GeoIP® IP Risk database

Identify risky IP addresses based on recently observed suspicious behavior

A short history of MaxMind

In 2002, MaxMind began providing IP intelligence through the GeoIP brand. Two years later, using GeoIP data, MaxMind developed the minFraud® service to combat the growing threat of online fraud. Since then, MaxMind has helped thousands of companies cut down fraud-related financial losses and chargebacks, and has reduced these companies' need for manual review of transactions.

GeoIP IP Risk database

MaxMind monitors billions of transactions every year to identify risky behavior that helps thousands of businesses protect themselves against fraud. MaxMind's real time risk scoring API, minFraud, is the best solution for this use case, but some users are unable to send transaction data to MaxMind for processing. Now, MaxMind is making high risk IP addresses available to select customers as a downloadable database, the GeoIP IP Risk database.

What is the IP Risk database?

The GeoIP IP Risk database contains all the IP networks that we have identified as associated with non-corporate proxies, VPNs, and other anonymous IP addresses, as well as other IP addresses that we have seen associated with risky activity. When we see risky activity associated with any of these networks (regardless of whether it is anonymous or not), the GeoIP IP Risk database will also provide an IP risk rating, which can help you assess the riskiness of IP addresses on a case by case basis.

How does the IP Risk database compare to the Anonymous IP database?

The GeoIP IP Risk database contains all the networks and data that can be found in the GeoIP Anonymous and Anonymous Plus databases. If you license the GeoIP IP Risk database, there will be no need to license the GeoIP Anonymous IP database.

In addition to all the data from the GeoIP Anonymous IP database, the IP Risk database contains IP addresses and networks that have been flagged as high risk based on our monitoring of internet traffic. The IP Risk database is an expansion of the Anonymous IP database, adding in new IP addresses that exhibit risky behavior, but which are not associated with a known anonymous network.

Where we have a risk signal for the IPs in the IP Risk database, an IP risk rating will be included. This means that some of the IPs that were already present in the Anonymous IP database will have a risk rating, and the new IPs that are exclusive to the IP Risk database will also have a risk rating.

Data fields in the IP risk database

The IP Risk database, like all GeoIP databases, is indexed by the network represented in CIDR notation. In addition to the network, it contains the following data fields (click on each data field name to learn more).

Data field name	Data field description
`ip_risk`	A rating of the riskiness of the IP address or network, derived from our realtime fraud detection service, minFraud, which screens billions of online transactions per year
`is_anonymous`	A flag used to identify IP addresses used by an anonymizing network.
`is_anonymous_vpn`	These are IP addresses registered to known services that offer users a tunnel to a VPN server, which serves to hide the true IP address.
`is_hosting_provider`	These are IP addresses associated with hosting services that are likely to be used as anonymizers. This anonymizer type also includes both registered and non-registered anonymizing VPN services.
`is_public_proxy`	These are proxies that are available for free and publicly posted.
`is_tor_exit_node`	These are IP addresses from which Tor users will access the internet. The Tor Project is an open network used by those who wish to maintain anonymity.
`is_residential_proxy`	These are IP addresses on a suspected anonymizing network that are registered under residential ISPs (does not include peer-to-peer proxy IPs).
`provider_name`	The name of the VPN provider associated with the network.
`anonymizer_confidence`	A score from 1 to 99 indicating the likelihood that the network is currently part of an actively used VPN service. At launch, only values of 30 and 99 will be provided, with more granular ratings introduced over time.
`network_last_seen`	The last day the network was detected in our analysis of VPN networks.

Not all IP networks have a risk rating attached to them, nor will all IP networks have anonymizer flags attached.

Use IP risk rating to identify bad actors

The IP risk rating tells you how risky we assess an IP or network to be based on activity that we've seen in our monitoring of internet traffic over the past 7 days. The higher the risk rating, the more likely the IP address is to be associated with risky behavior. You can use the ip_risk rating to decide whether to allow access to your products or services to low-risk anonymous IPs, and to restrict access to high-risk IPs which are not anonymous.

IP risk rating values

In our pilot version of the IP Risk database, you will see the following possible values for the IP risk rating. The higher the value, the more risky the IP. As we continue to refine the product and bring in more data sources, you may expect to see new values for ip_risk:

While IP Risk score values range from 0.01 to 99.99, in practice these tend to fall into a number of discrete buckets. The possible values that may appear in the dataset are subject to change without notice, but will remain within the specified range.

> **Lower scores** (closer to 0) indicate lower risk, meaning the transaction appears more legitimate.
>
> **Higher scores** (closer to 99) indicate higher risk, meaning the transaction has more characteristics associated with fraud.

What counts as "low" or "high" depends on your risk tolerance. MaxMind doesn't define fixed cutoffs. However, here's a general guide:

- Scores below 5.00 are often considered low risk and are commonly accepted by default.
- Scores above 30 or 50 are more suspicious and may be flagged for manual review or blocked entirely.

The threshold you set should reflect your business priorities. For example, if your focus is on reducing chargebacks, you may want to be stricter. If you're more concerned about conversion rates, you may allow higher-risk transactions through. MaxMind recommends adjusting the threshold over time based on your results.

Technical details

The GeoIP IP Risk database comes in two different file formats, updated daily:

- CSV (comma separated values)
  - good for importing into SQL and other databases
  - good for manipulating data and joining with other sources

	A	B	C	D	E	F	G	H
1	network	ip_risk	is_anonymous	is_anyonmous_v	is_hosting_provider	is_public_proxy	is_tor_exit_node	is_residential_proxy
2	6.141.138.214	75						
3	6.148.160.57	75						
4	7.245.246.166	45.25						
5	11.159.119.176	45.25						
6	11.91.182.146	45.25						
7	21.142.29.113	75						
8	26.120.245.158	45.25						
9	28.181.121.238	75	1			1		
10	29.93.165.191		1			1		
11	33.221.168.10	75	1			1		
12	214.240.174.215	45.25						

(Sample data for the CSV version of the GeoIP IP Risk database. See our developer tutorials to learn best practices for importing MaxMind CSV databases into MySQL and PostgreSQL.)

- MMDB (binary database)
  - good for fast lookups
  - smaller file size compared to the CSV version of a database
  - uses official client APIs from MaxMind

Data field name	Value type	Data field description
`ip_risk`	decimal	A percentage ranging from 0.01 to 99. For example, an IP risk score of 15.40 means that the transaction has a 15.4% chance of being fraudulent based on the IP address alone.
`is_anonymous`	boolean	This is `true` if the IP address belongs to any sort of anonymous network. Otherwise, the key is not included in the `traits` object.
`is_anonymous_vpn`	boolean	This is `true` if the IP address is registered to an anonymous VPN provider. Otherwise, the key is not included in the `traits` object. If a VPN provider does not register subnets under names associated with them, we will likely only flag their IP ranges using the is_hosting_ provider flag.
`is_hosting_provider`	boolean	This is `true` if the IP address belongs to a hosting or VPN provider (see description of `is_anonymous_vpn` flag). Otherwise, the key is not included in the traits object.
`is_public_proxy`	boolean	This is `true` if the IP address belongs to a public proxy. Otherwise, the key is not included in the `traits` object.
`is_tor_exit_node`	boolean	This is `true` if the IP address is a Tor exit node. Otherwise, the key is not included in the `traits` object.
`is_residential_proxy`	boolean	This is `true` if the IP address is on a suspected anonymizing network and belongs to a residential ISP (does not include peer-to-peer proxy IPs). Otherwise, the key is not included in the `traits` object.
`provider_name`	string	The name of the VPN provider (e.g., NordVPN, SurfShark, etc.) associated with the network. Note that MaxMind identifies a subset of VPN providers. A current list of VPN providers identified in the Anonymous Plus database is available on request.
`anonymizer_confidence`	integer	A score ranging from 1 to 99 that is our percent confidence that the network is currently part of an actively used VPN service. Currently we will only provide values of 30 and 99, but the number of values will increase as we improve our confidence ratings.
`network_last_seen`	string	The last day that the network was sighted in our analysis of anonymized networks. This is in the ISO 8601 date format.

MaxMind, Inc.
51 Pleasant Street #1020
Malden, MA 02148
USA
www.maxmind.com