

Intrusion



Shield OnPremise

Dashboard User Manual



Table of Contents

| | | | |
|--------------------------------------|----|-------------------------------------|----|
| Logging In | 3 | Users | 23 |
| | | Users | 23 |
| | | Logs | 23 |
| Dashboard Breakdown | 5 | | |
| Shield Activity | 5 | Admin | 24 |
| DNS Health | 5 | Shield Settings | 24 |
| TCP Health | 8 | Shield Mode | 24 |
| UDP Health | 11 | SNMP | 25 |
| Top High Risk Categories, 24H | 13 | Syslog | 25 |
| Top Killed Domains, 24H | 14 | Management Interface | 26 |
| Traffic Killed by Country, 24H | 14 | Remote Support | 26 |
| Country Risk Level | 15 | Landing Page Settings | 27 |
| Top Requested Domains | 16 | Overview | 27 |
| Offending Devices, 24H | 17 | Landing Page Logo | 27 |
| | | Landing Access IPs | 27 |
| Traffic Tab | 18 | Shield Info | 28 |
| Record Session | 18 | | |
| Map | 19 | Using Shield OnPremise | 29 |
| All Traffic | 20 | | |
| Reports | 20 | | |
| | | | |
| Permits | 21 | | |
| Manual Permits | 21 | | |
| Auto Permits | 22 | | |

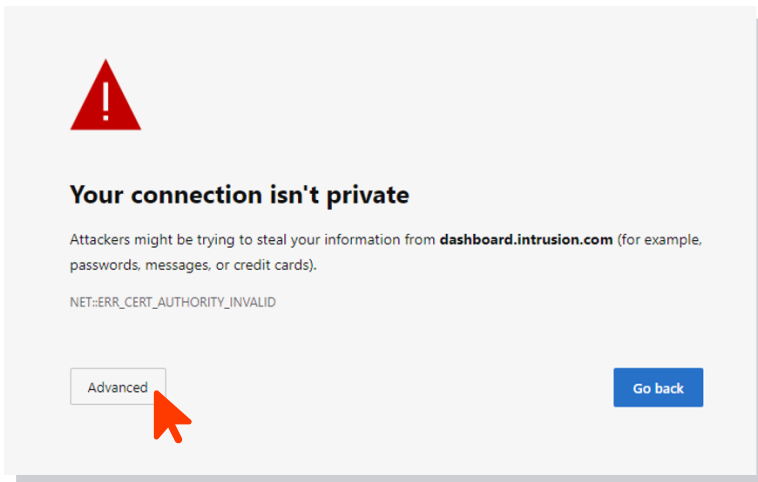


Logging In

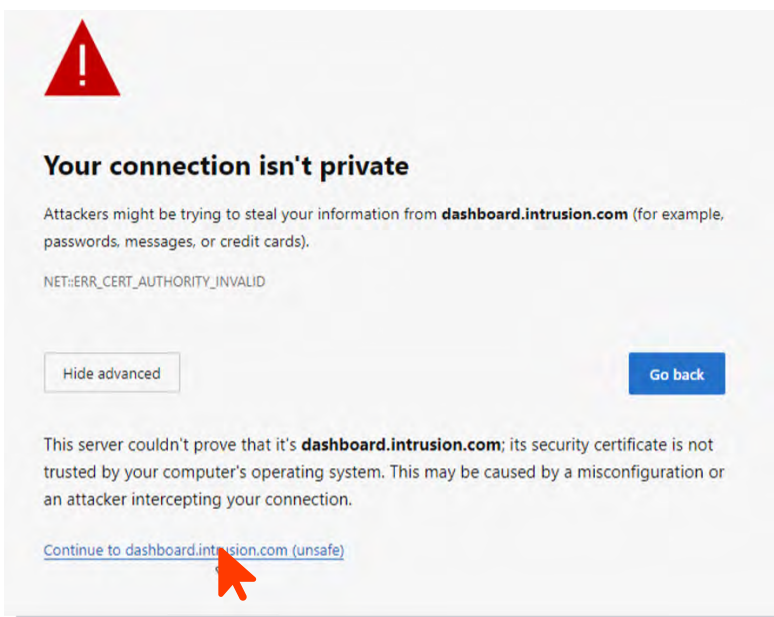
To log into the Shield Dashboard, launch a web browser and enter: dashboard.intrusion.com. If the page is unreachable, enter the IP address that was assigned to the Shield's Management port instead.

- > Upon successful connection to the Shield, a warning labeled "Your connection isn't private" will be displayed. This is because Shield uses a self-signed certificate.

Click **Advanced** to proceed.



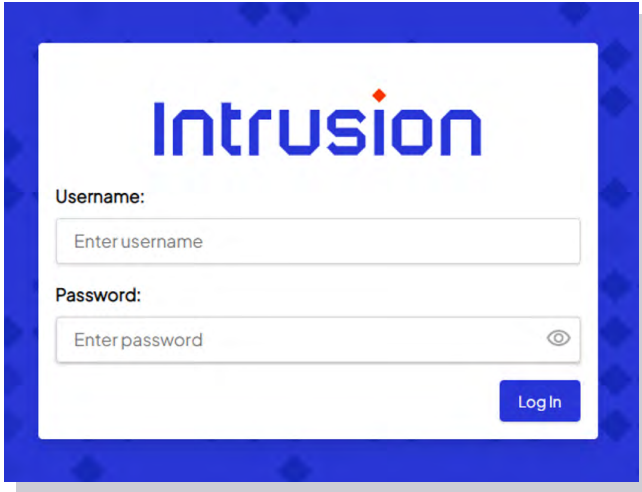
Next, click **Continue to dashboard.intrusion.com (unsafe)**





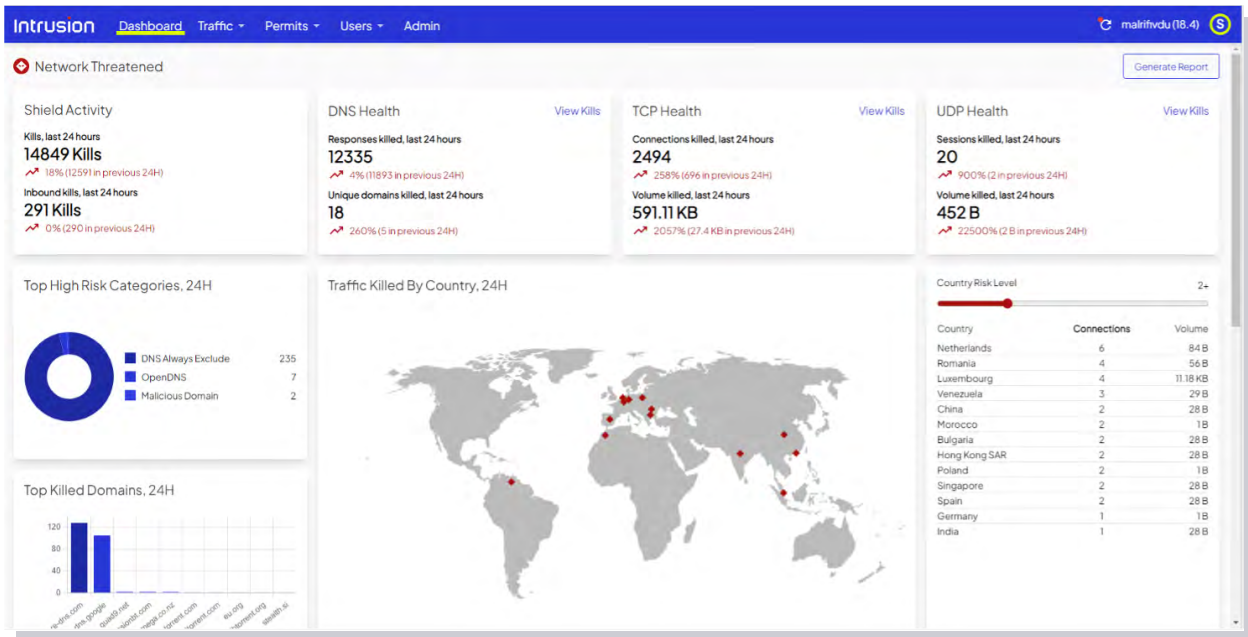
The dashboard login page should now be accessible.

- > Use the username and password that you received from Intrusion.
If you don't have this information, please contact customer support.
- > Once you're logged in, the main dashboard should be visible.



The dashboard will give you an overview of key security-related information generated by the Shield in the last 24 hours.

- > This information should instantly refresh your situational awareness, enabling you to gauge your current security posture at a glance.



Dashboard Breakdown

Shield Activity

The Shield Activity card displays the Shield's total kills within the last 24 hours.

- > That value is the sum of the DNS, TCP and UDP kills displayed on the three other cards to the right.
- > This card also shows the percent of change from the previous 24-hour period.
- > In addition, it also shows the total inbound kills and its corresponding percentage change.



DNS Health

The DNS Health card displays DNS responses killed over the last 24 hours, as well as a breakdown of the number of unique domains killed during that time. It also shows the percent of change from the previous 24-hour period.

- > A DNS response originating from a malicious host is indicative of a cyber attack.
- > To mitigate the risk of DNS-based attacks, Intrusion may block or kill a DNS response depending on the reputation of the DNS Query, the DNS response, or the Resolved IP.
- > In many cases, multiple DNS responses may come from the same domain. That domain is counted as one unique domain.

Click **View Kills** in the top right corner of the card to display a table showing relevant traffic details for DNS Health.

- > Each row in the table represents a DNS resolution passing through the Shield.





Traffic Details (5/13/2023 at 13:02:00 to 5/14/2023 at 13:02:00)

| Search for anything | | | | | | | | | | | |
|---------------------------------|------|--------|--------------|----------|--------------|-------|---------------|-----------|-----------------|---------------------|---------------------|
| Search | | Filter | Sort | Download | + Add Permit | | DNS Responses | | TCP Connections | UDP Sessions | |
| Status | Risk | VLAN | Client IP | Cli... | Server IP | Se... | Re... | Direction | Responses | First Seen | Last Seen |
| <input type="checkbox"/> Killed | 4 | | 172.16.133.6 | jsr... | 8.8.8.8 | | ap... | Inbound | 24 | 2023-05-14 13:45:05 | 2023-05-15 12:45:05 |
| <input type="checkbox"/> Killed | 4 | | 172.16.133.6 | jsr... | 8.8.8.8 | | 46... | Inbound | 24 | 2023-05-14 13:45:08 | 2023-05-15 12:45:08 |
| <input type="checkbox"/> Killed | 4 | | 172.16.133.6 | jsr... | 8.8.8.8 | | 97... | Inbound | 24 | 2023-05-14 13:45:04 | 2023-05-15 12:45:04 |
| <input type="checkbox"/> Killed | 4 | | 172.16.133.6 | jsr... | 8.8.8.8 | | ai... | Inbound | 48 | 2023-05-14 13:45:05 | 2023-05-15 12:45:07 |
| <input type="checkbox"/> Killed | 4 | | 172.16.133.6 | jsr... | 8.8.8.8 | | ad... | Inbound | 48 | 2023-05-14 13:45:03 | 2023-05-15 12:45:05 |
| <input type="checkbox"/> Killed | 4 | | 172.16.133.6 | jsr... | 8.8.8.8 | | ad... | Inbound | 24 | 2023-05-14 13:45:06 | 2023-05-15 12:45:06 |
| <input type="checkbox"/> Killed | 4 | | 172.16.133.6 | jsr... | 8.8.8.8 | | ad... | Inbound | 24 | 2023-05-14 13:45:07 | 2023-05-15 12:45:07 |
| <input type="checkbox"/> Killed | 4 | | 172.16.133.6 | jsr... | 8.8.8.8 | | ad... | Inbound | 24 | 2023-05-14 13:45:03 | 2023-05-15 12:45:03 |
| <input type="checkbox"/> Killed | 4 | | 172.16.133.6 | jsr... | 8.8.8.8 | | ad... | Inbound | 24 | 2023-05-14 13:45:06 | 2023-05-15 12:45:06 |
| <input type="checkbox"/> Killed | 4 | | 172.16.133.6 | jsr... | 8.8.8.8 | | ad... | Inbound | 24 | 2023-05-14 13:45:06 | 2023-05-15 12:45:06 |
| <input type="checkbox"/> Killed | 4 | | 172.16.133.6 | jsr... | 8.8.8.8 | | ad... | Inbound | 24 | 2023-05-14 13:45:03 | 2023-05-15 12:45:03 |
| <input type="checkbox"/> Killed | 4 | | 172.16.133.6 | jsr... | 8.8.8.8 | | ad... | Inbound | 24 | 2023-05-14 13:45:07 | 2023-05-15 12:45:07 |
| <input type="checkbox"/> Killed | 4 | | 172.16.133.6 | jsr... | 8.8.8.8 | | ad... | Inbound | 24 | 2023-05-14 13:45:02 | 2023-05-15 12:45:02 |

Items: 25 Showing 1 to 25 of 399 entries < > >>

The column descriptions are as follows:

| | |
|------------------------|--|
| Status | <p>Passed if the DNS response was allowed</p> <p>Killed if the DNS response was killed based on the reputation of the DNS Query, the DNS response, or the Resolved IP</p> <p>Note: if the Shield is in Observe mode, the Status column shows what would have been killed if the Shield was in Protect mode</p> |
| Risk | Risk level of the resolved DNS Query or DNS response (ranked from 1–5, with 1 being the lowest risk and 5 the highest) |
| VLAN | VLAN on which this packet was observed, if present |
| Client IP | IP address of the DNS Client performing the DNS query |
| Client Hostname | The derived hostname of the client IP as observed in other DNS requests |
| Server IP | IP address of the DNS Server answering the DNS query |
| Server Hostname | The derived hostname of the server IP as observed in other DNS requests |
| Requested | Hostname requested in the DNS transaction |



| | |
|------------------|---|
| Direction | <p>Direction of the DNS response:</p> <p>Inbound if the client IP is on an internal network and the server IP is on an external network</p> <p>Outbound if the client IP is on an external network and the server IP is on an internal network</p> <p>Internal if both client IP and server IP are on internal networks</p> <p>Unknown if both client IP and server IP are on external networks</p> <p><i>Note this is the direction of the response packet, not the query packet</i></p> |
| Responses | Count of DNS RR records that were observed. Note there may be multiple DNS RR records in one DNS packet |
| FirstSeen | First time this event was seen in the observation period, in local browser time |
| LastSeen | Last time this event was seen in the observation period, in local browser time |

Click on a row to drill down for more details.

| | | | | | | | | | |
|---|---|---|--------|--|-------|--|----|---------------------|---------------------|
| <input type="checkbox"/> - Killed | 4 | 172.16.133.6 | jsr... | 8.8.8.8 | ap... | Inbound | 24 | 2023-05-14 13:45:05 | 2023-05-15 12:45:05 |
| <p>Details</p> <p>Client IP: 172.16.133.6</p> <p>Client Hostname: jsrvr27.jaalam.net</p> <p>Server IP: 8.8.8.8</p> <p>Server Hostname:</p> <p>First Seen: 2023-05-14 13:45:05</p> <p>Last Seen: 2023-05-15 12:45:05</p> | | <p>DNS</p> <p>QNAME: api.freebase.com</p> <p>Domain: freebase.com</p> <p>CNAME: api.freebase.com</p> <p>Answer(s): 208.68.110.117</p> | | <p>Location</p> <p>Client Location: Local</p> <p>Server Location: US</p> | | <p>Risk</p> <p>Risk Source: api.freebase.com</p> <p>Risk Level: 4</p> <p>Risk Class: High Risk Category</p> <p>Risk Description:</p> <p>This domain was killed because it has content that has been categorized as high risk content: malware distribution, gambling, pornography, illegal activity, hacking, etc.</p> | | | |

The following table describes each attribute shown above:

Note: Some attributes have already been defined in the previous table.

| | |
|------------------------|---|
| QName | The hostname queried or requested in the DNS transaction |
| Domain | The derived registered domain name of the QName |
| CNAME | If the DNS response returns CNAME entries, the final CNAME that resolves to an IP address |
| Answers | The list of Ipv4 or Ipv6 addresses to which the DNS response resolves |
| Client Location | The approximate geolocation of the Client IP, based on an IP geolocation database |

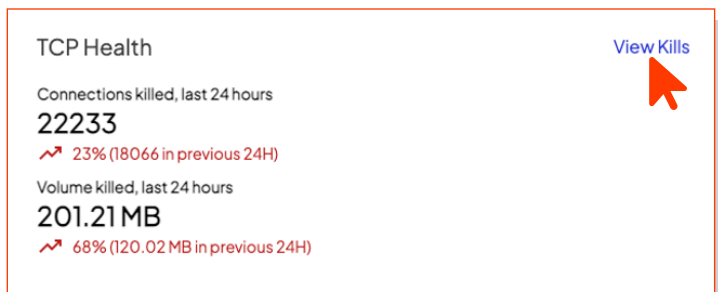


| | |
|-------------------------|---|
| Server Location | The approximate geolocation of the Server IP. If present, the traffic map and country listing will include statistics from this DNS record. |
| Risk Source | The QName, CNAME or Answer IP that resulted in potential risk |
| Risk Level | Level of risk for the DNS QName or CNAME (ranked 1–5, with 1 being the lowest risk and 5 being the highest risk) |
| Risk Class | Generic category of risk |
| Risk Description | Description of the risk class |

TCP Health

The TCP Health card displays TCP connections killed over the last 24 hours, as well as the volume (expressed in Bytes) of connections killed during that time. It also shows the percent of change for each value from the previous 24-hour period.

A device or host in your organization that purposely or inadvertently establishes a TCP connection with a malicious client or server can put your organization at risk. To mitigate that risk, Intrusion may kill the said TCP connection based on the reputation of the client or server.



Click **View Kills** in the top right corner of the card to display a table showing relevant traffic details for TCP Health.



Each row in the table represents a TCP connection passing through the Shield.

Traffic Details (5/16/2023 at 14:02:00 to 5/17/2023 at 14:02:00)

Search for anything Search Filter Sort Download + Add Permit ? DNS Responses TCP Connections UDP Sessions

| <input type="checkbox"/> | Status | VLAN | Client IP | Client Hostname | Server IP | Server Hostname | Port | Direction | Connections | First Seen | Last Seen |
|--------------------------|----------|------|---------------|-----------------|----------------|-----------------|-------|-----------|-------------|---------------------|---------------------|
| <input type="checkbox"/> | ▶ Killed | | 108.13.7.222 | | 172.16.133.78 | | 59306 | Inbound | 24 | 2023-05-17 14:45:05 | 2023-05-18 13:45:09 |
| <input type="checkbox"/> | ▶ Killed | | 172.16.133.12 | | 64.94.107.58 | | 80 | Outbound | 72 | 2023-05-17 14:45:03 | 2023-05-18 13:45:04 |
| <input type="checkbox"/> | ▶ Killed | | 172.16.133.12 | | 64.94.107.63 | | 80 | Outbound | 72 | 2023-05-17 14:45:03 | 2023-05-18 13:45:04 |
| <input type="checkbox"/> | ▶ Killed | | 172.16.133.16 | | 208.85.44.32 | | 80 | Outbound | 24 | 2023-05-17 14:45:06 | 2023-05-18 13:45:07 |
| <input type="checkbox"/> | ▶ Killed | | 172.16.133.18 | | 217.118.26.135 | ocsp... | 80 | Outbound | 24 | 2023-05-17 14:45:07 | 2023-05-18 13:45:08 |
| <input type="checkbox"/> | ▶ Killed | | 172.16.133.20 | | 64.94.107.18 | | 80 | Outbound | 48 | 2023-05-17 14:45:01 | 2023-05-18 13:45:03 |
| <input type="checkbox"/> | ▶ Killed | | 172.16.133.28 | | 64.94.107.55 | | 80 | Outbound | 72 | 2023-05-17 14:45:03 | 2023-05-18 13:45:04 |
| <input type="checkbox"/> | ▶ Killed | | 172.16.133.28 | | 64.94.107.62 | | 80 | Outbound | 384 | 2023-05-17 14:45:01 | 2023-05-18 13:45:09 |
| <input type="checkbox"/> | ▶ Killed | | 172.16.133.28 | | 167.8.226.13 | t.poi... | 80 | Outbound | 144 | 2023-05-17 14:45:07 | 2023-05-18 13:45:09 |
| <input type="checkbox"/> | ▶ Killed | | 172.16.133.29 | | 64.94.107.11 | | 80 | Outbound | 312 | 2023-05-17 14:45:01 | 2023-05-18 13:45:08 |
| <input type="checkbox"/> | ▶ Killed | | 172.16.133.29 | | 64.94.107.46 | | 80 | Outbound | 192 | 2023-05-17 14:45:01 | 2023-05-18 13:45:08 |
| <input type="checkbox"/> | ▶ Killed | | 172.16.133.30 | | 208.93.140.140 | orig-... | 80 | Outbound | 24 | 2023-05-17 14:45:05 | 2023-05-18 13:45:07 |
| <input type="checkbox"/> | ▶ Killed | | 172.16.133.39 | | 74.122.143.12 | al.int... | 80 | Outbound | 24 | 2023-05-17 14:45:01 | 2023-05-18 13:45:08 |

The column descriptions are as follows:

| | |
|------------------------|---|
| Status | <p>Passed if the TCP connection was allowed</p> <p>Killed if the TCP connection was killed based on the reputation of the TCP Client IP or TCP Server IP</p> <p>Note: if the Shield is in Observe mode, the Status column shows what would have been killed if the Shield was in Protect mode</p> |
| VLAN | VLAN on which this packet was observed, if present |
| Client IP | <p>IP address of the guessed endpoint performing the client role in the connection/session</p> <p>If the TCP SYN packet is observed, then the Client IP is known</p> <p>If the TCP SYN packet is not observed, then this is a guess based on sender/receiver port numbers</p> |
| Client Hostname | The derived hostname of the client IP as observed in other DNS requests |
| Server IP | <p>IP address of the guessed endpoint performing the server role in the connection/session</p> <p>For TCP, if the TCP SYN packet is observed, then the Server IP is known</p> <p>If the TCP SYN packet is not observed, then this is a guess based on sender/receiver port numbers</p> |
| Server Hostname | The derived hostname of the server IP as observed in other DNS requests |



| | |
|------------------------|--|
| Port | The TCP server port. If the TCP SYN packet is observed, then the server port is known If the TCP SYN packet is not observed, then this is a guess based on client/server port numbers |
| Direction | Direction of the client relative to the server Outbound if the client IP is on an internal network and the server IP is on an external network Inbound if the client IP is on an external network and the server IP is on an internal network Internal if both client IP and server IP are on internal networks Unknown if both client IP and server IP are on external networks |
| Responses (TCP) | Count of the number of TCP SYN packets observed for this ClientIP/ServerIP/ServerPort tuple, or a minimum value of 1 if the TCP handshake was not seen |
| FirstSeen | First time this event was seen in the observation period, in local browser time |
| LastSeen | Last time this event was seen in the observation period, in local browser time |

Click on a row to drill down for more details.

| <input type="checkbox"/> | Status | VLAN | Client IP | Clie... | Server IP | Serv... | Port | Direction | Connections | First Seen | Last Seen |
|---------------------------------|----------|------|-------------------------|---------|---------------|------------------------|-------|-----------|---------------------------|---------------------|---------------------|
| <input type="checkbox"/> | - Killed | | 108.13.7.222 | | 172.16.133.78 | | 59306 | Inbound | 24 | 2023-07-17 11:45:05 | 2023-07-18 10:45:09 |
| Details | | | TCP | | | Location | | | Risk | | |
| Client IP: 108.13.7.222 | | | Client Volume: 9.58 MB | | | Client Location: US | | | Risk Source: 108.13.7.222 | | |
| Client Hostname: | | | Server Volume: 62.48 KB | | | Server Location: Local | | | | | |
| Server IP: 172.16.133.78 | | | Port Desc: | | | | | | | | |
| Server Hostname: | | | | | | | | | | | |
| First Seen: 2023-07-17 11:45:05 | | | | | | | | | | | |
| Last Seen: 2023-07-18 10:45:09 | | | | | | | | | | | |

The following table describes each attribute shown above:

Note: Some attributes have already been defined in the previous table.

| | |
|------------------------|--|
| Client Volume | A sum of UDP payload observed (expressed in Bytes) sent from the client IP to the server IP for all connections associated with this row |
| Server Volume | A sum of UDP payload observed (expressed in Bytes) sent from the server IP to the client IP for all connections associated with this row |
| Client Location | The approximate geolocation of the Client IP, based on an IP geolocation database |



| | |
|------------------------|--|
| Server Location | The approximate geolocation of the Server IP If present, the traffic map and country listing will include statistics from this UDP record |
| Risk Source | The endpoint (client IP or server IP, or both) that triggered the risk alert |

UDP Health

The UDP Health card displays UDP sessions killed over the last 24 hours, as well as the volume (expressed in Bytes) of sessions killed during that time. It also shows the percent of change for each value from the previous 24-hour period.

A device or host in your organization that purposely or inadvertently takes part in a UDP session with a malicious client or server can put your organization at risk. To mitigate that risk, Intrusion may kill the said UDP session based on the reputation of the client or server.

UDP Health View Kills

Sessions killed, last 24 hours
1133
↗ 39% (816 in previous 24H)

Volume killed, last 24 hours
65.75 KB
↘ -66% (192.16 KB in previous 24H)

Click **View Kills** in the top right corner of the card to display a table showing relevant traffic details for UDP Health. Each row of the table represents a UDP session passing through the Shield.

Traffic Details (5/16/2023 at 14:02:00 to 5/17/2023 at 14:02:00)

Search for anything Search Filter Sort Download + Add Permit ? DNS Responses TCP Connections UDP Sessions

| <input type="checkbox"/> | Status | VLAN | Client IP | Client... | Server IP | Serve... | Port | Direction | Sessions | First Seen | Last Seen |
|--------------------------|----------|------|---------------|-----------|----------------|-----------|-------|-----------|----------|---------------------|---------------------|
| <input type="checkbox"/> | ▶ Killed | | 192.168.1.138 | | 54.203.171.68 | stun.k... | 123 | Outbound | 619 | 2023-05-17 14:30:10 | 2023-05-18 13:30:11 |
| <input type="checkbox"/> | ▶ Killed | | 192.168.2.41 | | 52.45.237.36 | | 123 | Outbound | 48 | 2023-05-17 15:00:05 | 2023-05-18 14:00:05 |
| <input type="checkbox"/> | ▶ Killed | | 172.16.133.40 | | 82.76.30.122 | | 8323 | Outbound | 48 | 2023-05-17 14:45:06 | 2023-05-18 13:45:07 |
| <input type="checkbox"/> | ▶ Killed | | 172.16.133.40 | | 202.79.18.77 | | 34878 | Outbound | 72 | 2023-05-17 14:45:05 | 2023-05-18 13:45:06 |
| <input type="checkbox"/> | ▶ Killed | | 192.168.1.138 | | 144.76.59.84 | | 36653 | Outbound | 383 | 2023-05-17 14:30:02 | 2023-05-18 13:30:10 |
| <input type="checkbox"/> | ▶ Killed | | 172.16.133.47 | | 80.216.214.203 | | 53951 | Outbound | 72 | 2023-05-17 14:45:06 | 2023-05-18 13:45:07 |



The column descriptions are as follows:

| | |
|------------------------|--|
| Status | Passed if the UDP session was allowed Killed if the UDP session was killed based on the reputation of the UDP Client IP or UDP Server IP. Note: if the Shield is in Observe mode, it shows what would have been killed if the Shield was in Protect mode |
| VLAN | VLAN on which this packet was observed, if present |
| Client IP | IP address of the guessed endpoint performing the client role in the connection/session For UDP , as UDP sessions are stateless, this is a guess based on sender/receiver port numbers. |
| Client Hostname | The derived hostname of the client IP as observed in other DNS requests |
| Server IP | IP address of the guessed endpoint performing the server role in the connection/session For UDP, as UDP sessions are stateless, this is a guess based on sender/receiver port numbers |
| Server Hostname | The derived hostname of the server IP as observed in other DNS requests |
| Port | The UDP server port. For UDP, this is a guess based on sender/receiver port numbers |
| Direction | Direction of the client relative to the server Outbound if the client IP is on an internal network and the server IP is on an external network Inbound if the client IP is on an external network and the server IP is on an internal network Internal if both client IP and server IP are on internal networks Unknown if both client IP and server IP are on external networks |
| Sessions (UDP) | Count of the number of packets observed for this ClientIP/ServerIP/ServerPort tuple |
| First Seen | First time this event was seen in the observation period, in local browser time |
| Last Seen | Last time this event was seen in the observation period, in local browser time |

Click on a row to drill down for more details.

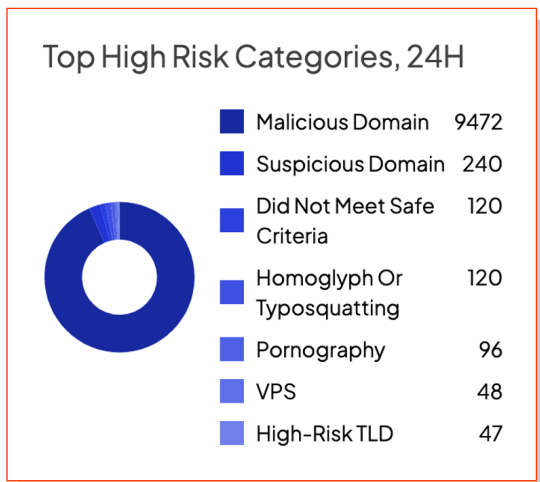
The following table describes each attribute shown above:

Note: Some attributes have already been defined in the previous table.

| | |
|------------------------|--|
| Client Volume | A sum of UDP payload observed (expressed in Bytes) sent from the client IP to the server IP for all connections associated with this row |
| Server Volume | A sum of UDP payload observed (expressed in Bytes) sent from the server IP to the client IP for all connections associated with this row |
| Client Location | The approximate geolocation of the Client IP, based on an IP geolocation database |
| Server Location | The approximate geolocation of the Server IP If present, the traffic map and country listing will include statistics from this UDP record |
| Risk Source | The endpoint (client IP or server IP, or both) that triggered the risk alert |

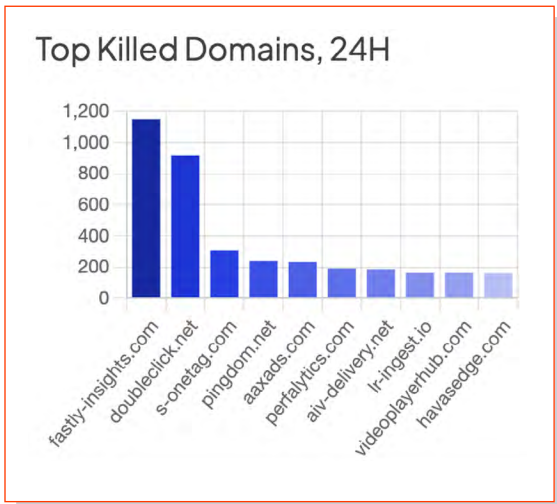
Top High Risk Categories, 24H

This chart shows a breakdown of top high risk categories and the number of kills for each category in the last 24 hours.



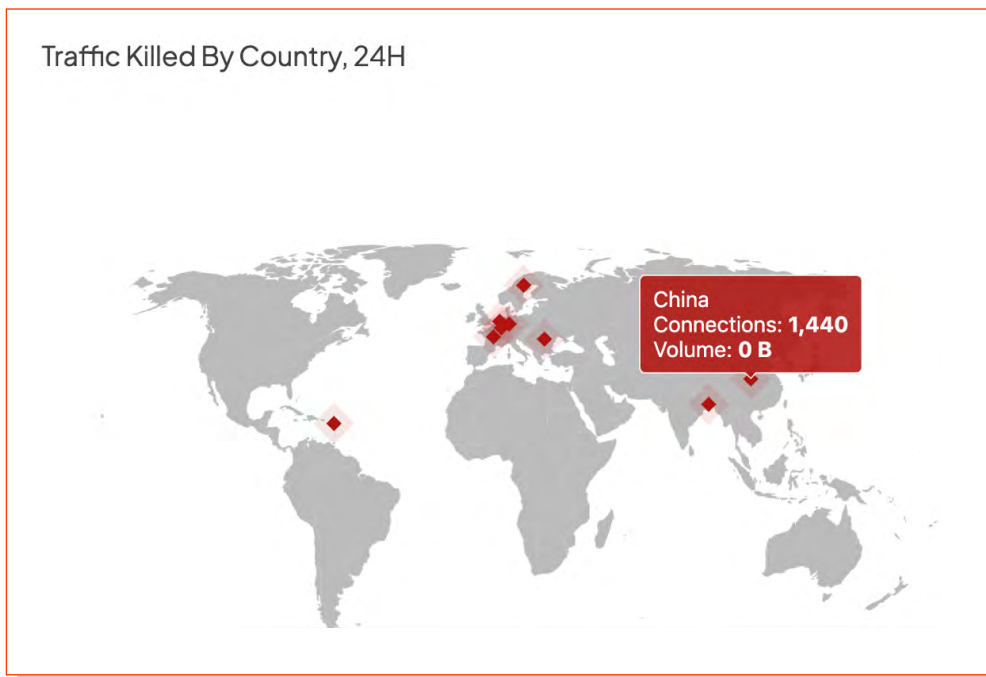
Top Killed Domains, 24H

This chart shows a breakdown of top killed domains, and the number of kills for each domain in the last 24 hours.



Traffic Killed By Country, 24H

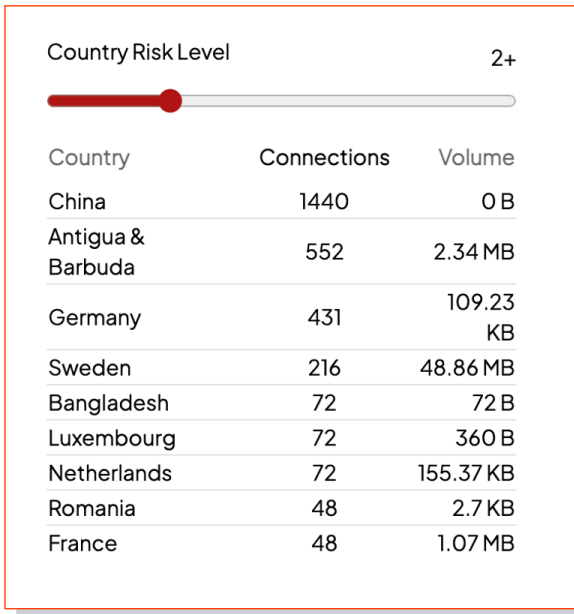
This map shows a breakdown of traffic killed by country, including the number of connections and volume killed. It directly correlates to the Country Risk Level Slider to the right.





Country Risk Level

This interactive slide chart shows Country, Connections, and Volume and reflects it on the map to the left. Move the slide to a chosen risk level to see the results displayed. The Country Risk Level value is a static value assigned per country based on the general risk level of threats emanating from that country. The Country Risk Level is representative of a country as a whole and is unrelated to the DNS Risk Level.






Top Requested Domains

This chart depicts the top requested domains, the number of requests, and the domain's percent of the total number of requests for the last 24 hours. Domains in red with the Intrusion avatar represent killed domains.

Top Requested Domains, 24H [View All](#)

| Domain | Requests | % of Total |
|---|----------|------------|
| akamaiedge.net | 3072 | 3.2% |
| stripe.com | 2874 | 3% |
| google.com | 2560 | 2.6% |
| akamai.net | 2256 | 2.3% |
| yahoo.com | 1870 | 1.9% |
| hulu.com | 1637 | 1.7% |
| microsoft.com | 1576 | 1.6% |
| amazon.com | 1416 | 1.5% |
| cloudfront.net | 1340 | 1.4% |
| salesforce.com | 1319 | 1.4% |
| amazonaws.com | 1318 | 1.4% |
| twitter.com | 1318 | 1.4% |
|  fastly-insights.com | 1145 | 1.2% |

Click **View All** to load a page that shows all the domains, as well as corresponding request count and percent of total.

Select an option button to filter by **All**, **Killed**, or **Passed** for the past 24 hours. You may also utilize the search bar to filter for a specific domain.

Dashboard / Domains Top Domains (24H)

| Domain | Requests | % Of Total |
|----------------|----------|------------|
| akamaiedge.net | 3072 | 3.2% |
| stripe.com | 2874 | 3% |
| google.com | 2560 | 2.6% |
| akamai.net | 2256 | 2.3% |
| yahoo.com | 1870 | 1.9% |
| hulu.com | 1637 | 1.7% |
| microsoft.com | 1576 | 1.6% |
| amazon.com | 1416 | 1.5% |
| cloudfront.net | 1340 | 1.4% |
| salesforce.com | 1319 | 1.4% |
| twitter.com | 1318 | 1.4% |

Domain Status

All

Killed

Passed



Offending Devices, 24H

This chart shows internal offending devices for the last 24 hours. Sorted by risk level, each item displays the risk level, device IP, domain (if available), number of killed connections, and the killed volume. The Offending Devices risk level is a calculated score based on the Domain Risk Level of the requests from the device in question and its volume of high-risk connections.

| Risk | Device IP | Domain | Killed Connections | Killed Volume |
|------|----------------|--------------------|--------------------|---------------|
| 4 | 172.16.133.6 | jsrvr27.jaalam.net | 4440 | 0 B |
| 4 | 172.16.133.41 | | 864 | 427.29 KB |
| 4 | 172.16.133.48 | | 360 | 38.16 KB |
| 4 | 172.16.133.54 | | 2256 | 5.62 MB |
| 4 | 172.16.133.56 | | 168 | 265.07 KB |
| 4 | 172.16.133.73 | | 552 | 24 B |
| 4 | 172.16.133.78 | | 1245 | 23.3 MB |
| 4 | 172.16.133.87 | | 288 | 12.1 MB |
| 4 | 172.16.133.113 | | 72 | 0 B |
| 4 | 172.16.133.132 | | 1272 | 1.31 MB |
| 4 | 192.168.1.138 | | 12510 | 58.59 MB |
| 2 | 172.16.133.45 | | 168 | 120 B |
| 2 | 172.16.133.93 | | 672 | 2.34 MB |
| 1 | 172.16.133.20 | | 168 | 46.31 KB |

Click **View All** to load a page that displays all the offending devices for the last 24 hours.

You can search for a specific device and filter by risk level or device IP/CIDR. You may also change how the information is sorted, as well as download the information in the form of a CSV or JSON file.

Dashboard / Devices

Offending Devices (24H)

Search...

| Risk Level | IP Address | Hostname | Volume | Count |
|------------|----------------|--------------------|-----------|-------|
| High | 172.16.133.6 | jsrvr27.jaalam.net | 0 B | 4440 |
| High | 172.16.133.41 | | 427.29 KB | 864 |
| High | 172.16.133.48 | | 38.16 KB | 360 |
| High | 172.16.133.54 | | 5.62 MB | 2256 |
| High | 172.16.133.56 | | 265.07 KB | 168 |
| High | 172.16.133.73 | | 24 B | 552 |
| High | 172.16.133.78 | | 23.3 MB | 1245 |
| High | 172.16.133.87 | | 12.1 MB | 288 |
| High | 172.16.133.113 | | 0 B | 72 |
| High | 172.16.133.132 | | 1.31 MB | 1272 |
| High | 192.168.1.138 | | 58.59 MB | 12510 |

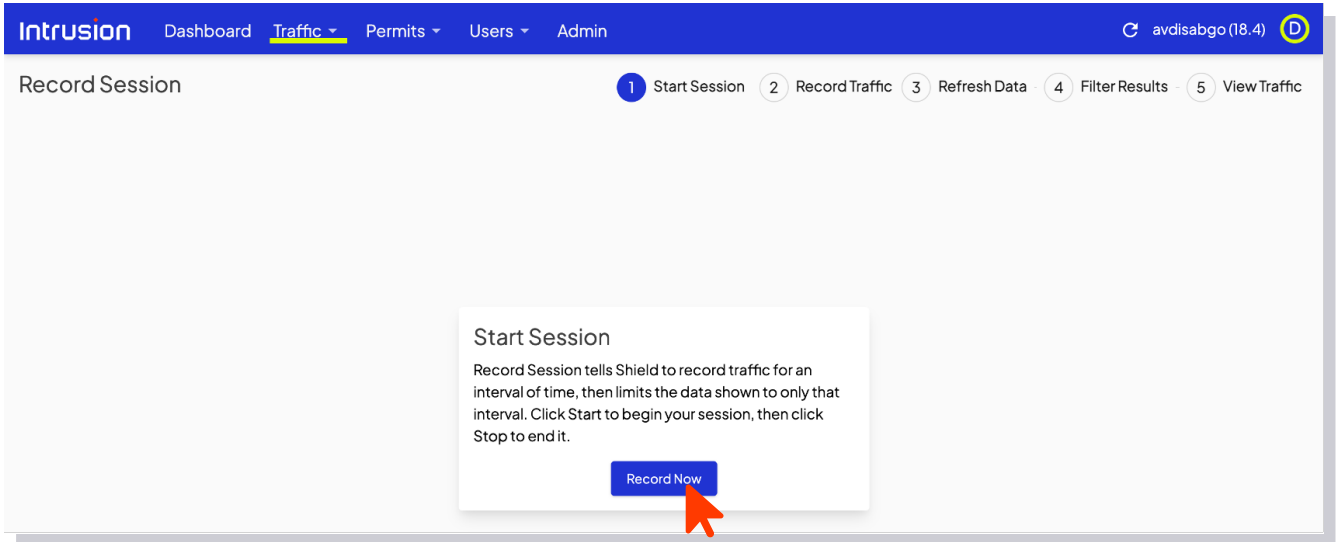


Traffic Tab

Record Session

Select **Record Now** to start a recording session.

Recorded sessions enable you to easily find connections that the Shield blocked. This is an excellent tool for troubleshooting.





Map

Select **Map** to open the interactive map page.

On the map, you can select specific countries to see attempted connections from that location to your network. The chart to the right of the map displays attempted connections, sorted by highest risk level, and gives further information. DNS, TCP, and UDP information is also displayed below the map. Click **DNS Responses**, **TCP Connections**, or **UDP Sessions** on the right side of the screen to view related information.

The screenshot shows the 'Intrusion' dashboard with the 'Traffic' tab selected. The main area is titled 'Traffic Map (Today)'. On the left is a world map with several countries highlighted in orange and red. On the right is a summary table:

| Risk | Location | Count | Killed Count | Vol. | Killed Vol. |
|------|--------------|----------|--------------|-----------|-------------|
| | Global | 12083098 | 22841 | 7.92 GB | 127.36 MB |
| 5 | Bangladesh | 39 | 39 | 39 B | 39 B |
| 5 | China | 780 | 780 | 0 B | 0 B |
| 5 | Romania | 26 | 26 | 1.46 KB | 1.46 KB |
| 4 | Brazil | 1430 | 0 | 18.71 MB | 0 B |
| 3 | Costa Rica | 39 | 0 | 0 B | 0 B |
| 3 | Finland | 13 | 0 | 78.96 KB | 0 B |
| 3 | France | 273 | 26 | 3.02 MB | 592.2 KB |
| 3 | Hong Kong | 326 | 0 | 2.68 MB | 0 B |
| 3 | Singapore | 598 | 0 | 273.53 KB | 0 B |
| 3 | South Africa | 26 | 0 | 187.97 KB | 0 B |

Below the map and table are navigation buttons: Search, Filter, Sort, Download, Add Permit. There are also tabs for 'DNS Responses', 'TCP Connections', and 'UDP Sessions'. At the bottom, a table shows a list of connection attempts with columns for Status, Risk, VLAN, Client IP, Server IP, Direction, Responses, First Seen, and Last Seen. The first few rows show 'Killed' status with a risk level of 4 and Client IP 172.16.133.6.



All Traffic

Select **All Traffic** to view DNS responses, TCP connections, or UDP sessions, based on user selection.

This tool is useful for sorting through a high volume of blocked connections to discover potential vulnerabilities. If you select a specific item, you'll be given the option to add a permit for the selected item. Before adding permits, read the section on Permits first.

| Status | Risk | VLAN | Client IP | Cli... | Server IP | Se... | Re... | Direction | Responses | First Seen | Last Seen |
|--|------|------|--------------|--------|-----------|-------|-------|-----------|-----------|---------------------|---------------------|
| <input checked="" type="checkbox"/> Killed | 4 | | 172.16.133.6 | jsr... | 8.8.8.8 | | ap... | Inbound | 14 | 2023-05-23 00:45:05 | 2023-05-23 13:45:05 |
| <input type="checkbox"/> Killed | 4 | | 172.16.133.6 | jsr... | 8.8.8.8 | | 46... | Inbound | 14 | 2023-05-23 00:45:09 | 2023-05-23 13:45:09 |
| <input type="checkbox"/> Killed | 4 | | 172.16.133.6 | jsr... | 8.8.8.8 | | 97... | Inbound | 14 | 2023-05-23 00:45:05 | 2023-05-23 13:45:05 |
| <input type="checkbox"/> Killed | 4 | | 172.16.133.6 | jsr... | 8.8.8.8 | | al... | Inbound | 28 | 2023-05-23 00:45:06 | 2023-05-23 13:45:07 |
| <input type="checkbox"/> Killed | 4 | | 172.16.133.6 | jsr... | 8.8.8.8 | | ad... | Inbound | 28 | 2023-05-23 00:45:04 | 2023-05-23 13:45:06 |
| <input type="checkbox"/> Killed | 4 | | 172.16.133.6 | jsr... | 8.8.8.8 | | ad... | Inbound | 14 | 2023-05-23 00:45:06 | 2023-05-23 13:45:06 |
| <input type="checkbox"/> Killed | 4 | | 172.16.133.6 | jsr... | 8.8.8.8 | | ad... | Inbound | 14 | 2023-05-23 00:45:08 | 2023-05-23 13:45:08 |
| <input type="checkbox"/> Killed | 4 | | 172.16.133.6 | jsr... | 8.8.8.8 | | ad... | Inbound | 14 | 2023-05-23 00:45:04 | 2023-05-23 13:45:04 |
| <input type="checkbox"/> Killed | 4 | | 172.16.133.6 | jsr... | 8.8.8.8 | | ad... | Inbound | 14 | 2023-05-23 00:45:06 | 2023-05-23 13:45:06 |

Reports

Select **Reports** to download a PDF report that captures a snapshot of kills, observed bandwidth, new domains, and new devices for a given day or month.

Daily

- [May 22, 2023](#)
- [May 21, 2023](#)
- [May 20, 2023](#)
- [May 19, 2023](#)
- [May 18, 2023](#)
- [May 17, 2023](#)
- [May 16, 2023](#)
- [May 15, 2023](#)
- [May 14, 2023](#)
- [May 13, 2023](#)
- [May 12, 2023](#)
- [May 11, 2023](#)
- [May 10, 2023](#)

Items: 25 Showing 1 to 25 of 799 entries

Monthly

- [January 2023](#)
- [December 2022](#)
- [November 2022](#)
- [October 2022](#)
- [September 2022](#)
- [August 2022](#)
- [July 2022](#)
- [June 2022](#)
- [May 2022](#)
- [April 2022](#)
- [March 2022](#)
- [February 2022](#)
- [January 2022](#)

Items: 25 Showing 1 to 16 of 16 entries



Permits

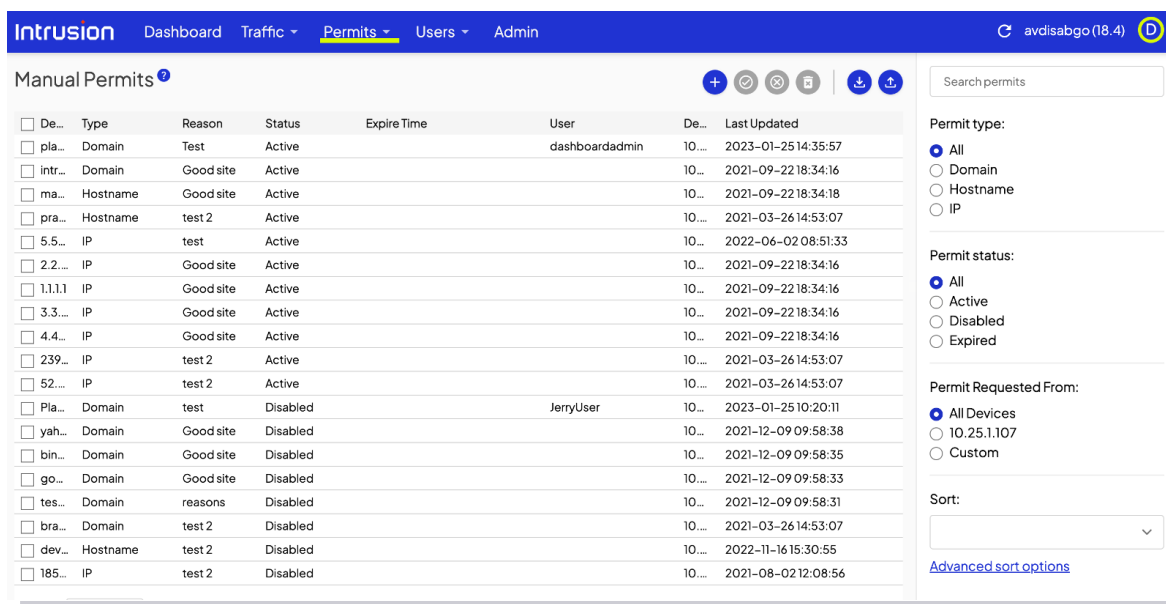
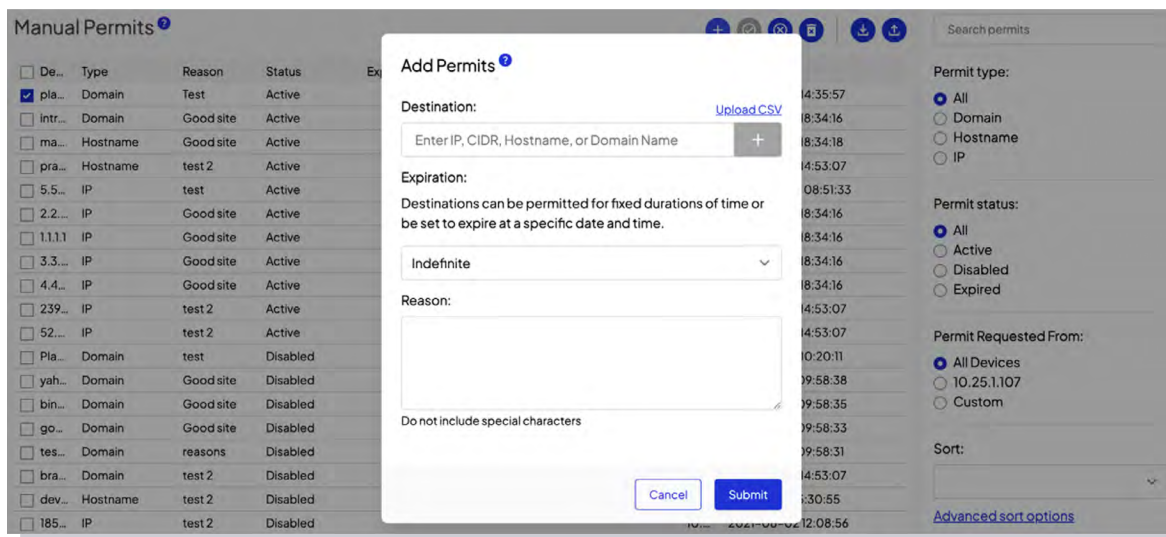
A permit essentially allows a chosen DNS, TCP, or UDP connection to pass through. Please remember to exercise caution when adding permits. Intrusion recommends only adding known, trusted connections, and not permitting more than necessary.

Manual Permits

Select **Manual Permits** to permit specific connections to override the Intrusion filter.

Specify an IP address, a domain or host or a CIDR range. Use the + button at the top of the page to add a permit.

Note: The reason field is required and special characters will not be accepted.





Auto Permits

Select **Auto Permits** to display a list of permits that were automatically added by the Shield.

If a DNS answer is observed for a domain that is on the Intrusion priority allow list or is a customer Manual Permit domain, but the resolved IP would otherwise be blocked, then an Auto Permit triggers a temporary unblock of that resolved IP for the duration of the DNS TTL. The chart shows both active and expired auto permits. You may filter the items based on permit type and status.

Intrusion Dashboard Traffic **Permits** Users Admin avdisabgo (18.4)

Auto Permits + ↓

| <input type="checkbox"/> D Type | Status | Count | First Sent | Last Sent | Expire Time |
|---------------------------------|---------|-------|---------------------|---------------------|---------------------|
| <input type="checkbox"/> 5. IP | Active | 2 | 2023-05-14 19:30:01 | 2023-05-21 19:30:01 | 2023-05-28 19:30:02 |
| <input type="checkbox"/> 3. IP | Active | 10 | 2023-05-14 19:30:01 | 2023-05-23 10:30:02 | 2023-05-24 08:40:15 |
| <input type="checkbox"/> 2. IP | Active | 2114 | 2021-12-10 16:45:02 | 2023-05-23 11:45:01 | 2023-05-23 16:56:22 |
| <input type="checkbox"/> 2. IP | Active | 12665 | 2021-12-10 11:45:01 | 2023-05-23 14:45:01 | 2023-05-23 15:38:40 |
| <input type="checkbox"/> 3. IP | Active | 212 | 2023-05-14 19:30:01 | 2023-05-23 14:30:01 | 2023-05-23 15:30:00 |
| <input type="checkbox"/> 2. IP | Active | 12653 | 2021-12-10 11:45:01 | 2023-05-23 14:45:01 | 2023-05-23 15:21:00 |
| <input type="checkbox"/> 2. IP | Expired | 12624 | 2021-12-10 11:45:01 | 2023-05-23 14:45:01 | 2023-05-23 15:10:56 |
| <input type="checkbox"/> 5. IP | Expired | 212 | 2023-05-14 20:00:06 | 2023-05-23 15:00:06 | 2023-05-23 15:01:06 |
| <input type="checkbox"/> 3. IP | Expired | 212 | 2023-05-14 20:00:06 | 2023-05-23 15:00:06 | 2023-05-23 15:01:06 |
| <input type="checkbox"/> 3. IP | Expired | 212 | 2023-05-14 20:00:06 | 2023-05-23 15:00:06 | 2023-05-23 15:01:06 |
| <input type="checkbox"/> 2. IP | Expired | 12653 | 2021-12-10 11:45:01 | 2023-05-23 14:45:01 | 2023-05-23 14:56:43 |
| <input type="checkbox"/> 7. IP | Expired | 12676 | 2021-12-10 11:45:01 | 2023-05-23 14:45:01 | 2023-05-23 14:55:02 |
| <input type="checkbox"/> 2. IP | Expired | 12639 | 2021-12-10 11:45:01 | 2023-05-23 14:45:01 | 2023-05-23 14:53:51 |
| <input type="checkbox"/> 7. IP | Expired | 12676 | 2021-12-10 11:45:01 | 2023-05-23 14:45:01 | 2023-05-23 14:53:48 |
| <input type="checkbox"/> 6. IP | Expired | 5540 | 2022-10-04 19:45:01 | 2023-05-23 14:45:01 | 2023-05-23 14:53:10 |
| <input type="checkbox"/> 6. IP | Expired | 5540 | 2022-10-04 19:45:01 | 2023-05-23 14:45:01 | 2023-05-23 14:53:10 |
| <input type="checkbox"/> 6. IP | Expired | 5540 | 2022-10-04 19:45:01 | 2023-05-23 14:45:01 | 2023-05-23 14:53:10 |
| <input type="checkbox"/> 6. IP | Expired | 5540 | 2022-10-04 19:45:01 | 2023-05-23 14:45:01 | 2023-05-23 14:53:10 |
| <input type="checkbox"/> 6. IP | Expired | 5540 | 2022-10-04 19:45:01 | 2023-05-23 14:45:01 | 2023-05-23 14:53:10 |

Permit type:
 All
 Domain
 Hostname
 IP

Permit status:
 All
 Active
 Disabled
 Expired

Sort:
 ↓
[Advanced sort options](#)



Users

Users

Select **Users** to load a page that shows a list of accounts currently enabled on the Shield. Administrators can change or add users.

Intrusion Dashboard Traffic ▾ Permits ▾ Users Admin avdisabgo (18.4)

Users

| Name | Role | Time Created |
|----------------|---------------|---------------------|
| amelia | Observer | 2022-06-30 16:29:53 |
| dashboard | User | 2020-09-28 21:27:07 |
| dashboardadmin | Administrator | 2020-12-03 12:22:19 |
| Giovina | User | 2022-12-08 09:27:09 |
| JerryObserver | Observer | 2023-01-25 10:16:25 |
| JerryUser | User | 2023-01-25 10:16:06 |
| Joelle | User | 2022-12-08 09:42:01 |
| JonathanR | Observer | 2023-01-26 12:58:31 |
| KenBevins | Administrator | 2023-01-17 10:35:18 |
| KenTest | User | 2023-02-21 17:10:52 |

Items: 50 ▾ Showing 1 to 10 of 10 entries |< < 1 > >|

Search users

User role:

- All
- Administrator
- User
- Observer

Sort:

Name ASC ▾

Logs

Select **Logs** to load a page that shows user activities, along with corresponding timestamp and IP address.

Intrusion Dashboard Traffic ▾ Permits ▾ Users Admin avdisabgo (18.4)

Logs

| Time | User | IP Address | Description |
|---------------------|----------------|----------------|--|
| 2023-05-23 16:08:45 | dashboardadmin | 10.25.1.107 | Started a new session. |
| 2023-05-23 14:34:25 | dashboardadmin | 10.25.1.107 | Started a new session. |
| 2023-05-23 12:56:23 | dashboardadmin | 10.25.1.107 | Started a new session. |
| 2023-05-23 11:57:32 | dashboardadmin | 10.25.1.107 | Started a new session. |
| 2023-05-23 10:27:39 | dashboardadmin | 10.25.1.107 | Started a new session. |
| 2023-05-18 14:44:01 | dashboardadmin | 100.69.141.130 | Started a new session. |
| 2023-05-18 14:07:02 | dashboardadmin | 100.69.141.130 | Started a new session. |
| 2023-05-15 13:39:03 | dashboardadmin | 100.69.141.130 | Started a new session. |
| 2023-05-15 12:31:08 | dashboardadmin | 100.69.141.130 | Started a refresh. |
| 2023-05-15 12:28:01 | dashboardadmin | 100.69.141.130 | Started a new session. |
| 2023-05-15 10:54:14 | dashboardadmin | 100.69.141.130 | Updated own password and/or preferences. |

Items: 50 ▾ Showing 1 to 50 of 9243 entries |< < 1 > >|

Search logs

Username:

Usernames are case sensitive

User Device:

- All Devices
- 10.25.1.107
- Custom

Sort:

Time DESC ▾

Admin

Shield Settings

The Admin page will only show if a user has admin access.

Shield Settings

Protect Mode
A Shield in Protect mode will analyze and report on all traffic and kill anything unsafe. A Shield in Observe mode will analyze and report on all traffic, but not kill anything. A Shield that is Off will not analyze nor report on any traffic, but will simply forward traffic.
[Change Shield Mode](#)

SNMP Disabled
Shield SNMP reports engine state, engine uptime, analyzed, forwarded, and rejected packets, and analyzed bytes.
Download SNMP MIBs documentation [here](#).

Syslog Disabled
Shield Syslog sends syslog messages when it kills traffic and will begin outputting syslog messages immediately upon success.

Management Interfaces Connected ●
Shield management interface configuration and Internet connectivity testing.
eno1 MAC: 2C:EA:7F:D7:4E:CE [Change Interface](#)

IP Type: DHCP DNS Type: Auto

Shield Mode

Click **Change Shield Mode** to change the operating mode of the Shield.

Protect Mode
A Shield in Protect mode will analyze and report on all traffic and kill anything unsafe. A Shield in Observe mode will analyze and report on all traffic, but not kill anything. A Shield that is Off will not analyze nor report on any traffic, but will simply forward traffic.
[Change Shield Mode](#)

- > **Protect Mode:** Records all traffic and blocks unsafe connections
- > **Observe Mode:** Records all traffic but does not block any connections
- > **Off:** The Shield analysis engine is off and all packets are forwarded without being analyzed, logged or blocked



Note: For quick network connection troubleshooting, place the Shield in Observe or Off mode.

If the connection works in Observe or Off, but not in Protect, the Shield may be blocking the connection.


Please contact customer support if you encounter any problems.

SNMP

This allows an admin to turn on the SNMP service and download the Shield SNMP MIB definitions for import into 3rd party SNMP monitoring tools.

The SNMP server reports interface statistics such as packet and bitrate counts, as well as number of kills.


SNMP Disabled 


Shield SNMP reports engine state, engine uptime, analyzed, forwarded, and rejected packets, and analyzed bytes. 

Download SNMP MIBs documentation [here](#).

Syslog

When turned on, this will give an admin the ability to configure syslog forwarding to a remote syslog server.

Syslog Disabled 

Shield Syslog sends syslog messages when it kills traffic and will begin outputting syslog messages immediately upon success. 



Management Interface

Shows the details of the Shield's management interface port. By default the management interface is assigned via DHCP.

Click **Change Interface** to manually configure the management interface.

Management Interfaces Connected ●

Shield management interface configuration and Internet connectivity testing.

eno1 MAC: 2C:EA:7F:D7:4E:CE [Change Interface](#)

| | |
|------------------------------|----------------------------|
| IP Type: DHCP | DNS Type: Auto |
| IP Address: 10.16.130.8 | Primary DNS: 10.12.14.16 |
| Subnet Mask: 255.255.0.0 | Secondary DNS: 10.16.14.16 |
| Default Gateway: 10.16.1.254 | Domain: intrusion.com |

Remote Support

This shows when remote support is active for the Shield, and gives the option to contact support.

Remote Support Online

Intrusion remote support is active. If you are experiencing any issues please [contact support](#).

Landing Page Settings

Overview

Gives a quick overview of the landing page.

Overview

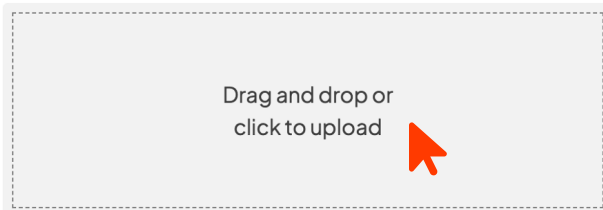
The Shield Landing Page appears to all devices behind a Shield when attempting to access a killed website. It will display the unsafe source(s) that caused the kill and allow the device to permit the source(s) if the device meets the Landing Access IPs criteria.

Landing Page Logo

You may add a logo that will show when an end user reaches the Shield blocked site page. To add a logo, drag and drop your image file into the space provided or click the space to upload your image file.

Logo

Replace the Intrusion logo on the Shield landing page with a custom image. Only JPG and PNG file types with a maximum size of 200kb accepted. File names are limited to letters, numbers, dashes and underscores.



JPG/PNG, max file size 200KB

Landing Access IPs

Here, you can specify which devices can add manual permits.

If no addresses are entered into this section, any user that reaches the Shield's blocked site page will be able to enter manual permits.

By entering an IP address or range in the dialogue box, you can limit the ability to add manual permits to devices with the specified IP addresses.

Users who attempt to add manual permits from devices with unauthorized IP addresses will be prompted to reach out to their network administrator.



IPs added here will allow machines bearing those IPs to manually add permits from the popup.

This policy does not affect the admin's ability to add permits from the dashboard. It is highly recommended that admins restrict the ability to add manual permits.

Landing Access IPs

Devices specified will be able to permit directly from the Shield Landing Page. If no devices are specified, any device which reaches the Shield Landing Page can permit directly from it.

IP/CIDR:

Devices:

Shield Info

Gives all information about the Shield.

Shield ID: avdisabgo

Shield Version: 18.4

Shield Build: 11

Description: Dell Inc. Not Specified

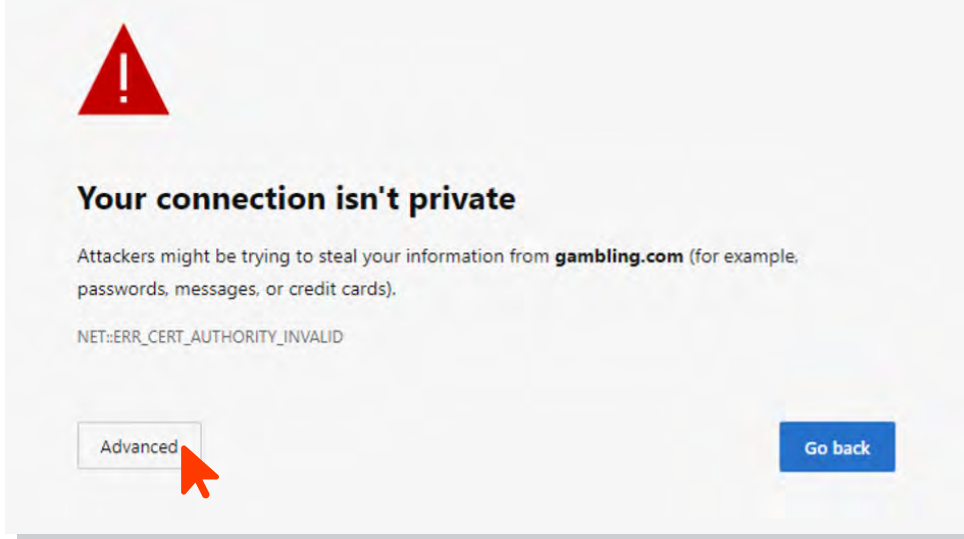
Issued to: *Bruce/Max

License Expiration: 9999/99/99

Serial Number: 3116R53

Using Shield OnPremise

Users who attempt to navigate to a site that the Shield blocks will see the page below.

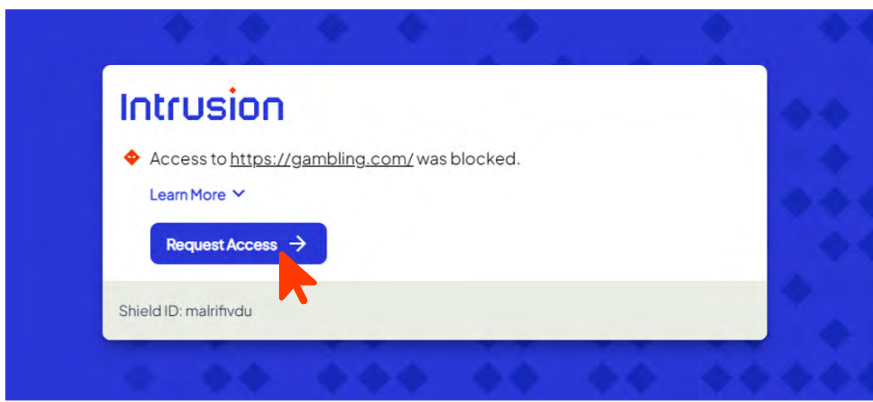


As was in the case when loading the dashboard, users will see an error caused by the Shield having a self-signed certificate.

| For them to proceed, have your users click **Advanced**.

Your users will then be forwarded to the Shield blocked site landing page.

| In order to proceed, they should click the **Request Access** button.





That user action will prompt the Shield to present you, the admin, a dialogue that looks very similar to the manual permit page in the dashboard.

Intrusion

Blocked Destination:

gambling.com Site only
Site and subdomains

Duration:

24 hours

15 minutes

60 seconds

Custom

Reason:

Reason for permit required

Submit ✓ Cancel ✕

Shield ID: malrifvdu

Check the connections to permit a specific site only or the site and all its subdomains.

However, if an admin has restricted the ability to add permits, the end user will be asked to contact the network administrator.

Intrusion

◆ Access to <https://gambling.com/> was blocked.

Please contact your network administrator to request access to this website.

Shield ID: malrifvdu Time: 3/16/2023 3:11:55 PM

User IP: 192.168.0.133

Please reach out to our customer support team with questions and feature suggestions.

Support@intrusion.com

1-888-637-7770 / Option 3