INTRUSION™

Protect everything. Trust nothing.

INTRUSION *Shield*
Dashboard User Guide

FAQ

‘What am I looking at?’

By default, the dashboard displays all connections seen by ***Shield***, whether blocked or unblocked, for all IP Addresses within your network.

‘What has *Shield* blocked?’

To view blocked connections only, click the ‘Filter’ button just above the table and change the ‘Status’ from ‘All’ to ‘Blocked’ (See ‘Filtering’ section for more details).

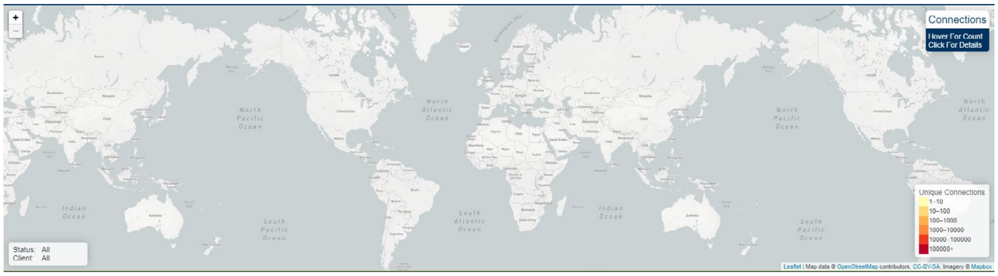
‘How do I see connections from just my device?’

To just show connections from your local IP address (seen in the upper-right corner of the dashboard), click the ‘Filter’ button just above the table and change the ‘Client’ from ‘All’ to Local’ (See ‘Filtering’ section for more details).

‘I can’t reach a website. how do I see if *Shield* is blocking it?’

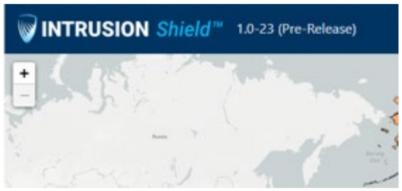
‘Go Live’ is an easy way to see what connections ***Shield*** is actively blocking from your device (See ‘Go Live’ section for more details).

Map

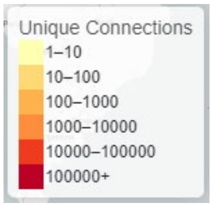


Status: All
Client: All

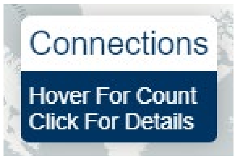
The map in the center of the screen is a quick way to discover which countries you connect to the most.



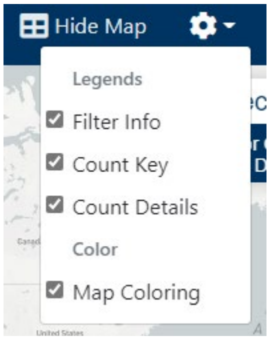
You can zoom in and out to see the details of the map either by scrolling or by using the plus and minus buttons in the upper-left hand corner of the map.



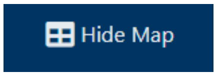
The countries on the map are colored according to the number of unique connections made with each country. The key in the bottom-right hand corner of the map displays the color code for the map. The darkest countries are the places you connect to the most, while the lighter countries are the countries you connect to less often. Uncolored countries mean you haven't connected there at all.



If you hover your mouse over a colorful country, the box in the upper-right hand corner will show you the number of unique connections to that country. If the connection count is greater than zero, you can click on the country to filter the table results to only show connections to the selected country. To undo this filter and show connections to every country again, simply click that country again or click on an ocean.

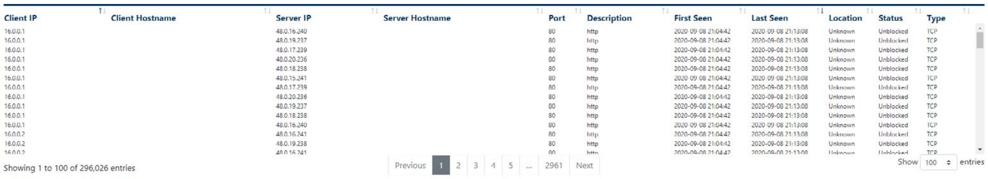


The Color Key, Connection Count, and Standard Filter Status (See 'Filtering' section for more details) legends can be removed by accessing the 'Gear' icon located in the upper-right hand corner of the screen. By default, all three legends are active, but you can easily remove one by unchecking the box. Map coloring can also be deactivated by unchecking the box next to 'Map Coloring'.



To hide the map completely and view the table only, click the 'Hide Map' button located in the upper-right hand corner of the screen. This can be undone by clicking the 'Show Map' button.

Table Details



Client IP	Client Hostname	Server IP	Server Hostname	Port	Description	First Seen	Last Seen	Location	Status	Type
16.0.0.1		48.0.16.240		80	http	2020-09-08 21:04:42	2020-09-08 21:13:08	Unknown	Unblocked	TCP
16.0.0.1		48.0.19.237		80	http	2020-09-08 21:04:42	2020-09-08 21:13:08	Unknown	Unblocked	TCP
16.0.0.1		48.0.17.239		80	http	2020-09-08 21:04:42	2020-09-08 21:13:08	Unknown	Unblocked	TCP
16.0.0.1		48.0.20.236		80	http	2020-09-08 21:04:42	2020-09-08 21:13:08	Unknown	Unblocked	TCP
16.0.0.1		48.0.18.238		80	http	2020-09-08 21:04:42	2020-09-08 21:13:08	Unknown	Unblocked	TCP
16.0.0.1		48.0.15.241		80	http	2020-09-08 21:04:42	2020-09-08 21:13:08	Unknown	Unblocked	TCP
16.0.0.1		48.0.17.239		80	http	2020-09-08 21:04:42	2020-09-08 21:13:08	Unknown	Unblocked	TCP
16.0.0.1		48.0.20.236		80	http	2020-09-08 21:04:42	2020-09-08 21:13:08	Unknown	Unblocked	TCP
16.0.0.1		48.0.19.237		80	http	2020-09-08 21:04:42	2020-09-08 21:13:08	Unknown	Unblocked	TCP
16.0.0.1		48.0.18.238		80	http	2020-09-08 21:04:42	2020-09-08 21:13:08	Unknown	Unblocked	TCP
16.0.0.1		48.0.16.240		80	http	2020-09-08 21:04:42	2020-09-08 21:13:08	Unknown	Unblocked	TCP
16.0.0.2		48.0.16.241		80	http	2020-09-08 21:04:42	2020-09-08 21:13:08	Unknown	Unblocked	TCP
16.0.0.2		48.0.19.238		80	http	2020-09-08 21:04:42	2020-09-08 21:13:08	Unknown	Unblocked	TCP
16.0.0.2		48.0.16.241		80	http	2020-09-08 21:04:42	2020-09-08 21:13:08	Unknown	Unblocked	TCP

Showing 1 to 100 of 296,026 entries

Each row of the table represents a single connection passing through your ***Shield***. The column descriptions are as follows:

- **Client IP:** The internal IP Address that initiated the connection.
- **Client Hostname:** The hostname of the internal IP Address that initiated the connection.
- **Server IP:** The internal or external IP Address that was connected to.
- **Server Hostname:** The hostname of the internal or external IP Address that was connected to.
- **Port:** The transport protocol used for the connection.
- **Description:** The assignment for the transport protocol used for the connection.
- **First Seen:** Timestamp for when the connection was initiated.
- **Last Seen:** Timestamp for when the connection was terminated.
- **Location:** Geographic estimate for the Server IP's location, will be 'Local' if internal or possibly 'Unknown'.
- **Status:** Indicates whether connection was 'Blocked' or 'Unblocked'.
- **Type:** Indicates connection type, either 'TCP', 'UDP', or 'DNS'.

To get more information about a specific connection, simply click on a row. This will reveal more details depending on the connection type, such as:

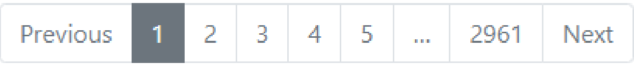
- **TCP Connection Count:** The number of 'syn' flags seen on the Client IP's side.
- **TCP/UDP Client Stream Bytes:** Total bytes streamed by the Client IP to the Server IP during the connection
- **TCP/UDP Server Stream Bytes:** Total bytes streamed by the Server IP to the Client IP during the connection
- **DNS Domain:** The domain of the hostname accessed
- **Location:** If known, will show the Country, Region, City, Latitude and Longitude of the Server IP. If the IP is internal, the Location will be 'Local'. If Latitude and Longitude values are available, you can click on the blue location icon, located to the right of these values, and ***Shield*** will display and zoom into the estimated location on the map.

- **Blocked:** If connection is blocked, there will be an option to 'Unblock' either the IP, Hostname, Domain or All available directly in the row. To quickly unblock one of these, simply click one of these and the 'Unblock' will be brought up. (See 'Unblock' section for more details).

To hide row details for a specific row, click the specified row again.

To hide row details for all rows in the table, click the 'Hide Details' button at the top of the table (See 'Table Actions' section for more details).

By default, only 100 rows are visible at a time. To change this, simply select the box located in the bottom-right-hand corner of the table that indicates 'Show 100 Entries'. You can choose to display up to 1,000 rows at once.



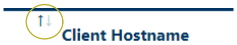
You will likely have large amounts of data in your table. To navigate through these pages of connection data, use the page numbers as well as the 'Previous' and 'Next' buttons located at the bottom of the table.

For more information about the data being shown, check the bottom-left corner of the table.

Sorting

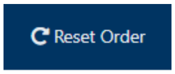
By default, the table is sorted by Last Seen in a descending order, then by Client IP in an ascending order.

However, you can easily sort your data by any column by selecting the arrows located to the right of any column title.



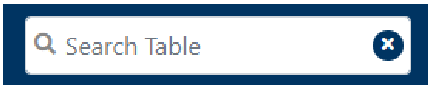
The upward arrow will sort the values in an ascending order. The downward arrow will sort the values in a descending order.

To sort by multiple columns, simply hold down the shift button while you select the columns you wish to sort by.



To revert the table back to default sorting,
simply hit the 'Reset Order' button at the top of the table.

Search

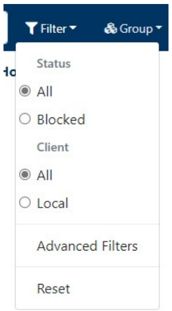


You can search for anything by simply typing a phrase or term into the ‘Search Table’ box in the upper-left-hand corner of the table and hit Enter on your keyboard.

To clear your search results, click the ‘X’ button located to the right of the search bar.

By default, the search bar will return results from all columns (See ‘Advanced Filtering’ section for more advanced searching options).

Filtering



In order to better understand your data, ***Shield*** Dashboard offers many comprehensive filtering options.

The most commonly used filtering options, known as Standard Filters, are available by clicking the ‘Filter’ button, located just above the table.

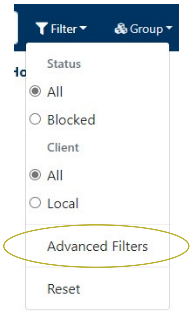
By default, the dashboard displays all connections, whether blocked or unblocked. To just show blocked connections, choose the ‘Blocked’ option under ‘Status’ in the ‘Filter’ dropdown menu.

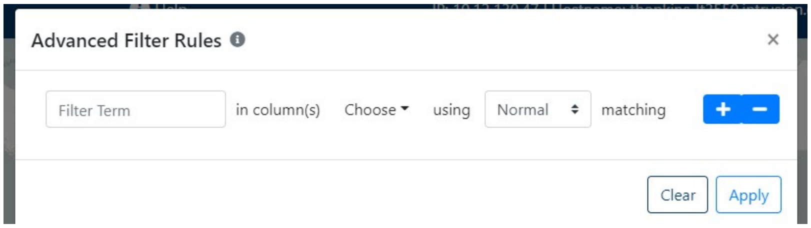
Also, by default, the dashboard displays all connections within your network. To just show connections from your local IP address, choose the ‘Local’ option under ‘Client’ in the ‘Filter’ dropdown menu.

Your currently selected Standard Filters can be seen in the bottom-left hand corner of the map.

Advanced Filtering

The Advanced Filter menu is located in the ‘Filter’ dropdown menu.





Up to five advanced filtering options can be applied at once. To add a new rule, simply click the ‘plus’ button on the right. To remove a rule, click the ‘minus’ button.

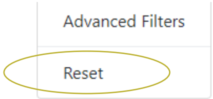
To create a customized rule, enter the phrase or term you wish to filter for. Then, select which columns to search for this term in. Next, choose which type matching you wish to apply:

- **Normal:** Matching based on if the specified column(s) value contains the filter term.

- **Exact:** Matching based on if the specified column(s) value matches exactly to the filter term.
- **Regex:** Matching based on if the specified column(s) value matches the regex in the filter term.
- **CIDR:** Matching based on if the specified column(s) IP fits inside the CIDR range in the filter term (Can only be used on IP columns).

To apply your new rule(s), select 'Apply' in the bottom-right corner of the menu. To clear your current rules, select 'Clear'.

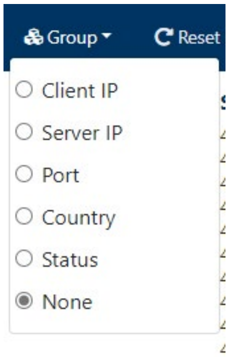
Standard and Advanced filtering will reset the map according to the data available in the table.



To reset all sorting, grouping, filtering, and search bar results, simply click the 'Reset' button at the bottom of the 'Filter' dropdown menu.

Group

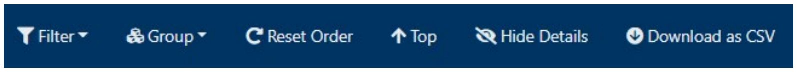
You can group table rows according to certain column values by clicking the 'Group' button located at the top of the table.



A dropdown menu will give you the option to sort by Client IP, Server IP, Port, Country, or Status. Selecting one of these options will reorder the table and group connections together by equivalent column values. When grouping by a column, the table will be resorted by that specified column, followed by the default sorting.

To reset the grouping, select the 'None' option in the dropdown menu.

Table Actions



From left to right, the table actions are as follows:

- **Reset Order:** This button resets the table sorting to default (See 'Sorting' section for more details).
- **Top:** This button scrolls the table back up to the top of the first row of the first page of the table.
- **Hide Details:** This button hides all currently open row details (See 'Table Details' sections for more details). This button is not available in 'Live' view.
- **Download as CSV:** This button generates CSV file containing all data in the currently filtered table as well as all available enrichment data from row details. This file is automatically downloaded and titled 'dashboard.csv'.

Unblock

If you find that ***Shield*** is blocking a website you need to access, you can easily unblock it in seconds.

Blocked connections will be bolded and red. You can either filter for blocked connections by selecting 'Blocked' under the 'Filter' menu or by searching for the blocked hostname in the search bar.

To easily find the connections that ***Shield*** is actively blocking, you can start a 'Live Session' by clicking the 'Go Live' button at the top of your screen. This will only record traffic to and from your device for the duration of the live session (See the 'Go Live' section for more details).

There are three ways to unblock connections:

1) **Row-Based Unblocking**
When you click on a blocked connection, the row will expand and give you the option to unblock either the 'Domain', 'Hostname' or 'IP'. Clicking one of these options will open up the 'Unblock Connections' menu. By default, connections will be unblocked indefinitely. However, you have the option to unblock for 15 minutes, 24 hours, or some custom time period. Finally, review your decision before hitting the 'Unblock' in the bottom-right corner of the menu.

2) **Select-Based Unblocking**
To select several rows to unblock, toggle the 'Row Unblock Selecting' button located in the upper-right hand corner of the table. Next, you can either select the rows you wish to unblock or click the icon with three horizontal lines to automatically select all blocked connections currently in the table. To unselect all rows, hit the 'x' button. Once you have selected all the connections you wish to unblock, click the icon of the unlocked lock and the 'Unblock Connections' menu will open. Here you can confirm which IP addresses, hostnames, and domain names you wish to unblock, specify a time period, and give a reason before hitting 'Unblock' button.

3) **Manual Unblocking**
   To manually unblock specific places, hit the ‘Unblock’ button located in the upper-right hand corner of the table. Here you can type the IP addresses, hostnames, or domain names you wish to unblock. You can list multiple entries separated by commas. Finally, specify a time period and give a reason before hitting ‘Unblock’.

Should I unblock the domain, hostname, or IP? (What’s the difference between a domain and a hostname?)

Domain names are places like intrusion.com, microsoft.com, and google.com, which are known as ‘one dot’ Top Level Domains because the domain name is left of the last dot. However there also many ‘two dot’ Top Level Domains such as microsoft.co.uk and redcross.org.au where the domain name is left of the second to last dot.

Hostnames are individual services and devices that are part of the registered domain such as mail.microsoft.com or ns1.microsoft.com.

Let’s pretend that the domain name, microsoft.com, is blocked on ***Shield***. If you decided you wanted to visit downloads.microsoft.com but still be blocked from receiving emails from them, then you should only unblock the hostname downloads.microsoft.com and not the whole domain. If you were to unblock the domain name, you are essentially unblocking every hostname that ends with ‘.microsoft.com’. This becomes very important when considering free hosting providers where not every hostname on the domain is safe.

Sometimes the domain name you need access will appear unblocked by ***Shield***, but you still cannot reach it. Copy the IP address from the DNS connection and search for it in the table. From there you will probably find that the IP address is being blocked on a different protocol. From here, simply click the connection and select unblock IP.

When you choose to unblock something, it will get unblocked immediately. So, if you still cannot reach the site, there may be a different block you missed.

We will review every unblock you make and consider unblocking it for everyone. If you unblock anything by mistake, contact us and we can fix it for you.

Go Live

Going live is the best way to see what connections ***Shield*** is actively blocking, which can be very helpful for debugging and unblocking.

Steps:

1) **Start a Live Session:**
   To start a live session, select the light blue 'Go Live' button at the top of your screen. When the 'Go Live' menu appears, click 'Start Live Session'. A timer will begin counting up for the duration of the session. There is a limit of 10 minutes to a live session.
2) **Stop a Live Session:**
   To stop a live session, hit the 'Stop Live Session' button located just below the timer.
3) **Show Live Session Data:**
   By default, only connections that were blocked and from your local IP Address will be shown, but this can be changed by adjusting the filter options before hitting the 'Show Live Session' button. The dashboard will now be in 'Live Mode' and only connections collected during the live session will be visible.

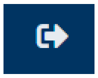
The dashboard is in 'Live Mode' if the heartbeat icon at the top your screen is red. During this mode, clicking on a row will automatically select it to be unblocked (See 'Select-Based Unblocking' for more details). Several features of the dashboard are unavailable during this mode such as filtering, grouping, refreshing, hiding all row details, and toggling between showing row details and selecting a row to unblock.

To exit 'Live Mode', hit this icon again and the page will refresh.

Refresh

To view the most recent connection data from ***Shield***, hit the 'Refresh' button at the top of your screen.

Sign Out



To exit the Dashboard, hit the 'Sign Out' button in the upper-right hand corner of the screen.