

ULTRADNS FIREWALL UI USER GUIDE

UltraDNS Firewall™ UI - Account User Guide

This guide provides detailed step-by-step examples and instructions for using the UltraDNS Firewall User Interface.

neustar®

This document is for informational purposes only. NEUSTAR MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Neustar.

Neustar may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Neustar, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, email address, logo, person, place, or event is intended or should be inferred.

© 2023 Neustar, Inc. All rights reserved.

Neustar Ultra Services and UltraCare are Neustar's trademarks and any use of these or any other Neustar mark without Neustar's express written consent is prohibited. All other trademarks and/or service marks identified or referenced are the property of their respective owners and subject to their usage requirements.

Table of Contents

| | |
|--|-----------|
| Overview | 1 |
| Logging In | 2 |
| Login Types and Roles | 3 |
| Sponsor | 3 |
| Account | 3 |
| Navigating the UltraDNS Firewall Portal | 5 |
| UltraDNS Firewall Portal Landing Page | 6 |
| Analytics | 8 |
| Source Networks | 8 |
| Redirect Details | 13 |
| Tools | 18 |
| Categorization Lookup | 18 |
| Policy Tester | 22 |
| Configuration | 27 |
| Source Networks | 27 |
| Resolvers | 35 |
| Redirect Settings | 38 |
| Black and White Lists | 53 |
| Status | 62 |
| Upcoming Events | 62 |
| Manage Account | 64 |
| Manage Account | 64 |
| Manage Users | 65 |
| Manage Profile | 70 |
| Audit | 71 |
| Filters | 72 |
| Support | 74 |
| Glossary | 75 |

Table of Figures

| | |
|--|----|
| Figure 1 UltraDNS Firewall - Security Solutions Login Page | 2 |
| Figure 2 UltraDNS Firewall Portal – Landing Page..... | 5 |
| Figure 3 UltraDNS Firewall Portal - Home Landing Page | 7 |
| Figure 4 Analytics - Source Networks Details..... | 9 |
| Figure 5 Analytics – Slate Breakdown Search Query | 10 |
| Figure 6 Analytics - Source Networks - Time Series | 11 |
| Figure 7 Analytics - Source Networks Slate Breakdown..... | 12 |
| Figure 8 Analytics - Source Networks – Details..... | 13 |
| Figure 9 Analytics - Redirect Details | 14 |
| Figure 10 Redirect Details – Breakdown Details | 15 |
| Figure 11 Analytics - Redirect Details - Slate Overview and Details..... | 16 |
| Figure 12 Analytics - Redirect Settings - Redirected Domains | 17 |
| Figure 13 Analytics - Redirect Settings - CPIP Details | 17 |
| Figure 14 Tools - Categorization Lookup..... | 18 |
| Figure 15 Tools - Categorization Lookup Return..... | 19 |
| Figure 16 Tools - Categorization Lookup – Dating | 20 |
| Figure 17 Tools - Categorization Lookup – Gambling..... | 21 |
| Figure 18 Tools - Categorization Lookup - Not Categorized..... | 22 |
| Figure 19 Tools - Policy Tester | 23 |
| Figure 20 Policy Tester - Domain..... | 23 |
| Figure 21 Policy Tester - Source Network..... | 24 |
| Figure 22 Policy Tester - Domain Option Results..... | 24 |
| Figure 23 Policy Tester – Domain | 25 |
| Figure 24 Policy Tester - IP Address and Resolver | 25 |
| Figure 25 Policy Tester - IP Address and Resolver Result | 26 |
| Figure 26 Configuration - Source Networks..... | 27 |
| Figure 27 Configuration - Add Source Network Details | 29 |
| Figure 28 Configuration - Edit a Source Network | 30 |
| Figure 29 Source Networks - Edit Source Network Details..... | 31 |
| Figure 30 Source Networks - Black / White Lists Configuration..... | 32 |
| Figure 31 Source Networks - Other Properties Options..... | 32 |
| Figure 32 Source Network - Category Filters | 33 |
| Figure 33 Configuration - Delete Source Network | 35 |
| Figure 34 Configuration - Resolvers..... | 36 |
| Figure 35 Configuration - Resolver - Edit Resolver Details..... | 37 |
| Figure 36 CPIP Setup Guide..... | 38 |
| Figure 37 Redirect Settings - Landing Page..... | 39 |
| Figure 38 Redirect Settings - NX Domain Response – Neustar Managed..... | 40 |
| Figure 39 Redirect Settings - NX Domain - Neustar Managed - Customized..... | 41 |
| Figure 40 NX Domain Response – Customer Managed..... | 42 |
| Figure 41 Redirect Settings – Category Redirects – Neustar Managed - Default | 43 |

| | |
|--|----|
| Figure 42 Category Redirects - Neustar Managed – Customized..... | 44 |
| Figure 43 Redirect Settings - Category Redirects - Default Message..... | 45 |
| Figure 44 Redirect Settings – Category Redirects - Custom Message..... | 46 |
| Figure 45 Redirect Settings – Category Redirects - Host Your Own..... | 47 |
| Figure 46 Redirect Settings – Blacklist – Neustar Managed – Default..... | 48 |
| Figure 47 Redirect Settings – Blacklist – Neustar Managed – Customized | 49 |
| Figure 48 Redirect Settings - BlackList - Default Message..... | 50 |
| Figure 49 Redirect Settings - Blacklist – Customized Message..... | 51 |
| Figure 50 Redirect Settings - Blacklist – Customer Managed..... | 52 |
| Figure 51 Configuration - Black & White Lists | 53 |
| Figure 52 Configuration - Import Blacklist .CSV Template..... | 54 |
| Figure 53 Configuration - Black List - Import Confirmation | 54 |
| Figure 54 Black & White Lists - Edit Black List..... | 55 |
| Figure 55 Black & White Lists - Edit Black List Details | 56 |
| Figure 56 Black & White Lists - Delete Black List..... | 57 |
| Figure 57 Black & White Lists - Add a White List..... | 58 |
| Figure 58 Configuration - Import White List .CSV Template | 59 |
| Figure 59 Configuration - White List - Import Confirmation..... | 59 |
| Figure 60 White Lists - Edit White List..... | 60 |
| Figure 61 White Lists - Delete White List..... | 61 |
| Figure 62 Service Status..... | 62 |
| Figure 63 Manage Account - View Account Details..... | 65 |
| Figure 64 Manage Account - Manager Users..... | 66 |
| Figure 65 Manage Users – Create New User..... | 67 |
| Figure 66 Manage Users - Manage User Details..... | 68 |
| Figure 67 Manage Users - Suspend a User | 68 |
| Figure 68 Manage User - Reactive Suspended User | 69 |
| Figure 69 Manage Profile..... | 70 |
| Figure 70 Audit Log Display | 71 |
| Figure 71 Audit Log – Filters | 72 |
| Figure 72 Audit Log - View Details | 73 |
| Figure 73 Support Page..... | 74 |

Overview

We are pleased to offer you **UltraDNS Firewall™**, a recursive DNS service that is built off of the same 30 node locations as UltraDNS, the Neustar Authoritative DNS platform. UltraDNS Firewall leverages BGP and Anycast to route queries in the most efficient manner, and guarantees that you can get to your favorite online website(s) or services in a timely fashion.

UltraDNS Firewall comes equipped with built-in DDoS protection to prevent attackers from taking the service down. Additionally, Neustar constantly monitors the usage of the UltraDNS Firewall network to ensure that no malicious attackers are leveraging the network for nefarious purposes. Furthermore, UltraDNS Firewall offers security capabilities such as category/content blocking (Malware, Gambling, etc.), control over how a customer is redirected when visiting a blocked site, and also allows administrators to set Whitelists or Blacklists.

Via the UltraDNS Firewall Portal, you can monitor and customize the content blocking of your traffic through the usage of various types of filters. To ease the process for you, blocking and filtering can be adjusted with the simple click of a button. Furthermore, you can even customize display messages that will appear for any websites that are blocked or can be possibly harmful. Finally, we have provided the ability for you to view reports that provide details about your queries, responses, and blocked or NXdomain data.

Logging In

The UltraDNS Firewall portal can be found at <https://portal.ultradnsfirewall.neustar/>

If you have an existing account on the portal, provide your username and password for your account, and then click on the **Login** button. If you have forgotten your password, click the **Reset Password** link and you will be sent a temporary password to your email address. The email will contain a link that will return you to the login screen, and will prompt you to create a new password for your account.

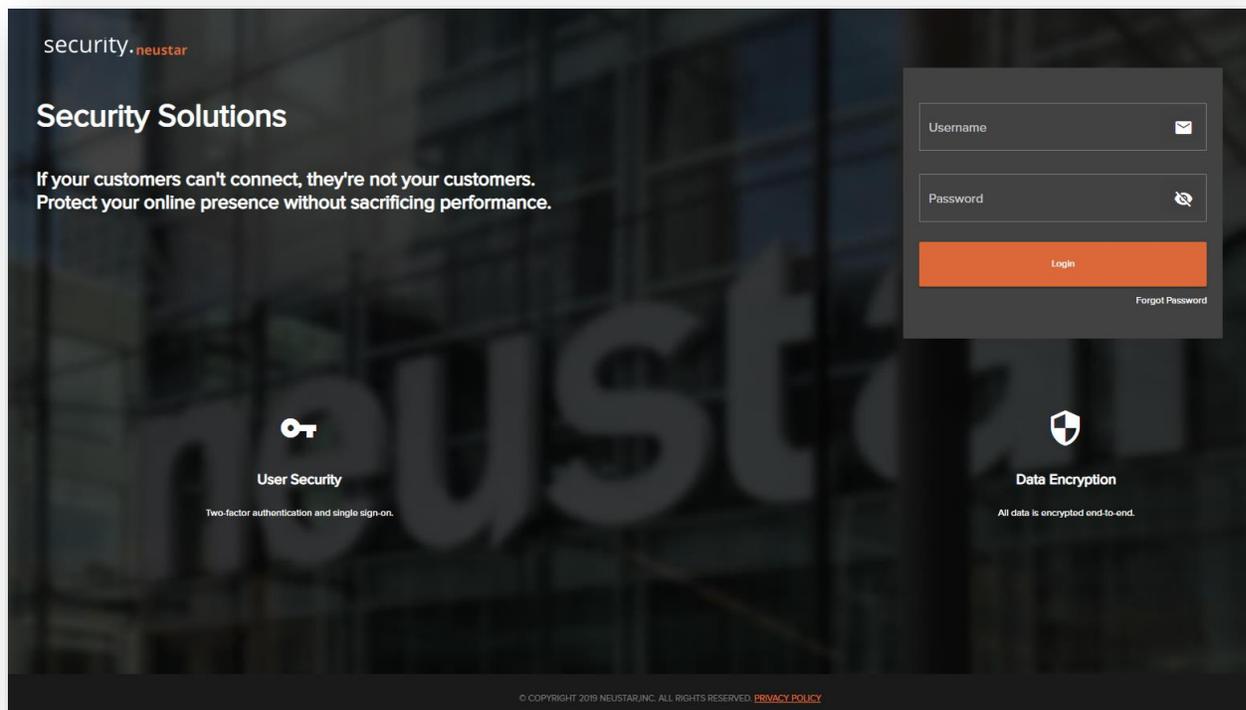


Figure 1 UltraDNS Firewall - Security Solutions Login Page

Login Types and Roles

There are two types of accounts available on the UltraDNS Firewall Portal: *Sponsors* and *Accounts*. Within each of the account types, there are two different roles that can be assigned: *Admin* and *Reporter*. Please find the appropriate account type and role combination below for further explanation of the accessibility and limitations to the portal.

This guide is designed to assist **Account** level users with navigating through the UltraDNS Firewall Portal, managing their users' details, and ultimately maintaining and customizing query details and restrictions.

Sponsor

The Sponsor account is a parent-level (top level) resource, and designed for re-sellers, partners, or very large customers associated with Neustar. Sponsors accounts must have VIPs designated to them.

Account

An Account is more restrictive in the actions that can be taken on the UltraDNS Firewall Portal. The Account type does not have a designated VIP, but rather, shares a default VIP that is set up by Neustar. Additionally:

- Sponsors can make changes to any Account types that have been provisioned.
- Sponsors need to give permission for an Account to have access to the Redirect Settings.
- Sponsors have access to the Resolver level Analytics, while Accounts do not.

Given the above level restrictions, an Account login-type still has the ability to view and edit details for the Sponsor under which it was created.

Each login-type can have one of two roles assigned to it, which either allow or restrict certain actions from being taken on the UltraDNS Firewall portal.

Admin

The Admin role provides read/write¹ access to the UltraDNS Firewall portal. Having the Admin role allows you to make changes to the Sponsor features, Account and User features.

This is the highest role that you can have on the portal.

¹ Read / Write Access – The Read privilege allows a user to only view information, while the Write access allows a user to edit information.

Reporter

The Reporter role provides read only access to all of the Accounts under the Sponsor, and all of the users under the Sponsor, as well as the Account.

Navigating the UltraDNS Firewall Portal

To navigate the UltraDNS Firewall Portal, use the left-hand side navigation menu to access the various features of your account. Each section expands out to display subsequent drop-down menus to provide additional navigation options within each section to make navigation easier.

Analytics – Displays reports and real time data for your account.

Tools – Provides additional methods in which to view and filter your query data.

Configuration – Allows you to setup and customize your Source Networks, Resolvers, Filtering and Redirect settings.

Audit – Displays a chronological view of all actions taken for your account, along with additional filtering tools for greater granularity for your search requests.

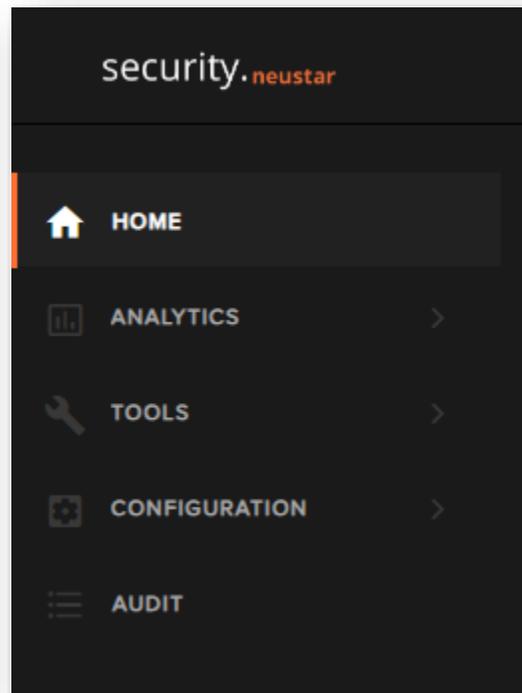


Figure 2 UltraDNS Firewall Portal – Landing Page

UltraDNS Firewall Portal Landing Page

When you log into the UltraDNS Firewall Portal, you will begin on the **HOME** section of the navigation dashboard.

The Home page displays the following details:

- **Quick Seven Day Overview**

- Responses for the current day (in orange) vs Responses received in the last seven days (in grey) for the selected Sponsor and Account (or all Accounts under the Sponsor) combination.
- The Responses count does not equal the total queries received, as responses can include Blocked traffic, NX Domain traffic, as well as Dropped traffic.
 - Blocked traffic – Traffic that is redirected to a block or warn page based upon policies set (by an Admin).
 - NX Domain traffic – Traffic that is redirected to a non-existent domain.

- **Traffic Trends** (broken down by traffic type) for the last seven days.

- **Top Blocked Categories** for the Sponsor / Account combination.

- The arrows indicate either an increase or decrease in the average type of traffic for the last seven days.
- The Slate (Breakdown) Chart displays the total percentage of a traffic type (filtering type) for the Sponsor. Within each type, you can hover over a segment to view the specific details (the segment will pop-out from the chart).

- **Top 10 Blocked Domains**

- Displays the ten most blocked domains based upon traffic / query volume for the Sponsor/Account combination in the last seven days.

- **Top 5 Source Networks**

- Displays the five source networks with the most traffic / query volume received in the last seven days. Additionally, each Source Network displays the type of traffic filtering applied, as well as the total percentage of traffic the specified source network received compared to all of the traffic the Sponsor/Account.
 - You can hover over the speedometer gauge to see the actual percentage of traffic the Source Network received.



Figure 3 UltraDNS Firewall Portal - Home Landing Page

Analytics

The Analytics section provides detailed graphical data for the various “features” within your account.

Source Networks

The Source Networks Analytics section displays the following details (by default) for the last seven days, if the account Administrator has created policies.

- **Queries** – Total number of queries received (per million).
- **Responses** – Total number of responses received (per million).
 - **Responses** – Displays the total number of responses received from the total query count.
 - **No Responses** – Displays the total number of the No responses that were received.
 - **Valid** – Displays the total number of valid responses received
 - **NX Domain** – Displays the total number of responses that were answered with an NX domain.
- **Actions** – Total number of “actions” taken based upon the Source Network settings.
 - **Redirect** – Displays the total number of redirects made (per thousand).
 - **Monitor** – Displays the total number of queries that are being monitored.

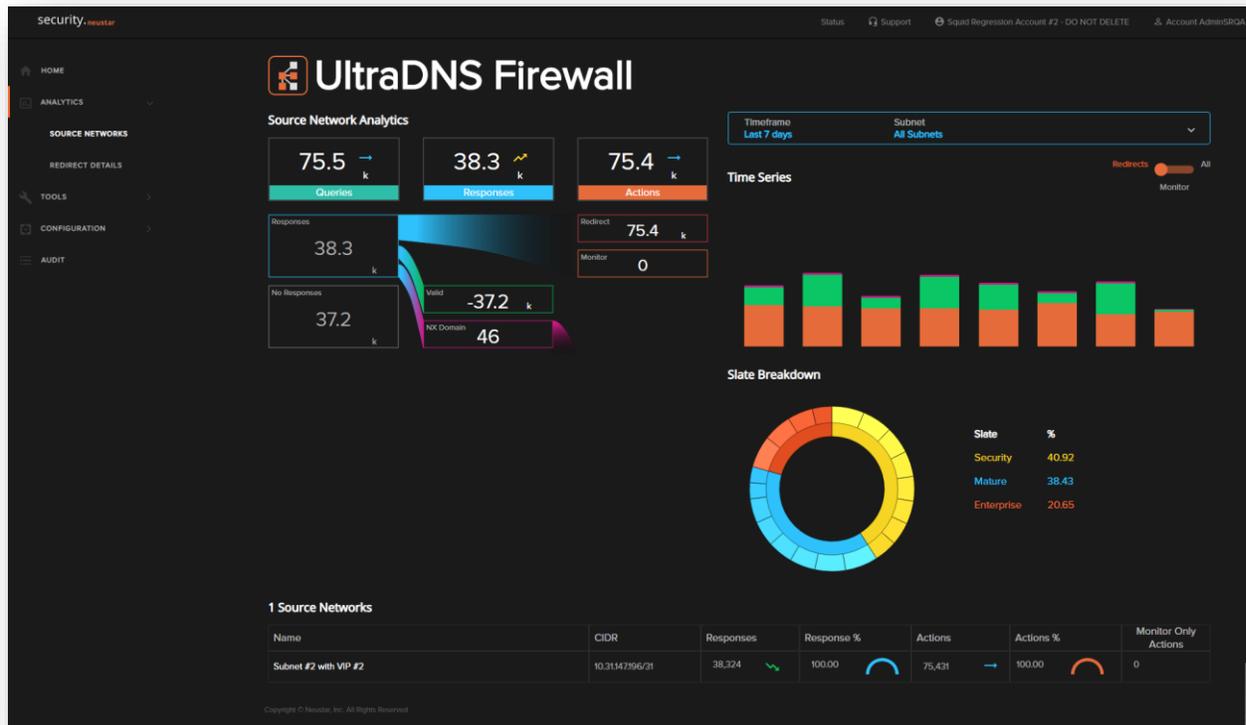


Figure 4 Analytics - Source Networks Details

Filtering Options

The filtering option allows you to customize the data and report details that are displayed. To access the Search Query, click into the **Timeframe / Subnet** box directly above the Slate Breakdown chart.

The screenshot shows a search query configuration panel with the following elements:

- Timeframe:** A dropdown menu currently set to "Last 7 days".
- Subnet:** A dropdown menu currently set to "All Subnets".
- From:** A date input field containing "9/6/2019" with a calendar icon to its right.
- To:** A date input field containing "9/13/2019" with a calendar icon to its right.
- Quick Select Time Frame:** A row of buttons: "Today", "Last 7 days", "Yesterday", "This Month", "Last Month", and "This Year".
- Buttons:** "Clear" and "Apply" buttons at the bottom right.

Figure 5 Analytics – Slate Breakdown Search Query

The Search Query offers the following options:

- **From Date** – Click on the **Calendar** icon to select a start date for your query.
- **To Date** – Click on the **Calendar** icon to select the ending date for your query.
- **Quick Select Time Frame** – Instead of using the From and To fields, you can select one of the pre-created time frames to apply to your search query.
 - **Today** – Will query starting from 01:00:00am of the current date up to the current time.
 - **Last 7 Days**
 - **Yesterday**
 - **This Month**
 - **Last Month**
 - **This Year**
- **Subnet** – The Subnet field allows you run your query against a specific subnet you have access to, or by default, you will get results for All Subnets.

Once you have made your selections, click the **Apply** button and the **Source Networks Analytics** details will be updated, the Time Series and Slate Breakdown chart will reconfigure, and the Source Networks details will update as well.

Time Series

The Time Series chart displays the consolidated data that matches the filtering criteria provided. By default, the Time Series will show the past seven days, with each chart displaying a full day's worth of data. Hover over a chart to see the condensed details for the day.

The Time Series also includes a toggle that allows you to view only the **Redirects**, or only the data captured from setting a subnet to **Monitor**, or you can view all responses.

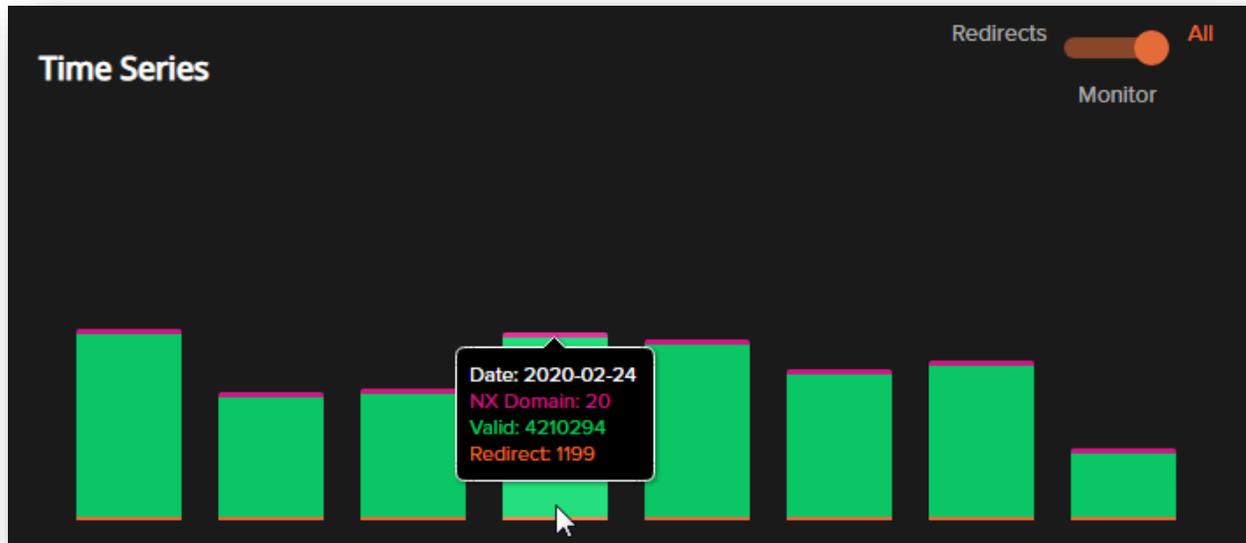


Figure 6 Analytics - Source Networks - Time Series

Slate Breakdown

The Slate Breakdown section displays the three categories of traffic categorization in a pop-out pie chart, and within each category, specific traffic types are viewable. This chart allows you to see specifically what types of traffic are being received, as well as the percentage of each type of sub-traffic. Hover over a section of the Slate chart to pop-out the section, and to view the details specific to that section.

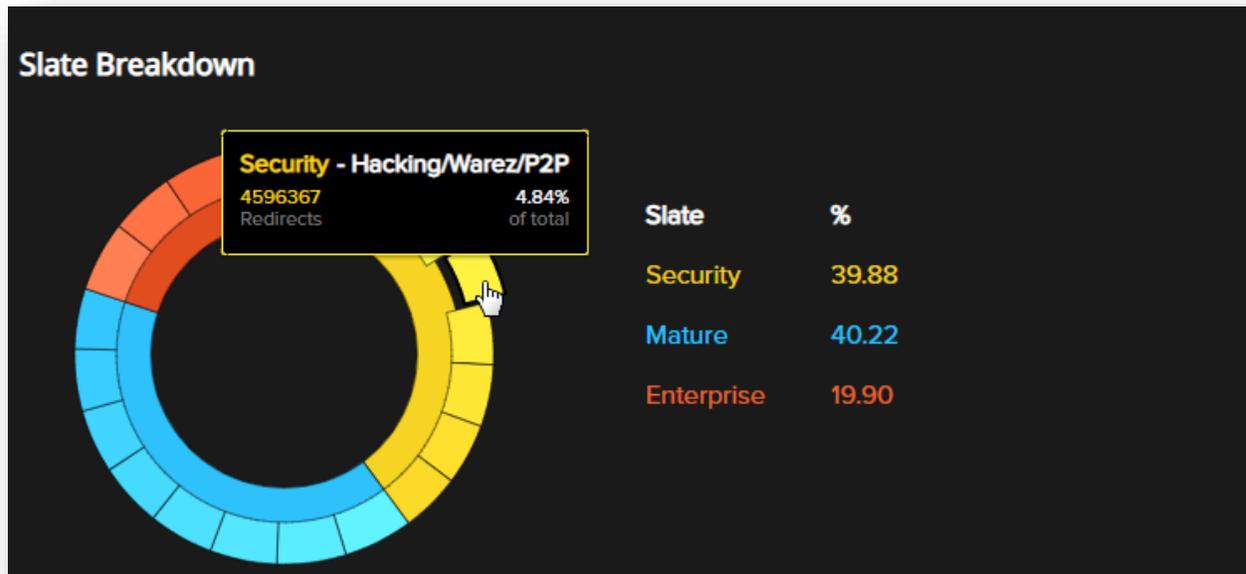


Figure 7 Analytics - Source Networks Slate Breakdown

In the above example, **Security** traffic made up 38.82% of all of the traffic received. Of that 38.82%:

- 6.02% was Parked Domains.
- 5.29% was Anonymous Proxies
- 5.03% was Hacking/Warez/P2P
- 5.02% was Spyware
- 4.75% was Phishing
- 4.41% was Malware
- 4.24% was Ransomware
- 4.06% was Bots/C2

Source Networks Breakdown

The Source Networks table at the bottom screen displays all of the Source Networks for the specific Sponsor/Account combination and the Subnet that was listed in the search query (by default, it will display **All Subnets** for the **Last 7 Days**).

The colored arrows indicate either an increase or decrease in the average type of traffic for the last seven days (or the configured time period). The speedometer gauge provides a visual graphic of the actual percentage of traffic the Source Network received compared to the other source networks listed.

| 1 Source Networks | | | | | |
|-----------------------|------------------|--|---|---|---|
| Name | CIDR | Responses | Response % | Actions | Actions % |
| Subnet #2 with VIP #2 | 10.31.147.174/31 | 92,052  | 100  | 175,621  | 100  |

Figure 8 Analytics - Source Networks – Details

The Source Network details are displayed as the following:

- **Name** – The name of the Source Network.
- **CIDR** – The CIDR for the Source Network.
- **Responses (Total)** – The total number of responses that were received by the subnet during the selected time period.
- **Response % (of the total)** – The percentage of responses that this particular subnet received out of the total number of responses received by all subnets under the designated account.
- **Actions** – The total number of actions taken for the responses that were received.
 - Response types can be found in the **Source Network Analytics** chart above.
- **Actions %** - The percentage of actions taken for this particular subnet out of the total number of actions taken for all subnets under the designated account.

Redirect Details

The Redirect Settings page displays the traffic that is redirected when an attempt to access a webpage(s) that has been blacklisted, or that contains content that has been blocked is made. The Redirect Details Analytics page displays the following details:

- **Queries** – Total number of queries received (in millions).
- **Responses** – Total number of responses given in response to queries.
- **Redirects** – The total number of responses that resulted in a redirect.



Figure 9 Analytics - Redirect Details

Redirect Details Breakdown

The Redirect Details Breakdown section provides an expanded view of the responses received for the currently selected query timeframe (by default, the Last 7 Days and All Subnets are displayed).

- **Responses** – Displays the total number of responses received during the specified timeframe.
 - **No Responses** – The total number of no responses returned.
 - **Valid** – The total number of responses received that were valid requests.
- **Redirects** – The total number of responses that were redirected per the filter settings.
 - **Block** – The total number of requests that were blocked due to blacklist filters.
 - **Warn** – The total number of requests that were flagged with a warning due to the blacklist filters.

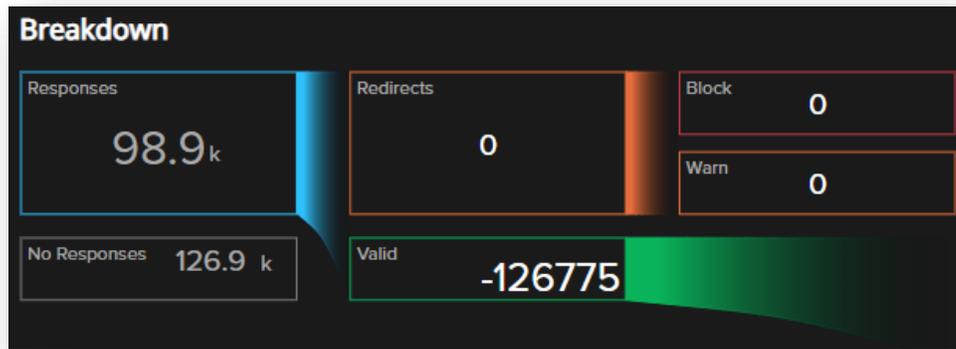


Figure 10 Redirect Details – Breakdown Details

Slate Overview

The Slate Overview section displays the three categories of traffic categorization in a pop-out pie chart, and within each category, specific traffic types are viewable along with the percentage of each traffic type versus the total query count.

The Slate Details list displays what types of traffic filters were used under each traffic category, along with an arrow indicating either an increase or decrease in the type of traffic filter.



Figure 11 Analytics - Redirect Details - Slate Overview and Details

Redirected Domains

The Redirected Domains section displays a list of the domains that were redirected either because they were blocked, or due to the warning filter. Clicking the arrow next to the domain name expands the list to display every entry from the Count column, with details about why the domain was redirected.

Additionally, the Redirected Domains sections lists the:

- Redirect % - Displays the percentage of redirects that came from the listed domain against the entire number of domain redirects during the specified query timeframe.
- Blocks – The total number of requests that were blocked due to blacklist filtering policies.
- Warns – The total number of requests that were returned with a warning for possibly violating the blacklist filtering policies.

| Subnet | Subnet CIDR | Type | Requested URL | Timestamp |
|-----------|-------------|-------|---|--------------------------|
| Undefined | Undefined | Block | http://mirror.fileplanet.com/centos/7.6.1810/extras/x86 | Sep 12, 2019, 4:19:35 AM |
| Undefined | Undefined | Block | http://mirror.fileplanet.com/centos/7.6.1810/extras/x86 | Sep 12, 2019, 4:19:35 AM |
| Undefined | Undefined | Block | http://mirror.fileplanet.com/centos/7.6.1810/extras/x86 | Sep 12, 2019, 4:19:35 AM |
| Undefined | Undefined | Block | http://mirror.fileplanet.com/centos/7.6.1810/extras/x86 | Sep 12, 2019, 4:19:35 AM |
| Undefined | Undefined | Block | http://mirror.fileplanet.com/centos/7.6.1810/extras/x86 | Sep 12, 2019, 4:19:35 AM |
| Undefined | Undefined | Block | http://mirror.fileplanet.com/centos/7.6.1810/extras/x86 | Sep 12, 2019, 4:19:35 AM |
| Undefined | Undefined | Block | http://mirror.fileplanet.com/centos/7.6.1810/extras/x86 | Sep 12, 2019, 4:19:34 AM |
| Undefined | Undefined | Block | http://mirror.fileplanet.com/centos/7.6.1810/extras/x86 | Sep 12, 2019, 4:19:34 AM |
| Undefined | Undefined | Block | http://mirror.fileplanet.com/centos/7.6.1810/extras/x86 | Sep 12, 2019, 4:19:34 AM |
| Undefined | Undefined | Block | http://mirror.fileplanet.com/centos/7.6.1810/extras/x86 | Sep 12, 2019, 4:19:34 AM |
| Undefined | Undefined | Block | http://mirror.fileplanet.com/centos/7.6.1810/extras/x86 | Sep 12, 2019, 4:19:34 AM |

Figure 12 Analytics - Redirect Settings - Redirected Domains

Capture Private IP Report Details

For accounts that have Capture Private IP (CPIP) enabled, the Redirect Details will display additional CPIP details for the URL / IP details when you expand a URL's contents.

| Domain | Count | Redirect % | Blocks | Warns |
|-------------------|-------|------------|--------|-------|
| sgowntfwkybawi.pw | 1172 | 10.52 | 1172 | 0 |

| Source | Source Network | Source IP | Type | Requested URL | Timestamp |
|--------|--------------------------------------|-----------------|-------|---------------------------|-------------------------|
| Cloud | WPM San Diego subnet 198.241.44.0/24 | 198.241.44.120 | Block | http://sgowntfwkybawi.pw/ | Mar 3, 2020, 9:30:23 PM |
| Cloud | WPM Ashburn subnet 156.154.119.0/24 | 156.154.119.164 | Block | http://sgowntfwkybawi.pw/ | Mar 3, 2020, 9:25:02 PM |
| Cloud | WPM San Diego subnet 198.241.44.0/24 | 198.241.44.120 | Block | http://sgowntfwkybawi.pw/ | Mar 3, 2020, 9:19:49 PM |
| Cloud | WPM San Diego subnet 198.241.44.0/24 | 198.241.44.120 | Block | http://sgowntfwkybawi.pw/ | Mar 3, 2020, 9:00:05 PM |
| Cloud | WPM San Diego subnet 198.241.44.0/24 | 198.241.44.120 | Block | http://sgowntfwkybawi.pw/ | Mar 3, 2020, 8:49:49 PM |
| Cloud | WPM Ashburn subnet 156.154.119.0/24 | 156.154.119.164 | Block | http://sgowntfwkybawi.pw/ | Mar 3, 2020, 8:34:47 PM |
| Cloud | WPM Ashburn subnet 156.154.119.0/24 | 156.154.119.164 | Block | http://sgowntfwkybawi.pw/ | Mar 3, 2020, 8:34:32 PM |

Figure 13 Analytics - Redirect Settings - CPIP Details

Tools

Categorization Lookup

The Categorization Lookup allows you to search for a specific Domain name to see what type of category or categories it currently falls under. This tool allows you to see why a certain domain might be getting blocked or encountering warnings due to its category labeling, which allows you to edit your blacklist filters if necessary.

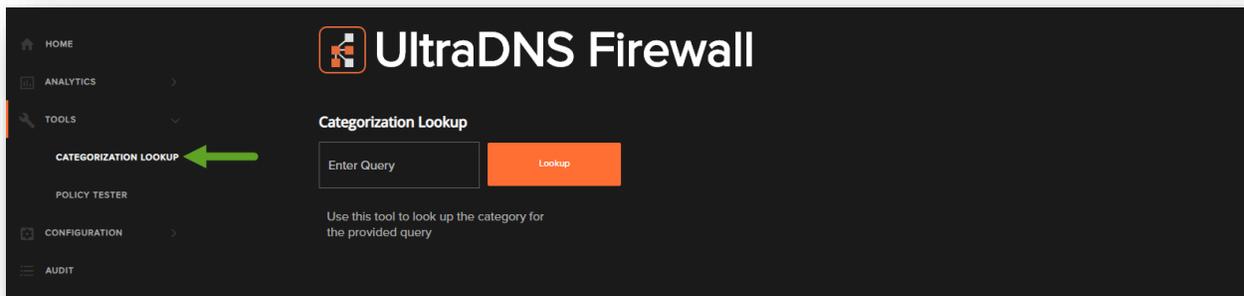


Figure 14 Tools - Categorization Lookup

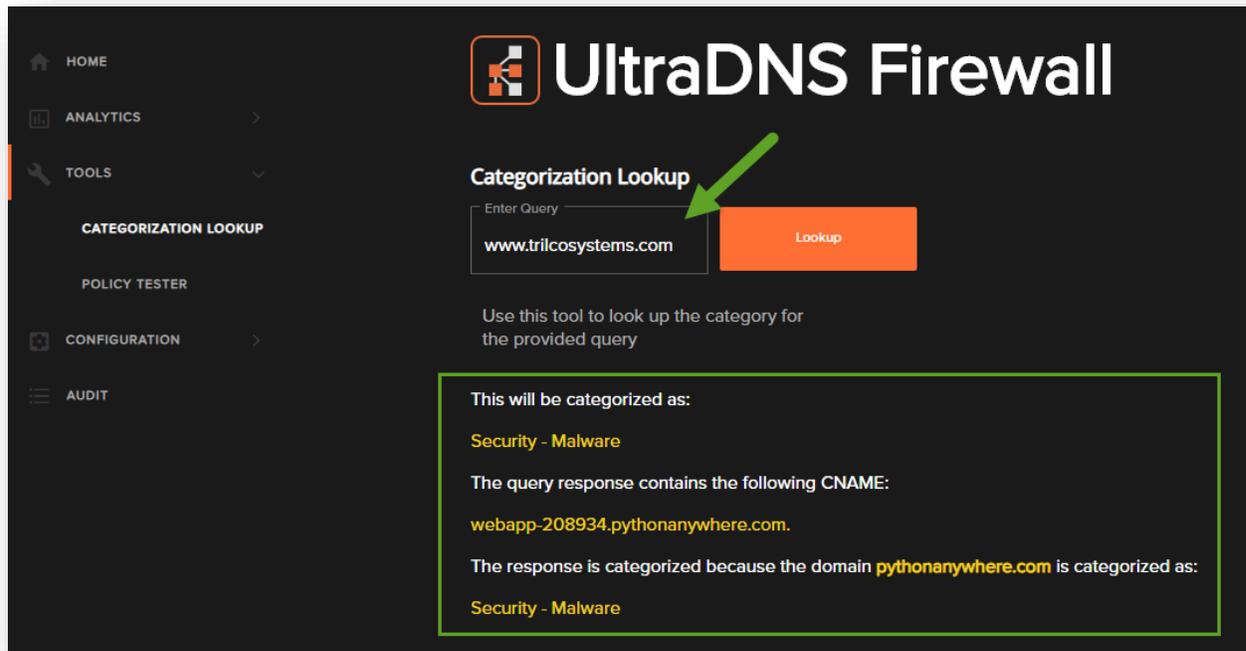
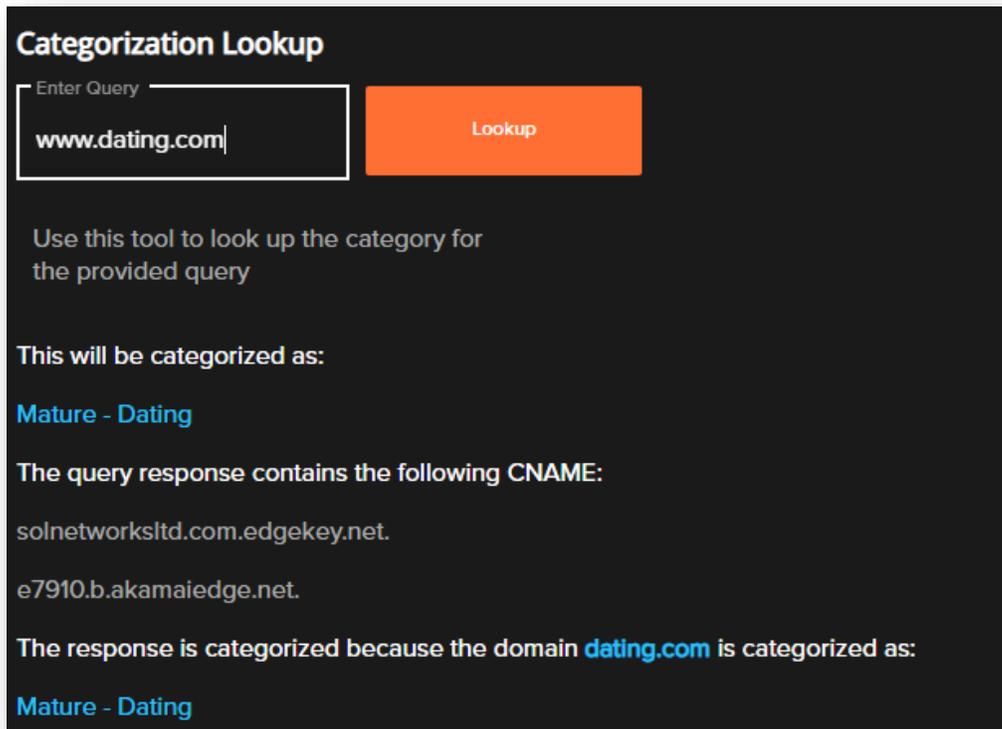


Figure 15 Tools - Categorization Lookup Return

The Categorization Lookup will also check CNAMEs or Uncategorized domains and return the result based upon that result.

For example, the above Domain www.trilcosystems.com has the CNAME pythonanywhere.com which is categorized as Malware, so the www.trilcosystems.com lookup is therefore categorized as Malware.

Additional result types are listed below.



Categorization Lookup

Enter Query

Use this tool to look up the category for the provided query

This will be categorized as:

Mature - Dating

The query response contains the following CNAME:

solnetworksltd.com.edgekey.net.
e7910.b.akamaiedge.net.

The response is categorized because the domain **dating.com** is categorized as:

Mature - Dating

Figure 16 Tools - Categorization Lookup – Dating

Categorization Lookup

Enter Query

Use this tool to look up the category for the provided query

The domain **www.poker.com** is categorized as:

- Enterprise - Gaming
- Mature - Gambling

The query response contains the following A records:

- 104.18.44.221
- 104.18.45.221

Figure 17 Tools - Categorization Lookup – Gambling

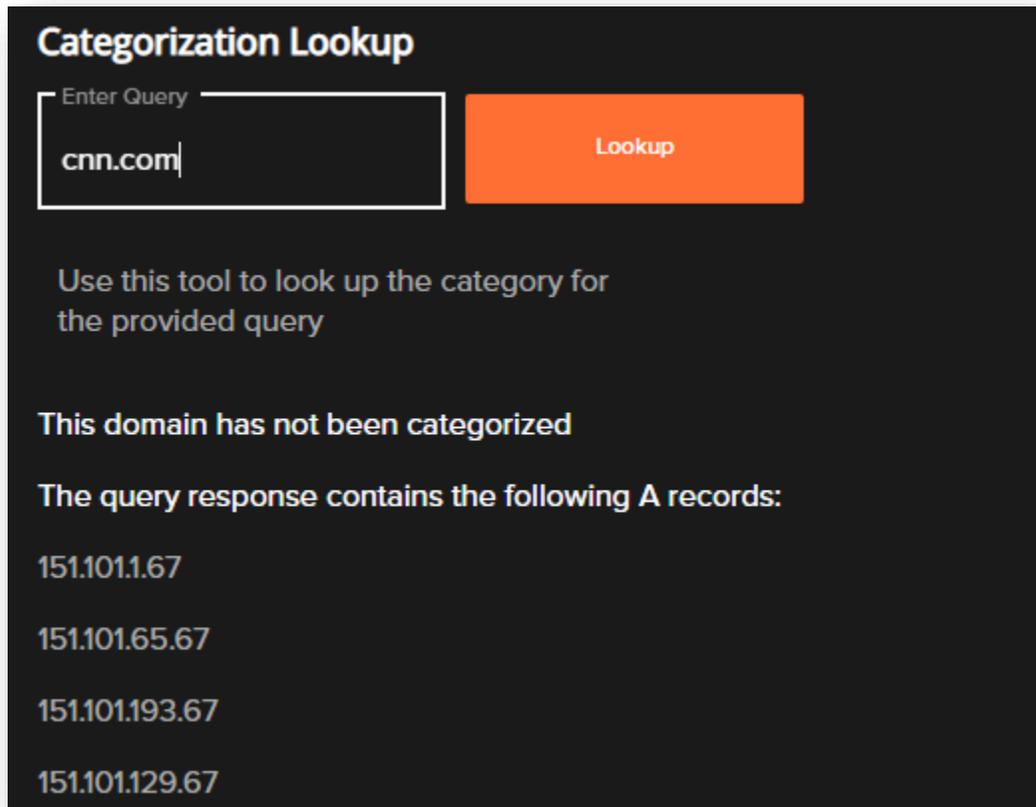


Figure 18 Tools - Categorization Lookup - Not Categorized

Policy Tester

The Policy Tester tool allows you to check the response for a provided query. This feature allows you to test whether or not your configurations will perform as expected (block malware, etc.) or if you need to adjust your settings.

There are two different methods you of testing you can choose from when performing the Policy Test: **Query using a Source Network** or **Query by specifying a resolver and source IP**.

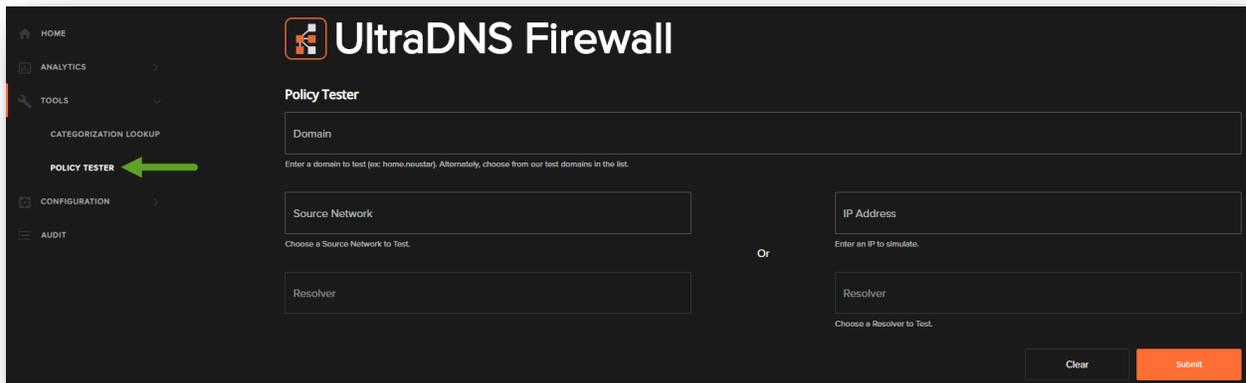


Figure 19 Tools - Policy Tester

Query Using a Source Network

1. Select a Domain from the drop-down list of available pre-configured domains, or provide your own.

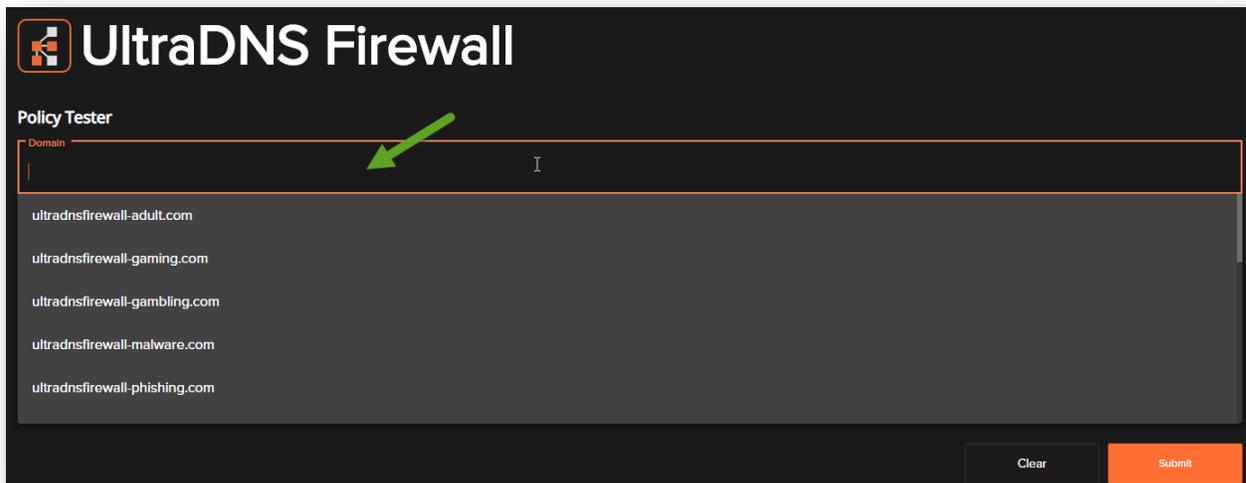
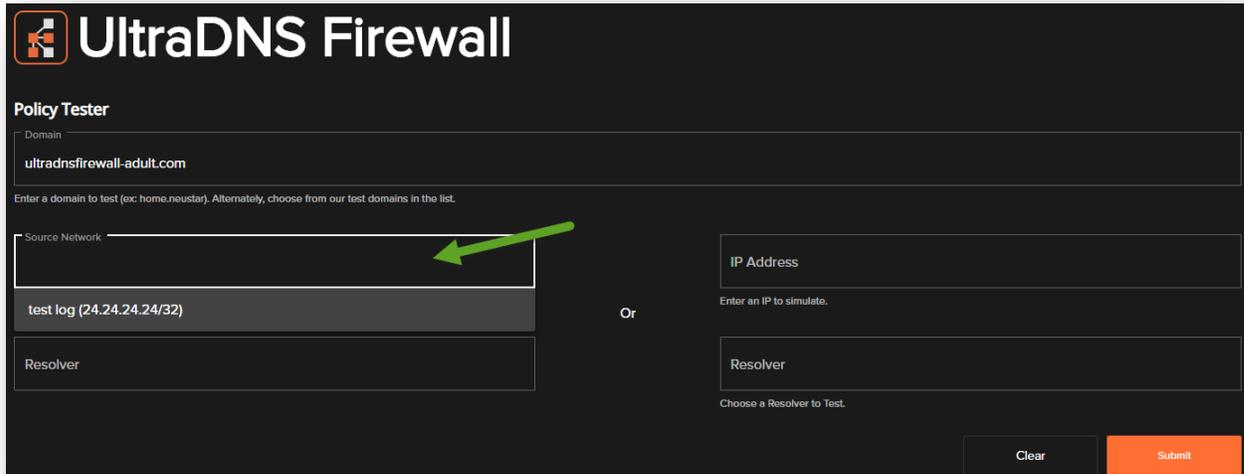


Figure 20 Policy Tester - Domain

2. Select a Source Network from the available list that are configured based upon the Sponsor/Account combination currently selected. The Resolver field will autofill afterwards.



UltraDNS Firewall

Policy Tester

Domain
ultradnsfirewall-adult.com

Enter a domain to test (ex: home.neustar). Alternately, choose from our test domains in the list.

Source Network
test log (24.24.24.24/32)

Resolver

IP Address
Enter an IP to simulate.

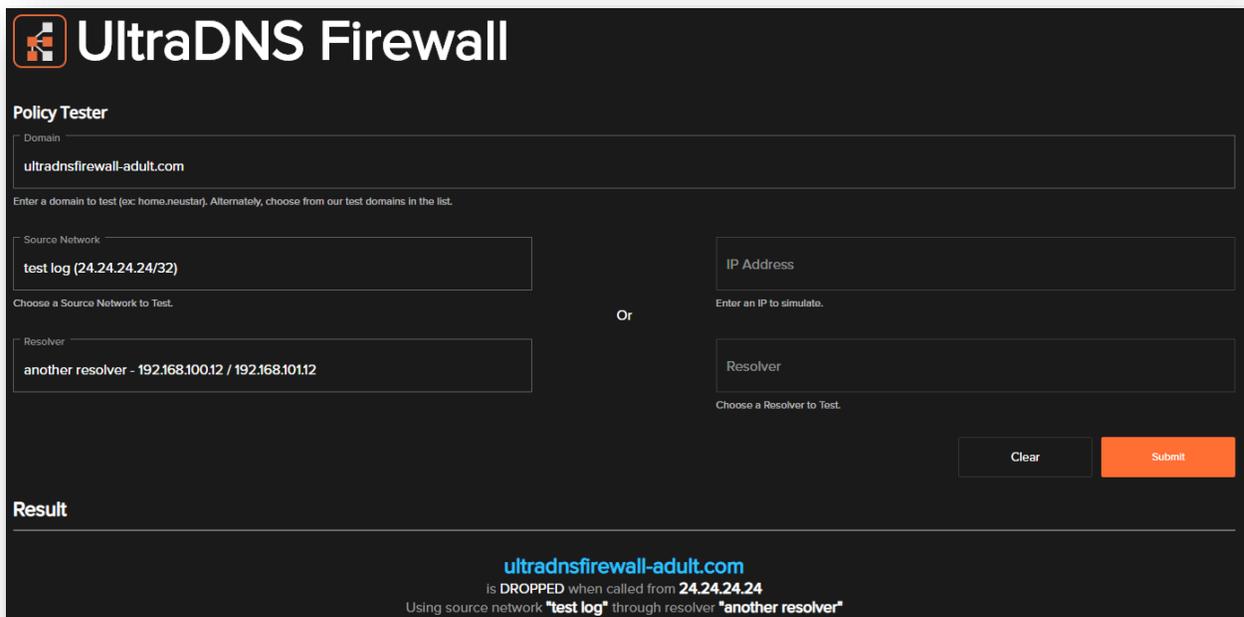
Resolver
Choose a Resolver to Test.

Clear Submit

Figure 21 Policy Tester - Source Network

3. Click the **Submit** button.

Once the test is complete, the results will be displayed at the bottom of the screen.



UltraDNS Firewall

Policy Tester

Domain
ultradnsfirewall-adult.com

Enter a domain to test (ex: home.neustar). Alternately, choose from our test domains in the list.

Source Network
test log (24.24.24.24/32)

Choose a Source Network to Test.

Resolver
another resolver - 192.168.100.12 / 192.168.101.12

IP Address
Enter an IP to simulate.

Resolver
Choose a Resolver to Test.

Clear Submit

Result

ultradnsfirewall-adult.com
is DROPPED when called from 24.24.24.24
Using source network "test log" through resolver "another resolver"

Figure 22 Policy Tester - Domain Option Results

Query Specifying Resolver and Source IP

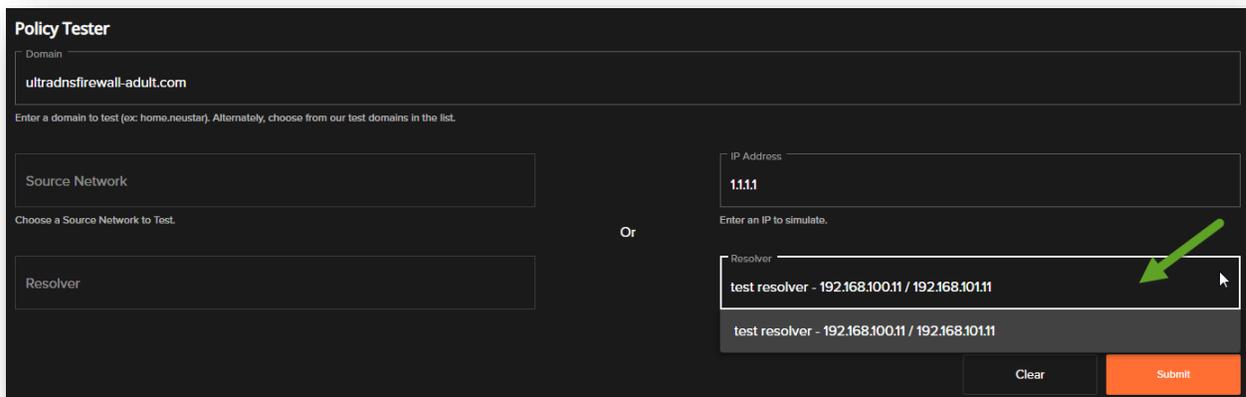
1. Select a Domain from the drop-down list of available domains, or provide your own.



The screenshot shows the 'UltraDNS Firewall' logo at the top left. Below it is the 'Policy Tester' section. A text input field labeled 'Domain' is highlighted with a green arrow. Below the input field is a list of domain suggestions: 'ultradnsfirewall-adult.com', 'ultradnsfirewall-gaming.com', 'ultradnsfirewall-gambling.com', 'ultradnsfirewall-malware.com', and 'ultradnsfirewall-phishing.com'. At the bottom right of the form are 'Clear' and 'Submit' buttons.

Figure 23 Policy Tester – Domain

2. Provide the (source) IP Address. *Only IPv4 addresses are supported at this time.*
3. Select the Resolver from the drop-down list.



The screenshot shows the 'Policy Tester' form with the 'Domain' field filled with 'ultradnsfirewall-adult.com'. Below it is a text input field for 'Source Network' and a text input field for 'IP Address' containing '1.1.1'. Below the 'Source Network' field is a text input field for 'Resolver'. Below the 'IP Address' field is a drop-down menu for 'Resolver' with two options: 'test resolver - 192.168.100.11 / 192.168.101.11' and 'test resolver - 192.168.100.11 / 192.168.101.11'. A green arrow points to the first option in the drop-down menu. At the bottom right are 'Clear' and 'Submit' buttons.

Figure 24 Policy Tester - IP Address and Resolver

4. Click the **Submit** button.

UltraDNS Firewall

Policy Tester

Domain
ultradnsfirewall-adult.com

Enter a domain to test (ex: home.neustar). Alternately, choose from our test domains in the list.

Source Network
Choose a Source Network to Test.

IP Address
1.1.1.1
Enter an IP to simulate.

Resolver
test resolver - 192.168.100.11 / 192.168.101.11
Choose a Resolver to Test.

Or

Clear Submit

Result

ultradnsfirewall-adult.com
is **DROPPED** when called from **1.1.1.1**
through resolver **test resolver**

Figure 25 Policy Tester - IP Address and Resolver Result

Configuration

Source Networks

The Source Networks page provides customization tools for directing where and how users are routed when they try to navigate to a blocked domain.

UltraDNS Firewall

Source Network

Total: 73 Source Networks Add Source Network

Filters

| Subnet | Resolver | Categories | Black Lists | White Lists | Other Attributes |
|---|--|--|-------------------|---------------------|------------------|
| NSSC - TWC - 1 98.101.26.224/29 This location created Tue Oct 17 201... | New Resolver 439 156.154.54.13 156.154.55.13 | Security 8 / 8 Mature 4 / 8 Enterprise 0 / 4 | Corp Wide Block | Corp Wide Whitelist | NX Domain |
| Vegas Internet 66.116.124.0/25 This location created Fri Dec 06 201... | New Resolver 439 156.154.54.13 156.154.55.13 | Security 8 / 8 Mature 8 / 8 Enterprise 0 / 4 | | | NX Domain |
| 5700 Innovation Dr 208.143.81.23/32 Dublin, OH 43016 | NSR Pair #1 156.154.54.1 156.154.55.1 | Security 8 / 8 Mature 8 / 8 Enterprise 0 / 4 | | | NX Domain |
| NSSC - TWC - 2 96.10.179.72/29 This location created Tue Oct 17 201... | New Resolver 439 156.154.54.13 156.154.55.13 | Security 8 / 8 Mature 4 / 8 Enterprise 0 / 4 | Corp Wide Block | Corp Wide Whitelist | NX Domain |
| 12740 Kenan Dr 64.128.240.176/28 Jacksonville, FL 32258 | NSR Pair #1 156.154.54.1 156.154.55.1 | Security 8 / 8 Mature 8 / 8 Enterprise 0 / 4 | | | NX Domain |
| New Location 172.19.3.0 172.19.3.0/24 This location created Wed Mar 15 20... | NSR Pair #1 156.154.54.1 156.154.55.1 | Security 8 / 8 Mature 8 / 8 Enterprise 3 / 4 | New Blacklist 279 | | Landing Page |
| NF - COX 216.54.113.88/29 This location created Tue Oct 17 201... | New Resolver 439 156.154.54.13 156.154.55.13 | Security 8 / 8 Mature 4 / 8 Enterprise 0 / 4 | Corp Wide Block | Corp Wide Whitelist | NX Domain |

Figure 26 Configuration - Source Networks

Subnet(s)

Each subnet is defined by its CIDR ('sy-der') address. The CIDR consists of a base IP address, the lowest IP address (IPv4 or IPv6), a slash, and then the number of bits (from the left) that defines the prefix.

For instance, 11.22.33.44/30 defines the subnet of addresses 11.22.33.44 through 11.22.33.47; four addresses in all.

VIP Subnet(s)

VIP Subnets allow you to inherit a specific set of policies from a designated VIP when creating a new Source Network. Without a VIP subnet you are randomly assigned to a subnet, and have to wait for the traffic / queries before you know which subnet you are on.

The VIP subnet feature is available for all users with the Admin role, and can be found in the Resolvers section.

The Source Network section displays the following information for an account:

- **Subnet**
- **Resolver**
- **Categories**
- **Black Lists**
- **White Lists**
- **Other Attributes**

Add New Subnets

Click the **Add Source Network** button to create a new Source Network for your Account.

Enter the Name, Description, Starting IP and CIDR length, and then select a Resolver from the drop-down menu to associate the Source Network to. Click the **Create Network** when you are finished.

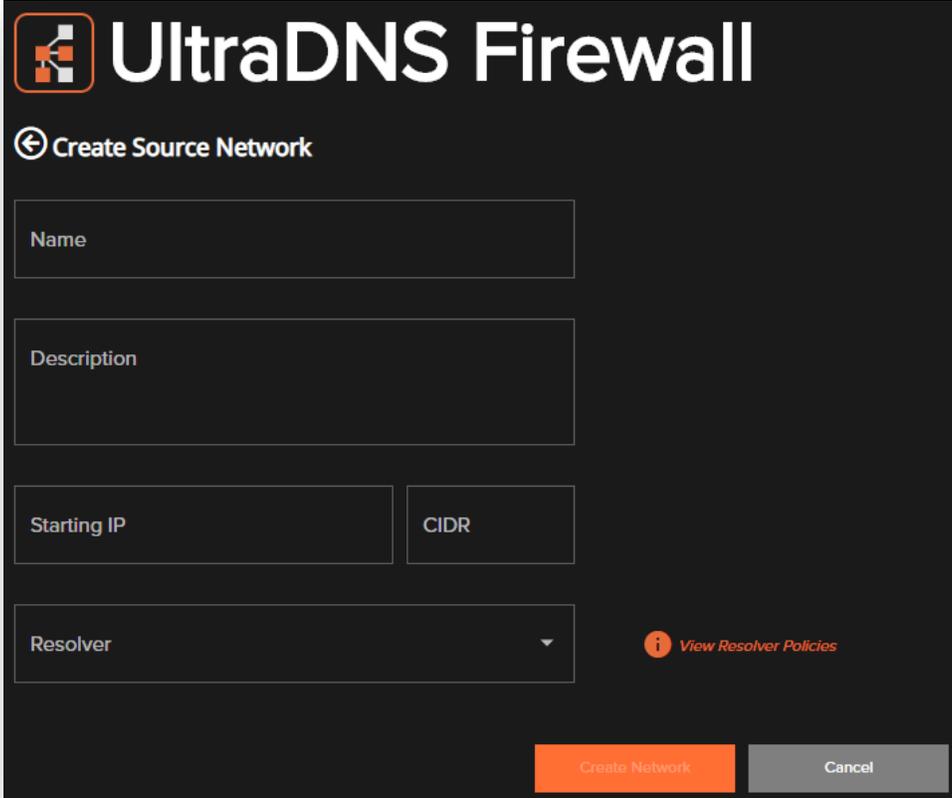
- The *Description* is an optional field, and will by default, display the date and time of creation unless details are provided.

If you have the admin role, you can also select a specific **VIP Resolver** from the drop-down menu.



If you are using an IPv4 address, the CIDR length can be between 13 – 32, while IPv6 address types will allow a CIDR length of 64 – 128.

If an illegal CIDR length type is provided, an error message will appear.



The screenshot shows the 'UltraDNS Firewall' interface with a 'Create Source Network' form. The form includes the following fields and elements:

- Name:** A text input field.
- Description:** A larger text input field.
- Starting IP:** A text input field.
- CIDR:** A text input field.
- Resolver:** A dropdown menu.
- View Resolver Policies:** A link with an information icon.
- Create Network:** An orange button.
- Cancel:** A grey button.

Figure 27 Configuration - Add Source Network Details

Editing a Subnet

Once your Source Network is created, you can hover over the Subnet details section and click the **pencil** icon that appears to open the edit screen. The Source Network details screen will appear.

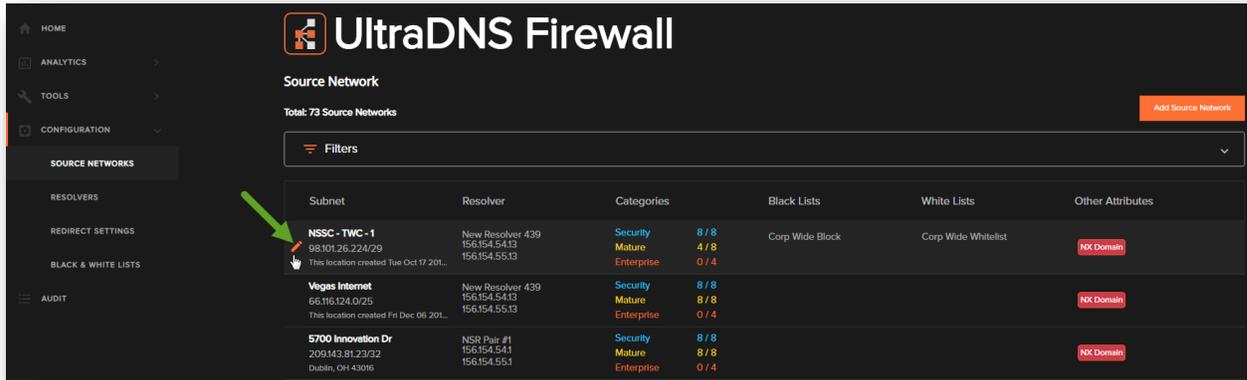


Figure 28 Configuration - Edit a Source Network

UltraDNS Firewall

Edit Source Network

Save Network

Basic Information

Name: 5700 Innovation Dr

Description: Dublin, OH 43016

Starting IP: 209.143.81.23 | CIDR: 32 | 1 IPs: 209.143.81.23 to 209.143.81.23

Resolver: NSR Pair #1 [View Resolver Policies](#)

Black / White Lists (Optional)

Black List: [Search] + White List: [Search] +

Other Properties

NXDomain - Non Existent Domain Redirection

Disabled Enabled [What's this?](#)

Delete Suspend Cancel Save And Continue To Filter Setup

Figure 29 Source Networks - Edit Source Network Details

Black / White Lists

To add a Black List or White List entry to your Source Network, it first must be configured in the *Black and White Lists* section under the **Configuration** menu.

Available Black Lists and White Lists can be selected by clicking into the search field (next to the Orange Plus icon), and then selecting the desired entry from the drop-down menu. Click the **+ (plus)** icon to add the selection to the associated List type above.

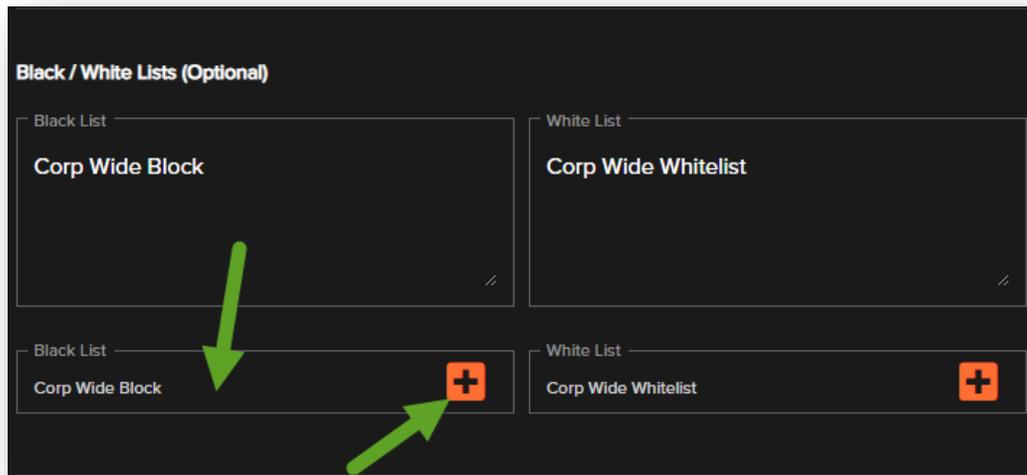


Figure 30 Source Networks - Black / White Lists Configuration

Other Properties

The Other Properties section contains the following two fields:

- **NX Domain** (Non Existent Domain Redirection) – When Enabled, if a domain name is not found, a special webpage with a message explaining that the lookup failed will be displayed, instead of the generic NXDomain return.
- **Monitor Only** – When this feature is enabled, filtering will be disabled so that only a diagnostic approach will be taken.



Figure 31 Source Networks - Other Properties Options

Category Filters

If you are editing the Source Network, click the **Save And Continue To Filter Setup** button to view the category filtering options.

The Category Filters allow you to set the blocking level for each category type available (Security, Mature, and Enterprise). Categories can be manually set to one of the following types:

- **Blocked** – All queries, received from the associated source network, that fall within this criterion, will be blocked.
- **Warned** – All queries received from the associated source network, that fall within this criterion, will get a warning.
- **Allow** – No action will be taken on queries that fall within this criterion.



Figure 32 Source Network - Category Filters

Clicking one of the options next to the Category type across the top will cause each sub-category below to inherit that filter type. For instance, if you click **Blocked** for Security, every Security sub-category will switch to Blocked.

If you opt to set each filter type individually and have a combination of the three filtering types, the Category section will be displayed as **Mixed**, instead of Blocked / Warned / Allow.

Click **Save Policy** when you are done making changes to the filters.

Suspend a Source Network

To suspend a Source Network from an account, click the **pencil icon** next to the desired Source Network name. Click the **Suspend** button, and then verify your action on the “Are You Sure” dialogue box.

A suspended Source Network will stop receiving traffic until it is Re-Activated.

Delete Source Networks

To delete a Source Network from an Account, click the **pencil icon** next to the desired Source Network Name. Click the **Delete** button, and then verify your action on the “Are You Sure” dialogue box.

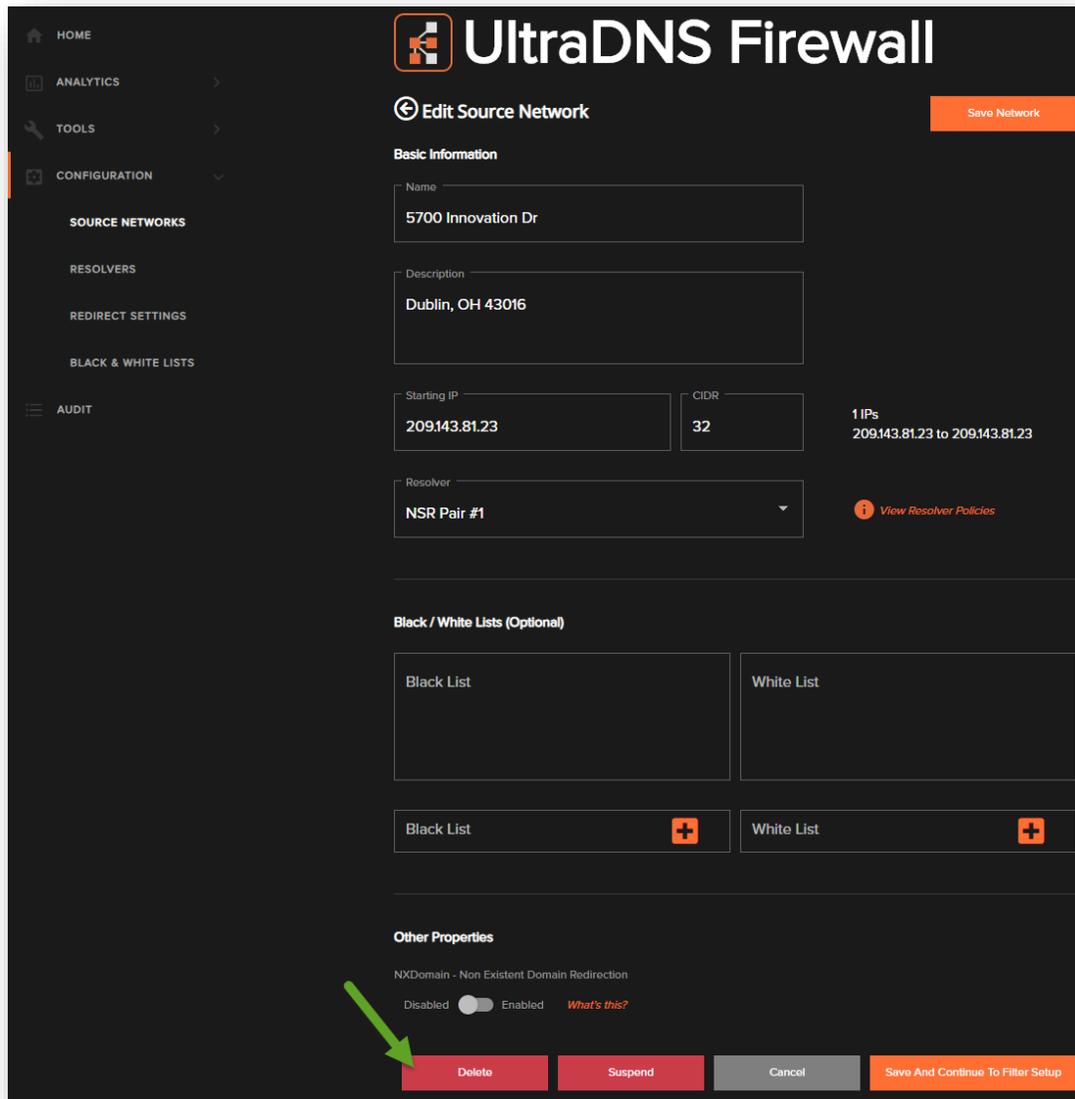


Figure 33 Configuration - Delete Source Network

Resolvers

Selecting the **Resolvers** option displays the current DNS Nameserver Pairs that are used to resolve domain names. The data being displayed are the *Virtual IP Addresses (VIPs)*, along with any policies, Blacklists and/or Whitelists that are assigned (which are used when creating subnets).

Before the Source Networks / Subnets can be configured, the Resolver and VIPs must be provided during your onboarding process. The management of the VIPs is maintained by a Neustar Administrator, even though you may see the pencil icon that traditionally allows you to edit the information in the cell.



The resolvers are configured by a Neustar Administrator during the customer onboarding process.

The screenshot shows the 'UltraDNS Firewall' interface. The left sidebar has a menu with 'RESOLVERS' highlighted by a green arrow. The main content area shows a table of resolvers with columns for Resolver, IPs, Categories, Black Lists, White Lists, and Other Attributes. There are three resolvers listed: NSR Pair #1, NSR IPv6 Pair #101, and New Resolver 439. Each row has a 'Policy Override' button.

| Resolver | IPs | Categories | Black Lists | White Lists | Other Attributes |
|---|--|--|-------------|-------------|---------------------------|
| NSR Pair #1 This nameserver pair created Tue F... | 156.154.54.1 156.154.55.1 | Security 0/8 Mature 0/8 Enterprise 0/4 | | | NX Domain Policy Override |
| NSR IPv6 Pair #101 This nameserver pair created Tue F... | 2610:A11018:0:0:0:0:65 2610:A11019:0:0:0:0:65 | Security 0/8 Mature 0/8 Enterprise 0/4 | | | NX Domain Policy Override |
| New Resolver 439 This Resolver created Mon Aug 28 2... | 156.154.54.13 156.154.55.13 | Security 0/8 Mature 0/8 Enterprise 0/4 | | | NX Domain Policy Override |

Figure 34 Configuration - Resolvers

The Resolver details are displayed as follows:

- **Resolver** - The Resolver column displays the Nameserver Pair along with the description data provided at the time of creation (default data includes creation date and time).
- **IPs** – Lists the IPs or the range of IPs associated to the Nameserver Pair.
- **Categories** - The Category Filter section displays the security/filtering information for the Nameserver pair. Filters include *block*, *warn*, and *off*.
- **Black Lists** – Displays all Blacklist filters that are assigned to the Nameserver pair. Filters include *block* (enabled), and *off*.
- **White Lists** - Displays all Whitelist filters that are assigned to the Nameserver pair. Filters include *pass* (allowed), and *off*.
- **Other Attributes** – Designates where users will be routed if there is an error finding the domain name, or if the domain name is not found.

Edit a Resolver

Once a Resolver has been created, you can click the **pencil** icon to edit the Resolver details. Additionally, this where you can edit the **Other Properties** options.

Account type users with the Admin role can edit the following fields:

- **Name**
- **Description**
- **Policy Override** – Enable or Disable

- Enabling the Policy Override feature allows policies on your subnets to override the existing policy on the resolver.

UltraDNS Firewall

← Edit Resolvers Save Resolver

Basic Information

Name
TEST_DO_NOT_DELETE_VIP

Description
This is used by end to end script View Resolvers

Other Properties

Policy Override
Disabled Enabled [What's this?](#)

Cancel

Figure 35 Configuration - Resolver - Edit Resolver Details

To edit any of the additional fields of a Resolver, requires a Sponsor with the Admin role.

Redirect Settings

The Redirect Settings section allows you to customize the landing page that users are redirected to when they attempt to access a webpage(s) that has been blacklisted, or that contains content that has been blocked due to filtering options.

The Redirect Settings customization(s) can be set at the account level by using the drop-down menu under “**in account**” at the top of the screen.

Each section provides the option to either have Neustar Manage the feature, provide a Custom Message, or Customer Managed.

CPIP

The Redirect Settings section will (depending on your configuration) display an option for Capture Private IP (CPIP). Additional details for how to enable and utilize the CPIP function can be found in the **Capture Private IP Data User Guide**.

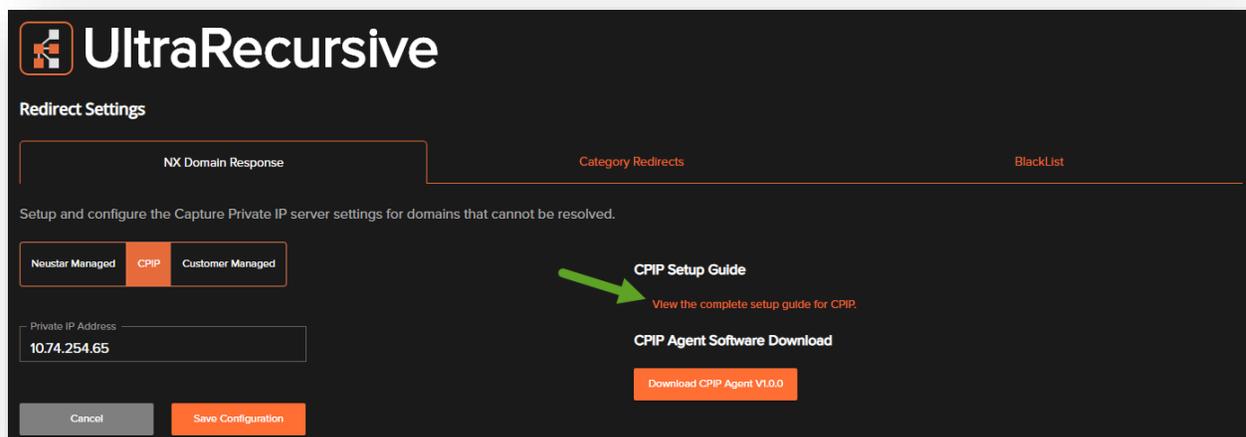


Figure 36 CPIP Setup Guide

The different options within Direct Settings are:

- *NX Domain Response*
- *Category Redirects*
- *Blacklist*

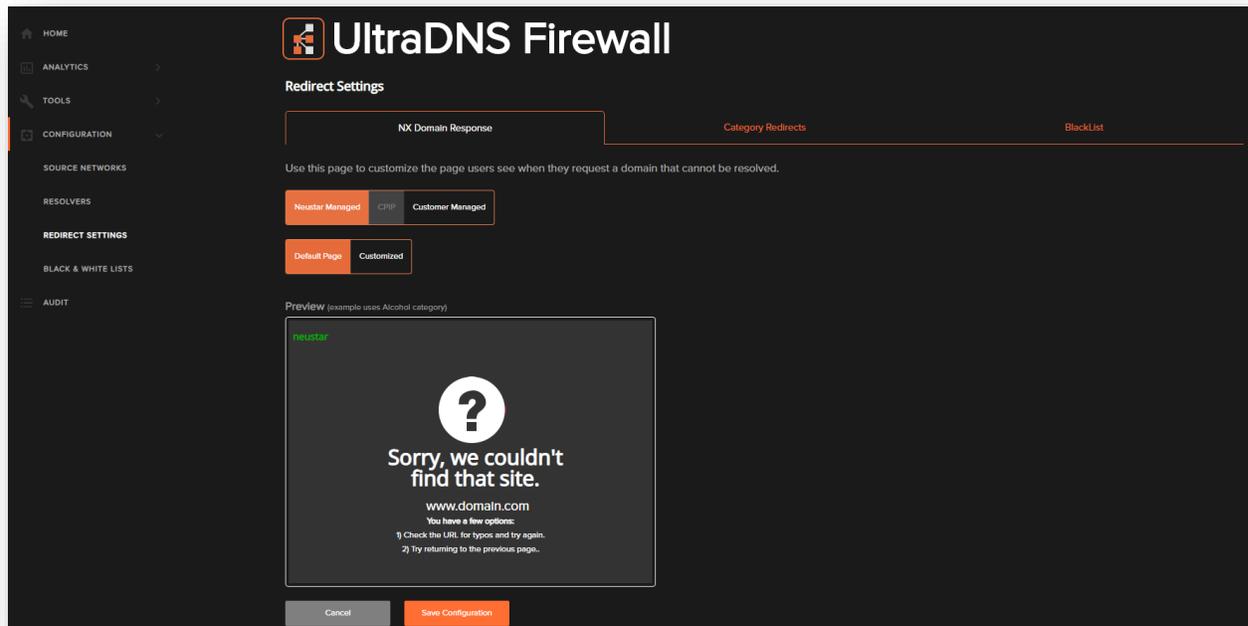


Figure 37 Redirect Settings - Landing Page

NX Domain Response

NX Domain Response allows you to customize the landing page that users are redirected to when they attempt to access a domain that does not exist. There are two methods in which you can manage the NX Domain Response details.

Neustar Managed

Selecting the **Neustar Managed** option provides you with an example of what your generic landing page will look like.

- **Default Page** – Displays the Company's logo in the upper left-hand corner, along with the default message "Sorry, we couldn't find that site."

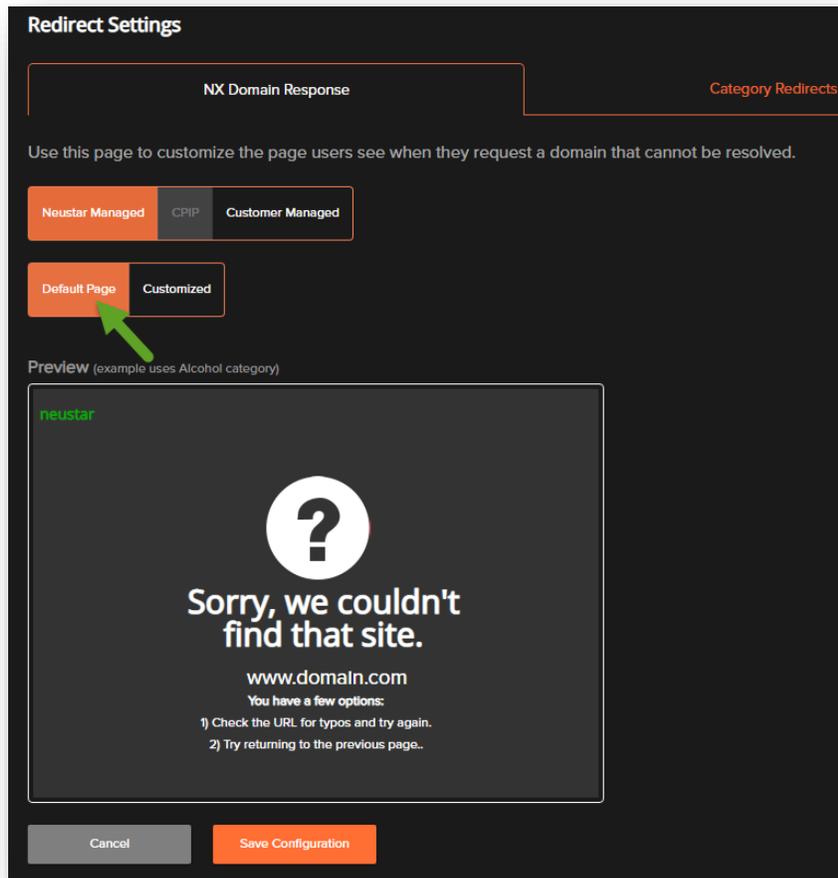


Figure 38 Redirect Settings - NX Domain Response – Neustar Managed

- **Customized** – Allows you to upload a custom image for the landing page.

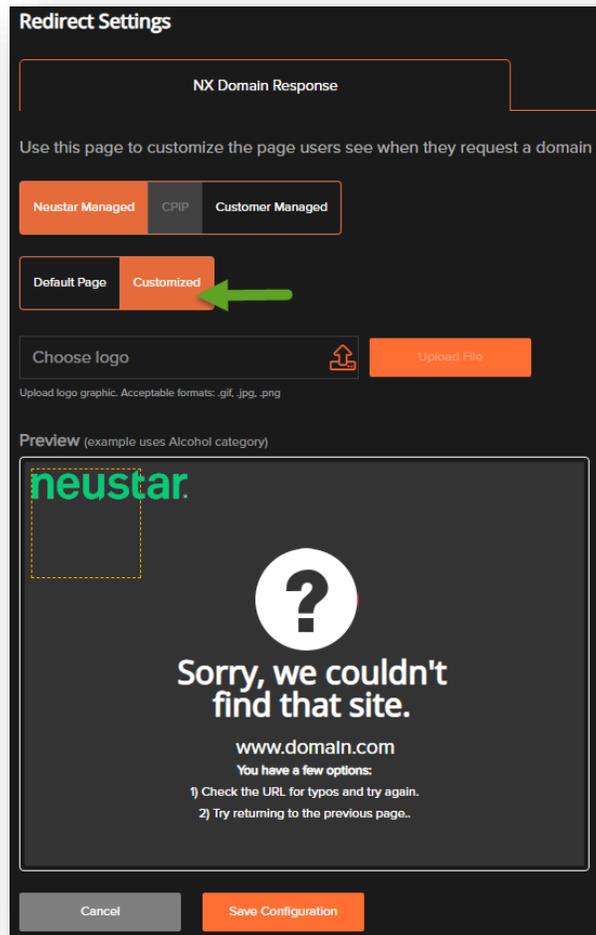


Figure 39 Redirect Settings - NX Domain - Neustar Managed - Customized

Customer Managed

Selecting the **Customer Managed** option allows you to dictate where to direct a user to, instead of providing the default error message and screen. Provide an IP address for the website you will direct users to and then click **Save Configuration**.

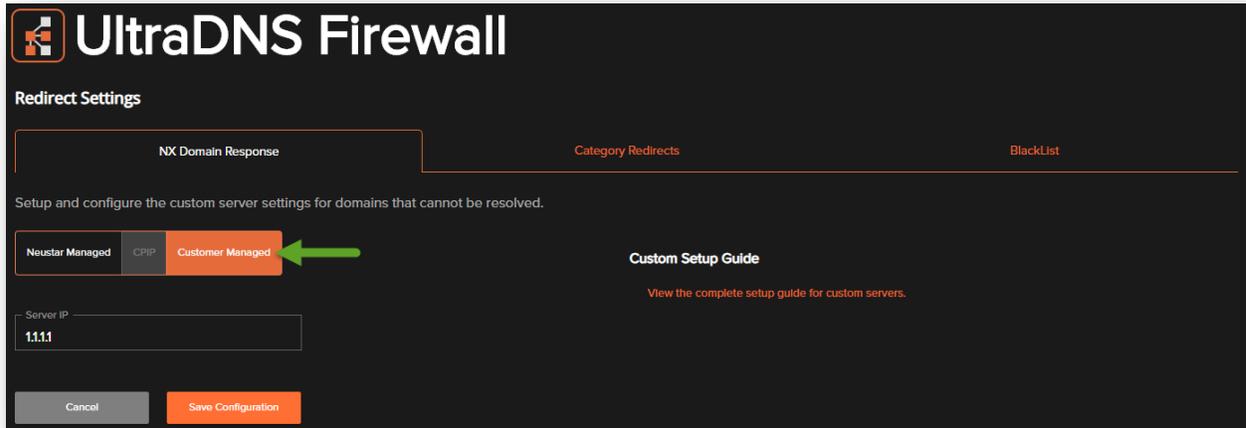


Figure 40 NX Domain Response – Customer Managed

Category Redirects

Category Redirects allows you to determine the warning/error message page that is displayed when users attempt to access a domain that matches a redirect category (Category Filter options). There are two ways in which you can manage the Category Redirects.

Neustar Managed

Selecting the **Neustar Managed** option displays an example of what your generic landing page will look like.

- **Default Page** – Displays your Company's logo in the upper left-hand corner, along with the default message "Site Blocked", and a short explanation as to what filter category the website is violating.

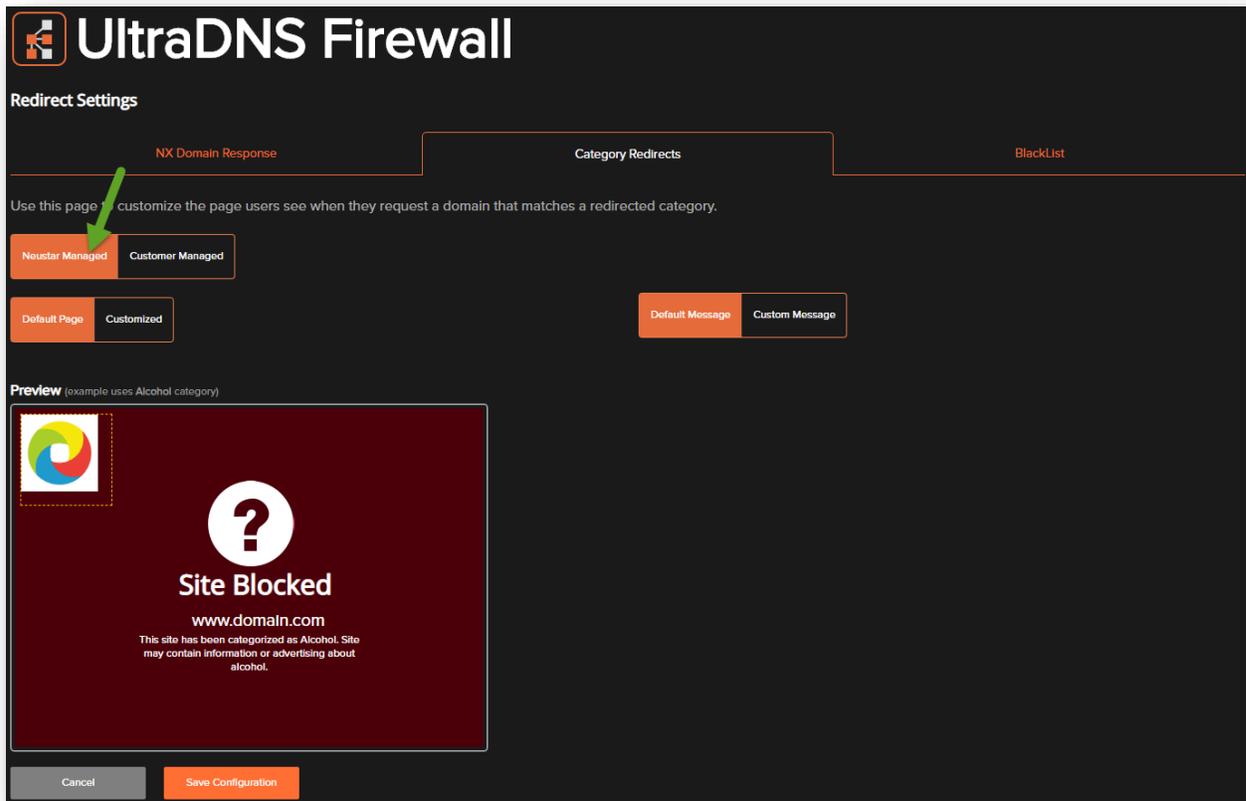


Figure 41 Redirect Settings – Category Redirects – Neustar Managed - Default

- **Customized** – Selecting the **Customized** option allows you to upload a custom image for the landing page.

Redirect Settings

NX Domain Response | **Category Redirects**

Use this page to customize the page users see when they request a domain that matches a redirected category.

Neustar Managed | **Customer Managed**

Default Page | **Customized** ← | **Default Message** | **Custom Message**

Choose logo

Choose a file in .jpg, .png or .gif format. Max size 200x200 pixels

Email address or URL

Preview (example uses Alcohol category)



?
Site Blocked
www.domain.com
This site has been categorized as Alcohol. Site may contain information or advertising about alcohol.

Figure 42 Category Redirects - Neustar Managed – Customized

The next option when configuring the Redirect Settings is to establish the message that will be displayed when a Category Redirect page is displayed.

- **Default Message** – Selecting the Default Message will display the neustar default content that is applied to every category type.

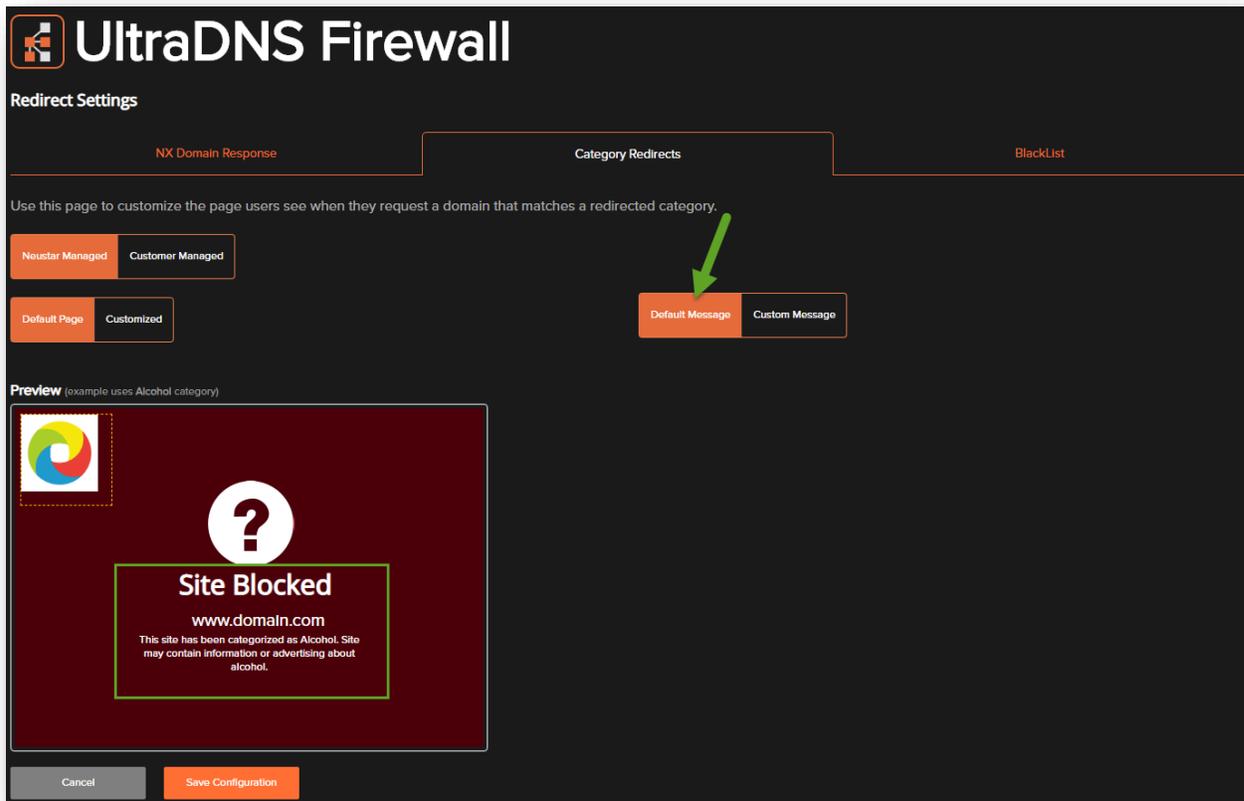


Figure 43 Redirect Settings - Category Redirects - Default Message

- **Custom** – Selecting Custom Message allows you to select the specific category type, and provide a **Message Heading** and a specific **Redirect Message** that will be displayed to users. Click **Save Configuration** when you are done.
 - You can provide custom headers and messages for each category type in the list. When you save a custom message per category type, the circle will become filled, showing you each category you have customized.

Redirect Settings

NX Domain Response | **Category Redirects** | **BlackList**

Use this page to customize the page users see when they request a domain that matches a redirected category.

Neustar Managed | **Customer Managed**

Default Page | **Customized**

Default Message | **Custom Message**

Preview (example uses Anonymous Proxies category)

Security | **Mature** | **Enterprise**

- Malware
- Phishing
- Anonymous Proxies**
- Spyware
- Parked Domains
- Hacking/Warez/P2P
- Ransomware
- Bots/C2

- Adult
- Gambling
- Pornography
- Violence
- Dating
- Drugs
- Alcohol
- Discrimination/Hate

- Gaming
- Social
- Sports
- Custom Category

Message Heading

Heading that shows above the message.

Message

Message to display to users.

Cancel | **Save Configuration**

Figure 44 Redirect Settings – Category Redirects - Custom Message

Customer Managed

Selecting the **Customer Managed** option allows you to provide an IP address that users will be directed to when they attempt to query a domain that either falls under the Blocked or Warned category filter settings.

Once you have made your selections, click the **Save Configuration** button.

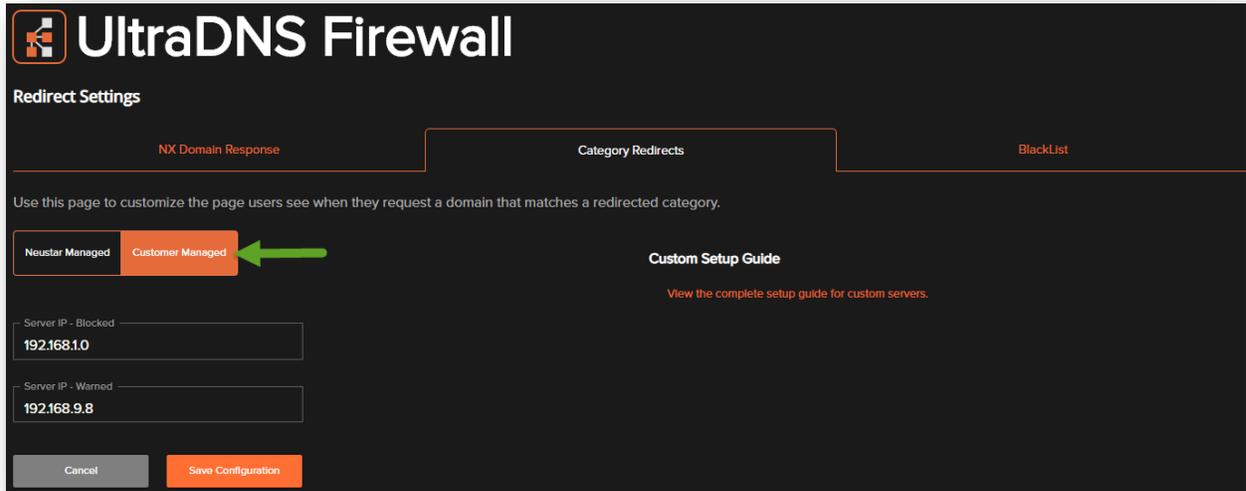


Figure 45 Redirect Settings – Category Redirects - Host Your Own

Blacklist

Blacklist allows you to customize the landing page that users are redirected to when they attempt to access a domain that is blocked due to Blacklist settings.

Neustar Managed

Selecting the **Neustar Managed Default** option provides you with an example of what your generic landing page will look like.

- **Default Page** – Selecting the Default Page option displays your Company’s logo in the upper left hand side, and a generic “Site Blocked” message with an explanation stating that the website is blacklisted.

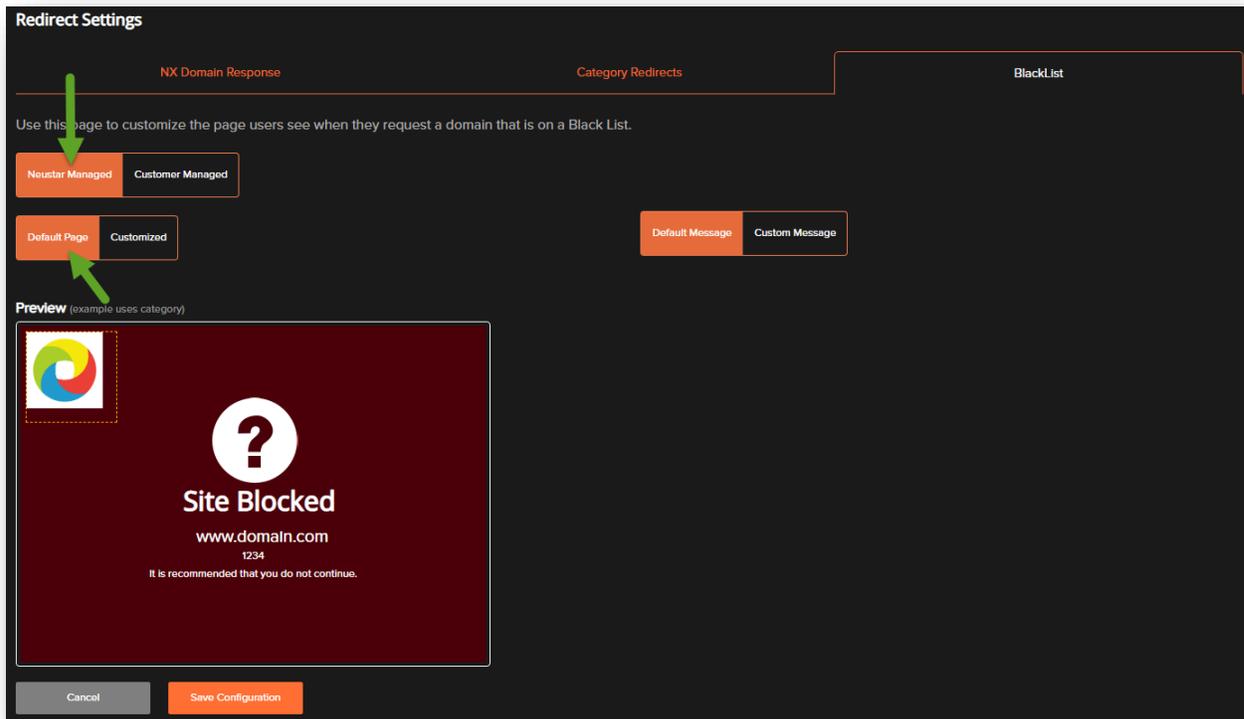


Figure 46 Redirect Settings – Blacklist – Neustar Managed – Default

- **Customized** - Selecting the **Customized** option allows you to upload a custom image for the landing page.

Redirect Settings

NX Domain Response Category Redirects **BlackList**

Use this page to customize the page users see when they request a domain that is on a Black List.

Neustar Managed Customer Managed

Default Page **Customized** Default Message Custom Message

Choose logo Upload File

Choose a file in .jpg, .png or .gif format. Max size 200x200 pixels

Email address or URL
google@google.com

Preview (example uses category)

Site Blocked
www.domain.com
1234
It is recommended that you do not continue.

Cancel Save Configuration

Figure 47 Redirect Settings – Blacklist – Neustar Managed – Customized

The next option when configuring the Redirect Settings is to establish the message that will be displayed when a BlackList page is displayed.

- **Default Message** – Selecting the Default Message will display the neustar default content that is applied to for queries that are Blacklisted.

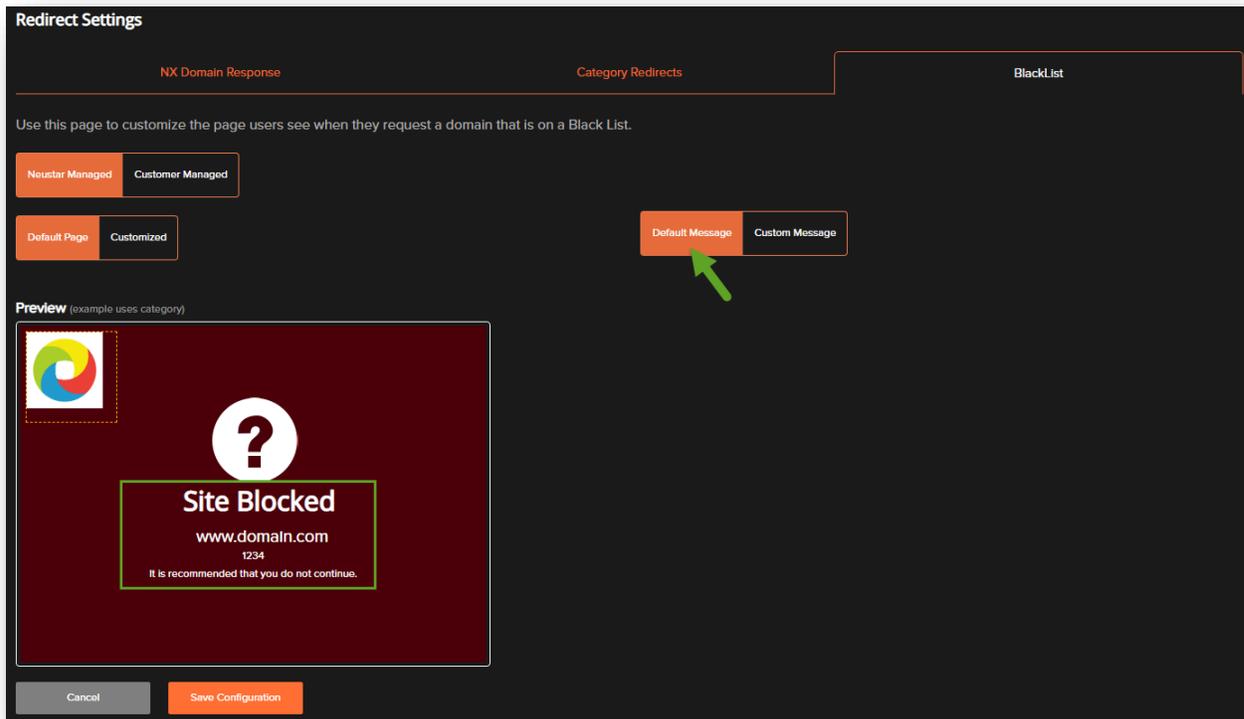


Figure 48 Redirect Settings - BlackList - Default Message

- **Custom Message** – Selecting Custom Message allows you to provide a specific message/label that will be displayed to users when they are redirected due to Blacklisting.

Redirect Settings

NX Domain Response Category Redirects **BlackList**

Use this page to customize the page users see when they request a domain that is on a Black List.

Neustar Managed **Customer Managed**

Default Page **Customized**

Default Message **Custom Message**

Label
1234

A message users will see when they attempt to access a black listed site.

Preview (example uses category)

Site Blocked
www.domain.com
1234
It is recommended that you do not continue.

Cancel **Save Configuration**

Figure 49 Redirect Settings - Blacklist – Customized Message

Customer Managed

Selecting **Customer Managed** option allows you to provide the IP address for the webpage that you want users to be redirected to when trying to navigate to a page that is restricted by the current blacklist settings.

Click **Save Configuration** after you have provided the IP address.

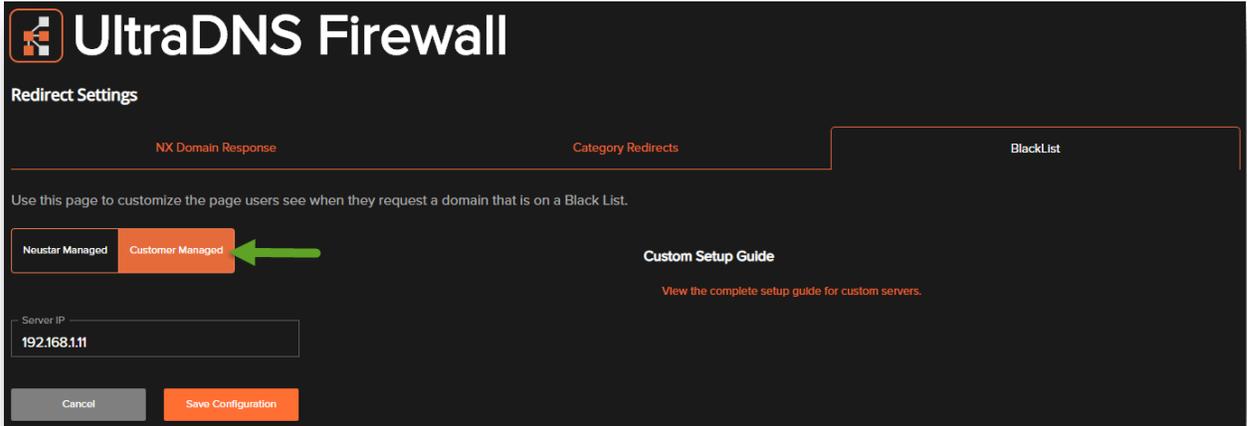


Figure 50 Redirect Settings - Blacklist – Customer Managed

Black and White Lists

The Black & White list section allows you to provide specific domains name that will either be blocked if traffic attempts are pointed towards it, or allowed through. *Black & White List features can be created at the Sponsor level, or for specified sub-accounts.*

| List Names | Count | Domains |
|--------------------|-------|--|
| New Blacklist 508 | 2 | example.com, www.example2.com |
| New Blacklist 848 | 1 | for.com |
| New Blacklist 968 | 2 | example.com, www.example.com |
| Avira | 4 | avira.com, test.com, testf.com, www.avira.com |
| Testing Blacklist | 1 | cnn.com |
| TomTest | 4 | tdjohnson.com, tdjohnson.net, www.clubug.com, www.minnstate.edu |
| New Blacklist 756 | 2 | example.com, www.example.com |
| New Blacklist 957- | 2 | facebook.com, messenger.com |
| New Blacklist 279 | 6 | 09135.com, 3813866.com, carce.cc, www.carce.cc, www.cnyes.com, www.js88811.com |
| New Blacklist 102- | 2 | www.youtube.com, youtube.com |

Figure 51 Configuration - Black & White Lists

Create Black Lists

To create a new Black List for an account, click the **Black Lists** tab, and then choose your creation method.

- **Add** – Manually enter the URLs that you wish to block traffic for.
- **Import Black List** – Upload a .CSV file of the various URLs you wish to block traffic for.

Import Blacklist

An additional way to add Blacklist details is to use the **Import** option. Click the **Import** button, and then select whether you want to *Append* (edit) or *Replace* the current Blacklist details for the account.

Click the **Choose File** button, and then select your .csv file. Once you select the file, click the **OK** button. The UltraDNS Firewall Portal will process your import request, and if the format is correct, your Blacklist will be populated with your provided details.

The format for your .csv file should match the following template example, with your first column being

labeled **Blacklist**, and your second column labeled **Domains**.

| | A | B |
|----|-------------------|-------------------|
| 1 | Blacklist | Domains |
| 2 | Black List Subnet | cnn.com |
| 3 | Black List Subnet | nbcnews.com |
| 4 | Black List Subnet | googleaa.xyz |
| 5 | Black List VIP1 | example.com |
| 6 | Black List VIP1 | www.google.com |
| 7 | Black List VIP1 | example.com |
| 8 | Black List VIP2 | amerisave.com |
| 9 | Black List VIP2 | bankofamerica.com |
| 10 | Black List VIP2 | amerisave.com |
| 11 | Deepti blacklist | demo.com |
| 12 | | |

Figure 52 Configuration - Import Blacklist .CSV Template

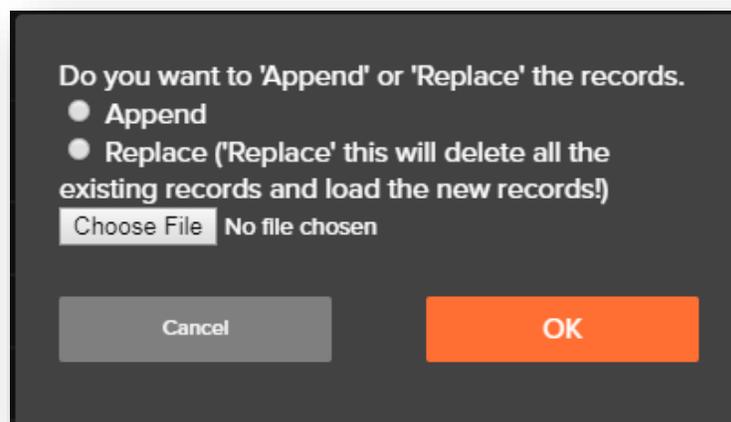


Figure 53 Configuration - Black List - Import Confirmation

Export Blacklist

To export your Blacklist details, click the **Export Black List** button. A .csv file will automatically download to your device. The exported Black List .csv file contains two columns: the first displaying the Black List name, and the second displays the domains associated to the Black List name.

Edit Blacklist

To edit the **Black Lists** page, click on the **pencil** icon that appears when you hover over a Blacklist entry.

UltraDNS Firewall

Black & White Lists

Black Lists White Lists

Create Black Lists to redirect any lookups to specific domains not filtered by category redirects.

Add Export Black List Import Black List

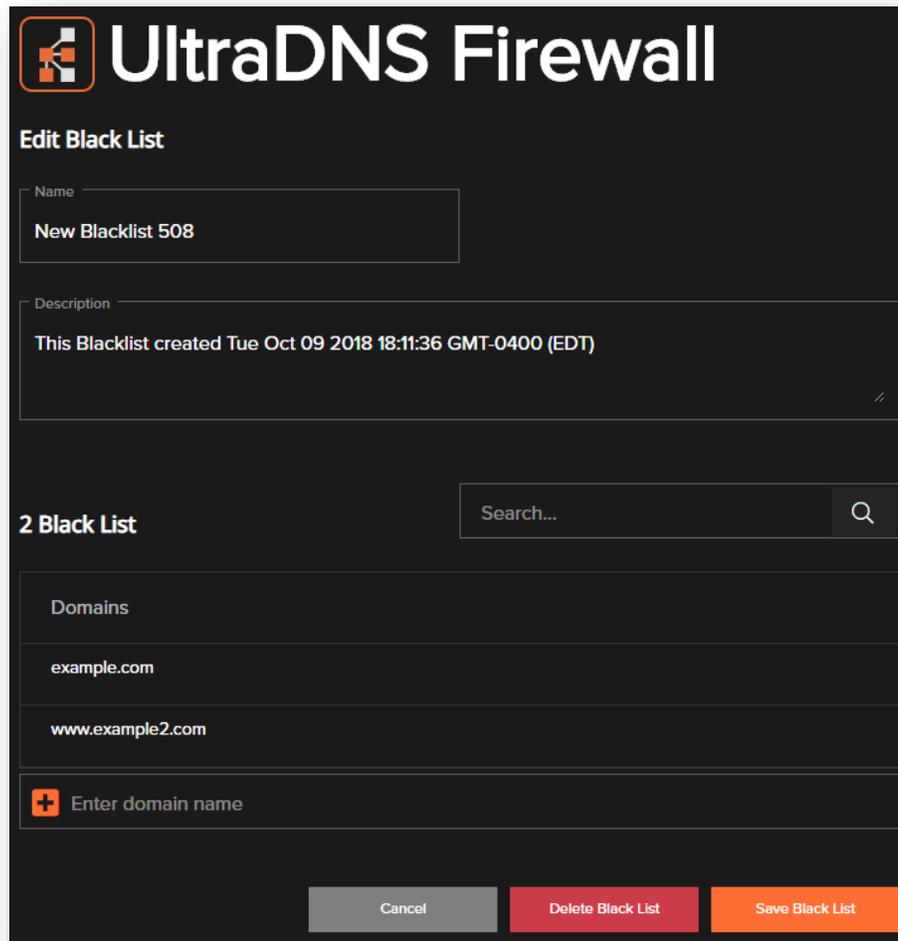
Filters

| List Names | Count | Domains |
|--------------------|-------|--|
| New Blacklist 508 | 2 | example.com, www.example2.com |
| New Blacklist 848 | 1 | tor.com |
| New Blacklist 368 | 2 | example.com, www.example.com |
| Avira | 4 | avira.com, test.com, test1.com, www.avira.com |
| Testing Blacklist | 1 | cnn.com |
| TomTest | 4 | tdjohnson.com, tdjohnson.net, www.clubtug.com, www.minnstate.edu |
| New Blacklist 756 | 2 | example.com, www.example.com |
| New Blacklist 957- | 2 | facebook.com, messenger.com |
| New Blacklist 279 | 6 | 091335.com, 3813856.com, carce.cc, www.carce.cc, www.cnyes.com, www.js888f11.com |
| New Blacklist 102- | 2 | www.youtube.com, youtube.com |

Items per page: 10 1 - 10 of 30

Figure 54 Black & White Lists - Edit Black List

When editing the Blacklist details, you can change the *Name* and the *Description*, and then add or remove additional Black List entries. Click the **Save Black List** button when you are done making changes.



UltraDNS Firewall

Edit Black List

Name
New Blacklist 508

Description
This Blacklist created Tue Oct 09 2018 18:11:36 GMT-0400 (EDT)

2 Black List

Domains

- example.com
- www.example2.com

+ Enter domain name

Cancel Delete Black List Save Black List

Figure 55 Black & White Lists - Edit Black List Details



Advanced Tip for editing multiple Black List entries:

Export your Blacklist items, update the .csv file with your changes, and then re-import and select the **Append** option, rather than manually editing several Blacklist entries.

Delete Black Lists

To delete a Black List entry, click the **pencil** icon in the Black List cell you want to delete, and then click the **Delete Black List** button. Confirm your action by clicking on the **Are You Sure** button that appears (scroll down if the message does not appear) to finalize the deletion.

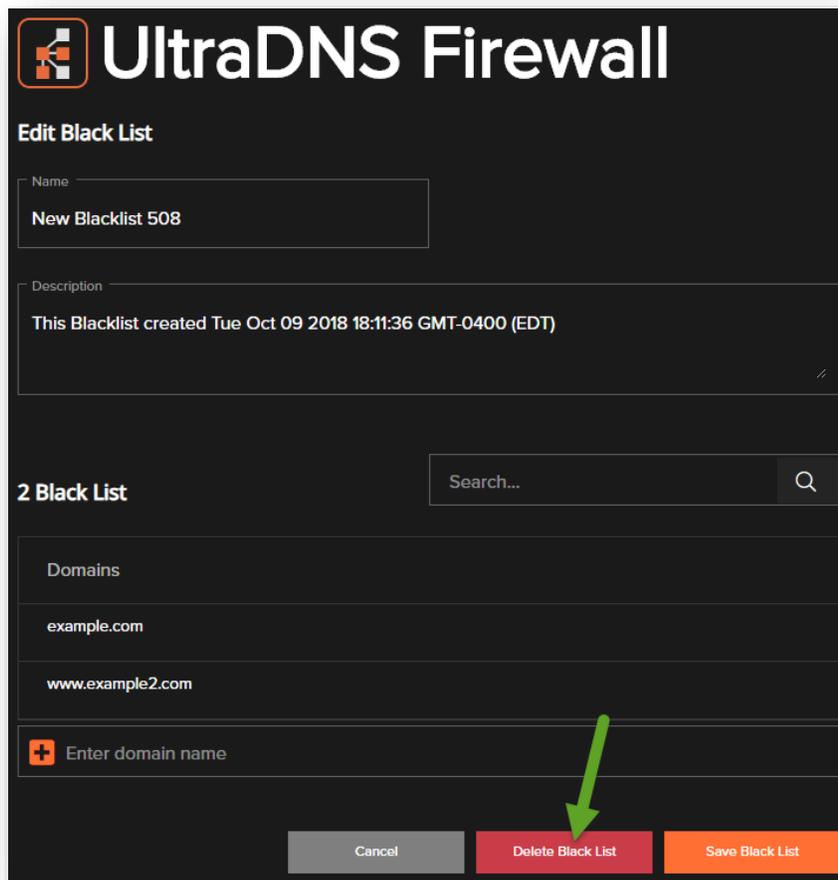
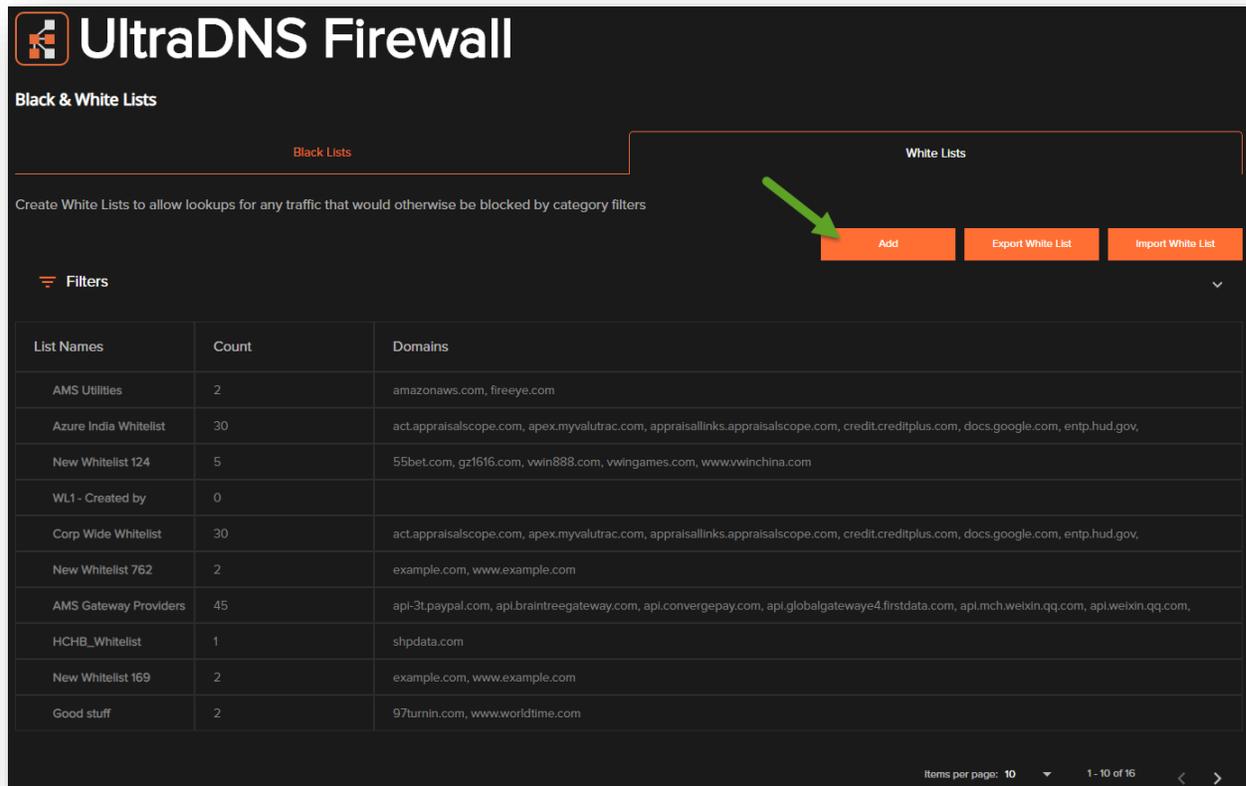


Figure 56 Black & White Lists - Delete Black List

Create Whitelist

To create a new Whitelist entry for an account, select the White List tab and then click the **Add** button.



UltraDNS Firewall

Black & White Lists

Black Lists | **White Lists**

Create White Lists to allow lookups for any traffic that would otherwise be blocked by category filters

Filters

Add | **Export White List** | **Import White List**

| List Names | Count | Domains |
|-----------------------|-------|--|
| AMS Utilities | 2 | amazonaws.com, freeeye.com |
| Azure India Whitelist | 30 | act.appraisalscope.com, apex.myvalutrac.com, appraisallinks.appraisalscope.com, credit.creditplus.com, docs.google.com, entp.hud.gov, |
| New Whitelist 124 | 5 | 55bet.com, gz1616.com, vwin888.com, vwingames.com, www.winchina.com |
| WL1 - Created by | 0 | |
| Corp Wide Whitelist | 30 | act.appraisalscope.com, apex.myvalutrac.com, appraisallinks.appraisalscope.com, credit.creditplus.com, docs.google.com, entp.hud.gov, |
| New Whitelist 762 | 2 | example.com, www.example.com |
| AMS Gateway Providers | 45 | api-3l.paypal.com, api.braintreeregateway.com, api.convergepay.com, api.globalgatewaye4.firstdata.com, api.mch.weixin.qq.com, api.weixin.qq.com, |
| HCHB_Whitelist | 1 | shpdata.com |
| New Whitelist 169 | 2 | example.com, www.example.com |
| Good stuff | 2 | 97turnin.com, www.worldtime.com |

Items per page: 10 | 1 - 10 of 16

Figure 57 Black & White Lists - Add a White List

Import White List

An additional way to add Whitelist details is to use the **Import** option. Click the **Import White List** button, and then select whether you want to *Append* (edit) or *Replace* the current Whitelist details for the account.

Click the **Choose File** button, and then select your .csv file. Once you select the file, click the **OK** button. The UltraDNS Firewall Portal will process your import request, and if the format is correct, your Whitelist will be populated with your provided details.

The format for your .csv file should match the following template example, with your first column being labeled **Whitelist**, and your second column labeled **Domains**.

| | A | B |
|----|-------------------|-------------------|
| 1 | Whitelist | Domains |
| 2 | White List Subnet | cnn.com |
| 3 | White List Subnet | nbcnews.com |
| 4 | White List Subnet | googleaa.xyz |
| 5 | White List VIP1 | example.com |
| 6 | White List VIP1 | www.google.com |
| 7 | White List VIP1 | example.com |
| 8 | White List VIP2 | amerisave.com |
| 9 | White List VIP2 | bankofamerica.com |
| 10 | White List VIP2 | amerisave.com |
| 11 | Deepti Whitelist | demo.com |
| 12 | | |

Figure 58 Configuration - Import White List .CSV Template

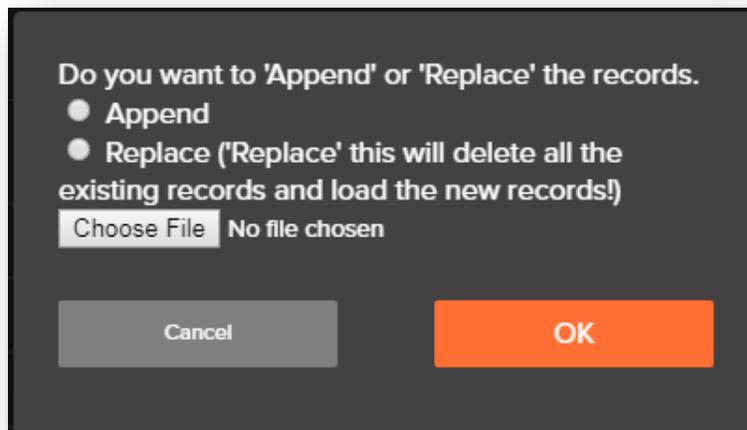


Figure 59 Configuration - White List - Import Confirmation

Export White List

To export your Whitelist details, click the **Export** button. A .csv file will automatically download to your device. The exported White List .csv file contains two columns: the first displaying the Whitelist name, and the second displays the domains associated to the Whitelist name.

Edit White List

To edit the **Whitelists** column, click on the **pencil** icon that appears when you hover over a Whitelist entry.

UltraDNS Firewall

Black & White Lists

Black Lists | White Lists

Create White Lists to allow lookups for any traffic that would otherwise be blocked by category filters

Filters

| List Names | Count | Domains |
|-----------------------|-------|--|
| AMS Utilities | 2 | amazonaws.com, fireeye.com |
| Azure India Whitelist | 30 | act.appraisalscope.com, apex.myvalutrac.com, appraisallinks.appraisalscope.com, credit.creditplus.com, docs.google.com, entp.hud.gov, |
| New Whitelist 124 | 5 | 55bet.com, gz1616.com, vwin888.com, vwingames.com, www.winchina.com |
| WL1 - Created by | 0 | |
| Corp Wide Whitelist | 30 | act.appraisalscope.com, apex.myvalutrac.com, appraisallinks.appraisalscope.com, credit.creditplus.com, docs.google.com, entp.hud.gov, |
| New Whitelist 762 | 2 | example.com, www.example.com |
| AMS Gateway Providers | 45 | api-3t.paypal.com, api.braintreegateway.com, api.convergepay.com, api.globalgatewaye4.firstdata.com, api.mch.weixin.qq.com, api.weixin.qq.com, |
| HCHB_Whitelist | 1 | shpdata.com |
| New Whitelist 169 | 2 | example.com, www.example.com |
| Good stuff | 2 | 97turnin.com, www.worldtime.com |

Items per page: 10 | 1 - 10 of 16

Figure 60 White Lists - Edit White List

When editing the White list details, you can change the *Name* of the White List, the *Description*, as well as Add or Remove White List entries to the list by clicking 'X' next to an entry.

When you are done making changes, click the **Save White List** button.



Advanced Tip for editing multiple Whitelist entries:

Export your Whitelist items, update the .csv file with your changes, and then re-import and select the **Append** option, rather than manually editing several Whitelist entries.

Delete Whitelist

To delete a Whitelist, click the **pencil** icon in the Whitelist cell you want to delete, and then click the **Delete White List** button.

UltraDNS Firewall

Edit White List

Name:

Description:

5 White List

Search...

| Domains |
|------------------|
| 55bet.com |
| gz1616.com |
| wwin888.com |
| wwingames.com |
| www.winchina.com |

Figure 61 White Lists - Delete White List

Status

The Service Status Dashboard displays the current service availability (1) for the various Neustar UltraDNS service offerings. Click on the link provided (<https://status.ultradns.neustar/>) to be directed to the UltraDNS System Status page, which is continuously updated with the most current information for service availability.

Upcoming Events

The bottom portion of the Service Status page displays any planned (2) upcoming events, or any advisories that users should be aware of that could impact accessibility to the portal, or specific services.

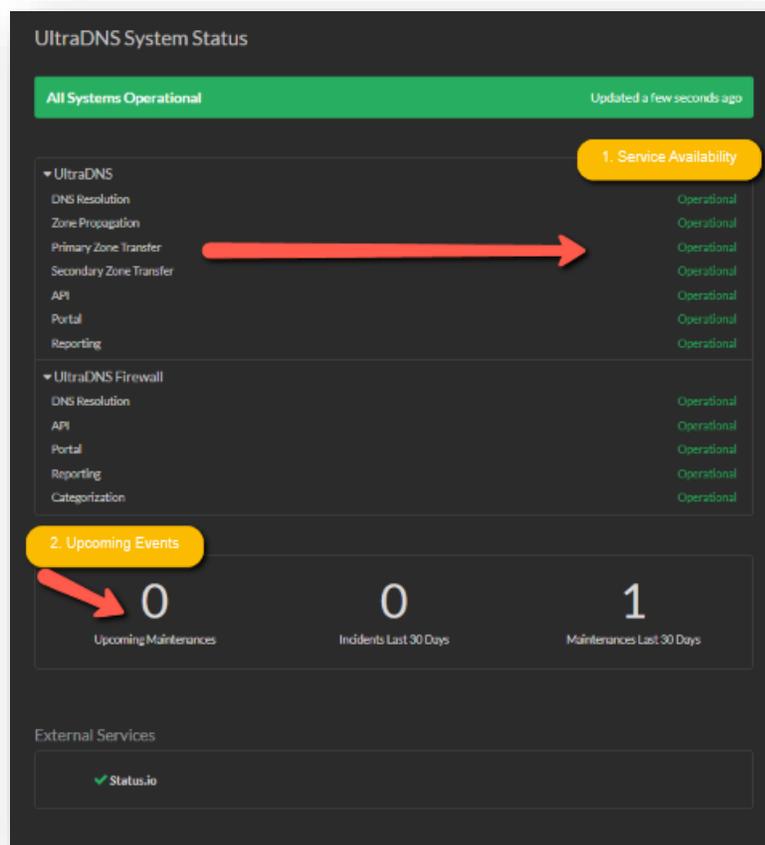
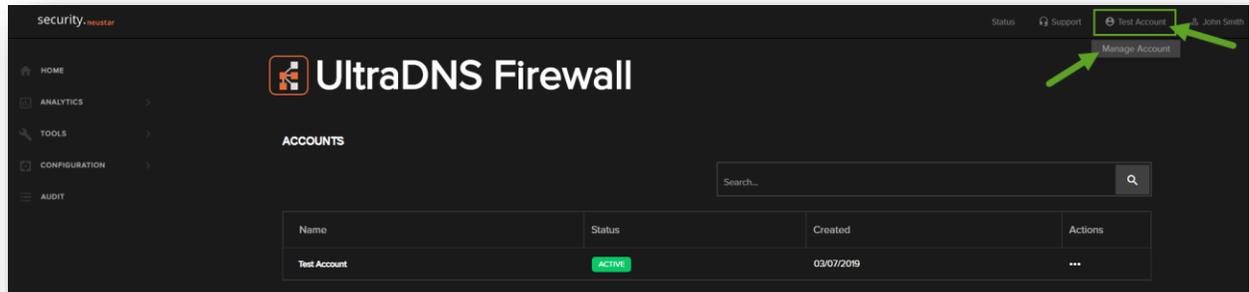


Figure 62 Service Status

Manage Account

Administrator Role Only

To manage your account details, click on the Account Name at the top of your screen, and then click **Manage Account**.

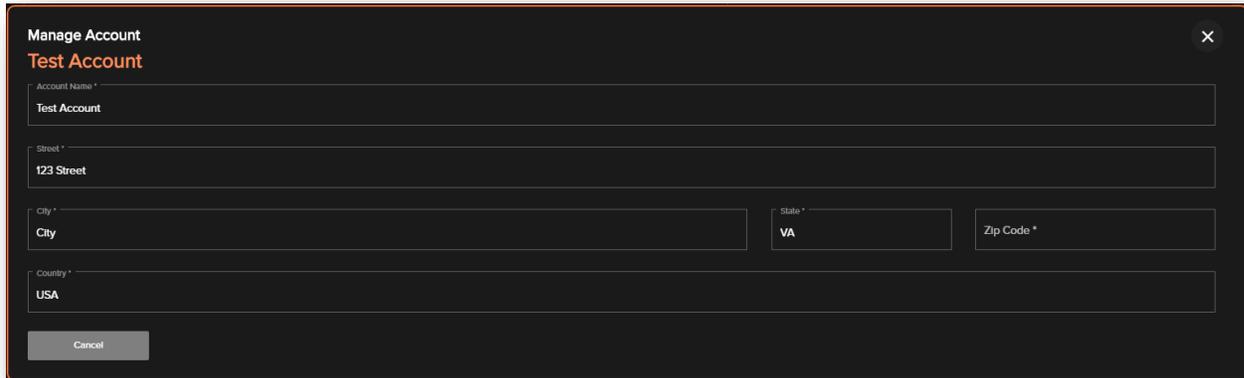


The Manage Accounts section displays:

- **Account Name**
- **Account Status** – Active or Suspended
- **Created Date**
- **Actions** – Click ellipsis to access the additional account management options.
 - **Manage Users**
 - **Manage Account**

Manage Account

To view the Account details hover over the account information, click on the ellipsis to the right-hand side, and then click **Manage Account**. As an Account type, you can see the details for the account but are prevented from making any changes.



The screenshot shows a 'Manage Account' dialog box with a dark background. At the top left, it says 'Manage Account' and 'Test Account' in orange. Below this are several input fields: 'Account Name *' with 'Test Account', 'Street *' with '123 Street', 'City *' with 'City', 'State *' with 'VA', 'Zip Code *', and 'Country *' with 'USA'. A 'Cancel' button is at the bottom left. A close button (X) is at the top right.

Figure 63 Manage Account - View Account Details

Delete an Account

An Account can only be deleted at the Sponsor level, or by a Neustar Administrator.

Manage Users

For users with the Admin role, the Manage Users section displays all of the current users associated to the Account. Each user's details are displayed as follows:

- **First Name**
- **Last Name**
- **Username**
- **Role**
- **Account Status**

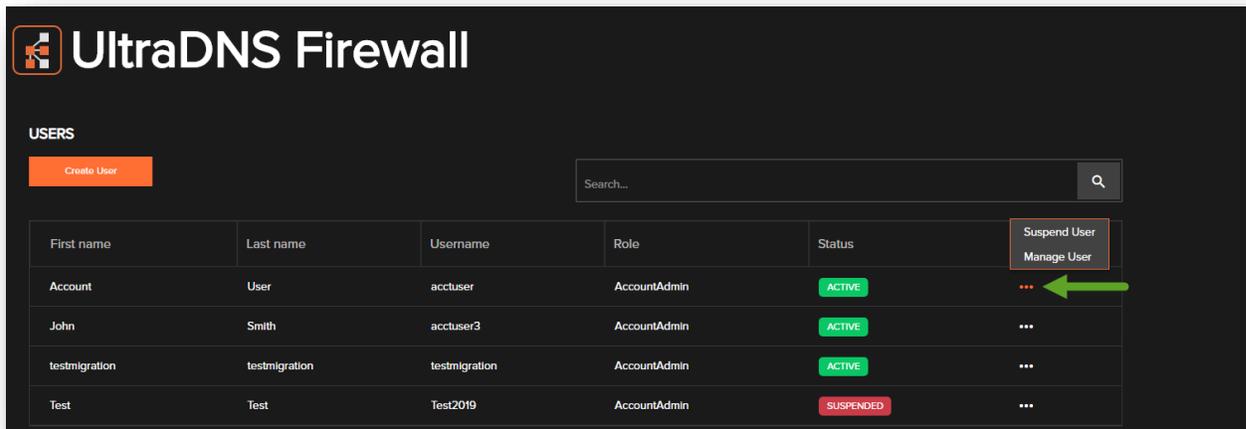


Figure 64 Manage Account - Manager Users

Create User

To create a new User, click the **Create User** button. The user name and email address must be unique, meaning, they cannot already be registered in the system.

Passwords:

- Between 8 and 32 characters
- At least one uppercase character
- At least one lowercase character
- At least one number
 - Special characters are allowed.

Note: The password cannot be the same as the username.

Click **Save** when finished. The new user will appear in the Users list on the *Manage Users* section.



The screenshot shows a 'Create User' form with the following fields:

- Username *
- Password
- Confirm password
- First name *
- Last name *
- Email *
- Phone *
- Role *

A 'Cancel' button is located at the bottom of the form.

Figure 65 Manage Users – Create New User

Manage User

To edit a user's account details, click on the ellipsis icon for the user, and then select **Manage User**.

You can update the following details:

- Username
- Password
- First and Last Name
- Email Address
- Phone Number
- Role

Once you are done making changes, click **Save**.



Manage User

Account User

Username *

acctuser

Password

Confirm password

First name *

Account

Last name *

User

Email *

aasima.khan@neustar.biz

Phone *

5712125364

Role *

AccountAdmin

Save

Cancel

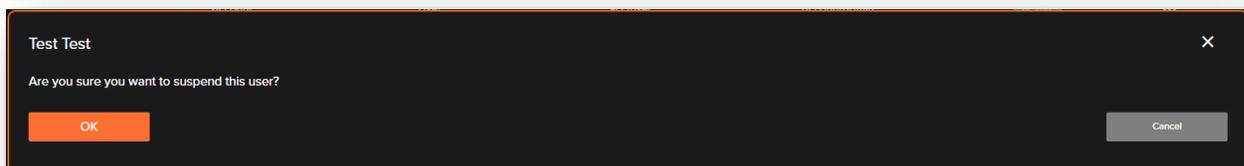
Figure 66 Manage Users - Manage User Details

Suspend a User

To suspend a user, click on the ellipsis for the user and select **Suspend User**.

Confirm the suspension by clicking the **OK** button.

While suspended, a user will not be able to log in to the UltraDNS Firewall Portal.



Test Test

Are you sure you want to suspend this user?

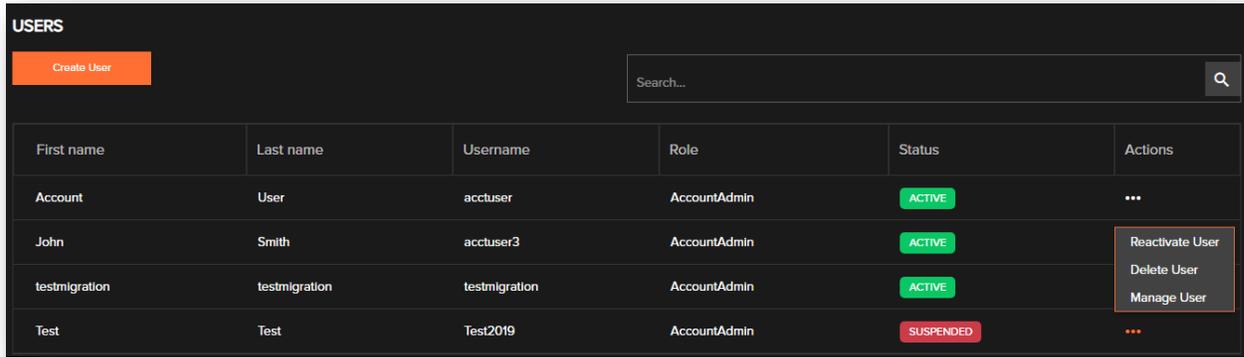
OK

Cancel

Figure 67 Manage Users - Suspend a User

Reactivate a User

Reactivating a user simply means un-suspending them from the UltraDNS Firewall portal. Click on the ellipsis for the user, and select **Reactive User**. Click the **OK** button to confirm the action. The user will immediately be reactivated and able to log back into the portal.



| First name | Last name | Username | Role | Status | Actions |
|---------------|---------------|---------------|--------------|-----------|---|
| Account | User | acctuser | AccountAdmin | ACTIVE | ... |
| John | Smith | acctuser3 | AccountAdmin | ACTIVE | Reactivate User Delete User Manage User |
| testmigration | testmigration | testmigration | AccountAdmin | ACTIVE | ... |
| Test | Test | Test2019 | AccountAdmin | SUSPENDED | ... |

Figure 68 Manage User - Reactive Suspended User

Delete a User

In order to delete a user, the user's status must first display Suspended. To delete a user, click the ellipsis for the user, and then select **Delete User**. Click the **OK** button to confirm the deletion.

Once deleted, the user is permanently removed from the UltraDNS Firewall portal. If you need to re-add the user, follow the *Create User* steps.

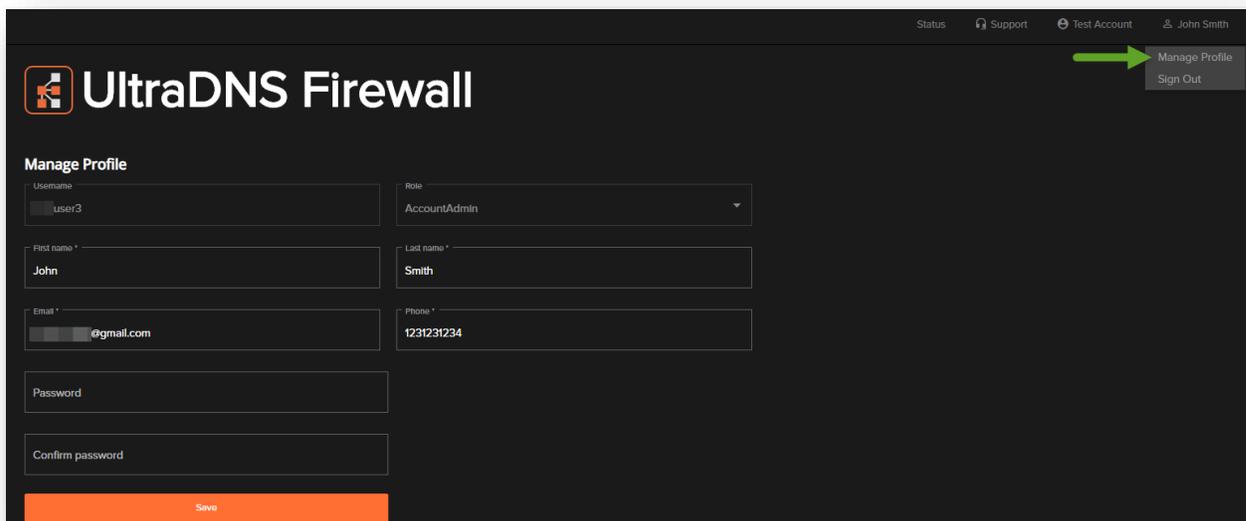
Manage Profile

To view your personal account details, click on your username in the upper right-hand side of your screen, and then click **Manage Profile**.

From the Manage Profile screen, you can:

- View your Username and Role
- Edit your First and Last name
- Edit your Email Address
- Edit your Phone Number
- Change your password

After making any changes, click the **Save** button.



The screenshot shows the 'Manage Profile' interface in the UltraDNS Firewall UI. At the top right, there is a user menu for 'John Smith' with options for 'Manage Profile' (highlighted with a green arrow) and 'Sign Out'. The main content area is titled 'Manage Profile' and contains several input fields: 'Username' (user3), 'Role' (AccountAdmin), 'First name' (John), 'Last name' (Smith), 'Email' (@gmail.com), and 'Phone' (1231231234). Below these are 'Password' and 'Confirm password' fields, and an orange 'Save' button at the bottom.

Figure 69 Manage Profile

Audit

The Audit page provides detailed information for actions and activities that are occurring within a specified Account. These actions can range from the creation of a user in an Account, to updates to a Whitelist domain. Each activity triggers an entry log creation, and each entry displays the following details:

- **UserName**
- **Sponsor**
- **Account**
- **Action**
- **Source**
- **Resource**

The Audit page by default, displays each audit entry per day, unless otherwise specified. You can click the **Load More** option at the bottom of the screen to retrieve additional Audit log entries.

UltraDNS Firewall

Audit Log

Filters

Sponsor: [Dropdown] Username: [Dropdown] Action: [Dropdown] Source: [Dropdown]

Account: [Dropdown] Resource: [Text] From: [Calendar] To: [Calendar]

Cancel Clear Apply

19 September 2019

| | | | | | |
|--------------|-----------|---------------|----------|---------|--------------|
| 20:01:29 UTC | User Name | Arturo Lizano | Action | MODIFY | View Details |
| | Sponsor | N/A | Source | API | |
| | Account | N/A | Resource | SPONSOR | |
| 19:58:34 UTC | User Name | Arturo Lizano | Action | MODIFY | View Details |
| | Sponsor | N/A | Source | API | |
| | Account | N/A | Resource | SPONSOR | |
| 19:51:52 UTC | User Name | Arturo Lizano | Action | MODIFY | View Details |
| | Sponsor | N/A | Source | API | |
| | Account | N/A | Resource | SPONSOR | |
| 19:51:24 UTC | User Name | Arturo Lizano | Action | MODIFY | View Details |
| | Sponsor | N/A | Source | API | |
| | Account | N/A | Resource | SPONSOR | |
| 19:46:57 UTC | User Name | Arturo Lizano | Action | MODIFY | View Details |
| | Sponsor | N/A | Source | API | |
| | Account | N/A | Resource | SPONSOR | |
| 19:42:48 UTC | User Name | Arturo Lizano | Action | MODIFY | View Details |
| | Sponsor | N/A | Source | API | |
| | Account | N/A | Resource | SPONSOR | |
| 17:47:54 UTC | User Name | Arturo Lizano | Action | ADD | View Details |
| | Sponsor | N/A | Source | WEB | |
| | Account | N/A | Resource | Network | |

Figure 70 Audit Log Display

Filters

The Audit filters menu can be opened by clicking the **down arrow** in the filters menu. After selecting your filtering options, click the **Apply** button. The **Clear** button will erase your filtering choices and return you to the main Audit landing page that displays the Audit log entries for the last 24 hours.

The available filtering options are:

- **Username** – Displays the various user's names that are associated to accounts under the Sponsor.
- **Resource**
- **Action** – Select an Action type from the drop-down menu to filter by, or provide a custom Action to search for.
- **From (Date)** – Click on the Calendar icon to select the month and day to start the audit log report for.
 - Use the left and right arrows to change the month, or click the down arrow next to the year to select a new year.
- **Source** - API or Web (portal)
- **To (Date)** - Click on the Calendar icon to select the month and day to end the audit log report.

Use the left and right arrows to change the month, or click the down arrow next to the year to select a new year.

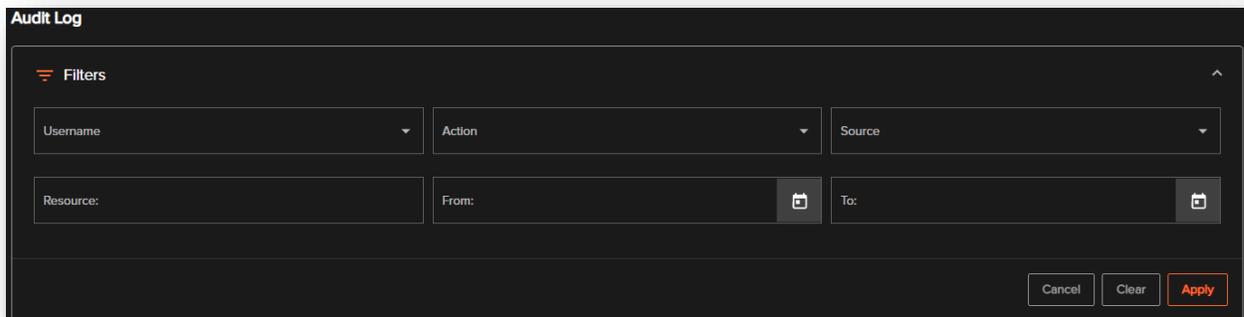


Figure 71 Audit Log – Filters

Each entry in the Audit log contains a **View Details** button that will provide a pop-out summary detail report of the audit log entry.

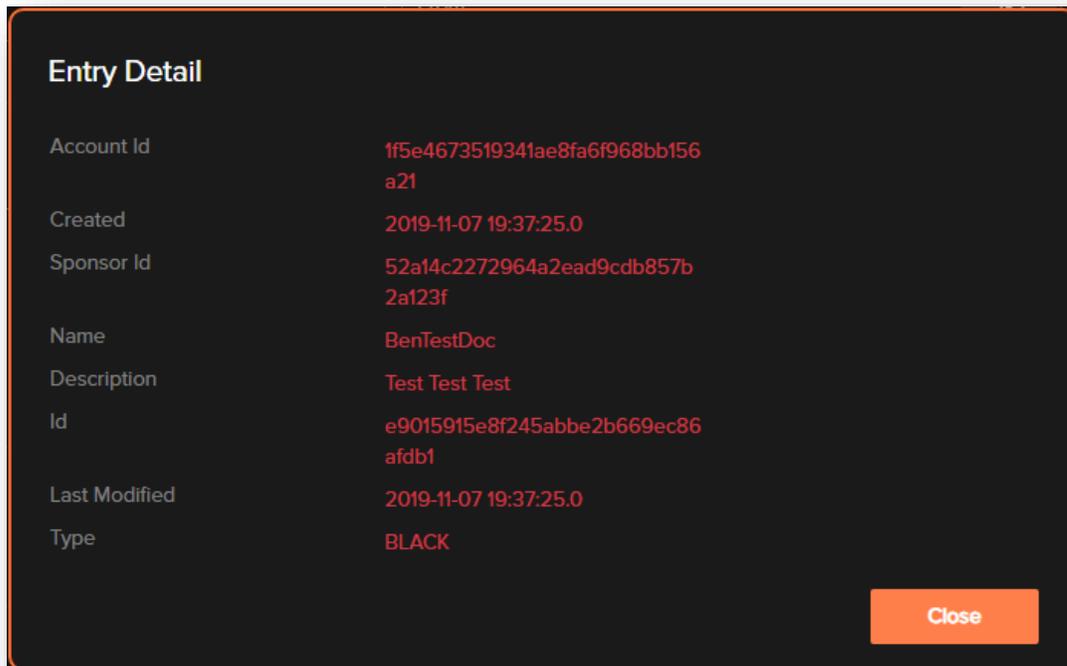


Figure 72 Audit Log - View Details

Your Account type and Role will determine the visibility of Audit Logs displayed on the screen.

Table 1 Audits App - User Role and Privilege Visibility

| Role | Visibility |
|-----------------------------------|--|
| Account Admin Account Reporter | Users are able to see all the CUD ² operations for all the resources under the Account, as well as each User associated to the Account. |

² CUD operations of the resources include: Sponsors, Accounts, Users, VIPs, Subnets, Blacklists, Whitelists, Category Filters, etc.

Support

Clicking on the **Support** link at the top of your screen will take you to our support page, where you can find additional user guides and support material, contact information, as well as a direct link to the Customer Support Portal.



Figure 73 Support Page

Glossary

Table 2 Glossary

| Acronym | Description |
|-----------------------------|---|
| Account | A customer account that uses sponsor-owned virtual addresses to resolve DNS from one or more client subnets. Accounts own the client subnets. Subnets contain individual clients (mostly workstations, laptops or mobile devices used by humans, although there's no restriction). Accounts are usually created under Sponsors, although some may be directly connected to Neustar. |
| Account User | Able to manage client subnets, assign and manage policies, manage black/white lists, and manage client lists. |
| Account Admin User | Administrative users can administer the UltraDNS Firewall system, add sponsors, network announcements, categories, and perform all functions of a Sponsor and Account user. |
| Blacklist | A list of domain names that are always blocked. Queries for names on this list will bypass normal proxy categorization and will be blocked immediately. Blacklists can be specific to a sponsor or account. |
| Category | A reason to block the DNS lookup of a domain name. Examples include: gambling, malware, phishing, kissing, and homosexuality. Additional categories can include travel, software, sports, and government, |
| Category Feed | A set of categories published together. Ideally, all domains on the internet would be found in one (or more) of their categories. In practice, there are more than 300 million domains and many are unlisted. |
| Category Publisher | A company or another institution that maintains and publishes lists of domain names that have been categorized and assembled into Category Feeds. |
| Category Slate | A UI concept that groups one or more categories to be blocked, warned or cleared together as a unit. Often this is thought of as a subset of the categories to be blocked, but a user invoking a slate can also get categories de-selected and leave other categories unchanged. For instance, malware, spyware and phishing might be grouped together as a slate with other security categories into a Security slate. |
| Client Identifier | A unique identifier for an individual client host on an account. This might be a hardware address or some other type of identifier yet to be determined. Client Identifiers are owned by the account. |
| Client Subnet | A non-RFC1918 CIDR block of addresses that belong to an account and will send DNS traffic. Subnets may be in the range /24 - /32 for IPv4 addresses and /64 - /128 for v6 addresses. |
| Network Announcement | An IPv4 or IPv6 network that will be anycasted over BGP from service node locations. Examples: 156.154.70.0/24, 2610:a1:1018::0/48 |
| NXDomain | A DNS error code indicating that a domain does not exist. |

| Acronym | Description |
|---------------------------|--|
| NXDomain Hijacking | The process of suppressing an NXDomain from the DNS resolver and returning the address of a landing page instead of NXDomain. |
| PSA | Professional Services Agreement. A contract for NSR Tech Support. |
| Policy | A composite filter that blocks certain domains from being resolved. A policy consists of a set of enabled categories, a set of blacklists, and a set of whitelists. Domains will be resolved if they are NOT listed in categories or blacklists, or if they are listed in a whitelist. |
| Source Network | Source Networks are used for directing where and how users are routed when they try to navigate to a blocked domain. |
| Whitelist | A list of domain names that are always allowed. Queries for names on this list will bypass the normal proxy categorization process and proceed directly to resolution. Whitelists can be specific to the Sponsor or Account. |