Click to verify

You can filter out website activity from an IP address or a range of IP addresses so the data generated by users at those IP addresses don't appear in your reports. You can't filter out internal traffic from app users. You can create up to 10 data filters per property. Warning: Once you apply a data filter, the effect on the data is permanent. For example, if you apply an exclude data filter, the excluded data is never processed and will never be available in Analytics or BigQuery. If you want to hide data from certain reports without permanently filtering out the data, use report filters instead. Filter out internal traffic For subtitles in your language, turn on YouTube captions. Select the settings icon at the bottom of the video player, then select "Subtitles/CC" and choose your language. Before you begin You need the Editor role at the property level to identify internal traffic and create, edit, and delete data filters. Step 1: Identify internal traffic By completing these steps, Analytics adds a traffic_type parameter to every incoming event. You can also manually add the parameter to your events. In Admin, under Data collection and modification, click Data streams. Note: The previous link opens to the last Analytics property you accessed. You can change the property using the property selector. You must be an Editor or above at the property level to identify internal traffic. Click a web data stream. In the web stream details, click Configure tag settings. Click Show more. Click Define internal traffic. Click Create. Enter a name for the rule. Enter a value for the traffic_type parameter. Note: traffic_type is the only event parameter for which you can define a value. internal is the default value, but you can enter a new value (e.g., emea_headquarters) to represent a location from which internal traffic originates. In IP address > Match type, select an operator. In IP address > Value, enter an address or range of addresses that identify traffic from the location you identified in Step 8. You can enter IPv4 or IPv6 addresses. You can also click "What's my IP address?" to find your public IP address. The Value field also supports the use of regular expressions (regex). The following examples show how to identify IP addresses for each operator: IP address equals: 172.16.1.1 IP address begins with: 10.0. IP address ends with: .255 IP address contains: .0.0. IP address is in range (ranges need to be expressed in CIDR notation): 24-bit block (e.g., 10.0.0.0 – 10.255.255.255): 10.0.0.0/8 20-bit block (e.g., 172.16.0.0 – 172.31.255.255): 172.16.0.0/12 16-bit block (e.g., 192.168.0.0 – 192.168.255.255): 192.168.0.0/16 IP address matches regular expression: 192\.0.* (Optional) Click Add condition to set multiple conditions. Any IP addresses that match the conditions will be marked as internal traffic. The conditions are OR conditions rather than AND conditions. Click Create. Using CIDR notation Classless Inter-Domain Routing (CIDR) notation is a way to represent ranges of IP addresses. The following examples use IPv4 addresses. CIDR-notation syntax is the same for IPv6 addresses. IPv4 addresses are 32-bit binary numbers with the values for each octet ranging from 0-255. For example, the IPv4 address 10.10.101.5 has the 32-bit binary equivalent of 00001010.00001010.01100101.00000101 When you express a range of IP addresses in CIDR notation, you indicate how many of the bits are fixed and how many can be of any value. For example, the CIDR notation for the range of addresses 192.128.255.0 - 192.168.255.255 is 192.168.255.0/24. /24 indicates that the first 24 bits (192.128.255) are fixed and the last 8 bits (.0) are wildcards that can take any value (0 is the standard wildcard). If you needed to indicate a range of 192.168.0.0 – 192.168.255.255, you would indicate that the first 16 bits of the address are fixed: 192.168.0.0/16. /16 indicates that the first 16 bits (192.168) are fixed and the last 16 bits (.0.0) are wildcards that can take any value. If you were using IPv6 addresses and wanted to express a range, you would use the same "slash-number" suffix to indicate how many bits of the range are fixed. For example, if the range were 0:0:0:0:0:ffff:c080:ff00 - 0:0:0:0:0:ffff:c080:ffff, you would express the range as 0:0:0:0:0:ffff:c080:ff00/120 (the first 120 bits are fixed). Learn more about CIDR notation. Step 2: Create a data filter In Admin, under Data collection and modification, click Data filters. Note: The previous link opens to the last Analytics property you accessed. You can change the property using the property selector. You must be an Editor or above at the property level to create a data filter. Click Create Filter. Choose Internal Traffic. Enter a name for the data filter. The name must: be unique among data filters in the same property begin with a unicode letter contain only unicode letters and numbers, underscores, and spaces contain up to 40 characters Choose Exclude to filter out events where the value of the traffic_type parameter matches the name you entered in step 10 above. Choose from the following filter states: Testing: Analytics identifies matching data with the "Test data filter name" dimension Active: Analytics applies the data filter to incoming data and makes permanent changes Inactive: Analytics isn't evaluating the filter Note: Your data that satisfies a test data filter is assigned to the "Test data filter name" dimension and given a value of the filter name. That data is available in Explore so you can validate your data filters before you activate them. Learn more Click Create. Testing a data filter Testing a data filter ensures it's successfully filtering out traffic from the IP addresses. Traffic from filtered IP addresses is added to the "Test data filter name" dimension with the filter name as the value. To find events triggered by a filtered IP address, you can build a free-form exploration with these settings: Technique: Free form Rows: Test data filter name, Event name Values: Event count Filter: "Test data filter name contains [the name of your data filter]" A data filter can take between 24 - 36 hours to apply. Check back later if no value is assigned. You can see your sign-in history, including the dates and times that your Gmail account was used. You can also see the IP addresses which were used to access your account. See your account activity On your computer, open Gmail. In the bottom right, click Details. Tip: You can also visit the Recent security events page to see security updates for your entire Google Account. Information shown on the "Activity on this account" page The "Activity on this account" page shows your sign-in records, and includes the information below. Concurrent session information In the "Concurrent session information" section, you'll see if you're signed in to Gmail on another device, browser, or location. Access type In the "Access type" section, you'll see the browser, device, or mail server (like POP or IMAP) that you accessed Gmail from. If you've authorized an application, you'll see the location (IP Address) of the 3rd party application. Location (IP address) You can see the last 10 IP addresses and approximate locations that accessed your Gmail account. If you got a warning about suspicious activity in your account, you might also see up to 3 additional IP addresses that have been labeled as suspicious. There are a few reasons you may see multiple IP addresses or locations in your activity: If you use POP or IMAP to read your mail on other services, like Apple Mail or Microsoft Outlook, this location information will be included, too. If you use Mail Fetcher, a Google IP will show up because your messages are being fetched through a Google server. If you use Gmail on a phone or tablet, your Internet service or mobile carrier's location may show up. This may be a location far from where you are. As long as the name of the carrier matches yours, this isn't unusual. Post to the help community Get answers from community members