Intrusion

SHIELD ONPREMISE TIER 1 SUPPORT

help.intrusion.com

Table of Contents

RESET AN ACCOUNT PASSWORD	3
PERMIT A DOMAIN/HOSTNAME/IP/CIDR	3
PROPER PORT CONFIGURATION	4
PORTS THAT NEED TO BE OPEN OUTBOUND	5
DNS OVER HTTPS	5
LANDING ACCESS IPS	6
CNAME RESOLUTION	6
TROUBLESHOOTING SITES NOT LOADING CORRECTLY	7
PERMITTING DOMAINS VS SUBDOMAINS	9
RESETTING THE ENGINE STATE	9

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.

Edit User	
Username: dashboard	
Change Password	
User	~
Delete	Cancel

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.

All	Shield	Traff	ic (Today)						
Se	arch for a	nything	9	Search	〒 Filter ↑↓ S	Sort 🛃	Download + Amd I	Permit	
	Status	Risk	VLAN	Client IP	Client Hostname	Server IP	Server Hostname	Requested	Di
	Killed	4	141		samsung.local	8.8.8.8	dns.google, ping2.ui	cdn-stv.adgrx.com	In
~	 Killed 	4	141		samsung.local	8.8.8.8	dns.google, ping2.ui	config.samsungads.c	In
~	 Killed 	4	141		intzadmin2.local	1.1.1.1	one.one.one.one, pi	f-log-extension.gra	In
~	Killed	4	141		intzadmin2.local	8.8.8.8	dns.google, ping2.ui	f-log-extension.gra	In
	 Killed 	4	141		samsung.local	8.8.8.8	dns.google, ping2.ui	gpm.samsungqbe.co	In
	 Killed 	4	141		samsung.local	8.8.8.8	dns.google, ping2.ui	log-config.samsung	In
	Killed	4	141		desktop-aopu2h7.lo.		intrusion.com, uno.i	a9lz9jq1.emltrk.com	In
	Killed	4	141		deadreconing2.local		intrusion.com, uno.i	bidder.criteo.com	In

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.

Enter IP, CIDR, Hostname, or Domain Name Expiration: Destinations can be permitted for fixed durations of time or be set to expire at a specific date and time. Indefinite Reason: Do not include special characters	Destination:	pload o
Expiration: Destinations can be permitted for fixed durations of time or be set to expire at a specific date and time. Indefinite Reason: Do not include special characters	Enter IP, CIDR, Hostname	e, or Domain Name +
Destinations can be permitted for fixed durations of time or be set to expire at a specific date and time. Indefinite Reason: Do not include special characters	Expiration:	\sim
Indefinite ~ Reason: Do not include special characters	Destinations can be permit set to expire at a specific da	ted for fixed durations of time or be ate and time.
Reason: Do not include special characters	Indefinite	```
Do not include special characters	Reason:	
Do not include special characters		
Do not include special characters		
Do not include special characters		
	Do not include special character	rs

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





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

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:	ſ	Devices:								
P/CIDR	+ Add	No Landing Access Restrictions.								

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"

Intrusion

Access to https://login.microsoftonline.us/e000d438-41ca-492b-bfe0-394c 9b9dc25c/oauth2/authorize?response_type=code&client_id=db9e263b-9623 -46de-a261-43ada5a65621&scope=openid&nonce=4dc4b4ae-2ab3-4a1a-b 8a6-fffc77ff3bb8&redirect_uri=https%3a%2f%2fsupplier.aerojet.com%2f&st ate=AppProxyState%3a%7b%22InvalidTokenRetry%22%3anull%2c%22IsMsof ba%22%3afalse%2c%22OriginalRawUrl%22%3a%22https%3a%5c%2f%5c% 2fsupplier.aerojet.com%5c%2f%22%2c%22RequestProfileId%22%3anull%2 c%22SessionId%22%3a%22dc1613c3-917d-475f-97aa-130d2a45782d%22%7 d%23EndOfStateParam%23&client-request-id=dc1613c3-917d-475f-97aa-13 Od2a45782d has been permitted, please try accessing it again. You may need to wait 2 minutes or clear your device's DNS cache.



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 <u>https://www.nslookup.io/cname-lookup/</u>

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

CNAME record for login.microsoftonline.com											
An authoritative DNS server (ns4-34.azure-dns.info.) responded with these DNS records when we queried it for the domain login.microsoftonline.com.											
login.mso.msidentity.com.	4h										

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.

Search fo	or anything		Search	च Filter ी↓ Sor	t 🛃 Down	nload + Add	?	DNS Respon	ons UDP Sessior		
Stat	us Risk	VLAN	Client IP	Client Hostname	Server IP	Server Hostname	Requested	Direction	Responses	First Seen	Last Seen
→ Kille	d 4	141	100.69.141.124	mschram-dmnjgb3.l	100.69.141.6	intrusion.com, uno.i	securepubads.g.dou	Internal	15	2024-05-23 10:27:40	2024-05-23 12:23:00
→ Kille	d 4	141	100.69.141.143	skull-1101.local	100.69.141.6	intrusion.com, uno.i	securepubads.g.dou	Internal	1	2024-05-23 12:21:51	2024-05-23 12:21:51
In Kille	d 4	141	100.69.141.154	jclements-76z2673.l	100.69.141.6	intrusion.com, uno.i	securepubads.g.dou	Internal	757	2024-05-23 08:44:02	2024-05-23 16:10:42
→ Kille	d 4	141	100.69.141.161	deadreconing2.local	100.69.141.6	intrusion.com, uno.i	securepubads.g.dou	Internal	50	2024-05-23 11:37:49	2024-05-23 16:57:05
Kille	d 4	141	100.69.141.161	deadreconing2.local	100.69.141.6	intrusion.com, uno.i	segment-data.zqtk.net	Internal	3	2024-05-23 11:55:25	2024-05-23 11:55:25
• Kille	d 4	141	100.69.141.72	rpaul-44nz573.local	100.69.141.6	intrusion.com, uno.i	segments.company	Internal	4	2024-05-23 16:23:51	2024-05-23 16:23:51
▼ Kille	d 4	141	100.69.141.124	mschram-dmnjgb3.l	100.69.141.6	intrusion.com, uno.i	sentry-next.wixpress	Internal	3	2024-05-23 11:23:15	2024-05-23 11:23:15
Details DNS Client IP: 100.69:141.124 QNAME: s Client Hostname: mschram-dmnjgb3Jocal Domain: w Server ID: 100.69:141.6 CNAME: s Server Hostname: intrusion.com, uno.intrusion.com sentry-ssl-4 First Seen: 2024-05-23 11:23:15 Answer(s): Last Seen: 2024-05-23 11:23:15 Answer(s):					ixpress.com s-east-1.elb.amazon 99, 3.225.60.63, 18.2	Location Client Locati Server Locat aws.com 10.80.173	on: Local ion: Local		Risk Risk So Risk Lee Risk Cla Risk De This do for risky phishin	urce: sentry-next.wixpre vel: 4 sss: Malicious domain scription: main/IP has appeared or v or malicious activity, to g, ransomware, and APT:	ss.com n threat lists recently include spamming, i.

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.

			□ ₽	<u>[-</u>]	0	â		D	Consc	ole	J.	ን≓ ≁	((;	кТул	+			?	×	
			→	\oslash	top	0	Filte				D	efault	leve	Is 🔻	9 30	क्षि (
			<u>h</u> f	ittps: or ti	//blog .ps on	<u>s.windo</u> updatir	ng to	om/ms the	edgeo new F	<u>dev/2</u> Force	020/ d Co	/ <u>09/1</u>	.7/s Mo	<u>tylin</u> de st	<u>g-for</u> andaro	-windo 1.	ws-hi	<u>gh-co</u>	ntra	
			S F	ailed et::E	l to lo RR_BLC	ad reso OCKED_BY	ource (_CLI	: ENT		<u>M3</u>	<u>3KD-</u>	YMV8	Y-6	<u>25W4-</u>	V96WF	-R28AJ	:1 🕀	Ø		
			A T f	racki rom l	.ng Pre .oading <u>//s.go</u>	ventior	n blo	cked /boom	a Scr <u>ieran</u> g	ript g <u>/M33</u>	reso	ource	- <u>62</u>	<u>home</u> . 5W4-V	<u>treas</u> 96WF-1	ury.go R28AJ.	ov/:58	2 Ø)		
			[w h	Inter ith p ittps:	ventic laceho <u>//go.m</u>	n] Imag lders. <u>icrosof</u>	ges lo Load F <u>t.co</u>	oaded even m/fwl	lazi ts ar _ink/;	ily a re de <u>?link</u>	nd r ferr id=2	repla red. 20481	ced See <u>13</u>	home	e.trea	<u>sury.</u> ;	<u>gov/:</u> 2	2125		
R	Ó In	spector () Con	sole D	Debugger	↑↓ Network	{} Sty	le Editor	Q Perf	ormance	F: s	torage	τ Ac	cessibility	888 App	lication	O: Memor			
Û	∀ Filt	er URLs					,					+ Q	0	All HT	ML CSS	JS XHR	Fonts Im	ages Mei	dia WS	j Other 🔽
Statu	s	Method	Domai	n			File								Initiat	or		Туре	Tran	sferred
200		GET	anglo	dingchoice	esmessages.g	oogle.com	AGSKWX	(1rf2J XF3	6EDrNuHE	EelQ6WeN	/lpnWy9	E6tQ6qfc	ESuxbai	van7ndNy	Rux 7f6b4	7b885c961c	1893a3d5	js	6.52	kB
200		GET	🔒 s.yii	mg.com		-	rapid3.js							-	7f6b4	7b885c961c	1893a3d5	js	37.15	5 kB
204		OPTIONS	🔒 pro	d.pyxis.atp	.fox		submit								fetch			plain	324 F	В
200		OPTIONS	🔒 pro	d.idgraph.	dt.fox		item								fetch			plain	345 8	В
0		GET	🔒 from	ntdoor.kno	itch.it		ingress?	prowser_u	rl=https://	/www.fox	news.co	m/&root	browse	er_url=http	s://v ktaq.r	<u>nin.js:1</u> (img)	gif	NS_E	ERROR_FAILURE
200		GET	🔒 stat	ic.foxnews	.com		legal-tex	t-swap.js?	v=2024052	22012951					<u>7f6b4</u>	7b885c961c	<u>1893a3d5</u>	js	1.61	kВ
-		C	0						050004001									1	4.57	

200 200 200

200

200

200

200

200

GET

GET

GET

POST

GET

GET

static.foxnews.com

🔒 global.ketchcdn.com

3p-geo.yahoo.com

static.foxnews.com

static.foxnews.com

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.

rd?d visid ver=4.4.0&d fieldgroup=MC&d rtbd=json&d ver=2&d verify=1& VisitorAPI.js:4 (xhr)

p?s=1197809846&t=Icrq4muWUICYBdcW,0.7403039381081394&_I=&_AO=0& rapid3.js:3 (beacon)

metrics.js?v=202306271641

config.json

scroll-up-header.js?v=20240522012951

weather.js?v=20240522012951



V Disabl

811 B

1.45 kB

3.92 kB

771 B

1.55 kB

1.68 kB

json

json

gif

7f6b47b885c961c1893a3d5... js

7f6b47b885c961c1893a3d5... js

7f6b47b885c961c1893a3d5... js

ktag.min.js:1 (fetch)

Traffic 👻	Permits 👻	Llsers 🗶 Admin				۱ [DN	IS Responses Sort Options 😵			
		DNS Responses Sort Options ?									
							<u> </u>	 Status 	×	ASC	DESC
Search	= Filter	 Status 	×	ASC	DESC		*	- Risk	×	ASC	DESC
bearen		Risk	×	ASC	DESC		\bigcirc	Last Seen	x	ASC	DESC
lient IP	Client Hostna	 Risk Class 	×	ASC	DESC		9				
	samsung local	 Direction 	×	ASC	DESC		^ '	 Risk Class 	×	ASC	DESC
	samsung local	 Requested 	×	ASC	DESC		. · ·	 Direction 	×	ASC	DESC
	intzadmin2 lor	 Client IP 	×	ASC	DESC			- Requested	x	ASC	DESC
	intzadmin2.loc	 Server IP 	×	ASC	DESC			- Client ID	×		DECC
	samsung local					-	_	Client IP	~	ASC	DESC
	samsung.local	VLAN		ASC	DESC						
	samsung.iocai	Client Hostname		ASC	DESC						
	desktop-aopu	Server Hostname		ASC	DESC						
	deadreconing.	Perponses		ASC	DESC						
	deadreconing.	Responses		730	DESC						
	samsung.local	First Seen		ASC	DESC						
	deadreconing.	Last Seen		ASC (DESC						
	samsung.local	Domain		ASC	DESC						
	skull-1101.loc			100	DIGG						
	skull-1101.loc	CNAME		ASC	DESC						

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.