Activity report, you can filter on Identity, Destination, Source IP, and Security Categories.

1. Report Type 2. Filter 3. Recipients 4. Schedule 5. Description

Choose the filters you'd like to apply to this scheduled report. By default, if no filters are configured, the report will apply to all traffic across your entire environment.

Filter by Identity: Select...

Filter by Destination: Enter a domain

Filter by Source IP: Enter an internal or external IP

Filter by Security Categories: No Security Category Filters Selected

CANCEL PREVIOUS NEXT

Note: If you are adding a destination (a domain) or a source IP address, press Enter after entering your filter or it will not save.

Once you've added filters, the report settings should look similar to the following example.

1. Report Type 2. Filter 3. Recipients 4. Schedule 5. Description

Choose the filters you'd like to apply to this scheduled report. By default, if no filters are configured, the report will apply to all traffic across your entire environment.

Filter by Identity: Demo

Filter by Destination: domain.com

Filter by Source IP: 123.123.123.123

Filter by Response: Allowed

Include All Traffic:

Filter by Categories: All Categories Selected

Filter by Security Categories: Phishing

CANCEL PREVIOUS NEXT

NOTE: Most reports will show Filter by Security Categories, but the Cloud Services report shows Filter by Classifications.

- In Step 3 of the wizard, add email address for recipients of the report and then click Next. Enter as many recipients as you like, pressing Enter, Space, Tab, or entering a comma or semicolon after each email.

Email addresses do not have to be associated with existing administrators of the system. You can add any email address, including mailing lists and recipients outside your organization; therefore, you should use caution to ensure you don't add anyone who shouldn't be receiving the data within the report you chose.

- In Step 4 of the wizard, schedule the frequency of when you'd like the report to be sent and click Next. Frequency can be set to Daily, Weekly, or Monthly. If the frequency is Daily, it can be either the previous calendar day or the last 24 hours from before the hour the report is scheduled to be delivered.

If the frequency is Weekly, it can be set to be previous calendar week (from the date the report is scheduled to be delivered), or the last seven days. The time of delivery will default to the logged in user's Umbrella's timezone, but if the recipients are in different time zones, you can configure them to receive reports during their work hours. If the recipient is an administrator or helpdesk staff expected to take action on information in the report, we recommend setting up a second report with the delivery time adjusted for their region.

Note: Attempting to schedule a report for a time on the current day, regardless of whether the report is scheduled in the future from the current time on that same day, will result in the report being scheduled on the next day at the earliest for weekly and monthly frequencies.

6. In Step 5 of the wizard, give your report a good descriptive name and then click Save. After you save the report, a summary of the report appears.

Name	Report Type	Frequency	Next Delivery
Previous Calendar Day Security Activity R...	Security Activity	Daily	1/9/2018 3:00 PM UTC-08:00

Review, Change or Delete a Scheduled Report

1. Navigate to Reporting > Management > Scheduled Reports and click a listed scheduled report. The wizard opens and lists information about the scheduled report, including who created the report and when, as well as the last time the report was modified and by whom.

Name	Report Type	Frequency	Next Delivery
Previous Calendar Day Security Activity Report	Security Activity	Daily	1/9/2018 3:00 PM UTC-08:00

1. Report Type
2. Filter
3. Recipients
4. Schedule
5. Description

Report type: Security Activity

Created by: Robi, 11/2/2017 2:32 PM

Last modified by: Robi, 11/2/2017 2:32 PM

Next delivery: 1/9/2018 3:00 PM

Last delivery: 1/8/2018 1:01 PM

[DELETE](#)

Security Activity				
Date	Time	Destination	Security Category	Identity
Sep. 28, ...	2:25:12 PM	http://rs.gwallet.co...	Malware	CGUILLOR-M
Sep. 28, ...	2:19:39 PM	d.href.asia	Drive-by Downl...	forwarder01.s
Sep. 28, ...	2:19:05 PM	http://vpaid.reelfeed...	Malware	forwarder01.s

[CANCEL](#)
[NEXT](#)
[SAVE](#)

NOTE: If you have not received the report after the next scheduled delivery date, check the spam filter at your mail server gateway, whether that's hosted locally or hosted in the cloud, as it's likely the email was quarantined at that level.

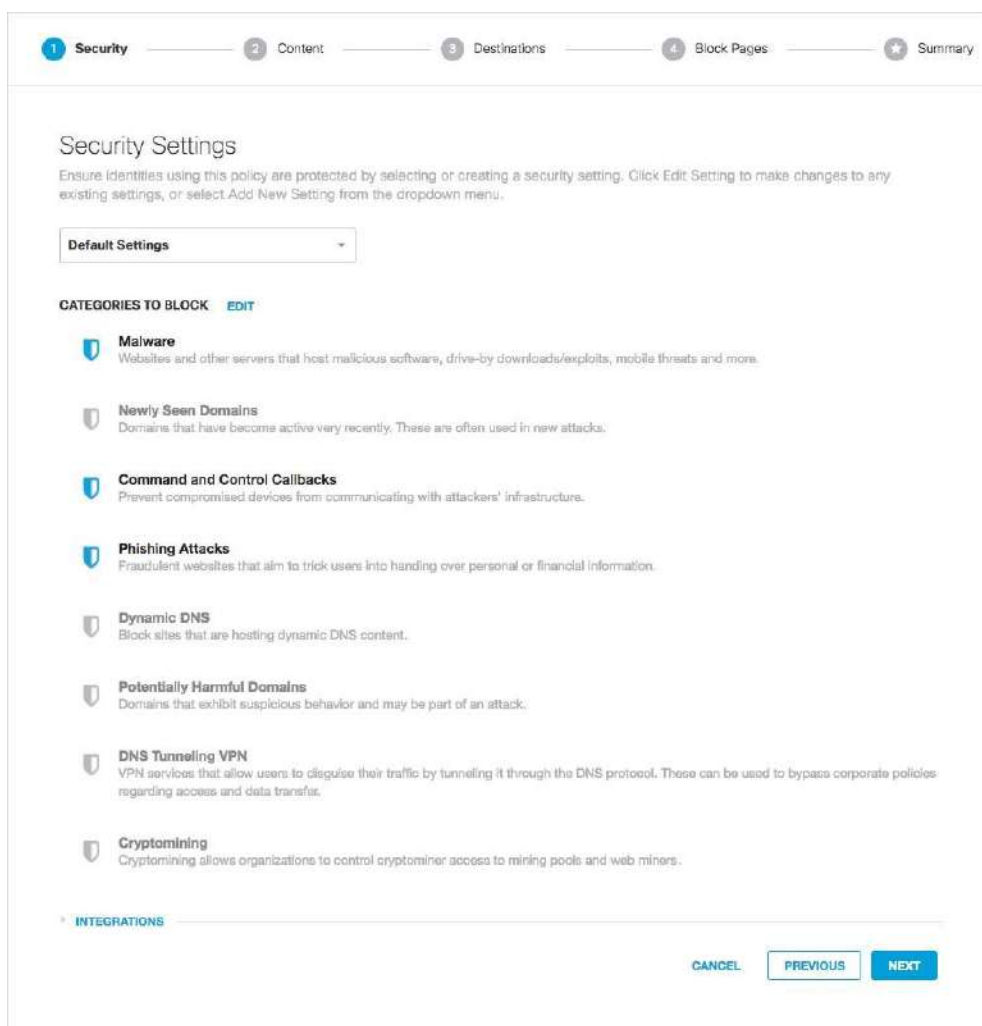
2. Click Next to make changes.
3. Click Delete to delete the scheduled report.

Understanding Security Categories

Cisco Umbrella's Security Categories are categories of security defence that Umbrella provides. We've categorized security threats to give you more control over exactly what you'd like to enable and report.

These categories are used in creating policies and in viewing reports for when things are blocked, or even when they are not. If a domain matches a security category but is not set to be blocked by a security setting in your policy, this is still reported as an allowed visit to a destination that matches one of the security categories. All of these security categories are important in understanding our other Umbrella reports, starting with the Security Overview Report.

1. Navigate to Policies > Management > All Policies and click through the wizard until you reach the Security Settings page.



The screenshot shows the 'Security Settings' configuration page in the Cisco Umbrella interface. At the top, there is a progress bar with five steps: 1. Security (active), 2. Content, 3. Destinations, 4. Block Pages, and 5. Summary. Below the progress bar, the page title is 'Security Settings' with a subtitle: 'Ensure identities using this policy are protected by selecting or creating a security setting. Click Edit Setting to make changes to any existing settings, or select Add New Setting from the dropdown menu.' A dropdown menu is set to 'Default Settings'. Under the heading 'CATEGORIES TO BLOCK' with an 'EDIT' link, there is a list of security categories, each with a shield icon and a description:

- Malware**: Websites and other servers that host malicious softwares, drive-by downloads/exploits, mobile threats and more.
- Newly Seen Domains**: Domains that have become active very recently. These are often used in new attacks.
- Command and Control Callbacks**: Prevent compromised devices from communicating with attackers' infrastructure.
- Phishing Attacks**: Fraudulent websites that aim to trick users into handing over personal or financial information.
- Dynamic DNS**: Block sites that are hosting dynamic DNS content.
- Potentially Harmful Domains**: Domains that exhibit suspicious behavior and may be part of an attack.
- DNS Tunneling VPN**: VPN services that allow users to disguise their traffic by tunneling it through the DNS protocol. These can be used to bypass corporate policies regarding access and data transfers.
- Cryptomining**: Cryptomining allows organizations to control cryptominer access to mining pools and web miners.

At the bottom of the page, there is an 'INTEGRATIONS' section and three buttons: 'CANCEL', 'PREVIOUS', and 'NEXT'.

By default, three security categories are enabled, Malware, Command Control Callbacks and Phishing. In general, we suggest that you find the right combination for your organization's policies—some identities may require a more strict security posture than others. However, there are some categories we recommend enabling for most or all identities, unless you are simply testing to see what Umbrella would have blocked.

NOTE

This does not mean you shouldn't use those categories in your policy, just that you should monitor your reports to see if these categories make sense to apply to your identities.

Categories

- Malware—Block requests to access servers hosting malware and compromised websites through any application, protocol, or port. *Recommended to be ON.*
- Newly Seen Domains—Detect domains that have been seen being queried for the first time very recently. For more important information on this category, [read here](#). *Off by default.*
- Command Control Callbacks—Prevent compromised devices from communicating with hackers' command and control servers via any application, protocol or port and help identify potentially infected machines on your network. *Recommended to be ON.* Note: this category was previously called 'botnet' in earlier versions of Umbrella. We've changed the name to better reflect what this security category prevents; the blocked destinations are the command and control for the botnet itself.
- Phishing Attacks—Protect users from fraudulent hoax websites designed to steal personal information *Recommended to be ON.*
- Dynamic DNS—Block sites that are hosting dynamic DNS content. *Off by default.*
- Potentially Harmful Domains—Domains that exhibit suspicious behavior and may be part of an attack. This category has a higher risk of unwanted detections. [Read more here](#). *Off by default.*
- DNS Tunnelling VPN—VPN services that allow users to disguise their traffic by tunnelling it through the DNS protocol. These can be used to bypass corporate policies regarding access and data transfer. *Off by default.*
- Cryptomining—Allows you to block identities from accessing known cryptomining pools where miners group together and share resources—processing power—to better gather and share cryptocurrencies, and from known web cryptomining source code repositories. By blocking cryptomining, Umbrella protects you from the recent emergence of cryptomining malware. *Off by default.*

All of these security categories are important in understanding our other Umbrella reports, starting with the Security Overview Report.

Integrations

There is also a sub-category—Integrations—that's available for some packages. The Integrations security category consists of domains that have been added to Umbrella through individual integrations. For more about integrations, read [here](#).

INTEGRATIONS

- Check Point**
Domains sent to Umbrella via Check Point Event notifications, based on the notification settings enabled within the Check Point dashboard.
- Cisco AMP Threat Grid**
Malicious domains retrieved from the Cisco AMP Threat Grid API for your organization-specific and global data sets.
- FireEye**
Domains sent to Umbrella via FireEye Event notifications, based on the notification settings enabled within the FireEye dashboard.
- ThreatConnect**
Domains sent to Umbrella via ThreatConnect Event notifications, based on the notification settings enabled within the ThreatConnect dashboard.
- ThreatQ**
Domains sent to Umbrella via ThreatQ Event notifications, based on the notification settings enabled within the ThreatQ dashboard.

Security Overview Report

What is the Security Overview Report?

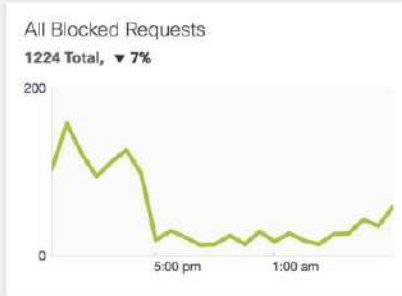
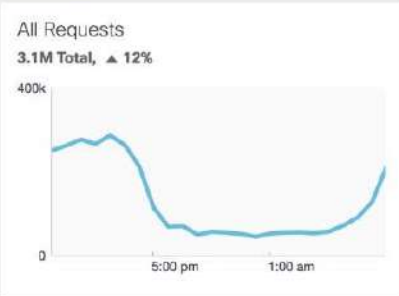
To help gain a better perspective of security-related activity within your Umbrella environment, the Security Overview report provides you with easy to read charts of your organization's identities and their activity. You can easily see what's going on with groups of identities and the types of internet requests they're making and where any problems might be popping up. Then you can pivot from this Security Overview report to more advanced reports and determine if there are security risks to your environment that require you take action.

Accessing the Security Overview Report

1. Navigate to Reporting > Core Reports > Security Overview.

The Security Overview report is divided into three main areas. At the top, you'll find overview charts for security events. The middle area provides you with a hierarchical view of your security activity—what is generating the most activity—and from which you can click through to other reports—Destination, Identity, and Activity Search. The bottom of the report is where you'll find statistical charts documenting the deployment activity for your organization.

FILTERS



Most Security Blocks

BY DESTINATION

BY IDENTITY

BY TYPE

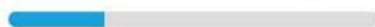
Identity	Blocked Requests	Identity	Blocked Requests
Allen TX	225	umbrella-eng SFO Range 1	7
forwarder01.sjc.opendns.com	156	EUFORRES-M-72KA	6
YVR	30	San Francisco	5
RTP NC	22	Isaf-0606	4
Vancouver	20	VPN	4

VIEW BLOCKED REQUESTS

1 of 2

Active Networks

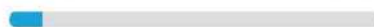
22/84 26% Active



VIEW NETWORKS

Active Roaming Clients

119/1240 10% Active



VIEW ROAMING CLIENTS

Active Virtual Appliances

10/10 100% Active



VIEW VIRTUAL APPLIANCES

Filtering based on time period

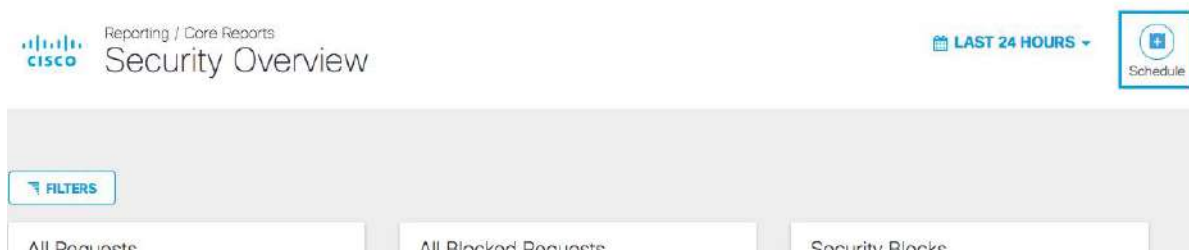
The Security Overview report is time-based and can be generated to show activity for the last 24 hours, the previous calendar day (yesterday), the last seven days, or the last month.



Schedule a report

You can schedule a report to be emailed to you at regular intervals. Your emailed report is a table showing an HTML version of the report and an attached CSV file containing the entire data set. Also included in your email is a link to a live version of the same report. To learn more about scheduled reports, see [Scheduling Reports](#).

1. Click Schedule.



2. Select the report type you'd like (you can only pick one) and click Next.
3. Add email addresses for the recipients of the report and click Next.
4. Schedule the frequency of when you'd like the report sent and click Next.
5. Give your report a meaningful name and click Save.

TIP

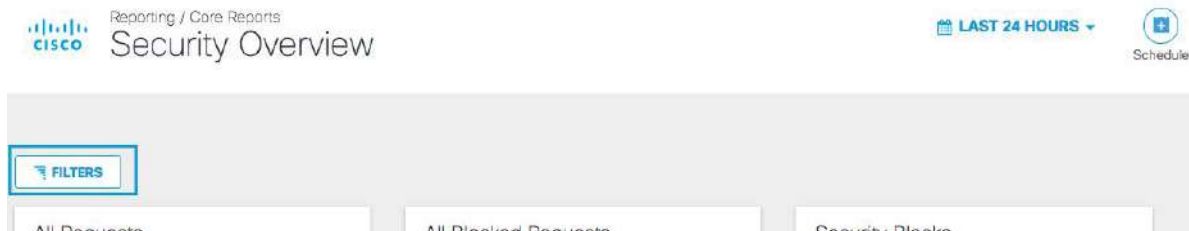
Umbrella reports are highly time dependent. The time is UTC by default, but can be changed to a different timezone on a per-user basis. Navigate to Settings > Accounts and update your account's time setting.

Filtering Security Activity

Filters allow you to change the types of events and identities shown in the security blocks section. You can toggle between "monitoring only mode" by

choosing *Security Blocks* or *All Security Events*. *All Security Events** includes those events tagged as security but were not blocked.

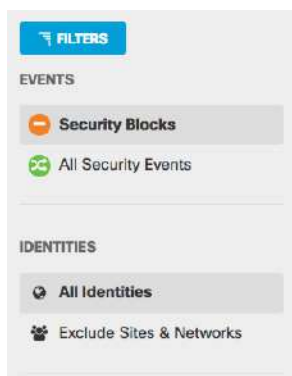
If filters are not visible, click Filters.



The report is intelligent enough to default to the correct mode, so if your organization has no security blocks for the time period selected, it will automatically default to All Security Events, showing the potential events that could have been blocked. If there are any security blocks for a time period, the report will show the blocks. This filter allows users to toggle back and forth between the two views.

Filters: Events and Identities

The Events and Identities filters work in conjunction with each other, meaning that they are always both on but can be set up in different combinations. You might select Events > Security Blocks in combination with Identities > All Identities or Events > Security Blocks with Exclude Sites & Networks.



Networks generate a far higher volume of traffic than a single computer so excluding them from the report can help identify particular machines with an unusually high volume of security events being blocked (or allowed, as the case may be).

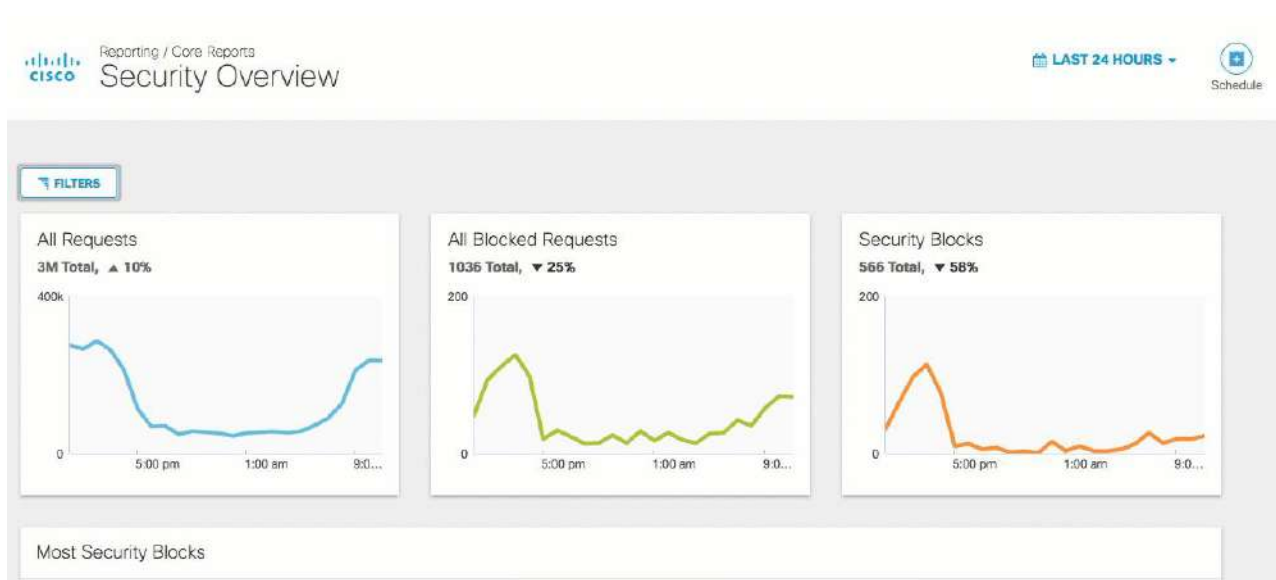
Selecting an Events filter changes the events returned for the most active destinations, identities, and request types:

- Security Blocks—Lists only those requests blocked by Umbrella for the selected time period.
- All Security Events—Lists all security events for the selected time period. This is the default view if there are no security events within the selected time period.

Selecting an Identities filter changes the identities returned for the most active destinations, identities, and request types:

- All Identities—Lists all requests for all identities for the selected period.
- Exclude Sites & Networks—Lists all requests for roaming clients and active directory (AD) users.

Selecting any combination of filter will change the charts to reflect that combination:

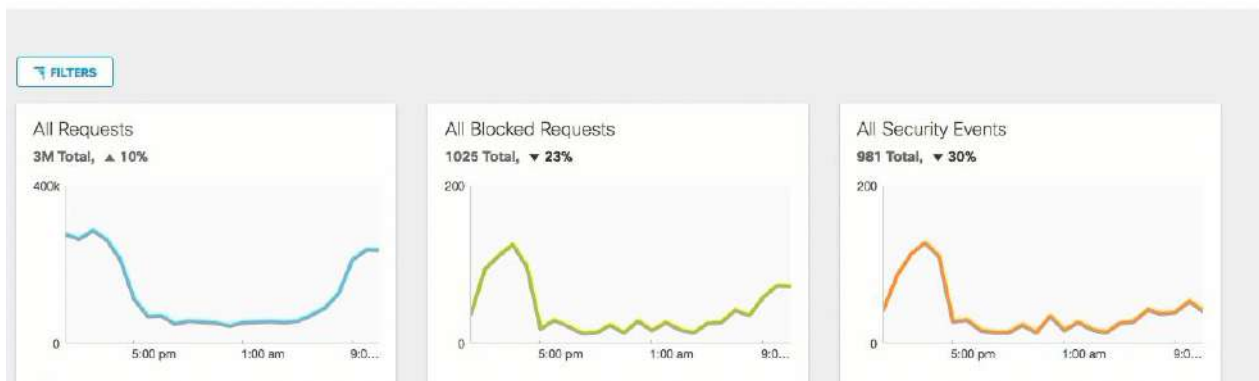


Events – Security Blocks and All Security Events

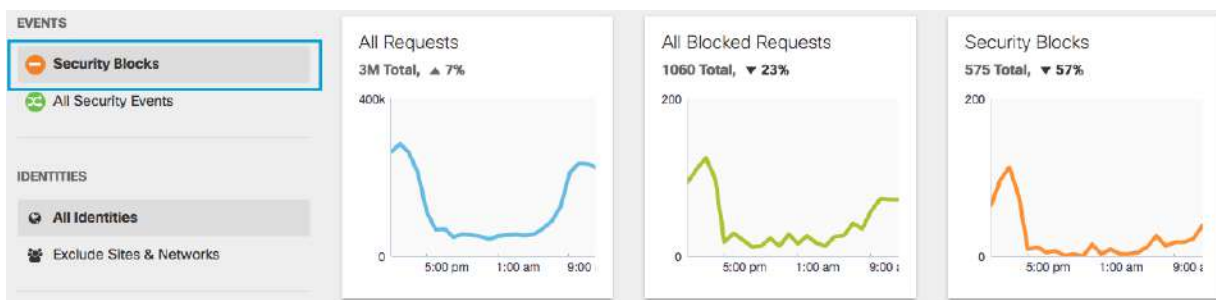
The top set of charts provides you with a quick and easy to follow overview of security activity that has occurred within your organization for the selected time period. Your view is based on the default Events filter selected:

- **Security Blocks**—If there has been a security event within the selected time period.
- **All Security Events**—If there has NOT been a security event within the selected time period.

You can quickly see spikes in activity that might indicate a change or threat to your environment that requires your attention. You can roll over each chart to see the number of events that occurred at that time and then click at that point to go the Activity Search page to see activity details for that specific time.



Security Blocks Filter



- All Requests—All requests (blocked and allowed) made within the selected time period.
- All Blocked Requests—All requests blocked within the selected time period. This includes requests blocked by content access settings (Policies > Policy Components > Content Categories) and requests blocked from your custom destination lists (Policies > Policy Components > Destination Lists).
- All Security Blocks—All blocks based on security category settings only, not including blocks as a result of destination lists or content categories. Security Blocks is shown if there are security blocks for the selected time period or if the Security Blocks filter is selected.

All Security Events Filter



- All Requests—All requests (blocked and allowed) made within the selected time period.

- All Blocked Requests—All requests blocked within the selected time period. This includes requests blocked by content access settings (Policies > Policy Components > Content Categories) and requests blocked from your custom destination lists (Policies > Policy Components > Destination Lists).
- All Security Events—A total of all security events that were blocked and that could have been blocked if the policy were adjusted to include the category as blocked for the identities in question. This helps show if policies should be tightened to block something you're missing, or if you're evaluating Umbrella and aren't ready to flip on enforcement. This is displayed if there are no security events for the selected time period or if All Security Events filter is selected.

Most Active Destination, Identity, or Request Type

You can view which destination, identity, or request type is generating the highest number of blocks within your environment. These are not the most active generally, just the ones that are most blocked. From the lists of most active types, you can click through to specific reports to get specific detail.

Use this information to determine which destinations, identities, or types are seeing the most activity and use them as a jumping off point to other more advanced reports. This can help you to determine if there are changes you need to make that will better protect your environment. As an example, here's a list of identities:

BY DESTINATION		BY IDENTITY	BY TYPE	
Identity	Blocked Requests	Identity	Blocked Requests	
San Francisco	1430	YVR test	94	
forwarder01.sjc.opendns.com	491	VPN Range	89	
forwarder02.sjc.opendns.com	343	Vancouver	75	
forwarder03.sjc.opendns.com	326	Office NAT 1	65	
forwarder04.sjc.opendns.com	270	KATHRYN-W-GDOPN	14	

VIEW BLOCKED REQUESTS 1 of 5 < >

Click View Blocked Requests to go to the Activity Search report and see a detailed list of all blocked requests.

By Destination

The By Destination tab lists security activity by destination. Either Blocked Requests or Requests are listed depending on the Events filter selected.

Most Security Blocks

BY DESTINATION		BY IDENTITY		BY TYPE	
Destination	Blocked Requests	Destination	Blocked Requests		
c3sl.aab2at4fygksthftg05g5ggfjhbichk73a0ebnumfjfoabyu57pc2s.aac7sr...46	46	c3sl.aac2at4fugs2dumiykg2dqm3o5f2l.5sz2avvg6ebdxid3ajwwrgzks4nk4kyzj...44	44		
c3sl.aab2at4f2vy23dob3guyr55br5at3flehlews5be6x3oxjy.gkv5hb05abbzy2ui...46	46	c3sl.aab2at4fywuzlcorvg2tjjevqulicjzsp.6hofsg3ubdykxufj6endzzy676hjmcp...44	44		
c3sl.aab2at4fug24fribyhq4et.tnicqccq6coez.lsoqzcfetfdnfmsfy6wvuf.sopzj...44	44	c3sl.aab2at4fywm5thrf2zoc4uznsvtdgltvgzcx6cdilag2cx36oqmwjak.7c3on3...42	42		
c3sl.aab2at4f3g46kzf4kzyzab4z.vrvauwnc4l5kjdvsqufrvu7hbaicnccox5mhmli...44	44	c3sl.aab2at4f3g46kzf4kzyzab4z.vrvauwnc4l5kjdvsqufrvu7hbaicnccox5mhmli...44	42		
c3sl.aab2at4f4he6tor3wmev66.ju4m3tux2afjzvgf5hagrbwvbxgopcidjge5ox...44	44	c3sl.aab2at4fzho33qmrnya37sj72migarfywcazbyrindhngre4an5cb4.wtpzpk7dxcz...40	40		

VIEW BLOCKED REQUESTS 1 of 10 < >

Click a destination to go to the [Destinations report](#) for that destination

By Identity

The By Identity tab lists security activity by identity. Either Blocked Requests or Requests are listed depending on the Events filter selected.

Most Security Blocks

BY DESTINATION		BY IDENTITY		BY TYPE	
Identity	Blocked Requests	Identity	Blocked Requests		
San Francisco	1430	YVR test	94		
forwarder01.sjc.opendns.com	491	VPN Range	89		
forwarder02.sjc.opendns.com	343	Vancouver	75		
forwarder03.sjc.opendns.com	326	Office NAT 1	65		
forwarder04.sjc.opendns.com	270	KATHRYNW-GD0PN	14		

VIEW BLOCKED REQUESTS 1 of 5 < >

Click an identity to go to the [Identities report](#).

By Type

The By Type tab lists security activity by request type (domain or URL). Either Blocked Requests or Requests are listed depending on the Events filter selected.



Click a type to go to the [Security Activity report](#).

Active Identities

At the bottom of the report, you'll find some helpful charts that encapsulate in percentages deployment activity for your organization. Active Networks, Active Roaming Clients, and Active Virtual Appliances quickly show you how many of each type are currently online and active.

Click [View <Type>](#) to jump to the individual identity type's page.



Security Activity Report

What is the Security Activity Report?

The Security Activity report highlights security events generated by your organization's identities visiting destinations flagged—but not necessarily blocked—by Umbrella security researchers as a threat. This includes security events filtered through the Intelligent Proxy and File Inspection. The Security Activity report enables discoverability to threats by showing traffic patterns, which you can group by type to better see patterns and thus better protect your network.

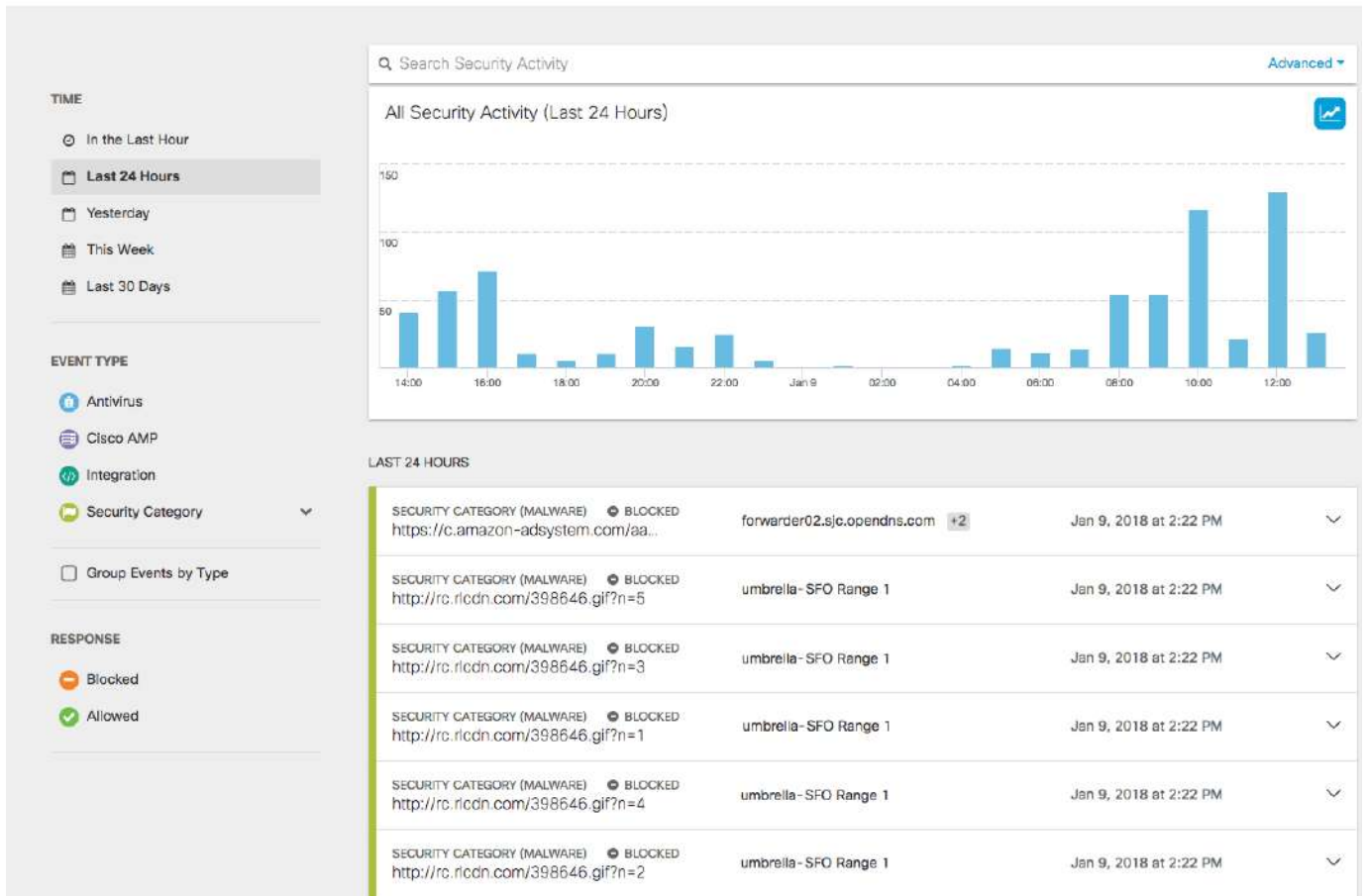
Activities captured by this report might include attempts to access sites hosting malware or phishing sites, botnet activity on infected machines on your local network, attempts to download malicious files—or more. To find out about each of the individual activities and categories you can report on, see [Understanding Security Categories](#).

Use the Security Activity report to see how you are currently being protected against threats and if there are any "holes" in your current protection. Is there a threat being posed against your system that you might be better protected against? Use the information available here to determine if security threats to your system have changed or if there are updates to your policies that you might need to make to protect yourself against threats that you are currently not protected against. You can easily determine what actions have occurred that have put your system at risk. You can see a destination that's been visited that's put you at risk. And with this information, you can make changes to Umbrella to protect yourself even more!

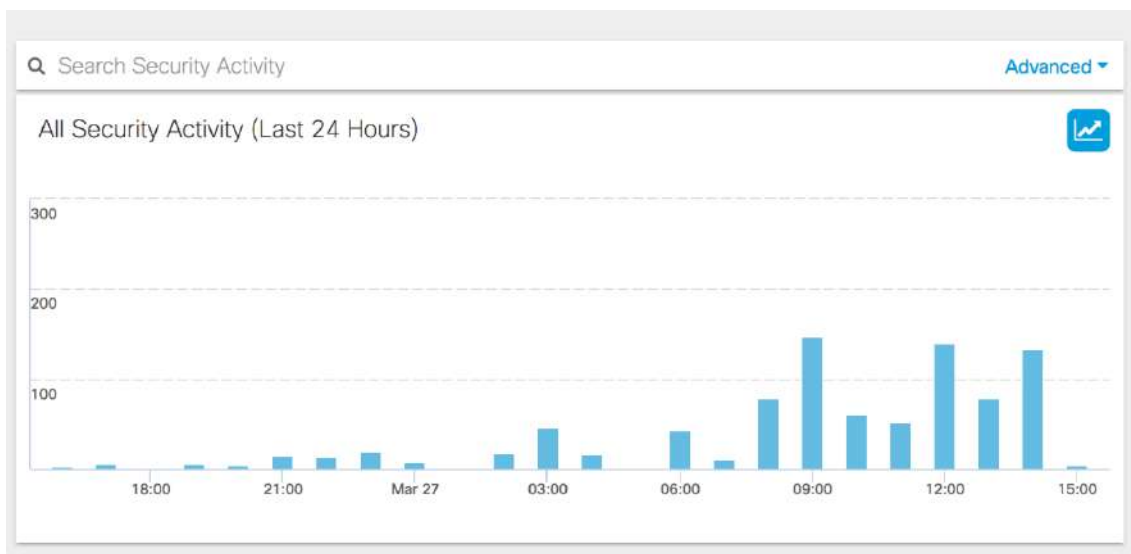
Accessing the Security Activity Report

1. Navigate to Reporting > Core Reports > Security Activity.

The Security Activity report opens, which defaults to a graph showing you all of the security events for your organization tracked over time.



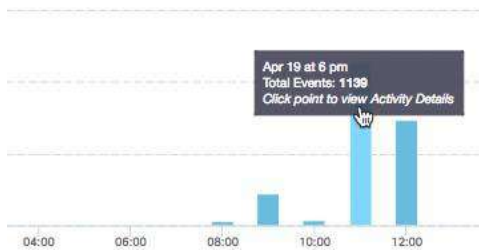
The graph shows any spikes or trends in your environment, possible outbreaks or—if you're lucky—times of relative calm. The y-axis is the number of events and the x-axis is the time period.



Hovering over a specific area in the summary report provides you with some high-level specifics for the selected time period.



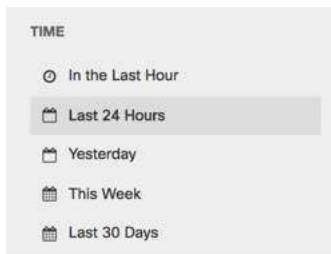
Clicking a bar in the graph takes you to the [Activity Search report](#) where you can view activity details for that time period.



Like other Umbrella reports, the Security Activity report is time-based. You can generate a report to document activities for the last hour, the last 24 hours, the previous calendar day (yesterday), the last seven days, and the last month. At any given time, the upper limit to the time period with which you can generate a report is 30 days.

NOTE: You may notice a difference between the time listed in the pop-up window and that displayed along the x-axis of your charts. The chart uses "local" time to track when the data was logged. The pop-up using the time configured for your account (Settings > Accounts). In these examples, the local time is Pacific > Vancouver; whereas, the account time is set to UTC. To sync times, navigate to Settings > Accounts and change time to local time—the time when data is being logged.

At any time you can change the time period within which Umbrella tracks security activity. Under Time, select a new time period.



TIP

Most, if not all, Umbrella reports are highly time dependent. The time is UTC by default, but can be changed to a different timezone on a per-user basis. Navigate to Settings > Accounts and update your account's time setting.

Search for Security Activity

It's easy to search for the security activity of an identity you're interested in.

1. Type the identity's name in the search bar at the top of the page and press Enter.



You can also perform a search based on a SHA256 hash or threat name. Just add the hash or threat name to the search box and press Enter.

A threat name is a name Umbrella security researchers have assigned to a piece of malware to identify a specific attack. For example, "Ransomware" or "Locky"—the first being a family of threats and the latter being a specific attack.



Advanced Search

1. Click Advanced.
2. Enter the specifics of your search and then click Apply. You don't have to enter information for each search field, but remember that the more information you can provide the more successful your search will be.

ADVANCED SEARCH ✕

Identity

Domain

CANCEL
APPLY

Accessing Event Details

Under the Security Activity bar graph, you'll find "cards" that stack the details of security events for the selected time period and [event types](#). Aggregated over time, these cards show you all the identities that have visited a destination within the selected time period.

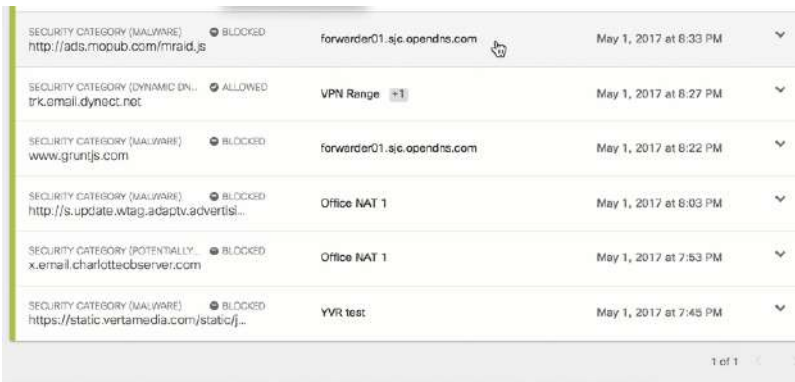
These cards stack data so that you are not overwhelmed by information and can focus on what is important to you.

YESTERDAY			
SECURITY CATEGORY (M... www.davecolland.com	BLOCKED	forwarder01	Apr 18, 2017 at 11:52 PM
SECURITY CATEGORY (DY... trk.email.dynect.net	ALLOWED	Office NAT 1	Apr 18, 2017 at 11:52 PM
INTEGRATION Cisco AMP Threat Grid	BLOCKED	YVR	Apr 18, 2017 at 11:49 PM
DISCO AMP 275a021bbfb6489e54d47189...	BLOCKED	Office NAT 1	Apr 18, 2017 at 11:47 PM
INTEGRATION Cisco AMP Threat Grid	BLOCKED	Office NAT 1	Apr 18, 2017 at 11:41 PM
SECURITY CATEGORY (M... www.comcast.net	BLOCKED	Office NAT 1	Apr 18, 2017 at 11:36 PM

Click an event to view its details. Each security activity card groups an event by destination and lists the details of the event including date & time, destination, and identity. Details differ slightly between event type, but all list destination and identity from which you can click through to the [Destinations](#) and [Identities](#) reports.

SECURITY CATEGORY (MALWARE) ● BLOCKED			
realarmy.org	Zoe-885		Jan 10, 2018 at 11:24 AM
Event Details			
Date & Time	Identity	External IP	
Jan 10, 2018 at 11:24 AM	Zoe-885	Roaming Computer	54.183.40.98
Destination	Categories	Result	
realarmy.org	Malware	Blocked	
	Internal IP	DNS Record Type	
	54.183.40.98	A	

Because each card includes all requests for the destination, you can click through the "cards" requests to see the details for each request including all the identities that triggered the event.



SECURITY CATEGORY (MALWARE)	BLOCKED	forwarder01.sjc.opendns.com	May 1, 2017 at 8:33 PM
SECURITY CATEGORY (DYNAMIC DN...)	ALLOWED	VPN Range +1	May 1, 2017 at 8:27 PM
SECURITY CATEGORY (MALWARE)	BLOCKED	forwarder01.sjc.opendns.com	May 1, 2017 at 8:22 PM
SECURITY CATEGORY (MALWARE)	BLOCKED	Office NAT 1	May 1, 2017 at 8:03 PM
SECURITY CATEGORY (POTENTIALLY...)	BLOCKED	Office NAT 1	May 1, 2017 at 7:53 PM
SECURITY CATEGORY (MALWARE)	BLOCKED	YVR test	May 1, 2017 at 7:45 PM

If a security event includes a +, it means that more than one identity is involved with this security event. You can click through the cards "stacked" requests and identify each identity.

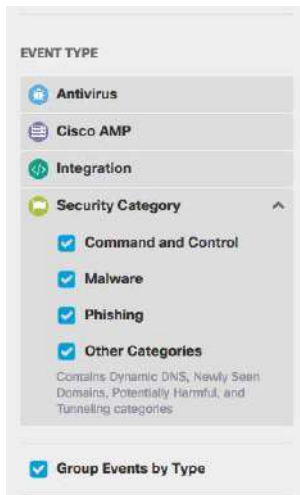


SECURITY CATEGORY (DYNAMIC DNS)	ALLOWED	forwarder02.sjc.opendns.com +1	Apr 20, 2017 at 10:44 PM
---------------------------------	---------	--------------------------------	--------------------------

Filtering Security Events

Security events listed are based on the following Event types:

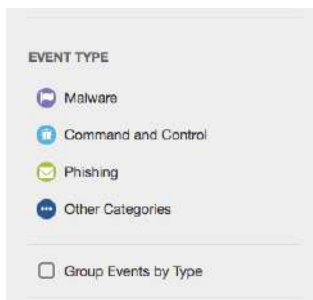
- Antivirus—Lists events that the Intelligent Proxy has filtered through a virus scan
- Cisco AMP—Lists events that the Intelligent Proxy has run through Cisco Advanced Malware Protection (AMP)
- Integration—Lists events allowed or blocked based on destination lists generated from custom or third party data feed integrations
- Security Category—Lists events allowed or blocked against selected security categories: Command and Control, Malware, Phishing, and Other Categories (Contains Dynamic DNS, Newly Seen Domains, Potentially Harmful, and Tunneling categories).



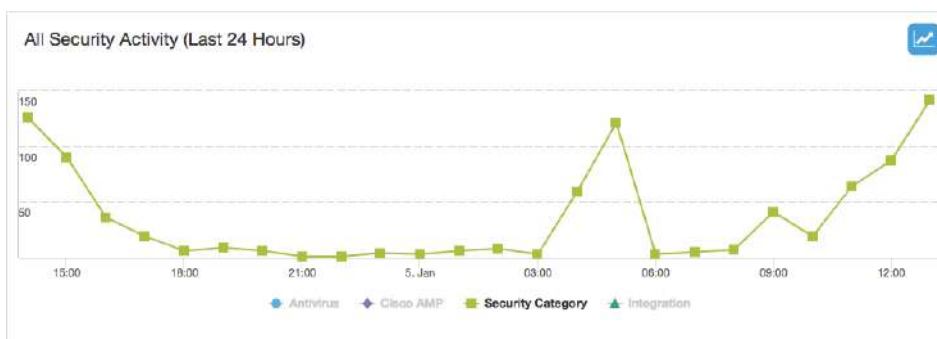
If you clear all sub-Security Category entries and then select Security Category, all security category events are grouped as one event.

Antivirus and Cisco AMP are only available with Umbrella Insights or Platform packages, or for MSPs and customers of those MSPs. For more information on upgrading your package, please contact your Cisco Umbrella representative.

Those without either the Umbrella Insights or Platform packages have access to a reduced set of security events.



When you filter based on an Event type and check Group Events by Type, you'll notice that the graph changes from a bar to a line.



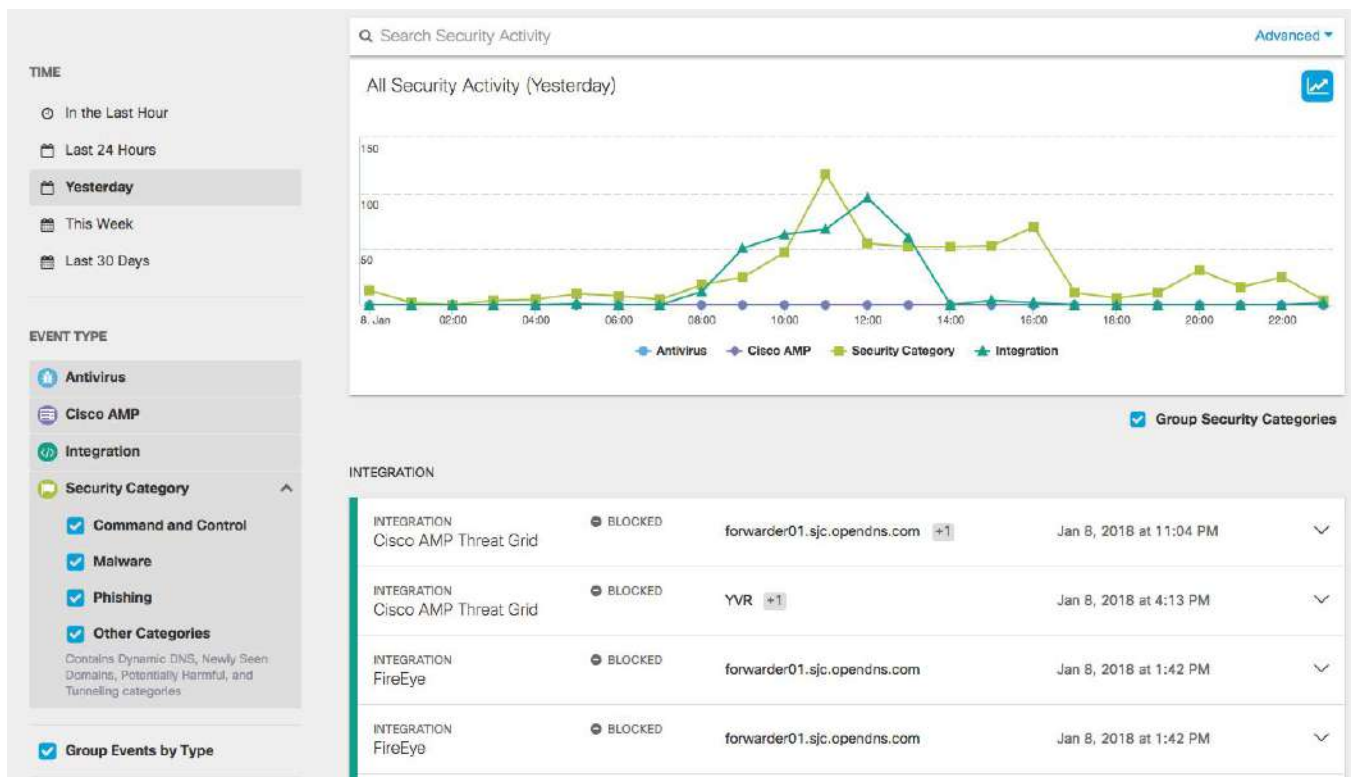
And security events are grouped together.

CISCO AMP			
CISCO AMP	BLOCKED	forwarder01	Jan 5, 2018 at 2:32 AM
e92af41ea36051ffe9f3c83abec97ce...			
1 of 1			
SECURITY CATEGORY			
SECURITY CATEGORY (PHISHING)	BLOCKED	SFO Range 1 +1	Jan 5, 2018 at 9:48 AM
internetbadguys.com			
SECURITY CATEGORY (PHISHING)	BLOCKED	YVR	Jan 4, 2018 at 11:18 PM
www.funinformatique.com			

Rolling over the line graph pops up a modal giving you an overview of the security event at that time on the graph. Clicking the line graph takes you to the [Activity Search report](#) where you can view activity details in even greater detail.



With Group Events by Type checked and more than one Event Type selected, the activity chart updates to show each selected event so that you can compare activities. Your graph may redraw itself to accommodate differences in event totals.



And you can filter based on the type of response, too:

- Blocked

- Allowed



Filter against Blocked to see what you are blocking and if there is anything you might not want to block.

Filter against Allowed to see what you could have blocked if you had enabled policies for those identities in block mode. Use this filter to determine the current strength of your policy and if you need to make changes.

If you select Antivirus or Cisco AMP as the Event Type, you cannot select Response > Allowed. Umbrella cannot allow viruses to pass through the system. These will always be blocked.

Activity Search Report

What is the Activity Search Report?

The Activity Search report helps you find the result of every DNS, URL, and IP request from your various identities, ordered in descending date and time. It lists all security (and non-security) related activity within the identities reporting to Umbrella for the selected time and also allows you to refine your search using filters to see only what you need to see. This can greatly assist you in determining if there are any security issues you may have within your organization that require your attention.

By clicking an identity or destination, you can quickly pivot from this report to the [Identities](#) and [Destinations](#) reports.

View the Activity Search Report

1. Navigate to Reporting > Core Reports > Activity Search.
This takes you to the default view of the Activity Search report, which lists all of your identities and the internet requests, or traffic events for your organization tracked over time. The default is 24 hours.

NOTE: The Activity Search is limited to 500 results per query. If you require more than this amount, we advise using the time filter to chunk the results by time, and exporting each set of results. Alternately, simply refine the filter to remove extra results you're not interested in.

Q Search request activity		Advanced	Columns	All Requests		
Filter By:	Q	Destination	Identity Used by Policy	Action	Tags	Categories
Response	Select All	San Francisco	5-22-0-app.agent.datadoghq.com	forwarder02.sjc.opendns.com	Allowed	
<input type="checkbox"/> Allowed		CITEIS - Allen TX	2-edge-chat.facebook.com	CITEIS - Allen TX	Allowed	Instant Messaging, Social Networking
<input type="checkbox"/> Blocked		CITEIS - Allen TX	clientservices.googleapis.com	CITEIS - Allen TX	Allowed	Search Engines
<input type="checkbox"/> Proxied		San Francisco	www.youtube.com	forwarder01.sjc.opendns.com	Allowed	Search Engines, Video Sharing
<input type="checkbox"/> Allowed: Destination List		CITEIS - Allen TX	chromeextension-pa.googleapis.com	CITEIS - Allen TX	Allowed	Search Engines
<input type="checkbox"/> Blocked: Destination List		CITEIS - Allen TX	safebrowsing.googleapis.com	CITEIS - Allen TX	Allowed	Search Engines
Protocol	Select All	YVR test	www.cisco.com	YVR test	Allowed	Software/Technology, Business Servi
<input type="checkbox"/> HTTP		CITEIS - Allen TX	js-agent.newrelic.com	CITEIS - Allen TX	Allowed	Software/Technology, Business Servi
<input type="checkbox"/> HTTPS		CITEIS - Allen TX	cloudsec.my.salesforce.com	CITEIS - Allen TX	Allowed	Software/Technology, Business Servi
Event Type	Select All	CITEIS - Allen TX	cloudsec--c-na3.content.force.com	CITEIS - Allen TX	Allowed	Software/Technology, Business Servi
<input type="checkbox"/> Antivirus		CITEIS - Allen TX	cloudsec.my.salesforce.com	CITEIS - Allen TX	Allowed	Software/Technology, Business Servi
<input type="checkbox"/> Application		CITEIS - Allen TX	global-x02wapi.webexconnect.com	CITEIS - Allen TX	Allowed	Software/Technology
<input type="checkbox"/> Cisco AMP		YVR test	www.cisco.com	YVR test	Allowed	Software/Technology, Business Servi
<input type="checkbox"/> Content Category		CITEIS - Allen TX	metrics-a.wbx2.com	CITEIS - Allen TX	Allowed	SaaS and B2B
<input type="checkbox"/> Destination List		CITEIS - Allen TX	googlemail.l.google.com	CITEIS - Allen TX	Allowed	Search Engines, Webmail
<input type="checkbox"/> Integration		CITEIS - Allen TX	x02wapi.webexconnect.com	CITEIS - Allen TX	Allowed	Software/Technology
<input type="checkbox"/> Security Category		CITEIS - Allen TX	x02wapi.webexconnect.com	CITEIS - Allen TX	Allowed	Software/Technology
Identity Type	Select All	CITEIS - Allen TX	drive.google.com	CITEIS - Allen TX	Allowed	File Storage, Software/Technology, G
<input type="checkbox"/> Computers		CITEIS - Allen TX	clients.l.google.com	CITEIS - Allen TX	Allowed	Search Engines
<input type="checkbox"/> Users		CITEIS - RTP NC	www.onenote.com	CITEIS - RTP NC	Allowed	File Storage, Software/Technology, In
<input type="checkbox"/> Roaming Computers		CITEIS - RTP NC	www.onenote.com	CITEIS - RTP NC	Allowed	File Storage, Software/Technology, In
<input type="checkbox"/> Network Devices		CITEIS - Allen TX	gmail-limap.l.google.com	CITEIS - Allen TX	Allowed	Search Engines
<input type="checkbox"/> Networks		CITEIS - Allen TX	www.googleapis.com	CITEIS - Allen TX	Allowed	Search Engines
<input type="checkbox"/> Sites		CITEIS - Allen TX	www.googleapis.com	CITEIS - Allen TX	Allowed	Search Engines
<input type="checkbox"/> Mobile Devices		CITEIS - RTP NC	googlemail.l.google.com	CITEIS - RTP NC	Allowed	Search Engines, Webmail
Tags	Select All	CITEIS - RTP NC	googlemail.l.google.com	CITEIS - RTP NC	Allowed	Search Engines, Webmail
<input type="checkbox"/> Test Tag		CITEIS - RTP NC	mail.google.com	CITEIS - RTP NC	Allowed	Search Engines, Webmail, Gmail
<input type="checkbox"/> Speedtest 3		CITEIS - Allen TX	mail.google.com	CITEIS - Allen TX	Allowed	Search Engines, Webmail, Gmail
<input type="checkbox"/> rat bastard		CITEIS - Allen TX	imap.gmail.com	CITEIS - Allen TX	Allowed	Search Engines, Webmail, Gmail
<input type="checkbox"/> test		CITEIS - Allen TX	imap.gmail.com	CITEIS - Allen TX	Allowed	Search Engines, Webmail, Gmail
<input type="checkbox"/> Easin Tag		CITEIS - Allen TX	apple.com	CITEIS - Allen TX	Allowed	Software/Technology
<input type="checkbox"/> new york		Vancouver	play.google.com	YVR test	Allowed	Ecommerce/Shopping, Movies, Searc
Security Categories	Select All	CITEIS - Allen TX	www.apple.com	CITEIS - Allen TX	Allowed	Software/Technology, Infrastructure
<input type="checkbox"/> BFox Test Integration		CITEIS - Allen TX	www.icloud.com	CITEIS - Allen TX	Allowed	File Storage, Software/Technology, V
<input type="checkbox"/> Check Point		San Francisco	likeabosh.hipchat.com	forwarder01.sjc.opendns.com	Allowed	Allow List, Chat, Instant Messaging, t
<input type="checkbox"/> Cisco AMP Threat Grid		San Francisco	likeabosh.hipchat.com	forwarder01.sjc.opendns.com	Allowed	Allow List, Chat, Instant Messaging, t
<input type="checkbox"/> Command and Control		CITEIS - Allen TX	safebrowsing.googleapis.com	CITEIS - Allen TX	Allowed	Search Engines
<input type="checkbox"/> Cryptomining		CITEIS - Allen TX	analytics.atlassian.com	CITEIS - Allen TX	Allowed	Software/Technology, SaaS and B2B
<input type="checkbox"/> Custom Feed 1		San Francisco	smtp.mailgun.org	forwarder02.sjc.opendns.com	Allowed	Allowed
<input type="checkbox"/> DNS Tunneling VPN		CITEIS - Allen TX	jeasie	CITEIS - Allen TX	Allowed	Allowed
Content Categories	Select All	CITEIS - Allen TX	play.google.com	CITEIS - Allen TX	Allowed	Ecommerce/Shopping, Movies, Searc
<input type="checkbox"/> Academic Fraud						
<input type="checkbox"/> Adult Themes						
<input type="checkbox"/> Adware						
<input type="checkbox"/> Alcohol						
<input type="checkbox"/> Anime/Manga/Webcomic						
<input type="checkbox"/> Arts						
<input type="checkbox"/> Astrology						
SEARCH OPTIONS						
<input type="checkbox"/> Include "Noisy" Domains						
Shows all requests, including common, high-traffic domains like CDNs and reverse lookups.						

Insights and Platform customers see all requests (DNS, URL, and IP) with a selector to filter down to a specific data type.

DNS only customers (Professional, Premium DNS, Branch, Roaming, and WLAN packages) will only see DNS data. For more information on upgrading

your package to include Proxy (URL) and IP support, please contact your Cisco Umbrella representative.

- From the Requests menu in the upper-right, choose one of All Requests, Domain Requests (DNS), URL Requests, or IP Requests. Filters will update to those that are relevant to the type of request you have chosen.



- Optionally, change the [time period](#) for your search.



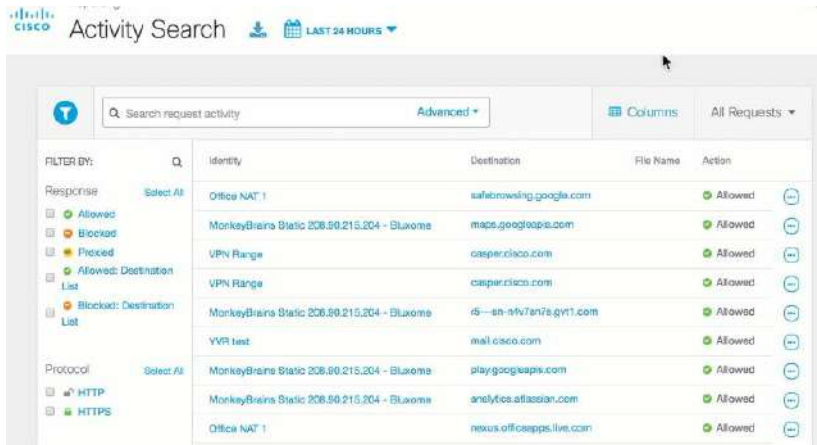
- Optionally, select Columns and then check or clear the information you want to see displayed. You can drag and drop items in the list to reorder their position on the page.

pe	Destination	Internal IP	External IP	Action	C
rorks	casper-dc.oel.cisco.com	67.215.87.13	67.215.87.13	Allowed	S
rorks	taa.webex.com	67.215.87.11	67.215.87.11	Allowed	S
rorks	a.crashlytics.com	67.215.87.11	67.215.87.11	Allowed	S
rorka	clients6.google.com	67.215.87.11	67.215.87.11	Allowed	S
rorks	www.ari.maapp.com.herokuapp.com	67.215.89.252	67.215.89.252	Allowed	S
rorks	api.ari.maapp.com	67.215.89.252	67.215.89.252	Allowed	S
rorks	autodiscover.cisco.com	67.215.89.252	67.215.89.252	Allowed	S
rorks	player.ooyala.com	67.215.87.11	67.215.87.11	Allowed	S
rorks	apple.com	67.215.87.11	67.215.87.11	Allowed	S
rorks	talk.google.com	67.215.87.11	67.215.87.11	Allowed	C
rorks	talk.google.com	67.215.87.11	67.215.87.11	Allowed	C

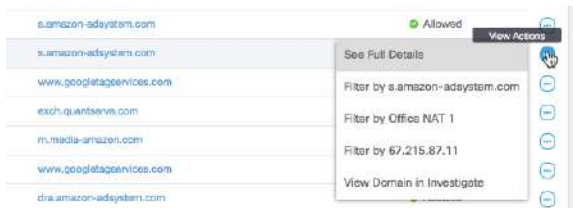
- Select [filters](#) and click Apply. Click the Filters icon to open the Search Filters box. Use the Search filters box to help you locate a filter. NOTE: There are no filters for IP Requests.



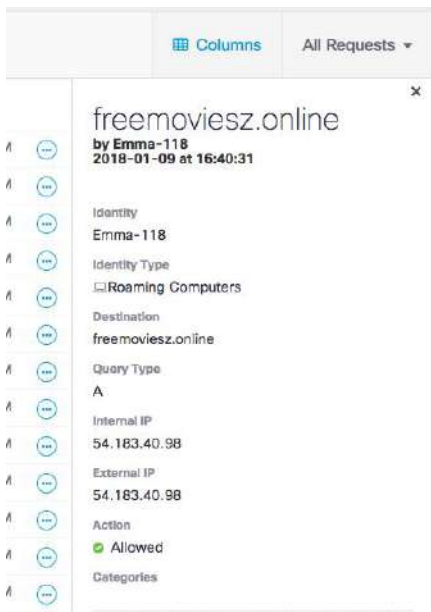
From your search results, you can click an identity or destination and go to their respective [Identities](#) or [Destinations](#) report. These reports give you even greater insight into your organization's internet activity.



6. To start learning more about the results of your activity search, click the View Actions icon for a result and choose an item from the menu.



With View Actions, you can view the full details of each activity result.



Use View Actions to refine your results by filtering based on a single internet activity. Filter activity so that you can see all result with the same identity, destination, or IP address.

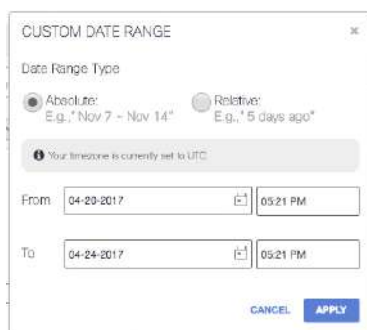
If you have access to Investigate, you can also click through to [Investigate](#) and view the domain URL, or IP address details there.

Time

Like other Umbrella reports, this Activity Search report is time-based. You can generate a search report to document activities for the last 24 hours, the previous calendar day (yesterday), the last seven days, the last month, or a custom date range.



If you want to search using a custom date range, select Custom range. Note that even with the custom date range, you are limited to a thirty-day time frame.



Selecting Relative Time lets you set a date range that is relative to the current day. For example, you might set a date range that starts six days ago and ends three days ago.

TIP

Most, if not all, Umbrella reports are highly time dependent. The time is UTC by default, but can be changed to a different timezone on a per-user basis. Navigate to Settings > Accounts and update your account's time setting.

Search for Activity

It's easy to search for the activity of a specific identity you're interested in. You can enter the destination (domain, IP or URL), the identity's name or a combination of both in the search bar at the top of the page and press Enter.

Any field in the 'Advanced' dropdown can be typed in directly.

NOTE: The IP portion of the Advanced Search allows a user to search for events associated with IP addresses on their network (either internal or the public egress IP address), it does not provide the capability to search for destination IP addresses.

1. Click Advanced to perform a more detailed search.
2. Enter the specifics of your search and then click Search. You don't have to enter information for each search field; just enough to yield the specific results. You can search for more than one domain at a time. When you add a domain, a new field appears so that you can add another domain.

NOTE: Search parameters differ between request types.

ADVANCED SEARCH ✕

Identity

Domain
 ✕
 ✕

URL

IP

CANCEL
APPLY

Use the filters (available on the left of the page) to refine your search so that you see exactly what you want. The "filter pills" that appear at the top of the page let you quickly see all of the filters that you have selected. They are arranged on the page chronologically, so if you get to a point where the last filter you've selected results in a search returning nothing you can clear the last filter selected by clicking X for that filter pill and you should see results again.

Advanced
CLEAR

Columns
All Requests

FILTER BY: Q

Response Select All

Allowed

Blocked

Proxied

Allowed: Destination List

Blocked: Destination List

Protocol Select All

HTTP

HTTPS

Identity Type Select All

Computers

Users

Roaming Computers

Network Devices

Networks

Sites

Mobile Devices

Security Categories Select All

Dynamic DNS

Command and Control

Malware

Phishing

Unauthorized IP Tunnel Access

Newly Seen Domains

Potentially Harmful

Identity	Identity Type	Destination	Action	Categories	Date & Time
Noah-19	Roaming Computers	medieval.it	Blocked	Malware	Jan 9, 2018 at 4:53 PM
Julia-863	Roaming Computers	koranhandphone.com	Blocked	Malware	Jan 9, 2018 at 4:52 PM
Mason-692	Roaming Computers	myfinanceservice.com	Blocked	Malware	Jan 9, 2018 at 4:49 PM
Jackson-594	Roaming Computers	worldonsearch.com	Blocked	Malware	Jan 9, 2018 at 4:48 PM
Liam-246	Roaming Computers	phum1.com	Blocked	Malware	Jan 9, 2018 at 4:48 PM
Nathan-420	Roaming Computers	kztechs.com	Blocked	Malware	Jan 9, 2018 at 4:47 PM
Zoe-951	Roaming Computers	wdvector.me	Blocked	Malware	Jan 9, 2018 at 4:47 PM
Chloe-237	Roaming Computers	teothemes.com	Blocked	Malware	Jan 9, 2018 at 4:46 PM
Aiden-213	Roaming Computers	date-4-u-today2.com	Blocked	Malware	Jan 9, 2018 at 4:46 PM
Emily-349	Roaming Computers	i24.com.ua	Blocked	Malware	Jan 9, 2018 at 4:46 PM
Noah-19	Roaming Computers	weightlossbodies4.world	Blocked	Malware	Jan 9, 2018 at 4:43 PM
William-582	Roaming Computers	digitalseas.io	Blocked	Malware	Jan 9, 2018 at 4:38 PM
Mason-708	Roaming Computers	betatransfer.net	Blocked	Malware	Jan 9, 2018 at 4:33 PM
Zoe-885	Roaming Computers	adsrvmedia.net	Blocked	Malware	Jan 9, 2018 at 4:33 PM
Aiden-213	Roaming Computers	nukussat.clan.su	Blocked	Malware, Blogs	Jan 9, 2018 at 4:28 PM
Aiden-213	Roaming Computers	adelgazarconsalud.info	Blocked	Malware	Jan 9, 2018 at 4:22 PM
Emily-349	Roaming Computers	mypornwap.me	Blocked	Malware	Jan 9, 2018 at 4:20 PM
Mason-692	Roaming Computers	colins.com	Blocked	Malware	Jan 9, 2018 at 4:18 PM
Sophia-388	Roaming Computers	1.ks.us	Blocked	Malware	Jan 9, 2018 at 4:17 PM
Loan-928	Roaming Computers	thfib.com	Blocked	Malware	Jan 9, 2018 at 4:17 PM

If filters are not visible, click the Toggle Filters icon.

38

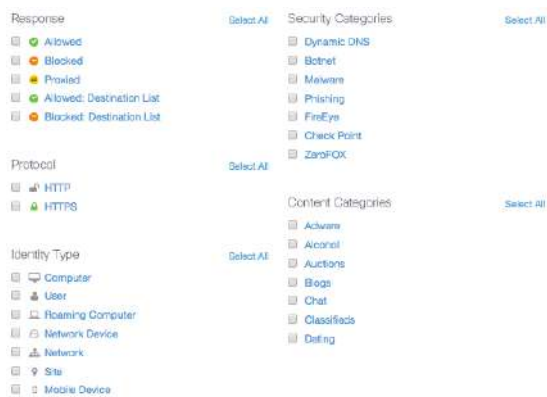


When you select a filter, it appears at the top of the page so that you can easily see how you are filtering your report. Quickly change how you're filtering your report filter by removing them here instead of searching for them on the side of the page.



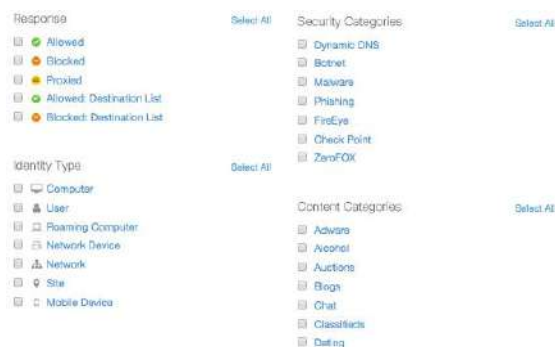
All Request Filters

Filter by response, protocol, identity type, security categories, and content categories. Select any or all of these filters.



Domain Request Filters

Filter by response, protocol, identity type, and security categories. Select any or all of these filters.



URL Request Filters

Filter by response, protocol, identity type, and security categories. Select any or all of these filters.

The image shows a filter configuration interface with four main sections, each containing a list of items with checkboxes and a 'Select All' button.

- Response:** Contains 'Allowed' (with a green checkmark icon) and 'Blocked' (with an orange circle icon).
- Protocol:** Contains 'HTTP' (with a red 'X' icon) and 'HTTPS' (with a green checkmark icon).
- Identity Type:** Contains 'User' (with a person icon), 'Roaming Computer' (with a laptop icon), 'Network' (with a network icon), and 'Site' (with a location pin icon).
- Security Categories:** Contains 'Dynamic DNS', 'Botnet', 'Malware', 'Phishing', 'Unauthorized IP Tunnel Access', 'Newly Seen Domains', and 'Potentially Harmful'.

Each section has a 'Select All' button to its left or right.

Identities Report

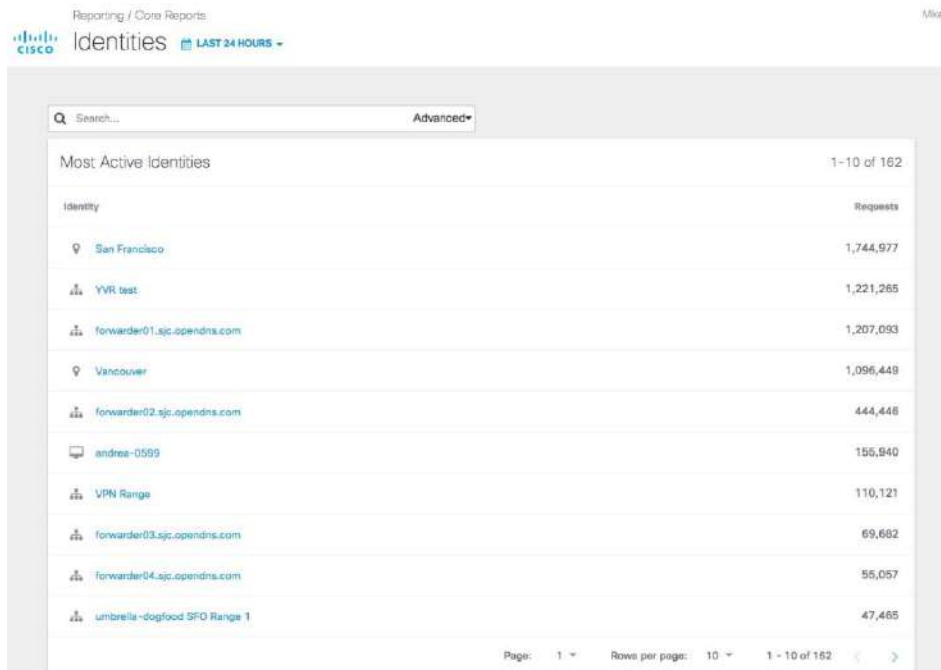
The Identities report gives you access to activity information about your identities, determining which are the most active and lets you know about the destinations they are visiting. From the top-level Identities report, you can access an Identities report that is specific to an identity. Here you can explore details about its activities at the domain level, determining which sites it has visited and when. This detailed information can help you determine if an identity has visited sites that you should block.

Note: The Identities report replaces the Security Insight report. Information that was included in the Security Insight report is now included in the Identities report.

This report is only available for customers with Umbrella Insights or Platform packages, or for MSPs and customers of those MSPs. For more information on upgrading your package, please contact your Cisco Umbrella representative.

Accessing Identities Reports

1. Navigate to Reporting > Core Reports > Identities.
This takes you to the top-level of the Identities reports page, which lists identities by requests made within the selected time period. The default is 24 hours.



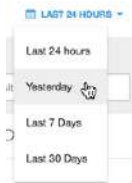
The screenshot shows the Cisco Umbrella reporting interface for Identities. The page title is "Identities" with a filter set to "LAST 24 HOURS". A search bar is present at the top. The main content is a table titled "Most Active Identities" showing the top 10 identities based on the number of requests. The table has two columns: "Identity" and "Requests".

Identity	Requests
San Francisco	1,744,977
YVR test	1,221,265
forwarder01.sjc.opendns.com	1,207,093
Vancouver	1,096,448
forwarder02.sjc.opendns.com	444,448
andrea-0599	155,940
VPN Range	110,121
forwarder03.sjc.opendns.com	69,682
forwarder04.sjc.opendns.com	55,057
umbrella-dogfood SFO Range 1	47,465

At the bottom of the table, there is a pagination control showing "Page: 1", "Rows per page: 10", and "1 - 10 of 162".

2. Click an identity to go to the Identities report for that identity.
For details about how to read an Identities report, see [Understanding an Identities Report](#).

Like other Umbrella reports, an Identities report is time-based. You can generate a report to document activities for the last 24 hours, the previous calendar day (yesterday), the last seven days, and the last month.



3. If you can't find an identity you're interested in, you can search for it.

When you search for an identity, the search bar dynamically updates to lists all identities related to your entry. You can select an identity from the resulting list or select All results with a name like: <name>.



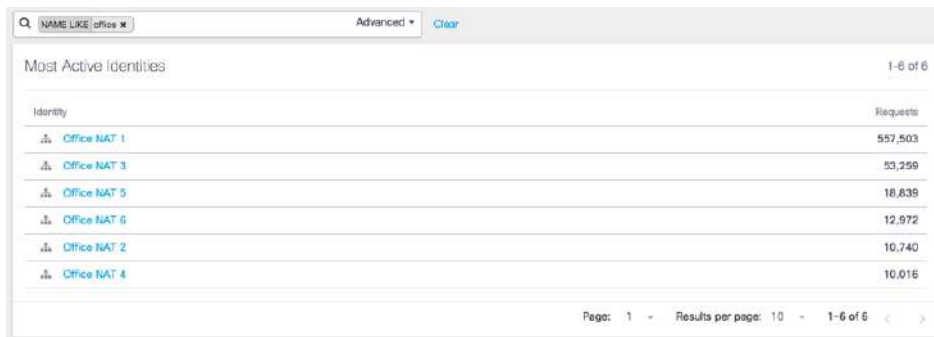
You can also perform an advanced search. Click Advanced in the search bar and the Advanced pop-up window opens.



Search by identity name or type, or both. This can help you narrow your search results if you want to see all identities of the same type or if there are multiple identities with the same name.

When you search for an identity, your results depend on the type of search parameters you have selected. Umbrella returns only the identity selected or all related identities. In our example, we've searched for all identities with a name like office that have been active within the last the last 24 hours. Umbrella returns any related identities along with the number of requests made by the

identity. For office, this search returns seven identities with Office Nat 1 being the most active within the last 24 hours.



Q NAME LIKE office x Advanced Clear

Most Active Identities 1-6 of 6

Identity	Requests
Office NAT 1	557,503
Office NAT 3	93,259
Office NAT 5	18,639
Office NAT 6	12,972
Office NAT 2	10,740
Office NAT 4	10,016

Page: 1 Results per page: 10 1-6 of 6

Understanding an Identities Report

An Identities report for an identity charts activities for that identity within the specified time period. The report is broken into three areas of reporting that help you answer critical questions about the activities of identities on your network:

- [Activity Charting](#)
- [Security Details](#)
- [Recent Activity](#).

Last Active: Feb 2, 2018 at 9:27 AM



Top Destinations

SECURITY | ALL

Destinations	Requests
stan.spgate.net	1,663
coinhive.com	1,623
stan.ideasp.com	846
stan.internetcalls.com	845
stan.schkund.de	841

[VIEW ALL DESTINATIONS](#)

Top Security Categories

FireEye Integration	10,194
Malware	7,118
Potentially Harmful	2,738
Cisco AMP Threat Grid Integration	193
Phishing	166
Dynamic DNS	78
Command and Control	52
Newly Seen Domains	4
DNS Tunneling VPN	2

[VIEW ALL CATEGORIES](#)

Recent Activity for San Francisco

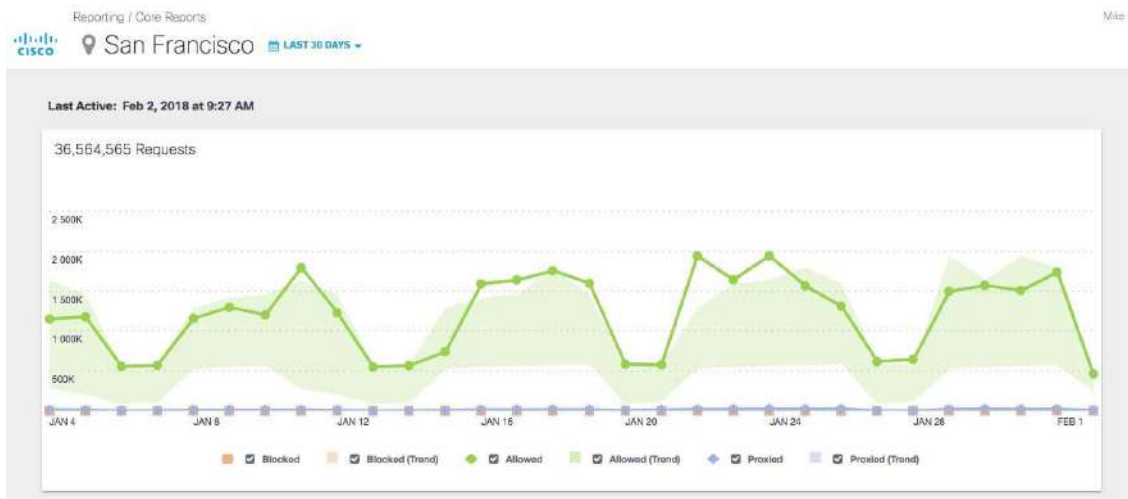
Destination	Response	External IP	Internal IP	Date & Time
conv-s.wts2.com	Allowed	192.168.1.1	10.10.10.10	Feb 2, 2018 at 9:27 AM
achm-noori.wts2.com	Allowed	192.168.1.1	10.10.10.10	Feb 2, 2018 at 9:27 AM
conv-s.wts2.com	Allowed	192.168.1.1	10.10.10.10	Feb 2, 2018 at 9:27 AM
clients6.google.com	Allowed	192.168.1.1	10.10.10.10	Feb 2, 2018 at 9:27 AM
analytics.etsiasan.com	Allowed	192.168.1.1	10.10.10.10	Feb 2, 2018 at 9:27 AM
api.amplitude.com	Allowed	192.168.1.1	10.10.10.10	Feb 2, 2018 at 9:27 AM
22.client-channel.google.com	Allowed	192.168.1.1	10.10.10.10	Feb 2, 2018 at 9:27 AM
api.amplitude.com	Allowed	192.168.1.1	10.10.10.10	Feb 2, 2018 at 9:27 AM
news.ycombinator.com	Allowed	192.168.1.1	10.10.10.10	Feb 2, 2018 at 9:27 AM
news.ycombinator.com	Allowed	192.168.1.1	10.10.10.10	Feb 2, 2018 at 9:27 AM

[VIEW ALL RECENT ACTIVITY](#) Page: 1 Rows per page: 10 1 - 10 of 100

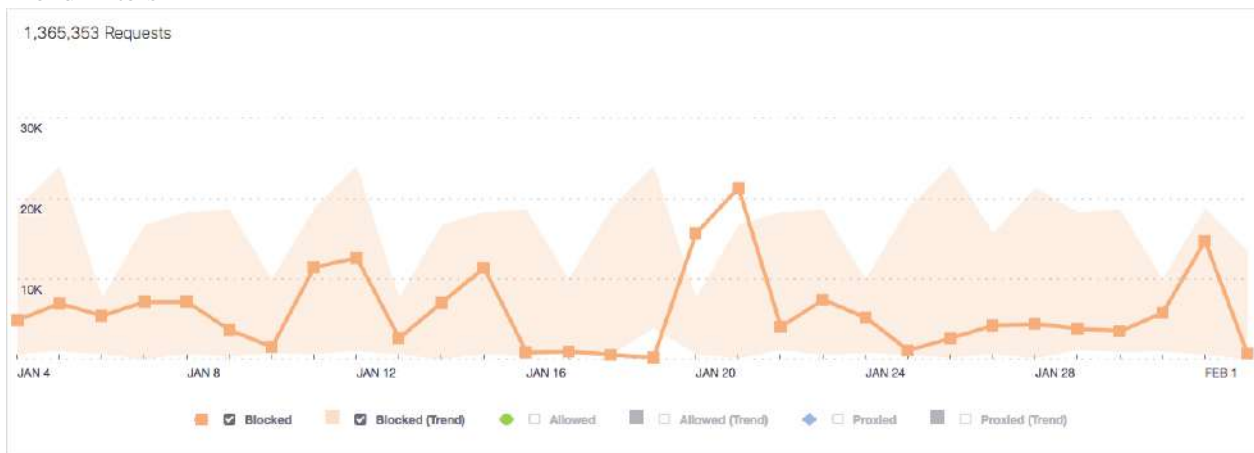
Note: You might notice that you cannot schedule an Identities report or download one either. This is due to the way in which information in this report is presented to you graphically rather than textually. If you'd like to see these features added to this report, email us with a request: umbrella-support@cisco.com.

Activity Charting

Activity charting graphically displays DNS activity for the selected identity within the selected time period. This visualization of DNS activities lets you quickly see where the peaks and valleys are for request activities by that identity. This can help in your investigation of any suspicious activities. At the top of the page, the report lists the number of requests the identity has made during the selected time period. To help you to compare various activities, you can turn various line graphs on and off, overlaying them for quick comparisons.



Trend Filters



A trend filter—Blocked (Trend), Allowed (Trend), and Proxied (Trend)—displays the lowest and highest points of activity along the chart's x-axis for the selected date based on activity going back seven weeks. You can use these filters to compare current activity against past activity. This can help you visualize traffic for an identity over time, letting you get a sense of what its

“normal” activity is, and by extension where there might some sort of unexpected activity or security risk.

Apply trend filters by selecting them underneath the chart. You can turn them all on or off, or just filter for one or two trends. Here, we’ve turned on the Blocked (Trend) filter and applied it against Blocked requests.

Once you’ve turned on a filter, when you hover over a point on the chart, you can see the trend details for that filter at that point in time.



For example, Blocked (Trend) versus current Blocked request activity. You’ll see in the chart above that on Jan 20—a Tuesday—the trend over the last seven Tuesdays has been a minimum of 612 blocked requests and a maximum of 7674. We can also see that for this day (Jan 20) there were 15666 blocked requests, which is more than double the trend of blocked requests for that day. This unusual activity may indicate a security problem that you can further investigate by clicking the Blocked point for this day, which takes you to the Activity Search report for the day clicked.

Security Details

The Security Details area divides itself into "Top Destinations" and "Top Security Categories." The information presented here helps you understand whether the activities of the identity you are investigating pose a risk and helps you determine if you need to make changes to your blocked and allowed destination lists.

Top Destinations	
SECURITY ALL	
Destinations	Requests
stun.sipgate.net	1,663
coathive.com	1,623
stun.ideasip.com	846
stun.internetcalls.com	845
stun.schlund.de	841

[VIEW ALL DESTINATIONS](#)

Top Security Categories	
FireEye Integration	10,194
Malware	7,118
Potentially Harmful	2,738
Cisco AMP Threat Grid Integration	193
Phishing	166
Dynamic DNS	78
Command and Control	52
Newly Seen Domains	4
DNS Tunneling VPN	2

[VIEW ALL CATEGORIES](#)

Top Destinations

Top Destinations lists requests that the identity has made to destinations that pose a security risk, be it malware, phishing, etc. You can also view all top destinations for the identity by selecting the All tab.

1. Click View All Destinations. This takes you to the Reporting > Additional Reports > Top Domains page.

Top Security Categories

Top Security Categories lists the type of security threats that have resulted from requests to visit malicious destinations.

1. Click View All Categories. This takes you to the Reporting > Additional Reports > Top Categories page.

Recent Activity

The Recent Activity area lets you investigate DNS activity for the identity. You can quickly see the destinations requested by the identity, the response to that request (blocked or allowed) and the IP from which the request originated. Viewing this information can help you make decisions about how to maintain your destination lists. Is an identity at risk because it is not being blocked from a malicious site or is it being blocked from domains to which it should have access? You can also use this information to monitor the DNS activities of an identity. Where is that identity going and should you be updating destination lists to block or allow this identity?

Recent Activity for San Francisco

Destination	Response	External IP	Internal IP	Date & Time
com-swtbx2.com	Allowed	[Redacted]	[Redacted]	Feb 2, 2018 at 9:27 AM
actm-norri.wbx2.com	Allowed	[Redacted]	[Redacted]	Feb 2, 2018 at 9:27 AM
com-swtbx2.com	Allowed	[Redacted]	[Redacted]	Feb 2, 2018 at 9:27 AM
clientsfi.google.com	Allowed	[Redacted]	[Redacted]	Feb 2, 2018 at 9:27 AM
analytics.attessa.in.com	Allowed	[Redacted]	[Redacted]	Feb 2, 2018 at 9:27 AM
api.amplitude.com	Allowed	[Redacted]	[Redacted]	Feb 2, 2018 at 9:27 AM
22.client-channel.google.com	Allowed	[Redacted]	[Redacted]	Feb 2, 2018 at 9:27 AM
api.amplitude.com	Allowed	[Redacted]	[Redacted]	Feb 2, 2018 at 9:27 AM
news.ycombinator.com	Allowed	[Redacted]	[Redacted]	Feb 2, 2018 at 9:27 AM
news.ycombinator.com	Allowed	[Redacted]	[Redacted]	Feb 2, 2018 at 9:27 AM

[VIEW ALL RECENT ACTIVITY](#) Page: 1 Rows per page: 10 1 - 10 of 100

1. Click View All Recent Activity to go to the Activity Search page (Reporting > Core Reports > Activity Search) where you can quickly view activity for the selected identity.