SHIELD ONPREMISE TIER 1 SUPPORT

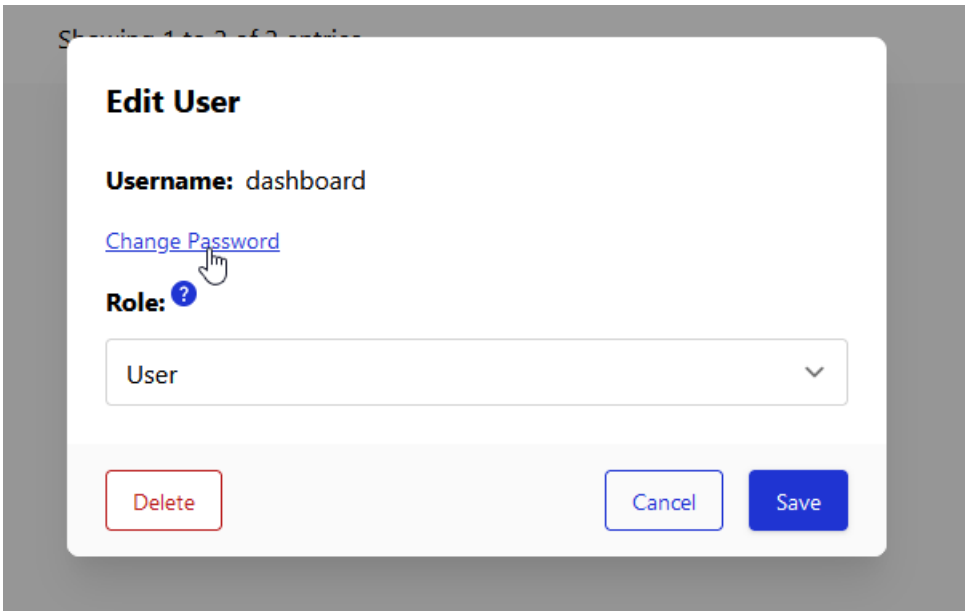
support@intrusion.com

help.intrusion.com

Table of Contents

Reset an Account Password

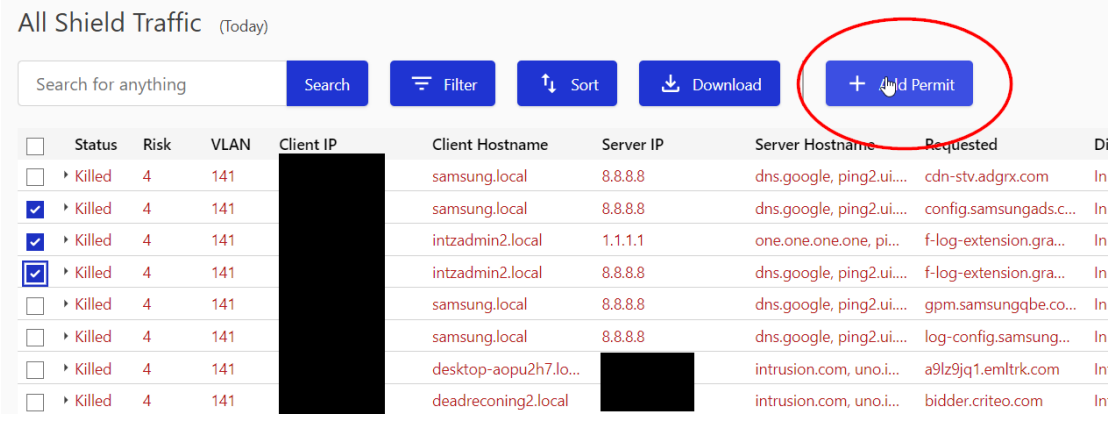
To reset an account password, log into an administrator account and navigate to the Users page. Select the user you would like to change the password for. You will need to meet the password security requirements. You may use the auto generation button. The next time somebody logs into this user account they will be asked to change the password.



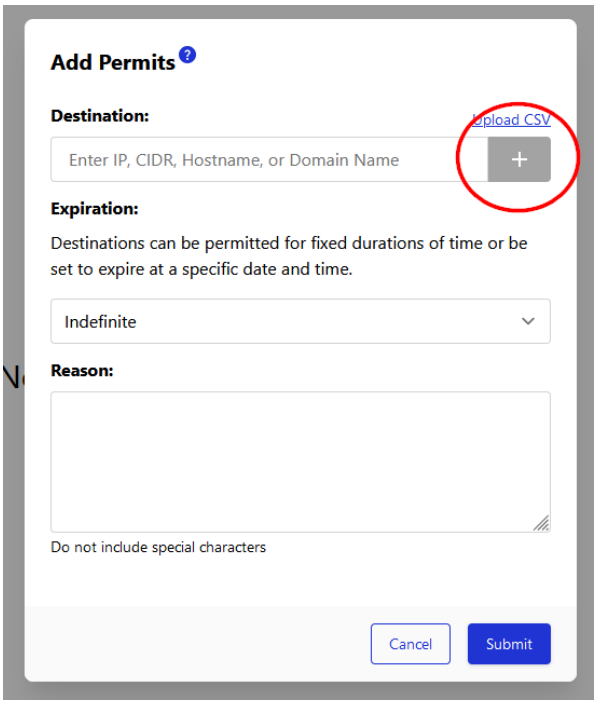
Permit a Domain/Hostname/IP/CIDR

There are many ways to permit a connection.

When viewing traffic on the dashboard, select the check box to the left of the blocked connection and click the "+ Add Permit" button. This will bring up a dialog box for permits.



To manually permit a connection by typing in the address, you may navigate to the permits > manual permits page. Click on add permit and the permit dialog box will appear. Be sure to click the + to the right of the connection text box to add it to the permit. You may enter hostnames, domains, IP addresses and CIDR ranges (192.168.1.1/24). This page will also allow you to manage your permits. Additionally, you may upload a CSV you downloaded from a Shield from the manual permits page to copy all the permits quickly.



Lastly, any user navigating to a blocked site will receive a connection redirect to the Shield's landing page where they will be able to permit the connection by selecting the domain/IP address they would like to permit. On the admin page of the dashboard, there is a section called Landing Access IPs. If any IP assignment is present in this setting, then only devices designated will be able to make permits, and other users will only see that the connection is blocked.

Proper Port Configuration

Shield is designed to work with 3 ethernet ports connected.

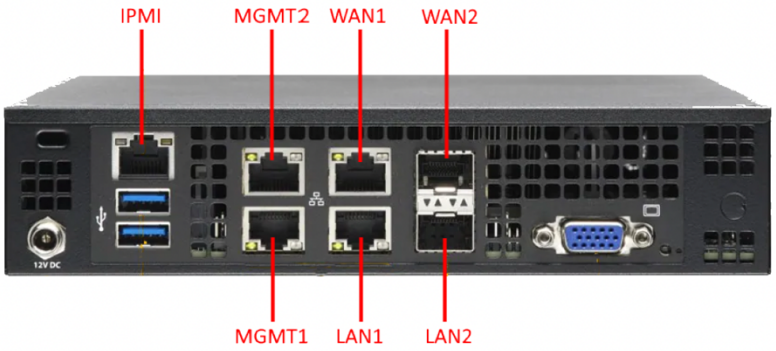
WAN should be connected to your gateway/firewall

LAN and MGMT should be connected to your internal switch.

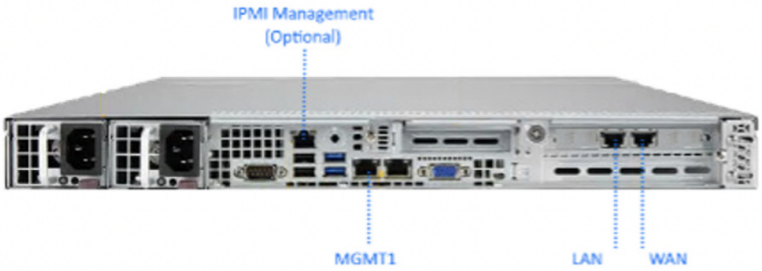
It is generally good practice that when installing a Shield for the first time to only connect the MGMT port to the switch and change the operating mode to Observe in the admin page before connecting the other ports.

Note, any connection from the internal switch to the gateway/firewall that is not Shield will cause a loop.

For S8



For S16



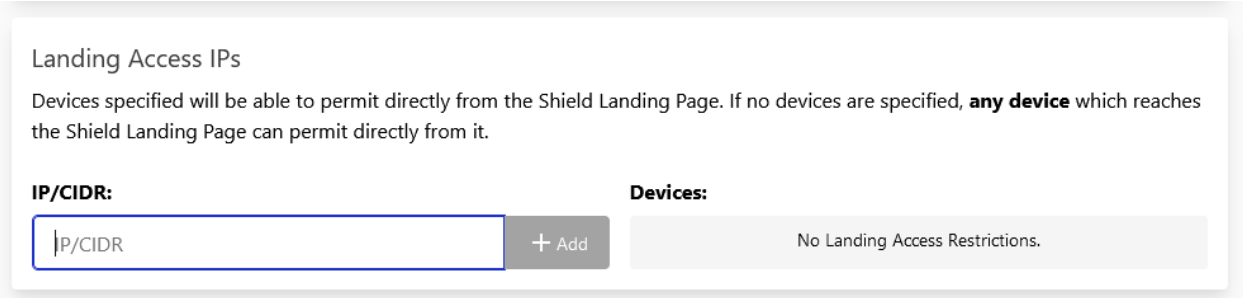
Ports that need to be open outbound

In most cases you should not need to change any configuration on a customer's firewall. However, if you run into issues with connecting the Shield to Intrusion servers to receive updates, you may need to create outbound port rules: UDP 54.188.121.229:2021 (Shield Remote) and TCP 198.58.73.19:443 (SUT).

DNS over HTTPS

Shield is designed to work with traditional DNS resolution. Browser configured DNS over HTTPS will not allow the Shield to function properly.
To disable this feature, look up how to do so on each browser.

Landing Access IPs

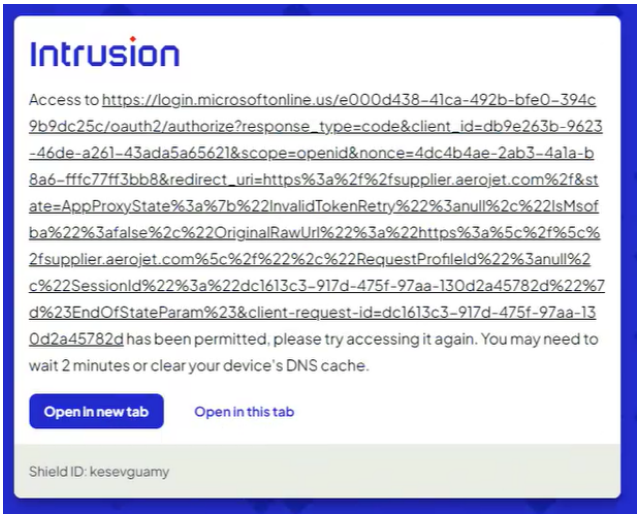


This option allows you to control what devices are allowed to make permits from the landing page. If there are any designations, then any device not on this list will only be shown that their connection is blocked without the option to permit it. If there are no designations, anybody who reaches the landing page will be able to select and permit any connection, save for a few that are explicitly disallowed by Intrusion Rules.

To keep your end users from permitting any site at whim, be sure to enter an authorized device's IP address (or range) to keep permit authorization limited to administrative staff.

CNAME resolution

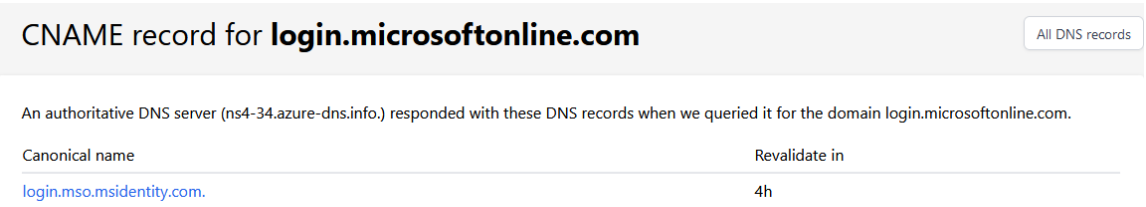
Occasionally you may see a user reach the landing page and it shows “access to <website> has been permitted”



In this case, the most common solution is to look for a CNAME and permit any that are not permitted and showing as blocked on the dashboard.

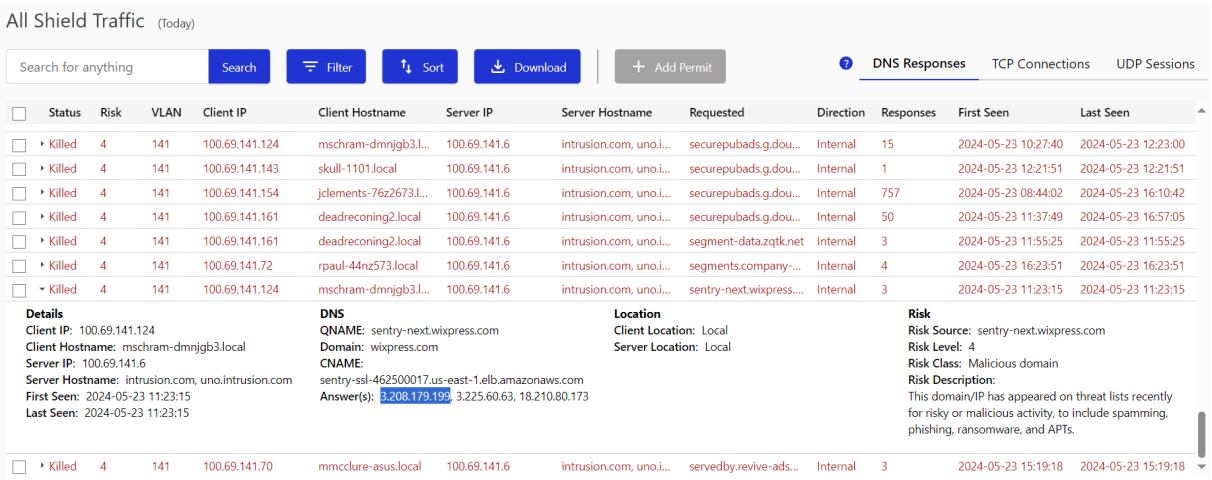
A useful website you can use is https://www.nslookup.io/cname-lookup/

Here you can find resources required for page loads that are preventing the Shield from connecting to the site properly.



Troubleshooting Sites Not Loading Correctly

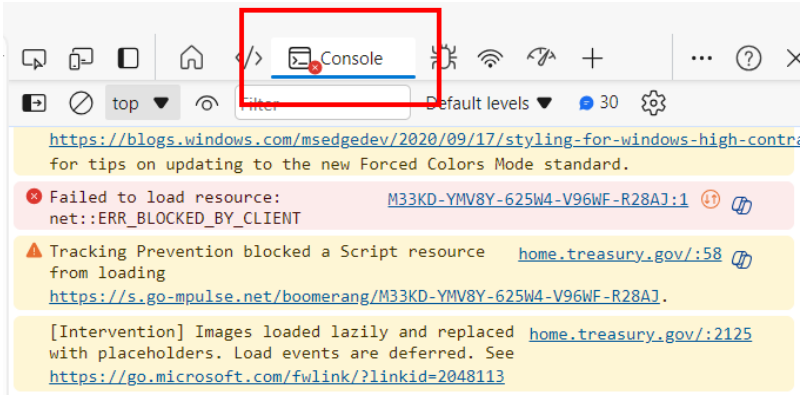
Sometimes when navigating to a site the page will give you a "page not found" error. It is possible that the Shield is allowing the main site but not allowing one of the site's resources from a different hostname. There are a few ways to go about finding these hidden hostnames.

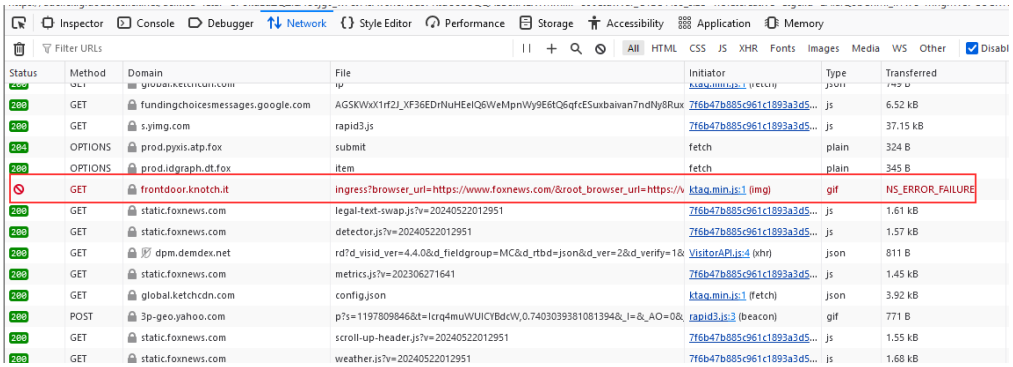


First, log into the dashboard and find the connection in question. Look for the IP and CNAME information in the middle-left column. Copy these and search the dashboard for them one by one. You may find associated hostnames and IP addresses. Alternatively, you can search a CNAME resolution site like the one mentioned earlier to see required hostnames and servers.

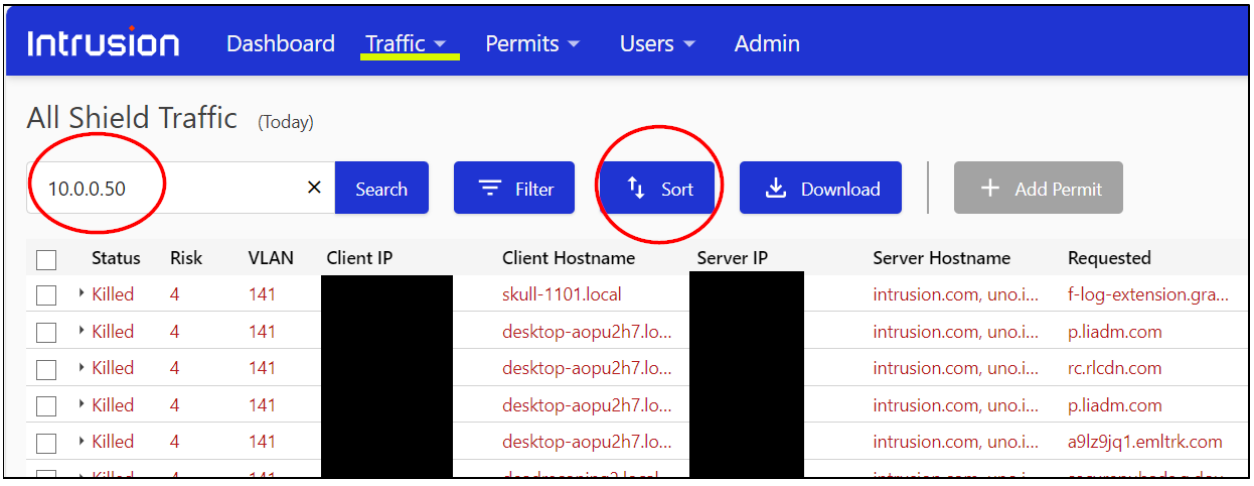
If this still does not work, you may attempt to navigate to the site with your browser's developer tools open. Look for resources that show as unable to load and see if you find those in the dashboard as blocks.

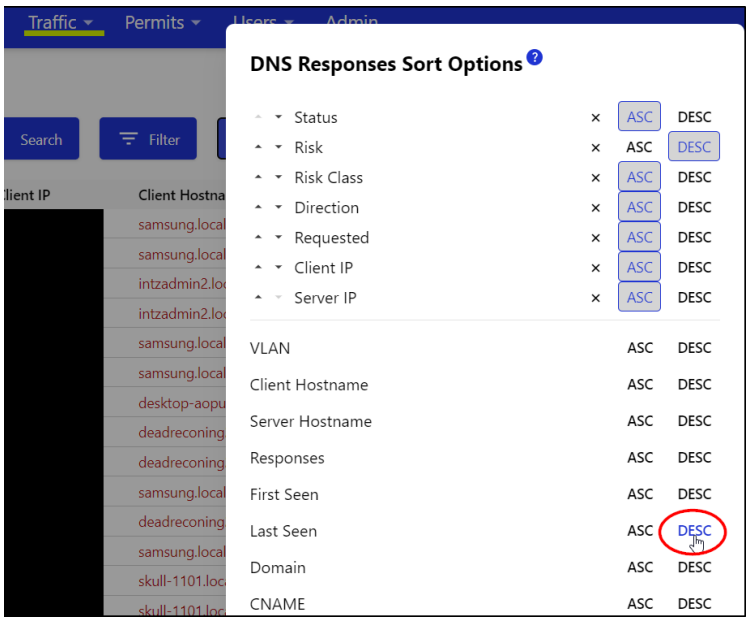
Depending on which browser you use, you may need to look at either the console or the network tab of the dev console to see unloaded connections.

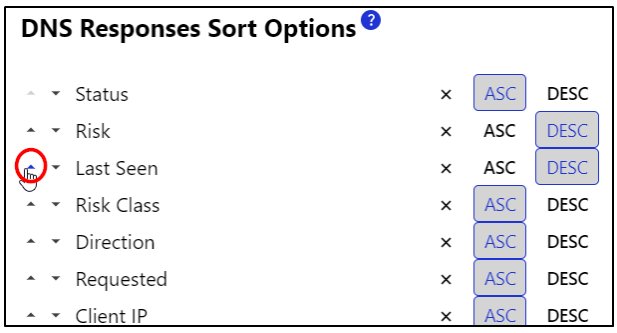




You can also do a search on the traffic or map page for the specific IP address of the device that is being blocked. Then, sort by last seen descending. You will need to raise the sort order to the top to make last seen appear first. Look for blocks that happened at the same time your website was requested.







Permitting Domains vs Subdomains

When making a new permit rule it is important to keep in mind how Shield treats domains and subdomains.
If you were to permit “support.google.com” then ONLY the support subdomain and below will be permitted. In this case, “mail.google.com” will not be included in that permit. Similarly, if you many subdomains, only the lower-level subdomains will be permitted.

However, if you permit the top-level domain such as “google.com” then ALL lower level subdomains under that top level domain will also be permitted. This also works if you permit the second level subdomain to permit all third, fourth, fifth etc. level subdomains. The lower your subdomain listed on the permit the more specific your permit becomes (and the more secure).

Resetting the Engine State

If your Shield is acting oddly, you may cycle the engine states to restart the Shield services. This can be useful if traffic stops passing properly or if you’re seeing blocks that should not happen. Note that this isn’t guaranteed to fix your issue but might help in getting Shield running again if it

is not operating properly. Please always contact intrusion support if doing this fixes an issue and provide as many details as possible.

On the Admin page, click to change the engine mode and set it to ‘off.’ This turns off the Shield logic and allows all traffic to pass through. This will cause downtime. When it is switched to ‘off’, you may turn the engine back to ‘protect’ or ‘observe.’ Note that while the engine is off, you will not be able to see the landing page or access the dashboard via dashboard.intrusion.com. You will need to navigate to it using the MGMT port’s IP address.